

Primeira Bateria de Questões Com Resolução Assistida

Arquitetura e Organização de
Computadores

Backup & Armazenamento



1. Julgue os itens seguintes, com relação às políticas de becape e recuperação de dados.

[118] O uso de snapshot é ideal como complemento aos becares granulares de arquivos, sendo possível voltar a imagem inteira de um sistema para um ponto anterior no tempo caso o sistema necessite ser restaurado.

[119] Uma das características da solução de becape Symantec NetBackup é a tecnologia de recuperação granular para máquinas virtuais, que permite que o conteúdo dos arquivos seja indexado e restaurado sem que haja necessidade de recuperar toda a máquina virtual.

[120] A técnica de deduplicação de dados na origem, ou seja, quando o becape está sendo realizado, é mais indicada para grandes volumes de dados.

1. Julgue os itens seguintes, com relação às políticas de backup e recuperação de dados.

 [118] O uso de snapshot é ideal como complemento aos backups granulares de arquivos, sendo possível voltar a imagem inteira de um sistema para um ponto anterior no tempo caso o sistema necessite ser restaurado.

 [119] Uma das características da solução de backup Symantec NetBackup é a tecnologia de recuperação granular para máquinas virtuais, que permite que o conteúdo dos arquivos seja indexado e restaurado sem que haja necessidade de recuperar toda a máquina virtual.

 ~~[120] A técnica de deduplicação de dados na origem, ou seja, quando o backup está sendo realizado, é mais indicada para grandes volumes de dados.~~

2. No que se refere a becape e restauração de dados, julgue os próximos itens.

[97] Mesmo com a realização de becares totais e incrementais dos bancos de dados, é possível haver perda de dados em casos de desastres.

[98] O becape total de um banco de dados permite que esse banco seja restaurado a qualquer ponto temporal específico.

2. No que se refere a becape e restauração de dados, julgue os próximos itens.

[97] Mesmo com a realização de becares totais e incrementais dos bancos de dados, é possível haver perda de dados em casos de desastres.

~~[98] O becape total de um banco de dados permite que esse banco seja restaurado a qualquer ponto temporal específico.~~

3. Acerca dos conceitos de armazenamento em disco e de replicação de dados, e de teoria e políticas de cópias de segurança (backups), julgue os itens a seguir.

[108] As cópias de segurança, ou backups, devem ser gravadas e guardadas em local seguro, bem como devem ser testadas periodicamente para certificação de que seu conteúdo é efetivamente recuperável.

[109] O custo de armazenamento de dados em discos rígidos magnéticos ou em discos de estado sólido é muito baixo atualmente. Assim, as soluções de armazenamento em que se utilizam fitas e fitotecas automatizadas tornaram-se obsoletas, visto que estas podem ser completamente substituídas, em qualquer cenário, por soluções de armazenamento em disco.

[110] Uma estratégia de replicação de dados que se baseia em replicação assíncrona tem como vantagens a garantia imediata da consistência dos dados em todas as cópias (réplicas) e a redução do tempo de resposta da confirmação final da transação de atualização.

3. Acerca dos conceitos de armazenamento em disco e de replicação de dados, e de teoria e políticas de cópias de segurança (backups), julgue os itens a seguir.

 [108] As cópias de segurança, ou backups, devem ser gravadas e guardadas em local seguro, bem como devem ser testadas periodicamente para certificação de que seu conteúdo é efetivamente recuperável.

 ~~[109] O custo de armazenamento de dados em discos rígidos magnéticos ou em discos de estado sólido é muito baixo atualmente. Assim, as soluções de armazenamento em que se utilizam fitas e fitotecas automatizadas tornaram-se obsoletas, visto que estas podem ser completamente substituídas, em qualquer cenário, por soluções de armazenamento em disco.~~

 ~~[110] Uma estratégia de replicação de dados que se baseia em replicação assíncrona tem como vantagens a garantia imediata da consistência dos dados em todas as cópias (réplicas) e a redução do tempo de resposta da confirmação final da transação de atualização.~~

4. Acerca dos conceitos de becape e de recuperação de dados, julgue os itens que se seguem.

[118] Os níveis de granularidade de um becape são completo, diferencial e aleatório.

[119] Becaques podem ser realizados para atender a três propósitos distintos: recuperação de desastres, recuperação operacional e arquivamento.

[120] Uma estratégia de becape de um sistema deve ser planejada considerando-se o RPO (recovery point objective e o RTO (response time objective) do negócio suportado pelo sistema.

4. Acerca dos conceitos de becape e de recuperação de dados, julgue os itens que se seguem.

~~[118] Os níveis de granularidade de um becape são completo, diferencial e aleatório.~~



[119] Becaques podem ser realizados para atender a três propósitos distintos: recuperação de desastres, recuperação operacional e arquivamento.



[120] Uma estratégia de becape de um sistema deve ser planejada considerando-se o RPO (recovery point objective e o RTO (response time objective) do negócio suportado pelo sistema.



5. A respeito de becape, assinale a opção correta.
- A. No planejamento de uma política de becape, deve-se considerar a verificação da periodicidade e da quantidade de dados a serem armazenados.
 - B. A realização periódica de teste de restauração não é considerada uma boa prática de becape, ainda que os dados estejam armazenados em fitas.
 - C. Na medição do desempenho do becape, não se deve considerar a mídia utilizada.
 - D. Não é recomendado que se utilizem discos rígidos para armazenar becares.
 - E. Os dispositivos ópticos são os melhores hardware disponíveis para a gravação de cópias de segurança no caso de ser necessário o armazenamento de grandes volumes de dados.

5. A respeito de becape, assinale a opção correta.

-  A. No planejamento de uma política de becape, deve-se considerar a verificação da periodicidade e da quantidade de dados a serem armazenados.
- B. A realização periódica de teste de restauração não é considerada uma boa prática de becape, ainda que os dados estejam armazenados em fitas.
- C. Na medição do desempenho do becape, não se deve considerar a mídia utilizada.
- D. Não é recomendado que se utilizem discos rígidos para armazenar becares.
- E. Os dispositivos ópticos são os melhores hardware disponíveis para a gravação de cópias de segurança no caso de ser necessário o armazenamento de grandes volumes de dados.

GABARITO



1. C, C, E

2. C, E

3. C, E, E

4. E, C, C

5. A

Primeira Bateria de Questões Com Resolução Assistida

Segurança em redes de computadores
Prevenção e tratamento de incidentes

1. No tocante a protocolos, serviços, padrões e topologias de redes, julgue os itens subsequentes.

[101] A topologia lógica de interconexão de uma rede corporativa complexa precisa refletir a topologia física dessa rede, de modo que os requisitos de segurança lógica da rede sejam de implementação direta a partir dos aspectos da segurança física das instalações de TI da organização.

1. No tocante a protocolos, serviços, padrões e topologias de redes, julgue os itens subsequentes.

 ~~[101] A topologia lógica de interconexão de uma rede corporativa complexa precisa refletir a topologia física dessa rede, de modo que os requisitos de segurança lógica da rede sejam de implementação direta a partir dos aspectos da segurança física das instalações de TI da organização.~~

2. Com relação à segurança em redes de computadores, julgue os itens subsequentes.

[158] Uma das fases do processo de tratamento e resposta a incidentes de segurança em redes de computadores é a preparação, na qual são sanitizadas mídias para armazenamento e confeccionados kits de ferramentas em meio read-only.

[160] VPNs implementam redes seguras a fim de prover confidencialidade, integridade e autenticidade em canais públicos compartilhados.

2. Com relação à segurança em redes de computadores, julgue os itens subsequentes.

 [158] Uma das fases do processo de tratamento e resposta a incidentes de segurança em redes de computadores é a preparação, na qual são sanitizadas mídias para armazenamento e confeccionados kits de ferramentas em meio read-only.

 [160] VPNs implementam redes seguras a fim de prover confidencialidade, integridade e autenticidade em canais públicos compartilhados.

3. Julgue os seguintes itens, relativos à segurança em redes de computadores.

- [96] O uso de criptografia SSL (Secure Socket Layer) como item de segurança nas transmissões de dados via Internet dificulta o monitoramento realizado por sistemas de detecção de intrusos (IDS) de redes. Uma solução para esse problema é o uso de proxies reversos, que permite retirar o processo de criptografia do servidor web e, conseqüentemente, possibilita ao IDS o monitoramento do tráfego.
- [97] A captura de quadros de redes wireless IEEE 802.11 geralmente não é alcançada com o uso do modo promíscuo da interface de rede, sendo necessário configurar a interface de rede para o modo de monitoramento (monitor mode). Além disso, pode haver restrições por parte do sistema operacional, como ocorre no Windows, o que impede a captura de quadros desse tipo.
- [98] O WIPS (Wireless Intrusion Prevention System) é um dispositivo que monitora o espectro de ondas de rádio, buscando identificar a presença de pontos de acesso não autorizados. Ao detectar a presença de sinais de rádio não autorizados, o WIPS pode enviar alerta ao administrador ou ao firewall da rede para prevenir possíveis ataques.

3. Julgue os seguintes itens, relativos à segurança em redes de computadores.

 [96] O uso de criptografia SSL (Secure Socket Layer) como item de segurança nas transmissões de dados via Internet dificulta o monitoramento realizado por sistemas de detecção de intrusos (IDS) de redes. Uma solução para esse problema é o uso de proxies reversos, que permite retirar o processo de criptografia do servidor web e, conseqüentemente, possibilita ao IDS o monitoramento do tráfego.

 [97] A captura de quadros de redes wireless IEEE 802.11 geralmente não é alcançada com o uso do modo promíscuo da interface de rede, sendo necessário configurar a interface de rede para o modo de monitoramento (monitor mode). Além disso, pode haver restrições por parte do sistema operacional, como ocorre no Windows, o que impede a captura de quadros desse tipo.

 [98] O WIPS (Wireless Intrusion Prevention System) é um dispositivo que monitora o espectro de ondas de rádio, buscando identificar a presença de pontos de acesso não autorizados. Ao detectar a presença de sinais de rádio não autorizados, o WIPS pode enviar alerta ao administrador ou ao firewall da rede para prevenir possíveis ataques.

4. Julgue os seguintes itens, relativos à segurança em redes de computadores.

[101] Traffic shaping é uma prática que tem sido adotada por empresas de telefonia e provedoras de acesso à Internet que, apesar de ser considerada abusiva por parte de órgãos de defesa do consumidor, geralmente é utilizada para otimizar o uso da largura de banda disponível, restringindo a banda para serviços que demandam a transferência de grande volume de dados, como P2P e FTP.

4. Julgue os seguintes itens, relativos à segurança em redes de computadores.

[101] Traffic shaping é uma prática que tem sido adotada por empresas de telefonia e provedoras de acesso à Internet que, apesar de ser considerada abusiva por parte de órgãos de defesa do consumidor, geralmente é utilizada para otimizar o uso da largura de banda disponível, restringindo a banda para serviços que demandam a transferência de grande volume de dados, como P2P e FTP.



5. Com relação à segurança em redes de computadores, julgue os itens que se seguem.

[83] Os bots são programas maliciosos armazenados na área de boot do disco de uma estação de trabalho. Eles são capazes de se reproduzir, de modo que o invasor consegue orientar o bot a realizar ataques em um ambiente em rede.

[84] Para segurança dos programas e dos sistemas, é comum as organizações armazenarem informações denominadas accounting, que identificam o responsável pelo processamento, o nome do programa, o tipo de processamento, a área de execução, a periodicidade, a prioridade, o tempo estimado, entre outros.

5. Com relação à segurança em redes de computadores, julgue os itens que se seguem.

 ~~[83] Os bots são programas maliciosos armazenados na área de boot do disco de uma estação de trabalho. Eles são capazes de se reproduzir, de modo que o invasor consegue orientar o bot a realizar ataques em um ambiente em rede.~~

 [84] Para segurança dos programas e dos sistemas, é comum as organizações armazenarem informações denominadas accounting, que identificam o responsável pelo processamento, o nome do programa, o tipo de processamento, a área de execução, a periodicidade, a prioridade, o tempo estimado, entre outros.

6. Considerando os conceitos de segurança em redes de comunicações, julgue os itens seguintes.

[106] Uma das vantagens da detecção de intrusão baseada em anomalias é a eficiência na detecção, comparativamente à detecção baseada em assinaturas, uma vez que não gera grande número de alarmes falsos.

[107] Com o filtro de pacotes de um roteador, um conjunto restrito de usuários internos pode receber, ao invés de endereços IP, o serviço Telnet, devendo esses usuários, se autenticarem antes de obter permissão para criar sessões Telnet com computadores externos.

6. Considerando os conceitos de segurança em redes de comunicações, julgue os itens seguintes.

 ~~[106] Uma das vantagens da detecção de intrusão baseada em anomalias é a eficiência na detecção, comparativamente à detecção baseada em assinaturas, uma vez que não gera grande número de alarmes falsos.~~

 ~~[107] Com o filtro de pacotes de um roteador, um conjunto restrito de usuários internos pode receber, ao invés de endereços IP, o serviço Telnet, devendo esses usuários, se autenticarem antes de obter permissão para criar sessões Telnet com computadores externos.~~

7. No que se refere à segurança em redes de computadores, julgue os itens a seguir.

[109] São dispositivos constitucionais relacionados com a segurança dos sistemas de informação em organizações públicas brasileiras: o direito à privacidade, que define a aplicação do sigilo das informações relacionadas à intimidade ou vida privada de alguém; o direito à informação e ao acesso aos registros públicos; o dever do estado de proteger documentos e obras; e o dever do estado de promover a gestão documental.

[111] Envenenamento ARP (ARP poisoning), SYN flooding attack e roubo de sessão TCP (TCP session hijacking) são tipos de ataque que estações pertencentes a uma rede IPv4 podem sofrer. Esses três tipos podem ser usados para produzir negação de serviço, com a diferença de que, para realizar o primeiro, o host atacante deve estar fisicamente localizado no mesmo segmento do host atacado, enquanto os dois últimos podem ser efetuados por meio da Internet.

7. No que se refere à segurança em redes de computadores, julgue os itens a seguir.

[109] São dispositivos constitucionais relacionados com a segurança dos sistemas de informação em organizações públicas brasileiras: o direito à privacidade, que define a aplicação do sigilo das informações relacionadas à intimidade ou vida privada de alguém; o direito à informação e ao acesso aos registros públicos; o dever do estado de proteger documentos e obras; e o dever do estado de promover a gestão documental.

[111] Envenenamento ARP (ARP poisoning), SYN flooding attack e roubo de sessão TCP (TCP session hijacking) são tipos de ataque que estações pertencentes a uma rede IPv4 podem sofrer. Esses três tipos podem ser usados para produzir negação de serviço, com a diferença de que, para realizar o primeiro, o host atacante deve estar fisicamente localizado no mesmo segmento do host atacado, enquanto os dois últimos podem ser efetuados por meio da Internet.

8. No que se refere à segurança em redes de computadores, julgue os itens a seguir.

[112] Os processos de definição, implantação e gestão de políticas de segurança da informação devem ser aprovados pelo pessoal de nível operacional e devem se subordinar às normas e procedimentos de segurança vigentes na organização.

[113] Se a segurança demandada por uma comunicação referir-se apenas à integridade das mensagens, é adequado o uso de hashes criptográficos, o que, além do mais, não apresenta o inconveniente da complexidade técnico-operacional que caracteriza o gerenciamento de chaves.

[114] Protetor contra surtos elétricos, sanitização de entrada de dados, proteção de memória, firewall de aplicação, controle de acesso com base em papéis, firewall statefull, verificação de antecedentes e sensores de fumaça são, respectivamente, meios de proteção contra ataques relativos a hardware, software, sistemas operacionais, aplicações, bancos de dados, redes, pessoas e ambiente físico.

8. No que se refere à segurança em redes de computadores, julgue os itens a seguir.

~~[112] Os processos de definição, implantação e gestão de políticas de segurança da informação devem ser aprovados pelo pessoal de nível operacional e devem se subordinar às normas e procedimentos de segurança vigentes na organização.~~



[113] Se a segurança demandada por uma comunicação referir-se apenas à integridade das mensagens, é adequado o uso de hashes criptográficos, o que, além do mais, não apresenta o inconveniente da complexidade técnico-operacional que caracteriza o gerenciamento de chaves.



[114] Protetor contra surtos elétricos, sanitização de entrada de dados, proteção de memória, firewall de aplicação, controle de acesso com base em papéis, firewall statefull, verificação de antecedentes e sensores de fumaça são, respectivamente, meios de proteção contra ataques relativos a hardware, software, sistemas operacionais, aplicações, bancos de dados, redes, pessoas e ambiente físico.



9. Acerca de prevenção e tratamento a ataques a redes de computadores, julgue os itens subsecutivos.

[118] O processo de tratamento e de resposta a incidentes de segurança da informação é independente da política de continuidade de negócio.

[119] Ataques de negação de serviço volumétricos são prevenidos de maneira eficaz por filtros orientados a conteúdo.

[120] Ataques de buffer overflow não são evitados com a inspeção de cabeçalhos.

9. Acerca de prevenção e tratamento a ataques a redes de computadores, julgue os itens subsecutivos.

 ~~[118] O processo de tratamento e de resposta a incidentes de segurança da informação é independente da política de continuidade de negócio.~~

 ~~[119] Ataques de negação de serviço volumétricos são prevenidos de maneira eficaz por filtros orientados a conteúdo.~~

 [120] Ataques de buffer overflow não são evitados com a inspeção de cabeçalhos.

10. A respeito de ataques a redes de computadores, prevenção e tratamento de incidentes, julgue os itens subsecutivos

[108] Responsabilidades e procedimentos de gestão devem ser estabelecidos para assegurar respostas rápidas, efetivas e ordenadas a incidente de segurança da informação.

[110] Nos casos em que uma ação de acompanhamento contra uma pessoa ou organização, após um incidente de segurança da informação, envolver uma ação legal (civil ou criminal), evidências devem ser coletadas, armazenadas e apresentadas em conformidade com as normas de armazenamento de evidências da jurisdição ou jurisdições pertinentes.

10. A respeito de ataques a redes de computadores, prevenção e tratamento de incidentes, julgue os itens subsecutivos

[108] Responsabilidades e procedimentos de gestão devem ser estabelecidos para assegurar respostas rápidas, efetivas e ordenadas a incidente de segurança da informação.

[110] Nos casos em que uma ação de acompanhamento contra uma pessoa ou organização, após um incidente de segurança da informação, envolver uma ação legal (civil ou criminal), evidências devem ser coletadas, armazenadas e apresentadas em conformidade com as normas de armazenamento de evidências da jurisdição ou jurisdições pertinentes.

GABARITO



1. E

2. C, C,

3. C, C, C

4. C

5. E, C

6. E, E

7. C, C

8. E, C, C

9. E, E, C

10. C, C

Segunda Bateria de Questões Com Resolução Assistida

Arquitetura e Organização de
Computadores

Backup & Armazenamento



1. Com base em serviços de armazenamento e tecnologias de backup, julgue os itens subsecutivos.

[107] A deduplicação consiste na realização de backups incrementais, nos quais são copiados somente os arquivos criados ou alterados desde o último backup normal ou incremental. Nesse tipo de técnica, os arquivos de backups são compactados antes de ser enviados à mídia de armazenamento, o que reduz o espaço necessário para armazenar os dados.

1. Com base em serviços de armazenamento e tecnologias de backup, julgue os itens subsecutivos.

~~[107] A deduplicação consiste na realização de backups incrementais, nos quais são copiados somente os arquivos criados ou alterados desde o último backup normal ou incremental. Nesse tipo de técnica, os arquivos de backups são compactados antes de ser enviados à mídia de armazenamento, o que reduz o espaço necessário para armazenar os dados.~~



2. Para que os dados mais importantes salvos em meio digital estejam protegidos contra perdas, é necessário estabelecer políticas, processos e procedimentos para a realização de cópias de segurança. Com relação a esse tema, julgue os itens que se seguem.

[82] Mediante o backup incremental, realiza-se a cópia apenas dos arquivos criados ou alterados após o último backup.

[83] A mesa de trabalho do administrador do ambiente operacional, é o local adequado para o armazenamento das cópias de segurança dos dados feitas em fitas, uma vez que, em caso de desastre, é fundamental a restauração rápida desses dados.

[84] É dispensável a realização de backup normal por organização que executa backup incremental armazenado em fitas, uma vez que a velocidade de recuperação deste backup é maior, dada a menor quantidade de dados a serem restaurados.

[85] Caso uma organização opte por soluções de software livre para a realização de backup de sua rede de dados, ela poderá utilizar tanto o Bacula quanto o NMIS, visto que ambos os softwares apresentam as mesmas funcionalidades.

2. Para que os dados mais importantes salvos em meio digital estejam protegidos contra perdas, é necessário estabelecer políticas, processos e procedimentos para a realização de cópias de segurança. Com relação a esse tema, julgue os itens que se seguem.



[82] Mediante o backup incremental, realiza-se a cópia apenas dos arquivos criados ou alterados após o último backup.



~~[83] A mesa de trabalho do administrador do ambiente operacional, é o local adequado para o armazenamento das cópias de segurança dos dados feitas em fitas, uma vez que, em caso de desastre, é fundamental a restauração rápida desses dados.~~



~~[84] É dispensável a realização de backup normal por organização que executa backup incremental armazenado em fitas, uma vez que a velocidade de recuperação deste backup é maior, dada a menor quantidade de dados a serem restaurados.~~



~~[85] Caso uma organização opte por soluções de software livre para a realização de backup de sua rede de dados, ela poderá utilizar tanto o Bacula quanto o NMIS, visto que ambos os softwares apresentam as mesmas funcionalidades.~~

3. No que diz respeito à desduplicação, julgue o item abaixo.

[85] A desduplicação de dados é uma técnica de becape que gerencia o crescimento explosivo de dados, fornece proteção e elimina dados redundantes do armazenamento, salvando uma única cópia dos dados idênticos e substituindo todas as outras por referência para essa cópia.

3. No que diz respeito à desduplicação, julgue o item abaixo.

[85] A desduplicação de dados é uma técnica de becape que gerencia o crescimento explosivo de dados, fornece proteção e elimina dados redundantes do armazenamento, salvando uma única cópia dos dados idênticos e substituindo todas as outras por referência para essa cópia.



4. Julgue o item que se segue, relativo às cópias de segurança.

[86] Tanto o becape incremental, quanto o diferencial copiam arquivos criados ou alterados desde o último becape normal, e o becape incremental não desmarca o atributo de arquivo.

4. Julgue o item que se segue, relativo às cópias de segurança.

 ~~[86] Tanto o backup incremental, quanto o diferencial copiam arquivos criados ou alterados desde o último backup normal, e o backup incremental não desmarca o atributo de arquivo.~~

5. A respeito de backup e restore, julgue os itens seguintes.

[61] Considere que, em uma empresa, seja realizado backup de segunda-feira a sexta-feira. Considere, ainda, que seja executado backup completo na segunda-feira e que sejam executados backups do tipo incremental de terça-feira a sexta-feira. Nessa situação, o backup realizado na quinta-feira não contemplará os dados do backup realizado na segunda-feira, mas contemplará os dados que foram modificados na quinta-feira.

[62] Se, na realização de backup completo do servidor de uma rede de computadores, o tamanho total dos dados for igual a 1,9 TB, não havendo nenhuma compressão, então, para atender a essa demanda, deve-se utilizar uma fita LTO2.

Atributo	Geração					
	LTO-1	LTO-2	LTO-3	LTO-4	LTO-5	LTO-6
Data de lançamento	2000	2003	2005	2007	2010	2012
Capacidade nativa de dados	100 GB	200 GB	400 GB	800 GB	1.5 TB	2.5 TB
Velocidade Max (MB/s)	20	40	80	120	140	160
Capacidade WORM?	Não	Não	Sim	Sim	Sim	Sim
Capacidade de encriptação?	Não	Não	Não	Sim	Sim	Sim
Espessura da fita	8,9 µm	8,9 µm	8,0 µm	6,6 µm	6,4 µm	6,1 µm
Tamanho da fita	609 m	609 m	680 m	820 m	846 m	846 m
Trilhas	384	512	704	896	1280	2176
Elementos de escrita	8	8	16	16	16	16
Voltas por banda	12	16	11	14	20	34
Densidade linear (bits/mm)	4880	7398	9638	13250	15142	15143 ^[3]
Codificação	RLL 1,7	PRML	PRML	PRML		

5. A respeito de backup e restore, julgue os itens seguintes.

 [61] Considere que, em uma empresa, seja realizado backup de segunda-feira a sexta-feira. Considere, ainda, que seja executado backup completo na segunda-feira e que sejam executados backups do tipo incremental de terça-feira a sexta-feira. Nessa situação, o backup realizado na quinta-feira não contemplará os dados do backup realizado na segunda-feira, mas contemplará os dados que foram modificados na quinta-feira.

 ~~[62] Se, na realização de backup completo do servidor de uma rede de computadores, o tamanho total dos dados for igual a 1,9 TB, não havendo nenhuma compressão, então, para atender a essa demanda, deve-se utilizar uma fita LTO2.~~

GABARITO



1. E

2. C, E, E, E

3. C

4. E

5. C, E

Segunda Bateria de Questões Com Resolução Assistida

Dispositivos de segurança:

FIREWALL, IDS, IPS

1. Acerca de controle de acesso e certificação digital, julgue os itens a seguir.

[76] Um dispositivo do tipo IDS (intrusion detection system) atua com proatividade, prevendo ataques e antecipando-se a explorações de vulnerabilidades, a partir de assinaturas frequentemente atualizadas

1. Acerca de controle de acesso e certificação digital, julgue os itens a seguir.

~~[76] Um dispositivo do tipo IDS (intrusion detection system) atua com proatividade, prevenindo ataques e antecipando-se a explorações de vulnerabilidades, a partir de assinaturas frequentemente atualizadas~~



2. Acerca das características e dos processos de mitigação de um ataque de negação de serviço distribuído, julgue os itens subsequentes.

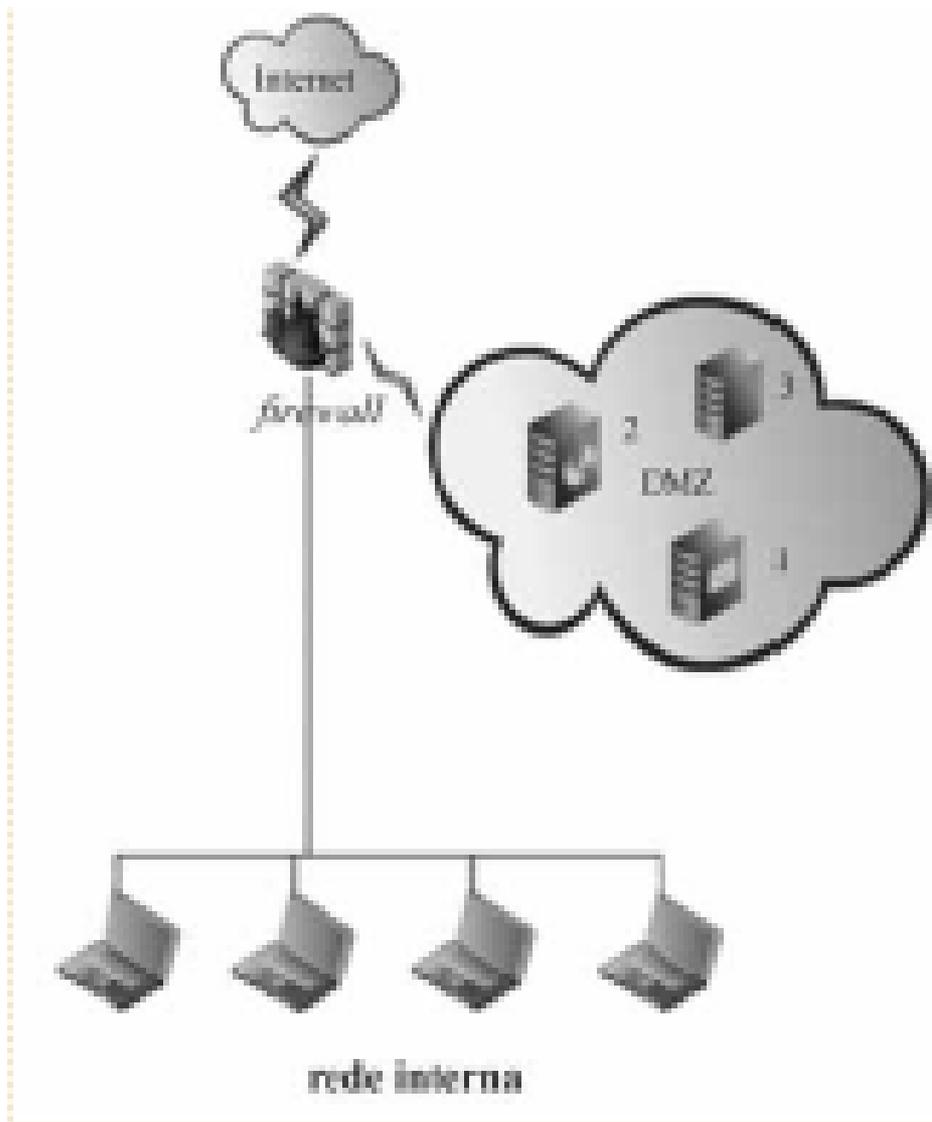
[84] Ataques de negação de serviço distribuído com base em HTTP devem ser mitigados em firewall de camada de aplicação. Nesse caso, se for utilizado o protocolo HTTPS, a mitigação não será possível porque os dados trafegados são cifrados.

[85] Um DDoS com base em ICMP será efetivo somente se for realizado no protocolo IPv4, uma vez que, em IPv6, o uso de ICMP é restrito para interface de loopback.

2. Acerca das características e dos processos de mitigação de um ataque de negação de serviço distribuído, julgue os itens subsequentes.

 ~~[84] Ataques de negação de serviço distribuído com base em HTTP devem ser mitigados em firewall de camada de aplicação. Nesse caso, se for utilizado o protocolo HTTPS, a mitigação não será possível porque os dados trafegados são cifrados.~~

 ~~[85] Um DDoS com base em ICMP será efetivo somente se for realizado no protocolo IPv4, uma vez que, em IPv6, o uso de ICMP é restrito para interface de loopback.~~



3. Considerado a figura acima, que representa a topologia simplificada da rede de dados de uma organização, julgue os itens a seguir.

[78] Se um IPS (intrusion prevention system) for instalado logo acima do firewall, haverá um ganho de segurança, visto que esse sistema poderá ser baseado em assinaturas de ataques e terá capacidade para bloquear possíveis ameaças.

[79] O firewall representado é um sistema que isola áreas distintas da rede de dados e que delimita os domínios de confiança.

[80] Qualquer usuário conectado à Internet pode acessar o servidor 2 da DMZ na porta 80, pois não foram implementadas políticas específicas para essa rede, que consiste em uma zona desmilitarizada.

[81] Como o servidor 1 está na DMZ, que, por definição, não tem controle de acesso, não será possível ao usuário da rede interna acessar e encaminhar uma mensagem eletrônica assinada com base em um algoritmo de criptografia de chaves públicas.

3. Considerado a figura acima, que representa a topologia simplificada da rede de dados de uma organização, julgue os itens a seguir.

[78] Se um IPS (intrusion prevention system) for instalado logo acima do



firewall, haverá um ganho de segurança, visto que esse sistema poderá ser baseado em assinaturas de ataques e terá capacidade para bloquear possíveis ameaças.

[79] O firewall representado é um sistema que isola áreas distintas da rede de dados e que delimita os domínios de confiança.



~~80] Qualquer usuário conectado à Internet pode acessar o servidor 2 da DMZ na porta 80, pois não foram implementadas políticas específicas para essa rede, que consiste em uma zona desmilitarizada.~~



~~81] Como o servidor 1 está na DMZ, que, por definição, não tem controle de acesso, não será possível ao usuário da rede interna acessar e encaminhar uma mensagem eletrônica assinada com base em um algoritmo de criptografia de chaves públicas.~~

4. Acerca de firewall, assinale a opção correta.

- A. Apesar de serem dependentes de aplicativos e de ignorar os endereços IPs, os firewalls de filtragem de pacotes são mais seguros em comparação com os do tipo proxy.
- B. Além de controlar e conectar o tráfego entre redes, um firewall pode criar redes privadas virtuais (VPN), suportar varreduras de vírus no correio eletrônico e filtrar aplicativos para bloquear acesso não autorizado aos aplicativos remotos.
- C. Em comparação com um firewall de filtragem de pacotes, os aplicativos de firewall e de proxy são mais rápidos, mais baratos e suportam o protocolo UDP.
- D. Os firewalls do tipo filtragem de pacotes são voltados para tratamento de códigos maliciosos, como, por exemplo, cavalos de troia.
- E. Os firewalls do tipo inspeção de pacotes com informação de estado funcionam nas camadas de 3 a 7 para proteção e tratamento de vírus de rede.

4. Acerca de firewall, assinale a opção correta.

- A. Apesar de serem dependentes de aplicativos e de ignorar os endereços IPs, os firewalls de filtragem de pacotes são mais seguros em comparação com os do tipo proxy.
-  B. Além de controlar e conectar o tráfego entre redes, um firewall pode criar redes privadas virtuais (VPN), suportar varreduras de vírus no correio eletrônico e filtrar aplicativos para bloquear acesso não autorizado aos aplicativos remotos.
- C. Em comparação com um firewall de filtragem de pacotes, os aplicativos de firewall e de proxy são mais rápidos, mais baratos e suportam o protocolo UDP.
- D. Os firewalls do tipo filtragem de pacotes são voltados para tratamento de códigos maliciosos, como, por exemplo, cavalos de troia.
- E. Os firewalls do tipo inspeção de pacotes com informação de estado funcionam nas camadas de 3 a 7 para proteção e tratamento de vírus de rede.

5. Acerca de proteção de estações de trabalho, julgue os próximos itens.

[89] Se o firewall pessoal estiver habilitado na estação de trabalho, ele será capaz de bloquear o tráfego de rede com destino final à estação de trabalho ao ser direcionado a uma porta específica.

[90] Entre as ações que integram o processo de hardening incluem-se desinstalar softwares desnecessários para o cotidiano do usuário na estação de trabalho e instalar antispysware

5. Acerca de proteção de estações de trabalho, julgue os próximos itens.

 [89] Se o firewall pessoal estiver habilitado na estação de trabalho, ele será capaz de bloquear o tráfego de rede com destino final à estação de trabalho ao ser direcionado a uma porta específica.

 [90] Entre as ações que integram o processo de hardening incluem-se desinstalar softwares desnecessários para o cotidiano do usuário na estação de trabalho e instalar antispysware

6. Julgue os itens seguintes, acerca de VPN e VPN-SSL.

[87] Quando se utiliza um firewall com funções de VPN, as mensagens entram cifradas na rede e somente são decifradas no nível de aplicação.

6. Julgue os itens seguintes, acerca de VPN e VPN-SSL.

~~[87] Quando se utiliza um firewall com funções de VPN, as mensagens entram cifradas na rede e somente são decifradas no nível de aplicação.~~



7. Assinale a opção em que são apresentadas as características genéricas de um firewall.
- A. Validar select executado por uma aplicação web em um banco de dados DB2.
 - B. Permitir acesso a um sistema e a análise de ataques por meio de estatísticas de anomalia relacionadas aos comportamentos dos usuários.
 - C. Analisar switches defeituosos na rede de computadores.
 - D. Capacidade para concentrar e filtrar os acessos dial-in à rede e suportar a funcionalidade de proxy para serviços FTP.
 - E. Criptografar os dados de uma aplicação de intranet na rede interna

7. Assinale a opção em que são apresentadas as características genéricas de um firewall.

- A. Validar select executado por uma aplicação web em um banco de dados DB2.
- B. Permitir acesso a um sistema e a análise de ataques por meio de estatísticas de anomalia relacionadas aos comportamentos dos usuários.
- C. Analisar switches defeituosos na rede de computadores.
-  D. Capacidade para concentrar e filtrar os acessos dial-in à rede e suportar a funcionalidade de proxy para serviços FTP.
- E. Criptografar os dados de uma aplicação de intranet na rede interna

GABARITO



1. E

6. E

2. E, E

7. D

3. C, C, E, E

4. B

5. C, C

Terceira Bateria de Questões Com Resolução Assistida

Arquitetura e Organização de
Computadores

Backup & Armazenamento



1. Acerca de uma política de becape determinada para ocorrer em dias úteis, de segunda a sexta-feira, julgue os itens seguintes.

[94] A restauração completa de um sistema levará mais tempo com o uso do becape diferencial que com o do becape completo.

[95] Se for executado, na segunda-feira, um becape completo e, nos outros dias em que a política ocorre, for feito becape diferencial, então um arquivo criado na terça-feira será incluído somente em um dos becares.

[96] O becape incremental requer o uso de maior espaço para armazenamento que o becape diferencial.

1. Acerca de uma política de becape determinada para ocorrer em dias úteis, de segunda a sexta-feira, julgue os itens seguintes.

 [94] A restauração completa de um sistema levará mais tempo com o uso do becape diferencial que com o do becape completo.

 ~~[95] Se for executado, na segunda-feira, um becape completo e, nos outros dias em que a política ocorre, for feito becape diferencial, então um arquivo criado na terça-feira será incluído somente em um dos becapes.~~

 ~~[96] O becape incremental requer o uso de maior espaço para armazenamento que o becape diferencial.~~

2. A respeito de teoria e políticas de backup e recuperação de dados, julgue os itens subsecutivos.

[115] A recuperação operacional visa restaurar dados perdidos durante tarefas de processamento rotineiro, como arquivos deletados acidentalmente ou corrupção de arquivos.

[116] O arquivamento é utilizado para preservação a longo prazo de informações.

[117] Os requisitos de RPO e RTO são adotados pelas organizações ao definir as estratégias de proteção de dados para a realização do arquivamento.

2. A respeito de teoria e políticas de backup e recuperação de dados, julgue os itens subsecutivos.

 [115] A recuperação operacional visa restaurar dados perdidos durante tarefas de processamento rotineiro, como arquivos deletados acidentalmente ou corrupção de arquivos.

 [116] O arquivamento é utilizado para preservação a longo prazo de informações.

 ~~[117] Os requisitos de RPO e RTO são adotados pelas organizações ao definir as estratégias de proteção de dados para a realização do arquivamento.~~

3. A respeito de teoria e políticas de becape e recuperação de dados, julgue os itens subsecutivos.

[118] Becaпе completo, incremental e cumulativo são estratégias que definem o nível de granularidade do backup e só podem ser utilizados de forma exclusiva.

[119] A recuperação de desastres visa a restauração dos dados em um local alternativo no caso de incapacidade do local de origem devido a um desastre.

[120] Becaпе quente e frio são métodos utilizados em equipamentos com e sem refrigeração, respectivamente.

3. A respeito de teoria e políticas de becape e recuperação de dados, julgue os itens subsecutivos.

 ~~[118] Bepape completo, incremental e cumulativo são estratégias que definem o nível de granularidade do backup e só podem ser utilizados de forma exclusiva.~~

 [119] A recuperação de desastres visa a restauração dos dados em um local alternativo no caso de incapacidade do local de origem devido a um desastre.

 ~~[120] Bepape quente e frio são métodos utilizados em equipamentos com e sem refrigeração, respectivamente.~~

4. Com relação a sistemas de replicação de dados e conceitos de becape e recuperação de dados, julgue os próximos itens

[119] Replicação de dados é uma técnica de armazenamento de dados para manter automaticamente a disponibilidade dos dados, a despeito das falhas do servidor.

[120] Para recuperar um sistema em que eram feitos ciclos de becape compostos por becape normal e becares incrementais, deve-se usar o último incremental, que conterà todos os dados.

4. Com relação a sistemas de replicação de dados e conceitos de backup e recuperação de dados, julgue os próximos itens

[119] Replicação de dados é uma técnica de armazenamento de dados para manter automaticamente a disponibilidade dos dados, a despeito das falhas do servidor.

~~[120] Para recuperar um sistema em que eram feitos ciclos de backup compostos por backup normal e backups incrementais, deve-se usar o último incremental, que conterà todos os dados.~~

5. Julgue os itens subsequentes, acerca de procedimentos de backup

- [107] Nos casos em que haja necessidade de recuperação de dados com grande rapidez, recomenda-se que o backup seja realizado na mesma mídia em que estejam armazenados os dados originais.
- [108] Apesar de terem um alto custo, os backups completos são os únicos que garantem a recuperação total dos dados em caso de incidentes.
- [109] Com o uso de backups incrementais a recuperação de um determinado arquivo muitas vezes exige a busca em vários arquivos de backup.
- [110] Em um ambiente em que haja alterações frequentes dos dados armazenados, em geral, os backups diferenciais são menos eficientes do que os backups referenciais.

5. Julgue os itens subsequentes, acerca de procedimentos de backup

~~[107] Nos casos em que haja necessidade de recuperação de dados com grande rapidez, recomenda-se que o backup seja realizado na mesma mídia em que estejam armazenados os dados originais.~~



~~[108] Apesar de terem um alto custo, os backups completos são os únicos que garantem a recuperação total dos dados em caso de incidentes.~~



[109] Com o uso de backups incrementais a recuperação de um determinado arquivo muitas vezes exige a busca em vários arquivos de backup.



[110] Em um ambiente em que haja alterações frequentes dos dados armazenados, em geral, os backups diferenciais são menos eficientes do que os backups referenciais.



6. Julgue os itens subsequentes, acerca de procedimentos de backup

[111] A implantação de procedimentos de backup garante a recuperação de todos os dados em caso de desastre, assegurando a disponibilidade dos dados com suas últimas atualizações.

[112] Para que a efetividade dos procedimentos de backup seja garantida, é necessário que os procedimentos de recuperação de dados sejam regularmente testados.

[113] Para garantir a preservação dos dados em situação de desastre, é suficiente, para qualquer caso, a realização de backup dos dados uma vez ao dia.

6. Julgue os itens subsequentes, acerca de procedimentos de backup

 ~~[111] A implantação de procedimentos de backup garante a recuperação de todos os dados em caso de desastre, assegurando a disponibilidade dos dados com suas últimas atualizações.~~

 [112] Para que a efetividade dos procedimentos de backup seja garantida, é necessário que os procedimentos de recuperação de dados sejam regularmente testados.

 ~~[113] Para garantir a preservação dos dados em situação de desastre, é suficiente, para qualquer caso, a realização de backup dos dados uma vez ao dia.~~

7. Considere que uma organização mantenha em sua estrutura de tecnologia da informação um servidor de arquivos em funcionamento. Nesse contexto, julgue os itens subsequentes acerca de segurança da informação

[118] Suponha que as cópias de segurança dos arquivos armazenados nesse servidor sejam feitas em todos os dias úteis, por completo, isto é, todos os arquivos desse servidor são copiados diariamente para uma mídia externa, e que esse procedimento tem consumido grande quantidade de mídias para as cópias de segurança. Nesse caso, uma forma de diminuir o consumo de espaço de armazenamento das cópias de segurança é alterar o formato do backup de completo para incremental.

[120] Se as mídias das cópias de segurança são enviadas para outro local, fisicamente distante do servidor de arquivos, pelo menos uma vez a cada cinco dias úteis e tendo em vista que o transporte desses dados é feito por uma empresa terceirizada, uma forma de aumentar a segurança dessa informação é efetuar procedimento para criptografar os dados armazenados nas mídias.

7. Considere que uma organização mantenha em sua estrutura de tecnologia da informação um servidor de arquivos em funcionamento. Nesse contexto, julgue os itens subsequentes acerca de segurança da informação

[118] Suponha que as cópias de segurança dos arquivos armazenados nesse servidor sejam feitas em todos os dias úteis, por completo, isto é, todos os arquivos desse servidor são copiados diariamente para uma mídia externa, e que esse procedimento tem consumido grande quantidade de mídias para as cópias de segurança. Nesse caso, uma forma de diminuir o consumo de espaço de armazenamento das cópias de segurança é alterar o formato do backup de completo para incremental.

[120] Se as mídias das cópias de segurança são enviadas para outro local, fisicamente distante do servidor de arquivos, pelo menos uma vez a cada cinco dias úteis e tendo em vista que o transporte desses dados é feito por uma empresa terceirizada, uma forma de aumentar a segurança dessa informação é efetuar procedimento para criptografar os dados armazenados nas mídias.

8. A respeito da administração de unidades de fita linear tape open (LTO), julgue os itens seguintes.

[119] Considere que o administrador de rede necessite efetuar backups em mídias que possuam a capacidade mínima de armazenamento de 459 GB já compactados. Nesse caso, fitas do tipo LTO1 podem atender a essa demanda.

[120] Uma operação de backup cotidiana, que repete a gravação de dados em várias mídias LTO5 em uma biblioteca de backup, gera desperdícios. Para diminuir esse desperdício, o administrador poderá utilizar o recurso de deduplicação disponível no seu software de backup, pois as mídias LTO5 suportarão essa operação.

Atributo	Geração					
	LTO-1	LTO-2	LTO-3	LTO-4	LTO-5	LTO-6
Data de lançamento	2000	2003	2005	2007	2010	2012
Capacidade nativa de dados	100 GB	200 GB	400 GB	800 GB	1.5 TB	2.5 TB
Velocidade Max (MB/s)	20	40	80	120	140	160
Capacidade WORM?	Não	Não	Sim	Sim	Sim	Sim
Capacidade de encriptação?	Não	Não	Não	Sim	Sim	Sim
Espessura da fita	8,9 µm	8,9 µm	8,0 µm	6,6 µm	6,4 µm	6,1 µm
Tamanho da fita	609 m	609 m	680 m	820 m	846 m	846 m
Trilhas	384	512	704	896	1280	2176
Elementos de escrita	8	8	16	16	16	16
Voltas por banda	12	16	11	14	20	34
Densidade linear (bits/mm)	4880	7398	9638	13250	15142	15143 ^[3]
Codificação	RLL 1,7	PRML	PRML	PRML		

8. A respeito da administração de unidades de fita linear tape open (LTO), julgue os itens seguintes.

 ~~[119] Considere que o administrador de rede necessite efetuar backups em mídias que possuam a capacidade mínima de armazenamento de 459 GB já compactados. Nesse caso, fitas do tipo LTO1 podem atender a essa demanda.~~

 [120] Uma operação de backup cotidiana, que repete a gravação de dados em várias mídias LTO5 em uma biblioteca de backup, gera desperdícios. Para diminuir esse desperdício, o administrador poderá utilizar o recurso de deduplicação disponível no seu software de backup, pois as mídias LTO5 suportarão essa operação.

9. Julgue os itens seguintes, relativos a backup e restauração de dados.

[101] Para se proceder à cópia diária dos dados e à restauração total dos dados de um servidor de rede de uma empresa em menor tempo possível, o backup completo será mais adequado que o backup incremental.

[102] Em um processo de backup para um servidor de rede em que os dados sejam, diariamente, copiados para uma mídia que depois será armazenada em um cofre, se, após a compressão dos dados, o tamanho do arquivo de backup for igual a 16 Gb, recomenda-se a utilização da fita DAT do tipo DDS-3, que possui capacidade suficiente para armazenar essa quantidade de dados.

9. Julgue os itens seguintes, relativos a backup e restauração de dados.

 [101] Para se proceder à cópia diária dos dados e à restauração total dos dados de um servidor de rede de uma empresa em menor tempo possível, o backup completo será mais adequado que o backup incremental.

 ~~[102] Em um processo de backup para um servidor de rede em que os dados sejam, diariamente, copiados para uma mídia que depois será armazenada em um cofre, se, após a compressão dos dados, o tamanho do arquivo de backup for igual a 16 Gb, recomenda-se a utilização da fita DAT do tipo DDS-3, que possui capacidade suficiente para armazenar essa quantidade de dados.~~

GABARITO



1. C, E, E

8. E, C

2. C, C, E

9. C, E

3. E, C, E

4. C, E

5. E, E, C, C

6. E, C, E

7. C, C

Terceira Bateria de Questões Com Resolução Assistida

Dispositivos de segurança:

FIREWALL, IDS, IPS

1. A propósito de segurança de redes e certificação digital, julgue os itens subsecutivos.

[118] Firewalls conhecidos como filtro de pacotes, que atuam na camada de transporte do TCP/IP, são capazes de filtrar o tráfego de rede identificando o uso de softwares como Skype e Gtalk, sem a necessidade de filtrar o endereço IP da conexão.

[119] Ferramentas utilizadas para detecção de intrusão em redes adotam o recurso de captura de pacotes para análise e detecção de assinaturas de ataques conhecidos.

1. A propósito de segurança de redes e certificação digital, julgue os itens subsecutivos.

 ~~[118] Firewalls conhecidos como filtro de pacotes, que atuam na camada de transporte do TCP/IP, são capazes de filtrar o tráfego de rede identificando o uso de softwares como Skype e Gtalk, sem a necessidade de filtrar o endereço IP da conexão.~~

 [119] Ferramentas utilizadas para detecção de intrusão em redes adotam o recurso de captura de pacotes para análise e detecção de assinaturas de ataques conhecidos.

2. A respeito de firewall, julgue os itens subsecutivos.

[67] Um firewall que trabalha especificamente na camada de aplicação tem a capacidade de estabelecer regras para registrar e descartar pacotes que sejam destinados a um endereço IP e a uma porta específica.

[68] Considere que, em um servidor com serviço de firewall habilitado e em funcionamento, o administrador de rede tenha verificado que existe muito tráfego de flags SYN do protocolo TCP, sem que ocorra o retorno da flag ACK do host a que foi destinada a flag SYN. Nessa situação, é possível que regras de firewall estejam descartando os pedidos de abertura de conexão.

2. A respeito de firewall, julgue os itens subsecutivos.

 ~~[67] Um firewall que trabalha especificamente na camada de aplicação tem a capacidade de estabelecer regras para registrar e descartar pacotes que sejam destinados a um endereço IP e a uma porta específica.~~

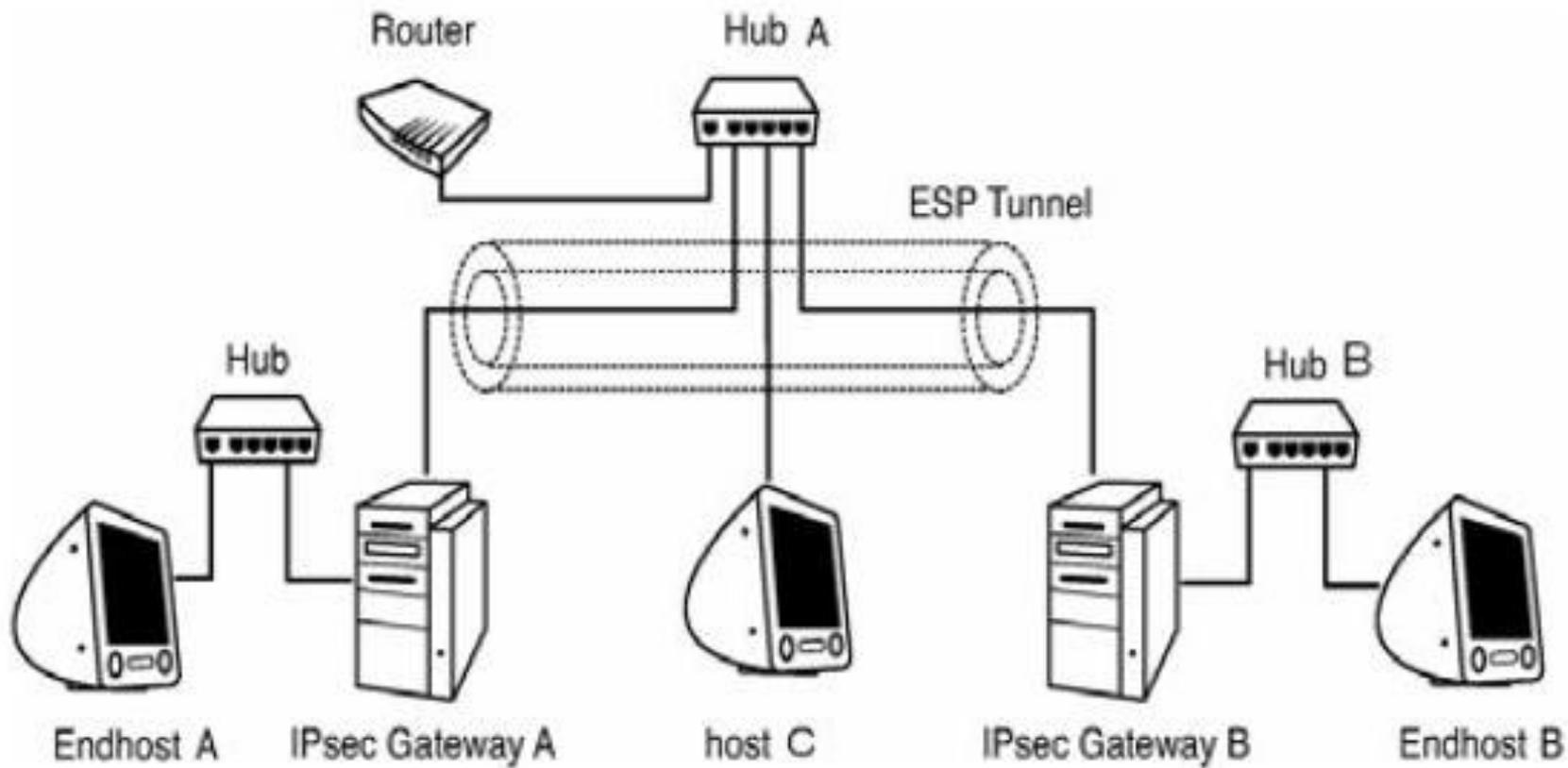
 [68] Considere que, em um servidor com serviço de firewall habilitado e em funcionamento, o administrador de rede tenha verificado que existe muito tráfego de flags SYN do protocolo TCP, sem que ocorra o retorno da flag ACK do host a que foi destinada a flag SYN. Nessa situação, é possível que regras de firewall estejam descartando os pedidos de abertura de conexão.

3. Julgue os itens subsecutivos, referentes a firewall e VPN (virtual private network).

[59] Considere que, em uma rede dotada de firewall, um computador infectado por vírus esteja enviando grande quantidade de emails via servidor de email dessa rede. Nessa situação, até que o vírus seja removido do computador infectado, o firewall tem a capacidade de bloquear o acesso entre o computador e o servidor de email sem tornar indisponível, ao servidor de email, o uso dos outros computadores da mesma rede.

3. Julgue os itens subsecutivos, referentes a firewall e VPN (virtual private network).

 [59] Considere que, em uma rede dotada de firewall, um computador infectado por vírus esteja enviando grande quantidade de emails via servidor de email dessa rede. Nessa situação, até que o vírus seja removido do computador infectado, o firewall tem a capacidade de bloquear o acesso entre o computador e o servidor de email sem tornar indisponível, ao servidor de email, o uso dos outros computadores da mesma rede.



4. O modelo da figura acima apresenta elementos individualmente nomeados e presentes em uma rede hipotética, acerca dos quais é possível inferir características de protocolos de segurança.

Julgue os itens seguintes, acerca das informações apresentadas e de dispositivos de segurança de redes de computadores.

[171] Se os Endhosts A e B trocarem vários pacotes por meio de seus respectivos gateways, então não haverá modo fácil de o host C identificar quais dos pacotes IP trafegados entre os gateways A e B são relativos à comunicação entre os Endhosts A e B.

[172] Considerando a necessidade de instalar um IDS para proteger a rede A, algumas opções podem ser adotadas, entre elas a de usar um sistema passivo ou ativo, bem como a de usar um sistema baseado em host ou em rede. Se a solução for adotar um sistema passivo e com base em host, então o host C poderá ser uma máquina adequada para essa necessidade. Se a solução for adotar um sistema reativo e embasado na rede, então podem-se usar os gateways A ou B. Se a solução for adotar um sistema reativo e baseado em host, então se poderá usar o host C.

4. O modelo da figura acima apresenta elementos individualmente nomeados e presentes em uma rede hipotética, acerca dos quais é possível inferir características de protocolos de segurança.

Julgue os itens seguintes, acerca das informações apresentadas e de dispositivos de segurança de redes de computadores.

[171] Se os Endhosts A e B trocarem vários pacotes por meio de seus respectivos gateways, então não haverá modo fácil de o host C identificar quais dos pacotes IP trafegados entre os gateways A e B são relativos à comunicação entre os Endhosts A e B.

~~[172] Considerando a necessidade de instalar um IDS para proteger a rede A, algumas opções podem ser adotadas, entre elas a de usar um sistema passivo ou ativo, bem como a de usar um sistema baseado em host ou em rede. Se a solução for adotar um sistema passivo e com base em host, então o host C poderá ser uma máquina adequada para essa necessidade. Se a solução for adotar um sistema reativo e embasado na rede, então podem se usar os gateways A ou B. Se a solução for adotar um sistema reativo e baseado em host, então se poderá usar o host C.~~

5. Com relação a segurança de hosts e redes, julgue os itens seguintes

[168] Uma técnica comumente usada na segurança de redes é o estabelecimento de um perímetro de segurança cuja finalidade é controlar o tráfego ingresso na rede e o egresso da rede.

[169] Roteadores de borda, firewalls, IDSs, IPSs e VPNs são alguns dos principais elementos do perímetro de segurança da rede.

[172] Em geral, os firewalls inspecionam todo o pacote, enquanto os IDSs inspecionam apenas os cabeçalhos.

5. Com relação a segurança de hosts e redes, julgue os itens seguintes

 [168] Uma técnica comumente usada na segurança de redes é o estabelecimento de um perímetro de segurança cuja finalidade é controlar o tráfego ingresso na rede e o egresso da rede.

 [169] Roteadores de borda, firewalls, IDSs, IPSs e VPNs são alguns dos principais elementos do perímetro de segurança da rede.

 ~~[172] Em geral, os firewalls inspecionam todo o pacote, enquanto os IDSs inspecionam apenas os cabeçalhos.~~

GABARITO



1. E, C

2. E, C

3. C

4. C, E

5. C, C, E

Quarta Bateria de Questões Com Resolução Assistida

Arquitetura e Organização de
Computadores

RAID



1. Acerca das configurações de RAID em hardware, julgue os itens que se seguem.

[111] As soluções de RAID 1 necessitam de, no mínimo, dois discos, possuem bom desempenho e fornecem redundância de dados.

[112] As soluções de RAID 0 necessitam de, no mínimo, dois discos, possuem excelente desempenho e asseguram redundância de dados.

1. Acerca das configurações de RAID em hardware, julgue os itens que se seguem.

 [111] As soluções de RAID 1 necessitam de, no mínimo, dois discos, possuem bom desempenho e fornecem redundância de dados.

 ~~[112] As soluções de RAID 0 necessitam de, no mínimo, dois discos, possuem excelente desempenho e asseguram redundância de dados.~~

2. No que diz respeito aos conceitos de RAID, julgue os itens que se seguem.

[81] A principal diferença do RAID 6 para o RAID 5 é que, em vez de utilizar dois discos para redundância, o RAID 6 utiliza apenas um, com o dobro de bits de paridade.

[82] Com a adoção, para uso doméstico, do RAID 10, que abrange o conceito do RAID 0 e do RAID 1, obtêm-se ao mesmo tempo ganho de desempenho e redundância; entretanto, um dos problemas de se usar RAID 10, em vez de usar somente o RAID 0, é o custo mais alto com a compra de mais HDs para redundância.

2. No que diz respeito aos conceitos de RAID, julgue os itens que se seguem.

 ~~[81] A principal diferença do RAID 6 para o RAID 5 é que, em vez de utilizar dois discos para redundância, o RAID 6 utiliza apenas um, com o dobro de bits de paridade.~~

 [82] Com a adoção, para uso doméstico, do RAID 10, que abrange o conceito do RAID 0 e do RAID 1, obtêm-se ao mesmo tempo ganho de desempenho e redundância; entretanto, um dos problemas de se usar RAID 10, em vez de usar somente o RAID 0, é o custo mais alto com a compra de mais HDs para redundância.

3. Com base na tabela acima, julgue o próximo item relativo a desempenho.

tipo de disco	n.º de discos	RAID	IOPS individual
SSD	2	1	3300
SATA	6	5	130
SAS	8	10	180

[83] De acordo com os dados acima, o IOPS total dos três discos é 8810.

3. Com base na tabela acima, julgue o próximo item relativo a desempenho.

tipo de disco	n.º de discos	RAID	IOPS individual
SSD	2	1	3300
SATA	6	5	130
SAS	8	10	180

~~[83] De acordo com os dados acima, o IOPS total dos três discos é 8810.~~



4. Acerca de entradas e saídas de dados, julgue o item abaixo.

[58] O esquema de organização de discos RAID aumenta o desempenho e a confiabilidade em sistemas de armazenamento. Na configuração RAID 5, utiliza-se um sistema de paridade para manter a integridade dos dados, no qual os arquivos são divididos em fragmentos de tamanho configurável e, para cada grupo de fragmentos, é gerado um fragmento adicional com códigos de paridade, que são armazenados de maneira distribuída.

4. Acerca de entradas e saídas de dados, julgue o item abaixo.

[58] O esquema de organização de discos RAID aumenta o desempenho e a confiabilidade em sistemas de armazenamento. Na configuração RAID 5, utiliza-se um sistema de paridade para manter a integridade dos dados, no qual os arquivos são divididos em fragmentos de tamanho configurável e, para cada grupo de fragmentos, é gerado um fragmento adicional com códigos de paridade, que são armazenados de maneira distribuída. **ANULADA**

5. Acerca de RAID e switches de rede, julgue os itens a seguir.

[74] Para aumentar a disponibilidade dos dados com redundância de discos e escalabilidade, pode-se utilizar o RAID tipo 5.

5. Acerca de RAID e switches de rede, julgue os itens a seguir.

[74] Para aumentar a disponibilidade dos dados com redundância de discos e escalabilidade, pode-se utilizar o RAID tipo 5.



6. Acerca de RAID, julgue os itens a seguir.

[69] Um arranjo do tipo RAID 10, comparado a discos sem nenhum arranjo, tem melhor desempenho no armazenamento das informações e na redundância dos dados.

[70] É possível implementar um arranjo do tipo RAID 6 usando três discos rígidos com a mesma capacidade de armazenamento.

6. Acerca de RAID, julgue os itens a seguir.

 [69] Um arranjo do tipo RAID 10, comparado a discos sem nenhum arranjo, tem melhor desempenho no armazenamento das informações e na redundância dos dados.

 ~~[70] É possível implementar um arranjo do tipo RAID 6 usando três discos rígidos com a mesma capacidade de armazenamento.~~

7. Com referência a sistemas de arquivos e a sistemas RAID, julgue o item seguinte.

[56] Em sistemas de arquivos NTFS, a tabela-mestra de arquivos (MTF) é dividida em seis partições de tamanhos variáveis. Para prover tolerância a falhas nessa configuração, é necessário e suficiente organizá-los utilizando-se RAID nível 4, pois, quanto maior o número de discos do arranjo, menor será a possibilidade de falha.

7. Com referência a sistemas de arquivos e a sistemas RAID, julgue o item seguinte.

 ~~[56] Em sistemas de arquivos NTFS, a tabela mestra de arquivos (MTF) é dividida em seis partições de tamanhos variáveis. Para prover tolerância a falhas nessa configuração, é necessário e suficiente organizá-los utilizando-se RAID nível 4, pois, quanto maior o número de discos do arranjo, menor será a possibilidade de falha.~~

8. Julgue os itens subsecutivos, relativos a armazenamento de informações

[101] O software RAID é comumente utilizado para implementar soluções simples e de baixo custo para a proteção de dados, além de oferecer um nível de desempenho superior ao das soluções que se baseiam em hardware RAID.

8. Julgue os itens subsecutivos, relativos a armazenamento de informações

 ~~[101] O software RAID é comumente utilizado para implementar soluções simples e de baixo custo para a proteção de dados, além de oferecer um nível de desempenho superior ao das soluções que se baseiam em hardware RAID.~~

9. No que concerne a RAID e deduplicação, julgue os itens que se seguem.

[98] O arranjo de disco do tipo RAID 10 tem por objetivo agregar maior velocidade à gravação dos dados e promover redundância, caso algum disco do arranjo seja danificado.

9. No que concerne a RAID e deduplicação, julgue os itens que se seguem.

 [98] O arranjo de disco do tipo RAID 10 tem por objetivo agregar maior velocidade à gravação dos dados e promover redundância, caso algum disco do arranjo seja danificado.

10. A respeito do conceito de RAID (redundant array of inexpensive disks), julgue o próximo item.

[83] RAID 0 é uma solução mais voltada para o desempenho do que para a segurança e a tolerância a falhas. Ao serem utilizados três discos, nesse tipo de arranjo, todos os discos serão gravados com partes do mesmo arquivo em stripping e apresentarão os dados distribuídos de forma completamente uniforme

10. A respeito do conceito de RAID (redundant array of inexpensive disks), julgue o próximo item.

 ~~[83] RAID 0 é uma solução mais voltada para o desempenho do que para a segurança e a tolerância a falhas. Ao serem utilizados três discos, nesse tipo de arranjo, todos os discos serão gravados com partes do mesmo arquivo em stripping e apresentarão os dados distribuídos de forma completamente uniforme~~

GABARITO



1. C, E

2. E, C

3. E

4. ANULADO

5. C

6. C, E

7. E

8. E

9. C

10. E

Quarta Bateria de Questões Com Resolução Assistida

Dispositivos de segurança:

FIREWALL, IDS, IPS

1. Com relação a sistemas de proteção IDS, IPS e VLANs, assinale a opção correta.
 - A. O IDS (intrusion detection system) refere-se a meios técnicos de descobrir acessos não autorizados a uma rede, que podem indicar a ação de um cracker ou de funcionários mal-intencionados.
 - B. IPS (intrusion prevention systems), também denominado IDP (intrusion detection and prevention), são dispositivos de monitoramento de rede e(ou) atividades maliciosas de sistema empregados. Entre as suas funções estão a identificação das atividades maliciosas e a geração de log de informações acerca dessa atividade.
 - C. Os sistemas IPS são colocados em linha, contudo são incapazes de prevenir ativamente ou bloquear as intrusões detectadas.
 - D. O IPS envia alarme, prende os pacotes maliciosos, redefine a conexão e(ou) bloqueia o tráfego a partir do endereço IP incorreto.
 - E. São dois os métodos de estabelecer uma VLAN: o de marcação de quadro (frame-tagging), que não modifica a informação contida no quadro da camada 2, e o de filtragem de quadro (frame-filtering).

1. Com relação a sistemas de proteção IDS, IPS e VLANs, assinale a opção correta.

-  A. O IDS (intrusion detection system) refere-se a meios técnicos de descobrir acessos não autorizados a uma rede, que podem indicar a ação de um cracker ou de funcionários mal-intencionados.
- B. IPS (intrusion prevention systems), também denominado IDP (intrusion detection and prevention), são dispositivos de monitoramento de rede e(ou) atividades maliciosas de sistema empregados. Entre as suas funções estão a identificação das atividades maliciosas e a geração de log de informações acerca dessa atividade.
- C. Os sistemas IPS são colocados em linha, contudo são incapazes de prevenir ativamente ou bloquear as intrusões detectadas.
- D. O IPS envia alarme, prende os pacotes maliciosos, redefine a conexão e(ou) bloqueia o tráfego a partir do endereço IP incorreto.
- E. São dois os métodos de estabelecer uma VLAN: o de marcação de quadro (frame-tagging), que não modifica a informação contida no quadro da camada 2, e o de filtragem de quadro (frame-filtering).

2. Acerca de segurança na Internet e dispositivos de segurança de redes de computadores, julgue os itens que se seguem.

[64] Firewalls podem ser usados para estabelecer a chamada zona deslimitarizada (DMZ), que é um segmento de rede localizado entre a rede protegida e a rede desprotegida.

[65] Um IDS (intrusion detection system) permite monitorar o tráfego de rede em busca de atividades consideradas suspeitas, sem, entretanto, agir diretamente sobre as suspeitas identificadas.

2. Acerca de segurança na Internet e dispositivos de segurança de redes de computadores, julgue os itens que se seguem.

 [64] Firewalls podem ser usados para estabelecer a chamada zona deslimitarizada (DMZ), que é um segmento de rede localizado entre a rede protegida e a rede desprotegida.

 ~~[65] Um IDS (intrusion detection system) permite monitorar o tráfego de rede em busca de atividades consideradas suspeitas, sem, entretanto, agir diretamente sobre as suspeitas identificadas.~~

3. órgão público, visando identificar o atual nível de proteção da rede de computadores das organizações públicas para as quais presta serviços, desenvolveu um conjunto de processos de avaliação de segurança da informação em redes de computadores. Empregando métodos analíticos e práticos, os auditores coletaram várias informações acerca da rede e produziram diversas declarações, sendo algumas delas consistentes com o estado da prática e outras incorretas. A esse respeito, julgue os itens.

[101] O uso de firewalls na rede de computadores é mais eficaz na prevenção de incidentes que para o tratamento dos eventuais incidentes que nela ocorrem. Os firewalls stateless, ou de filtragem de pacotes, são especialmente eficazes no bloqueio a vários tipos de ataques, como phishing e spoofing.

3. órgão público, visando identificar o atual nível de proteção da rede de computadores das organizações públicas para as quais presta serviços, desenvolveu um conjunto de processos de avaliação de segurança da informação em redes de computadores. Empregando métodos analíticos e práticos, os auditores coletaram várias informações acerca da rede e produziram diversas declarações, sendo algumas delas consistentes com o estado da prática e outras incorretas. A esse respeito, julgue os itens.

~~[101] O uso de firewalls na rede de computadores é mais eficaz na prevenção de incidentes que para o tratamento dos eventuais incidentes que nela ocorrem. Os firewalls stateless, ou de filtragem de pacotes, são especialmente eficazes no bloqueio a vários tipos de ataques, como phishing e spoofing.~~



4. órgão público, visando identificar o atual nível de proteção da rede de computadores das organizações públicas para as quais presta serviços, desenvolveu um conjunto de processos de avaliação de segurança da informação em redes de computadores. Empregando métodos analíticos e práticos, os auditores coletaram várias informações acerca da rede e produziram diversas declarações, sendo algumas delas consistentes com o estado da prática e outras incorretas. A esse respeito, julgue os itens.

[103] Considere que os auditores identifiquem, entre a rede de uma organização e a Internet, um sistema em funcionamento que realiza a filtragem e correção automática do fluxo de pacotes e datagramas estabelecidos entre os hosts da organização e aqueles da Internet. Considere também que o referido sistema realiza inspeção e eventuais ajustes nos pedidos e respostas http que trafegam em ambos sentidos. Nesse caso, diante das informações mencionadas, é correto afirmar que tal sistema pode ser classificado como de prevenção de intrusão em rede NIPS (network intrusion prevention system) e não apenas como de detecção de intrusão IDS (intrusion detection system).

4. órgão público, visando identificar o atual nível de proteção da rede de computadores das organizações públicas para as quais presta serviços, desenvolveu um conjunto de processos de avaliação de segurança da informação em redes de computadores. Empregando métodos analíticos e práticos, os auditores coletaram várias informações acerca da rede e produziram diversas declarações, sendo algumas delas consistentes com o estado da prática e outras incorretas. A esse respeito, julgue os itens.

[103] Considere que os auditores identifiquem, entre a rede de uma organização e a Internet, um sistema em funcionamento que realiza a filtragem e correção automática do fluxo de pacotes e datagramas estabelecidos entre os hosts da organização e aqueles da Internet. Considere também que o referido sistema realiza inspeção e eventuais ajustes nos pedidos e respostas http que trafegam em ambos sentidos. Nesse caso, diante das informações mencionadas, é correto afirmar que tal sistema pode ser classificado como de prevenção de intrusão em rede NIPS (network intrusion prevention system) e não apenas como de detecção de intrusão IDS (intrusion detection system).



5. Os sistemas IDS (Intrusion Detection System) têm-se tornado componentes cada vez mais importantes em redes de computadores de várias corporações. Com referência aos IDS e suas características, julgue os seguintes itens.
- Apesar de ser uma ferramenta de segurança altamente específica, um IDS não deve ser utilizado em conjunto com um firewall, porque a quantidade de ataques que um IDS detecta é relativamente pequena em redes consideradas grandes.
 - Um IDS pode detectar, de acordo com configurações específicas, se uma rede ou se um nodo em uma rede está sofrendo um ataque de DDoS (Distributed Denial of Service).
 - Para a detecção de intrusão, um IDS usa técnicas de detecção de anomalia, detecção de uso impróprio (misuse detection) ou detecção de assinatura, entre outras técnicas.
 - A técnica de detecção de anomalia consiste em o IDS reconhecer características consideradas como um padrão normal de funcionamento da rede. Qualquer variação brusca nesse padrão de comportamento é considerada como uma tentativa de intrusão na rede.

5. Os sistemas IDS (Intrusion Detection System) têm-se tornado componentes cada vez mais importantes em redes de computadores de várias corporações. Com referência aos IDS e suas características, julgue os seguintes itens.

~~• Apesar de ser uma ferramenta de segurança altamente específica, um IDS não deve ser utilizado em conjunto com um firewall, porque a quantidade de ataques que um IDS detecta é relativamente pequena em redes consideradas grandes.~~



• Um IDS pode detectar, de acordo com configurações específicas, se uma rede ou se um nodo em uma rede está sofrendo um ataque de DDoS (Distributed Denial of Service).



• Para a detecção de intrusão, um IDS usa técnicas de detecção de anomalia, detecção de uso impróprio (misuse detection) ou detecção de assinatura, entre outras técnicas.



• A técnica de detecção de anomalia consiste em o IDS reconhecer características consideradas como um padrão normal de funcionamento da rede. Qualquer variação brusca nesse padrão de comportamento é considerada como uma tentativa de intrusão na rede.



6. Com relação à segurança em redes de computadores, julgue os itens subsequentes

[159] Firewalls, IDS e IPS são dispositivos que têm finalidades idênticas, porém tipicamente operam de formas distintas: o primeiro inspeciona integralmente os datagramas e reage bloqueando o tráfego indesejado; o segundo também inspeciona integralmente os datagramas, mas não bloqueia o tráfego indesejado, apenas emite alertas; e o terceiro inspeciona apenas os cabeçalhos dos datagramas e, como o primeiro, reage bloqueando o tráfego indesejado.

6. Com relação à segurança em redes de computadores, julgue os itens subsequentes

~~[159] Firewalls, IDS e IPS são dispositivos que têm finalidades idênticas, porém tipicamente operam de formas distintas: o primeiro inspeciona integralmente os datagramas e reage bloqueando o tráfego indesejado; o segundo também inspeciona integralmente os datagramas, mas não bloqueia o tráfego indesejado, apenas emite alertas; e o terceiro inspeciona apenas os cabeçalhos dos datagramas e, como o primeiro, reage bloqueando o tráfego indesejado.~~



7. Quanto aos ataques a redes de computadores, seus tipos e malwares empregados, julgue os itens a seguir

[101] A neutralização de backdoors é mais eficaz por meio de dispositivos de IPS e IDS que por meio de firewalls e sniffers.

7. Quanto aos ataques a redes de computadores, seus tipos e malwares empregados, julgue os itens a seguir

~~[101] A neutralização de backdoors é mais eficaz por meio de dispositivos de IPS e IDS que por meio de firewalls e sniffers.~~



8. Acerca dos dispositivos de segurança de redes de computadores, julgue os itens subsequentes.

[96] Um proxy, ao agir no lugar do cliente ou do usuário para prover acesso a um serviço de rede, protege tanto o cliente quanto o servidor de uma conexão direta.

[97] IDS e IPS são sistemas que protegem a rede de intrusões, diferindo no tratamento dado quando uma intrusão é detectada. Especificamente, o IPS limita-se a gerar alertas e ativar alarmes, e o IDS executa contramedidas, como interromper o fluxo de dados referente à intrusão detectada.

[98] A ocorrência de falsos positivos normalmente acarreta consequências mais graves para as redes que utilizam IDS do que para aquelas que usam IPS.

[99] A inspeção de estados visa determinar se um pacote pode entrar ou sair de uma rede, tendo por base a verificação de informações localizadas no cabeçalho do pacote.

[100] Tanto na filtragem quanto na inspeção que se baseiam em estado, a informação de estado é mantida em uma tabela até que a conexão se encerre (como no tráfego TCP) ou ao atingir um limite de tempo (como no caso de tráfego TCP, UDP e ICMP).

8. Acerca dos dispositivos de segurança de redes de computadores, julgue os itens subsequentes.

[96] Um proxy, ao agir no lugar do cliente ou do usuário para prover acesso a um serviço de rede, protege tanto o cliente quanto o servidor de uma conexão direta.



~~[97] IDS e IPS são sistemas que protegem a rede de intrusões, diferindo no tratamento dado quando uma intrusão é detectada. Especificamente, o IPS limita-se a gerar alertas e ativar alarmes, e o IDS executa contramedidas, como interromper o fluxo de dados referente à intrusão detectada.~~



~~[98] A ocorrência de falsos positivos normalmente acarreta consequências mais graves para as redes que utilizam IDS do que para aquelas que usam IPS.~~



~~[99] A inspeção de estados visa determinar se um pacote pode entrar ou sair de uma rede, tendo por base a verificação de informações localizadas no cabeçalho do pacote.~~



[100] Tanto na filtragem quanto na inspeção que se baseiam em estado, a informação de estado é mantida em uma tabela até que a conexão se encerre (como no tráfego TCP) ou ao atingir um limite de tempo (como no caso de tráfego TCP, UDP e ICMP).



9. Com relação a dispositivos de segurança de redes, julgue os próximos itens.

[110] Nos firewalls que utilizam inspeção de estado, esta é realizada no estado das conexões TCP.

[111] Os firewalls que usam filtragem de pacote tomam decisões de encaminhamento a partir de informações presentes nos cabeçalhos dos pacotes.

[112] Os IDS e IPS embasados em detecção por assinatura podem apresentar ocorrência de falsos-positivos, sendo mais severos os efeitos nos IPS que nos IDS.

9. Com relação a dispositivos de segurança de redes, julgue os próximos itens.

~~[110] Nos firewalls que utilizam inspeção de estado, esta é realizada no estado das conexões TCP.~~



[111] Os firewalls que usam filtragem de pacote tomam decisões de encaminhamento a partir de informações presentes nos cabeçalhos dos pacotes.



[112] Os IDS e IPS embasados em detecção por assinatura podem apresentar ocorrência de falsos-positivos, sendo mais severos os efeitos nos IPS que nos IDS.



10. Um firewall tem três interfaces, conectadas da seguinte forma: uma à rede externa; outra à rede interna; e a terceira a uma DMZ. Nessa situação, considerando que o firewall registre todas as suas ações referentes ao exame do tráfego, julgue os itens seguintes

[99] Nessa situação, as regras do firewall devem: permitir acesso da rede externa apenas aos servidores presentes na DMZ; negar acesso do tráfego da rede externa que tenha como origem endereços da rede interna; e negar acesso do tráfego da rede interna que tenha como origem endereços distintos dos utilizados na rede interna.

[100] Para a proteção do firewall em questão, é correto posicionar um IDS ou IPS, preferencialmente o último, entre a rede externa e o firewall.

[101] A presença de vários registros idênticos referentes a um mesmo fluxo de tráfego é consistente com um firewall que tem por base a inspeção de pacotes.

10. Um firewall tem três interfaces, conectadas da seguinte forma: uma à rede externa; outra à rede interna; e a terceira a uma DMZ. Nessa situação, considerando que o firewall registre todas as suas ações referentes ao exame do tráfego, julgue os itens seguintes

 [99] Nessa situação, as regras do firewall devem: permitir acesso da rede externa apenas aos servidores presentes na DMZ; negar acesso do tráfego da rede externa que tenha como origem endereços da rede interna; e negar acesso do tráfego da rede interna que tenha como origem endereços distintos dos utilizados na rede interna.

 ~~[100] Para a proteção do firewall em questão, é correto posicionar um IDS ou IPS, preferencialmente o último, entre a rede externa e o firewall.~~

 [101] A presença de vários registros idênticos referentes a um mesmo fluxo de tráfego é consistente com um firewall que tem por base a inspeção de pacotes.

GABARITO



1. A

6. E

2. C, E

7. E

3. E

8. C, E, E, E, C

4. C

9. E, C, C

5. E, C, C, C

10. C, E, C

Quarta Bateria de Questões Com Resolução Assistida

Dispositivos de segurança: **Proxies**

1. Julgue os próximos itens, com relação a auditoria, prevenção de intrusão e proxy.

[83] Os servidores proxy criam um cache com as solicitações de cada usuário, de forma a otimizar consultas futuras de um mesmo usuário, sendo esse cache de uso exclusivo de seu respectivo usuário.

1. Julgue os próximos itens, com relação a auditoria, prevenção de intrusão e proxy.

 ~~[83] Os servidores proxy criam um cache com as solicitações de cada usuário, de forma a otimizar consultas futuras de um mesmo usuário, sendo esse cache de uso exclusivo de seu respectivo usuário.~~

2. A respeito da segurança de redes de computadores, julgue os itens de 86 a 90.

[86] Se um firewall estiver entre dois segmentos físicos de rede e o endereçamento de uma rede for 192.168.1.0/25 e da outra, 192.168.1.0/26, para que os computadores desses dois segmentos possam se comunicar entre si, é obrigatório utilizar o recurso de NAT (network address translation) no firewall.

[89] O serviço de proxy no sistema operacional Linux, provido pelo software Squid, utiliza o protocolo HTTP, sendo capaz de fazer cache de páginas web estáticas e otimizar o acesso, diminuindo o consumo do link de Internet. Além disso, é capaz de filtrar acessos a sítios web definidos previamente em sua configuração.

2. A respeito da segurança de redes de computadores, julgue os itens de 86 a 90.

 ~~[86] Se um firewall estiver entre dois segmentos físicos de rede e o endereçamento de uma rede for 192.168.1.0/25 e da outra, 192.168.1.0/26, para que os computadores desses dois segmentos possam se comunicar entre si, é obrigatório utilizar o recurso de NAT (network address translation) no firewall.~~

 [89] O serviço de proxy no sistema operacional Linux, provido pelo software Squid, utiliza o protocolo HTTP, sendo capaz de fazer cache de páginas web estáticas e otimizar o acesso, diminuindo o consumo do link de Internet. Além disso, é capaz de filtrar acessos a sítios web definidos previamente em sua configuração.

3. A respeito de segurança de redes de comunicação, julgue os itens que se seguem.

[118] O uso de proxy reverso torna mais rápido o acesso a um servidor de páginas web, tendo em vista que ele faz cache das páginas acessadas.

3. A respeito de segurança de redes de comunicação, julgue os itens que se seguem.

[118] O uso de proxy reverso torna mais rápido o acesso a um servidor de páginas web, tendo em vista que ele faz cache das páginas acessadas.



4. Com relação a aspectos de intranet e de Internet, julgue os itens que se seguem.

[119] No caso de se utilizar um servidor proxy firewall para acessar um sítio na Internet, o cliente não troca pacotes de informações diretamente com o servidor solicitado.

4. Com relação a aspectos de intranet e de Internet, julgue os itens que se seguem.

[119] No caso de se utilizar um servidor proxy firewall para acessar um sítio na Internet, o cliente não troca pacotes de informações diretamente com o servidor solicitado.



5. Julgue os itens a seguir, a respeito de segurança da informação.

[91] O bloqueio seguro a uma rede restrita de uma empresa poderá ser efetuado por meio de uma DMZ. Para a criação de uma DMZ dessa natureza, é suficiente utilizar um firewall do tipo Proxy.

5. Julgue os itens a seguir, a respeito de segurança da informação.

~~[91] O bloqueio seguro a uma rede restrita de uma empresa poderá ser efetuado por meio de uma DMZ. Para a criação de uma DMZ dessa natureza, é suficiente utilizar um firewall do tipo Proxy.~~



6. A respeito de roteadores, switches, proxies, Internet e intranet, julgue os próximos itens

[70] Caching web proxy constitui um web proxy usado como cache para páginas da Internet e arquivos disponíveis em servidores remotos da Internet, para que possam ser acessados mais rapidamente pelos clientes de uma rede local (LAN).

[73] Proxy constitui um servidor que recebe requisições de clientes e normalmente as repassa a servidores específicos, podendo, opcionalmente, alterar a requisição do cliente ou a resposta do servidor final e, algumas vezes, disponibilizar, ele próprio, o recurso requisitado, sem necessidade de repassar a requisição a outro servidor.

6. A respeito de roteadores, switches, proxies, Internet e intranet, julgue os próximos itens

 [70] Caching web proxy constitui um web proxy usado como cache para páginas da Internet e arquivos disponíveis em servidores remotos da Internet, para que possam ser acessados mais rapidamente pelos clientes de uma rede local (LAN).

 [73] Proxy constitui um servidor que recebe requisições de clientes e normalmente as repassa a servidores específicos, podendo, opcionalmente, alterar a requisição do cliente ou a resposta do servidor final e, algumas vezes, disponibilizar, ele próprio, o recurso requisitado, sem necessidade de repassar a requisição a outro servidor.

7. O endereço IP de uma rede local é 10.100.100.0/24 e a única saída para a Internet é um roteador de saída cujo endereço IP é 200.20.20.1/30. Considerando que o administrador dessa rede tenha definido a utilização do NAT, julgue os itens seguintes.

[82] Se existir um servidor web respondendo na porta 443 na rede 10, então, a fim de tornar esse servidor visível na Internet, o roteador deverá ser configurado para encaminhar todos os pacotes com destino o endereço IP 200.20.20.1 na porta 443 para o IP interno do servidor web. Ao retornar os pacotes, o roteador deverá modificar o IP de origem para 200.20.20.1.

[83] Se o administrador utilizar um proxy na rede 10, o NAT para esse proxy deve usar o endereço IP 200.20.20.1 para a internet e o roteador de saída deve fazer o tratamento da conversão de endereços.

7. O endereço IP de uma rede local é 10.100.100.0/24 e a única saída para a Internet é um roteador de saída cujo endereço IP é 200.20.20.1/30. Considerando que o administrador dessa rede tenha definido a utilização do NAT, julgue os itens seguintes.

 [82] Se existir um servidor web respondendo na porta 443 na rede 10, então, a fim de tornar esse servidor visível na Internet, o roteador deverá ser configurado para encaminhar todos os pacotes com destino o endereço IP 200.20.20.1 na porta 443 para o IP interno do servidor web. Ao retornar os pacotes, o roteador deverá modificar o IP de origem para 200.20.20.1.

 [83] Se o administrador utilizar um proxy na rede 10, o NAT para esse proxy deve usar o endereço IP 200.20.20.1 para a internet e o roteador de saída deve fazer o tratamento da conversão de endereços.

GABARITO



1. E

6. C, C

2. E, C

7. C, C

3. C

4. C

5. E

Quinta Bateria de Questões Com Resolução Assistida

Arquitetura e Organização de
Computadores

RAID



1. Acerca dos tipos e características do RAID, é correto afirmar que
- A. RAID 5, também conhecido como paridade distribuída intercalada por blocos, espalha os dados em todos os discos do arranjo e a paridade em um disco exclusivo, havendo redundância em nível de blocos e redundância em nível lógico.
 - B. RAID 6 tem similaridade com o RAID 5, porém, nessa solução, os dados e informações extras e códigos para correção de erros, para proteger contra múltiplas falhas, ficam espalhados em todos os discos do conjunto.
 - C. RAID 01, combinação do RAID 0 com o RAID 1, provê bom desempenho e boa confiabilidade, porém, possui como desvantagem não poder ser implementado no hardware do array de armazenamento.
 - D. RAID 0 se refere a arrays de discos com espelhamento no nível de blocos com redundância em nível lógico e paridade nos discos espelhados.
 - E. RAID 1 se refere a arrays de discos com espalhamento no nível de blocos sem redundância em nível lógico e sem paridade nos discos espalhados.

1. Acerca dos tipos e características do RAID, é correto afirmar que

- A. RAID 5, também conhecido como paridade distribuída intercalada por blocos, espalha os dados em todos os discos do arranjo e a paridade em um disco exclusivo, havendo redundância em nível de blocos e redundância em nível lógico.
-  B. RAID 6 tem similaridade com o RAID 5, porém, nessa solução, os dados e informações extras e códigos para correção de erros, para proteger contra múltiplas falhas, ficam espalhados em todos os discos do conjunto.
- C. RAID 01, combinação do RAID 0 com o RAID 1, provê bom desempenho e boa confiabilidade, porém, possui como desvantagem não poder ser implementado no hardware do array de armazenamento.
- D. RAID 0 se refere a arrays de discos com espelhamento no nível de blocos com redundância em nível lógico e paridade nos discos espelhados.
- E. RAID 1 se refere a arrays de discos com espalhamento no nível de blocos sem redundância em nível lógico e sem paridade nos discos espalhados.

2. Julgue os itens seguintes, que versam sobre RAID (Redundant Array of Independent Disks).

[78] Em um arranjo de discos em RAID tipo 6, são necessários 3 discos para o arranjo, e não há suporte a discos de spare.

[79] Em um arranjo de discos em RAID 5, é suportada a falha de até dois discos sem que sejam comprometidas a integridade e a disponibilidade dos dados armazenados.

[80] Em um arranjo de RAID tipo 0 que utilize dois discos e tenha outro de spare, em caso de problemas com um dos discos do arranjo, é possível manter os dados íntegros e dois discos em funcionamento.

2. Julgue os itens seguintes, que versam sobre RAID (Redundant Array of Independent Disks).

~~[78] Em um arranjo de discos em RAID tipo 6, são necessários 3 discos para o arranjo, e não há suporte a discos de spare.~~



~~[79] Em um arranjo de discos em RAID 5, é suportada a falha de até dois discos sem que sejam comprometidas a integridade e a disponibilidade dos dados armazenados.~~



[80] Em um arranjo de RAID tipo 0 que utilize dois discos e tenha outro de spare, em caso de problemas com um dos discos do arranjo, é possível manter os dados íntegros e dois discos em funcionamento.



3. Julgue os itens a seguir, relativos a conceitos e tecnologias de armazenamento de dados.

[76] Para se parecerem com um único disco para o software, todos os RAIDs adquirem a propriedade de distribuição dos dados pelos dispositivos, o que permite operações em paralelo.

3. Julgue os itens a seguir, relativos a conceitos e tecnologias de armazenamento de dados.

[76] Para se parecerem com um único disco para o software, todos os RAIDs adquirem a propriedade de distribuição dos dados pelos dispositivos, o que permite operações em paralelo.



4. Na configuração de um equipamento storage que contém 12 discos padrão SAS (serial attached SCSI) foi implementado um arranjo de disco RAID 6. Nessa situação, esse arranjo
- A. não suporta qualquer disco danificado sem perder dados.
 - B. reserva dois discos para armazenamento da paridade dos dados.
 - C. não armazena dados sobre a paridade dos dados.
 - D. reserva um disco para armazenamento da paridade dos dados.
 - E. reserva metade dos discos para redundância dos dados.

4. Na configuração de um equipamento storage que contém 12 discos padrão SAS (serial attached SCSI) foi implementado um arranjo de disco RAID 6. Nessa situação, esse arranjo

A. não suporta qualquer disco danificado sem perder dados.

 B. reserva dois discos para armazenamento da paridade dos dados.

C. não armazena dados sobre a paridade dos dados.

D. reserva um disco para armazenamento da paridade dos dados.

E. reserva metade dos discos para redundância dos dados.

5. Julgue os itens a seguir, referentes a tecnologias de RAID.

[145] Apesar de possível, é inadequado usar o RAID em duas partições em um mesmo disco físico, em virtude da possibilidade de perda de dados em caso de falha.

[146] O RAID 10 é uma tecnologia empregada para garantir a redundância de dados de forma rápida e necessita de, no mínimo, dois discos físicos para ser implementado.

5. Julgue os itens a seguir, referentes a tecnologias de RAID.

 [145] Apesar de possível, é inadequado usar o RAID em duas partições em um mesmo disco físico, em virtude da possibilidade de perda de dados em caso de falha.

 ~~[146] O RAID 10 é uma tecnologia empregada para garantir a redundância de dados de forma rápida e necessita de, no mínimo, dois discos físicos para ser implementado.~~

6. Acerca de RAID, julgue os itens que se seguem.

[112] Para a implementação de RAID do tipo 6, é necessário um disco para armazenar a paridade dos dados. Esse tipo de arranjo de discos suporta a falha de somente um disco, que ainda assim consegue manter o acesso aos dados armazenados no arranjo.

[113] Para atender à demanda de um servidor que necessita de alto desempenho no acesso aos dados gravados nos seus discos rígidos, o administrador deve optar por RAID do tipo 0, em vez de discos rígidos individuais.

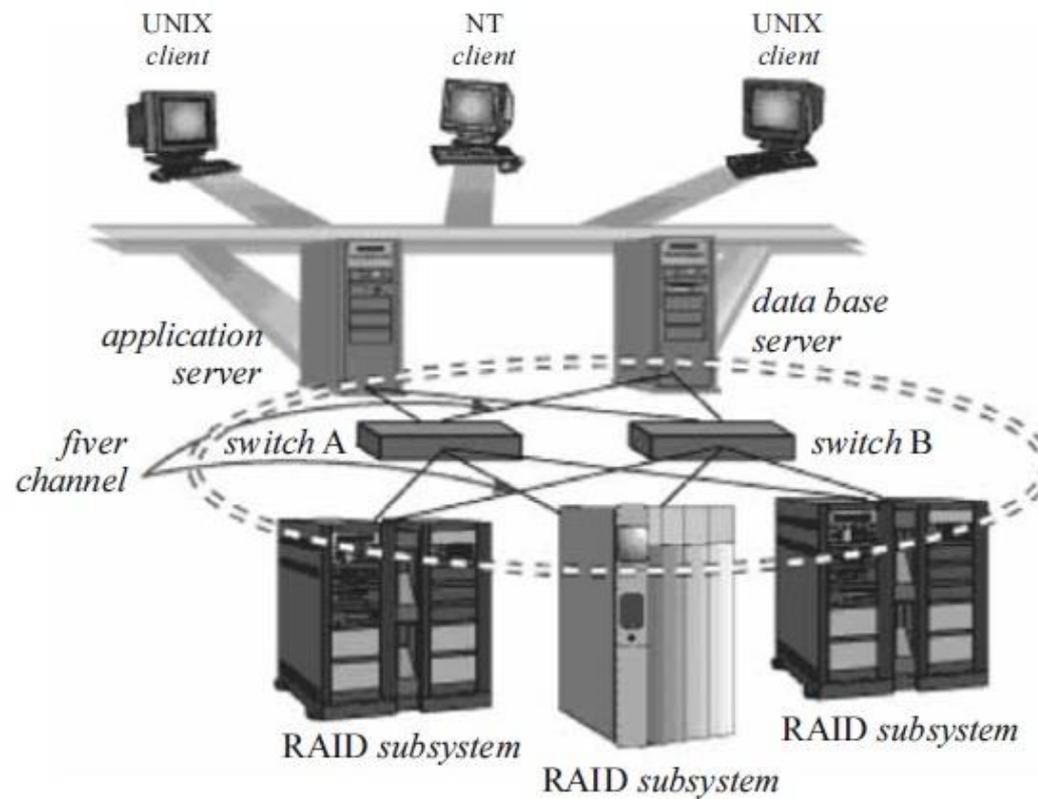
[114] Ao se utilizar um arranjo de disco do tipo RAID 5, são necessários pelo menos dois discos rígidos com o mesmo tamanho, para que o arranjo funcione corretamente.

6. Acerca de RAID, julgue os itens que se seguem.

 ~~[112] Para a implementação de RAID do tipo 6, é necessário um disco para armazenar a paridade dos dados. Esse tipo de arranjo de discos suporta a falha de somente um disco, que ainda assim consegue manter o acesso aos dados armazenados no arranjo.~~

 [113] Para atender à demanda de um servidor que necessita de alto desempenho no acesso aos dados gravados nos seus discos rígidos, o administrador deve optar por RAID do tipo 0, em vez de discos rígidos individuais.

 ~~[114] Ao se utilizar um arranjo de disco do tipo RAID 5, são necessários pelo menos dois discos rígidos com o mesmo tamanho, para que o arranjo funcione corretamente.~~



Internet: <www.storagesearch.com/auspexart.html>.

7. Considerando que, na figura apresentada, o sistema de armazenamento de discos empregue a tecnologia RAID (redundant array of independent/inexpensive drives), comumente presente nesse tipo de sistema, julgue os itens subsecutivos.

[99] As tecnologias RAID proporcionam aumento do desempenho do acesso a disco, em decorrência da distribuição de blocos de dados em estrias (stripes), por meio de discos diferentes, que podem ser acessados concorrentemente.

[100] Em tecnologia RAID 5, são usados dados redundantes que possibilitam a recuperação de dados caso um dos discos do arranjo falhe. Essa tecnologia, no entanto, não permite a recuperação de dados caso haja falha simultânea de dois discos que contenham blocos de dados de um mesmo arquivo.

[101] A tecnologia RAID 0 pressupõe a existência de dois ou mais discos configurados com dados distribuídos redundantemente entre eles, de modo que, caso um dos discos do arranjo falhe, as configurações RAID 0 introduzem um mecanismo eficiente de proteção contra perda de dados..

7. Considerando que, na figura apresentada, o sistema de armazenamento de discos empregue a tecnologia RAID (redundant array of independent/inexpensive drives), comumente presente nesse tipo de sistema, julgue os itens subsecutivos.

 [99] As tecnologias RAID proporcionam aumento do desempenho do acesso a disco, em decorrência da distribuição de blocos de dados em estrias (stripes), por meio de discos diferentes, que podem ser acessados concorrentemente.

 [100] Em tecnologia RAID 5, são usados dados redundantes que possibilitam a recuperação de dados caso um dos discos do arranjo falhe. Essa tecnologia, no entanto, não permite a recuperação de dados caso haja falha simultânea de dois discos que contenham blocos de dados de um mesmo arquivo.

 ~~[101] A tecnologia RAID 0 pressupõe a existência de dois ou mais discos configurados com dados distribuídos redundantemente entre eles, de modo que, caso um dos discos do arranjo falhe, as configurações RAID 0 introduzem um mecanismo eficiente de proteção contra perda de dados.~~

8. Com relação aos tipos de servidores e RAID, julgue os itens subsequentes.

[59] Em uma solução específica de hardware do tipo storage, é possível configurar diferentes tipos de RAID ao mesmo tempo. Assim, é possível obter segurança de dados, incrementar velocidade de leitura/escrita de dados e maximizar a possibilidade de tolerância a falhas em disco, com RAID 0, 1 e 5, respectivamente.

[61] Servidores de aplicação e de banco de dados podem ser instalados em máquinas que disponham de controladoras RAID que permitem gerenciar vários discos ao mesmo tempo, com exceção de discos de SSD (solid-state drive), que são voltados para notebooks e outros mobiles, não indicados para serem utilizados em servidores.

8. Com relação aos tipos de servidores e RAID, julgue os itens subsequentes.

 ~~[59] Em uma solução específica de hardware do tipo storage, é possível configurar diferentes tipos de RAID ao mesmo tempo. Assim, é possível obter segurança de dados, incrementar velocidade de leitura/escrita de dados e maximizar a possibilidade de tolerância a falhas em disco, com RAID 0, 1 e 5, respectivamente.~~

 ~~[61] Servidores de aplicação e de banco de dados podem ser instalados em máquinas que disponham de controladoras RAID que permitem gerenciar vários discos ao mesmo tempo, com exceção de discos de SSD (solid state drive), que são voltados para notebooks e outros mobiles, não indicados para serem utilizados em servidores.~~

9. A respeito de soluções de alta disponibilidade, julgue os itens a seguir.

[97] O arranjo de RAID (redundant arrays of inexpensive disks) do tipo 1 é capaz de melhorar o desempenho de gravação dos dados, visto que, nesse tipo de arranjo, os dados são gravados de forma distribuída e simultânea, sem redundância de gravação quando restaurados em caso de pane em um disco rígido do arranjo.

[98] A implementação do arranjo de RAID do tipo 5 possibilita redundância dos dados e deve ser feita com, no mínimo, três discos rígidos.

9. A respeito de soluções de alta disponibilidade, julgue os itens a seguir.

 ~~[97] O arranjo de RAID (redundant arrays of inexpensive disks) do tipo 1 é capaz de melhorar o desempenho de gravação dos dados, visto que, nesse tipo de arranjo, os dados são gravados de forma distribuída e simultânea, sem redundância de gravação quando restaurados em caso de pane em um disco rígido do arranjo.~~

 [98] A implementação do arranjo de RAID do tipo 5 possibilita redundância dos dados e deve ser feita com, no mínimo, três discos rígidos.

10. A respeito da tecnologia RAID (redundant array of independent disks) julgue o próximo item.

[80] O sistema RAID consiste em um conjunto de dois ou mais discos rígidos com dois objetivos básicos. O primeiro, por meio de uma técnica chamada divisão de dados (data stripping ou RAID 1), consiste em tornar o sistema de disco mais rápido, enquanto o segundo, mediante uma técnica chamada espelhamento (mirroring ou RAID 0), consiste em tornar o sistema de disco mais seguro. Essas duas técnicas podem ser usadas isoladamente ou em conjunto.

10. A respeito da tecnologia RAID (redundant array of independent disks) julgue o próximo item.

~~[80] O sistema RAID consiste em um conjunto de dois ou mais discos rígidos com dois objetivos básicos. O primeiro, por meio de uma técnica chamada divisão de dados (data stripping ou RAID 1), consiste em tornar o sistema de disco mais rápido, enquanto o segundo, mediante uma técnica chamada espelhamento (mirroring ou RAID 0), consiste em tornar o sistema de disco mais seguro. Essas duas técnicas podem ser usadas isoladamente ou em conjunto.~~



GABARITO



1. B

2. E, C, C

3. C

4. B

5. C, E

6. E, C, E

7. C, C, E

8. E, E

9. E, C

10.E

Quinta Bateria de Questões Com Resolução Assistida

Dispositivos de segurança: **NAT, VPN**

1. Acerca da rede privada virtual (VPN) e de suas formas de uso, julgue os itens subsequentes.

[113] Em VPN com uso de IPSEC, são suportados basicamente dois modos de operação: o modo transporte, que é utilizado para ligação de túneis virtuais; e o modo túnel, para estabelecer comunicação entre dois hosts, apenas.

[114] Geralmente, VPN site-to-site permite que recursos de uma localidade sejam disponibilizados para usuários em outra localidade remota por meio de um canal de comunicação seguro mediante o uso da Internet.

[115] Em soluções modernas de VPN user-to-site, o processo de autenticação de um usuário remoto pode ser feito pelo servidor VPN ou este servidor pode delegar essa função a um servidor de autenticação. Nesse segundo caso, soluções de autenticação por certificação digital não são suportadas.

1. Acerca da rede privada virtual (VPN) e de suas formas de uso, julgue os itens subsequentes.

 ~~[113] Em VPN com uso de IPSEC, são suportados basicamente dois modos de operação: o modo transporte, que é utilizado para ligação de túneis virtuais; e o modo túnel, para estabelecer comunicação entre dois hosts, apenas.~~

 [114] Geralmente, VPN site-to-site permite que recursos de uma localidade sejam disponibilizados para usuários em outra localidade remota por meio de um canal de comunicação seguro mediante o uso da Internet.

 ~~[115] Em soluções modernas de VPN user-to-site, o processo de autenticação de um usuário remoto pode ser feito pelo servidor VPN ou este servidor pode delegar essa função a um servidor de autenticação. Nesse segundo caso, soluções de autenticação por certificação digital não são suportadas.~~

2. Acerca do NAT (network address translation) em um gateway com a função de conectar a rede interna de uma organização à Internet, julgue os itens seguintes

[85] Se o gateway for configurado no modo bridge (ponte), uma estação de trabalho que utilize o IP privado 192.168.0.100, com máscara de rede 255.255.255.0, poderá acessar a Internet sem a intervenção do recurso NAT, isto é, sem que ocorra a tradução de endereço no gateway.

[86] O endereço e a porta de origem inscritos nos pacotes que, provenientes da Internet, passam pelo gateway com destino a uma estação de trabalho na rede interna podem ser alterados pela variante do NAT conhecida como NAPT (network address and port translation).

[87] O gateway encarregado de fazer o NAT para o tráfego originado na rede interna e destinado à Internet armazena, em uma tabela NAT, as informações acerca das conexões correntes. Caso uma pane ocasione perda dos dados dessa tabela, as conexões TCP não serão destruídas, pois esse protocolo tem recursos para preservar as conexões nessa situação.

[88] Por padrão o NAT funciona adequadamente com os protocolos TCP e UDP. Caso seja criado um protocolo de transporte diferente para acesso a uma aplicação, que necessite atravessar o gateway para ser acessada, cujo tráfego sofra o processo de NAT, o acesso a essa aplicação falhará.

[89] As estações de trabalho da rede interna podem acessar a Internet utilizando endereços IPs privados. Para isso, é necessário que as estações de trabalho tenham, em suas configurações de rede, o endereço do equipamento de gateway e este deve ter a capacidade de trocar nos pacotes encaminhados à Internet o endereço privado por um endereço público.

2. Acerca do NAT (network address translation) em um gateway com a função de conectar a rede interna de uma organização à Internet, julgue os itens seguintes

 ~~[85] Se o gateway for configurado no modo bridge (ponte), uma estação de trabalho que utilize o IP privado 192.168.0.100, com máscara de rede 255.255.255.0, poderá acessar a Internet sem a intervenção do recurso NAT, isto é, sem que ocorra a tradução de endereço no gateway.~~

 [86] O endereço e a porta de origem inscritos nos pacotes que, provenientes da Internet, passam pelo gateway com destino a uma estação de trabalho na rede interna podem ser alterados pela variante do NAT conhecida como NAPT (network address and port translation).

 ~~[87] O gateway encarregado de fazer o NAT para o tráfego originado na rede interna e destinado à Internet armazena, em uma tabela NAT, as informações acerca das conexões correntes. Caso uma pane ocasione perda dos dados dessa tabela, as conexões TCP não serão destruídas, pois esse protocolo tem recursos para preservar as conexões nessa situação.~~

 ~~[88] Por padrão o NAT funciona adequadamente com os protocolos TCP e UDP. Caso seja criado um protocolo de transporte diferente para acesso a uma aplicação, que necessite atravessar o gateway para ser acessada, cujo tráfego sofra o processo de NAT, o acesso a essa aplicação falhará.~~

 [89] As estações de trabalho da rede interna podem acessar a Internet utilizando endereços IPs privados. Para isso, é necessário que as estações de trabalho tenham, em suas configurações de rede, o endereço do equipamento de gateway e este deve ter a capacidade de trocar nos pacotes encaminhados à Internet o endereço privado por um endereço público.

3. Assinale a opção correta acerca de NAT (network address translation).

- A. Apesar de não fornecer recursos de conexão de tráfego, como rastreamento de usuário, sítios ou conexões, a NAT permite que administradores de redes proíbam acesso a determinados sítios.
- B. O mecanismo de NAT é utilizado exclusivamente por roteadores que operam na camada 3 ou acima.
- C. Na NAT do tipo dinâmica sobrecarregada vários endereços IP não registrados são mapeados para um único endereço IP registrado, utilizando diferentes portas.
- D. Na NAT do tipo dinâmica sobreposta um endereço IP não registrado é mapeado para um endereço IP, registrado com uma base unívoca.
- E. Em uma mesma rede, não é possível usar a NAT e o DHCP, pois eles são mutuamente exclusivos.

3. Assinale a opção correta acerca de NAT (network address translation).

- A. Apesar de não fornecer recursos de conexão de tráfego, como rastreamento de usuário, sítios ou conexões, a NAT permite que administradores de redes proíbam acesso a determinados sítios.
- B. O mecanismo de NAT é utilizado exclusivamente por roteadores que operam na camada 3 ou acima.
-  C. Na NAT do tipo dinâmica sobrecarregada vários endereços IP não registrados são mapeados para um único endereço IP registrado, utilizando diferentes portas.
- D. Na NAT do tipo dinâmica sobreposta um endereço IP não registrado é mapeado para um endereço IP, registrado com uma base unívoca.
- E. Em uma mesma rede, não é possível usar a NAT e o DHCP, pois eles são mutuamente exclusivos.

4. Acerca de VPN (Virtual Private Network), assinale a opção correta.

- A. Uma VPN provê uma utilização do canal de comunicação mais racional, por não manter links permanentes entre os pontos de comunicação, mas não possui a função de autenticar pacotes de dados em relação à sua origem.
- B. Funções de hash, MACs (Message Authentication Codes) e assinaturas digitais visam assegurar a integridade das mensagens em uma VPN.
- C. Embora uma VPN possua maior custo do que as linhas dedicadas, ela fornece confidencialidade por meio de criptografia com chave pública ou privada.
- D. RADIUS (Remote Authentication Dial-In User Service) e CHAP (Challenge-Handshake Authentication Protocol) garantem às VPNs não repúdio e disponibilidade, respectivamente.
- E. Os protocolos de tunelamento são limitados às linhas dedicadas e aos circuitos virtuais permanentes e, portanto, não podem ser utilizados em VPNs.

4. Acerca de VPN (Virtual Private Network), assinale a opção correta.

- A. Uma VPN provê uma utilização do canal de comunicação mais racional, por não manter links permanentes entre os pontos de comunicação, mas não possui a função de autenticar pacotes de dados em relação à sua origem.
-  B. Funções de hash, MACs (Message Authentication Codes) e assinaturas digitais visam assegurar a integridade das mensagens em uma VPN.
- C. Embora uma VPN possua maior custo do que as linhas dedicadas, ela fornece confidencialidade por meio de criptografia com chave pública ou privada.
- D. RADIUS (Remote Authentication Dial-In User Service) e CHAP (Challenge-Handshake Authentication Protocol) garantem às VPNs não repúdio e disponibilidade, respectivamente.
- E. Os protocolos de tunelamento são limitados às linhas dedicadas e aos circuitos virtuais permanentes e, portanto, não podem ser utilizados em VPNs.

5. Julgue os itens seguintes, acerca de VPN e VPN-SSL.

[85] As redes VPN oferecem suporte apenas ao protocolo IP.

[86] O SSL tunnel VPN permite que o navegador acesse aplicações e serviços de rede por meio de um túnel que ele esteja executando sob o SSL.

[87] Quando se utiliza um firewall com funções de VPN, as mensagens entram cifradas na rede e somente são decifradas no nível de aplicação.

5. Julgue os itens seguintes, acerca de VPN e VPN-SSL.

~~[85] As redes VPN oferecem suporte apenas ao protocolo IP.~~



[86] O SSL tunnel VPN permite que o navegador acesse aplicações e serviços de rede por meio de um túnel que ele esteja executando sob o SSL.



~~[87] Quando se utiliza um firewall com funções de VPN, as mensagens entram cifradas na rede e somente são decifradas no nível de aplicação.~~



6. Julgue os itens subsecutivos, referentes a firewall e VPN (virtual private network).

[58] VPN que utilize o protocolo IPSEC (IP security) tem mecanismos para a validação da confidencialidade e da integridade dos dados transmitidos.

6. Julgue os itens subsecutivos, referentes a firewall e VPN (virtual private network).

[58] VPN que utilize o protocolo IPSEC (IP security) tem mecanismos para a validação da confidencialidade e da integridade dos dados transmitidos.



7. Em relação à VPN (virtual private network), julgue os próximos itens.

[72] Em VPN do tipo USER-TO-SITE, o túnel só é estabelecido se for utilizado o protocolo IPSec.

[73] Em VPN do tipo SITE-TO-SITE, o usuário é o responsável pelo estabelecimento do túnel.

7. Em relação à VPN (virtual private network), julgue os próximos itens.

~~[72] Em VPN do tipo USER-TO-SITE, o túnel só é estabelecido se for utilizado o protocolo IPSec.~~



~~[73] Em VPN do tipo SITE-TO-SITE, o usuário é o responsável pelo estabelecimento do túnel.~~



8. Em relação a segurança da informação, julgue os itens seguintes.

[84] Em uma VPN com IPSEC é possível fazer uso do 3DES com algoritmo de criptografia que emprega três chaves de 56 bits.

[85] O recurso VPN (virtual private network), utilizado para interligar de forma segura dois pontos através de um meio público como a Internet, pode fazer uso de IPSEC, que recorre ao ESP (encapsulating security payload) para manter a confidencialidade dos dados e à AH (authentication header) para garantir a integridade dos dados.

8. Em relação a segurança da informação, julgue os itens seguintes.

 [84] Em uma VPN com IPSEC é possível fazer uso do 3DES com algoritmo de criptografia que emprega três chaves de 56 bits.

 [85] O recurso VPN (virtual private network), utilizado para interligar de forma segura dois pontos através de um meio público como a Internet, pode fazer uso de IPSEC, que recorre ao ESP (encapsulating security payload) para manter a confidencialidade dos dados e à AH (authentication header) para garantir a integridade dos dados.

9. Com relação a switches, roteadores e NAT (network address translation), julgue os itens subsequentes.

[89] Considere que uma empresa tenha dez computadores que precisam ser conectados à Internet, mas disponha de apenas um endereço IP válido. Nesse caso, recomenda-se a utilização de NAT, pois cada computador terá um endereço privado dentro da LAN e, por meio da porta TCP de destino que se deseja acessar no endereço remoto, o dispositivo responsável por implementar NAT conseguirá identificar o retorno da resposta ao computador interno.

9. Com relação a switches, roteadores e NAT (network address translation), julgue os itens subsequentes.

 ~~[89] Considere que uma empresa tenha dez computadores que precisam ser conectados à Internet, mas disponha de apenas um endereço IP válido. Nesse caso, recomenda-se a utilização de NAT, pois cada computador terá um endereço privado dentro da LAN e, por meio da porta TCP de destino que se deseja acessar no endereço remoto, o dispositivo responsável por implementar NAT conseguirá identificar o retorno da resposta ao computador interno.~~

10. No que concerne a VPN (Virtual Private Network), julgue os itens subsequentes.

[59] Em um filtro de pacotes que atue como firewall em uma rede por onde se verifique tráfego VPN IPSEC (Internet Protocol Security), é necessário liberar a porta 500 e o protocolo UDP (User Datagram Protocol) para o funcionamento da VPN.

[60] O uso do protocolo AH (Authentication Header) no IPSEC (Internet Protocol Security) de uma VPN tem a função de garantir a confidencialidade dos dados trafegados.

10. No que concerne a VPN (Virtual Private Network), julgue os itens subsequentes.

 [59] Em um filtro de pacotes que atue como firewall em uma rede por onde se verifique tráfego VPN IPSEC (Internet Protocol Security), é necessário liberar a porta 500 e o protocolo UDP (User Datagram Protocol) para o funcionamento da VPN.

 ~~[60] O uso do protocolo AH (Authentication Header) no IPSEC (Internet Protocol Security) de uma VPN tem a função de garantir a confidencialidade dos dados trafegados.~~

GABARITO



1. E, C, E

2. E, C, E, E, C

3. C

4. B

5. E, C, E

6. C

7. E, E

8. C, C

9. E

10. C, E

Quinta Bateria de Questões Com Resolução Assistida

Dispositivos de segurança: **Proxies**

1. Julgue os próximos itens, com relação a auditoria, prevenção de intrusão e proxy.

[83] Os servidores proxy criam um cache com as solicitações de cada usuário, de forma a otimizar consultas futuras de um mesmo usuário, sendo esse cache de uso exclusivo de seu respectivo usuário.

1. Julgue os próximos itens, com relação a auditoria, prevenção de intrusão e proxy.

 ~~[83] Os servidores proxy criam um cache com as solicitações de cada usuário, de forma a otimizar consultas futuras de um mesmo usuário, sendo esse cache de uso exclusivo de seu respectivo usuário.~~

2. A respeito da segurança de redes de computadores, julgue os itens de 86 a 90.

[86] Se um firewall estiver entre dois segmentos físicos de rede e o endereçamento de uma rede for 192.168.1.0/25 e da outra, 192.168.1.0/26, para que os computadores desses dois segmentos possam se comunicar entre si, é obrigatório utilizar o recurso de NAT (network address translation) no firewall.

[89] O serviço de proxy no sistema operacional Linux, provido pelo software Squid, utiliza o protocolo HTTP, sendo capaz de fazer cache de páginas web estáticas e otimizar o acesso, diminuindo o consumo do link de Internet. Além disso, é capaz de filtrar acessos a sítios web definidos previamente em sua configuração.

2. A respeito da segurança de redes de computadores, julgue os itens de 86 a 90.

 ~~[86] Se um firewall estiver entre dois segmentos físicos de rede e o endereçamento de uma rede for 192.168.1.0/25 e da outra, 192.168.1.0/26, para que os computadores desses dois segmentos possam se comunicar entre si, é obrigatório utilizar o recurso de NAT (network address translation) no firewall.~~

 [89] O serviço de proxy no sistema operacional Linux, provido pelo software Squid, utiliza o protocolo HTTP, sendo capaz de fazer cache de páginas web estáticas e otimizar o acesso, diminuindo o consumo do link de Internet. Além disso, é capaz de filtrar acessos a sítios web definidos previamente em sua configuração.

3. A respeito de segurança de redes de comunicação, julgue os itens que se seguem.

[118] O uso de proxy reverso torna mais rápido o acesso a um servidor de páginas web, tendo em vista que ele faz cache das páginas acessadas.

3. A respeito de segurança de redes de comunicação, julgue os itens que se seguem.

[118] O uso de proxy reverso torna mais rápido o acesso a um servidor de páginas web, tendo em vista que ele faz cache das páginas acessadas.



4. Com relação a aspectos de intranet e de Internet, julgue os itens que se seguem.

[119] No caso de se utilizar um servidor proxy firewall para acessar um sítio na Internet, o cliente não troca pacotes de informações diretamente com o servidor solicitado.

4. Com relação a aspectos de intranet e de Internet, julgue os itens que se seguem.

[119] No caso de se utilizar um servidor proxy firewall para acessar um sítio na Internet, o cliente não troca pacotes de informações diretamente com o servidor solicitado.



5. Julgue os itens a seguir, a respeito de segurança da informação.

[91] O bloqueio seguro a uma rede restrita de uma empresa poderá ser efetuado por meio de uma DMZ. Para a criação de uma DMZ dessa natureza, é suficiente utilizar um firewall do tipo Proxy.

5. Julgue os itens a seguir, a respeito de segurança da informação.

~~[91] O bloqueio seguro a uma rede restrita de uma empresa poderá ser efetuado por meio de uma DMZ. Para a criação de uma DMZ dessa natureza, é suficiente utilizar um firewall do tipo Proxy.~~



6. A respeito de roteadores, switches, proxies, Internet e intranet, julgue os próximos itens

[70] Caching web proxy constitui um web proxy usado como cache para páginas da Internet e arquivos disponíveis em servidores remotos da Internet, para que possam ser acessados mais rapidamente pelos clientes de uma rede local (LAN).

[73] Proxy constitui um servidor que recebe requisições de clientes e normalmente as repassa a servidores específicos, podendo, opcionalmente, alterar a requisição do cliente ou a resposta do servidor final e, algumas vezes, disponibilizar, ele próprio, o recurso requisitado, sem necessidade de repassar a requisição a outro servidor.

6. A respeito de roteadores, switches, proxies, Internet e intranet, julgue os próximos itens

 [70] Caching web proxy constitui um web proxy usado como cache para páginas da Internet e arquivos disponíveis em servidores remotos da Internet, para que possam ser acessados mais rapidamente pelos clientes de uma rede local (LAN).

 [73] Proxy constitui um servidor que recebe requisições de clientes e normalmente as repassa a servidores específicos, podendo, opcionalmente, alterar a requisição do cliente ou a resposta do servidor final e, algumas vezes, disponibilizar, ele próprio, o recurso requisitado, sem necessidade de repassar a requisição a outro servidor.

7. O endereço IP de uma rede local é 10.100.100.0/24 e a única saída para a Internet é um roteador de saída cujo endereço IP é 200.20.20.1/30. Considerando que o administrador dessa rede tenha definido a utilização do NAT, julgue os itens seguintes.

[82] Se existir um servidor web respondendo na porta 443 na rede 10, então, a fim de tornar esse servidor visível na Internet, o roteador deverá ser configurado para encaminhar todos os pacotes com destino o endereço IP 200.20.20.1 na porta 443 para o IP interno do servidor web. Ao retornar os pacotes, o roteador deverá modificar o IP de origem para 200.20.20.1.

[83] Se o administrador utilizar um proxy na rede 10, o NAT para esse proxy deve usar o endereço IP 200.20.20.1 para a internet e o roteador de saída deve fazer o tratamento da conversão de endereços.

7. O endereço IP de uma rede local é 10.100.100.0/24 e a única saída para a Internet é um roteador de saída cujo endereço IP é 200.20.20.1/30. Considerando que o administrador dessa rede tenha definido a utilização do NAT, julgue os itens seguintes.

 [82] Se existir um servidor web respondendo na porta 443 na rede 10, então, a fim de tornar esse servidor visível na Internet, o roteador deverá ser configurado para encaminhar todos os pacotes com destino o endereço IP 200.20.20.1 na porta 443 para o IP interno do servidor web. Ao retornar os pacotes, o roteador deverá modificar o IP de origem para 200.20.20.1.

 [83] Se o administrador utilizar um proxy na rede 10, o NAT para esse proxy deve usar o endereço IP 200.20.20.1 para a internet e o roteador de saída deve fazer o tratamento da conversão de endereços.

GABARITO



1. E

6. C, C

2. E, C

7. C, C

3. C

4. C

5. E

Sexta_Bateria de Questões Com Resolução Assistida

Arquitetura e Organização de
Computadores

RISC CISC



1. Acerca da arquitetura de servidores, julgue o item seguinte.

[101] Atualmente, os fabricantes de computadores têm adotado exclusivamente a arquitetura RISC para o desenvolvimento de chips para processadores, dado o melhor desempenho dessa arquitetura em relação à arquitetura CISC.

1. Acerca da arquitetura de servidores, julgue o item seguinte.

 ~~[101] Atualmente, os fabricantes de computadores têm adotado exclusivamente a arquitetura RISC para o desenvolvimento de chips para processadores, dado o melhor desempenho dessa arquitetura em relação à arquitetura CISC.~~

2. Acerca das arquiteturas de hardware de servidores RISC, CISC e Mainframe, julgue os itens a seguir.

[96] A abordagem da arquitetura CISC (complex instruction set computer) procura minimizar o número de ciclos para que uma instrução seja executada, e aumenta, em contrapartida, o número de instruções por programa.

[97] A arquitetura RISC (reduced instruction set computer) busca reduzir o número de ciclos necessários para que uma instrução seja executada, sendo amplamente utilizada em processadores que têm por base o conjunto de instruções x86, desde as primeiras versões desses processadores.

[98] Os mainframes IBM recentes possuem, em sua arquitetura de hardware, não apenas uma CPU (central processing unit), mas também um CPC (central processor complex), o qual pode conter diferentes tipos de processadores a serem utilizados para diferentes propósitos.

2. Acerca das arquiteturas de hardware de servidores RISC, CISC e Mainframe, julgue os itens a seguir.

 ~~[96] A abordagem da arquitetura CISC (complex instruction set computer) procura minimizar o número de ciclos para que uma instrução seja executada, e aumenta, em contrapartida, o número de instruções por programa.~~

 ~~[97] A arquitetura RISC (reduced instruction set computer) busca reduzir o número de ciclos necessários para que uma instrução seja executada, sendo amplamente utilizada em processadores que têm por base o conjunto de instruções x86, desde as primeiras versões desses processadores.~~

 [98] Os mainframes IBM recentes possuem, em sua arquitetura de hardware, não apenas uma CPU (central processing unit), mas também um CPC (central processor complex), o qual pode conter diferentes tipos de processadores a serem utilizados para diferentes propósitos.

3. A respeito das arquiteturas de hardware RISC e CISC, assinale a opção correta.
- A. A unidade de medida mais eficiente e mais utilizada para a comparação dos processados de ambas as arquiteturas é o MIPS (milhões de instruções por segundo).
 - B. As máquinas RISC executam instruções com maior rapidez do que as máquinas CISC, já que o faz por meio de subprogramas e não por meio da execução direta pelo hardware.
 - C. Diversamente do que ocorre na arquitetura RISC, na CISC as chamadas de funções ocorrem basicamente no processador, empregando-se um número menor de registradores, o que contribui para um aumento no desempenho total do processador.
 - D. Na arquitetura CISC, não se permite a utilização de muitos modos de endereçamento para realizar uma instrução que retorne o resultado da divisão de A por B.
 - E. O pipelining, execução de várias instruções simultaneamente no processador, é utilizado tanto em máquinas RISC quanto CISC.

3. A respeito das arquiteturas de hardware RISC e CISC, assinale a opção correta.
- A. A unidade de medida mais eficiente e mais utilizada para a comparação dos processados de ambas as arquiteturas é o MIPS (milhões de instruções por segundo).
 - B. As máquinas RISC executam instruções com maior rapidez do que as máquinas CISC, já que o faz por meio de subprogramas e não por meio da execução direta pelo hardware.
 - C. Diversamente do que ocorre na arquitetura RISC, na CISC as chamadas de funções ocorrem basicamente no processador, empregando-se um número menor de registradores, o que contribui para um aumento no desempenho total do processador.
 - D. Na arquitetura CISC, não se permite a utilização de muitos modos de endereçamento para realizar uma instrução que retorne o resultado da divisão de A por B.
 - E. O pipelining, execução de várias instruções simultaneamente no processador, é utilizado tanto em máquinas RISC quanto CISC.



4. A respeito das arquiteturas de hardware existentes em servidores, julgue os itens que se seguem

[86] Mainframes são computadores de grande porte projetados para lidar com grande vazão de dados e para serem altamente confiáveis e seguros.

[87] Um mainframe possui múltiplas unidades de processamento, sendo cada unidade um processador comum, tipicamente Intel ou AMD.

[88] Processadores RISC e CISC diferem, fundamentalmente, no tamanho e na complexidade do conjunto de instruções.

4. A respeito das arquiteturas de hardware existentes em servidores, julgue os itens que se seguem

 [86] Mainframes são computadores de grande porte projetados para lidar com grande vazão de dados e para serem altamente confiáveis e seguros.

 ~~[87] Um mainframe possui múltiplas unidades de processamento, sendo cada unidade um processador comum, tipicamente Intel ou AMD.~~

 [88] Processadores RISC e CISC diferem, fundamentalmente, no tamanho e na complexidade do conjunto de instruções.

5. No que concerne a RISC e CISC, julgue os itens a seguir

[84] Para que seja possível a execução otimizada de chamada de funções, máquinas RISC fazem uso de registradores da unidade central de processamento para armazenar parâmetros e variáveis em chamadas de rotina e funções.

[85] A arquitetura RISC possui um conjunto de instruções menor que o CISC; em consequência disso, o sistema que utiliza a arquitetura RISC produz resultados com menor desempenho que um sistema que utilize CISC.

5. No que concerne a RISC e CISC, julgue os itens a seguir

 [84] Para que seja possível a execução otimizada de chamada de funções, máquinas RISC fazem uso de registradores da unidade central de processamento para armazenar parâmetros e variáveis em chamadas de rotina e funções.

 ~~[85] A arquitetura RISC possui um conjunto de instruções menor que o CISC; em consequência disso, o sistema que utiliza a arquitetura RISC produz resultados com menor desempenho que um sistema que utilize CISC.~~

6. Em relação aos sistemas de numeração, à organização e à arquitetura de computadores, julgue os itens a seguir.

[66] Uma das características das arquiteturas RISC é a utilização em larga escala de pipelining.

[68] O decodificador de instrução é o dispositivo mais complexo de um processador, pois ele contém a lógica necessária para realizar a movimentação de instruções a partir do processador e para o processador, por meio de sinais de controle emitidos em instantes de tempo programados.

6. Em relação aos sistemas de numeração, à organização e à arquitetura de computadores, julgue os itens a seguir.

 [66] Uma das características das arquiteturas RISC é a utilização em larga escala de pipelining.

 ~~[68] O decodificador de instrução é o dispositivo mais complexo de um processador, pois ele contém a lógica necessária para realizar a movimentação de instruções a partir do processador e para o processador, por meio de sinais de controle emitidos em instantes de tempo programados.~~

7. Em ambientes de datacenters bancários, é comum a coexistência de recursos de hardware considerados de plataforma baixa e os de plataforma alta. Acerca das razões técnicas que causam essa coexistência, julgue os itens seguintes.

[89] Ambientes de plataforma baixa podem ser implementados, indiferentemente, por meio das plataformas RISC ou CISC.

7. Em ambientes de datacenters bancários, é comum a coexistência de recursos de hardware considerados de plataforma baixa e os de plataforma alta. Acerca das razões técnicas que causam essa coexistência, julgue os itens seguintes.

~~[89] Ambientes de plataforma baixa podem ser implementados, indiferentemente, por meio das plataformas RISC ou CISC.~~



8. Com referência às arquiteturas de hardware RISC, Intel e storage, julgue os itens subsequentes.

[84] As máquinas RISC utilizam os registradores da CPU para armazenar parâmetros e variáveis em chamadas de rotina e funções.

[85] O paralelismo tem duas formas gerais: paralelismo no nível de instrução e paralelismo no nível de processador. O primeiro não é realizado nas arquiteturas RISC, pois requer maior complexidade nas operações.

[86] Atualmente, os processadores Intel contêm um núcleo RISC que executa as instruções mais simples - que normalmente são as mais comuns - em um único ciclo de caminho de dados, enquanto interpreta as instruções mais complexas no modo CISC.

8. Com referência às arquiteturas de hardware RISC, Intel e storage, julgue os itens subsequentes.

[84] As máquinas RISC utilizam os registradores da CPU para armazenar parâmetros e variáveis em chamadas de rotina e funções.

~~[85] O paralelismo tem duas formas gerais: paralelismo no nível de instrução e paralelismo no nível de processador. O primeiro não é realizado nas arquiteturas RISC, pois requer maior complexidade nas operações.~~

[86] Atualmente, os processadores Intel contêm um núcleo RISC que executa as instruções mais simples - que normalmente são as mais comuns - em um único ciclo de caminho de dados, enquanto interpreta as instruções mais complexas no modo CISC.

9. Com referência às características das arquiteturas RISC e Intel, julgue os itens que se seguem.

[111] Na arquitetura RISC, os processadores são projetados com um número elevado de registradores, pois a grande maioria das operações é do tipo registrador-registrador.

[112] Um computador com a arquitetura RISC trabalha com instruções de formato simples, as quais são executadas por microcódigo.

9. Com referência às características das arquiteturas RISC e Intel, julgue os itens que se seguem.

 [111] Na arquitetura RISC, os processadores são projetados com um número elevado de registradores, pois a grande maioria das operações é do tipo registrador-registrador.

 ~~[112] Um computador com a arquitetura RISC trabalha com instruções de formato simples, as quais são executadas por microcódigo.~~

10. A respeito das arquiteturas de computadores RISC e CISC, assinale a opção correta.
- A. Os computadores que implementam simultaneamente as arquiteturas RISC e CISC dispõem de processadores híbridos: um núcleo RISC executa instruções mais simples, enquanto instruções mais complexas são interpretadas na arquitetura CISC.
 - B. Na arquitetura RISC, é realizada mais de uma instrução em um ciclo de relógio.
 - C. A arquitetura CISC utiliza intensamente microcódigos que interpretam cada micro-operação de uma instrução.
 - D. Para melhoria de desempenho, a arquitetura CISC utiliza o princípio de paralelismo na execução de instrução, de forma a melhor explorar a técnica pipelining.
 - E. A abordagem RISC permite a simplificação de compiladores, uma vez que é mais simples gerar uma sequência de instruções de máquina a partir de instruções semelhantes a comandos de alto nível.

10. A respeito das arquiteturas de computadores RISC e CISC, assinale a opção correta.

-  A. Os computadores que implementam simultaneamente as arquiteturas RISC e CISC dispõem de processadores híbridos: um núcleo RISC executa instruções mais simples, enquanto instruções mais complexas são interpretadas na arquitetura CISC.
- B. Na arquitetura RISC, é realizada mais de uma instrução em um ciclo de relógio.
- C. A arquitetura CISC utiliza intensamente microcódigos que interpretam cada micro-operação de uma instrução.
- D. Para melhoria de desempenho, a arquitetura CISC utiliza o princípio de paralelismo na execução de instrução, de forma a melhor explorar a técnica pipelining.
- E. A abordagem RISC permite a simplificação de compiladores, uma vez que é mais simples gerar uma sequência de instruções de máquina a partir de instruções semelhantes a comandos de alto nível.

GABARITO



1. E

2. E, E, C

3. E

4. C, E, C

5. C, E

6. C, E

7. E

8. C, E, C

9. C, E

10. A

Sexta Bateria de Questões Com Resolução Assistida

Dispositivos de segurança: **Proxies**

1. De acordo com a ABNT NBR ISO/IEC 27002, devem ser implementados controles contra códigos maliciosos. Um mecanismo de controle contra esses códigos consiste no serviço de
- A. páginas web.
 - B. compartilhamento de arquivos.
 - C. roteamento de computadores.
 - D. resolução de nomes.
 - E. proxy integrado com antivírus.

1. De acordo com a ABNT NBR ISO/IEC 27002, devem ser implementados controles contra códigos maliciosos. Um mecanismo de controle contra esses códigos consiste no serviço de

~~A. páginas web.~~

~~B. compartilhamento de arquivos.~~

~~C. roteamento de computadores.~~

~~D. resolução de nomes.~~

E. proxy integrado com antivírus.

2. No que concerne a firewall, julgue os itens a seguir.

- [101] Os gateways de técnica de inspeção de estado comparam o padrão de bits de cada pacote de dados com um padrão conhecido e confiável, em vez de examinar os dados contidos no pacote.
- [103] Em uma rede de computadores que utiliza o firewall do tipo roteador de barreira, o endereço IP dos pontos da rede interna é substituído pelo endereço do servidor de segurança da rede.
- [104] Quando a rede de comunicação dispõe de firewall do tipo gateway servidor de proxy, é necessário o uso programas de administração para a filtragem dos pacotes com base no endereço IP.

2. No que concerne a firewall, julgue os itens a seguir.

[101] Os gateways de técnica de inspeção de estado comparam o padrão de bits de cada pacote de dados com um padrão conhecido e confiável, em vez de examinar os dados contidos no pacote.



~~[103] Em uma rede de computadores que utiliza o firewall do tipo roteador de barreira, o endereço IP dos pontos da rede interna é substituído pelo endereço do servidor de segurança da rede.~~



~~[104] Quando a rede de comunicação dispõe de firewall do tipo gateway servidor de proxy, é necessário o uso programas de administração para a filtragem dos pacotes com base no endereço IP.~~



3. Julgue os itens subsecutivos, referentes a proxy cache e proxy reverso.

[114] Proxy reverso pode encaminhar uma solicitação para um número de porta diferente da porta na qual a solicitação foi recebida originalmente.

[115] O proxy cache permite otimizar o tráfego originado da Internet, o que diminui o congestionamento e aumenta a velocidade de transferência de dados, contudo ele não desempenha nenhuma função relacionada com a segurança da rede de comunicação.

3. Julgue os itens subsecutivos, referentes a proxy cache e proxy reverso.

[114] Proxy reverso pode encaminhar uma solicitação para um número de porta diferente da porta na qual a solicitação foi recebida originalmente.



~~[115] O proxy cache permite otimizar o tráfego originado da Internet, o que diminui o congestionamento e aumenta a velocidade de transferência de dados, contudo ele não desempenha nenhuma função relacionada com a segurança da rede de comunicação.~~



4. A respeito dos conceitos de qualidade de serviço (QoS) e de segurança em redes de computadores, julgue os próximos itens.

[65] O firewall proxy de uma rede, quando recebe uma mensagem externa de um processo cliente-usuário, executa um processo de servidor para receber a solicitação, abre o pacote e determina se a solicitação é legítima. Em caso positivo, ele executa um processo cliente e envia a mensagem para o verdadeiro servidor na rede; em caso negativo, a mensagem é eliminada e um aviso de erro é enviado para o usuário externo.

4. A respeito dos conceitos de qualidade de serviço (QoS) e de segurança em redes de computadores, julgue os próximos itens.

[65] O firewall proxy de uma rede, quando recebe uma mensagem externa de um processo cliente-usuário, executa um processo de servidor para receber a solicitação, abre o pacote e determina se a solicitação é legítima. Em caso positivo, ele executa um processo cliente e envia a mensagem para o verdadeiro servidor na rede; em caso negativo, a mensagem é eliminada e um aviso de erro é enviado para o usuário externo.



5. Considere que a equipe de suporte técnico de determinada empresa necessite fazer escolhas, configurações e procedimentos concernentes a segurança da informação da rede de computadores dessa empresa. Nessa situação, julgue os itens seguintes.

[84] Se a empresa instalar um servidor proxy, este permitirá que se mantenha um registro dos sítios visitados pelos funcionários, contudo a utilização desse servidor causaria pequeno aumento do tempo de resposta a requisições HTTP de clientes.

[85] Ao se instalar um servidor proxy squid em computador com sistema operacional Linux, o serviço deve ser criado no usuário root, por motivo de segurança.

5. Considere que a equipe de suporte técnico de determinada empresa necessite fazer escolhas, configurações e procedimentos concernentes a segurança da informação da rede de computadores dessa empresa. Nessa situação, julgue os itens seguintes.

 ~~[84] Se a empresa instalar um servidor proxy, este permitirá que se mantenha um registro dos sítios visitados pelos funcionários, contudo a utilização desse servidor causaria pequeno aumento do tempo de resposta a requisições HTTP de clientes.~~

 ~~[85] Ao se instalar um servidor proxy squid em computador com sistema operacional Linux, o serviço deve ser criado no usuário root, por motivo de segurança.~~

6. Na rede de computadores de uma organização pública brasileira com diversos ativos, como, por exemplo, switches, roteadores, firewalls, estações de trabalho, hosts servidores de aplicação web, servidores de bancos de dados, é comum a ocorrência de ataques e de outros incidentes que comprometem a segurança de seus sistemas. Nessa organização, a definição de políticas e metodologias adequadas para se lidar com esse tipo de problema cabe ao departamento de TI.

A partir da situação apresentada acima, julgue os itens relativos à segurança da informação.

[180] Se o administrador da rede de computadores tiver de escolher entre implantar um proxy firewall ou um firewall do tipo packet filter, a sua decisão deverá basear-se em um dos dois critérios seguintes: necessidade de atuação na camada de aplicação ou maior vazão de dados. Se o critério preponderante for o primeiro, então, a decisão deve ser favorável à instalação de proxy firewalls; se for o segundo, deve ser escolhido um packet filter.

6. Na rede de computadores de uma organização pública brasileira com diversos ativos, como, por exemplo, switches, roteadores, firewalls, estações de trabalho, hosts servidores de aplicação web, servidores de bancos de dados, é comum a ocorrência de ataques e de outros incidentes que comprometem a segurança de seus sistemas. Nessa organização, a definição de políticas e metodologias adequadas para se lidar com esse tipo de problema cabe ao departamento de TI.

A partir da situação apresentada acima, julgue os itens relativos à segurança da informação.

[180] Se o administrador da rede de computadores tiver de escolher entre implantar um proxy firewall ou um firewall do tipo packet filter, a sua decisão deverá basear-se em um dos dois critérios seguintes: necessidade de atuação na camada de aplicação ou maior vazão de dados. Se o critério preponderante for o primeiro, então, a decisão deve ser favorável à instalação de proxy firewalls; se for o segundo, deve ser escolhido um packet filter.



7. Com relação a firewalls, julgue os itens subseqüentes

- Em uma rede protegida por firewall composto por proxies, quando um cliente, fora da rede, se comunica com um servidor, na rede, um proxy se faz passar pelo servidor e intermedeia a comunicação.
- Firewalls embasados em proxy são capazes de tratar diversos protocolos de aplicação. Por exemplo, um proxy de FTP deve ser capaz de tratar o protocolo de aplicação FTP para poder se fazer passar por esse serviço.

7. Com relação a firewalls, julgue os itens subseqüentes

-  Em uma rede protegida por firewall composto por proxies, quando um cliente, fora da rede, se comunica com um servidor, na rede, um proxy se faz passar pelo servidor e intermedeia a comunicação.
-  Firewalls embasados em proxy são capazes de tratar diversos protocolos de aplicação. Por exemplo, um proxy de FTP deve ser capaz de tratar o protocolo de aplicação FTP para poder se fazer passar por esse serviço.

8. Com relação segurança em redes de computadores, julgue os itens a seguir

[119] Com um proxy HTTP no firewall, os usuários remotos podem estabelecer uma conexão HTTP/TCP com o proxy, que examina o URL contido na mensagem de solicitação. Se a página solicitada for permitida para o host de origem, o proxy estabelece uma segunda conexão HTTP/TCP com o servidor e para ele encaminha a solicitação.

8. Com relação segurança em redes de computadores, julgue os itens a seguir

[119] Com um proxy HTTP no firewall, os usuários remotos podem estabelecer uma conexão HTTP/TCP com o proxy, que examina o URL contido na mensagem de solicitação. Se a página solicitada for permitida para o host de origem, o proxy estabelece uma segunda conexão HTTP/TCP com o servidor e para ele encaminha a solicitação.



9. Com relação a firewalls, proxies e IDS, julgue os itens seguintes

[144] Proxies têm funções idênticas a firewalls, mas, enquanto os proxies operam nas camadas TCP/IP 3 e 4, os firewalls atuam no nível da aplicação.

9. Com relação a firewalls, proxies e IDS, julgue os itens seguintes

~~[144] Proxies têm funções idênticas a firewalls, mas, enquanto os proxies operam nas camadas TCP/IP 3 e 4, os firewalls atuam no nível da aplicação.~~



GABARITO



1. E

2. C, E, E

3. C, E

4. C

5. E, E

6. C

7. C, C

8. C

9. E

Sétima Bateria de Questões Com Resolução Assistida

Arquitetura e Organização de
Computadores

SISTEMAS DE NUMERAÇÃO



1. Julgue os próximos itens a respeito de sistemas de numeração e aritmética computacional.

[56] No sistema binário, a operação de multiplicação dos números 1011 e 101 resulta no número 1000101.

[57] No sistema binário, a operação de subtração dos números 101101 e 100111 tem como resultado o número 000110.

1. Julgue os próximos itens a respeito de sistemas de numeração e aritmética computacional.

~~[56] No sistema binário, a operação de multiplicação dos números 1011 e 101 resulta no número 1000101.~~



[57] No sistema binário, a operação de subtração dos números 101101 e 100111 tem como resultado o número 000110.



2. Considerando-se os números 22B e 11E em hexadecimal, é correto afirmar que a diferença entre esses dois números, também em hexadecimal, é igual a

- A. 103.
- B. 10C.
- C. 10D.
- D. 11C.
- E. 11D.

2. Considerando-se os números 22B e 11E em hexadecimal, é correto afirmar que a diferença entre esses dois números, também em hexadecimal, é igual a

A. 103.

B. 10C.

 C. 10D.

D. 11C.

E. 11D.

3. A respeito de sistemas de entrada, saída e armazenamento, sistemas de numeração e de codificação e aritmética computacional, julgue os itens subsequentes.

[62] No sistema binário, a subtração dos números 1101110 e 10111 é igual a 1010111.

[63] No sistema binário, multiplicando-se os números 1011 e 1010 obtém-se o número 1101110.

[65] O número 1985 na base decimal é igual a 7121 em hexadecimal.

[66] O número 75 na base octal corresponde ao número 96 na base decimal.

3. A respeito de sistemas de entrada, saída e armazenamento, sistemas de numeração e de codificação e aritmética computacional, julgue os itens subsequentes.

 [62] No sistema binário, a subtração dos números 1101110 e 10111 é igual a 1010111.

 [63] No sistema binário, multiplicando-se os números 1011 e 1010 obtém-se o número 1101110.

 ~~[65] O número 1985 na base decimal é igual a 7121 em hexadecimal.~~

 ~~[66] O número 75 na base octal corresponde ao número 96 na base decimal.~~

4. Com relação aos sistemas de numeração e à aritmética computacional, julgue os itens subsequentes.

[65] O endereço codificado em hexadecimal como 10F é representado na base 2 pelo número 100001111.

[66] A soma dos endereços representados em hexadecimal pelos números 243A e B7D6 resulta no endereço DC10, também representado na base 16.

[67] Um espaço de armazenamento correspondente a 8 megabytes equivale, aproximadamente, a 2^{16} megabits.

4. Com relação aos sistemas de numeração e à aritmética computacional, julgue os itens subsequentes.

[65] O endereço codificado em hexadecimal como 10F é representado na base 2 pelo número 100001111.



[66] A soma dos endereços representados em hexadecimal pelos números 243A e B7D6 resulta no endereço DC10, também representado na base 16.



~~[67] Um espaço de armazenamento correspondente a 8 megabytes equivale, aproximadamente, a 2^{16} megabits.~~



5. O endereço IP

10001110111100000000111110101011, em binário, é equivalente, em decimal, a

- A. 124.241.15.172.
- B. 141.243.15.171.
- C. 142.240.15.171.
- D. 143.242.14.171.
- E. 144.241.14.172.

5. O endereço IP

10001110111100000000111110101011, em binário, é equivalente, em decimal, a

A. 124.241.15.172.

B. 141.243.15.171.

 C. 142.240.15.171.

D. 143.242.14.171.

E. 144.241.14.172.

GABARITO



1. E, C
2. C
3. C, C, E, E
4. C, C, E
5. C

Sétima Bateria de Questões Com Resolução Assistida

Malware: **Vírus de computador,
cavalo de tróia, adware, spyware,
backdoors, keylogger, worms**

1. Em relação à segurança e à proteção de informações na Internet, julgue os itens subsequentes

[107] Cavalo de Tróia, também conhecido como trojan, é um programa malicioso que, assim como os worms, possui instruções para auto-replicação.

[108] Spyware é um programa ou dispositivo que monitora as atividades de um sistema e transmite a terceiros informações relativas a essas atividades, sem o consentimento do usuário. Como exemplo, o keylogger é um spyware capaz de armazenar as teclas digitadas pelo usuário no teclado do computador.

[109] Vírus são programas que podem apagar arquivos importantes armazenados no computador, podendo ocasionar, até mesmo, a total inutilização do sistema operacional.

[110] Um tipo específico de phishing, técnica utilizada para obter informações pessoais ou financeiras de usuários da Internet, como nome completo, CPF, número de cartão de crédito e senhas, é o pharming, que redireciona a navegação do usuário para sítios falsos, por meio da técnica DNS cache poisoning.

1. Em relação à segurança e à proteção de informações na Internet, julgue os itens subsequentes

~~[107] Cavalo de Tróia, também conhecido como trojan, é um programa malicioso que, assim como os worms, possui instruções para auto-replicação.~~



[108] Spyware é um programa ou dispositivo que monitora as atividades de um sistema e transmite a terceiros informações relativas a essas atividades, sem o consentimento do usuário. Como exemplo, o keylogger é um spyware capaz de armazenar as teclas digitadas pelo usuário no teclado do computador.



[109] Vírus são programas que podem apagar arquivos importantes armazenados no computador, podendo ocasionar, até mesmo, a total inutilização do sistema operacional.



[110] Um tipo específico de phishing, técnica utilizada para obter informações pessoais ou financeiras de usuários da Internet, como nome completo, CPF, número de cartão de crédito e senhas, é o pharming, que redireciona a navegação do usuário para sítios falsos, por meio da técnica DNS cache poisoning.



2. Julgue os seguintes itens, relativos à segurança em redes de computadores.

[100] Phishing é a técnica empregada por vírus e cavalos de tróia para obter informações confidenciais do usuário, como, por exemplo, dados bancários.

2. Julgue os seguintes itens, relativos à segurança em redes de computadores.

~~[100] Phishing é a técnica empregada por vírus e cavalos de tróia para obter informações confidenciais do usuário, como, por exemplo, dados bancários.~~



3. Os computadores conectados em redes ou à Internet estão expostos ao ataque de muitos tipos de programas maliciosos. Acerca desses programas, julgue os itens subsequentes:

[89] Para que seja instalado em um computador, é necessário que o spyware seja explicitamente executado pelo usuário.

[90] Um cavalo de tróia é um tipo de programa malicioso que, uma vez instalado no computador, possibilita o seu controle remotamente.

[91] Um vírus é um programa malicioso que tem a capacidade de se auto-replicar, independentemente da execução de qualquer outro programa.

3. Os computadores conectados em redes ou à Internet estão expostos ao ataque de muitos tipos de programas maliciosos. Acerca desses programas, julgue os itens subsequentes:



[89] Para que seja instalado em um computador, é necessário que o spyware seja explicitamente executado pelo usuário.



[90] Um cavalo de tróia é um tipo de programa malicioso que, uma vez instalado no computador, possibilita o seu controle remotamente.



~~[91] Um vírus é um programa malicioso que tem a capacidade de se auto-replicar, independentemente da execução de qualquer outro programa.~~

4. Acerca da identificação de códigos maliciosos e de técnicas de phishing e spam, julgue os próximos itens

[93] Uma das maneiras de se combater, com antecedência, o ataque de phishing é a utilização de um servidor NFS (network file system) na rede local para os usuários.

[94] Em computador infectado com um código malicioso conhecido como cavalo de tróia (trojan), não são disponibilizadas portas para acessos de outros computadores.

[95] Uma das técnicas de phishing consiste em envenenar cache de servidores DNS, fornecendo, assim, URLs falsas aos usuários que consultam esse servidor DNS e apontando para servidores diferentes do original.

4. Acerca da identificação de códigos maliciosos e de técnicas de phishing e spam, julgue os próximos itens

 ~~[93] Uma das maneiras de se combater, com antecedência, o ataque de phishing é a utilização de um servidor NFS (network file system) na rede local para os usuários.~~

 ~~[94] Em computador infectado com um código malicioso conhecido como cavalo de tróia (trojan), não são disponibilizadas portas para acessos de outros computadores.~~

 [95] Uma das técnicas de phishing consiste em envenenar cache de servidores DNS, fornecendo, assim, URLs falsas aos usuários que consultam esse servidor DNS e apontando para servidores diferentes do original.

5. Malware é qualquer tipo de software que pode causar algum impacto negativo sobre a informação, podendo afetar sua disponibilidade, integridade e confidencialidade. Outros softwares são produzidos para oferecer proteção contra os ataques provenientes dos malwares. Com relação a esse tema, julgue os próximos itens.

[37] Firewalls são dispositivos de segurança que podem evitar a contaminação e a propagação de vírus. Por outro lado, antivírus são ferramentas de segurança capazes de detectar e evitar ataques provenientes de uma comunicação em rede.

[38] Os vírus, ao se propagarem, inserem cópias de seu próprio código em outros programas, enquanto os worms se propagam pelas redes, explorando, geralmente, alguma vulnerabilidade de outros softwares.

5. Malware é qualquer tipo de software que pode causar algum impacto negativo sobre a informação, podendo afetar sua disponibilidade, integridade e confidencialidade. Outros softwares são produzidos para oferecer proteção contra os ataques provenientes dos malwares. Com relação a esse tema, julgue os próximos itens.

 ~~[37] Firewalls são dispositivos de segurança que podem evitar a contaminação e a propagação de vírus. Por outro lado, antivírus são ferramentas de segurança capazes de detectar e evitar ataques provenientes de uma comunicação em rede.~~

 [38] Os vírus, ao se propagarem, inserem cópias de seu próprio código em outros programas, enquanto os worms se propagam pelas redes, explorando, geralmente, alguma vulnerabilidade de outros softwares.

6. Acerca da segurança da informação, julgue os itens subsequentes.

[57] Considere que uma mensagem de correio eletrônico, supostamente vinda do provedor de Internet, sob a alegação de que o computador que recebia a mensagem estava infectado por um vírus, sugeria que fosse instalada uma ferramenta de desinfecção. Considere ainda que na verdade, a ferramenta oferecida era um programa malicioso que, após a instalação, tornou os dados pessoais do usuário acessíveis ao remetente da mensagem. Nessa situação hipotética, é correto afirmar que houve um ataque de engenharia social.

6. Acerca da segurança da informação, julgue os itens subsequentes.

[57] Considere que uma mensagem de correio eletrônico, supostamente vinda do provedor de Internet, sob a alegação de que o computador que recebia a mensagem estava infectado por um vírus, sugeria que fosse instalada uma ferramenta de desinfecção. Considere ainda que na verdade, a ferramenta oferecida era um programa malicioso que, após a instalação, tornou os dados pessoais do usuário acessíveis ao remetente da mensagem. Nessa situação hipotética, é correto afirmar que houve um ataque de engenharia social.



7. A respeito da segurança de redes de computadores, julgue os itens

[87] Os ataques a computadores na Internet acontecem de diversas formas. Uma delas é a negação de serviço, na qual o computador atacado recebe diversas tentativas de acesso a determinado serviço até que usuário e senha sejam finalmente descobertos. Tal ataque é conhecido como DDoS (distributed denial of service).

7. A respeito da segurança de redes de computadores, julgue os itens

~~[87] Os ataques a computadores na Internet acontecem de diversas formas. Uma delas é a negação de serviço, na qual o computador atacado recebe diversas tentativas de acesso a determinado serviço até que usuário e senha sejam finalmente descobertos. Tal ataque é conhecido como DDoS (distributed denial of service).~~



8. Com relação a sistemas antivírus e malwares, em geral, julgue os próximos itens.

[71] Um mesmo vírus de computador é capaz de infectar várias máquinas. Uma estação de trabalho, normalmente, pode conter vários vírus diferentes e aptos a serem executados ao mesmo tempo.

[72] Uma característica dos vírus de computador do tipo worm é a sua incapacidade de se disseminar autonomamente: eles necessitam da intervenção de um usuário que os execute e, só assim, se propagam e infectam outros usuários.

8. Com relação a sistemas antivírus e malwares, em geral, julgue os próximos itens.

 [71] Um mesmo vírus de computador é capaz de infectar várias máquinas. Uma estação de trabalho, normalmente, pode conter vários vírus diferentes e aptos a serem executados ao mesmo tempo.

 ~~[72] Uma característica dos vírus de computador do tipo worm é a sua incapacidade de se disseminar autonomamente: eles necessitam da intervenção de um usuário que os execute e, só assim, se propagam e infectam outros usuários.~~

9. Julgue os itens subsequentes, acerca de antivírus.

[99] Os vírus do tipo mutante são capazes de modificar a estrutura de arquivos, para dificultar sua detecção por antivírus.

[100] Os vírus do tipo hoax são facilmente detectados pelas ferramentas de antivírus que utilizam técnicas de detecção por assinaturas, pois fazem uso de macros já conhecidas de vírus.

[101] As ferramentas de antivírus que realizam a verificação do tipo heurística detectam somente vírus já conhecidos, o que reduz a ocorrência de falsos positivos.

9. Julgue os itens subsequentes, acerca de antivírus.

[99] Os vírus do tipo mutante são capazes de modificar a estrutura de arquivos, para dificultar sua detecção por antivírus.



~~[100] Os vírus do tipo hoax são facilmente detectados pelas ferramentas de antivírus que utilizam técnicas de detecção por assinaturas, pois fazem uso de macros já conhecidas de vírus.~~



~~[101] As ferramentas de antivírus que realizam a verificação do tipo heurística detectam somente vírus já conhecidos, o que reduz a ocorrência de falsos positivos.~~



10. Quanto à segurança em rede de computadores, julgue os itens .

[76] Worm é um vírus que tem a capacidade de auto-replicação, espalhando-se rapidamente de uma rede para outra, mas somente causa danos se for ativado pelo usuário.

[77] Adware é qualquer programa que, depois de instalado, automaticamente executa, mostra ou baixa publicidade para o computador. Alguns desses programas têm instruções para captar informações pessoais e passá-la para terceiros, sem a autorização ou o conhecimento do usuário, o que caracteriza a prática conhecida como spyware.

[78] Backdoor consiste em uma falha de segurança que pode existir em um programa de computador ou sistema operacional. Essa falha permite que sejam instalados vírus de computador ou outros programas maliciosos, conhecidos como malware, utilizando-se exclusivamente de serviços executados em background.

[79] Keylogger é um programa de computador do tipo spyware cuja finalidade é monitorar tudo o que for digitado, a fim de descobrir senhas de banco, números de cartão de crédito e afins. Alguns casos de phishing e determinados tipos de fraudes virtuais baseiam-se no uso de keylogger.

10. Quanto à segurança em rede de computadores, julgue os itens .

 ~~[76] Worm é um vírus que tem a capacidade de auto-replicação, espalhando-se rapidamente de uma rede para outra, mas somente causa danos se for ativado pelo usuário.~~

 [77] Adware é qualquer programa que, depois de instalado, automaticamente executa, mostra ou baixa publicidade para o computador. Alguns desses programas têm instruções para captar informações pessoais e passá-la para terceiros, sem a autorização ou o conhecimento do usuário, o que caracteriza a prática conhecida como spyware.

 ~~[78] Backdoor consiste em uma falha de segurança que pode existir em um programa de computador ou sistema operacional. Essa falha permite que sejam instalados vírus de computador ou outros programas maliciosos, conhecidos como malware, utilizando-se exclusivamente de serviços executados em background.~~

 [79] Keylogger é um programa de computador do tipo spyware cuja finalidade é monitorar tudo o que for digitado, a fim de descobrir senhas de banco, números de cartão de crédito e afins. Alguns casos de phishing e determinados tipos de fraudes virtuais baseiam-se no uso de keylogger.

GABARITO



1. E, E, C, C, C

2. E

3. C, C, E

4. E, E, C

5. E, C

6. C

7. E

8. C, E

9. C, E, E

10. E, C, E, C

Oitava Bateria de Questões Com Resolução Assistida

Arquitetura e Organização de
Computadores

PROCESSADORES



1. Acerca dos conceitos de computadores e sistemas computacionais, julgue os próximos itens.

[53] A unidade de controle é o elemento da unidade central de processamento responsável por emitir os sinais de controle para ativar a realização de cada etapa do ciclo da instrução, sendo iguais esses sinais de controle para todas as instruções.

1. Acerca dos conceitos de computadores e sistemas computacionais, julgue os próximos itens.

 ~~[53] A unidade de controle é o elemento da unidade central de processamento responsável por emitir os sinais de controle para ativar a realização de cada etapa do ciclo da instrução, sendo iguais esses sinais de controle para todas as instruções.~~

2. Acerca das arquiteturas de hardware de servidores RISC, CISC e Mainframe, julgue os itens a seguir.

[98] Os mainframes IBM recentes possuem, em sua arquitetura de hardware, não apenas uma CPU (central processing unit), mas também um CPC (central processor complex), o qual pode conter diferentes tipos de processadores a serem utilizados para diferentes propósitos.

2. Acerca das arquiteturas de hardware de servidores RISC, CISC e Mainframe, julgue os itens a seguir.

[98] Os mainframes IBM recentes possuem, em sua arquitetura de hardware, não apenas uma CPU (central processing unit), mas também um CPC (central processor complex), o qual pode conter diferentes tipos de processadores a serem utilizados para diferentes propósitos.



3. Em relação aos processadores e à tecnologia SCSI, julgue os itens subsecutivos.

[66] O processador Intel i7, quarta geração, suporta criptografia totalmente por hardware, por meio de seis instruções das quais quatro suportam a cifragem e decifragem do Intel AES-IN.

[67] Os processadores AMD Athlon X2 possuem uma memória cache efetiva total com tamanho máximo de 1.280 Kb.

3. Em relação aos processadores e à tecnologia SCSI, julgue os itens subsecutivos.

 ~~[66] O processador Intel i7, quarta geração, suporta criptografia totalmente por hardware, por meio de seis instruções das quais quatro suportam a cifragem e decifragem do Intel AES-128.~~

 ~~[67] Os processadores AMD Athlon X2 possuem uma memória cache efetiva total com tamanho máximo de 1.280 Kb.~~

4. Acerca de arquiteturas de computadores, tipos de memória e barramentos, julgue os itens subsequentes.

[71] Em um sistema com múltiplos processadores, uma ou mais configurações de PCI (peripheral component interconnect) podem ser conectadas ao barramento do sistema por meio de pontes.

4. Acerca de arquiteturas de computadores, tipos de memória e barramentos, julgue os itens subsequentes.

 [71] Em um sistema com múltiplos processadores, uma ou mais configurações de PCI (peripheral component interconnect) podem ser conectadas ao barramento do sistema por meio de pontes.

5. Com relação aos principais componentes, à organização e aos sistemas operacionais dos microcomputadores, julgue os itens que se seguem.

[103] O barramento de endereço é unidirecional, ou seja, a informação flui da CPU para a memória ou dispositivos de entrada ou saída, mas jamais em sentido contrário.

[104] Em um microcomputador, a referência para a troca de informações é a CPU, desse modo, a operação de escrita ocorre quando a CPU recebe dados de um dispositivo de entrada.

5. Com relação aos principais componentes, à organização e aos sistemas operacionais dos microcomputadores, julgue os itens que se seguem.

 [103] O barramento de endereço é unidirecional, ou seja, a informação flui da CPU para a memória ou dispositivos de entrada ou saída, mas jamais em sentido contrário.

 ~~[104] Em um microcomputador, a referência para a troca de informações é a CPU, desse modo, a operação de escrita ocorre quando a CPU recebe dados de um dispositivo de entrada.~~

6. Julgue o próximo item, relativo a sistemas concorrentes.

[57] Na computação paralela, todos os processadores estão presentes no mesmo circuito integrado, enquanto, na computação distribuída, cada processador encontra-se geograficamente separado por longas distâncias.

6. Julgue o próximo item, relativo a sistemas concorrentes.

~~[57] Na computação paralela, todos os processadores estão presentes no mesmo circuito integrado, enquanto, na computação distribuída, cada processador encontra-se geograficamente separado por longas distâncias.~~



7. Julgue os itens subsecutivos, acerca de noções básicas de arquitetura de computadores.

[52] Entre as responsabilidades do caminho de dados do processador, pode-se destacar a realização de operações aritméticas.

[53] Um barramento é um enlace de comunicação utilizado para conectar o processador exclusivamente a um periférico.

[54] A unidade de controle do processador é responsável por comandar o caminho de dados, a memória e os periféricos, de acordo com as instruções de um programa.

7. Julgue os itens subsecutivos, acerca de noções básicas de arquitetura de computadores.

[52] Entre as responsabilidades do caminho de dados do processador, pode-se destacar a realização de operações aritméticas.

~~[53] Um barramento é um enlace de comunicação utilizado para conectar o processador exclusivamente a um periférico.~~

[54] A unidade de controle do processador é responsável por comandar o caminho de dados, a memória e os periféricos, de acordo com as instruções de um programa.

8. Acerca da arquitetura de processadores, julgue os itens abaixo.

[60] A dificuldade crescente em resfriar os processadores comerciais é um dos principais fatores que levaram a indústria a uma mudança de paradigma, que deu origem aos processadores de múltiplos núcleos para computadores pessoais.

8. Acerca da arquitetura de processadores, julgue os itens abaixo.

[60] A dificuldade crescente em resfriar os processadores comerciais é um dos principais fatores que levaram a indústria a uma mudança de paradigma, que deu origem aos processadores de múltiplos núcleos para computadores pessoais.



9. Acerca da organização e arquitetura de computadores e dos componentes de um computador, julgue os itens a seguir.

[51] A diminuição do tamanho dos chips resulta em ganho de desempenho em hardware, uma vez que leva ao aumento da relação entre resistência e capacitância, pois as interconexões de fio se tornam mais finas, aumentando a resistência, e os fios estão mais próximos, aumentando a capacitância.

[52] Arquitetura de computador refere-se aos atributos de um sistema visíveis a um programador, ou seja, atributos que possuem impacto direto sobre a execução lógica de um programa. Nesse contexto, é considerada uma questão arquitetural, por exemplo, se uma instrução de multiplicação será realizada por uma unidade de multiplicação especial ou por um mecanismo que faça uso repetido da unidade de adição do sistema.

9. Acerca da organização e arquitetura de computadores e dos componentes de um computador, julgue os itens a seguir.

 [51] A diminuição do tamanho dos chips resulta em ganho de desempenho em hardware, uma vez que leva ao aumento da relação entre resistência e capacitância, pois as interconexões de fio se tornam mais finas, aumentando a resistência, e os fios estão mais próximos, aumentando a capacitância.

 ~~[52] Arquitetura de computador refere-se aos atributos de um sistema visíveis a um programador, ou seja, atributos que possuem impacto direto sobre a execução lógica de um programa. Nesse contexto, é considerada uma questão arquitetural, por exemplo, se uma instrução de multiplicação será realizada por uma unidade de multiplicação especial ou por um mecanismo que faça uso repetido da unidade de adição do sistema.~~

10. A respeito das arquiteturas de hardware existentes em servidores, julgue os itens que se seguem

[86] Mainframes são computadores de grande porte projetados para lidar com grande vazão de dados e para serem altamente confiáveis e seguros.

[87] Um mainframe possui múltiplas unidades de processamento, sendo cada unidade um processador comum, tipicamente Intel ou AMD.

10. A respeito das arquiteturas de hardware existentes em servidores, julgue os itens que se seguem

 [86] Mainframes são computadores de grande porte projetados para lidar com grande vazão de dados e para serem altamente confiáveis e seguros.

 ~~[87] Um mainframe possui múltiplas unidades de processamento, sendo cada unidade um processador comum, tipicamente Intel ou AMD.~~

GABARITO



1. E

2. C

3. E, E

4. C

5. C, E

6. E

7. C, E, C

8. C

9. C, E

10. C, E

Oitava Bateria de Questões Com Resolução Assistida

Malware: **Vírus de computador,
cavalo de tróia, adware, spyware,
backdoors, keylogger, worms**

1. No que concerne à segurança, julgue os itens subsequentes.

[69] Os firewalls que mantêm o estado das conexões atuam na camada de rede, mas podem tomar decisões com base em informações das camadas de transporte e aplicação. Por esse motivo, conseguem perceber mais facilmente as tentativas de DOS (denial of service) nos servidores protegidos por esse firewall.

1. No que concerne à segurança, julgue os itens subsequentes.

[69] Os firewalls que mantêm o estado das conexões atuam na camada de rede, mas podem tomar decisões com base em informações das camadas de transporte e aplicação. Por esse motivo, conseguem perceber mais facilmente as tentativas de DOS (denial of service) nos servidores protegidos por esse firewall.



2. A respeito de segurança de redes de comunicação, julgue os itens que se seguem.

[119] DDOS (distributed denial of service) é um tipo de ataque que tem a finalidade de inviabilizar o funcionamento de um computador. Para isso, a partir de vários computadores, é enviada grande quantidade de requisições a determinado serviço, a fim de consumir os recursos do computador alvo do ataque.

2. A respeito de segurança de redes de comunicação, julgue os itens que se seguem.

[119] DDOS (distributed denial of service) é um tipo de ataque que tem a finalidade de inviabilizar o funcionamento de um computador. Para isso, a partir de vários computadores, é enviada grande quantidade de requisições a determinado serviço, a fim de consumir os recursos do computador alvo do ataque.



3. Considerando-se que ataques do tipo DOS (denial of service), conhecidos como ataques de negação de serviço, são capazes de indisponibilizar um serviço de rede, enviando um número de solicitações muito além do normal, uma das ações que permitem diminuir o impacto imediato desse tipo de ataque é a de
- A. restringir a quantidade de conexões simultâneas aceitas no servidor para a manutenção do serviço disponível.
 - B. utilizar o protocolo HTTPS.
 - C. impedir acessos remotos para administração do servidor.
 - D. instalar um sniffer de rede, configurando-o para monitorar o tráfego.
 - E. monitorar o consumo de banda da rede

3. Considerando-se que ataques do tipo DOS (denial of service), conhecidos como ataques de negação de serviço, são capazes de indisponibilizar um serviço de rede, enviando um número de solicitações muito além do normal, uma das ações que permitem diminuir o impacto imediato desse tipo de ataque é a de

A. restringir a quantidade de conexões simultâneas aceitas no servidor para a manutenção do serviço disponível.



~~B. utilizar o protocolo HTTPS.~~

~~C. impedir acessos remotos para administração do servidor.~~

~~D. instalar um sniffer de rede, configurando-o para monitorar o tráfego.~~

~~E. monitorar o consumo de banda da rede~~

4. Quanto aos ataques a redes de computadores, seus tipos e malwares empregados, julgue os itens a seguir.

[100] Ataques de phishing são potencialmente mais comprometedores da disponibilidade que ataques de DDoS (distributed denial of service) provocados por worms.

4. Quanto aos ataques a redes de computadores, seus tipos e malwares empregados, julgue os itens a seguir.

~~[100] Ataques de phishing são potencialmente mais comprometedores da disponibilidade que ataques de DDoS (distributed denial of service) provocados por worms.~~

5. Quanto à segurança em rede de computadores, julgue os itens .

[71] Uma rede interna pode ser protegida contra o IP spoofing por meio da aplicação de filtros; como exemplo, se a rede tem endereços do tipo 100.200.200.0, então o firewall deve bloquear tentativas de conexão originadas externamente, caso a origem tenha endereços de rede do tipo 100.200.200.0.

[72] Em um ataque do tipo DoS (denial of service attack), os pacotes de resposta trazem informações do usuário para o hacker/cracker.

[73] O DDoS (distributed denial of service) é um tipo de ataque coordenado, no qual diversos hosts são atacados e coordenados pelo hacker, para a realização de ataques simultâneos aos alvos.

[74] O SYN flooding é um tipo de ataque que explora o mecanismo de conexões IP, gerando um grande número de requisições em um servidor web.

[75] Cavalo de tróia é um software legítimo que o usuário utiliza normalmente, mas, ao mesmo tempo, executa outras funções ilegais, como enviar mensagens e arquivos para o hacker ou abrir portas de entrada para futuras invasões.

5. Quanto à segurança em rede de computadores, julgue os itens .

 [71] Uma rede interna pode ser protegida contra o IP spoofing por meio da aplicação de filtros; como exemplo, se a rede tem endereços do tipo 100.200.200.0, então o firewall deve bloquear tentativas de conexão originadas externamente, caso a origem tenha endereços de rede do tipo 100.200.200.0.

 ~~[72] Em um ataque do tipo DoS (denial of service attack), os pacotes de resposta trazem informações do usuário para o hacker/cracker.~~

 [73] O DDoS (distributed denial of service) é um tipo de ataque coordenado, no qual diversos hosts são atacados e coordenados pelo hacker, para a realização de ataques simultâneos aos alvos.

 ~~[74] O SYN flooding é um tipo de ataque que explora o mecanismo de conexões IP, gerando um grande número de requisições em um servidor web.~~

 [75] Cavalo de tróia é um software legítimo que o usuário utiliza normalmente, mas, ao mesmo tempo, executa outras funções ilegais, como enviar mensagens e arquivos para o hacker ou abrir portas de entrada para futuras invasões.

6. órgão público, visando identificar o atual nível de proteção da rede de computadores das organizações públicas para as quais presta serviços, desenvolveu um conjunto de processos de avaliação de segurança da informação em redes de computadores. Empregando métodos analíticos e práticos, os auditores coletaram várias informações acerca da rede e produziram diversas declarações, sendo algumas delas consistentes com o estado da prática e outras incorretas. A esse respeito, julgue os itens.

[101] O uso de firewalls na rede de computadores é mais eficaz na prevenção de incidentes que para o tratamento dos eventuais incidentes que nela ocorrem. Os firewalls stateless, ou de filtragem de pacotes, são especialmente eficazes no bloqueio a vários tipos de ataques, como phishing e spoofing.

[102] Considere que, utilizando um sniffer junto ao segmento que liga a rede de uma organização à Internet, um dos auditores identifique, durante poucos segundos, a ocorrência de milhares de pacotes SYN e SYN/ACK trafegando na rede, para os quais não havia correspondentes pacotes ACK. Considere ainda que o auditor constate que os endereços fonte dos pacotes SYN e os endereços destino dos pacotes SYN/ACK eram de um host desconhecido pela organização, enquanto os endereços destino dos pacotes SYN e os endereços fonte dos pacotes SYN/ACK eram de um host pertencente à rede DMZ da organização. Nesse caso, a partir dos dados coletados, é correto inferir que a organização poderia estar, naquele momento, sofrendo um ataque de negação de serviço DOS (denial of service).

6. órgão público, visando identificar o atual nível de proteção da rede de computadores das organizações públicas para as quais presta serviços, desenvolveu um conjunto de processos de avaliação de segurança da informação em redes de computadores. Empregando métodos analíticos e práticos, os auditores coletaram várias informações acerca da rede e produziram diversas declarações, sendo algumas delas consistentes com o estado da prática e outras incorretas. A esse respeito, julgue os itens.

 ~~[101] O uso de firewalls na rede de computadores é mais eficaz na prevenção de incidentes que para o tratamento dos eventuais incidentes que nela ocorrem. Os firewalls stateless, ou de filtragem de pacotes, são especialmente eficazes no bloqueio a vários tipos de ataques, como phishing e spoofing.~~

 [102] Considere que, utilizando um sniffer junto ao segmento que liga a rede de uma organização à Internet, um dos auditores identifique, durante poucos segundos, a ocorrência de milhares de pacotes SYN e SYN/ACK trafegando na rede, para os quais não havia correspondentes pacotes ACK. Considere ainda que o auditor constate que os endereços fonte dos pacotes SYN e os endereços destino dos pacotes SYN/ACK eram de um host desconhecido pela organização, enquanto os endereços destino dos pacotes SYN e os endereços fonte dos pacotes SYN/ACK eram de um host pertencente à rede DMZ da organização. Nesse caso, a partir dos dados coletados, é correto inferir que a organização poderia estar, naquele momento, sofrendo um ataque de negação de serviço DOS (denial of service).

7. As vulnerabilidades de segurança da família de protocolos TCP/IP têm sido ativamente exploradas nos últimos anos, visando à realização de ataques a sistemas computacionais interconectados à Internet. Em contrapartida a esses ataques, vários mecanismos e sistemas de proteção, defesa e contra-ataque têm sido criados, como firewalls, IPSs (intrusion prevention systems) e IDSs (intrusion detection systems). Com relação a vulnerabilidades e ataques às redes de computadores, julgue os itens seguintes.

- I Entre os métodos de ataque relacionados a DoS (denial of service), está o ataque de smurf, concentrado na camada IP, embasado no protocolo ICMP, no spoof de endereços fonte em pacotes e com amplificação por meio de repasse de pacotes dirigidos a endereço de broadcast.
- II O ataque ping da morte (ping of death), ainda comum nos sistemas Windows sem a proteção de firewalls, gera DoS devido à fragmentação entre as camadas de rede e de enlace, bem como devido à geração de buffer overflow.
- III A tentativa de ataque embasada no spoof de endereços IP do tipo non-blind spoofing tem maior sucesso quando o alvo atacado estiver na mesma sub-rede do atacante.
- IV Quando um spoofing IP tem por objetivo principal a negação de serviço e, não, a captura de sessão, há menor necessidade de um atacante manipular os números de sequência e acknowledgement presentes no cabeçalho de pacotes TCP.
- V Ataques do tipo SYN flooding em geral são bem sucedidos quando esgotam a capacidade de recebimento de datagramas UDP por parte dos hosts alvos.

Estão certos apenas os itens

- A. I, II e III.
- B. I, II e V.
- C. I, III e IV.
- D. II, IV e V.
- E. III, IV e V.

7. As vulnerabilidades de segurança da família de protocolos TCP/IP têm sido ativamente exploradas nos últimos anos, visando à realização de ataques a sistemas computacionais interconectados à Internet. Em contrapartida a esses ataques, vários mecanismos e sistemas de proteção, defesa e contra-ataque têm sido criados, como firewalls, IPSs (intrusion prevention systems) e IDSs (intrusion detection systems). Com relação a vulnerabilidades e ataques às redes de computadores, julgue os itens seguintes.

- I Entre os métodos de ataque relacionados a DoS (denial of service), está o ataque de smurf, concentrado na camada IP, embasado no protocolo ICMP, no spoof de endereços fonte em pacotes e com amplificação por meio de repasse de pacotes dirigidos a endereço de broadcast.
- II O ataque ping da morte (ping of death), ainda comum nos sistemas Windows sem a proteção de firewalls, gera DoS devido à fragmentação entre as camadas de rede e de enlace, bem como devido à geração de buffer overflow.
- III A tentativa de ataque embasada no spoof de endereços IP do tipo non-blind spoofing tem maior sucesso quando o alvo atacado estiver na mesma sub-rede do atacante.
- IV Quando um spoofing IP tem por objetivo principal a negação de serviço e, não, a captura de sessão, há menor necessidade de um atacante manipular os números de sequência e acknowledgement presentes no cabeçalho de pacotes TCP.
- V Ataques do tipo SYN flooding em geral são bem sucedidos quando esgotam a capacidade de recebimento de datagramas UDP por parte dos hosts alvos.

Estão certos apenas os itens

~~A. I, II e III.~~

~~B. I, II e V.~~

C. I, III e IV.

~~D. II, IV e V.~~

~~E. III, IV e V.~~



8. A respeito de ataques a redes de computadores e de incidentes de segurança, julgue os itens.

- [81] O incidente denominado DDoS deve ser tratado de maneira diferente de outros tipos de incidente de segurança, pois dificilmente um firewall ou IDS gerará log. Sua notificação de incidente deve informar o cabeçalho e o conteúdo completos da mensagem recebida pelo usuário.
- [82] Um ataque de negação de serviço (DoS) não é uma invasão do sistema e objetiva tornar os recursos de um sistema indisponíveis para seus utilizadores. O ataque tenta indisponibilizar páginas hospedadas em servidores web e produz como efeito uma invalidação por sobrecarga.
- [83] No phishing, diversas máquinas zumbis comandadas por um mestre fazem requisições ao mesmo tempo, gerando sobrecarga do recurso atacado, o que pode levar a máquina servidora a reiniciar ou a travar.
- [84] No ping flood, o atacante sobrecarrega o sistema vítima com pacotes ICMP echo request (pacotes ping). Para o ataque ser bem sucedido, o atacante deve possuir maior largura de banda que a vítima, que, ao tentar responder aos pedidos, irá consumir a sua própria largura de banda, impossibilitando-a de responder a pedidos de outros utilizadores. Uma das formas de prevenir esse tipo de ataque é limitar o tráfego de pacotes ICMP echo request.
- [85] No syn flood ou ataque syn, o atacante envia uma sequência de requisições syn para um sistema-alvo visando uma sobrecarga direta na camada de transporte e indireta na camada de aplicação do modelo OSI.

8. A respeito de ataques a redes de computadores e de incidentes de segurança, julgue os itens.

~~[81] O incidente denominado DDoS deve ser tratado de maneira diferente de outros tipos de incidente de segurança, pois dificilmente um firewall ou IDS gerará log. Sua notificação de incidente deve informar o cabeçalho e o conteúdo completos da mensagem recebida pelo usuário.~~

[82] Um ataque de negação de serviço (DoS) não é uma invasão do sistema e objetiva tornar os recursos de um sistema indisponíveis para seus utilizadores. O ataque tenta indisponibilizar páginas hospedadas em servidores web e produz como efeito uma invalidação por sobrecarga.

~~[83] No phishing, diversas máquinas zumbis comandadas por um mestre fazem requisições ao mesmo tempo, gerando sobrecarga do recurso atacado, o que pode levar a máquina servidora a reiniciar ou a travar.~~

[84] No ping flood, o atacante sobrecarrega o sistema vítima com pacotes ICMP echo request (pacotes ping). Para o ataque ser bem sucedido, o atacante deve possuir maior largura de banda que a vítima, que, ao tentar responder aos pedidos, irá consumir a sua própria largura de banda, impossibilitando-a de responder a pedidos de outros utilizadores. Uma das formas de prevenir esse tipo de ataque é limitar o tráfego de pacotes ICMP echo request.

[85] No syn flood ou ataque syn, o atacante envia uma sequência de requisições syn para um sistema-alvo visando uma sobrecarga direta na camada de transporte e indireta na camada de aplicação do modelo OSI.

9. Com relação a malwares, julgue os próximos itens.

- [86] Um adware difere de um spyware pela intenção. O primeiro é projetado para monitorar atividades de um sistema e enviar informações coletadas para terceiros, e o segundo é projetado especificamente para apresentar propagandas.
- [87] O cavalo de tróia (trojan horse) não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser executado para se propagar. Sua propagação se dá por meio da exploração de vulnerabilidades existentes ou de falhas na configuração de software instalados em computadores.
- [88] Ao se executar um programa previamente infectado - como, por exemplo, ao se abrir arquivo anexado a e-mail ou ao se instalar programas de procedência duvidosa ou desconhecida -, um vírus pode infectar o computador. Um vírus de macro é parte de um arquivo normalmente manipulado por algum aplicativo que utiliza macros e que, para ser executado, necessita que o arquivo que o contém esteja aberto para que ele execute uma série de comandos automaticamente e infecte outros arquivos no computador.
- [89] Um worm pode realizar diversas funções maliciosas, como a instalação de keyloggers ou screenloggers, o furto de senhas e outras informações sensíveis, como números de cartões de crédito, a inclusão de backdoors, para permitir que um atacante tenha total controle sobre o computador, e a alteração ou destruição de arquivos.
- [90] O worm costuma ser apenas um único arquivo que necessita ser executado para que infecte o computador destinatário e, de modo distinto do vírus ou do cavalo de tróia, não costuma infectar outros arquivos e nem propagar, automaticamente, cópias de si mesmo.

9. Com relação a malwares, julgue os próximos itens.

 ~~[86] Um adware difere de um spyware pela intenção. O primeiro é projetado para monitorar atividades de um sistema e enviar informações coletadas para terceiros, e o segundo é projetado especificamente para apresentar propagandas.~~

 ~~[87] O cavalo de tróia (trojan horse) não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser executado para se propagar. Sua propagação se dá por meio da exploração de vulnerabilidades existentes ou de falhas na configuração de software instalados em computadores.~~

 [88] Ao se executar um programa previamente infectado - como, por exemplo, ao se abrir arquivo anexado a e-mail ou ao se instalar programas de procedência duvidosa ou desconhecida -, um vírus pode infectar o computador. Um vírus de macro é parte de um arquivo normalmente manipulado por algum aplicativo que utiliza macros e que, para ser executado, necessita que o arquivo que o contém esteja aberto para que ele execute uma série de comandos automaticamente e infecte outros arquivos no computador.

 ~~[89] Um worm pode realizar diversas funções maliciosas, como a instalação de keyloggers ou screenloggers, o furto de senhas e outras informações sensíveis, como números de cartões de crédito, a inclusão de backdoors, para permitir que um atacante tenha total controle sobre o computador, e a alteração ou destruição de arquivos.~~

 ~~[90] O worm costuma ser apenas um único arquivo que necessita ser executado para que infecte o computador destinatário e, de modo distinto do vírus ou do cavalo de tróia, não costuma infectar outros arquivos e nem propagar, automaticamente, cópias de si mesmo.~~

10. Julgue os próximos itens no que se refere a ataques a redes de computadores e malwares.

[67] DoS e DDoS são ataques que têm por finalidade a indisponibilização dos serviços das redes. Um IDS, corretamente instalado e configurado, é capaz de proteger totalmente a rede de ataques do tipo DoS, mas não protege a rede de ataques do tipo DDoS.

[68] Cavalo de tróia é um malware que instala-se em uma máquina, sem que seu usuário perceba, para extrair ou destruir dados sem autorização. Esse tipo de programa é executado automaticamente e em background sempre que a máquina é inicializada.

10. Julgue os próximos itens no que se refere a ataques a redes de computadores e malwares.

 ~~[67] DoS e DDoS são ataques que têm por finalidade a indisponibilização dos serviços das redes. Um IDS, corretamente instalado e configurado, é capaz de proteger totalmente a rede de ataques do tipo DoS, mas não protege a rede de ataques do tipo DDoS.~~

 ~~[68] Cavalo de tróia é um malware que instala-se em uma máquina, sem que seu usuário perceba, para extrair ou destruir dados sem autorização. Esse tipo de programa é executado automaticamente e em background sempre que a máquina é inicializada.~~

GABARITO



1. C

2. C

3. A

4. E

5. C, E, C, E, C

6. E, C

7. C

8. E, C, E, C, C

9. E, E, C, E, E

10. E, E

Nona Bateria de Questões Com Resolução Assistida

Arquitetura e Organização de
Computadores
BARRAMENTOS



1. Em relação aos processadores e à tecnologia SCSI, julgue os itens subsecutivos.

[68] Na tecnologia SCSI, a transmissão de sinais no modo LVD (low-voltage differential) restringe-se a cabos com até 12 m de comprimento.

1. Em relação aos processadores e à tecnologia SCSI, julgue os itens subsecutivos.

[68] Na tecnologia SCSI, a transmissão de sinais no modo LVD (low-voltage differential) restringe-se a cabos com até 12 m de comprimento.



2. Julgue os itens que se seguem, relativos a conceitos de computação

[53] USB é um tipo de porta serial de comunicação que utiliza o conceito de plug and play.

[54] A comunicação entre os dispositivos de processamento e os demais periféricos instalados em um computador é feita pela placa-mãe.

2. Julgue os itens que se seguem, relativos a conceitos de computação

 [53] USB é um tipo de porta serial de comunicação que utiliza o conceito de plug and play.

 [54] A comunicação entre os dispositivos de processamento e os demais periféricos instalados em um computador é feita pela placa-mãe.

3. Considerando o padrão USB 3.0 utilizado em componentes periféricos de microcomputadores, julgue os itens subsecutivos.

[91] O gerenciamento de energia em dispositivos USB 3.0 é mais eficiente que em dispositivos USB 2.0 ou anterior. Ainda prevê que tanto o computador quanto o dispositivo iniciem a economia de energia quando estão operando em modo inativo.

[93] O padrão USB 3.0 suporta transferências em modo full-duplex..

3. Considerando o padrão USB 3.0 utilizado em componentes periféricos de microcomputadores, julgue os itens subsecutivos.

 [91] O gerenciamento de energia em dispositivos USB 3.0 é mais eficiente que em dispositivos USB 2.0 ou anterior. Ainda prevê que tanto o computador quanto o dispositivo iniciem a economia de energia quando estão operando em modo inativo.

 [93] O padrão USB 3.0 suporta transferências em modo full-duplex..



4. Considerando a figura acima, que ilustra um esquema básico de um computador, julgue os itens a seguir.

[51] O processador executa os programas, faz os cálculos e toma as decisões, de acordo com as instruções armazenadas na memória.

[52] O barramento é uma via de comunicação de baixa velocidade por onde circulam os dados tratados pelo computador.

[53] A memória é o dispositivo responsável pelas entradas e saídas de dados do computador.



4. Considerando a figura acima, que ilustra um esquema básico de um computador, julgue os itens a seguir.

[51] O processador executa os programas, faz os cálculos e toma as decisões, de acordo com as instruções armazenadas na memória.



~~[52] O barramento é uma via de comunicação de baixa velocidade por onde circulam os dados tratados pelo computador.~~



~~[53] A memória é o dispositivo responsável pelas entradas e saídas de dados do computador.~~



5. Julgue os itens subsecutivos, acerca de noções básicas de arquitetura de computadores.

[51] Periféricos são dispositivos responsáveis pelas funções de entrada e saída do computador, como, por exemplo, o monitor e o teclado.

[53] Um barramento é um enlace de comunicação utilizado para conectar o processador exclusivamente a um periférico.

5. Julgue os itens subsecutivos, acerca de noções básicas de arquitetura de computadores.

 [51] Periféricos são dispositivos responsáveis pelas funções de entrada e saída do computador, como, por exemplo, o monitor e o teclado.

 ~~[53] Um barramento é um enlace de comunicação utilizado para conectar o processador exclusivamente a um periférico.~~

6. Julgue os itens a seguir, relativos a barramentos de computadores.

[56] Uma desvantagem em se utilizar um barramento está na criação de um gargalo de comunicação, o qual pode limitar a vazão máxima de entrada/saída do sistema.

[57] A utilização de um barramento apresenta duas principais vantagens, que são a versatilidade e o baixo custo. Dado que novos dispositivos podem facilmente ser adicionados ao sistema ou utilizados em diferentes sistemas.

6. Julgue os itens a seguir, relativos a barramentos de computadores.

 [56] Uma desvantagem em se utilizar um barramento está na criação de um gargalo de comunicação, o qual pode limitar a vazão máxima de entrada/saída do sistema.

 [57] A utilização de um barramento apresenta duas principais vantagens, que são a versatilidade e o baixo custo. Dado que novos dispositivos podem facilmente ser adicionados ao sistema ou utilizados em diferentes sistemas.

7. Com relação aos processadores utilizados em computadores, julgue os itens a seguir

[51] Entre outras funções, o barramento - com seus canais de comunicação - interliga os vários componentes de um sistema de computação.

7. Com relação aos processadores utilizados em computadores, julgue os itens a seguir

[51] Entre outras funções, o barramento - com seus canais de comunicação - interliga os vários componentes de um sistema de computação.



8. Com relação aos barramentos de entrada e saída, julgue os itens seguintes

[57] Entre outras, o PCI Express oferece as seguintes vantagens sobre PCI: usa tecnologia serial provendo performance escalável; alta banda passante; link ponto a ponto para cada dispositivo em vez de um barramento compartilhado.

[58] O barramento AGP impede, para a execução de operações complexas, o acesso à memória principal diretamente.

[59] O padrão USB 2.0 atinge velocidades mais altas que as versões anteriores, porém preserva o modelo host-dispositivo, o protocolo de comunicação e a interface de software.

8. Com relação aos barramentos de entrada e saída, julgue os itens seguintes

 [57] Entre outras, o PCI Express oferece as seguintes vantagens sobre PCI: usa tecnologia serial provendo performance escalável; alta banda passante; link ponto a ponto para cada dispositivo em vez de um barramento compartilhado.

 [58] O barramento AGP impede, para a execução de operações complexas, o acesso à memória principal diretamente.

 [59] O padrão USB 2.0 atinge velocidades mais altas que as versões anteriores, porém preserva o modelo host-dispositivo, o protocolo de comunicação e a interface de software.

9. A respeito de componentes de um computador, sistemas de entrada, saída e armazenamento, julgue os itens subsequentes.

[53] A velocidade de transferência de dados de um dispositivo externo, como um drive de CD-ROM, é menor que a velocidade de uma CPU; por esse motivo, utiliza-se um barramento de sistema para a conexão de periféricos com a CPU.

[55] Para executar tarefas que demandem grande quantidade de acessos ao disco rígido para leitura e gravação de dados, o uso de um computador com disco rígido padrão IDE é melhor que o de um computador com padrão SCSI.

9. A respeito de componentes de um computador, sistemas de entrada, saída e armazenamento, julgue os itens subsequentes.

 [53] A velocidade de transferência de dados de um dispositivo externo, como um drive de CD-ROM, é menor que a velocidade de uma CPU; por esse motivo, utiliza-se um barramento de sistema para a conexão de periféricos com a CPU.

 ~~[55] Para executar tarefas que demandem grande quantidade de acessos ao disco rígido para leitura e gravação de dados, o uso de um computador com disco rígido padrão IDE é melhor que o de um computador com padrão SCSI.~~

10. Julgue os itens a seguir, referentes a sistemas de entrada, saída e armazenamento em computadores

[80] As funções mais importantes de um módulo de E/S podem ser divididas nas seguintes categorias: controle e temporização, comunicação com o processador, comunicação com dispositivos, área de armazenamento temporário de dados e detecção de erros.

[81] As principais técnicas de entrada/saída (E/S) utilizadas em computadores são: E/S programada, E/S dirigida por interrupção e acesso direto à memória. A última é efetuada sob controle direto e contínuo do programa que requisitou a operação de E/S.

10. Julgue os itens a seguir, referentes a sistemas de entrada, saída e armazenamento em computadores

 [80] As funções mais importantes de um módulo de E/S podem ser divididas nas seguintes categorias: controle e temporização, comunicação com o processador, comunicação com dispositivos, área de armazenamento temporário de dados e detecção de erros.

 ~~[81] As principais técnicas de entrada/saída (E/S) utilizadas em computadores são: E/S programada, E/S dirigida por interrupção e acesso direto à memória. A última é efetuada sob controle direto e contínuo do programa que requisitou a operação de E/S.~~

GABARITO



1. C

2. C, C

3. C, C

4. C, E, E

5. C, E

6. C, C

7. C

8. C, E, C

9. C, E

10. C, E

Nona Bateria de Questões Com Resolução Assistida

Dispositivos de segurança: **NAT, VPN**

1. Acerca da rede privada virtual (VPN) e de suas formas de uso, julgue os itens subsequentes.

[113] Em VPN com uso de IPSEC, são suportados basicamente dois modos de operação: o modo transporte, que é utilizado para ligação de túneis virtuais; e o modo túnel, para estabelecer comunicação entre dois hosts, apenas.

[114] Geralmente, VPN site-to-site permite que recursos de uma localidade sejam disponibilizados para usuários em outra localidade remota por meio de um canal de comunicação seguro mediante o uso da Internet.

[115] Em soluções modernas de VPN user-to-site, o processo de autenticação de um usuário remoto pode ser feito pelo servidor VPN ou este servidor pode delegar essa função a um servidor de autenticação. Nesse segundo caso, soluções de autenticação por certificação digital não são suportadas.

1. Acerca da rede privada virtual (VPN) e de suas formas de uso, julgue os itens subsequentes.

 ~~[113] Em VPN com uso de IPSEC, são suportados basicamente dois modos de operação: o modo transporte, que é utilizado para ligação de túneis virtuais; e o modo túnel, para estabelecer comunicação entre dois hosts, apenas.~~

 [114] Geralmente, VPN site-to-site permite que recursos de uma localidade sejam disponibilizados para usuários em outra localidade remota por meio de um canal de comunicação seguro mediante o uso da Internet.

 ~~[115] Em soluções modernas de VPN user-to-site, o processo de autenticação de um usuário remoto pode ser feito pelo servidor VPN ou este servidor pode delegar essa função a um servidor de autenticação. Nesse segundo caso, soluções de autenticação por certificação digital não são suportadas.~~

2. Acerca do NAT (network address translation) em um gateway com a função de conectar a rede interna de uma organização à Internet, julgue os itens seguintes

[85] Se o gateway for configurado no modo bridge (ponte), uma estação de trabalho que utilize o IP privado 192.168.0.100, com máscara de rede 255.255.255.0, poderá acessar a Internet sem a intervenção do recurso NAT, isto é, sem que ocorra a tradução de endereço no gateway.

[86] O endereço e a porta de origem inscritos nos pacotes que, provenientes da Internet, passam pelo gateway com destino a uma estação de trabalho na rede interna podem ser alterados pela variante do NAT conhecida como NAPT (network address and port translation).

[87] O gateway encarregado de fazer o NAT para o tráfego originado na rede interna e destinado à Internet armazena, em uma tabela NAT, as informações acerca das conexões correntes. Caso uma pane ocasione perda dos dados dessa tabela, as conexões TCP não serão destruídas, pois esse protocolo tem recursos para preservar as conexões nessa situação.

[88] Por padrão o NAT funciona adequadamente com os protocolos TCP e UDP. Caso seja criado um protocolo de transporte diferente para acesso a uma aplicação, que necessite atravessar o gateway para ser acessada, cujo tráfego sofra o processo de NAT, o acesso a essa aplicação falhará.

[89] As estações de trabalho da rede interna podem acessar a Internet utilizando endereços IPs privados. Para isso, é necessário que as estações de trabalho tenham, em suas configurações de rede, o endereço do equipamento de gateway e este deve ter a capacidade de trocar nos pacotes encaminhados à Internet o endereço privado por um endereço público.

2. Acerca do NAT (network address translation) em um gateway com a função de conectar a rede interna de uma organização à Internet, julgue os itens seguintes

 ~~[85] Se o gateway for configurado no modo bridge (ponte), uma estação de trabalho que utilize o IP privado 192.168.0.100, com máscara de rede 255.255.255.0, poderá acessar a Internet sem a intervenção do recurso NAT, isto é, sem que ocorra a tradução de endereço no gateway.~~

 [86] O endereço e a porta de origem inscritos nos pacotes que, provenientes da Internet, passam pelo gateway com destino a uma estação de trabalho na rede interna podem ser alterados pela variante do NAT conhecida como NAPT (network address and port translation).

 ~~[87] O gateway encarregado de fazer o NAT para o tráfego originado na rede interna e destinado à Internet armazena, em uma tabela NAT, as informações acerca das conexões correntes. Caso uma pane ocasione perda dos dados dessa tabela, as conexões TCP não serão destruídas, pois esse protocolo tem recursos para preservar as conexões nessa situação.~~

 ~~[88] Por padrão o NAT funciona adequadamente com os protocolos TCP e UDP. Caso seja criado um protocolo de transporte diferente para acesso a uma aplicação, que necessite atravessar o gateway para ser acessada, cujo tráfego sofra o processo de NAT, o acesso a essa aplicação falhará.~~

 [89] As estações de trabalho da rede interna podem acessar a Internet utilizando endereços IPs privados. Para isso, é necessário que as estações de trabalho tenham, em suas configurações de rede, o endereço do equipamento de gateway e este deve ter a capacidade de trocar nos pacotes encaminhados à Internet o endereço privado por um endereço público.

3. Assinale a opção correta acerca de NAT (network address translation).

- A. Apesar de não fornecer recursos de conexão de tráfego, como rastreamento de usuário, sítios ou conexões, a NAT permite que administradores de redes proíbam acesso a determinados sítios.
- B. O mecanismo de NAT é utilizado exclusivamente por roteadores que operam na camada 3 ou acima.
- C. Na NAT do tipo dinâmica sobrecarregada vários endereços IP não registrados são mapeados para um único endereço IP registrado, utilizando diferentes portas.
- D. Na NAT do tipo dinâmica sobreposta um endereço IP não registrado é mapeado para um endereço IP, registrado com uma base unívoca.
- E. Em uma mesma rede, não é possível usar a NAT e o DHCP, pois eles são mutuamente exclusivos.

3. Assinale a opção correta acerca de NAT (network address translation).

- A. Apesar de não fornecer recursos de conexão de tráfego, como rastreamento de usuário, sítios ou conexões, a NAT permite que administradores de redes proíbam acesso a determinados sítios.
- B. O mecanismo de NAT é utilizado exclusivamente por roteadores que operam na camada 3 ou acima.
-  C. Na NAT do tipo dinâmica sobrecarregada vários endereços IP não registrados são mapeados para um único endereço IP registrado, utilizando diferentes portas.
- D. Na NAT do tipo dinâmica sobreposta um endereço IP não registrado é mapeado para um endereço IP, registrado com uma base unívoca.
- E. Em uma mesma rede, não é possível usar a NAT e o DHCP, pois eles são mutuamente exclusivos.

4. Acerca de VPN (Virtual Private Network), assinale a opção correta.

- A. Uma VPN provê uma utilização do canal de comunicação mais racional, por não manter links permanentes entre os pontos de comunicação, mas não possui a função de autenticar pacotes de dados em relação à sua origem.
- B. Funções de hash, MACs (Message Authentication Codes) e assinaturas digitais visam assegurar a integridade das mensagens em uma VPN.
- C. Embora uma VPN possua maior custo do que as linhas dedicadas, ela fornece confidencialidade por meio de criptografia com chave pública ou privada.
- D. RADIUS (Remote Authentication Dial-In User Service) e CHAP (Challenge-Handshake Authentication Protocol) garantem às VPNs não repúdio e disponibilidade, respectivamente.
- E. Os protocolos de tunelamento são limitados às linhas dedicadas e aos circuitos virtuais permanentes e, portanto, não podem ser utilizados em VPNs.

4. Acerca de VPN (Virtual Private Network), assinale a opção correta.

- A. Uma VPN provê uma utilização do canal de comunicação mais racional, por não manter links permanentes entre os pontos de comunicação, mas não possui a função de autenticar pacotes de dados em relação à sua origem.
-  B. Funções de hash, MACs (Message Authentication Codes) e assinaturas digitais visam assegurar a integridade das mensagens em uma VPN.
- C. Embora uma VPN possua maior custo do que as linhas dedicadas, ela fornece confidencialidade por meio de criptografia com chave pública ou privada.
- D. RADIUS (Remote Authentication Dial-In User Service) e CHAP (Challenge-Handshake Authentication Protocol) garantem às VPNs não repúdio e disponibilidade, respectivamente.
- E. Os protocolos de tunelamento são limitados às linhas dedicadas e aos circuitos virtuais permanentes e, portanto, não podem ser utilizados em VPNs.

5. Julgue os itens seguintes, acerca de VPN e VPN-SSL.

[85] As redes VPN oferecem suporte apenas ao protocolo IP.

[86] O SSL tunnel VPN permite que o navegador acesse aplicações e serviços de rede por meio de um túnel que ele esteja executando sob o SSL.

[87] Quando se utiliza um firewall com funções de VPN, as mensagens entram cifradas na rede e somente são decifradas no nível de aplicação.

5. Julgue os itens seguintes, acerca de VPN e VPN-SSL.

~~[85] As redes VPN oferecem suporte apenas ao protocolo IP.~~



[86] O SSL tunnel VPN permite que o navegador acesse aplicações e serviços de rede por meio de um túnel que ele esteja executando sob o SSL.



~~[87] Quando se utiliza um firewall com funções de VPN, as mensagens entram cifradas na rede e somente são decifradas no nível de aplicação.~~



6. Julgue os itens subsecutivos, referentes a firewall e VPN (virtual private network).

[58] VPN que utilize o protocolo IPSEC (IP security) tem mecanismos para a validação da confidencialidade e da integridade dos dados transmitidos.

6. Julgue os itens subsecutivos, referentes a firewall e VPN (virtual private network).

[58] VPN que utilize o protocolo IPSEC (IP security) tem mecanismos para a validação da confidencialidade e da integridade dos dados transmitidos.



7. Em relação à VPN (virtual private network), julgue os próximos itens.

[72] Em VPN do tipo USER-TO-SITE, o túnel só é estabelecido se for utilizado o protocolo IPSec.

[73] Em VPN do tipo SITE-TO-SITE, o usuário é o responsável pelo estabelecimento do túnel.

7. Em relação à VPN (virtual private network), julgue os próximos itens.

~~[72] Em VPN do tipo USER-TO-SITE, o túnel só é estabelecido se for utilizado o protocolo IPSec.~~



~~[73] Em VPN do tipo SITE-TO-SITE, o usuário é o responsável pelo estabelecimento do túnel.~~



8. Em relação a segurança da informação, julgue os itens seguintes.

[84] Em uma VPN com IPSEC é possível fazer uso do 3DES com algoritmo de criptografia que emprega três chaves de 56 bits.

[85] O recurso VPN (virtual private network), utilizado para interligar de forma segura dois pontos através de um meio público como a Internet, pode fazer uso de IPSEC, que recorre ao ESP (encapsulating security payload) para manter a confidencialidade dos dados e à AH (authentication header) para garantir a integridade dos dados.

8. Em relação a segurança da informação, julgue os itens seguintes.

 [84] Em uma VPN com IPSEC é possível fazer uso do 3DES com algoritmo de criptografia que emprega três chaves de 56 bits.

 [85] O recurso VPN (virtual private network), utilizado para interligar de forma segura dois pontos através de um meio público como a Internet, pode fazer uso de IPSEC, que recorre ao ESP (encapsulating security payload) para manter a confidencialidade dos dados e à AH (authentication header) para garantir a integridade dos dados.

9. Com relação a switches, roteadores e NAT (network address translation), julgue os itens subsequentes.

[89] Considere que uma empresa tenha dez computadores que precisam ser conectados à Internet, mas disponha de apenas um endereço IP válido. Nesse caso, recomenda-se a utilização de NAT, pois cada computador terá um endereço privado dentro da LAN e, por meio da porta TCP de destino que se deseja acessar no endereço remoto, o dispositivo responsável por implementar NAT conseguirá identificar o retorno da resposta ao computador interno.

9. Com relação a switches, roteadores e NAT (network address translation), julgue os itens subsequentes.

 ~~[89] Considere que uma empresa tenha dez computadores que precisam ser conectados à Internet, mas disponha de apenas um endereço IP válido. Nesse caso, recomenda-se a utilização de NAT, pois cada computador terá um endereço privado dentro da LAN e, por meio da porta TCP de destino que se deseja acessar no endereço remoto, o dispositivo responsável por implementar NAT conseguirá identificar o retorno da resposta ao computador interno.~~

10. No que concerne a VPN (Virtual Private Network), julgue os itens subsequentes.

[59] Em um filtro de pacotes que atue como firewall em uma rede por onde se verifique tráfego VPN IPSEC (Internet Protocol Security), é necessário liberar a porta 500 e o protocolo UDP (User Datagram Protocol) para o funcionamento da VPN.

[60] O uso do protocolo AH (Authentication Header) no IPSEC (Internet Protocol Security) de uma VPN tem a função de garantir a confidencialidade dos dados trafegados.

10. No que concerne a VPN (Virtual Private Network), julgue os itens subsequentes.

 [59] Em um filtro de pacotes que atue como firewall em uma rede por onde se verifique tráfego VPN IPSEC (Internet Protocol Security), é necessário liberar a porta 500 e o protocolo UDP (User Datagram Protocol) para o funcionamento da VPN.

 ~~[60] O uso do protocolo AH (Authentication Header) no IPSEC (Internet Protocol Security) de uma VPN tem a função de garantir a confidencialidade dos dados trafegados.~~

GABARITO



1. E, C, E

2. E, C, E, E, C

3. C

4. B

5. E, C, E

6. C

7. E, E

8. C, C

9. E

10. C, E