Segurança Operacional

Gustavo Pinto Vilar

ITnerante

Gustavo Vilar

- Mini – CV
  - PPF / DPF – Papiloscopista Policial Federal
  - Pós-Graduado em Docência do Ensino Superior – UFRJ
  - Graduado em Ciência da Computação e Processamento de Dados – ASPER/PB
  - Aprovações: PRF 2002, PF 2004, MPU 2010, ABIN 2010

Gustavo Vilar

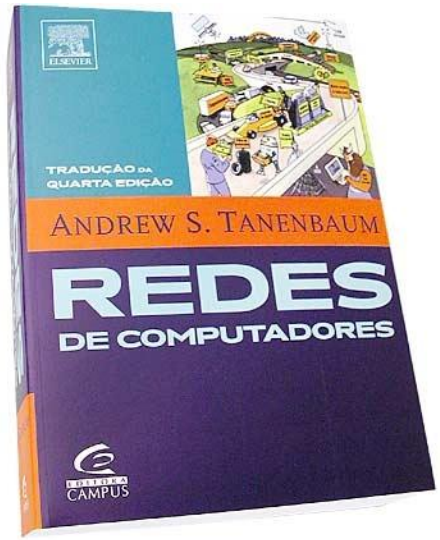
- Contatos:
  - gustavopintovilar@gmail.com
  - p3r1t0f3d3r4l@yahoo.com.br

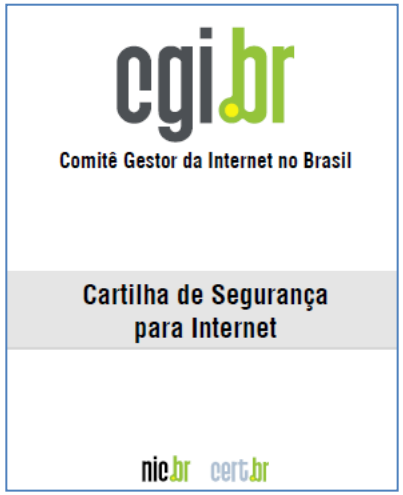
ITnerante

Escopo

- Abordar os assuntos mais recorrentes e com fortes tendências para concursos atuais
- Familiarizar o concursando com os tipos de questões mais freqüentes.
- Abordar as metodologias de resolução de questões das principais bancas

Bibliografia





ITnerante

Segurança Operacional – Carga Horária

- 14 vídeo aulas (04h16m27s)
  - Segurança
    - Conceitos iniciais
    - Questões
  - Malwares
    - Conceitos
    - Questões
  - Fundamentos da segurança perimetral (+)
  - Firewall
    - Conceitos
    - Filtros de pacotes
    - Proxies
    - Comparativos entre as tecnologias
    - Arquiteturas de firewall
    - Questões
  - IDS e IPS
    - Conceitos
    - Pontos de implementação
    - Implementação híbrida e honeypot
    - Questões

ITnerante

Segurança Operacional

Conceitos Iniciais

ITnerante

Informação

- A informação hoje em dia é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e conseqüentemente precisa ser protegido.

Informação

- Pode existir em muitas formas.

  Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é fundamental que seja sempre protegida adequadamente.

Proteção da Informação

- Se refere a ameaças ligadas a fatores tecnológicos e não tecnológicos
- Garantir a continuidade dos negócios, minimizando possíveis danos e maximizando o retorno sobre investimentos e as oportunidades de negócio

Confidencialidade

Proteção contra exposição **não autorizada**.

- **Acesso** somente por pessoas **autorizadas**

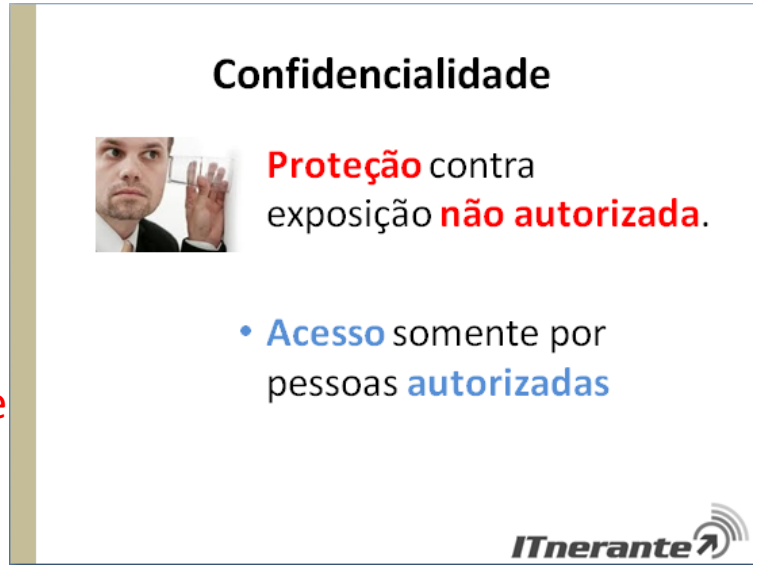
Integridade

- **Proteção** contra modificação **não autorizada**
- **Modificação** somente pelas partes **autorizadas**

Disponibilidade

- **Acesso** disponível às **entidades autorizadas** sempre que **necessário**

- OBS: Não confundir com confidencialidade



ITnerante

Autenticidade

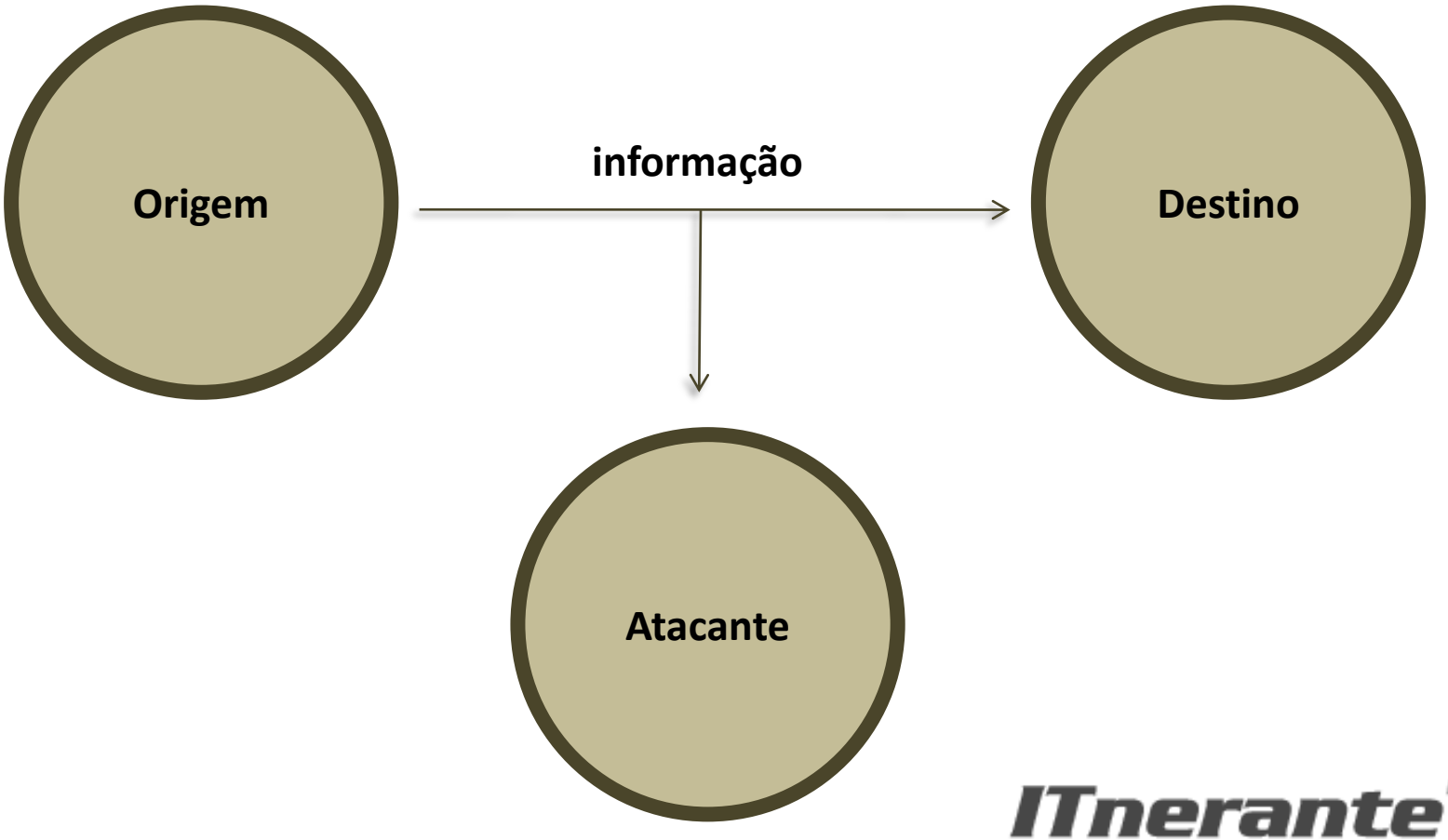
- **Remetente** e/ou **destinatário** devem ser corretamente identificados
- “Afirmação”

Irretratabilidade / Não-repúdio

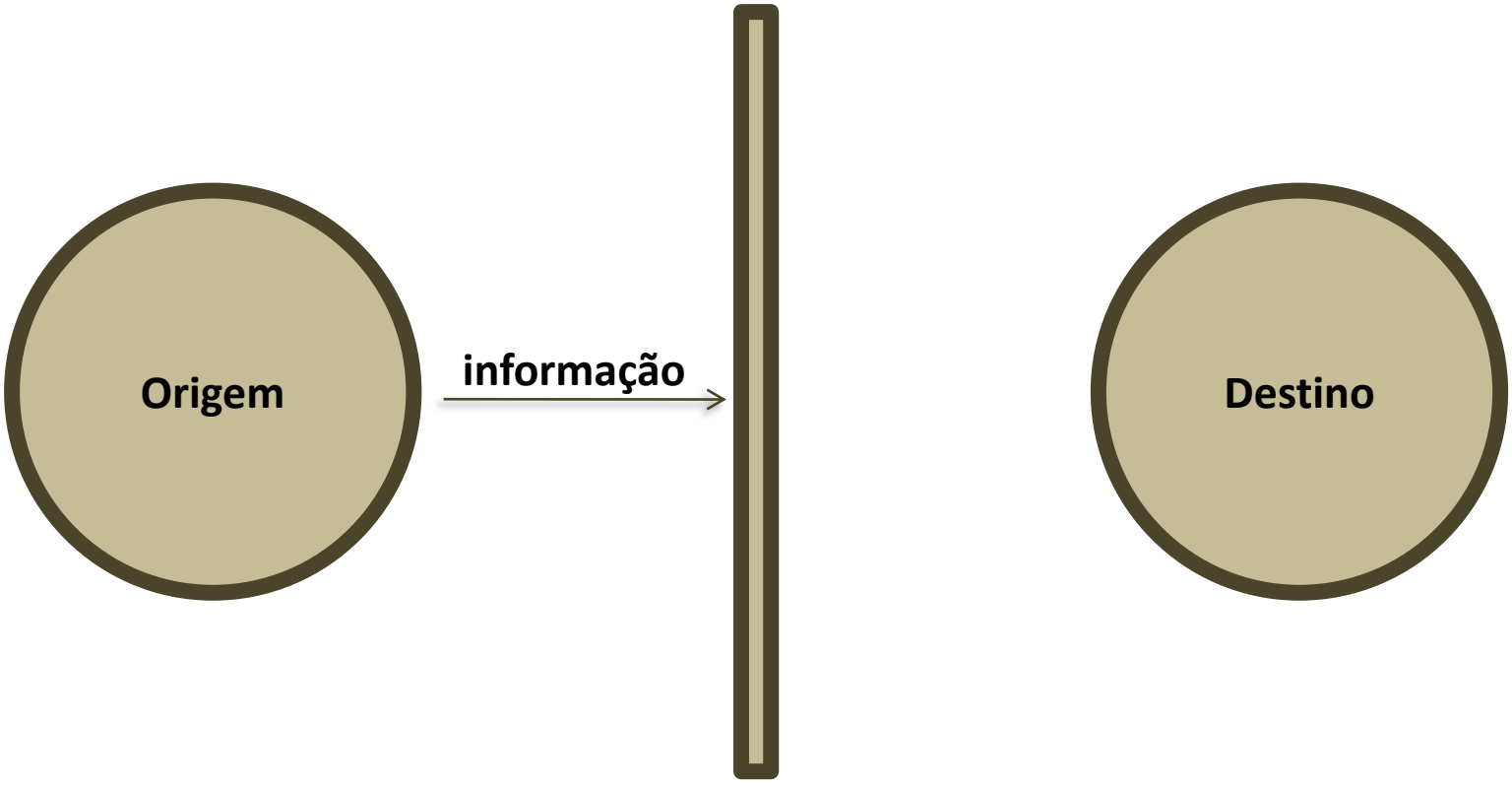
- **Proteção** contra **negação** de **envio** (ou **recepção**) de determinada informação
- “Negação”

Fluxo normal

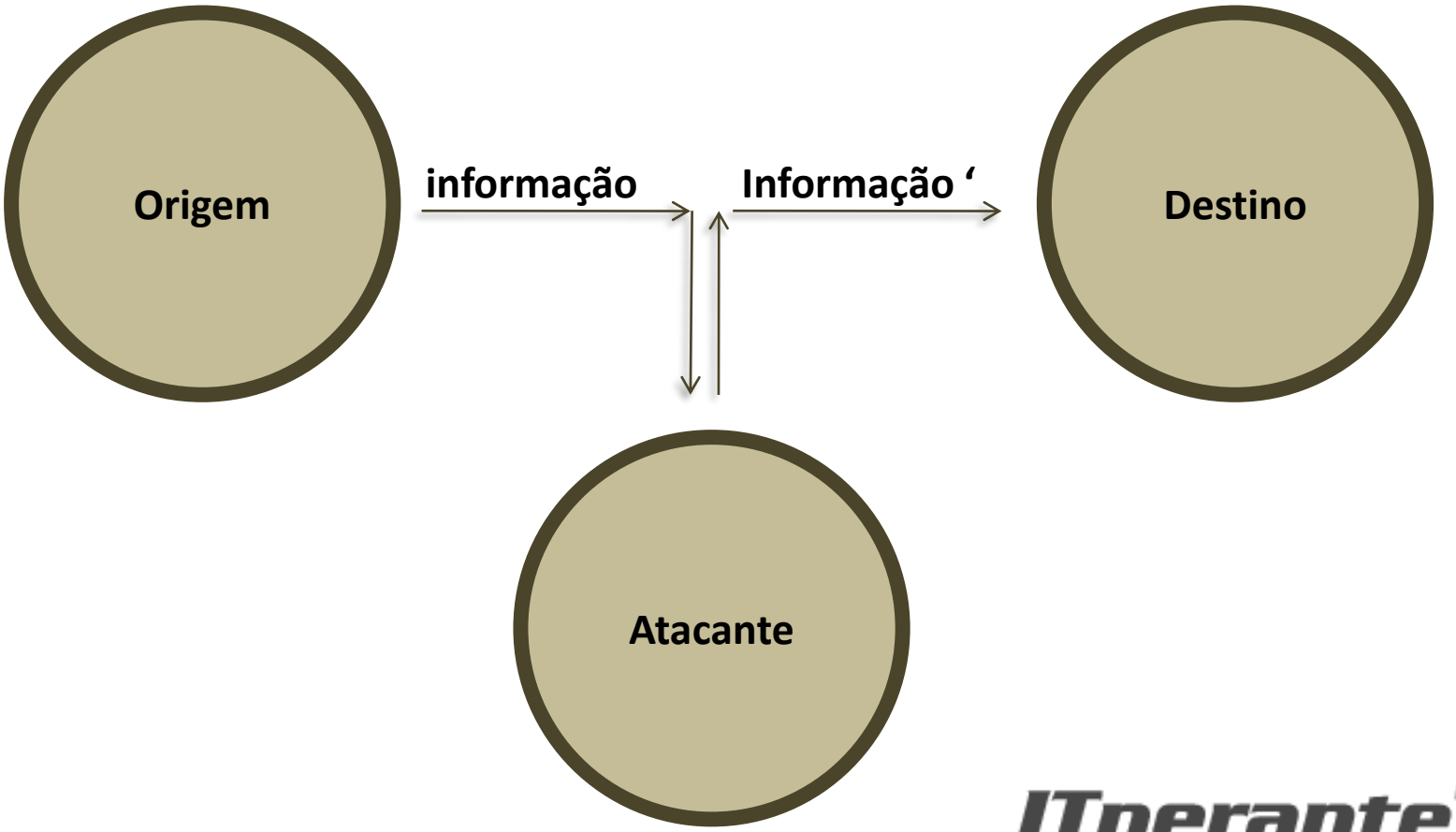
Interceptação



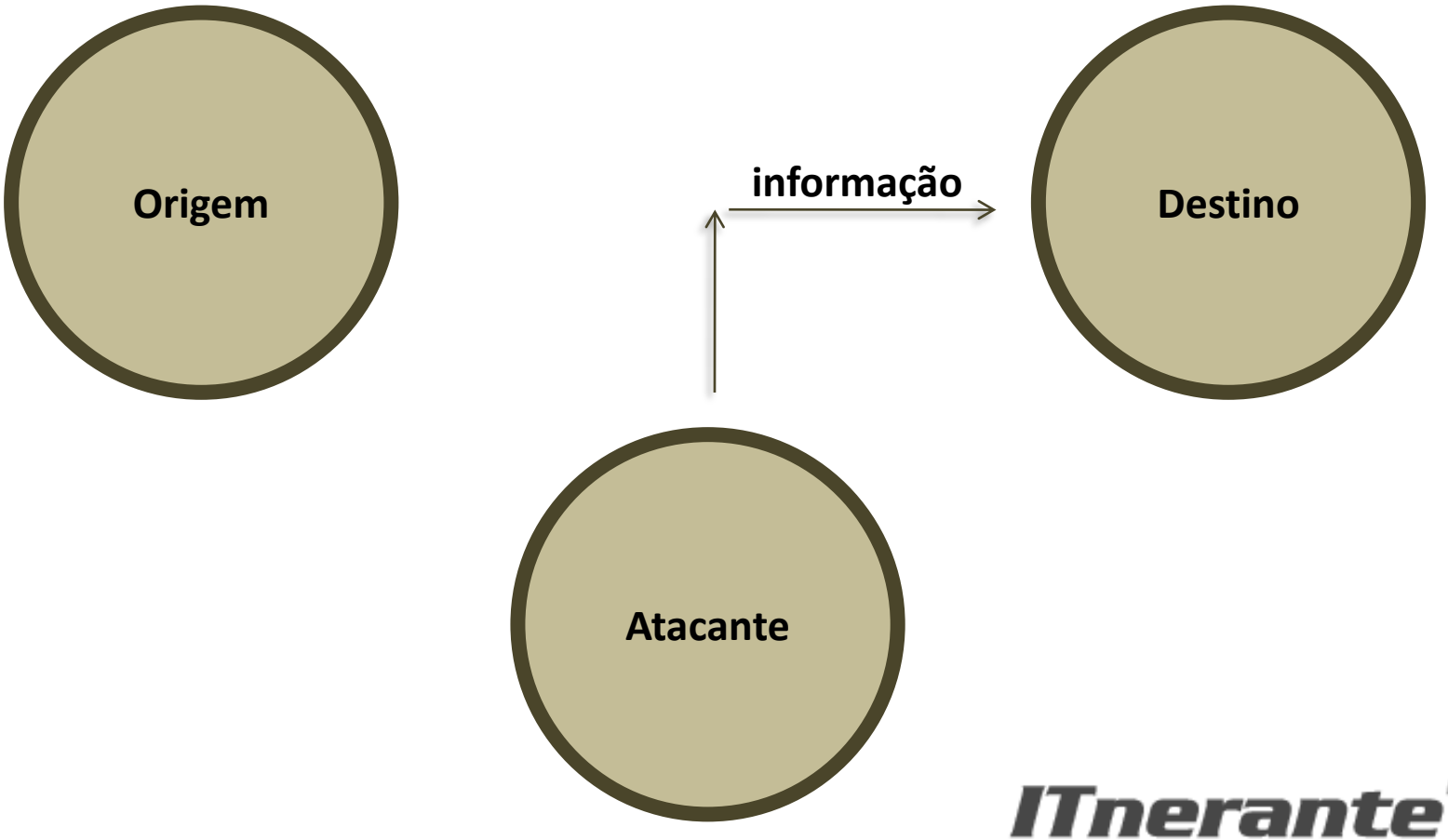
Interrupção



Modificação



Fabricação



Bateria de questões de aprendizagem

Conceitos Iniciais

ITnerante

1. Pref de Porto Alegre – CONSULPLAN 2011 – Municipal – Analista de TI

NÃO é um atributo da segurança da informação

A. confidencialidade.
B. integridade.
C. autoridade.
D. disponibilidade.
E. autenticidade.

2. COPERGÁS– FCC 2011 – Superior - Analista de Sistemas

No processo de auditoria, objetivando garantir a segurança da informação, devem ser contemplados nas validações os requisitos de

A. confidencialidade, integridade e disponibilidade.
B. confidencialidade, conformidade e confiabilidade.
C. eficiência, integridade e disponibilidade.
D. eficiência, conformidade e confiabilidade.
E. integridade, conformidade e confiabilidade.

3. TRT 24 Região – FCC 2011 – Analista Judiciário – tecnologia da Informação

Considere:

I. Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

II. Salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

III. Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Na ISO/IEC 17799, I, II e III correspondem, respectivamente, a

A. disponibilidade, integridade e confiabilidade.
B. confiabilidade, integridade e distributividade.
C. confidencialidade, integridade e disponibilidade.
D. confidencialidade, confiabilidade e disponibilidade.
E. integridade, confiabilidade e disponibilidade.

4. TRE RN – FCC 2011 – Técnico Judiciário – Programação de sistemas

Em relação à segurança em redes de computadores existem ataques de negação de serviços, onde o acesso a um sistema é interrompido ou impedido, deixando de estar disponível; ou uma aplicação, cujo tempo de execução é crítico, é atrasada ou abortada. Trata-se de um ataque que compromete o aspecto da

A. autenticidade.
B. confidencialidade.
C. disponibilidade.
D. integridade.
E. interoperabilidade.

5. TRF 4 Região – FCC 2010 – Técnico Judiciário – Operação de Computadores

Os atributos básicos da segurança da informação são:

a. Confidencialidade, Integridade e Direcionamento.

b. Comunicabilidade, Integridade e Disponibilidade.

c. Confidencialidade, Integridade e Disponibilidade.

d. Confidencialidade, Interface e Disponibilidade.

e. Comunicabilidade, Interface e Disponibilidade.

6. Banco do Brasil– CESPE 2009 – Gestão de Segurança - Certificação

Assinale a opção correspondente à propriedade que não é alcançada com o uso de técnicas da criptografia para proteção da informação.

a. Integridade

b. Autenticidade

c. Irretratabilidade (não-repúdio)

d. Confidencialidade

e. Disponibilidade

7. MEC– FGV 2009 – Analista de segurança – Pol. de Segurança

ISO 17799 constitui um padrão de recomendações para práticas na Gestão de Segurança da Informação. Ele permite que uma empresa construa de forma muita rápida uma política de segurança com controles eficientes. De acordo com o estabelecido no padrão, avalie as afirmativas a seguir.

I. Um primeiro termo visa garantir que as informações sejam acessíveis apenas para aqueles que estão autorizados a acessá-las.

II. Um segundo tem por objetivo salvaguardar a exatidão e a inteireza das informações e os métodos de processamento,

III. Um terceiro assegura que os usuários autorizados tenham acesso às informações e aos ativos associados quando necessário.

Esses três termos são denominados, respectivamente:

a. integridade, confidencialidade e disponibilidade.
b. integridade, disponibilidade e confidencialidade.
c. confidencialidade, integridade e disponibilidade.
d. confidencialidade, disponibilidade e integridade.
e. disponibilidade, confidencialidade e integridade.

8. TRE4 MT – CESPE 2010 – Técnico Judiciário – Operação de Computadores

A respeito dos conceitos de segurança da informação, assinale a opção correta.

a. Disponibilidade é a garantia de que o acesso à informação seja obtido apenas por pessoas autorizadas.

b. Confidencialidade é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

c. No processo de autorização para a instalação de processamento da informação, importante para a segurança da informação, hardware e software são verificados de maneira independente; não há necessidade de se garantir compatibilidade com outros componentes do sistema.

d. Os controles de criptografia visam proteger a confidencialidade, a autenticidade e a integridade das informações consideradas de risco e para as quais outros controles não fornecem proteção adequada.

e. Assinaturas digitais, para serem implementadas por meio de técnicas criptográficas, necessitam de, pelo menos, dois pares de chaves relacionadas. Um par é utilizado para criar uma assinatura (privada), e o outro, para verificar a assinatura (pública).

9. TRF 4 Região – FCC 2009 – Técnico Judiciário – Operação de Computadores

Informações são ativos que, como qualquer outro ativo importante para os negócios, possuem valor para uma organização e conseqüentemente precisam ser protegidos adequadamente. A segurança de informações tem por objetivo garantir a proteção contra uma gama de ameaças, para assegurar a continuidade dos negócios, minimizar prejuízos e maximizar o retorno de investimentos e oportunidades comerciais. As informações podem existir sob muitas formas. Podem ser impressas ou escritas em papel, armazenadas eletronicamente, enviadas pelo correio ou usando meios eletrônicos, mostradas em filmes, ou faladas em conversas. Qualquer que seja a forma que as informações assumam, ou os meios pelos quais sejam compartilhadas ou armazenadas, elas devem ser sempre protegidas adequadamente.

ISO/IEC 17799:2000: Tecnologia da Informação - Código de prática para gestão da segurança de informações, p. VI (com adaptações).

A respeito de segurança da informação, julgue os próximos itens.

- A confidencialidade tem o objetivo de garantir que apenas pessoas autorizadas tenham acesso à informação. Essa garantia deve ser obtida em todos os níveis, desde a geração da informação, passando pelos meios de transmissão, até chegar ao seu destino e ser devidamente armazenada ou, se necessário, destruída sem possibilidade de recuperação.
- O processo de proteção da informação contra modificações não autorizadas ou acidentais, conhecido como processo de irretratabilidade, garante a integridade da informação, mas não necessariamente garante que o seu conteúdo esteja correto.

Gabarito

1. C
2. A
3. C
4. C
5. C
6. E
7. C
8. D
9. C, E

Segurança Operacional

Malware

Malware

- **Mal**icious Soft**ware**

- É um termo genérico.
- Abrange todos os tipos de programa especificamente desenvolvidos para executar ações maliciosas em um sistema.
- São espécies: Vírus, worms, trojan horses, spywares...

Vírus

- Programa (ou parte) de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador
- O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção
- Possui um rol muito extenso de atividades

Worm

- Programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo.
- Auto-replicante, não precisa de outro programa para se propagar
- Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores
- Consumo de recursos e degradação de desempenho de redes e computadores

Trojan Horses

- Executa, além de suas funções, funções clandestinas, pois trata-se de software que executa também atividades não previstas
- “Cavalo” deve ser executado
- Trojan contém vírus, worm, keylogger ou qualquer outra coisa
- Distingue-se de um vírus ou de um worm por não infectar outros arquivos, nem propagar cópias de si mesmo automaticamente

Bot

- Ro**bot**
- De modo similar ao worm, o bot é um programa capaz se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de softwares instalados em um computador.
- Adicionalmente ao worm, dispõe de mecanismos de comunicação com o invasor, permitindo que o bot seja controlado remotamente.
- Normalmente, o bot se conecta a um servidor de IRC (Internet Relay Chat) e entra em um canal (sala) determinado, esperando instruções do invasor
- Botnets são redes formadas por computadores infectados com bots

Spyware

- Violação da confidencialidade
- monitorar atividades de um sistema e enviar as informações coletadas para terceiros.

Códigos maliciosos – Keyloggers

- Captura e armazena as teclas digitadas
- Screenloggers e mouseloggers são variantes que fazem a gravação da tela, além do teclado

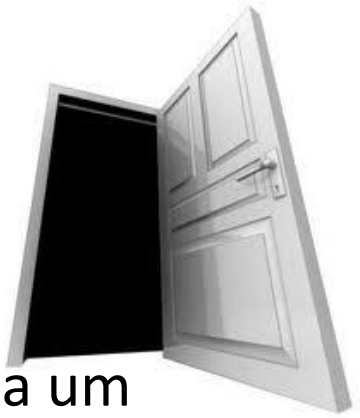
Adware

- **Ad**vertisement – propaganda
- projetado para apresentar propagandas, seja através de um browser, seja através de algum outro programa instalado em um computador.
- Têm sido incorporados a softwares e serviços (legítimo)
- Nada impede a execução de serviços ilegítimos em background

Bomba Lógica

- Depende de hospedeiro
- Ativados sob determinada condição

Backdoors



- Programas que permitem o RETORNO de um invasor a um computador comprometido.
- A forma usual de inclusão de um backdoor consiste na disponibilização de um novo serviço ou substituição de um determinado serviço por uma versão alterada, normalmente possuindo recursos que permitam acesso remoto (através da Internet).
- Podem existir, também, sob a forma de pacotes de softwares como NetBus e BackOrifice
- Sua existência não pressupõe invasão. Alguns softwares, por, exemplo, alegam necessidades administrativas

Códigos maliciosos – Rootkit

- Um invasor, ao realizar uma invasão, pode utilizar mecanismos para esconder e assegurar a sua presença no computador comprometido. O conjunto de programas que fornece estes mecanismos é conhecido como rootkit.
- **Não** é utilizado **para obter** acesso privilegiado em um computador, mas sim para mantê-lo

Bateria de questões de aprendizagem

Malware

ITnerante

1. Pref de Porto Alegre – Consulplan 2011 – Analista de TI

1. Analise as afirmativas.

I. Rootkits é um tipo de malware cuja principal intenção é se camuflar, impedindo que seu código seja encontrado por qualquer antivírus.

II. Um rootkit é um programa com código mal intencionado que busca se esconder de softwares de segurança e do usuário utilizando diversas técnicas avançadas de programação.

III. Os rootkits possuem esse nome por serem inicialmente "kits" de programas para a plataforma Windows.

Está(ão) correta(s) apenas a(s) afirmativa(s)

A. I, II

B. I, III

C. II, III

D. II

E. I, II, III

2. INFRAERO – FCC 2011 – Analista Superior III – rede e Suporte

São programas maliciosos que exploram vulnerabilidades existentes ou falhas na configuração de softwares instalados em um computador e que dispõem de mecanismos de comunicação com o invasor, para permitir que o programa seja controlado remotamente e o invasor, com presença assegurada, possa desferir os ataques ao computador comprometido e/ou a outros computadores. Trata-se de

A. Vírus e Worm.
B. Bot e Rootkit.
C. Trojan e Spyware.
D. Spyware e adware.
E. Worm e Exploits.

3. COFEN – Consulplan 2011 – Webdesigner

10. Com relação aos conceitos de vírus, worms, cavalos de troia, analise:

I. Um vírus é um código de computador que se anexa a um programa ou arquivo para poder se espalhar entre os computadores, infectando-os à medida que se desloca. Os vírus podem danificar software, hardware e arquivos.

II. Um worm, assim como um vírus, cria cópias de si mesmo de um computador para outro, mas faz isso automaticamente. Primeiro, ele controla recursos no computador que permitem o transporte de arquivos ou informações. Depois que o worm contamina o sistema, ele se desloca sozinho. O grande perigo dos worms é a sua capacidade de se replicar em grande volume.

III. O cavalo de troia (uma subclasse de vírus), geralmente se alastra sem a ação do usuário e distribui cópias completas (possivelmente modificadas) de si mesmo através das redes. Um cavalo de troia pode consumir memória e largura de banda de rede, o que pode travar o seu computador. São programas que não têm influência em diretivas e direitos de acesso externo, agem como disseminadores de códigos que danificam o funcionamento do Sistema Operacional.

Está(ão) correta(s) apenas a(s) afirmativa(s):

A. I, II, III

B. I, II

C. II, III

D. I

E. III

4. COFEN – Consulplan 2011 – Técnico Judiciário – Tecnologia da Informação

Um tipo de software especificamente projetado para apresentar propagandas por meio de browsers na Internet é um:

a. spyware.
b. rootkit.
c. adware.
d. backdoor.
e. keylogger.

5. CFA – IADES 2010 – Técnico em Suporte de Redes

Os vírus de macro são pequenos programas que infectam os computadores através dos

A. drivers de dispositivos.
B. arquivos de dados.
C. arquivos executáveis, com extensão .EXE.
D. arquivos executáveis, com extensão .COM.

6. TJ-AC – FMP 2010 – Analista de Suporte

26. Considere as afirmações abaixo:

I. Um cavalo de Tróia (trojan) é um código que aparentemente executa uma ação, mas na verdade realiza outra, como, por exemplo, instalar um programa de porta de fundos (backdoor), um vírus ou um verme.

II. Um vírus necessita se anexar a um programa existente ao passo que um verme é um programa independente que se propaga via rede.

III. O sistema operacional GNU/Linux é imune a vírus e a vermes.

IV. As mensagens não-solicitadas (spam) podem ser usadas como meio de difusão de programas maliciosos.

V. Hoaxes são histórias falsas recebidas por e-mail, sites de relacionamentos e na Internet em geral, cujo conteúdo, além das conhecidas correntes, consiste em apelos dramáticos de cunho sentimental ou religioso, supostas campanhas filantrópicas, humanitárias ou de socorro pessoal ou, ainda, falsos vírus que ameaçam destruir, contaminar ou formatar o disco rígido do computador.

A quantidade de afirmações corretas é:

A. 1
B. 2
C. 3
D. 4
E. 5

7. MPE-SE – FCC 2009 – Analista MP – Análise de Sistemas

É uma forma fraudulenta de obtenção de senhas informadas pelos usuários em teclados virtuais exibidos nas páginas de acesso de instituições financeiras:

a. opt-in.
b. rootkit.
c. proxy.
d. keylogger.
e. screenlogger.

8.Liquigás – CETRO 2008 – Profissional Jr – Informática – Análise de Sistemas

Considere as seguintes definições:

I. De modo similar ao Worm, é um programa capaz se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de softwares instalados em um computador. Adicionalmente ao Worm, dispõe de mecanismos de comunicação com o invasor, permitindo que seja controlado remotamente.

II. É o conjunto de programas, utilizado por um invasor, que oferece mecanismos para esconder e assegurar a presença do invasor no computador comprometido. O invasor terá acesso privilegiado ao computador comprometido.

III. Permite mapear potenciais vulnerabilidades em outros computadores.

Tais definições correspondem, respectivamente, a

a. Vírus de macro, Toolkit e Spam.
b. Bot, Rootkit e Scanner.
c. Bug, Worm, Sniffer.
d. Spam, Bot e Toolkit.
e. Bug, Spam e Rootkit.

9. TCU – CESPE 2007 – ACE – Auditoria de TI

- [153] São características típicas dos malwares: cavalos de tróia aparentam realizar atividades úteis; adwares obtêm e transmitem informações privadas do usuário; backdoors estabelecem conexões para fora da rede onde se encontram; worms modificam o código de uma aplicação para propagar-se em uma rede; e botnets realizam ataques articulados por meio de um controle remoto.

- [154] Rootkits apresentam portabilidade entre plataformas e devem ser manuseados conforme os controles estabelecidos no capítulo relativo à aquisição, desenvolvimento e manutenção de sistemas de informação da NBR 17799.

10. TRF 2 Região – FCC 2007 – Técnico Judiciário – Informática

Ao realizar uma invasão, um invasor pode se esconder e assegurar a sua presença no computador comprometido por meio de mecanismos denominados

a. adware.
b. rootkit.
c. spyware.
d. backdoor.
e. botnet.

Gabarito

1. A
2. B
3. B
4. C
5. B
6. D
7. E
8. B
9. E, E
10. B

Segurança Operacional

Fundamentos da Segurança Perimetral

ITnerante

Proteger...

- O que
  - Dados e informações – CID
  - Recursos – Hardware, software, storage
  - Imagem...
- Contra o que / quem
  - Invasão
  - DoS
  - Furto de informações
  - Vândalos
  - Espiões
  - Administradores
  - Usuários internos e externos
  - Crackers...

O que querem os invasores

- Atacantes passivos (C)
- Atacantes ativos (C, D, A, I)

- Motivações
  - Ganhos financeiros
  - Desafios pessoais
  - Auto-afirmação perante grupos sociais
  - Vingança
  - **Insatisfação profissional**
  - Curiosidade

Camadas de Segurança

- Desencorajar
- Dificultar
- Discriminar
- Detectar
- Deter
- Diagnosticar

Mecanismos de Segurança

- Ameaças lógicas
  - vírus, acessos remotos à rede, backup desatualizados, violação de senhas, etc.
- Controles Lógicos
  - Impedem ou limitam o acesso à informação que está em ambiente controlado, geralmente eletrônico

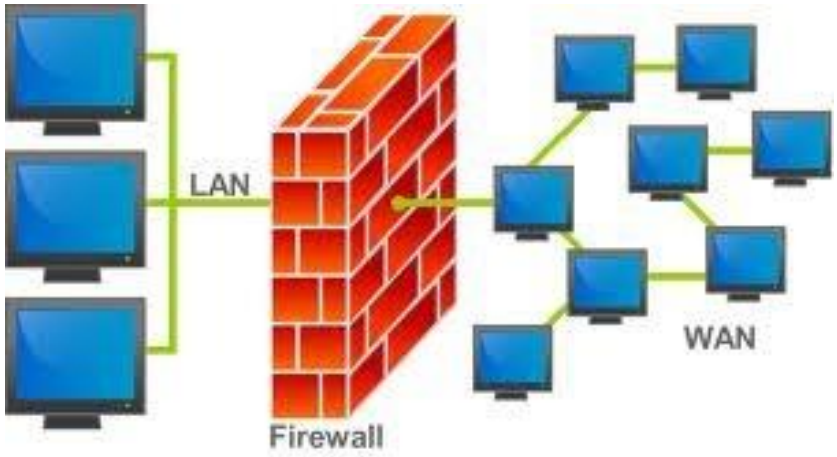
- Ameaças físicas
  - Incêndio, desabamentos, relâmpagos, alagamentos, acesso indevido de pessoas, forma inadequada de tratamento e manuseio do material
- Controles Físicos
  - Limitam o contato ou acesso direto à informação ou à infra-estrutura
  - Técnicas de proteção de dados não têm serventia nenhuma se a segurança física não for mantida

Segurança Operacional

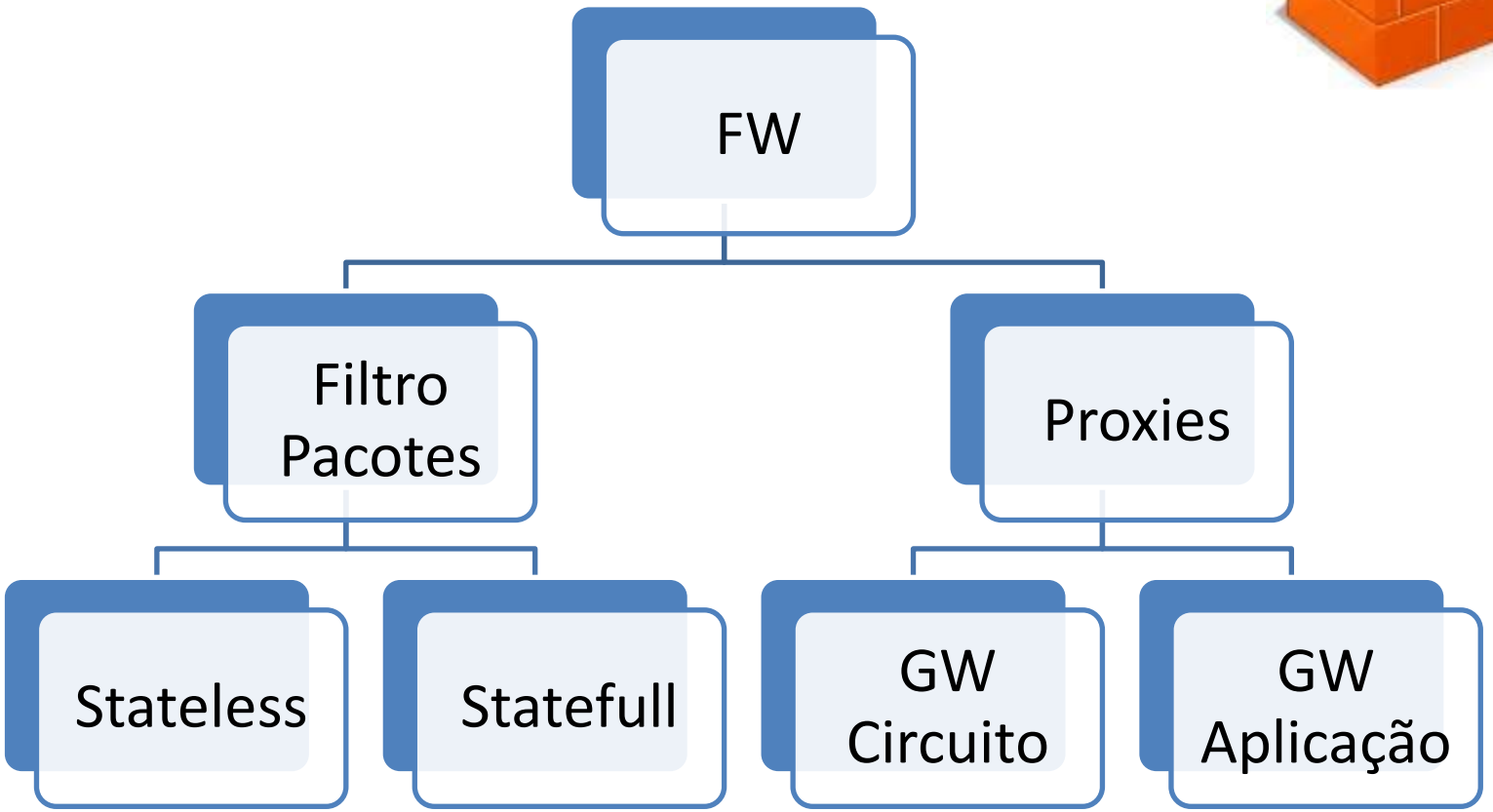
Firewall

Firewall

- Ponto entre duas ou mais redes
- Controle e autenticação e registro do tráfego
- Primeiros FW foram instalados em roteadores
- Adição de novas funcionalidades ao FW
- Políticas: Blacklist & Whitelist
- O que é protegido pelo FW?



Espécies de FW



Tecnologias de FW

Filtros de Pacote

- Operam nas camadas de rede e transporte
  - Stateless
  - Statefull

Proxies

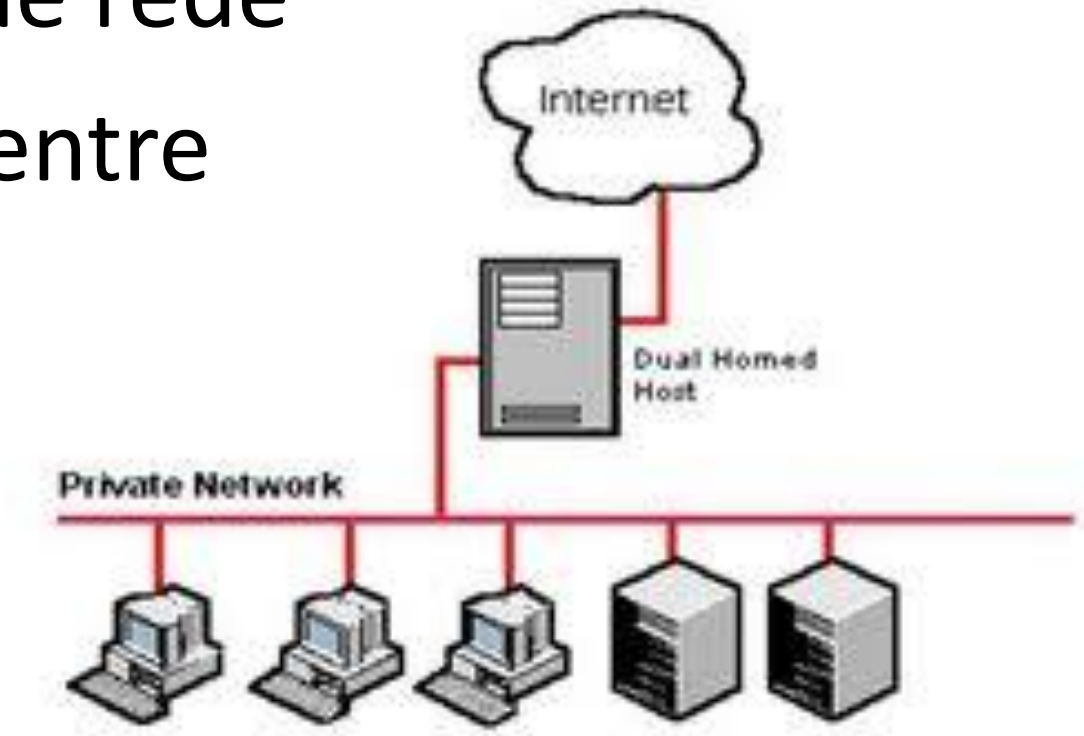
- Operam na camada de aplicação (TCP/IP)
  - Circuit-level gateway
  - Application-level gateway

Arquiteturas

- Dual Homed-host
- Screened Host
- Screened Subnet

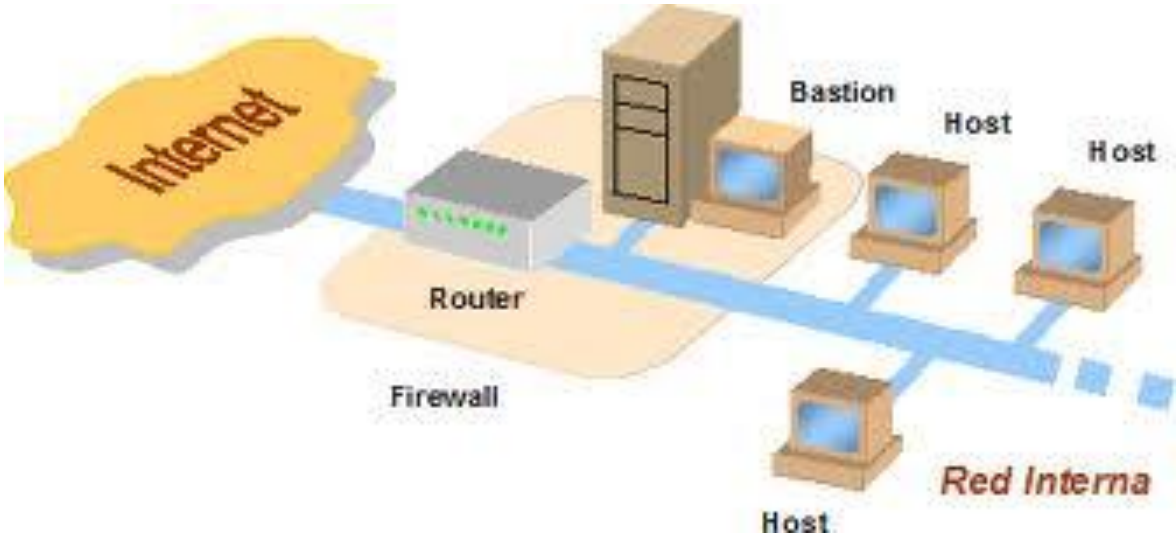
Dual Homed-host

- Equipamento munido de duas interfaces de rede
- Separador entre 02 redes



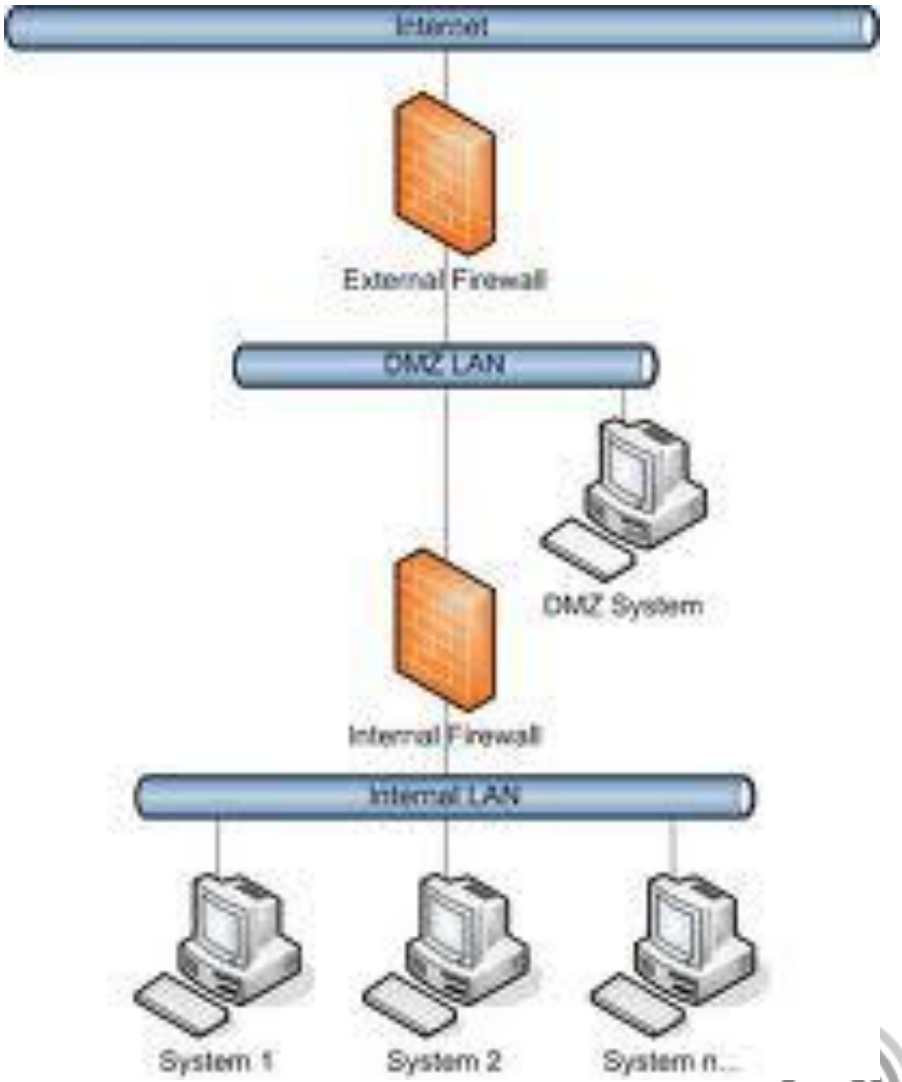
Screened host

- Filtro de pacotes
  + bastion host
- Bastion host está
  dentro da rede



Screened Subnet

- Bastion host na DMZ
- DMZ abriga serviços oferecidos para a rede externa



Funcionalidades adicionais aos FW

- NAT
- VPN
- Autenticação e Certificação
- Balanceamento de carga
- Alta disponibilidade

Bateria de questões de aprendizagem

FW

ITnerante

1. TRT 19– FCC 2011 – Tecnico Judiário – Tecnologia da Informação

Interceptação e Análise de Tráfego são ataques passivos à segurança. Para se defender contra esses tipos de ataque deve-se realizar a

A. configuração de firewall e DMZ (zona desmilitarizada).
B. configuração e aplicação de filtros no servidor.
C. autenticação, e garantir a integridade das informações através de certificação digital e criptografia (assinatura digital).
D. codificação (criptografia) dos dados, evitando que o seu conteúdo se torne disponível mesmo se interceptado.
E. aplicação de segurança física dos recursos de processamento e comunicação de dados

2. Banco da Amazônia – CESPE 2010 – TI – Segurança da Informação

Conjunto I

```
allow tcp from any to any
deny tcp from any to any 80
deny tcp from any to any 21
```

Conjunto II

```
permit tcp any any eq 22
permit tcp any any eq 25
permit tcp any any eq 53
permit tcp any any eq 80
permit tcp any any eq 110
permit tcp any any eq 443
permit udp any any eq 53
permit icmp any any
```

A respeito de firewalls, e considerando os conjuntos de regras acima e que os serviços estejam utilizando as suas portas default, julgue os itens que seguem.

101 As regras do conjunto I permitem todo o tráfego TCP, exceto para as portas 21 e 80

102 O conjunto II implementa uma política para DNS que permite consultas, mas bloqueia transferências de zona.

103 Os tráfegos HTTP e HTTPS são permitidos pelas regras dos conjuntos I e II.

104 Os dois conjuntos apresentados permitem correio eletrônico.

105 Apenas o conjunto II permite o tráfego ICMP.

3. FINEP – CESGRARIO 2011 – Analista - Suporte

- Defesa em profundidade é o processo de dispor componentes de segurança em camadas para tirar proveito do melhor de cada um. Esse conceito envolve o perímetro, a rede interna e um fator humano. Com relação ao perímetro, o componente de segurança capaz de impedir que um código móvel malicioso seja transferido da rede externa, por uma aplicação executada por um usuário em uma estação da rede interna, através da correta utilização de um protocolo de comunicação, permitido pela política de segurança da empresa, é

A. Firewall Proxy
B. Firewall com Estado
C. Firewall sem Estado
D. Rede Screened
E. Servidor VPN

4. INMETRO – CESPE 2010 – Pesquisador – Infra e redes de TI

Assinale a opção que apresenta apenas elementos que trabalham com controles de acesso físico aos recursos de um ambiente organizacional.

a. catraca, firewall, sensor de presença
b. firewall, antivírus, sensor de RFID
c. sensor de presença, firewall, antivírus
d. sensor de RFID, antivírus, catraca
e. sensor de presença, catraca, sensor de RFID

5. Prefeitura de Natal – ESAF 2008 – Auditor do Tesouro Municipal

Analise as seguintes afirmações relacionadas à Segurança da Informação.

I. Um Firewall pode ser configurado com a seguinte política: o que não é expressamente permitido, é proibido.

II. Um Firewall evita invasões que partam de máquinas na rede onde se encontra a máquina invadida.

III. O spoofing é uma técnica de subversão de sistemas que ocorre quando um pacote é feito e enviado para parecer que veio da rede interna, mesmo que tenha vindo de uma rede externa.

IV. Uma rede corporativa protegida por um Firewall instalado entre a rede interna e o acesso ao backbone da Internet garante a segurança mesmo que algumas máquinas não utilizem acesso à Internet via Modem próprio desde que estes utilizem protocolo PPP ou SLIP.

Indique a opção que contenha todas as afirmações verdadeiras.

a. I e II

b. II e III

c. III e IV

d. I e III

e. II e IV

6. Prefeitura de Natal 2008 – ESAF – Auditor do T. Municipal - Informática

Analise as seguintes afirmações relacionadas à Segurança da Informação e os objetivos do controle de acesso:

I. A disponibilidade é uma forma de controle de acesso que permite identificar os usuários legítimos da informação para que lhes possa ser liberado o acesso, quando solicitado.

II. A confidencialidade é uma forma de controle de acesso que evita que pessoas não autorizadas tenham acesso à informação para criá-la, destruí-la ou alterá-la indevidamente.

III. O IDS (Intrusion Detection System) é um dispositivo complementar à proteção contra invasão de redes, que inspeciona uma rede de dentro para fora, identifica e avalia padrões suspeitos que podem identificar um ataque à rede e emite um alarme quando existe a suspeita de uma invasão.

IV. A integridade é uma forma de controle de acesso que evita o acesso de pessoas não autorizadas a informações confidenciais, salvaguardando segredos de negócios e protegendo a privacidade de dados pessoais.

Indique a opção que contenha todas as afirmações verdadeiras.

A. I e II

B. II e III

C. III e IV

D. I e III

E. II e IV

Gabarito

1. D
2. E, E, C, C, C
3. A
4. E
5. D
6. D

Segurança Operacional

IDS e IPS

ITnerante

Mudança e evolução do ambiente

Mudança de abordagem

- Monitoramento de perímetro passou para monitoramento interno
- Bolsões de segurança
  - Acesso a recursos internos

Evolução do ambiente

- Organizações desconectadas das redes públicas
- Conexão com a filial
- Acesso remoto por modem
- Conexão com a internet
- Provisão de serviços para internet
- Provisão de acesso do bancos de dados

IDS

- Detectar atividades suspeitas, impróprias, incorretas ou anômalas
- É um complemento do firewall, pois analisa os serviços permitidos
- Ferramenta passiva *

IPS

- “IDS que operam no modo INLINE”
- Admite posicionamentos Antes e Depois do Firewall
- Ferramenta ativa*

Análises: Resultados possíveis

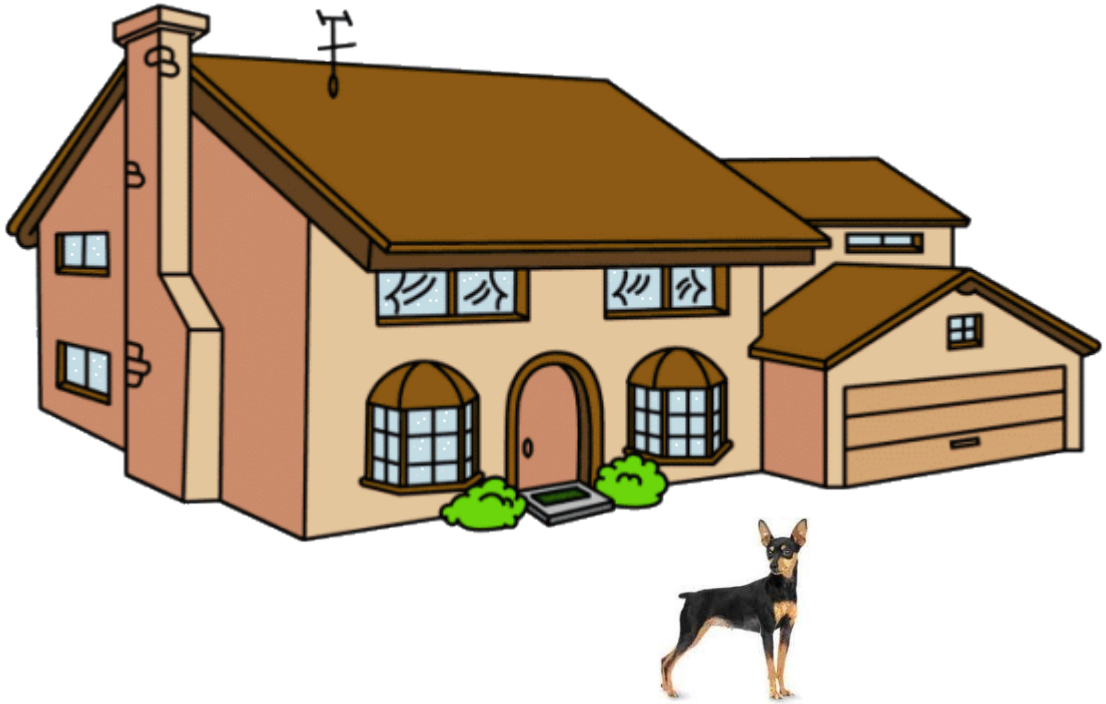
- Normal

  - Tráfego suspeito detectado como suspeito
  - Tráfego legítimo detectado como legítimo

Anormal

  - Tráfego suspeito não detectado
  - Tráfego legítimo detectado como suspeito

Analogia: “A residência”



Comparativo

IDS

- “Se recuperam do ataque”
- IDS: Geram alarmes
  - Natureza dos IDS
    - Passiva
    - Ativa (pós-detecção)

IPS

- “Previnem o ataque”
- IPS: Executam contramedidas (interrupções de fluxos de dados)
- Está em modo IN-LINE com o firewall

Segurança Operacional

IDS e IPS

ITnerante

Metodologias de Detecção

Knowledge-Based-Intrusion Detection

- conhecimento sobre ataques se deriva do conhecimento de especialistas humanos
- Fundamentada em bases de dados com info sobre ataques CONHECIDOS
- Gera Poucos Falsos positivos se comparado ao Behavior-Based

Behavior-Based Intrusion Detection

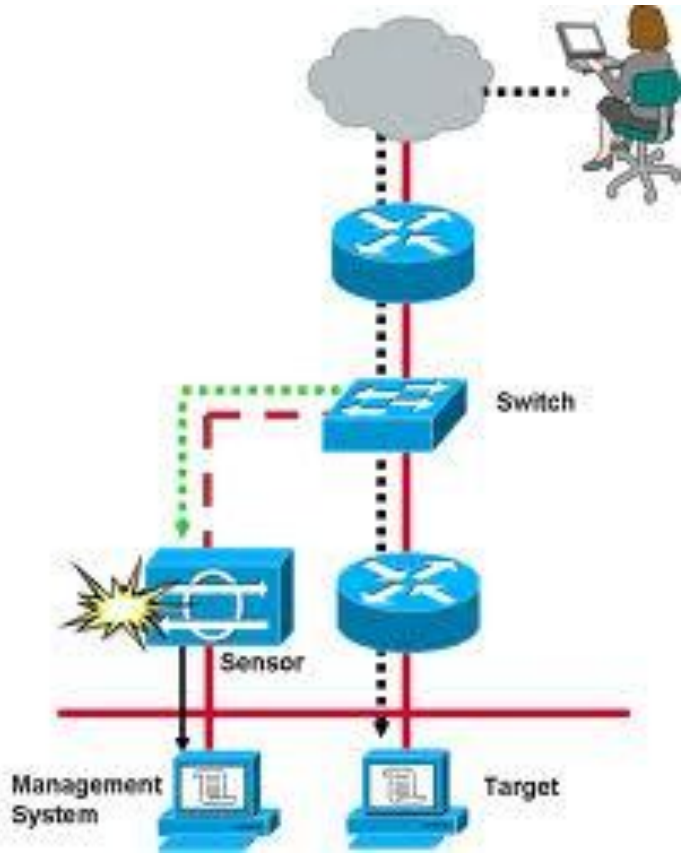
- intrusões podem ser detectadas com base em desvios de comportamento dos usuários ou sistemas
- Qualquer comportamento suspeito, diferente do padrão, é considerado intrusivo

Pontos de implementação

Host Based - HIDS

- Análise de logs e de indicadores de estado do sistema
- Detecta ataques físicos ao computador
- Detecta ataques criptográficos
- Faz a leitura de logs

Pontos de implementação



Network Based - NIDS

- Monitora o tráfego no segmento de rede
- Detecção de ataques à rede em TEMPO REAL
- Partes
  - Sensores
  - Console

Implementação híbrida

- Combinação de pontos fortes do HIDS e NIDS
- Persiste o problema da escalabilidade
- Está mais para um HIDS que opera como um NIDS do que o inverso
- HIDS + Pilha de protocolos

Honeypot

- Não é necessariamente um tipo de IDS
- Não contém dados ou aplicações importantes para a organização
- Objetivo: Passar-se por equipamento legítimo
- Não existem falsos positivos pois o tráfego é real

Bateria de questões de aprendizagem

IDS, IPS

ITnerante

1. TRE PE– FCC 2011 – Profissional Básico – Analista Judiciário – Analista de Sistema

Em relação a firewall, IPS e IDS é correto afirmar:

A. NIDS são instalados em servidores para analisar o tráfego de forma individual em uma rede, tais como, logs de sistema operacional, logs de acesso e logs de aplicação.

B. O IDS usa sua capacidade de detecção e algumas funcionalidades de bloqueio, típicas de um firewall, para notificar e bloquear eficazmente qualquer tipo de ação suspeita ou indevida.

C. O firewall do tipo Roteador de Barreira não examina cada pacote, em vez disso, compara o padrão de bits do pacote com um padrão sabidamente confiável.

D. Poder avaliar hipertextos criptografados, que, normalmente, não são analisados por firewalls tradicionais de rede, constitui uma vantagem do firewall de aplicação.

E. Um conjunto IDS/IPS instalado em um switch pode ser considerado do tipo HIDS/HIPS, dada a sua atuação na detecção e prevenção de intrusões com base no comportamento e no histórico do tráfego de dados do dispositivo de rede.

2. INFRAERO – FCC 2011 – Profissional Básico – Analista Superior III – Rede e Suporte

Em relação aos sistemas de proteção de rede,

A. um exemplo típico de tentativa suspeita que é detectada pelo HIDS é o login sem sucesso em aplicações que utilizam autenticação de rede. Nesse caso, HIDS informará ao administrador de rede que existe um usuário tentando utilizar uma aplicação que ele não tem permissão.

B. o IPS é uma ferramenta utilizada para monitorar o tráfego da rede, detectar e alertar sobre ataques e tentativas de acessos indevidos e, embora não bloqueie uma ação, tem a capacidade de verificar se esta ação é ou não uma ameaça para um segmento de rede.

C. a função dos stateful inspection firewalls é analisar o tráfego ao nível do IP e TCP/UDP, construindo tabelas de estado das ligações à Internet para prevenir os ataques do tipo spoofing, replaying, entre outros.

D. os Proxies atuam de acordo com informação de estado, sem considerar as regras de acesso estáticas, e possibilitam o uso de filtragem com base na informação de nível de pacote.

E. os appliances NAC compõem uma arquitetura mais elaborada, pois integram soluções de terceiros na infraestrutura de rede envolvendo switches next generation com suporte à tecnologia NAC.

3. UFPA– CEPS UFPA 2011 – Profissional Básico – Analista de TI - Suporte

Quanto às funções de um IDS e de um Firewall, é correto afirmar:

A. O firewall permite a filtragem de arquivos contendo vírus. O IDS permite a remoção de vírus.

B. O IDS permite o compartilhamento de arquivos. O firewall permite a filtragem de pacotes em uma rede de computadores.

C. O IDS permite a instalação de programas em um computador. O firewall permite a remoção de programas maliciosos em um computador.

D. O IDS é uma ferramenta que permite a detecção de intrusão em uma rede de computadores. O firewall permite a filtragem de pacotes em uma rede de computadores.

E. O firewall é um mecanismo que permite identificar atacantes que estejam invadindo a rede de computadores. O IDS possibilita remover vírus de computadores em rede.

4. TRT 19– FCC 2011 – Tecnico Judiário – Tecnologia da Informação

É INCORRETO afirmar que um firewall

A. de filtragem de pacotes pode encaminhar ou bloquear pacotes com base nas informações disponíveis nos cabeçalhos da camada de rede ou de transporte.

B. não pode ser utilizado para negar acesso a dado host ou serviço em uma organização.

C. proxy, faz a filtragem na camada de aplicação.

D. de filtragem de pacotes, usa uma tabela de filtragem para decidir quais pacotes devem ser descartados.

E. pode filtrar todos os pacotes que chegam destinados a determinado host ou serviço como HTTP.

5. Banco da Amazônia – CESPE 2010 – TI – Suporte Técnico

Quanto a conceitos relacionados a firewall, julgue os itens subseqüentes.

87. O firewall, recurso projetado para atuar na camada 3 do modelo OSI, é incapaz de analisar informações inerentes às camadas superiores desse modelo.

88. É importante que o sistema operacional da máquina na qual o firewall está sendo executado seja confiável e seguro para que ela não seja facilmente invadida e o firewall, comprometido.

89. Uma zona desmilitarizada (DMZ) é uma porção da rede onde encontram-se, geralmente, os servidores de acesso externo da organização, como por exemplo, WWW e FTP. A DMZ é criada com o intuito de isolar e proteger a rede interna da organização contra acessos externos. Nesse caso, o firewall deixa passar os acessos destinados à DMZ e bloqueia os acessos destinados à rede interna.

6. ABIN– CESPE 2010 – Agente Técnico de Inteligência – Tecnologia da Informação

Com relação à prevenção de intrusão, julgue os itens subseqüentes.

116 Em um sistema de detecção de intrusão de rede, a assinatura consiste em um padrão que é verificado no tráfego, com o objetivo de detectar certo tipo de ataque.

117 Em uma rede de comunicação, os sistemas de prevenção de intrusão fazem a coleta e análise dos dados originados em uma máquina que hospeda o serviço; após a coleta, esses dados podem ser analisados localmente ou enviados para uma máquina remota.

118 Os sistemas de prevenção de intrusão embasados em rede são incompatíveis com aqueles que têm base em estação, o que impossibilita a existência de sistemas híbridos.

7. ANA – ESAF 2009 – Analista Administrativo - Administração de redes e Segurança

No contexto de detecção de intrusos, a ausência de alerta quanto à ocorrência de um evento real representa

a. falso positivo
b. falso negativo.
c. inundação de alertas.
d. ação de sniffers.
e. ação de proxies.

8. BACEN– FCC 2006 – Analista – Área 1

A captura de pacotes da rede, buscando sinais de ataques externos, sem interferir no funcionamento ou desempenho dos *hosts, caracteriza um sistema de detecção de intrusão baseado em*

A. rede.
B. *host.*
C. localização.
D. conhecimento.
E. comportamento.

Gabarito

1.D

2.C

3.D

4.B

5.E, C, C

6.C, E, E

7.B

8.A