

Segurança Operacional

Ataques a Sistemas Computacionais

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

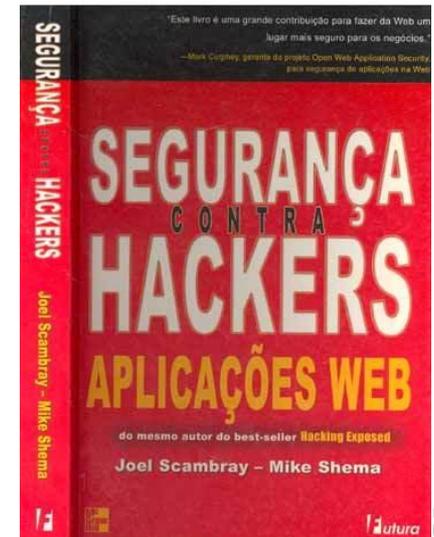
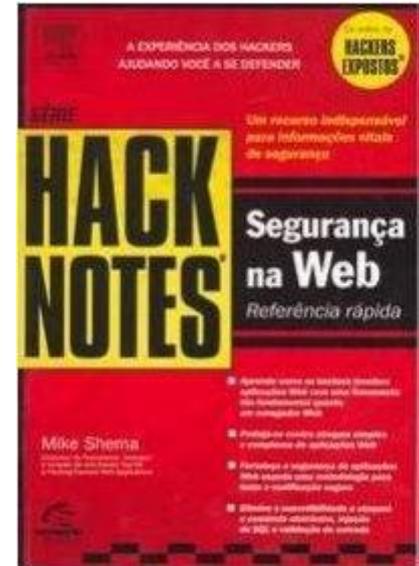
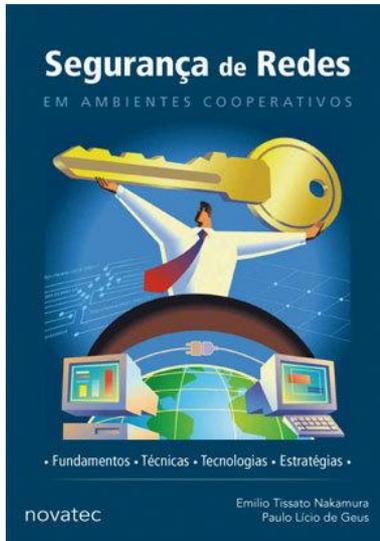
- p3r1t0f3d3r4l@yahoo.com.br



Escopo

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

Bibliografia



Segurança Operacional IV – Carga Horária

• 11 vídeo aulas (03h51m24s / 00h21m02s)

- Invasores
 - considerações iniciais
 - etapas de um ataque
- Anatomia de um ataque
 - Footprinting, varredura
 - Enumeração de vulnerabilidades, ataque, cobertura de rastros, manutenção do acesso
- Ataques aos S.Os
 - Reconstrução de memória, Buffer Overflow
- Ataques de negação de serviço
 - DoS, DDoS, PDoS
- Phishing, Spoofing, Evil Twin, DNS, MITM
- SQL Injection, XSS
- CSRF, Sequestro de sessões
- Primeira bateria de questões de aprendizagem
- Segunda bateria de questões de aprendizagem
- Terceira bateria de questões de aprendizagem



Segurança Operacional

Fracionando o ataque

Os Invasores

- Ativos
 - Querem alterar (ou forçar o vazamento)
- Passivos
 - Apenas ler o que não têm direito
- Principais motivações para ataques eletrônicos
 - Ganhos financeiros
 - Desafios pessoais
 - Autoafirmação perante grupos sociais
 - Vingança
 - Insatisfação profissional
 - Os principais atacantes são pessoas internas à organização ou com ela relacionados
 - Curiosidade



Níveis de Proteção

- No Security
 - Segurança não é importante
- Security Through Obscurity
 - Ninguém conhece como funciona o sistema
- Segurança de host
 - Proteção individual dos equipamentos
- Segurança de rede
 - Proteção ampla
 - Restrição de pontos de acesso
 - Elementos de segurança em redes
 - Segurança nas camadas OSI



Visibilidade da Segurança

- Dilema
- Somente se torna visível quando ocorrem problemas
- Alto custo
 - Produtos
 - Infraestrutura
 - Recursos humanos especializados
 - Atualização tecnológica



Mecanismos de segurança

- Específicos
 - Cifragem;
 - Assinatura digital;
 - Troca de informação de autenticação;
 - Preenchimento de tráfego;
 - Controle de roteamento;
 - Certificação digital.
- Pervasivos / Universais
 - Funcionalidade confiável;
 - Rótulo de segurança;
 - Detecção de evento;
 - Registros de auditoria;
 - Recuperação de segurança.
- Educação
 - Treinamento
 - Consciência
 - Gestão
- OBS: Quanto mais completo for o arcabouço tecnológico na proteção à informação nos ambientes computacionais, melhores são as chances de êxito



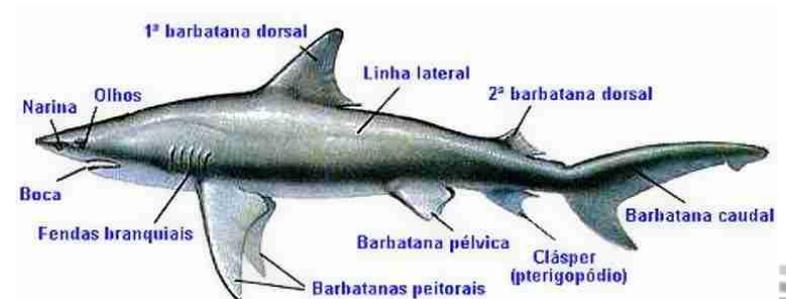
Considerações sobre Segurança

- Entender a natureza dos ataques é fundamental
- Novas tecnologias trazem novas vulnerabilidades
- Novas formas de ataques são criadas
- Aumento da conectividade = aumento nas possibilidades de ataques
- Existência de ataques direcionados e oportunistas
- A defesa é mais complexa do que um ataque
- Aumento dos crimes digitais



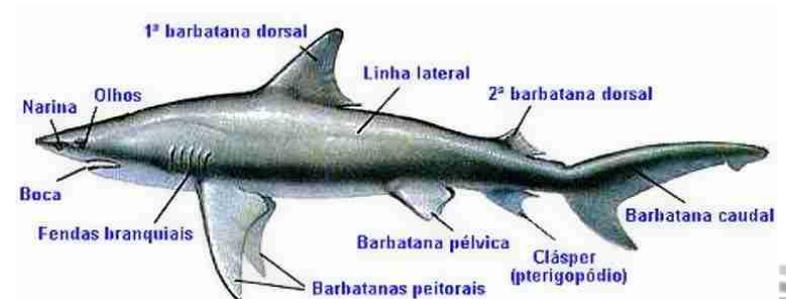
Anatomia de um Ataque

1. Footprinting
2. Varreduras
3. Enumeração de vulnerabilidades
4. Ataque
5. Cobertura dos rastros
6. Manutenção do acesso



Anatomia de um Ataque

1. Footprinting
2. Varreduras
3. Enumeração de vulnerabilidades
4. Ataque
5. Cobertura dos rastros
6. Manutenção do acesso



Footprinting

- Antes de iniciar o ataque, algumas etapas são necessárias para conhecer mais sobre o alvo
- É o primeiro passo para uma intrusão
- Propósito: descobrir informações úteis, como
 - Emails dos usuários
 - Informações de rede
 - Links importantes
- O que buscar
 - Informações sobre domínio
 - Jornais on-line
 - etc



Footprinting

- Levantamento de informações do alvo
 - Planejamento de um ataque
 - Dumpster Diving ou Thrashing
 - Engenharia Social
 - Explora as fraquezas humanas e sociais
 - Ataca o elo mais fraco que é o ser humano
 - Análise de documentos em mesas e disfarces



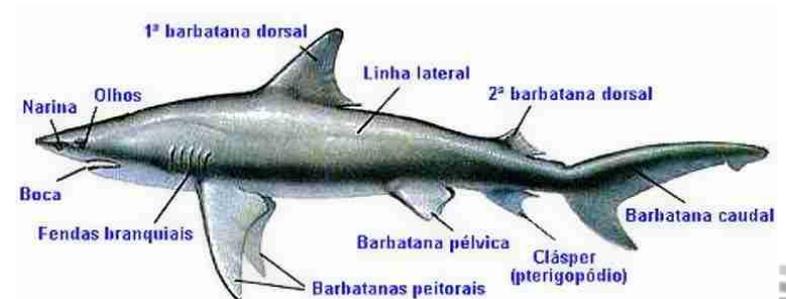
Procedendo o Footprinting

- Manualmente
- Programas
- Passos
 - Determinar o Escopo
 - Informação Publica Disponível
 - WHOIS
 - Interrogação de DNS
 - Reconhecimento da topologia da rede
- Packet Sniffing / Passive Eavesdropping
- Firewalking
- IPSpoofing



Anatomia de um Ataque

1. Footprinting
2. **Varreduras**
3. Enumeração de vulnerabilidades
4. Ataque
5. Cobertura dos rastros
6. Manutenção do acesso



Procedendo a Varredura

- Intuito: descobrir computadores ativos em uma determinada rede e quais portas esses sistemas estão rodando
 - Scanners de portas
 - Enumerar serviços disponíveis e versões
- Como descobrir computadores ativos?
 - ICMP echo (8) e echo reply (0)
- Descobrimo portas abertas
 - Varreduras em serviços SNMP, SMTP, SMB, RPC
 - Scanners de Vulnerabilidades
 - Softwares
 - NMAP, Strobe, NetCat, SuperScan



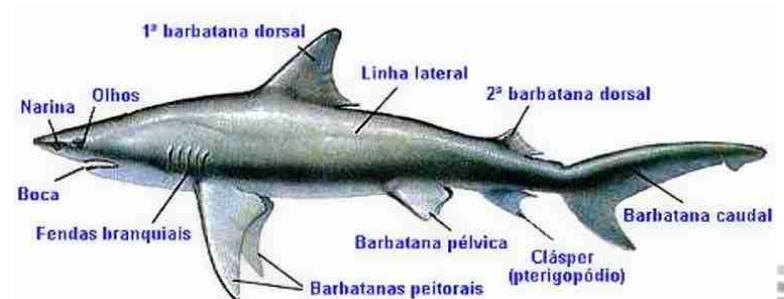
Procedendo a Varredura

- Detecção de SO
 - FIN
 - ISN
 - DF Bit
 - TCP Window Size
 - ACK
 - TTL
- Como driblar o IDS
 - Random port scan
 - Slow Scan
 - Fragmentation Scanning
 - Decoy
 - Coordinate Scans



Anatomia de um Ataque

1. Footprinting
2. Varreduras
- 3. Enumeração de vulnerabilidades**
4. Ataque
5. Cobertura dos rastros
6. Manutenção do acesso



Enumeração de Vulnerabilidades

- Nessa etapa já temos hosts e portas
- Quais serviços e recursos estão rodando?
 - É aqui que enumeramos os recursos para o passo seguinte
- Após o port scanning, as vulnerabilidades específicas para cada serviço oferecido serão procuradas
- O port Scanning economiza esforço nesta fase
- Podem existir falsos positivos e falsos negativos



Enumeração de Vulnerabilidades

- Descuberta do SO / Fingerprinting
 - Não confundir com footprinting
 - Invasor tem por objetivo determinar QUAL S.O. do host alvo
 - Exploração da pilha tcp/ip do alvo
 - Flags
 - A sutileza na manipulação e flags de datagramas
 - TTL em respostas ICMP
 - Presa fácil para IDS
 - TCP timestamp indica a quanto tempo o sistema está no ar
- Fingerprint scanners
 - NMAP, NSAT, BLASTER, PHOBIA, NESSUS, QUESO



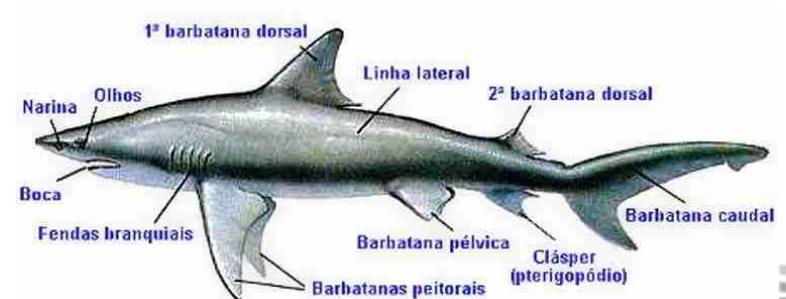
Enumeração de Vulnerabilidades

- Enumeração dos serviços
 - Leitura de banners
 - Consiste em conectar-se a porta aberta do sistema e ler o banner do serviço
- Enumeração de usuários
 - Tentativa de enumerar os usuários do sistema
 - Exemplo: telnet www.viasky.com.br 25
 - VRFY fulano
 - Enviar emails para vários emails da empresa
- Enumeração de ferramentas para um ataque - Uso de exploits



Anatomia de um Ataque

1. Footprinting
2. Varreduras
3. Enumeração de vulnerabilidades
- 4. Ataque**
5. Cobertura dos rastros
6. Manutenção do acesso



Execução do Ataque

- Ataques Lógicos
 - Instalação de backdoor
 - Instalar Trojans
 - Instalar Logcleans
 - Instalar Sniffers
 - Apagamento de logs
 - Ataques DoS, DDoS, DRDoS
 - Monitoramento da rede
 - Penetração no sistema
 - Inserção de códigos maliciosos ou informações falsas
 - Flooding de pacotes para prejudicar a disponibilidade



Execução do Ataque

- Ataque físico
 - Aos equipamentos, softwares e dispositivos de armazenamento
 - Ataque é realizado diretamente sobre o sistema
 - Não necessita de técnicas de ataques remotos
 - Combatido através do controle de acesso às áreas restritas
 - Políticas de segurança
 - Uso de sniffers ou Keyloggers



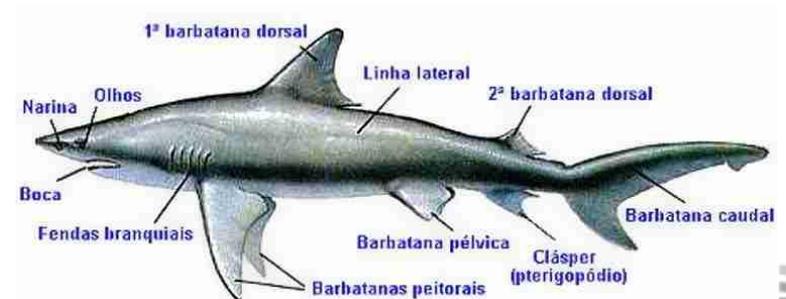
Execução do Ataque

- Resultados de um ataque bem sucedido
 - Monitoramento não autorizado
 - Vazamento de info sensíveis
 - Modificação de servidores e bases de dados
 - Negação ou corrupção de serviços
 - Fraude ou perda financeira
 - Imagem ou reputação prejudicada
 - Trabalho extra para recuperação dos recursos
 - Perda de negócios, clientes e oportunidades



Anatomia de um Ataque

1. Footprinting
2. Varreduras
3. Enumeração de vulnerabilidades
4. Ataque
5. **Cobertura dos rastros**
6. Manutenção do acesso



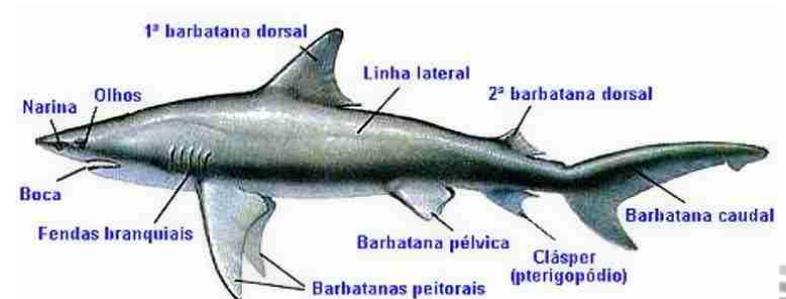
Cobertura dos Rastros

- Apagamento de logs
- formatação de sistemas
- Troca de arquivos de sistema
- Por isso é Importante o uso de um IDS



Anatomia de um Ataque

1. Footprinting
2. Varreduras
3. Enumeração de vulnerabilidades
4. Ataque
5. Cobertura dos rastros
6. **Manutenção do acesso**



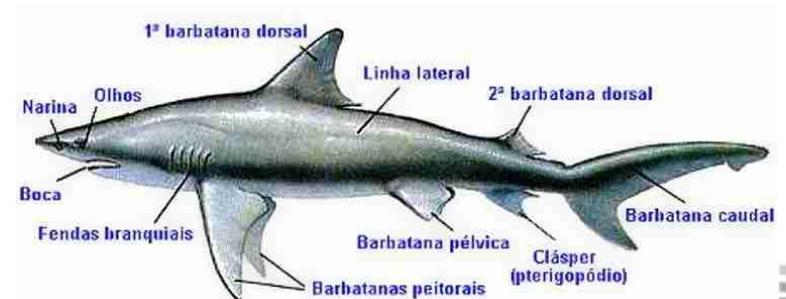
Manutenção do Acesso

- Backdoors
- “É preciso fazer valer o esforço anterior”
- OBS: Ataques são sempre intencionais, tanto ativa quanto passivamente. Ameaças podem ser acidentais ou intencionais, podendo ser ativas ou passivas



Anatomia de um Ataque

1. Footprinting
2. Varreduras
3. Enumeração de vulnerabilidades
4. Ataque
5. Cobertura dos rastros
6. Manutenção do acesso



Ataques aos S.Os

- Bases para os Ataques
 - Elevação de Privilégios
 - Execução remota de código arbitrário
 - Acesso a arquivos
 - Negação de Serviço



Ataques aos S.Os

- Reconstrução de memória
 - A informação está na memória do computador
 - Alocação de memória por um programa
 - O SO marca o espaço de memória como indisponível para outros programas
 - Ninguém pode utilizá-la ou examiná-la.
 - Quando o programa encerra, o SO libera esse espaço
 - Mas não o sobrescreve
 - A informação ficará lá até ser sobrescrita



Ataques aos S.Os

- Buffer Overflow
- Buffer
 - Região temporária da memória
 - São guardados dados para processamento posterior
 - Também usados para armazenar dados quando a taxa recebida > taxa para processamento
 - Analogia: fila do banco
- Overflow
 - Transbordamento
 - Analogia às cheias do rio
 - Chuvas fazem rios transbordarem para locais onde não deveria estar naturalmente



Ataques aos S.Os

- O BO consiste em armazenar, em um buffer de tamanho fixo, dados maiores que o seu tamanho.
 - técnica de tentar armazenar mais dados do que a memória suporta, causando erros e possibilitando a entrada do invasor
 - Geralmente, o atacante consegue o domínio do programa atacado e privilégio de administrador na máquina hospedeira
 - Se o programa em questão tiver privilégios no sistema, podendo realizar ações como administrador ou superusuário, ele irá começar a executar instruções que não estão programadas



A	A	A	A	A	A	A	A	B	B
0	0	0	0	0	0	0	0	0	9

A	A	A	A	A	A	A	A	B	B
'e'	'x'	'c'	'e'	's'	's'	'i'	'v'	'o'	'\0'



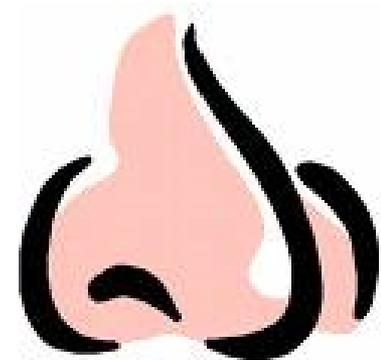
Ataques aos S.Os

- Conseqüências do B.O.
 - Funcionamento errôneo do programa
 - Valor da variável B corrompido
 - Travamento do programa
 - Vulnerabilidade a exploits



Ataques: Sniffing

- São em geral agentes passivos
 - Captura de informações de rede por meio de um software de escuta de rede
- Ataque à CONFIDENCIALIDADE
- Formas
 - Passiva
 - Meios não comutados (hub e barramento)
 - Difícil de ser detectado
 - Ativa
 - Dispositivos comutados
 - Mais fácil detecção
- Raramente interferem no funcionamento da rede
- Um sniffer ideal não injeta pacotes na rede, não responde a qualquer tipo de requisição e não precisa sequer ter um endereço da rede
- Na prática, a principal característica visível de um sniffer é uma interface em modo promíscuo sem o aval do administrador da rede



Ataques: Negação de Serviço

- Os ataques de negação de serviço fazem com que os recursos sejam explorados de maneira agressiva, de modo que usuários legítimos ficam impossibilitados de utilizá-los
- A disponibilidade de um recurso é intencionalmente bloqueada ou prejudicada
 - Worm gera a negação de serviço
- Atacante envia vários pacotes ou requisições de serviço de uma vez, objetivando sobrecarregar o servidor ou sobrecarga dos links
- Podem ser
 - Locais
 - Remotos



Ataques: Negação de Serviço

- Locais

- O atacante possui acesso local à máquina
- Usuário legítimo
- Ladrão de senha
- O atacante deve executar comandos locais na máquina

- Objetivos

- Degradação de Sistema
- Destruição de arquivos (Tornar o recurso inutilizável)
- Esgotamento de espaço em memória
- Esgotamento de espaço em disco
- Esgotamento de I-nodes



Ataques: Negação de Serviço

- Remotos

- O atacante não precisa estar logado na máquina e nem executar comandos locais nela
- Remotamente, de alguma forma, ele derruba o serviço

- Objetivos

- Degradação de Sistema
- Destruição de arquivos (Tornar o recurso inutilizável)
- Esgotamento de espaço em memória
- Esgotamento de espaço em disco
- Esgotamento de I-nodes



Ataques: Negação de Serviço

- Ambientes para DoS
- Programas mal elaborados com bugs
 - Pacotes indevidamente construídos derrubam serviços
 - Pilha TCP/IP antigas mal implementadas
 - Pilhas TCP/IP bem programadas deveriam descartar certos pacotes
 - Implementações antigas se perdiam e caíam
- DOS baseados no comportamento correto do TCP/IP
 - Não existem correções para esse tipo de ataque
 - Falhas existem e continuarão existindo
 - Só resta nos defendermos deles (SYN FLOOD por exemplo)



Ataques: Negação de Serviço

- Espécies de DoS
- DoS
 - Denial of Service - Negação de Serviço
 - O atacante utiliza UM computador para tirar de operação um serviço ou computador(es) conectado(s) à Internet
 - O ataque parte de um único ponto
- DDoS
 - Distributed Denial of Service
 - Se caracteriza também por não ser fácil de identificar o atacante que tem o "domínio do fato"
 - Ataque distribuído
 - Os ataques não são baseados no uso de um único computador, mas centenas ou milhares para lançar coordenadamente o ataque
 - Procuram ocupar toda a banda disponível para o acesso a um computador ou rede causando grande lentidão ou até mesmo indisponibilizando qualquer comunicação com este computador ou rede



Ataques: Negação de Serviço

- PDoS
 - Phlashing/permanent Denial of Service
 - Voltado para dispositivos controlados por firmware
 - Dano permanente no firmware, forçando sua substituição ou reinstalação de hardware
 - Ex: Impressoras, roteadores, etc...



Ataques: Phishing



- Também conhecido como *phishing scam*
- FRAUDE que se dá através do envio de mensagem não solicitadas, passando-se por comunicação de uma instituição conhecida e que procura induzir o acesso a páginas fraudulentas (falsificadas), projetadas para FURTAR DADOS PESSOAIS E FINANCEIROS de usuários.
- Uso de spywares
- Mensagens induzindo instalação de códigos
- Ocorre por email, mensagem instantânea, SMS, etc
- Muitas mensagens de phishing induzem a vítima a uma ação imediata, fazendo-a agir primeiro e pensar depois
 - Preenchimento de formulários

Ataques: Spoofing

- O endereço real do atacante é alterado, evitando assim que ele seja encontrado
- É uma espécie de impostura da identidade do remetente
- Modificação de campos de identificação, se passando por outro host
- Não é um ataque propriamente dito, mas sim parte dele*
- Viabiliza o cache poisoning



Ataques: Spoofing

- Modalidades

- ARP Spoofing

- MAC verdadeiro + IP falso

- MAC Duplication

- Alternativa ao ARP Spoofing
 - Clonagem de endereço MAC

- IP Spoofing

- DNS Spoofing



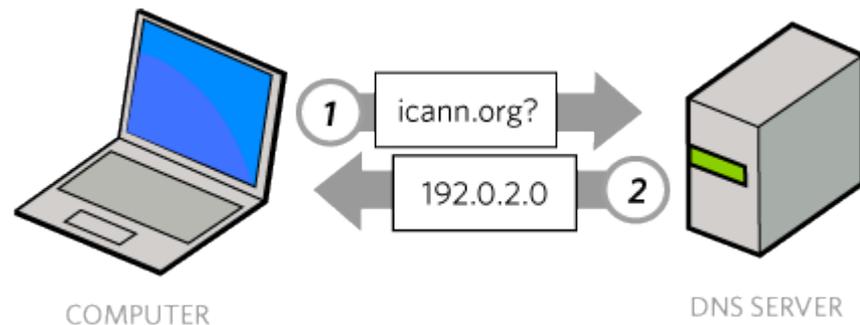
Ataques: Evil Twin

- Ataque a rede sem fio
- Criação de access point igual ao verdadeiro
- Repasse do tráfego ao atacante



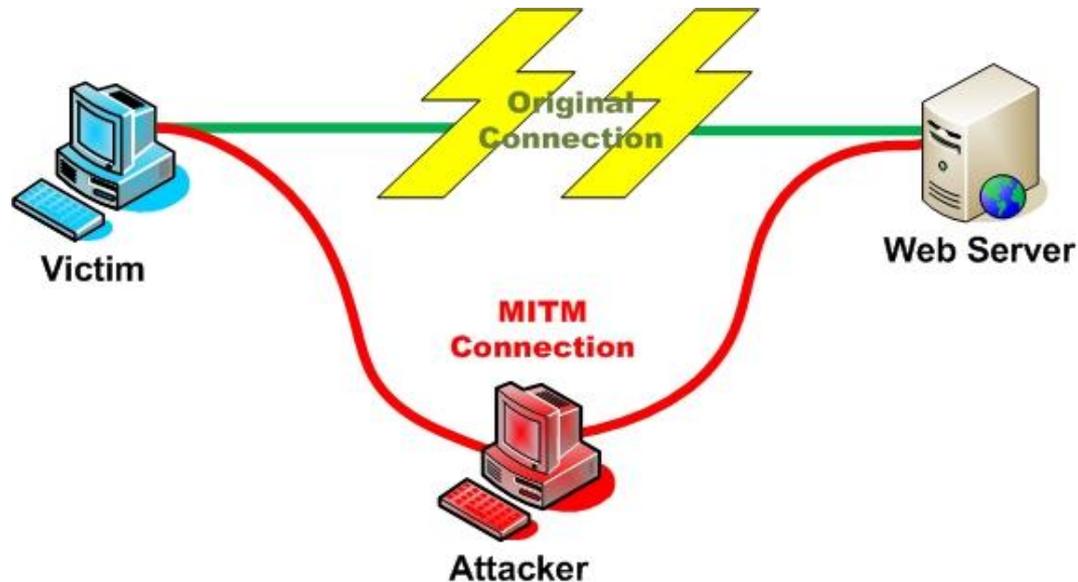
Ataques: ao DNS

- Roubo de conexão do usuário no servidor DNS
 - Capturar informações na rede para fazer login no DNS
- Referrals
 - Atacante usa escuta de rede para capturar requisições de um servidor para o seu servidor raiz e se passa por ele, respondendo com informações falsas
- Cache Poisoning
 - Atacante se passa pelo servidor DNS raiz e envia pacotes ao servidor DNS mudando endereços de sites conhecidos
 - Chama-se “envenenamento” porque assim que a “cache” de endereços obtém o primeiro endereço falso pode passar a pedir outros endereços a esse endereço falso, falsificando todo o conteúdo



Ataques: MITM

- Man-in-the-middle
 - Atacante atua como intermediário
 - Nenhuma das partes toma conhecimento
 - Além de interceptar, pode modificar as informações e permanecer conectado após a saída da vítima



Ataques no nível de aplicação

- **SQL Injection**

- Algumas aplicações não validam as entradas de usuários permitindo que hackers executem comandos diretamente no banco de dados de uma aplicação
- Manipulação de uma instrução SQL através das variáveis que compõem os parâmetros recebidos por um script
- Este tipo de ataque consiste em passar parâmetros a mais via barra de navegação do navegador



Ataques no nível de aplicação

- **SQL Injection**

- explora a vulnerabilidade de segurança da camada de banco de dados de uma aplicação
- inserindo instruções não esperadas pelo banco de dados
- Aplicações sem validação de entrada



Ataques no nível de aplicação

- **SQL Injection**
- Defesas
 - uso de views, stored procedures e cursors pode evitar ataques de SQL injection
 - NUNCA montar expressões SQL "no braço" dentro de seu código. sempre usar Prepared Statements
 - Ou seja, criar a query, que pode ser de qualquer tipo, deixando os valores das variáveis indefinidos



Ataques no nível de aplicação

- **Instrução Original:**
 - SELECT id, nome, sobrenome FROM aprovados
- **Instrução refinada**
 - SELECT id, nome, sobrenome FROM aprovados WHERE nome = 'José' AND sobrenome = 'Silva';
 - Se a aplicação não fizer o tratamento apropriado do conteúdo inserido pelo usuário, o mesmo pode fazer o uso acidental do caractere de aspas simples
- **Instrução com uso malicioso da aspa simples**
 - SELECT id, nome, sobrenome FROM aprovados WHERE nome = 'jo'sé' AND sobrenome = 'silva';
 - SELECT id, nome, sobrenome FROM aprovados WHERE nome = 'jo'; DROP TABLE aprovados; --' AND sobrenome = 'silva';



Ataques no nível de aplicação

- **XSS (Cross Site Scripting)**

- Ataque baseado em induzir o navegador web do usuário a executar um script malicioso dentro do contexto de um site confiável
- A exploração bem sucedida deste ataque permite ao hacker embutir um código malicioso (na forma de Javascript ou VBScript) em campos de entrada, os quais são inseridos de volta para a resposta do servidor
- Isto permite ao hacker a execução de um código arbitrário em um usuário desatento que tenha acesso permitido ao site escolhido como vítima
- Precisamos de códigos web que executem localmente
 - Javascript, VB Script
- javascript:document.cookie
 - Coleta de informações nos cookies
 - Logins, senhas, etc
 - Roubo de sessão



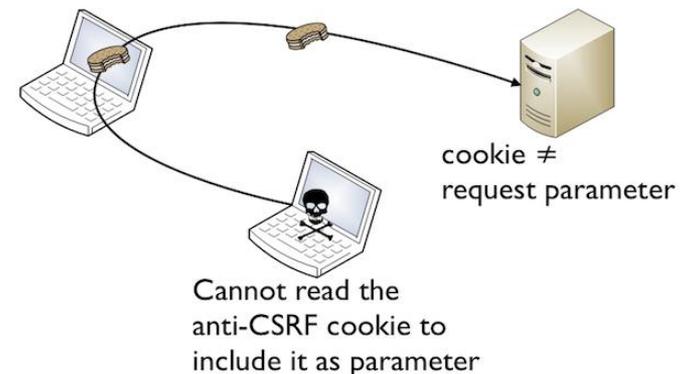
Ataques no nível de aplicação

- **XSS/CSS (Cross Site Scripting)**
- Persistente
 - Fica sempre no servidor
- Não persistente
 - Alterações somente no conteúdo da requisição
- Independentemente da persistência, a execução é sempre no cliente e para enganar o cliente, devido a uma falha no servidor



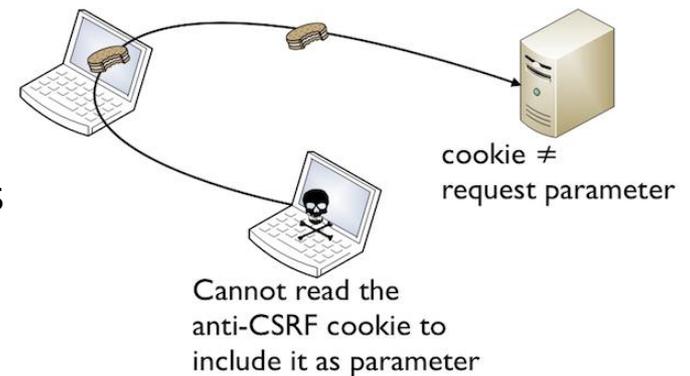
Ataques no nível de aplicação

- **CSRF (Cross Site Scripting Request Forgery)**
 - Consiste em inserir requisições em uma sessão já aberta pelo usuário, explorando a confiança que um site tem do navegador
 - Atua após a obtenção do cookie gerado pela aplicação após a autenticação
 - Por meio do cookie, o servidor acredita estar se comunicando com o usuário real e autenticado
 - Inibido por captcha
 - Somente o ser humano teria condições de digitá-lo



Ataques no nível de aplicação

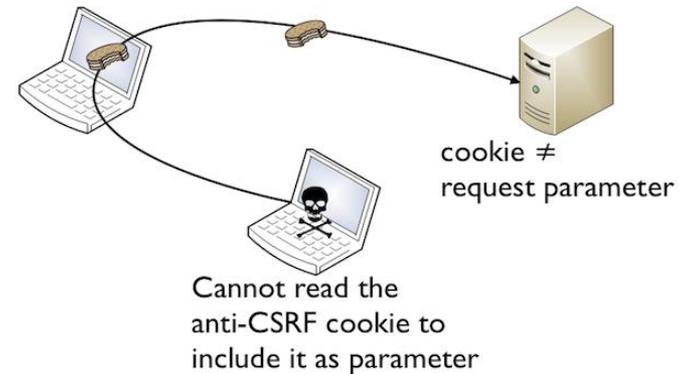
- **CSRF (Cross Site Scripting Request Forgery)**
- **Processo Básico**
 - O usuário se autentica em uma aplicação web alvo.
 - O usuário utiliza a mesma instância de browser para navegar em um site mal intencionado.
 - Este site manipula o browser para que seja feita uma requisição à aplicação alvo
 - Como há uma sessão autenticada aberta para o usuário, a aplicação alvo executa a operação conforme a requisição recebida.
- Este ataque é extremamente difícil de ser detectado, dado que um identificador de sessão correto e válido será incluído na requisição recebida pela aplicação e a requisição partirá do mesmo browser e endereço IP das requisições legítimas. A aplicação web não sabe como separar a requisição correspondente ao ataque das requisições legítimas



Ataques no nível de aplicação

- **XSS x CSRF**

- XSS tira proveito da confiança que o usuário tem no site
- CSRF tira proveito da confiança que o site tem no usuário



Ataques: Sequestro de Conexões

- Conexões TCP são definidas por quatro informações essenciais: endereço IP de origem, porta TCP de origem, endereço IP do destino, porta TCP do destino
- Todo byte enviado por um host é identificado com um número de sequencia que é conhecido pelo receptor
- O número de sequencia do primeiro byte é definido durante a abertura da conexão e é diferente para cada uma delas
- Geralmente o atacante descobre um número de sequencia válido a partir da observação (sniffing) de pacotes, descobrindo assim a função matemática utilizada para calcular os números de sequencias
- pode conseguir a sessão do usuário explorando Cross Site Scripting ou tendo acesso físico à máquina do usuário legítimo



Bateria de questões de aprendizagem 1

Segurança Operacional – Módulo IV
Ataques a Sistemas Computacionais

TRF 1 – FCC 2011 – Técnico Judiciário – Operador de Computador

1. Um tipo de ataque que envolve personagens, tais como, Master (máquina que recebe os parâmetros para o ataque e comanda os agentes) e Agentes (máquinas que efetivamente concretizam o ataque contra uma ou mais vítimas), que inundam os servidores alvo com um volume enorme de pacotes é denominado
- A. Flooding.
 - B. DDoS.
 - C. Buffer Overflow.
 - D. Spoofing.
 - E. Sniffers.

TRT 22– FCC 2010 – Técnico Judiciário – TI

2. É um aplicativo usado tanto pelas áreas de segurança, para análise de vulnerabilidades, quanto por pessoas mal intencionadas, para identificarem portas abertas e planejarem invasões:

- A. Denial of Service.
- B. Port Scan.
- C. Buffer Overflow.
- D. DNS Spoofing.
- E. Brute Force Attack.

3. Um conjunto de computadores está sendo utilizado para tirar de operação um serviço de determinado órgão público. Essa situação configura o ataque do tipo
- A. Replay.
 - B. SQL Injection.
 - C. XSS.
 - D. Buffer Overflow.
 - E. DDoS.

TRT 20 – FCC 2010 - Analista Judiciário - TI

4. Um ataque do gênero Denial of Service (DoS) tem como principal objetivo sobrecarregar o computador alvo até ele parar de responder ou, até mesmo, desligar. Enquadram-se nesse gênero os ataques

I. Buffer Overflow.

II. PING of Death.

III. SYN Flooding.

IV. Smurf.

Está correto o que se afirma em

- A. I, II e III, apenas.
- B. I, III e IV, apenas.
- C. II, III e IV, apenas.
- D. III e IV, apenas.
- E. I, II, III e IV.

AL / SP – FCC 2010 – Agente Técnico Legislativo – Seg Redes

5. Durante aproximadamente 25 minutos na tarde do dia 25 de junho de 2009, usuários do Google News receberam como resposta a suas buscas uma página cuja mensagem dizia que a busca parecia advir de alguma espécie de vírus e que, antes de prosseguir, deveria ser digitado o texto exibido numa imagem (captcha). O que aconteceu foi que o sistema de segurança do Google detectou um repentino e explosivo aumento nas buscas por Michael Jackson, procedentes de diferentes origens, e interpretou este fenômeno como um "ataque".

O tipo de ataque contra o qual o sistema de segurança do Google reagiu automaticamente é conhecido como

- A. port scanning.
- B. code injection.
- C. buffer overflow.
- D. cookie hijacking.
- E. flooding.

BACEN – CESGRANRIO 2010 – Analista Área 1

6. Analise o fragmento de código, executado no servidor, de uma aplicação WEB.

```
protected void btnAddCompany_Click(object sender, EventArgs e)
{
    string connStr =
        "Server=(local);Database=Production;Integrated Security=SSPI";

    string cmdStr =
        "insert into Companies (CompanyName, Phone) values ('" +
        txtCompanyName.Text + "\", '\" + txtPhone.Text + \"')";

    using (SqlConnection conn = new SqlConnection(connStr))
        using (SqlCommand cmd = new SqlCommand(cmdStr, conn))
            {
                conn.Open();
                cmd.ExecuteNonQuery();
            }
}
```

Considerando-se que o fragmento acima lê dados de formulários preenchidos por usuários, o código é vulnerável ao ataque de

A. buffer overflow, já que o tamanho

da entrada não é verificado no objeto connStr.

B. buffer overflow, mesmo que o método em questão esteja declarado como protegido.

C. cross site scripting, pois não protege contra injeção de código javascript em cookies.

D. sql injection, pois permite que o objeto cmdStr seja montado de forma maliciosa.

E. sql injection, pois permite que o banco de dados seja especificado por parâmetros.

7. Quanto à segurança da informação, é correto afirmar:

- A. Buffer Overflow é um ataque que pode ser realizado para sobrecarregar o poder de resposta de um servidor em um sistema de informação.
- B. Vírus de macro é um programa malicioso que vasculha um computador secretamente capturando e gravando todas as digitações, acessos aos websites visitados, quando acessados a partir de arquivos com extensão .doc.
- C. Inutilizar, mesmo que momentaneamente, um sistema de informação, incapacitando seu servidor de responder às requisições feitas pelos clientes, é o objetivo do ataque DoS (Denial of Service).
- D. Exigir identificação dos remetentes das mensagens que chegam, bem como autenticar as assinaturas digitais das mensagens de correio a serem enviadas, é tarefa que pode ser realizada por um firewall.
- E. Dominar o sistema do usuário para ser manipulado por uma entidade externa é o objetivo do vírus Spyware.

8. Acerca dos dispositivos e mecanismos de segurança de redes e sistemas, julgue os itens seguintes.

[74] Buffer overflows são explorados unicamente via ataque proveniente da rede.

[75] SQL injection normalmente é evitado apenas pela atuação no front end da aplicação

9. Uma máquina isolada devido a um ataque DNS (Domain Name System) representa

- A. ação de spywares.
- B. negação de serviço.
- C. varredura de portas.
- D. ação de um vírus.
- E. falsificação DNS.

PC/PE – IPAD 2006 – Perito Criminal

10. Sobre os principais tipos de ataques utilizados pelos hackers, considere:

1. Buffer overflow, SQL injection e cross-site scripting são técnicas de ataque que se utilizam dos campos de entrada de dados nos sites ou aplicações Web.
2. Numa rede protegida por um firewall apenas com filtragem de pacotes a técnica de IP spoofing pode ser eficaz na tentativa de burlar a segurança.
3. Numa rede sem fio, onde o access point utiliza como única proteção uma ACL (access control list) por MAC Address, a técnica de MAC spoofing pode ser eficaz na tentativa de invasão.
4. Engenharia social é uma técnica de proteção utilizada pelos administradores de segurança para educar os usuários contra a possível tentativa de hackers obterem informações de forma espontânea.

Podemos afirmar que está (ão) correta(s) as afirmativas:

- A. 1, 2 e 3.
- B. 1, 2 e 4.
- C. 2 e 4.
- D. 1 e 2.
- E. 2, apenas.

Gabarito

1. B

2. B

3. E

4. E

5. E

6. D

7. C

8. E, E

9. B

10.A

Bateria de questões de aprendizagem 2

Segurança Operacional – Módulo IV
Ataques a Sistemas Computacionais

DATAPREV – CESPE 2006 – Analista de TI - Redes

1. No referente a segurança de rede e controle de acesso, julgue os itens que se seguem.

[66] O MAC flooding pode ser eficazmente evitado por meio da filtragem baseada em endereço físico.

[67] A restrição na capacidade de aprendizado de endereços nas portas de um switch é suficiente para evitar o ARP spoofing.

[68] Um roteador com filtros de pacotes ativos é eficaz para deter ataques de buffer overflow.

[69] Ataques ao STP (spanning tree protocol - IEEE 802.1D) podem potencializar ataques como o do MAC flooding e o do ARP spoofing.

[70] O uso de duplos tags pode levar uma VLAN a acessar outra indevidamente.

2. O perfil completo de segurança de uma organização, criado por invasores, é
- A. uma instalação de porta dos fundos.
 - B. uma varredura.
 - C. uma penetração.
 - D. uma enumeração.
 - E. um *footprinting*.

PRODERJ– FEC 2002 – Analista

3. Sobre segurança de redes de computadores, marque V [Verdadeira] ou F [Falsa] nas afirmativas abaixo:
- () Antes de realizar um ataque bem sucedido a uma rede de computadores, o invasor precisa executar três passos fundamentais: footprinting, que é a coleta de informações sobre a segurança da rede; a varredura, que determina quais são os sistemas que poderão ser atingidos; e a enumeração, que é a extração de contas válidas ou recursos compartilhados mal protegidos.
 - () A varredura de portas é usada para enviar pacotes para um sistema alvo, de forma a obter uma resposta e identificar se o sistema está ativo ou não. A varredura ping é o processo que determina quais serviços estão em execução ou no estado de escuta, permitindo que o sistema operacional e os aplicativos em uso sejam descobertos pelo atacante.
 - () Os firewalls de pacotes de filtragem utilizam as Listas de Controle de Acesso (ACLs - Access Control Lists) ou regras para determinar se o tráfego está autorizado a passar do ambiente externo para o interior da rede ou do interior da rede para o ambiente externo.
 - () O tunelamento ICMP é a tecnologia que permite o empacotamento de dados reais em um cabeçalho ICMP. Os roteadores e firewalls que fazem uso desta técnica estão mais protegidos dos ataques UDP. A opção com as letras na ordem correta é:
- A. V V V F;
 - B. V F F F;
 - C. V F V F;
 - D. F F V V;
 - E. F F F V.

TJ-AC – CESPE 2002 – Analista de Sistemas

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

- Os ataques de negação de serviço a um determinado alvo caracterizam-se pela exaustão de seus recursos computacionais e(ou) pelo esgotamento da capacidade de seus canais de comunicações. Por exemplo, o smurfing combina o spoofing com os broadcasts direcionados, podendo ser evitados desabilitando- se o mapeamento dos broadcasts de camada 3 para camada 2 no roteador. Já os ataques DDoS aliam técnicas de sistemas distribuídos ao ataque de negação de serviço; em algumas implementações, um nó-mestre controla nós-escravos, por meio de um aplicativo cliente- servidor com base no ICMP, enquanto os escravos realizam flooding de UDP e TCP SYN contra o alvo. Contudo, a maioria dos serviços em rede está imune a ataques de negação de serviço.
- Os buffer overflows exploram deficiências de programas que utilizam linguagens de programação fracamente tipificadas. Porém, firewalls e IDS proveem defesa adequada a ataques de buffer overflow e constituem soluções eficientes que não impactam os serviços de uma rede. Em particular, os firewalls têm sua melhor implementação em kernels modificados de sistemas operacionais de uso geral, dado o melhor desempenho destes em aplicações de tempo real, aliado a interfaces gráficas de fácil utilização.
- Um IDS conectado a um switch opera adequadamente quando configurado com espelhamento de porta ou em modo debug.
- Um IDS é capaz de detectar ataques de buffer overflow ao utilizar uma assinatura contendo sequencias de bytes correspondentes ao código de NO-OP da arquitetura que se deseja proteger.
- A sobre-escrita de um fragmento de dados em uma parte do fragmento inicial já recebido provoca negação de serviço em sistemas que tenham bugs na implementação da remontagem de fragmentos de informação.

Gabarito

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

Bateria de questões de aprendizagem 3

Segurança Operacional – Módulo IV
Ataques a Sistemas Computacionais

DPF – CESPE 2002 – Perito Criminal Federal

1. Com relação aos comprometimentos de máquinas originados a partir da exploração de uma sobrecarga de *buffer (buffer overflow)*, julgue os itens abaixo.
 - A ocorrência de comprometimento está restrita aos sistemas de código aberto.
 - O comprometimento independe da linguagem utilizada na implementação do programa específico que tem seu *buffer sobrecarregado*.
 - Pode-se evitar o *buffer overflow* utilizando-se *firewalls na proteção das máquinas*.
 - O *buffer overflow* consiste em injetar uma cadeia de caracteres longa o suficiente para ocupar totalmente o *buffer atacado*, seguindo-se uma chamada de sistema que executa o código malicioso.
 - O *buffer overflow* genérico utiliza, na sua implementação, o fato de que, na cadeia de caracteres do *buffer*, só podem ocorrer caracteres distintos do delimitador de cadeias, sendo, então, normalmente utilizado no preenchimento do *buffer* o código correspondente ao *NOOP* do sistema-alvo, facilitando a estimação do endereço de retorno da chamada de sistema.

MPE AP – FCC 2012 – Analista Ministerial - TI

2. É um tipo específico de phishing que envolve o redirecionamento da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS (Domain Name System). Neste caso, quando o usuário tenta acessar um site legítimo, o navegador Web é redirecionado, de forma transparente, para uma página falsa.

O tipo de phishing citado no texto é conhecido como

- A. advance fee fraud.
- B. hoax.
- C. pharming.
- D. defacement.
- E. source spoofing.

INFRAERO – FCC 2011 – Analista Superior III – Rede e Suporte

3. No contexto das ameaças e vulnerabilidades de rede, considere:

- I. Cross-site Scripting (XSS) é uma vulnerabilidade em sites web que permite que um indivíduo malicioso execute código Javascript no site alvo no contexto do usuário e, dessa forma, poder roubar credenciais de acesso ou até executar comandos em nome do administrador.
- II. Phishing é uma fraude virtual que chega por e-mail com a tentativa de convencer o usuário de que ele precisa preencher um formulário com seus dados ou clicar em um determinado link para baixar um arquivo, que na verdade é um vírus, e o site, se acessado, roubará todos os dados digitados.
- III. IP Spoof permite ataques como o envenenamento de cache do DNS. Na maioria das vezes, ele é realizado via UDP, já que o protocolo TCP usa a proteção handshake.
- IV. No ataque SYN flooding, o atacante inicia muitas conexões TCP em um curto período de tempo, atacando o three-way handshake e passa a enviar SYNs e não responder aos SYN-ACK, deixando em aberto os estabelecimentos de conexão até ocupar todos os buffers de conexão no servidor.

Está correto o que consta em

- A. I, II e III, apenas.
- B. I, II e IV, apenas.
- C. I, III e IV, apenas.
- D. II, III e IV, apenas.
- E. I, II, III e IV.

4. Com relação a procedimentos de segurança da informação, julgue os itens subsequentes

[86] O denominado firewall de estado é um tipo de firewall mais simples que atua na camada de rede (camada 3), para filtrar tráfego a partir de endereços IP de origem e destino e a partir da porta TCP ou UDP.

[87] IPSpoofing é uma técnica utilizada para mascarar pacotes IP por meio de endereços errados, a fim de que não seja possível identificar o endereço IP e para que não se permita a identificação do invasor.

MPS – CESPE 2010 – Tecnologia da Informação

5. Os geradores de transação (GTs) aguardam silenciosamente no computador até que o usuário se autentique, por exemplo, em um home banking ou loja virtual. Uma vez autenticado, o sítio geralmente cria um cookie de sessão, usado para autenticar mensagens subsequentes a partir do navegador. Esses cookies de sessão residem no navegador e se mostram acessíveis por um malware. Um GT pode, com o usuário autenticado no sítio, usar o cookie de sessão para gerar transações em nome do usuário, transferindo fundos de sua conta ou comprando itens a serem enviados como presente. Para o sítio, uma transação gerada por um GT se mostra idêntica a uma transação legítima realizada pelo usuário, pois se origina do mesmo IP usado pelo usuário na mesma hora do dia, tornando-a difícil de ser percebida por ferramentas.

Tendo o texto acima como referência inicial, julgue os próximos itens referentes ao GT.

[118] O CAPTCHA (completely automated public turing test to tell computers and humans apart) é uma alternativa para combater o GT.

[119] O SSL (secure socket layer) não pode ser considerado uma contramedida ao GT.

[120] Uma das vulnerabilidades que habilitam o uso do GT é o cross site script request forgery (CSRF).

TRF 4 – FCC 2010 – Técnico Judiciário

6. Em redes de computadores, é o tipo de ataque em que o espião intercepta a comunicação entre dois usuários, de forma que o usuário A comunique-se com ele mesmo pensando ser o usuário B, e o usuário B também o faz, pensando ser o usuário A.

Trata-se de

- A. SYN Flooding.
- B. Pharming.
- C. Man-in-The-Middle.
- D. DoS.
- E. Spoofing.

Gabarito

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