Estratégia CONCURSOS

Aula 14

Redes de Computadores e Segurança da Informação para Concursos - Curso Regular 2017

Professor: André Castro

Facebook: André Castro (Professor)
Twitter e Periscope: @andrehsc

AULA 14

SUMÁRIO PÁGINA

CRONOGRAMA DO CURSO

AULA	CONTEÚDO	DATA
Aula 0 **Demonstrativa**	~~Conceitos Básicos de Redes, Meios de Transmissão, Tipos de rede e conexão, Topologias de rede, Classificação das Redes; Transmissão de Sinais; Cabeamento Estruturado.~~	29/12
Aula 1	~~Elementos de interconexão de redes de computadores (hubs, bridges, switches, roteadores, gateways). Arquitetura e protocolos de redes de comunicação: modelo de referência OSI e arquitetura TCP/IP;~~	05/01
Aula 2	~~Ethernet, ATM, X.25, Frame Relay, outros protocolo; Tecnologias de Redes de Acesso;~~	12/01

Aula 3	~~STP e RSTP; 802.1.q (VLAN); 802.1p, 802.1x, EAP, Redes sem Fio e Aspectos de Segurança;~~	19/01
Aula 4	~~IPv4 e IPv6; Endereçamento de Rede; ICMP; IGMP; NAT, ARP/RARP; Internet das Coisas; Troca de Tráfego - PTT~~	26/01
Aula 5	~~MPLS, TCP; UDP e SCTP;~~	02/02
Aula 6	~~HTTP, HTTPS, DHCP, FTP, DNS, SMTP, POP, IMAP, NTP v4; SSH; TELNET;~~	09/02
Aula 7	~~Gerenciamento de Redes: SNMP; Ferramentas de Gerenciamento; VPN~~	16/02
Aula 8	~~Protocolos de Roteamento – Rip, OSPF, BGP, outros; Protocolos de Roteamento Multicast; VRRP~~;	23/02
Aula 9	~~Análise de Tráfego;~~	02/03
Aula 10	~~QoS – Intserv e Diffserv; Redes e Protocolos Multimídia; SIP; H.323; MGCP~~	09/03
Aula 11	~~X.500 e LDAP; Serviços de Autenticação: Radius, TACACS, TACACS+, Kerberus; NFS, SAMBA e CIFS~~	16/03
Aula 12	~~Conceitos Básicos; Princípios de Segurança; Mecanismos de Segurança; Controle Físico e Lógico. Princípios Normativos.~~	23/03
Aula 13	~~Firewall, Proxy, IpTables, IDS/IPS, SELinux, ICAP; SSL/TLS e IPSeC~~	30/03
.Aula 14	Ataques em redes e aplicações corporativas: DDoS, DoS, IP spoofing, port scan, session hijacking, buffer overflow, SQL Injection, cross-site scripting, spear phishing; Malwares;	06/04
Aula 15	Sistemas de Criptografia: Criptografia simétrica e assimétrica. Certificação Digital e assinatura digital; Funções HASH;	13/04
Aula 16	Cluster, GRID e Balanceamento de Carga; Cloud Computing: IaaS, PaaS, SaaS, outros;	20/04
Aula 17	Redes de Armazenamento: SAN, NAS, DAS. Tecnologias, estratégias e Ferramentas de Backup; Tipos de Armazenamento; Deduplicação; ILM	27/04

Vamos dar continuidade ao nosso curso pessoal!

Portanto, vamos avançar!!!

1. Ataques a Redes de Computadores

Chegamos a um tópico muito bacana pessoal! Vamos falar sobre ataques a redes (Internet) e, consequentemente, abordaremos diversos aspectos de envolvidos na Segurança da Informação.

Atualmente, grandes empresas têm investido pesado em tecnologias e soluções com vistas a mitigar as vulnerabilidades que podem ser exploradas por pessoas mal-intencionadas. E aqui já podemos abordar o conceito do elo mais fraco.

Este está relacionado à ideia de um atacante sempre buscar descobrir uma vulnerabilidade ou um meio que, através do menor esforço possível, ele conseguirá alcançar o objetivo do ataque.

Assim, de nada adianta um ambiente ter regras de firewall altamente precisas, com outros equipamentos parrudos se não há uma conscientização dos usuários, através de normas e políticas, para que não haja vazamento de dados através da engenharia social. Em regra, esse tipo de ataque é aquele que gera o resultado com o menor esforço.

Portanto, devemos ter um ambiente equilibrado em todos os setores e áreas nos diversos quesitos de segurança.

a. Ataques na Internet

Na era da Internet das coisas, temos diversos dispositivos conectados à Internet e, obviamente, sujeitos a uma infinidade de possíveis ataques e más intenções de usuários da rede. Em termos gerais, muitas são as possíveis motivações que levam esses usuários a tais ações. Podemos citar:

- ***Demonstração de Poder*** – Expor vulnerabilidade de empresas ou determinados ambientes com o objetivo de se ter algum tipo de vantagem pessoal no futuro.
- ***Motivações financeiras*** – Obter informações confidenciais e privilegiadas para desenvolvimento de golpes que geram algum tipo de "lucro".

- ***Motivações ideológicas*** – Invadir sistemas para passar um recado ou divulgar uma imagem que representa uma ideologia ou determinada linha de pensamento.
- ***Motivações comerciais*** – Em um mercado cada vez mais competitivo em que indisponibilidade de serviços e sistemas geram grandes prejuízos financeiro e de imagens, pode-se ter agentes específicos que atuam de forma mal intencionada para este fim.

Frente a essas motivações, diversas técnicas de ataques que são desenvolvidas, além de ferramentas para levantamento de informações que antecedem as ações dos atacantes, as quais veremos a seguir.

❖ Exploração de Vulnerabilidades

Segundo o Cert.br, uma vulnerabilidade "é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança".

Tais vulnerabilidades estão presentes em diversos locais, equipamentos, softwares ou pessoas. Como exemplos, podemos citar um desenvolvimento falho de um sistema operacional ou programa ou ainda bugs intrínsecos em equipamentos, como switches, roteadores ou firewalls.

Assim, a partir de tais vulnerabilidades, o atacante pode obter informações privadas, invadir sistemas e até controlar sua máquina para ser instrumentos em outros ataques. Veremos alguns tipos desses ataques ainda nessa aula.

❖ Varredura em Redes – Scan

A varredura em redes é uma técnica que geralmente antecede ataques. Essa técnica visa a obtenção de informações que subsidiarão as ações dos atacantes, como a busca de vulnerabilidades.

Um ataque bem planejado busca conhecer o ambiente da vítima. Assim, a partir desse conhecimento, pode-se traçar um plano de ação com vistas a reduzir os esforços e não deixar rastros.

Como exemplos, podemos citar a obtenção de informações dos sistemas operacionais dos servidores e de suas atualizações. Caso se verifique que o servidor está com as atualizações defasadas, pode-se buscar vulnerabilidades a serem exploradas.

Outro exemplo de varredura é com vistas a se obter informações dos serviços e portas utilizadas por um servidor. Assim, pode-se utilizar portas "abertas" de forma indevida para gerar acessos indevidos a essa máquina.

Uma das principais ferramentas utilizadas para este fim é o NMAP. Esta ferramenta pode ser facilmente instalada em um dispositivo e a partir deste, insere-se um IP que será o alvo da varredura. Quando executado internamente em uma rede, pode-se obter informações extremamente relevantes do ambiente. Quando rodados externamente, tende a sofrer bloqueio ou filtragem de firewall que reconhecem a varredura.

Importante lembrarmos que a varredura também possui um tipo de execução legítima, quando, pessoas devidamente autorizadas e mediante um plano de comunicação do procedimento a ser realizado, fazem a varredura para efeito de auditoria ou verificação de aspectos de segurança, sejam eles preventivas ou corretivas.

❖ Falsificação de e-mail (E-mail spoofing)

Antes de falarmos especificamente do e-mail spoofing, vamos conceituar o termo spoof, pois é algo de diversas questões e podemos agilizar nossas resoluções com este assunto bem consolidado.

O termo Spoofing está diretamente relacionado ao assunto de falsificação ou adulteração de alguma informação com vistas a alteração de algum tipo de identidade ou identificador. Duas são as principais intenções com isso:

1. Se passar por alguma pessoa, instituição ou dispositivo que possua certo grau de confiabilidade e legitimidade para dar confiança à informação enviada. Por exemplo, posso enviar e-mails em nome da Receita Federal para obter informações dos usuários.
2. Esconder informações da origem de tal forma que não seja possível a identificação ou o rastreamento do atacante.

Assim, o Spoofing pode ser aplicado a e-mails, endereços IP ou MAC, entre outros.

Como tópico dessa nossa abordagem, temos o e-mail spoofing. Essa técnica geralmente é utilizada previamente a outro tipo de ataque mais prejudicial, como a propagação de códigos maliciosos, envios e replicação de spans e golpes de phishing.

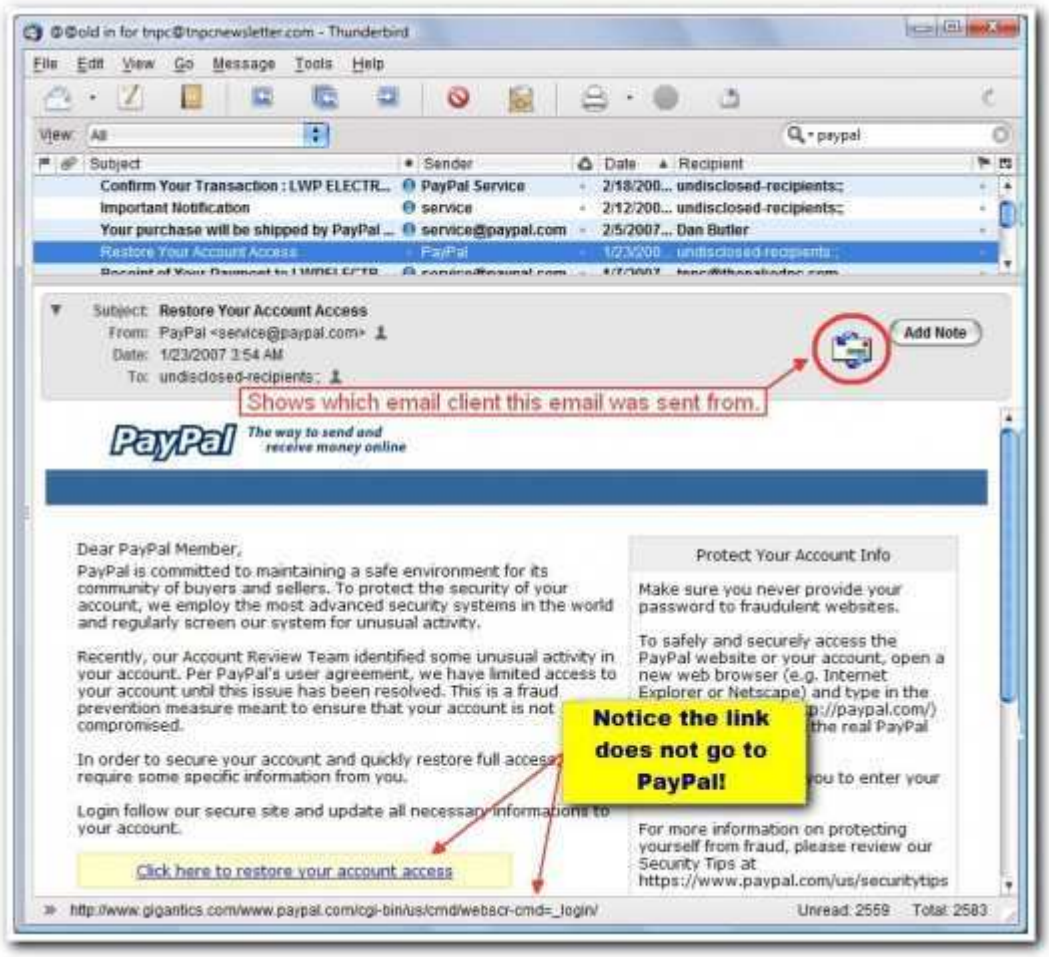
É um recurso básico para realização de SCAM! E aqui, muita atenção pessoal! Não é SCAN (varredura) e sim SCAM (foco na enganação do usuário) com M!!!

Para se manipular as informações dos e-mails, basta-se adulterar os dados do cabeçalho do SMTP, mais especificamente, do campo FROM, além dos campos REPLY-TO e RETURN-PATH.

Alguns exemplos clássicos que recebemos diariamente em nossos e-mails são:

- Atacantes se passando por alguém conhecido, solicitando que você clique em um link ou execute um arquivo anexo;
- Atacantes se passando por seu banco, solicitando que você siga um link fornecido na própria mensagem e informe dados da sua conta bancária;
- Atacantes se passando por administrador do serviço de e-mail que você utiliza, solicitando informações pessoais e ameaçando bloquear a sua conta caso você não as envie.

A partir da imagem abaixo, podemos ainda listas algumas observações:

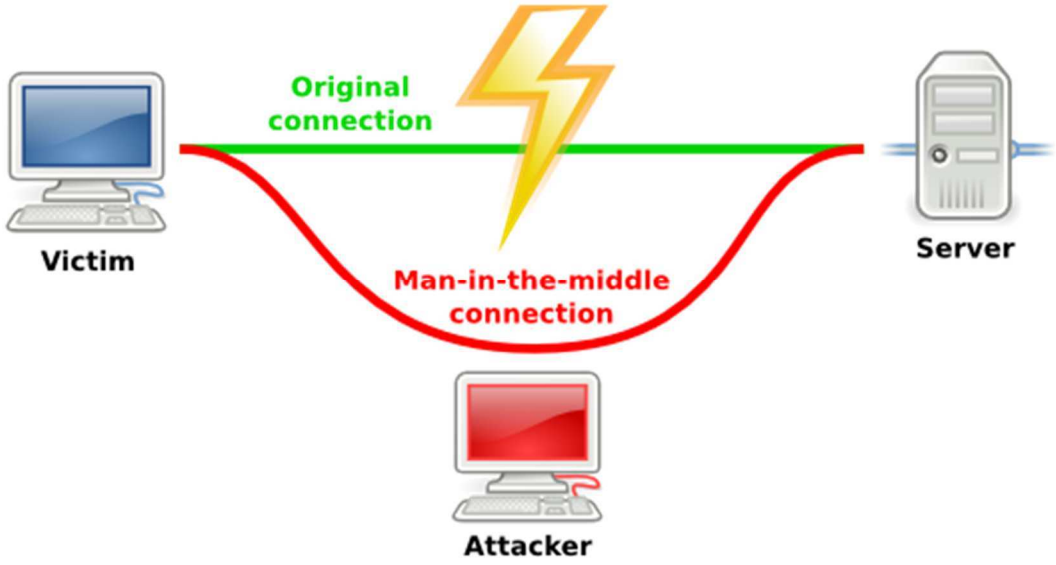


Perceba que o atacante está se passando pela empresa PayPal. Entretanto, no link a ser clicado, há um redirecionamento para uma página falsa ou ilegítima.

❖ Man in the Middle

Este é um tipo de ataque básico que possui mais um caráter conceitual, de modo que pode ser implementado por diversas técnicas.

A sua principal característica é a capacidade de se inserir no meio de uma comunicação entre dois nós. Assim, ao invés de se ter uma comunicação direta entre as vítimas, tem-se o estabelecimento de duas novas conexões, conforme podemos perceber na imagem a seguir:



Desse modo, o atacante consegue ter acesso a todos os dados trafegados na comunicação. Assim, ele pode ainda agir de algumas formas:

- Pode simplesmente acessar e extrair os dados violando a confidencialidade. Para mitigar esse tipo de ataque, pode-se utilizar a criptografia para tornar os dados ilegíveis;

- Pode modificar os dados, ainda que não consiga ter acesso ao conteúdo de forma direta, violando assim a Integridade. Para mitigar esse tipo de ataque, pode-se utilizar recursos que visam controlar a integridade dos dados como cálculos de verificação ou funções HASH;

- Pode simplesmente escolher quais mensagens devem ou não chegar até o destino, eliminando as demais, violando assim o princípio da Disponibilidade. Para mitigar esse tipo de ataque, pode-se utilizar técnicas de controle semelhantes às que são implementadas pelo protocolo TCP para confirmação de recebimento;

- Pode usar a identidade do usuário para realizar a autenticação em serviços diversos, violando o princípio da autenticidade. Esse tipo de ataque, também é conhecido como ataque REPLAY. Para

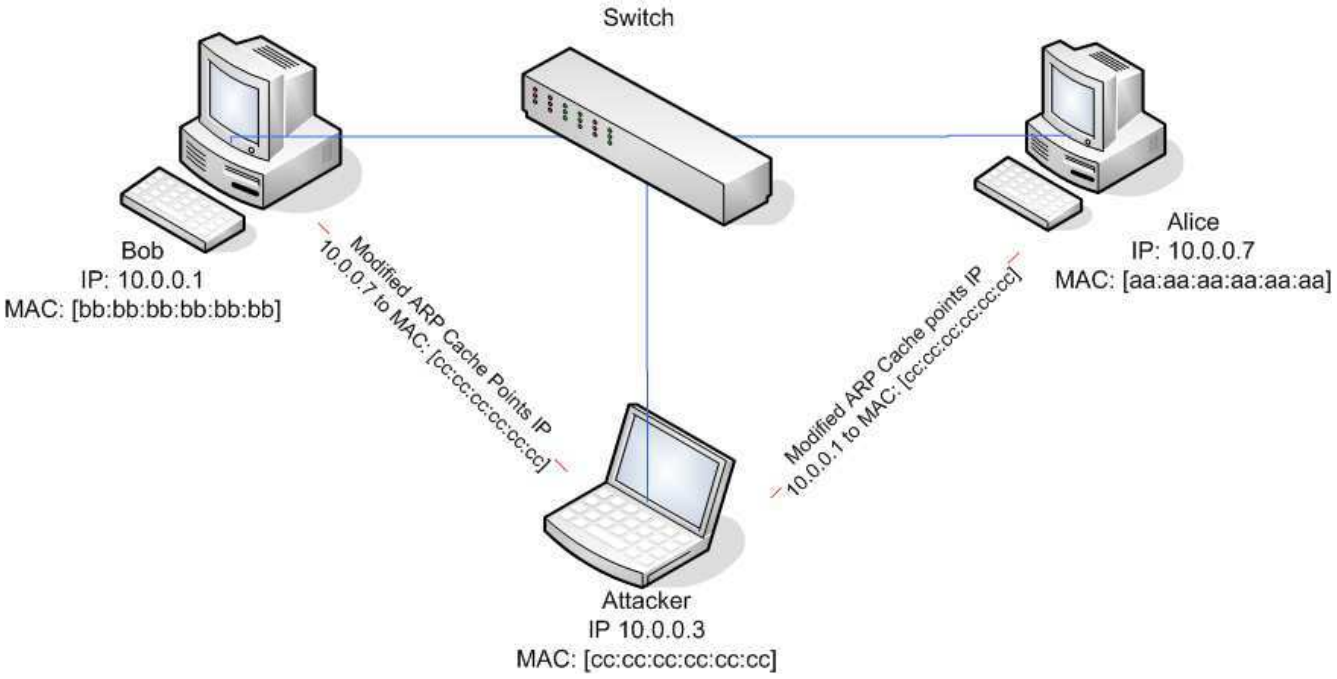
mitigar esse tipo de ataque, pode-se utilizar de chaves dinâmicas de sessão com prazo curto e temporário de validade.

❖ ARP Spoofing ou ARP Poisoning

Dando continuidade ao assunto de falsificação, temos agora aplicado ao protocolo ARP. Como já vimos, o ARP tem a característica de traduzir endereços IP para endereços MAC. O procedimento padrão do ARP é o envio de um ARP request para todos da rede de tal modo que somente o "dono" de determinado endereço IP deveria responder com a informação de seu endereço MAC através da mensagem ARP REPLY.

Entretanto, no ARP Poisoning, não é isso que acontece. O objetivo aqui é assumir a identidade de outro host da rede com vistas a interceptar o tráfego que deveria ser direcionado à vítima passando a obter informações privadas.

Vamos verificar na prática como isso acontece. Vamos partir da imagem abaixo:



O atacante envia a informação para BOB com o intuito de se passar por ALICE dizendo que o IP 10.0.0.7 tem como MAC correspondente o

cc:cc:cc:cc:cc:cc, quando o correto seria aa:aa:aa:aa:aa:aa, que é o endereço da ALICE.

Faz o mesmo procedimento ao enviar a informação para ALICE se passando por BOB, ao informar que o endereço 10.0.0.1 possui como MAC correspondente o endereço MAC cc:cc:cc:cc:cc:cc, quando o correto deveria ser bb:bb:bb:bb:bb:bb.

Assim, o atacante envenenou as tabelas ARP de ALICE e BOB. Agora, sempre que a ALICE encaminhar uma mensagem para BOB, ela será redirecionada para o ATACANTE e vice-versa.

Esse é um ataque extremamente fácil de ser realizado, tanto a nível do próprio Sistema Operacional como através de ferramentas, como CAIN&ABEL.

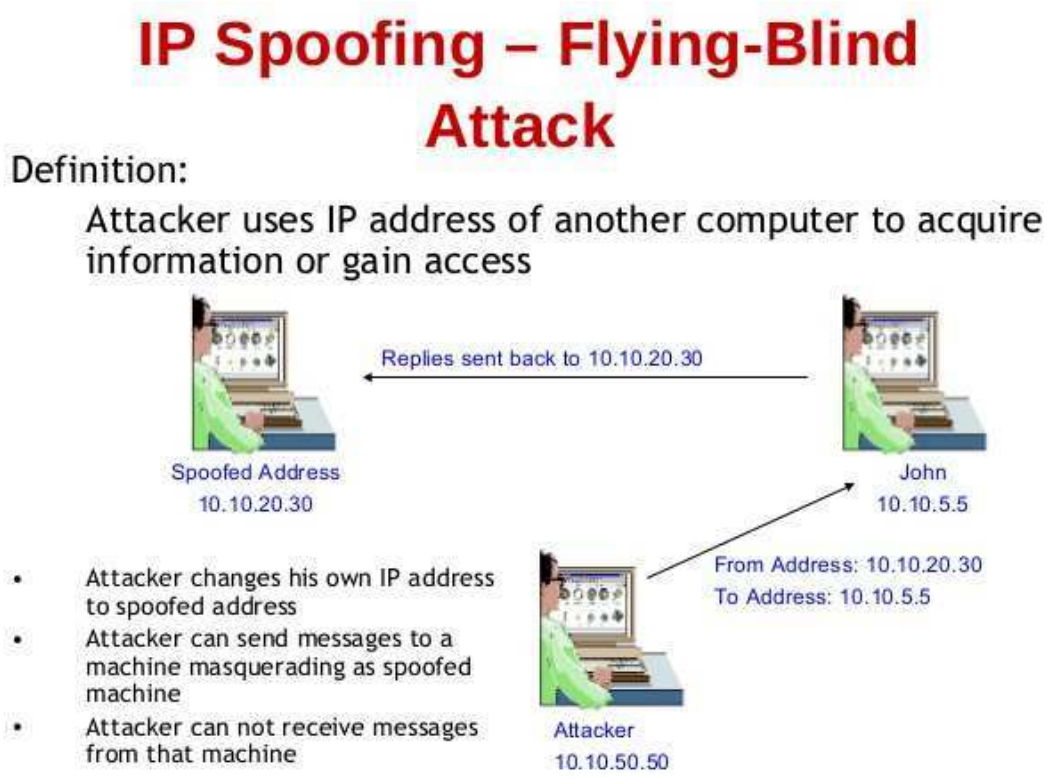
❖ IP Spoofing

Temos aqui um ataque bastante simples com o objetivo de mascarar ataques de rede com o intuito de não deixar rastros que possam incriminar um atacante.

Ou seja, digamos que determinado atacante queira fazer uma varredura em um firewall de uma instituição. Nesse caso, adultera-se os pacotes IP de tal modo a mascarar o IP real do atacante. O mesmo princípio se aplica quando se objetiva a derrubada de um servidor, através de DoS, por exemplo, que veremos mais à frente.

Se um volume muito grande de requisições parte de um mesmo host, gera-se uma suspeita de que está sendo realizado um ataque. Assim, pode-se adulterar os pacotes dando a impressão que são vários hosts realizando requisições distintas.

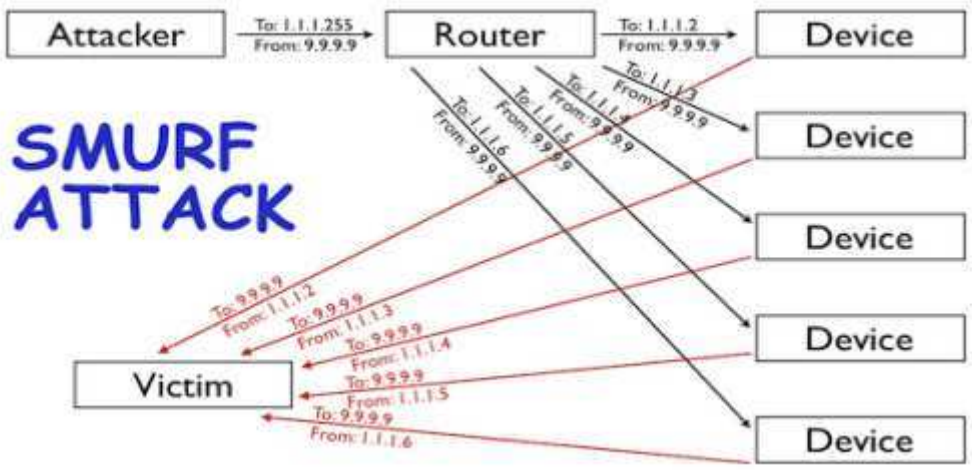
Outros tipos de ataques também são gerados a partir do IP Spoofing. Vamos analisar a imagem abaixo:



Percebam que o atacante enviou uma informação para JOHN. O IP original do atacante é 10.10.50.50. Entretanto, ele adultera a origem de tal modo que a resposta enviada por JOHN agora vá para endereço adulterado, a saber: 10.10.20.30. Veremos que esse princípio é utilizado para gerar ataques de negação de serviço.

❖ Ataque SMURF

A partir do SPOOFING de IP, pode-se gerar ataques mais elaborados e potentes. Um exemplo deles é o ataque SMURF. Esse tipo de ataque consiste em enviar ataques de resposta à vítima a partir de mensagens do tipo echo request para um endereço de broadcast com o "IP SPOOFADO" da vítima. A figura a seguir nos ajuda a entender este conceito:



Assim, o atacante sabendo que o IP da vítima é o 9.9.9.9, ele adultera o campo FROM do pacote IP de uma mensagem do tipo echo request. Essa mensagem possui como destino um IP de Broadcast de alguma rede que responde a PINGS.

Em seguida, o roteador distribuirá essas mensagens para todos os nós que fazem parte daquela rede. Assim, cada nó responderá às requisições com uma mensagem do tipo ECHO REPLY. Entretanto, como o IP de origem corresponde ao endereço IP da vítima, todo esse tráfego será redirecionado à vítima, gerando indisponibilidade do serviço.

❖ Interceptação de tráfego (Sniffing)

Interceptação de tráfego, ou sniffing, é uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de sniffers (Ex. Wireshark e TCPDump). Esta técnica pode ser utilizada de forma:

> **Legítima:** por administradores de redes, para detectar problemas, analisar desempenho e monitorar atividades maliciosas relativas aos computadores ou redes por eles administrados.
>
> **Maliciosa:** por atacantes, para capturar informações sensíveis, como senhas, números de cartão de crédito e o conteúdo de arquivos confidenciais que estejam trafegando por meio de conexões inseguras, ou seja, sem criptografia.

Note que as informações capturadas por esta técnica são armazenadas na forma como trafegam, ou seja, informações que trafegam criptografadas apenas serão úteis ao atacante se ele conseguir decodificá-las.

❖ Força Bruta

Como o próprio nome já diz, busca descobrir uma senha ou alguma outra informação através do método de tentativa e erro de forma exaustiva.

Esse tipo de ataque demonstra a importância de se ter senhas grandes de complexas com o objetivo de tornar esse tipo de ataque inviável.

O grau de desempenho desse ataque está diretamente relacionado à capacidade de processamento computacional de um atacante.

Os mesmos conceitos de força bruta se aplicam também à quebra de chaves criptográficas para que seja possível a interpretação de dados criptografados.

As tentativas de adivinhação baseiam-se em:

- Dicionários de diferentes idiomas e que podem ser facilmente obtidos na Internet;
- Listas de palavras comumente usadas, como personagens de filmes e nomes de times de futebol;
- Substituições óbvias de caracteres, como trocar "a" por "@" e "o" por "0"";
- Sequências numéricas e de teclado, como "123456", "qwert" e "1qaz2wsx";
- Informações pessoais, de conhecimento prévio do atacante ou coletadas na Internet em redes sociais e blogs, como nome, sobrenome, datas e números de documentos.

❖ Desfiguração de página (Defacement)

Desfiguração de página, defacement ou pichação, é uma técnica que consiste em alterar o conteúdo da página Web de um site. Possui um caráter unicamente de vandalismo, sendo inclusive referenciado por algumas bancas como tal.

As principais formas que um atacante, neste caso, também chamado de defacer, pode utilizar para desfigurar uma página Web são:

- Explorar erros da aplicação Web;
- Explorar vulnerabilidades do servidor de aplicação Web;
- Explorar vulnerabilidades da linguagem de programação ou dos pacotes utilizados no desenvolvimento da aplicação Web;
- Invadir o servidor onde a aplicação Web está hospedada e alterar diretamente os arquivos que compõem o site;
- Furtar senhas de acesso à interface Web usada para administração remota.

Para ganhar mais visibilidade, chamar mais atenção e atingir maior número de visitantes, geralmente, os atacantes alteram a página principal do site, porém páginas internas também podem ser alteradas.

Muita atenção, pois, o conceito que acabamos de ver é diferente do PHISHING, que veremos a seguir.

❖ Phishing

A ideia aqui não é invadir algum sistema para adulterá-lo, mas sim, copiar uma página legítima e divulgar às vítimas para obtenção de informações privadas. O principal meio de divulgação das páginas falsas é por e-mail através de SPAM.

Assim, pode-se gerar um aviso de um banco, por exemplo, para que a vítima acesse a página e regularize determinada condição. A vítima, ao clicar no link enviado pelo atacante, será redirecionado para a página falsa, sendo um clone da página legítima do banco.

A vítima então acaba incluindo os seus dados bancários de acesso à conta na página falsa dando acesso ao atacante à sua conta bancária. Assim, é muito importante estarmos atentos às URL's, de fato. Verificar sempre se estas correspondem aos endereços legítimos dos sites.

Outro conceito atrelado ao Phishing é o Spear Phishing. Esse tipo de ataque é similar ao Phishing com a diferença de ter um destino específico, como uma empresa ou órgão governamental, produzindo assim um ataque customizado através da falsificação de e-mails.

❖ Pharming

Este tipo de ataque ocorre quando um tráfego que originalmente deveria ir para um site legítimo é redirecionado para outro. Percebam a diferença do Phishing padrão. No Phishing o usuário já dispara o acesso à uma página falsa na origem, enquanto no Pharming, há um desvio ao longo da rede, sendo quase que transparente para o usuário.

Essa forma de ataque pode ocorrer de diversas formas, como por meio da alteração do DNS (DNS Poisoning), em que se faz um apontamento para um IP de destino que armazena conteúdo similar, porém, é um site malicioso para se obter dados. Esse tipo de ataque pode acontecer tanto nos arquivos de configuração de DNS local quando em um servidor de consulta.

❖ Negação de Serviço (Denial of Service – DoS)

Este tipo de ataque busca comprometer o princípio de Segurança conhecido como disponibilidade. Assim, efetua-se o ataque para "tirar" um serviço do ar.

Para se retirar um serviço do ar, deve-se esgotar algum tipo de recurso de determinado sistema que inviabilize o atendimento de novas requisições. Isso pode acontecer por uma indisponibilidade total (desligamento ou travamento de sistemas), ou com funcionalidade intermitente, de tal modo que o sistema fique tão lento que inviabilize sua utilização.

Este tipo de ataque pode se dar das seguintes formas:

- Envio de um grande volume de requisições para um serviço específico (como acesso à uma página WEB), consumindo seus recursos de processamento, quantidade de sessões suportadas, banda de internet, memória, disco, entre outros;
- Exploração de vulnerabilidade em programas causando sua indisponibilidade.

❖ Negação de Serviço Distribuído (Distributed Denial of Service)

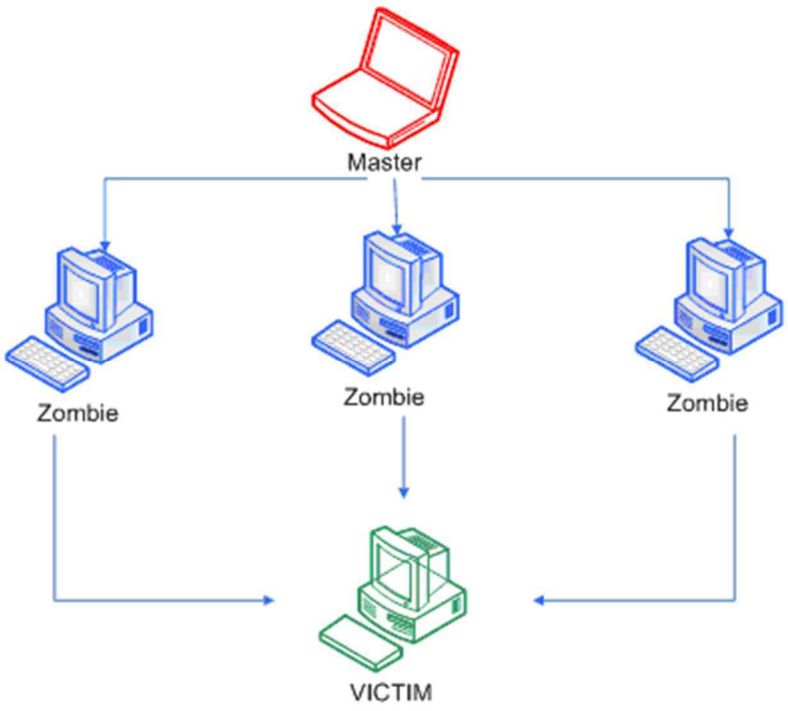
Tem os mesmos princípios do ataque DoS, porém, é tratado de forma coordenada e distribuída, sejam por computadores envolvidos de forma voluntária ou de forma involuntária (zumbis).

O mais usual é o segundo método. Assim, antes de efetuar esse tipo de ataque, um atacante precisa controlar uma rede de computadores zumbis, muitas vezes chamadas de botnets. Desse modo, o atacante envia o comando para que todos os dispositivos controlados enviem requisições de forma simultânea a um host específico (vítima), gerando indisponibilidade do serviço.

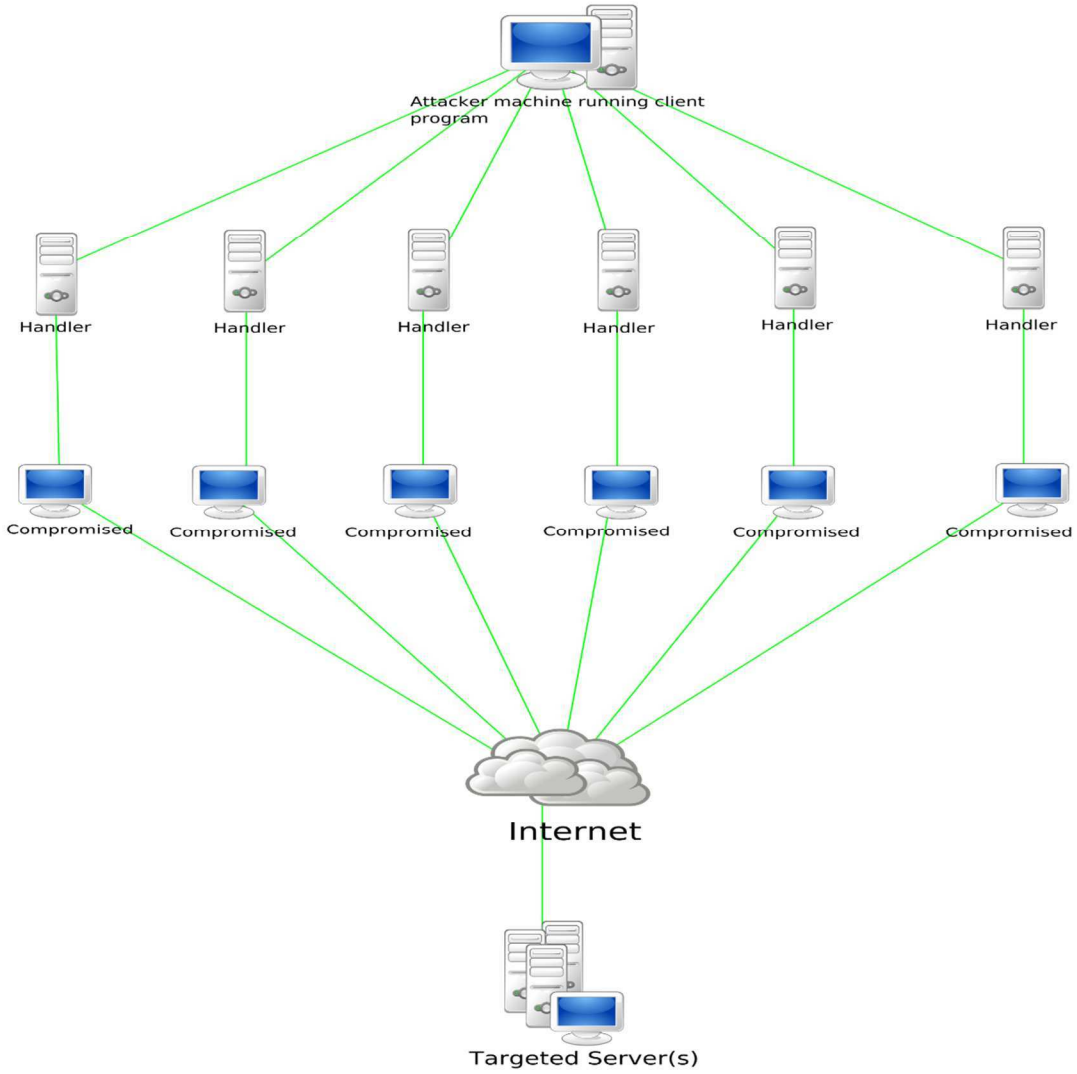
Este tipo de ataque tem um alto grau de sucesso devido à grande dificuldade de se detectar e reagir a tempo a esse tipo de ataque. Na maioria das vezes a ação é reativa com vistas a mitigar o prejuízo.

A principal reação se dá através do contato com a operadora responsável pelo provimento do acesso à Internet com vistas a bloquear determinada região ou rota BGP que está originando esse grande volume de requisições.

A figura abaixo nos traz uma representação visual de um ataque do tipo DDoS:

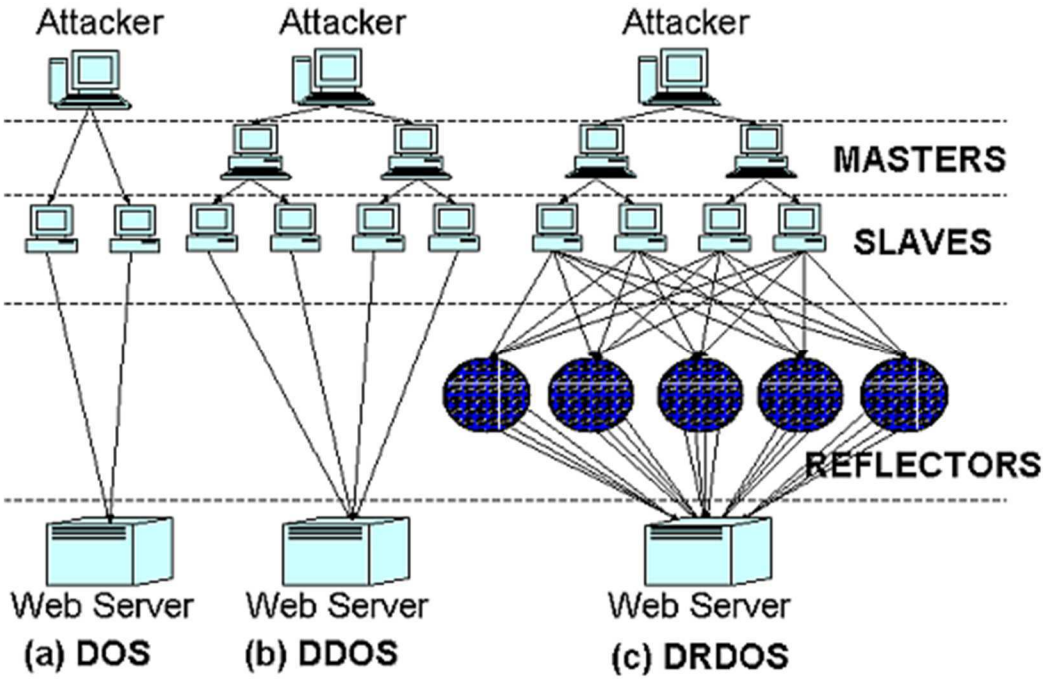


Ataques mais elaborados e robustos de DDoS acabam por construir redes hierárquicas com controles descentralizados, gerando um volume ainda maior. A imagem abaixo nos apresenta esse cenário:



Um ataque específico de DDoS que surge para aumentar ainda mais o poder de fogo é o DRDoS ou DDoS Refletor. A ideia é utilizar zumbis para enviar requisições com endereços forjados para usuários legítimos e não infectados. Entretanto, devido ao IP forjado gerado pelos zumbis, os hosts legítimos encaminham o tráfego (resposta às requisições) à vítima, algo semelhante ao que vimos no SMURF ATTACK.

Entretanto, com o volume, tem-se um poder de fogo muito maior. Percebam que o ataque, diferentemente do DDoS padrão, não ocorre de forma direta dos zumbis para a vítima, e sim, por intermediários que funcionam como refletores. A figura abaixo nos apresenta uma comparação entre os três tipos:



Vamos falar um pouco mais sobre as principais medidas que podem ser adotadas frente a ataques do tipo DDoS. Há de se mencionar, que nem toda medida é absoluta de tal forma que a junção de várias delas torna o sistema mais robusto. Como vimos, o DDoS busca esgotar recursos de determinadas formas, seja no processamento, consumo de memória, banda, entre outros.

Portanto, ao se evitar pontos únicos de falha, ou seja, possíveis gargalos, inevitavelmente obtém-se um ambiente mais robusto.

As principais técnicas e medidas são:

- **Superestimar recursos de rede (largura de banda) e recursos computacionais:** A ideia é ter cada vez mais largura de banda e recursos computacionais de tal modo que exigirá ainda mais potência nos ataques de DDoS para esgotar os recursos. Entretanto, é uma solução um tanto cara manter recursos dessa forma, principalmente, considerando que estes ficarão ociosos em

condições normais. Por esse motivo, acaba se tornando inviável muitas vezes.

- **Estabelecimento de padrões de tráfego:** Monitorar o fluxo e traçar perfil de acesso e utilização permite aos gerentes de rede bloquearem acessos que fogem ao padrão. Além disso, pode-se determinar marcos específicos como uma *Baseline* de comportamento que permite uma reação de forma mais rápida em caso de comportamento estranho.

  Entretanto, esse tipo de operação pode gerar falsos positivos, ou seja, tráfego legítimos que possuem um caráter de exceção e serão tratados como possíveis ataques.

- **Encaminhar o tráfego inválido para "buracos negros":** Como o perfil desses ataques geralmente utilizam requisições falsas ou incompletas ao servidor, busca-se descartar ou desconsiderar esse tipo de tráfego. Para tanto, pode-se redirecioná-los por rotas nulas, chamadas de "buracos negros". Como não há a resposta de informação de que os pacotes estão sendo descartados, dificulta-se a ação alternativa por parte dos atacantes.

  Há de se mencionar que atacantes mais experientes já possuem pleno conhecimento dessas técnicas e não esperam uma resposta nos casos de rotas inválidas. Essa técnica visa simplesmente à mitigação dos danos provenientes desse tipo de ataque.

- **Utilização de serviços de distribuição de conteúdo:** Focado em reduzir a carga de um eventual ataque, pode-se utilizar serviços específicos de fornecimento de conteúdo (CDN's). Assim, pode-se manter informações específicas nas CDN's de modo a desonerar o consumo de recursos nos servidores principais da aplicação. Entretanto, devido ao volume a ser utilizado, também pode se tornar inviável em termos financeiros.

- **Hardening de Sistemas:** A configuração segura com vistas a eliminar possíveis vulnerabilidades de sistemas operacionais e serviços. Assim, pode-se tornar o ambiente mais robusto e menos suscetível a esse tipo de ataque.

Temos um link muito bacana gerado pelo CERT dos Estados Unidos que traz uma visão geral a respeito do DDoS, desde suas principais técnicas de implementação e contramedidas. Recomendo a leitura do artigo de apenas três páginas:
https://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf

❖ SPIM (Spam over Instant Messager)

O tão conhecido SPAM possui uma variação para serviços de mensagem instantânea. Chama-se SPAM via IM. Nesse caso, os indivíduos mal intencionados utilizam dois métodos de transferência de código malicioso. Eles podem enviar um arquivo com vírus, trojan ou spyware, ou podem fazer uso de engenharia social. Uma vez que o código é executado, o usuário poderá ter sua lista de contados violada e roubada, propagando o ataque para outros usuários.

❖ Ataques de Engenharia Social

A partir da enganação da vítima por meio social, pode-se obter informações privilegiadas para se gerar ataques. Existem várias técnicas que usam a engenharia social, quais sejam:

- **Vishing** – Trata-se de uma prática em que o sujeito que inicia um ataque vai fazer uso de um sistema telefônico (VoiP, por exemplo) para ter acesso a informações pessoais da vítima;
- **Phishing ou Spear Phishing** – Conforme já vimos;
- **Hoax** – Trata-se de uma mentira que, quando divulgada por veículos de disseminação em massa, pode parecer verdade. Essa disseminação pode utilizar os diversos meios de comunicação.
- **Whaling** – São ataques altamente direcionados com vistas a ludibriar executivos do alto escalão de uma organização.

❖ Sequestro de dados - Ransomware

Um ataque que tem ganhado cada vez mais expressão é o de sequestro de dados. Neste tipo de ataque, o atacante obtém acesso privilegiado ao sistema da vítima e realiza criptografia dos dados da vítima. Assim, os dados passam a estar inacessíveis, dependendo da inserção da chave criptográfica para decriptar os dados.

O atacante então exige um valor a ser pago para disponibilização da chave à vítima para que ela possa acessar seus dados novamente.

Além disso, o atacante geralmente agrega ameaças de destruição dos dados e que o "resgate" deve ser pago em um período específico, geralmente, 3 dias.

---

b. Malwares

Avançando um pouco mais a nossa conversa, vamos discutir diversos termos e nomes que caracterizam os mais diversos ataques.

Vamos começar trazendo a definição de um MALWARE. Nada mais é do que um software malicioso, dando origem ao termo em questão (MALICIOUS SOFTWARE).

Desse modo, podemos perceber que um MALWARE é o conceito mais genérico no que tange a ataques a rede. Podemos ter MALWARES com o objetivo de roubar dados, roubar identidades, traçar perfis, gerar danos aos hardwares e sistemas, entre muitas outras hipóteses. Assim, apresentarei a vocês os tipos de MALWARES mais conhecidos e cobrados em prova. Antes disso, é importante termos em mente algumas formas que esses MALWARES infectam os dispositivos:

- **Exploração de vulnerabilidades intrínsecas em programas**:
  - Aqui temos a importância de manter programas atualizados e sempre utilizar programas legítimos.
- **Pela execução automática de mídias removíveis infectadas, como pen-driver**:
  - Recomenda-se desabilitar a auto execução de mídias para evitar este tipo de ataque. Caso tenha um arquivo infectado, ele dependerá de execução para se propagar, ou seja, sem a auto execução, já teremos um fator de dificuldade para o sucesso do MALWARE;
- **Pelo acesso a Páginas Web Maliciosas:**
  - Vários pontos podem ser explorados ao se acessar uma página desse tipo, seja através da exploração de vulnerabilidade do próprio Browser, ou downloads de arquivos infectados, entre outros;

- **Pela ação direta de atacantes que ao invadir os computadores, inserem códigos e programas indesejados**;
    - Devemos ter senhas de acesso mais complexas, controlar as portas de acesso aos dispositivos, entre outras técnicas que dificultam o acesso indevido às máquinas. A esses procedimentos damos o nome de HARDENING. Ou seja, busca-se "endurecer" o servidor de tal forma que ele não fique tão vulnerável;

Vamos conhecer então os principais tipos de MALWARES existentes e suas características.

❖ VÍRUS

Esse tipo de Malware nada mais é do que um código que pode ser representado por um programa ou parte de um programa com a capacidade de gerar cópias de si mesmo e se inserindo em outros programas ou arquivos, além de executar tarefas específicas no computador da vítima como deleção de arquivos, instalação de outros programas, redução de configurações de segurança, desestabilização do sistemas e ocupação de espaço de armazenamento.

Um termo chave do VÍRUS é que este depende de uma ação direta do usuário ou do SO em termos de execução do programa ou abertura de um arquivo infectado. Então o simples fato do arquivo está no seu computador não implica que você tenha necessariamente sido infectado.

O principal meio utilizado para propagação é a própria Internet ou mídias removíveis, como pen drives. E aqui temos uma dica de segurança: não devemos deixar ativado a auto execução de arquivos seja através de downloads da Internet ou na inserção de mídias removíveis no computador.

Existem alguns conceitos que categorizam os vírus em tipos conforme a sua forma de ação. Para não deixarmos lacunas, vamos verificar quais são:

- **Vírus de Boot:** Infecta a área de inicialização dos sistemas operacionais, também conhecido como MBR (Master Boot Record) do disco rígido. Esse tipo de vírus não corrompe arquivos específicos, mas sim, todo o disco. Os antivírus comuns de

sistemas operacionais não são capazes de detectar esse tipo vírus, sendo necessário uma varredura antes da inicialização do sistema para sua detecção.

- **Vírus de Arquivo:** Infecta arquivos de programas executáveis, geralmente, nas extensões .EXE e .COM. Ao se executar o referido programa, ativa-se o vírus.

- **Vírus Residente:** Este é carregado diretamente na memória RAM do SO toda vez que o SO é iniciado. Este tipo de vírus pode ser extremamente danoso, bloqueando acessos à memória RAM, interromper determinados processos e funções a serem executadas e inclusive, alterar tais funções para fins maliciosos.

- **Vírus propagado por e-mail:** recebido como um arquivo anexo a um e-mail cujo conteúdo tenta induzir o usuário a clicar sobre este arquivo, fazendo com que seja executado. Quando entra em ação, infecta arquivos e programas e envia cópias de si mesmo para os e-mails encontrados nas listas de contatos gravadas no computador.

- **Vírus de script**: escrito em linguagem de script, como VBScript e JavaScript, e recebido ao acessar uma página Web ou também por e-mail, como um arquivo anexo ou como parte do próprio e-mail escrito em formato HTML. Pode ser automaticamente executado, dependendo da configuração do navegador Web e do programa leitor de e-mails do usuário.

- **Vírus de macro**: tipo específico de vírus de script, escrito em linguagem de macro (série de comandos e instruções que podem ser agrupadas em um simples comando), que tenta infectar arquivos manipulados por aplicativos que utilizam esta linguagem como, por exemplo, os que compõe o Microsoft Office (Excel, Word e PowerPoint, entre outros). Geralmente são escritas em linguagens como Visual Basic para Aplicações (VBA) e ficam armazenadas nos próprios documentos. Este o motivo das MACROS serem bloqueadas nativamente por estes programas devendo o usuário habilitá-la manualmente para macros legítimas.

- **Vírus de telefone celular**: vírus que se propaga de celular para celular por meio da tecnologia bluetooth ou de mensagens MMS

(Multimedia Message Service). A infecção ocorre quando um usuário permite o recebimento de um arquivo infectado e o executa. Após infectar o celular, o vírus pode destruir ou sobrescrever arquivos, remover ou transmitir contatos da agenda, efetuar ligações telefônicas e drenar a carga da bateria, além de tentar se propagar para outros celulares.

Assim, o Vírus busca manter-se indetectável para se propagar ao máximo nos programas de um computador. Assim, surgiu o conceito de Vírus Stealth, um malware que evita a sua detecção através de técnicas de programação.

Além disso, tem-se ainda os chamados vírus metamórficos e polimórficos, que são executados e automaticamente conseguem transformar-se, ou seja, modificam seu próprio código, dificultando e adiando a detecção da ameaça pelo antivírus.

❖ WORM

Outro malware muito comum é o WORM. Este possui como principal característica a capacidade de se propagar pela rede de computadores através do envio de cópias de seu código a outros dispositivos. Além disso, o Worm busca explorar vulnerabilidades específicas dos sistemas, diferentemente do Vírus.

Devido ao seu grande poder de propagação na rede, acaba por gerar um grande consumo de processamento e banda, prejudicando bastante a qualidade dos sistemas e da rede. Pode ter uma propagação a nível global ao longo da Internet nos casos da existência de vulnerabilidades presentes nos mais diversos sistemas.

❖ SPYWARE

Este tipo de malware foca na obtenção de informações de um host ou sistemas através do monitoramento de suas atividades. Assim, pode-se enviar informações a um terceiro qualquer para consolidar os dados obtidos e tentar coletar informações relevantes para outros fins.

Assim como já vimos anteriormente, pode ser dividido em uso legítimo e malicioso. O primeiro, pode ser instalado pelo próprio usuário para monitorar ações em seu dispositivo por outros usuários ou ainda com o

consentimento deste para monitoramento de uma instituição de trabalho, por exemplo.

Já o modo malicioso fere o princípio da privacidade da pessoa ou do usuário, podendo ser obtidas senhas de acesso e outras informações privilegiadas.

Ainda em relação ao spyware, podemos categorizá-lo em espécies divididas tanto pela sua finalidade como pela forma de obtenção dos dados. Vamos alguns dos principais:

- **Keylogger**: capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de Internet Banking.

  Por esse motivo, foi desenvolvido o teclado virtual, de tal modo que o usuário não necessita digitar senhas diretamente em sem teclado, mas sim, através de cliques do mouse. Assim, caso haja um Keylogger na máquina do usuário, este não será capaz de coletar as informações digitas.

- **Screenlogger:** similar ao Keylogger, é capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em sites de Internet Banking. Desse modo, podemos considerar inclusive como sendo uma evolução do Keylogger.

  Para evitar este tipo de ataque, foi desenvolvido teclados virtuais que “embaralham” os caracteres em cada acesso, ou seja, a sequência de digitação da senha nunca será a mesma, inviabilizando, portanto, a dedução dos números e letras pela posição do teclado virtual.

- **Adware:** projetado especificamente para apresentar propagandas direcionadas ao perfil do usuário. Pode ser usado para fins legítimos, quando incorporado a programas e serviços, como

forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos (como o google adwords). Aqui, muitos usuários não concordam com essa política do google, entretanto, ao instalar seu navegador ou SO ou outros sistemas, muitos de nós damos o devido consentimento ao marcar a opção “Eu li e aceitos os termos. ”

Também pode ser usado para fins maliciosos, quando as propagandas apresentadas são direcionadas, de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo feito.

Alguns Adwares mais complexos e danosos possuem a capacidade de sequestrar e invadir os navegadores dos usuários. Assim, altera-se páginas iniciais de acesso, mecanismos de pesquisas, redirecionamentos automáticos, entre outros, com a finalidade de controlar, até certo ponto, a navegação do usuário. Importante delimitar a ação desse tipo de ataque, pois a finalidade não é criar zumbis ou inserir vírus, entre outros.

❖ CAVALO DE TRÓIA (TROJAN)

Cavalos de Tróia são programas que entram no sistema operacional escondidos atrás de outros programas. Assim, o usuário recebe um programa imaginando que este foi desenvolvido para determinado propósito, porém, escondido dentro dele, há um código malicioso. Um detalhe a ser observado é que, de fato, o programa principal executará as operações esperadas trazendo alguma credibilidade ao usuário para que ele não desconfie.

Típicos cavalos de Tróia que são amplamente divulgados são programas para “craquear” produtos originais através da geração de códigos ou números de série.

Outros tipos bastante difundidos são aqueles mascarados sobre produtos desenvolvidos para aumentar o desempenho de seu computador ou até mesmo antivírus ou antimalwares. Ele de fato pode realizar buscar e achar aspectos legítimos, porém, sempre mascarando seu verdadeiro propósito com algum malware.

Outro ponto a se observar é que o cavalo de Tróia não se restringe a esconder um único tipo de malware. Pode carregar diversos tipos, sejam simultâneos ou não.

❖ BACKDOOR

Este tipo de código malicioso busca gerar algum meio para acesso futuro de um atacante. A ideia aqui não é somente invadir um sistema, mas manter o acesso. Então após alguma invasão, como por exemplo, um cavalo de Tróia, o atacante instala um backdoor que abrirá alguma porta no dispositivo para acesso futuro, podendo agregar outros códigos e tomar controle total da vítima.

❖ ROOTKIT

É um tipo de malware que tem se popularizado bastante pela sua efetividade de invasão e controle, além da dificuldade de detecção. O ROOTKIT é um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido. Percebam que seu foco não é na invasão em si, mas sim na manutenção do acesso indevido. Busca realizar operações como:

1. Remover evidências de registros em arquivos de logs;
2. Instalar outros códigos maliciosos, como backdoors;
3. Esconder atividades e informações como arquivos, diretórios, processos, entre outros;
4. Mapear potenciais vulnerabilidades a serem exploradas em outros computadores na rede a qual a vítima está inserida e capturar informações através da interceptação de tráfego;

Tais ações são possíveis mediante após a invasão e escalada de privilégios em um Sistema Operacional, obtendo o maior nível de acesso possível em um computador. Nos casos de ambientes UNIX, temos o modo ROOT. Para ambientes Windows, temos o modo SYSTEM.

Diversos tipos de Rootkits podem ser carregados em um sistema, como por exemplo:

- Kernel Rootkits (carregado no Kernel do SO);
- Virtual Rootkits (Agem na camada de virtualização de um sistema);

- Firmware Rootkit (Agem nos componentes de hardware, como placas de vídeo, controladoras, etc);
- Library Rootkit (Carregado no módulo de bibliotecas de um SO).

❖ BOT e BOTNET

Já introduzimos esse conceito quando falamos de ataques DDoS. Os BOTS são programas que permitem a comunicação e controle do invasor sobre o sistema da vítima através de acessos remotos. Para tanto, utiliza-se de vulnerabilidades presentes nos sistemas dos usuários. A sua propagação se dá de modo semelhante ao Worm, através da replicação de seus códigos e envio pela rede, e-mail ou outros meios.

Desse modo, havendo o controle por parte do invasor, este poderá disparar diversos tipos de ataques utilizando o sistema da vítima, como ataques de negação de serviço, furto de dados de outras vítimas e envios de SPAM, contando com a dificuldades de se rastrear a origem real do ataque.

Como vimos, esses BOTS são conhecidos como zumbis (Zombies), uma vez que tal programa fica inerte até que haja o interesse do invasor para utiliza-lo para algum fim específico.

Desse modo, ao se construir diversos controles de vários BOTS, cria-se, portanto, uma BOTNET, ou seja, uma rede de BOTS ou zumbis. A ideia é controlar cada vez mais vítimas com vistas a potencializar ainda mais os ataques. Essas redes são inclusive comercializadas no mercado negro. Ou seja, caso você seja demitido de uma empresa e queira desferir um ataque contra ela, você pode entrar em contato com algum dono de BOTNET e pagar um valor de aluguel, por exemplo, para ter essa rede disponível para um ataque à empresa que te demitiu.

❖ BOMBA LÓGICA

Outro tipo de malware que consiste em programas que são disparados a partir de eventos específicos e predefinidos. Como exemplo, podemos ter uma data ou um conjunto de caracteres digitados. Geralmente são instaladas a partir de usuários que já possuem acesso ao sistema da vítima.

Temos uma tabela apresentada na cartilha do cert.br através do link cartilha.cert.br/malware muito interessante que traz um resumo das principais características de alguns tipos de malware.

Códigos Maliciosos							
	Vírus	*Worm*	*Bot*	*Trojan*	*Spyware*	*Backdoor*	*Rootkit*
Como é obtido:							
Recebido automaticamente pela rede		✓	✓				
Recebido por *e-mail*	✓	✓	✓	✓	✓		
Baixado de *sites* na Internet	✓	✓	✓	✓	✓		
Compartilhamento de arquivos	✓	✓	✓	✓	✓		
Uso de mídias removíveis infectadas	✓	✓	✓	✓	✓		
Redes sociais	✓	✓	✓	✓	✓		
Mensagens instantâneas	✓	✓	✓	✓	✓		
Inserido por um invasor		✓	✓	✓	✓	✓	✓
Ação de outro código malicioso		✓	✓	✓	✓	✓	✓
Como ocorre a instalação:							
Execução de um arquivo infectado	✓						
Execução explícita do código malicioso		✓	✓	✓	✓		
Via execução de outro código malicioso						✓	✓
Exploração de vulnerabilidades		✓	✓			✓	✓
Como se propaga:							
Insere cópia de si próprio em arquivos	✓						
Envia cópia de si próprio automaticamente pela rede		✓	✓				
Envia cópia de si próprio automaticamente por *e-mail*		✓	✓				
Não se propaga				✓	✓	✓	✓
Ações maliciosas mais comuns:							
Altera e/ou remove arquivos	✓			✓			✓
Consome grande quantidade de recursos		✓	✓				
Furta informações sensíveis			✓	✓	✓		
Instala outros códigos maliciosos		✓	✓	✓			✓
Possibilita o retorno do invasor						✓	✓
Envia *spam* e *phishing*			✓				
Desfere ataques na Internet		✓	✓				
Procura se manter escondido	✓				✓	✓	✓

c. Ataque na Camada de Aplicação

Dando continuidade à nossa discussão dos diversos tipos de ataques, vamos focar agora em ataque que acontecem na camada de aplicação do modelo OSI. Esse tipo de ataque tem crescido bastante uma vez que não depende de conhecimento de aspectos da rede, mas tão somente uma codificação e programação maliciosa a nível da camada 7 do modelo OSI.

Portanto, vamos conhecer os principais ataques dessa camada.

❖ Cross-Site-Scripting (XSS)

O XSS é uma técnica de obter informações do usuário após este ser persuadido a entrar em um site com scripts que são executados no computador da vítima. Uma vez que se executa tal script, com os devidos privilégios de usuário, podem ser executadas rotinas diversas no dispositivo.

Esse tipo de ataque tem crescido bastante, se tornando como um dos principais na atualidade. Dois são os principais tipos de ataques XSS. O primeiro, é conhecido como não persistente e o segundo, persistente.

Esses ataques exploram uma vulnerabilidade no servidor de aplicação de determinado sistema e modificam o código inserindo código malicioso. A partir de então, todos que entrarem nesse link, que até um primeiro momento é legítimo, será afetado.

Esses ataques de XSS são frequentemente utilizados para causar danos, seja através da obtenção de dados dos usuários, como o prejuízo de imagem da instituição que está “hospedando” o código malicioso.

Percebam que, apesar do código residir no servidor de aplicação, a atuação do XSS não é contra o servidor de aplicação, mas sim, aos usuários daquele serviço, onde de fato o script será executado.

Assim, pode-se sequestrar as sessões dos usuários através de cookies, alterar códigos HTML no lado do cliente, redirecionar usuários para sites maliciosos (phishing) e alterar os objetos para captura de entradas de usuários.

Para se evitar esse tipo de ataque podemos extrair do guia OWASP, o seguinte.

"Deve-se separar os dados não confiáveis do ativo no navegador. Como exemplos, temos:

1. Filtrar adequadamente todos os dados não confiáveis com base no contexto HTML (corpo, atributo, Javascript, CSS ou URL)
2. Criar Listas Brancas ou de entradas positivas. Entretanto, não possui uma defesa completa, uma vez que muitas aplicações requerem caracteres especiais em sua entrada. Tal validação deve, tanto quanto possível, validar o tamanho, caracteres, formato, e as regras de negócio sobre os dados antes de aceitar a entrada.
3. Para conteúdo do tipo RICH, considere o uso de bibliotecas de auto sanitização. Ou seja, deve-se realizar filtros que consigam remover TAGS potencialmente danosa, validando de forma adequada as entradas de dados dos usuários.
4. Implementação de CSP – Content Security Policy em todo o site. "

❖ Injeção SQL (SQL Injection)

Ataque bastante conhecido e difundido, porém, com grande nível de sucesso nos dias atuais. Esse tipo de ataque também explora uma vulnerabilidade da aplicação (página web, por exemplo).

Esse tipo de ataque permite que determinado usuário malicioso manipule as entradas de banco de dados nos envios de requisições ou consultas à base de dados de alguma aplicação.

Assim, caso não haja o devido bloqueio de operações, pode-se, por exemplo, complementar um comando de consulta a uma tabela que visa retornar uma lista, com um "DROP TABLE", por exemplo, podendo gerar perda de todos os dados ali armazenados.

❖ Injeção LDAP (LDAP Injection)

Possui estrutura de funcionamento semelhante ao SQL injection no sentido de manipulação de entradas.

No caso do LDAP injection, temos uma técnica para explorar aplicações web que fazem interface com servidores LDAP sem que as informações inseridas sejam verificadas, podendo fazer o envio de comando indesejados e ganhar acessos indevidos, podendo modificar informações e executar comandos com acessos privilegiados.

❖ Injeção XML (XML Injection)

Seguindo o mesmo modelo, temos agora a injeção na linguagem XML. Ocorre quando o atacante cria um XML com entradas maliciosas explorando vulnerabilidades em sistemas que não aplicam as validações devidas.

❖ Vulnerabilidade Dia Zero (Zero Day Vulnerability)

Como sabemos, o processo de desenvolvimento de aplicações e sistemas é extenso. Há procedimentos de testes, homologação, betas, entre outros. Entretanto, por diversas vezes, alguns sistemas ainda são disponibilizados com falhas ou vulnerabilidades que são descobertos posteriormente pelo fabricante ou desenvolvedor. Assim, as vulnerabilidades existentes entre o período da descoberta e de correção é conhecido como vulnerabilidade Dia Zero.

❖ Buffer Overflow

Temos aqui uma clássica falha de programação que possibilita ao usuário malicioso gerar indisponibilidade de serviços ou sistemas. A ideia básica é simples: aloca-se uma informação que exige espaço em memória ou registradores maior do que se suporta, gerando um travamento da aplicação.

Um exemplo simples é na soma de número binários, por exemplo. Vamos supor que determinado campo receba entradas para gerar respostas de soma binária. O campo de resposta, suporta apenas 4 bits, ou seja, o maior valor suportado é 1111.

Entretanto, o que acontecerá se somarmos 1111 com 1111? Simples não? Teremos 10000! Ou seja, necessita-se de 5 bits para representar o valor, porém, este campo só suporta 4 bits! Temos aqui um possível CRASH do sistema!

Outro tipo de utilização desse ataque é para explorar áreas indevidas na memória do servidor ou da vítima. Isso acontece quando não há o devido tratamento dos dados de uma entrada no sistema. Assim, um invasor busca injetar strings que extrapolam o tamanho máximo permitido na entrada de um campo.

Ao fazer isso, o invasor consegue injetar códigos nas áreas de memória que não deveriam ser acessadas.

❖ Complementos Maliciosos (Malicious Add-ons)

Os Add-ons são complementos a diversos sistemas que permitem a inclusão de recursos adicionais, sejam em navegadores, aplicativos de PC, entre outros.

Nem sempre se verifica a legitimidade dos complementos disponibilizados, situação essa que pode gerar a instalação de códigos maliciosos.

❖ Sequestro de Sessão (Session Hijacking)

A ideia aqui é simples. A vítima realiza o estabelecimento de uma sessão com determinado servidor web. Um terceiro malicioso, monitorando a comunicação, realiza o spoofing de IP da máquina da vítima e força com que o servidor responda à requisição original para ele. Desse modo, ele se passa pela vítima com a sessão já estabelecida e encerra a sessão com a vítima, tomando conta de toma comunicação. Esse é o modo ativo do sequestro de sessão.

O modo passivo apenas monitora e coleta dados da sessão, sem encerrar a sessão com a vítima.

❖ Ameaça Persistente Avançada (APT - Advanced Persistent Threat)

O conceito que se aplica aqui está voltado ao direcionamento de um ataque a determinada vítima de forma concentrada, a partir de diversas técnicas, como as já vistas acima, com a utilização de recursos diversos da rede para processamento dessas investidas. Geralmente se organizam em times ou grupos altamente coordenados para efetuarem os ataques.

Desse modo, podemos dizer que os ataques APT são direcionados, porém, não podemos afirmar que todos os ataques direcionados são do tipo APT.

Esse tipo de ataque pode ser dividido em 5 fases básicas:

1. ***Reconhecimento*** – Faz-se o levantamento de informações do ambiente da vítima com o objetivo de entender o cenário a ser atacado.
2. ***Incursão ou Investida*** – Geralmente se utiliza de engenharia social para invadir a rede de alguma organização. Assim, implanta-se algum malware para explorar vulnerabilidades;
3. ***Descoberta*** – Uma vez dentro do ambiente da vítima, o atacante busca evitar sua detecção a partir de ações lentas e discretas com a finalidade de mapear as defesas a partir de uma visão interna da organização e criar um plano de ataque com vistas a explorar o máximo de vulnerabilidades possíveis para garantir o sucesso do ataque.
4. ***Captura*** – O atacante consegue invadir os sistemas e capturar informações.
5. ***Extração*** – Finalmente, a partir das informações capturadas, o atacante busca ter acesso a esses dados, enviando via rede para sua base de ataque.

Todo ataque APT tem um objetivo e propósito em relação a determinado adversário ou vítima. Os principais são roubo de dados confidenciais, como descrições de projetos, contratos e informações patenteadas. Temos ainda o fato de que a finalidade não é “roubo” ou “desvio” de dinheiro de alguma forma, mas sim obter informações para que o atacante se torne tão capaz em conhecimento quanto a vítima.

d. Ataques a Redes sem Fio

Um ponto que tem começado a surgir em provas são os ataques a redes sem fio. Apesar de já serem amplamente difundidos no cenário atual, para efeito de prova, podemos considerar como um assunto novo.

Os ataques de redes sem fio buscam explorar as diversas brechas existentes na própria estrutura ou arquitetura de implementação da

tecnologia. Há de se lembrar que, nos ambientes de redes sem fio, os dados enviados pelos dispositivos possuem um caráter de Broadcast, ou seja, todos os dispositivos dentro daquele *range* específico de alcance do sinal poderão interceptar o tráfego. Desse modo, vamos conhecer alguns dos principais ataques utilizados nesses ambientes.

Mas antes, gostaria apenas de lembrar que as redes sem fio são, nos casos do 802.11, extensões da rede cabeada. Dessa feita, a maioria dos ataques possíveis de serem realizados nos ambientes com fio também poderão ser utilizados nas redes sem fio.

❖ Wardriving

Essa terminologia define um método que busca procurar redes sem fio através de uma antena de alto alcance conectada a um dispositivo móvel qualquer, preferencialmente, um laptop.

Esta procura geralmente é feita a partir de um automóvel e possui como principal objetivo a enumeração das redes em busca de redes abertas, desprotegidas ou com sistemas de proteção suscetíveis a quebra.

De forma complementar, utiliza-se recursos de GPS com vistas a mapear em softwares que disponibilizam mapas, como o GOOGLE MAPS. Desse modo, apresenta-se no mapa as diversas redes com os seus respectivos nomes (SSID), bem como suas tecnologias de acesso e autenticação (WEP, WPA, WPA2).

Atualmente já existem software específicos que realizam essas tarefas, como é o caso do Kismet, para ambientes UNIX.

❖ Rogue Access Point (Pontos de Acesso Não autorizados)

Esse tipo de ataque visa explorar brechas na infraestrutura de uma rede sem fio. Busca-se configurar um access point para receber conexões de outros dispositivos na rede como se fosse um access point legítimo na rede.

Uma vez que seja configurado tal equipamento, todos os dados enviados e recebidos pelos dispositivos atrelados ao access point não autorizados poderão ser capturados e tratados pelo atacante.

Com vistas a amplificar esse ataque, geralmente configura-se access points com técnicas de autenticação fracas ou inclusive abertas para se tornar um atrativo para as vítimas.

Assim, quando a vítima pensa que está tirando alguma vantagem ao se conectar a uma rede alheia de maneira indevida, na verdade, ela está entregando todo o seu fluxo de dados a um eventual atacante.

Um exemplo clássico desse modelo é um atacante sentar em uma lanchonete do McDonalds e configurar seu computador ou um access point acesso de terceiros. Assim, os clientes da referida lanchonete, se conectariam à rede achando que está em uma rede legítima do McDonalds, quando, na prática, estão sendo vítimas de um ataque.

Por esse motivo, jamais devemos acessar recursos privados como e-mails particulares ou corporativos, bancos, ou outras plataformas que tratam dados de maneira sigilosa.

❖ Ataque de Engenharia Elétrica

Essa técnica tem como objetivo gerar indisponibilidade da rede sem fio ou, pelo menor, prejudicar a qualidade da transmissão de dados. Como a rede sem fio atua em frequência específicas, que podem ser facilmente obtidas pelos atacantes, acabam por ficar vulneráveis a um alto grau de interferência.

A ideia é simplesmente ter um equipamento ou uma antena que gere sinal de alta intensidade na mesma frequência de operação da referida rede, gerando assim uma relação Sinal-Ruído baixa que impede o funcionamento adequado da rede, impedindo, inclusive, que novos usuários se associem à rede sem fio.

❖ Bluejacking

Esse tipo de ataque, como o próprio nome já nos ajuda a lembrar, busca explorar o modelo de comunicação por bluetooth. O seu funcionamento é similar ao SPAM, lá do contexto de correio eletrônico. Entretanto, para o bluetooth, utiliza-se o protocolo OBEX para tal finalidade.

Geralmente esse tipo de ataque não gera danos às vítimas. Estas acabam por receber mensagens de texto com propagandas ou informações indesejadas de outros dispositivos que estejam próximos. Caso o dispositivo suporte mensagens multimídia – MMS – estas também podem ser utilizadas.

A principal proteção contra esse tipo de ataque é não habilitar o modo "visível" de seu aparelho quando estiver com o bluetooth ativado, invocando assim o método de segurança por obscuridade ou desconhecimento.

❖ Bluesnarfing

Outro tipo de ataque que também habita em redes bluetooth é o bluesnarfing. Esse tipo de ataque possui um caráter invasivo que fere a privacidade, podendo atingir ainda a confidencialidade de determinados dados nos aparelhos das vítimas.

Essa técnica permite que o atacante tenha acesso à agenda, lista de contatos, correios eletrônicos, mensagens de textos, entre outros recursos do aparelho da vítima.

Com o surgimento de técnicas de autenticação para a sincronização ou o emparelhamento de dispositivos via bluetooth, essa técnica perdeu força.

e. NMAP

Algumas questões abordam características mais específicas do NMAP, como parâmetros e técnicas utilizadas para a varredura. A principal referência para as informações aqui apresentadas é o próprio site nmap.org.

Assim, aproveitaremos a discussão da ferramenta para entender o funcionamento das principais técnicas utilizadas, muitas das vezes,

utilizando a própria estrutura dos principais protocolos da arquitetura TCP/IP.

O NMAP é uma ferramenta gratuita e de código aberto utilizado tanto de forma legítima (auditoria de segurança) como ilegítima (descoberta de informações da rede). A estrutura padrão do comando executado pelo NMAP se dá da seguinte forma:

nmap [Scan Type(s)] [Options] {target specification}

Onde

Scan Type(s) - determina a técnica utilizada e o tipo de resultado esperado.

Options – campo opcional para complemento da varredura.

Target specification – IP do alvo.

Além disso, pode-se utiliza o parâmetro "-p" para se determinar portas específicas a serem varridas no alvo.

Analisando os possíveis parâmetros a serem utilizados, poderemos perceber que alguns deles são intuitivos em relação às Flags correspondentes do protocolo TCP. Vamos conhecê-los:

- **-sT** - Com esse parâmetro é feito um escaneamento através de tentativas de conexão TCP – TCP CONNECT (). Essa forma é muito fácil de ser identificada por firewalls e IDS. Caso se consiga uma conexão em determinada porta, tem-se o indicativo que esta porta está aberta. Caso não seja especificado nenhum tipo de parâmetro, este será o padrão utilizado.

- **-sS** - A tentativa será com pacotes TCP com a flag SYN ligada, ou seja, como apenas uma requisição de conexão – TCP SYN (HALF OPEN). Nesse método, um pacote SYN é enviado, caso haja resposta (um pacote SYN-ACK seja recebido), é porque a porta está aberta. Caso seja recebido um RST é porque está fechada. Se a resposta vier positiva (SYN-ACK), o nmap envia outro RST fechando a conexão, de modo que a conexão não se

complete. A vantagem desse método é que fica mais difícil a detecção do portscan, pois ele não abre uma conexão TCP completa, se assemelhando a um procedimento legítimo;

- **-sF** – Também conhecido como método STEALTH. Esse método envia pacotes FIN para o alvo, caso não haja resposta, a porta está aberta, caso seja recebido um pacote RST, é porque está fechada. Esse método é útil, pois alguns firewalls podem detectar a chegada de pacotes SYN, detectando o método TCP SYN, esse modo elimina essa possibilidade de detecção. Existem outras duas variações desse parâmetro, quais sejam**: nmap –sX** (Xmas Tree -> envia as flag FIN, URG e PUSH no pacote FIN); **nmap –sN** (null scan -> não envia flag no pacote FIN);

- **-sA** – Também conhecido como ACK SCAN. Esse método é utilizado para mapear o firewall alvo. Ele pode determinar o tipo de firewall e se ele apenas bloqueia os pacotes SYN.

- **-sP** - Também conhecido como PING SCAN. Nesse método são enviados pacotes "ICMP echo request" para o alvo. Caso não haja resposta, é enviado um pacote TCP ACK para a porta 80 ou então um pacote SYN (se nenhum das anteriores responder), isso tudo porque alguns firewalls bloqueiam o "ping". Ele é utilizado para ver se a máquina alvo está ativa ou não.

- **-sU** - Nesse método, um pacote UDP de 0 byte é enviado, caso seja recebido um "ICMP port Unreachable" é porque a porta está fechada, caso contrário, está aberta.

- **-sO** - É usado para tentar determinar os protocolos suportados pelo host;
- **-O** – Também conhecido como TCP/IP FINGERPRINT. Esse método ativa a identificação remota do sistema operacional. Ela usa várias informações recebidas e as compara com a base de dados dos sistemas operacionais conhecidos, detectando qual o sistema usado na máquina. -A - Verifica a porta e o serviço que está rodando.

Além dessas opções, o nmap possui muitas outras, como por exemplo o scan rápido (**nmap -F**) ou então a opção de não pingar a máquina antes de realizar o scan (**nmap -P0**).

Em adição a esses métodos de scan, o nmap oferece a opção de escolher "políticas", de modo a dificultar a detecção pelo IDS da máquina alvo. As opções são "Paranoid", "Sneaky", "Polite", "Normal", "Aggressive" ou "Insane".

A opção "Paranoid" escaneia de 5 em 5 minutos cada porta, a "Sneaky", de 15 em 15 segundos e assim evoluindo. A vantagem do "scan" ser mais lento é que dificulta a descoberta pelo IDS da máquina alvo. A opção padrão é a normal.

Como exemplo, podemos verificar a imagem abaixo como resultado de um SCAN de uma rede através do seguinte comando:

nmap -sS 192.168.0.0/24 -p 1-150

```
[root@linuxserver root]: nmap -sS 192.168.0.0/24 -p 1-150

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Interesting ports on  (192.168.0.1):
(The 149 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh

Interesting ports on  (192.168.0.65):
(The 148 ports scanned but not shown below are in state: closed)
Port       State       Service
111/tcp    open        sunrpc
139/tcp    open        netbios-ssn

Interesting ports on  (192.168.0.66):
(The 149 ports scanned but not shown below are in state: closed)
Port       State       Service
139/tcp    open        netbios-ssn

Interesting ports on  (192.168.0.242):
(The 149 ports scanned but not shown below are in state: closed)
Port       State       Service
139/tcp    open        netbios-ssn

Interesting ports on  (192.168.0.252):
(The 149 ports scanned but not shown below are in state: closed)
Port       State       Service
139/tcp    open        netbios-ssn


Nmap run completed -- 256 IP addresses (5 hosts up) scanned in 5 seconds
```

Percebamos que serão apresentadas quais portas TCP estão abertas em cada host ativo na rede.

Esse tipo de ferramenta se encontra em constante evolução, explorando a cada dia novas técnicas a partir das características dos protocolos utilizados. Na prática, em termos de equipamentos, devemos sempre buscar por firewalls e IPS no intuito de identificar e filtrar esse tipo de varredura. Além disso, a configuração apenas dos serviços essenciais em cada servidor é uma técnica altamente recomendada que faz parte do escopo de HARDENING de servidores (aplicação de regras rígidas para garantida de segurança).

Facebook: André Castro (Professor)
Twitter e Periscope: @andrehsc

LISTA DE EXERCÍCIOS COMENTADOS

1. CESPE – STJ/Analista Judiciário – Suporte em TI/2015

Uma vez que a varredura simples de portas é facilmente detectada por firewalls, outros tipos de mensagens passaram a ser utilizadas para mapeamento de serviços de redes, como por exemplo, as de RESET e as de SYN-ACK, que sinalizariam tentativa legítima de conexão, e, ainda, pacotes de resposta DNS (domain name system), que são respostas a mensagens geradas internamente.

Comentários:

No caso da questão, temos a explicitação de três técnicas muito comuns, apesar de também já serem detectados por firewalls mais avançados. No caso da RST, caso chegue um pacote com a flag RST marcada e a porta está fechada, a RFC do TCP define que deverá ser enviado uma resposta com um novo RST. Caso contrário, deve-se descartar o pacote.

Já com o SYN-ACK, esse conjunto é típico de resposta de uma tentativa de abertura de conexão em portas abertas no ato de estabelecimento de conexão. As demais flags podem ser utilizadas para se gerar uma infinidade de possibilidades de varreduras de portas.

Em relação aos pacotes de respostas DNS, vale lembrar, que em regra, são do tipo UDP e que também podem ser utilizados para mapeamento de portas. O DNS é muito utilizado para varredura de rede.

Gabarito: C

2. CESPE – ANTAQ/Analista administrativo – Infra de TI/2014

Em um ataque de DDoS, que objetiva deixar inacessível o recurso computacional para os usuários legítimos, um computador mestre

controla milhares de computadores zumbis que acessam um sistema ao mesmo tempo (um servidor web, por exemplo), com o objetivo de esgotar seus recursos.

Comentários:
Questão bem tranquila a respeito da utilização de botnets para gerar ataques do tipo DDoS com fim a gerar indisponibilidade de serviços.

Gabarito: C

---

3. CESPE – ANTAQ/Analista administrativo – Infra de TI/2014

O ataque de spear phishing, que é uma tentativa de fraude por falsificação de email, tem como alvo uma organização específica e objetiva, normalmente, conseguir acesso não autorizado a dados sigilosos.

Comentários:
Pessoal, bem tranquilo, certo?

Gabarito: C

---

4. CESPE – TC-DF/Analista de Administração Pública – Sistemas de TI/2014

Utilizado para a captura ilegal de informações de uma máquina em rede, o spoofing analisa o tráfego da rede e coleta dados sigilosos como senhas e endereços

Comentários:
O tipo de ataque que realiza análise de tráfego é o sniffing e não spoofing como afirma a questão. Lembrando que o mesmo sniffing pode ser utilizado de forma legítima na administração de redes, por exemplo.

Gabarito: E

---

5. CESPE – MPU/Analista – Suporte e Infraestrutura/2013

O combate à contaminação por um worm pode ser realizada por meio da utilização de antivírus no computador que se deseja proteger

Comentários:

Temos aqui uma questão de cunho bastante prático. Os antivírus, como o próprio nome diz, foram desenvolvidos para combater vírus em dispositivos. Entretanto, com a evolução das soluções, há uma sobreposição muito grande de ferramentas que são capazes de detectar diversos tipos de malwares, além daqueles para os quais foram desenvolvidos especificamente.

Assim, no cenário atual, os antivírus possuem uma base de dados gigantesca que não se restringe a vírus, contemplando também assinaturas de outros malwares, como, por exemplo, de worms.

Gabarito: C

---

6. CESPE – MPOG/Técnico de Nível Superior/2013

Ataques de negação de serviço volumétricos, distribuídos ou não, envolvem flooding para esgotamento de recursos e spoofing para dificultar o rastreamento da origem.

Comentários:

Como sempre, ataques bem sucedidos não se restringem a um único tipo. Assim, ataques de DoS ou DDoS não se restringem a causar indisponibilidade de serviços, mas também, de tornar o ataque irrastreável. Para tanto, pode-se utilizar o spoofing para mascarar o IP de origem do ataque, ou seja, do controlador Master de uma botnet, por exemplo.

Gabarito: C

---

7. CESPE – SERPRO/Analista de Desenvolvimento/2013

Um ataque à infraestrutura de conectividade de um banco à Internet, interrompendo o acesso a seus serviços de home banking, afeta a disponibilidade.

Comentários:

Se afetamos a conectividade de dispositivos que fornecem um serviço, esses estarão inacessíveis ou pelo menos, intermitentes no acesso. Isso gerará problemas de acessos aos serviços de tal modo que o serviço fique indisponível. Ou seja, afeta-se claramente o princípio da disponibilidade.

Gabarito: C

---

8. CESPE – INPI/Analista de Planejamento – Infraestrutura de TI/2013

Worm é um programa que possui código malicioso, capaz de se disseminar, por meio de uma rede, para vários computadores.

Comentários:
Temos a descrição da principal característica dos Worms.

Gabarito: C

---

9. CESPE – INPI/Analista de Planejamento – Infraestrutura de TI/2013

A principal atividade de programas com códigos maliciosos e que funcionam na função de keylogger é apresentar propagandas não solicitadas pelo usuário, direcionando-o a sítios maliciosos.

Comentários:
Não, né pessoal? Keylogger busca capturar as informações digitadas pelos usuários. O que temos descrito na assertiva é o Adware.

Gabarito: E

---

10. CESPE – INPI/Analista de Planejamento – Infraestrutura de TI/2013

Um spyware pode ser utilizado de forma legítima ou maliciosa, pois sua função é monitorar atividades de um sistema, além de coletar e enviar informações a terceiros.

Comentários:

Lembrando que o spyware, ao ser usado de forma legítima, permite a um administrador de redes monitorar o acesso e navegação dos usuários de uma rede, verificando assim as regras e políticas as quais estes estão submetidos.

Gabarito: C

---

11. CESPE – INPI/Analista de Planejamento – Infraestrutura de TI/2013

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.

Comentários:
Mais uma questão a respeito do DDoS e seus conceitos básicos. Percebam a frequência que este assunto é cobrado em provas.

Gabarito: C

---

12. CESPE – TJ-AC/Técnico Judiciário – Informática/2012

O funcionamento de um computador que tenha sofrido um ataque conhecido como phishing pode ser comprometido, sendo os dados gravados nesse computador armazenados em um disco corrompido.

Comentários:
Uma mistura de vários termos que não possuem relação entre si. Phishing tem o objetivo de capturar dados sigilosos de usuários através de páginas falsas. E o disco corrompido, professor? Não sei mesmo o que passou na cabeça do examinador, mas que bom que ele nos ajudou com esse absurdo.

Gabarito: E

---

13. CESPE – TJ-AC/Técnico Judiciário – Informática/2012

Os bots e os worms são tipos de programas maliciosos que se propagam enviando cópias de si mesmos pela rede de computadores.

Comentários:
Vimos que ambos possuem basicamente a mesma forma de propagação. Lembrando que o bot, diferentemente do worm, possibilita a comunicação do invasor e da vítima, de tal modo que seu sistema passa a ser controlado.

Gabarito: C

14.CESPE – TJ-AC/Técnico Judiciário – Informática/2012

Computadores conectados à Internet e infectados por bots são vulneráveis, estando sujeitos ao controle de criminosos que podem comandar um ataque de negação de serviço.

Comentários:
Reforçando o que acabamos de ver na questão anterior.

Gabarito: C

15.CESPE – TJ-AC/Técnico Judiciário – Informática/2012

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

Comentários:
Exatamente isso. Lembremos que os casos clássicos de spywares são aqueles programas que vamos dando “next”, “next” e “next” e quando vemos, demos a devida autorização para execução e instalação em nosso ambiente.

Gabarito: C

16.CESPE – TJ-AC/Técnico Judiciário – Informática/2012

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

Comentários:

Pessoal, temos aqui um problema conceitual. Vimos que o TROJAN é apenas um meio de entrada para diversos outros tipos de malwares, entre eles os BOTS, sendo que estes últimos possuem como característica o controle remoto de determinado dispositivo.

Entretanto, acabam que por diversas vezes, esses conceitos acabam se sobrepondo, levando a autores, como Tanenbaum, falarem de forma genérica a respeito do TROJAN, conforme trecho abaixo:

"*O mais provável é que o (Cavalo de Troia) se conecte a alguma porta IP e espere pelas instruções, transformando a máquina em um zumbi pronto para enviar spam ou executar qualquer ordem que seja da vontade de seu mestre remoto.*"

Portanto, utilizemos essa questão para traçar a linha de pensamento do CESPE a esse respeito.

Gabarito: C

17.CESPE – TJ-AC/Técnico Judiciário – Informática/2012

A atualização automática on-line do sistema operacional é uma prática que garante que o computador não sofrerá infecção por bots.

Comentários:

A atualização automática é um importantíssimo recurso para a segurança uma vez que ela possibilita a correção de falhas e vulnerabilidades existentes no sistema. Entretanto, não há relação com a prevenção contra bots, muito menos no sentido de "Garantir" tal condição.

Gabarito: E

18.CESPE – TJ-AC/Técnico Judiciário – Informática/2012

Por serem de difícil detecção, os worms só podem ser combatidos por ferramentas específicas para esse fim, que se denominam antiworms.

Comentários:
Lembrando que os worms geram impactos que são, muitas das vezes, bem perceptíveis, não sendo difícil ao menos suspeitar de sua presença. Além disso, vimos que antivírus comumente disponibilizados, inclusive em versões gratuitas, são capazes de detectar worms, não exigindo, portanto, ferramentas específicas para este fim.

Gabarito: E

19.CESPE – TJ-AC/Técnico Judiciário – Informática/2012

O uso de programas antivírus continuamente atualizados é uma prática suficiente para se evitar que um worm contamine um computador.

Comentários:
Apesar dos antivírus serem extremamente eficientes contra worms, não é possível garantir a plena prevenção, pois, os antivírus mais modernos são baseados em assinaturas específicas ou através de análise comportamental. Assim, caso exista um WORM novo que não conste na base de dados das assinaturas de um antivírus e consiga burlar o lado comportamental, este dispositivo poderá sim ser infectado.

Gabarito: E

20.CESPE – TRE/RS / Analista Judiciário/2015

Acerca de sistemas de segurança, ataques e malwares, assinale a opção correta.

A) A fase de disparo de um verme ou worm é caracterizada pela busca de outros sistemas para infectar, por meio de exame das tabelas de hosts ou repositórios semelhantes de endereços de sistemas remotos.

B) Em um ataque DDoS refletor, o atacante é capaz de implantar software zumbi em diversas máquinas distribuídas pela Internet, divididas em zumbis mestres e zumbis escravos. No ataque, o atacante coordena e

dispara os zumbis mestres, que coordenam e disparam os zumbis escravos, e esses efetivamente enviam pacotes maliciosos para os alvos.

C) No caso da identificação indevida de tráfego como intrusão por um sistema IDS, ou identificação de falsos positivos, a adoção de contramedidas rígidas, como o bloqueio do tráfego, poderá contribuir para a quebra da disponibilidade da informação que deveria fluir pela rede.

D) A técnica avançada dos sistemas antivírus conhecida como sistema digital imune permite que um programa antivírus detecte vírus polimórficos complexos e mantenha altas velocidades de varredura.

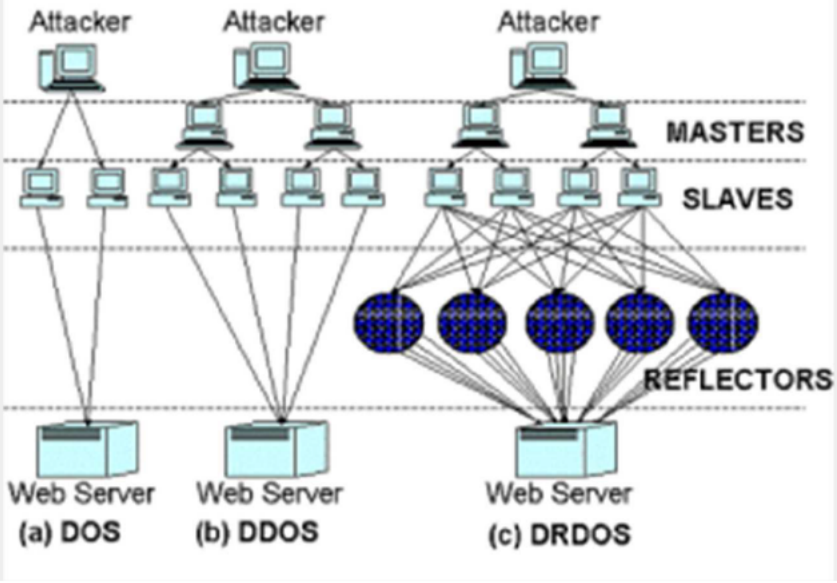
E) Os tipos mais agressivos de adware incluem os sequestradores de navegadores, que exploram fragilidades nos sistemas navegadores para baixar e instalar automaticamente códigos maliciosos de clientes para redes zumbis ou botnets.

Comentários:

Vamos aos itens:

a) O Worm simplesmente busca alcançar todos os dispositivos de rede que estão ao seu alcance. A fase de disparo está relacionado ao conceito de vírus, em que de fato ele realiza a ação maliciosa para qual foi proposto. INCORRETO

b) Pessoal, a figura abaixo nos mostra os tipos de ataque DoS, DDoS e DRDoS. Percebam que no DRDoS ou DDoS refletor, os zumbis não atacam diretamente a vítima: INCORRETO



c) Esse, de fato, é o risco de se aumentar o nível de controle em um IDS ou de se habilitar o modo de análise por comportamento. Quando se categoriza tráfegos legítimos como intrusões e aplica-se contramedidas para bloqueio do tráfego, lembrando sempre que o IDS apenas detecta e não bloqueia automaticamente como o IPS, tem-se uma prejudicialidade ao princípio da disponibilidade. CORRETO

d) Esse recurso foi criado pela IBM e symantech. Possui diversos benefícios, entretanto, detectar vírus polimórficos não é uma delas. Mais informações
em https://www.symantec.com/avcenter/reference/dis.tech.brief.pdf

INCORRETO

e) De fato os adwares mais agressivos possuem a capacidade de sequestrar e invadir navegadores. Mas seu objetivo final não é criar zumbis e inseri-los em botnets mas tão somente controlar e direcionar a navegação da vítima para áreas específicas. INCORRETO

Gabarito: C

21.CESPE – FUNPRESP/ Área 8/2016

Um ataque de XSS (cross site script) não permite a injeção de código em formulários HTTP.

Comentários:

Muito pelo contrário. A ideia do ataque é justamente injetar códigos, como o JAVASCRIPT, nas páginas e formulários, para posterior captura de dados dos usuários.

Gabarito: E

22.CESPE – FUNPRESP/ Área 8/2016

O SQL Injection caracteriza-se por permitir que, ao se fazer um POST via formulário HTTP, a codificação base64 retorne todos os comandos que um banco SQL suporte.

Comentários:

O SQL injection objetiva injetar comandos SQL em campos de entrada de dados em determinados sites ou páginas. Desse modo, quando o servidor for processar a informação enviada, como por exemplo via POST, na prática, ele vai rodar o comando SQL injetado e poderá apresentar informações indevidas, como a listagem dos usuários e senhas cadastradas no respectivo banco de dados do servidor.

Gabarito: E

CAIU na prova!

LISTA DE EXERCÍCIOS COMENTADOS COMPLEMENTARES

23.FCC – TCM-GO/Auditor de Controle Externo – Informática/2015

E-mail spoofing é uma técnica que pode ser utilizada para propagação de códigos maliciosos, envio de spam e golpes de phishing. Esta técnica consiste em

a) alterar as configurações de um servidor de e-mail para que dispare uma infinidade de e-mails falsos até encher a caixa de correio de um ou muitos usuários.

b) falsificar o protocolo SMTP para inspecionar os dados trafegados na caixa de e-mail do usuário, por meio do uso de programas específicos.

c) alterar os campos do cabeçalho de um e-mail, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.

d) efetuar buscas minuciosas no computador do usuário, com o objetivo de identificar informações sigilosas.

e) alterar os campos do protocolo SMTP, de forma que os e-mails do usuário sejam direcionados para outra conta sem que ele saiba.

Comentário:

Sempre lembrando pessoal que o termo "spoofing" está relacionado à falsificação ou adulteração da informação. No caso do email spoofing, busca-se forjar a origem de um remetente, conforme descrição no item C. Assim, posso enviar um email para uma vítima me passando pela instituição Banco do Brasil, por exemplo.

Gabarito: C

24.FCC – TJ-AP/Analista Judiciário – TI/2014

Vários computadores de uma rede estão gerando spam, disseminando vírus, atacando computadores e servidores de forma não prevista pelos administradores. Foi identificado um malware que é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados nos computadores infectados, tornando-os zumbis. Tal comportamento é tipicamente ocasionado por uma ação de

a) adware.

b) botnet.

c) keylogger.

d) spyware.

e) phishing.

Comentário:

Se temos uma rede com dispositivos controlados por um terceiro com comportamento de disseminação de malwares ou sendo utilizados para fins ilegítimos, temos claramente uma rede de zumbis, também conhecida como botnet.

Gabarito: B

25.FCC – TCE-GO/Analista de Controle Externo – TI/2014

A melhor maneira de evitar ataques de Cross-Site Scripting (XSS) em aplicações web é

a) validar adequadamente as entradas de dados dos usuários.

b) criar sessões nos processos de autenticação de usuários.

c) utilizar linguagens de programação orientadas a objeto para garantir o encapsulamento dos dados.

d) criptografar dados nas transações entre cliente e servidor.

e) utilizar, nos formulários, nomes de variáveis diferentes dos nomes dos campos da tabela do banco de dados.

Comentário:

Pessoal, vimos que o recurso de sanitização é extremamente importante na prevenção contra ataques do tipo XSS.

Gabarito: A

26.FCC – TRF – 1ªRegião/Técnico Judiciário – Informática/2014

Quando um site importante usa um único servidor web para hospedá-lo, esse servidor se torna vulnerável a ataques. Um destes ataques tenta sobrecarregar o servidor com um número muito grande de requisições HTTP coordenadas e distribuídas - utilizando um conjunto de computadores e/ou dispositivos móveis - fazendo com que o servidor não consiga responder às requisições legítimas e se torne inoperante. Este tipo de ataque é conhecido como

a) broadcast flood.

b) DDoS.

c) XSS.

d) ACK flood.

e) DoS.

Comentário:

Pessoal, se falamos de indisponibilidade via sobrecarga no servidor, falamos de negação de serviço. Entretanto, devemos buscar entender se falamos de um simples DoS, ou um ataque mais elaborado de DDoS. Assim, quando encontramos o trecho "**número muito grande de requisições HTTP coordenadas e distribuídas**" temo uma característica clássica de ataque DDoS.

Gabarito: B

27.FCC – TRT-9ª Região (PR) – Analista Judiciário – TI/2013

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 você tenta acessar um site legítimo, o seu navegador Web é redirecionado, de forma transparente, para uma página falsa. Este redirecionamento pode ocorrer:

- por meio do comprometimento do servidor de DNS do provedor que você utiliza;

- pela ação de códigos maliciosos projetados para alterar o comportamento do serviço de DNS do seu computador;

- pela ação direta de um invasor, que venha a ter acesso às configurações do serviço de DNS do seu computador ou modem de banda larga.

Este tipo de fraude é chamado de

a) Pharming.
b) Hoax.
c) Advanced Phishing.
d) Furto de Identidade.
e) Fraude de antecipação de recursos.

Comentário:

Temos então a descrição da forma de funcionamento dos ataques do tipo PHARMING.

Gabarito: A

28.FCC – TST/Analista Judiciário – TI/2012

Vírus de computador e outros programas maliciosos (Malwares) agem de diferentes formas para infectar e provocar danos em computadores. O Malware que age no computador capturando as ações e as informações do usuário é denominado

a) Cavalo de Troia.
b) Keyloggers.
c) Backdoors.
d) Spyware.
e) Worm.

Comentário:

Pessoal, lembremos sempre que o spyware possui a característica de obter informações do usuário. Lembremos do termo em inglês "spy", de espião. O Keylogger é uma especificidade de um tipo de malware capaz de obter informações na captura de dígitos de um teclado. Se considerarmos a digitação como uma ação e uma senha de usuário, também poderíamos entender que o keylogger possui as características do enunciado.

Entretanto pessoal, não vamos caçar coisas onde não existe. Vamos nos ater às palavras chaves. Em nenhum momento no enunciado foi explicitado o fato específico da captura na digitação.

Gabarito: D

29.FCC – MPE-AP/Analista Ministerial – TI/2012

Sobre o tratamento de incidentes, analise:

I. Propagação de vírus ou outros códigos maliciosos.

II. Ataques de engenharia social.

III. Modificações em um sistema, sem o conhecimento ou consentimento prévio de seu proprietário.

IV. Ocorrência de monitoramento indevido de troca de mensagens.

Constitui exemplos de incidente de segurança que deve ser reportado o que consta em:

a) I, II, III e IV.
b) I e III, apenas.
c) II e IV, apenas.
d) I e II, apenas.
e) III e IV, apenas.

Comentário:

Pessoal, todos os itens apresentados são exemplos de ações caracterizadas como maliciosas, sendo necessário o seu devido registro e identificação, para posterior tratamento por equipes especializadas.

Gabarito: A

30.FCC – MPE-AP/Analista Ministerial – TI/2012

Sobre spyware é correto afirmar:

a) Trojans são programas spyware que parecem ser apenas cartões virtuais animados, álbuns de fotos, jogos ou protetores de tela e que são instalados automaticamente no computador do usuário com o objetivo de obter informações digitadas por meio do teclado físico ou virtual.
b) Adware é um programa spyware projetado especificamente para apresentar propagandas. É usado apenas para fins legítimos, incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos.
c) São softwares exclusivamente de uso malicioso projetados para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Executam ações que podem comprometer a privacidade do usuário e a segurança do computador.

d) Keylogger é um programa spyware capaz de capturar e armazenar as teclas digitadas pelo usuário. Sua ativação não pode ser condicionada a uma ação prévia do usuário, como o acesso a um site de Internet Banking.

e) Screenlogger é um tipo de spyware capaz de armazenar a posição do cursor e a tela apresentada no monitor nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais.

Comentário:

Vamos comentar os itens:

a) Trojans não são spywares. São programas específicos criados para invasão de um sistema e distribuição de outros códigos maliciosos no ambiente da vítima. INCORRETO.
b) O uso de Adware não se restringe ao modo legítimo, tendo seu uso de forma maliciosa bastante explorado. INCORRETO
c) Os spywares podem ter seu uso de forma maliciosa e legítima também, conforme vimos em teoria. INCORRETO
d) A ativação do keylogger pode sim ser disparada a partir de eventos específicos. Assim, não há necessidade de se monitorar toda e qualquer inserção de dados por parte do usuário, mas tão somente aqueles dados que possam conter dados sigilosos, como no momento de acesso a uma página de banco ou email. INCORRETO

Nos resta então a alternativa E que descreve a característica do screenlogger de forma correta.

Gabarito: E

31.FCC – MPE-AP/Técnico Ministerial – Informática/2012

Ataques desse tipo buscam explorar a falta de tratamento dos dados de uma entrada do sistema. Desta maneira tenta-se injetar strings maiores que as permitidas com o objetivo de invadir certas áreas da memória. Este ataque permite inclusive injetar aplicações na máquina invadida, como backdoors, trojans e sistemas de controle remoto, como o VNC.

O texto fala do ataque de

a) SYN Flood.
b) Escala de Privilégios.
c) Buffer Overflow.
d) ARP Cache Poising.
e) RIP Spoofing.

Comentário:
Vimos que o tipo de ataque Buffer Overflow pode ser utilizado para duas finalidades. A primeira é para gerar indisponibilidade e a segunda, para acessar áreas indevidas da memória dos sistemas.

Gabarito: C

32.FCC – TCE-CE/Analista de Controle Externo – Auditoria de TI/2015

Após o exame no computador do funcionário de uma instituição foi detectada sua participação em um ataque de DDoS sem seu conhecimento, em que seu computador atuava como um "zumbi", controlado remotamente por um atacante. Isso ocorreu porque o computador estava infectado por
A) adware.
B) rootkit.
C) bot.
D) spyware.
E) trojan.

Comentário:
Pessoal, questão bem tranquila, certo? Vimos que os computadores zumbis estão sujeitos ao malware do tipo BOT. Assim, podem ser controlados remotamente para disparar ataques de forma descentralizada.

Gabarito: C

33.TRT – 14ª Região (RO e AC)/Analista Judiciário – TI/2011

Analise as seguintes características de software:

I. Especificamente projetado para apresentar propagandas, quer por intermédio de um browser quer por meio de algum outro programa instalado.
II. Monitorar atividades de um sistema e enviar as informações coletadas para terceiros.

De acordo com cgi.br, I e II são tipos de software categorizados, respectivamente, como
A) trojan e worm.
B) adware e worm.
C) adware e spyware.
D) spyware e trojan.
E) phishing e spam.

Comentário:
Temos algumas palavras chaves aí, certo pessoal? Falou em propaganda, estamos falando de ADWARE.

E, conforme vimos, o malware responsável por monitorar as ações dos usuários, podendo atuar de forma lícita e ilícita é o spyware, ok?

Gabarito: C

34.FCC – TRT – 5ª Região (BA)/Analista Judiciário – TI/2013

Um site de segurança publicou uma notícia informando sobre um tipo de e-mail falso que vem atacando as redes sociais. Trata-se de um falso aviso de segurança informando que a conta será bloqueada caso não seja atualizada. Com aparência semelhante à do Facebook, este tipo de e-mail oferece um link para que a pessoa acesse uma página da rede social para iniciar o processo de atualização dos dados. Na verdade, o que ocorre ao clicar no link é a instalação de um spyware, capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador.

O spyware capaz de realizar o que está sublinhado no texto, de acordo com a cartilha de segurança para internet do CERT.BR, é denominado:
A) Adware.
B) Keylogger.
C) Rootkit.
D) Bot.
E) Trojan.

Comentário:
Vimos em nossa aula que o spyware pode utilizar diversas ferramentas e malwares complementares com vistas a obter mais informações dos usuários infectados.

Como dois exemplos básicos, podemos citar o Keylogger, que vai monitorar e capturar todas as teclas pressionadas pelo usuário; e o Screenlogger, que é capaz de capturar a tela do usuário.

Gabarito: B

35.FCC – TCE-GO/Analista de Controle Externo – TI/2014

Ao tentar entrar em alguns sites de comércio eletrônico para comprar produtos de seu interesse, Maria percebeu que estava sendo redirecionada para sites muito semelhantes aos verdadeiros, mas que não ofereciam conexão segura, nem certificado digital. Pela característica do problema, é mais provável que Maria esteja sendo vítima de
A) vírus.
B) worm.
C) trojan.
D) backdoor.
E) pharming.

Comentário:
Vimos que o Pharming exerce exatamente a função descrita no enunciado. Há de se mencionar que sites falsos não possuirão as informações de certificação digital dos sites originais. Assim, para validarmos os acessos em caso de dúvidas, é altamente recomendável que

se verifique as informações contidas no certificado utilizado para validação do site.

O cenário apresentado pode acontecer pelo simplesmente comprometimento do servidor DNS da rede que faz um redirecionamento local, a configuração local do DNS em sua máquina ou de um servidor DNS na rede responsável por divulgar o endereço IP responsável pelo nome de domínio em questão.

Gabarito: E

36.FCC – TCE-SP/Agente da Fiscalização Financeira – Conhecimento Básicos/2010

Mensagem não solicitada e mascarada sob comunicação de alguma instituição conhecida e que pode induzir o internauta ao acesso a páginas fraudulentas, projetadas para o furto de dados pessoais ou financeiros do usuário. Trata-se especificamente de
A) keylogger.
B) scanning.
C) botnet.
D) phishing.
E) rootkit.

Comentário:
E agora sim temos a descrição padrão da ação de um phishing comum.

Gabarito: D

37.FCC – TRE-RR/Analista Judiciário – Análise de Sistemas/2015

Rootkits exploram vulnerabilidades do sistema operacional de um computador e são usados para
A) transformar um computador em zumbi.
B) criar uma conta anônima de e-mail para enviar spam.
C) substituir a página inicial de navegação por uma página de propaganda forçada.

D) esconder e assegurar a presença de invasor ou de malware em um computador comprometido.
E) capturar imagens da tela e de caracteres digitados no teclado do computador

Comentário:
Vimos que os ROOTKITS são um conjunto de programas e técnicas que buscam esconder e garantir a presença do invasor ou de outro código malicioso. Assim, a detecção de malwares em uma vítima de ROOTKIT pode ser mais complicado.

Gabarito: D

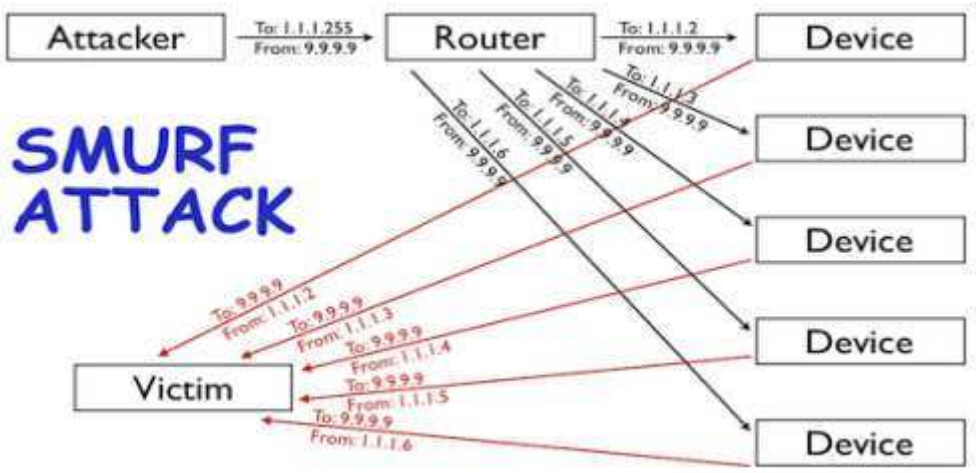
38.FCC – TRF 3ª Região (SP MS)/Analista Judiciário – Informática/2014

Qualquer ataque planejado para fazer uma máquina ou software ficar indisponível e incapaz de executar sua funcionalidade básica é conhecido como ataque de negação de serviço (Denial of Service − DOS). Há diversos tipos de ataque DOS sendo que, um deles, tira vantagem de redes mal configuradas que possuem um endereço de difusão (broadcast) pelo qual o usuário pode enviar um pacote que é recebido por todos os endereços IP da rede. Este tipo de ataque explora esta propriedade enviando pacotes ICMP com um endereço fonte configurado para o alvo e com um endereço destino configurado para o endereço de difusão da rede.

O tipo de ataque descrito acima é conhecido como
A) sniffing.
B) inundação por SYN.
C) ACK TCP.
D) smurf.
E) falsificação de IP.

Comentário:
Vimos que ataques DDoS que utilizam o redirecionamento de tráfego ICMP a partir de redes que permitem o tráfego de broadcast são

chamados de SMURFS. Para lembrarmos o modelo, vamos verificar a figura abaixo:



Gabarito: D

39.FCC – TRT – 15ª Região (Campinas-SP)/Técnico Judiciário – TI/2015

O usuário de um computador conectado à internet está se queixando que, repentinamente, começaram a aparecer janelas com anúncios na tela do computador. Considerando a possibilidade de que um malware está atacando o computador do usuário, o sintoma relatado aparenta ser a ação de um malware do tipo

A) Rootkit.
B) Backdoor.
C) Adware.
D) Botnet.
E) Spyware.

Comentário:

Mais uma vez pessoal, temos aí o termo de anúncios ou propaganda. Isso nos leva então ao malware do tipo Adware, certo?

Gabarito: C

40.FCC – TRT – 15ª Região (Campinas-SP)/Técnico Judiciário – TI/2015

Sobre um programa de código malicioso − malware, considere:

I. É notadamente responsável por consumir muitos recursos devido à grande quantidade de cópias de si mesmo que costuma propagar e, como consequência, pode afetar o desempenho de redes e a utilização de computadores.
II. Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.
III. Diferente do vírus, não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores.

Os itens I, II e III tratam de características de um
A) Trojan Proxy.
B) Keylogger.
C) Scan.
D) Worm.
E) Spoofing.

Comentário:
Pessoal, vimos essas características para o WORM certo? Inclusive, a questão nos traz essa revisão das principais diferenças em relação ao vírus.

Gabarito: D

41.FCC – TRT – 15ª Região (Campinas-SP)/Técnico Judiciário – TI/2015

Considere, abaixo, as células assinaladas por um tique, como características de códigos maliciosos.

Como é obtido:	*Vírus*	*Bot*	*Spyware*	I.	II.
Recebido automaticamente pela rede		✔			
Recebido por *e-mail*	✔	✔	✔		
Baixado de *sites* na Internet	✔	✔	✔		
Inserido por um invasor		✔	✔	✔	✔
Ação de outro código malicioso		✔	✔	✔	✔
Como ocorre a instalação:					
Via execução de outro código malicioso				✔	✔
Exploração de vulnerabilidades		✔		✔	✔
Ações maliciosas mais comuns:					
Altera e/ou remove arquivos	✔				✔
Instala outros códigos maliciosos		✔			✔
Possibilita o retorno do invasor				✔	✔

Imagem da Questão
Neste caso, I e II correspondem, correta e respectivamente a
A) Rootkit e Backdoor.
B) Rootkit e Trojan.
C) Trojan e Rootkit.
D) Backdoor e Rootkit.
E) Trojan e Backdoor.

Comentário:

Tabela retirada da cartilha do cert.bt. O perigo aqui está em considerar o Trojan nas alternativas. O trojan pessoal não busca explorar vulnerabilidades e ser executado a partir de outro código. Ele é o responsável por realizar tais funções para outros códigos, como o backdoor e o Rootkit.

Uma outra observação seria na diferença então do Rootkit e do backdoor. Vale lembrar que o backdoor tem como objetivo tão somente permitir a volta do atacante à máquina da vítima, enquanto o Rootkit, implementa outros recursos com vistas a esconder os malwares ali inseridos, tomar ações a nível de administrador, entre outros.

Gabarito: D

42.FCC – TRT – 13ª Região (PB)/Analista Judiciário – TI/2014

Atualmente existem inúmeras formas pelas quais os malwares (software malicioso) se disseminam e atuam. Por exemplo, o tipo de malware conhecido como Worms é caracterizado

A) pela exibição de anúncios na tela do computador sem autorização.

B) por monitorar as atividades de um sistema e enviar os dados coletados, por meio da rede, para utilização fraudulenta.

C) pela capacidade de se propagar, automaticamente, por meio de redes, enviando cópias de si para outros computadores.

D) pela utilização das falhas no sistema operacional para obter o controle do equipamento infectado.

E) por monitorar as ações de digitação realizada pelos usuários do computador infectado.

Comentário:

Mais uma questão bem simples e objetiva a respeito das características do WORM, certo pessoal?

Apenas observando os demais temos:

a) ADWARE
b) SPYWARE
d) Malwares em um caráter geral
e) KEYLOGGER

Gabarito: C

43.FCC – MPE-CE/Analista Ministerial – Ciências da Computação/2013

Há diferentes tipos de vírus. Alguns procuram permanecer ocultos, infectando arquivos do disco e executando uma série de atividades sem o conhecimento do usuário. Há outros que permanecem inativos durante certos períodos, entrando em atividade apenas em datas específicas. Alguns dos tipos de vírus mais comuns são apresentados nas afirmativas abaixo. Assinale o que NÃO se trata de um vírus.

A) Propaga-se de celular para celular por meio de bluetooth ou de mensagens MMS. A infecção ocorre quando um usuário permite o recebimento de um arquivo infectado e o executa. Após infectar o celular, pode destruir ou sobrescrever arquivos, remover ou transmitir contatos da agenda, efetuar ligações telefônicas e drenar a carga da bateria.

B) Recebido como um arquivo anexo a um e-mail, que tenta induzir o usuário a clicar sobre este arquivo para que seja executado. Quando entra em ação, infecta arquivos e programas e envia cópias de si mesmo para os e-mails encontrados nas listas de contatos gravadas no computador.

C) Escrito em linguagem de script, recebido ao acessar uma página web ou por e-mail, como um arquivo anexo ou parte do próprio e-mail escrito em HTML. Pode ser automaticamente executado, dependendo da configuração do browser e do leitor de e-mails do usuário.

D) Escrito em linguagem de macro e tenta infectar arquivos manipulados por aplicativos que utilizam esta linguagem como, por exemplo, os que compõem o Microsoft Office.

E) Após infectar um computador, tenta se propagar e continuar o processo de infecção. Para isso, necessita identificar os computadores alvos para os quais tentará se copiar, o que pode ser feito efetuando uma varredura na rede e identificando os computadores ativos.

Comentário:
Questão retirada mais uma vez dos exemplos apresentados de tipos de Virus na cartilha do Cert.br.

Assim, temos para cada item:

a) Virus de Celular;
b) Virus de e-mail;
c) Virus de Script;
d) Virus de Macro

O último item nos traz a propagação via rede, que é uma característica de WORM e não vírus.

Gabarito: E

44.FCC – TRT -14ª Região (RO e AC)/Analista Judiciário – TI/2016

Um atacante introduziu um dispositivo em uma rede para induzir usuários a se conectarem a este dispositivo, ao invés do dispositivo legítimo, e conseguiu capturar senhas de acesso e diversas informações que por ele trafegaram. A rede sofreu um ataque de
(A) varredura.
(B) interceptação de tráfego.
(C) negação de serviço.
(D) força bruta.
(E) personificação.

Comentário:
Trecho extraído diretamente da cartilha do cert.br, no link a seguir.
http://cartilha.cert.br/redes/

Ataque de personificação: um atacante pode introduzir ou substituir um dispositivo de rede para induzir outros a se conectarem a este, ao invés do dispositivo legítimo, permitindo a captura de senhas de acesso e informações que por ele passem a trafegar.

Gabarito: E

Chegamos ao término da nossa aula de hoje pessoal!

Um grande abraço e até a próxima aula.

Facebook: *André Castro (Professor):*
https://www.facebook.com/ProfessorAndreCastro/
https://www.facebook.com/profile.php?id=100010923731255

Twitter e Periscope: *@andrehsc*

CAIU na prova!

LISTA DE EXERCÍCIOS

1. CESPE – STJ/Analista Judiciário – Suporte em TI/2015

Uma vez que a varredura simples de portas é facilmente detectada por firewalls, outros tipos de mensagens passaram a ser utilizadas para mapeamento de serviços de redes, como por exemplo, as de RESET e as de SYN-ACK, que sinalizariam tentativa legítima de conexão, e, ainda, pacotes de resposta DNS (domain name system), que são respostas a mensagens geradas internamente.

---

2. CESPE – ANTAQ/Analista administrativo – Infra de TI/2014

Em um ataque de DDoS, que objetiva deixar inacessível o recurso computacional para os usuários legítimos, um computador mestre controla milhares de computadores zumbis que acessam um sistema ao mesmo tempo (um servidor web, por exemplo), com o objetivo de esgotar seus recursos.

---

3. CESPE – ANTAQ/Analista administrativo – Infra de TI/2014

O ataque de spear phishing, que é uma tentativa de fraude por falsificação de email, tem como alvo uma organização específica e objetiva, normalmente, conseguir acesso não autorizado a dados sigilosos.

---

4. **CESPE – TC-DF/Analista de Administração Pública – Sistemas de TI/2014**

Utilizado para a captura ilegal de informações de uma máquina em rede, o spoofing analisa o tráfego da rede e coleta dados sigilosos como senhas e endereços

---

5. **CESPE – MPU/Analista – Suporte e Infraestrutura/2013**

O combate à contaminação por um worm pode ser realizada por meio da utilização de antivírus no computador que se deseja proteger

---

6. **CESPE – MPOG/Técnico de Nível Superior/2013**

Ataques de negação de serviço volumétricos, distribuídos ou não, envolvem flooding para esgotamento de recursos e spoofing para dificultar o rastreamento da origem.

---

7. **CESPE – SERPRO/Analista de Desenvolvimento/2013**

Um ataque à infraestrutura de conectividade de um banco à Internet, interrompendo o acesso a seus serviços de home banking, afeta a disponibilidade.

---

8. **CESPE – INPI/Analista de Planejamento – Infraestrutura de TI/2013**

Worm é um programa que possui código malicioso, capaz de se disseminar, por meio de uma rede, para vários computadores.

---

9. **CESPE – INPI/Analista de Planejamento – Infraestrutura de TI/2013**

A principal atividade de programas com códigos maliciosos e que funcionam na função de keylogger é apresentar propagandas não solicitadas pelo usuário, direcionando-o a sítios maliciosos.

---

10. **CESPE – INPI/Analista de Planejamento – Infraestrutura de TI/2013**

Um spyware pode ser utilizado de forma legítima ou maliciosa, pois sua função é monitorar atividades de um sistema, além de coletar e enviar informações a terceiros.

11.CESPE – INPI/Analista de Planejamento – Infraestrutura de TI/2013

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.

12.CESPE – TJ-AC/Técnico Judiciário – Informática/2012

O funcionamento de um computador que tenha sofrido um ataque conhecido como phishing pode ser comprometido, sendo os dados gravados nesse computador armazenados em um disco corrompido.

13.CESPE – TJ-AC/Técnico Judiciário – Informática/2012

Os bots e os worms são tipos de programas maliciosos que se propagam enviando cópias de si mesmos pela rede de computadores.

14.CESPE – TJ-AC/Técnico Judiciário – Informática/2012

Computadores conectados à Internet e infectados por bots são vulneráveis, estando sujeitos ao controle de criminosos que podem comandar um ataque de negação de serviço.

15.CESPE – TJ-AC/Técnico Judiciário – Informática/2012

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

16.CESPE – TJ-AC/Técnico Judiciário – Informática/2012

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

17.CESPE – TJ-AC/Técnico Judiciário – Informática/2012

A atualização automática on-line do sistema operacional é uma prática que garante que o computador não sofrerá infecção por bots.

18.CESPE – TJ-AC/Técnico Judiciário – Informática/2012

Por serem de difícil detecção, os worms só podem ser combatidos por ferramentas específicas para esse fim, que se denominam antiworms.

19.CESPE – TJ-AC/Técnico Judiciário – Informática/2012

O uso de programas antivírus continuamente atualizados é uma prática suficiente para se evitar que um worm contamine um computador.

20.CESPE – TRE/RS / Analista Judiciário/2015

Acerca de sistemas de segurança, ataques e malwares, assinale a opção correta.

A) A fase de disparo de um verme ou worm é caracterizada pela busca de outros sistemas para infectar, por meio de exame das tabelas de hosts ou repositórios semelhantes de endereços de sistemas remotos.

B) Em um ataque DDoS refletor, o atacante é capaz de implantar software zumbi em diversas máquinas distribuídas pela Internet, divididas em zumbis mestres e zumbis escravos. No ataque, o atacante coordena e dispara os zumbis mestres, que coordenam e disparam os zumbis escravos, e esses efetivamente enviam pacotes maliciosos para os alvos.

C) No caso da identificação indevida de tráfego como intrusão por um sistema IDS, ou identificação de falsos positivos, a adoção de contramedidas rígidas, como o bloqueio do tráfego, poderá contribuir para a quebra da disponibilidade da informação que deveria fluir pela rede.

D) A técnica avançada dos sistemas antivírus conhecida como sistema digital imune permite que um programa antivírus detecte vírus polimórficos complexos e mantenha altas velocidades de varredura.

E) Os tipos mais agressivos de adware incluem os sequestradores de navegadores, que exploram fragilidades nos sistemas navegadores para baixar e instalar automaticamente códigos maliciosos de clientes para redes zumbis ou botnets.

21.CESPE – FUNPRESP/ Área 8/2016

Um ataque de XSS (cross site script) não permite a injeção de código em formulários HTTP.

22.CESPE – FUNPRESP/ Área 8/2016

O SQL Injection caracteriza-se por permitir que, ao se fazer um POST via formulário HTTP, a codificação base64 retorne todos os comandos que um banco SQL suporte.

LISTA DE EXERCÍCIOS COMPLEMENTARES

23.FCC – TCM-GO/Auditor de Controle Externo – Informática/2015

E-mail spoofing é uma técnica que pode ser utilizada para propagação de códigos maliciosos, envio de spam e golpes de phishing. Esta técnica consiste em

a) alterar as configurações de um servidor de e-mail para que dispare uma infinidade de e-mails falsos até encher a caixa de correio de um ou muitos usuários.

b) falsificar o protocolo SMTP para inspecionar os dados trafegados na caixa de e-mail do usuário, por meio do uso de programas específicos.

c) alterar os campos do cabeçalho de um e-mail, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.

d) efetuar buscas minuciosas no computador do usuário, com o objetivo de identificar informações sigilosas.

e) alterar os campos do protocolo SMTP, de forma que os e-mails do usuário sejam direcionados para outra conta sem que ele saiba.

24.FCC – TJ-AP/Analista Judiciário – TI/2014

Vários computadores de uma rede estão gerando spam, disseminando vírus, atacando computadores e servidores de forma não prevista pelos administradores. Foi identificado um malware que é capaz de se propagar

automaticamente, explorando vulnerabilidades existentes em programas instalados nos computadores infectados, tornando-os zumbis. Tal comportamento é tipicamente ocasionado por uma ação de

a) adware.
b) botnet.
c) keylogger.
d) spyware.
e) phishing.

25.FCC – TCE-GO/Analista de Controle Externo – TI/2014

A melhor maneira de evitar ataques de Cross-Site Scripting (XSS) em aplicações web é

a) validar adequadamente as entradas de dados dos usuários.
b) criar sessões nos processos de autenticação de usuários.
c) utilizar linguagens de programação orientadas a objeto para garantir o encapsulamento dos dados.
d) criptografar dados nas transações entre cliente e servidor.
e) utilizar, nos formulários, nomes de variáveis diferentes dos nomes dos campos da tabela do banco de dados.

26.FCC – TRF – 1ªRegião/Técnico Judiciário – Informática/2014

Quando um site importante usa um único servidor web para hospedá-lo, esse servidor se torna vulnerável a ataques. Um destes ataques tenta sobrecarregar o servidor com um número muito grande de requisições HTTP coordenadas e distribuídas - utilizando um conjunto de computadores e/ou dispositivos móveis - fazendo com que o servidor não consiga responder às requisições legítimas e se torne inoperante. Este tipo de ataque é conhecido como

a) broadcast flood.
b) DDoS.
c) XSS.
d) ACK flood.
e) DoS.

27.FCC – TRT-9ª Região (PR) – Analista Judiciário – TI/2013

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 você tenta acessar um site legítimo, o seu navegador Web é redirecionado, de forma transparente, para uma página falsa. Este redirecionamento pode ocorrer:

- por meio do comprometimento do servidor de DNS do provedor que você utiliza;

- pela ação de códigos maliciosos projetados para alterar o comportamento do serviço de DNS do seu computador;

- pela ação direta de um invasor, que venha a ter acesso às configurações do serviço de DNS do seu computador ou modem de banda larga.

Este tipo de fraude é chamado de
a) Pharming.
b) Hoax.
c) Advanced Phishing.
d) Furto de Identidade.
e) Fraude de antecipação de recursos.

28.FCC – TST/Analista Judiciário – TI/2012

Vírus de computador e outros programas maliciosos (Malwares) agem de diferentes formas para infectar e provocar danos em computadores. O Malware que age no computador capturando as ações e as informações do usuário é denominado
a) Cavalo de Troia.
b) Keyloggers.
c) Backdoors.
d) Spyware.
e) Worm.

29.FCC – MPE-AP/Analista Ministerial – TI/2012

Sobre o tratamento de incidentes, analise:

I. Propagação de vírus ou outros códigos maliciosos.

II. Ataques de engenharia social.

III. Modificações em um sistema, sem o conhecimento ou consentimento prévio de seu proprietário.

IV. Ocorrência de monitoramento indevido de troca de mensagens.

Constitui exemplos de incidente de segurança que deve ser reportado o que consta em:
a) I, II, III e IV.
b) I e III, apenas.
c) II e IV, apenas.
d) I e II, apenas.
e) III e IV, apenas.

30.FCC – MPE-AP/Analista Ministerial – TI/2012

Sobre spyware é correto afirmar:

a) Trojans são programas spyware que parecem ser apenas cartões virtuais animados, álbuns de fotos, jogos ou protetores de tela e que são instalados automaticamente no computador do usuário com o objetivo de obter informações digitadas por meio do teclado físico ou virtual.
b) Adware é um programa spyware projetado especificamente para apresentar propagandas. É usado apenas para fins legítimos, incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos.
c) São softwares exclusivamente de uso malicioso projetados para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Executam ações que podem comprometer a privacidade do usuário e a segurança do computador.
d) Keylogger é um programa spyware capaz de capturar e armazenar as teclas digitadas pelo usuário. Sua ativação não pode ser condicionada a uma ação prévia do usuário, como o acesso a um site de Internet Banking.

e) Screenlogger é um tipo de spyware capaz de armazenar a posição do cursor e a tela apresentada no monitor nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais.

31.FCC – MPE-AP/Técnico Ministerial – Informática/2012

Ataques desse tipo buscam explorar a falta de tratamento dos dados de uma entrada do sistema. Desta maneira tenta-se injetar strings maiores que as permitidas com o objetivo de invadir certas áreas da memória. Este ataque permite inclusive injetar aplicações na máquina invadida, como backdoors, trojans e sistemas de controle remoto, como o VNC.

O texto fala do ataque de

a) SYN Flood.
b) Escala de Privilégios.
c) Buffer Overflow.
d) ARP Cache Poising.
e) RIP Spoofing.

32.FCC – TCE-CE/Analista de Controle Externo – Auditoria de TI/2015

Após o exame no computador do funcionário de uma instituição foi detectada sua participação em um ataque de DDoS sem seu conhecimento, em que seu computador atuava como um "zumbi", controlado remotamente por um atacante. Isso ocorreu porque o computador estava infectado por
A) adware.
B) rootkit.
C) bot.
D) spyware.
E) trojan.

33.TRT – 14ª Região (RO e AC)/Analista Judiciário – TI/2011

Analise as seguintes características de software:

I. Especificamente projetado para apresentar propagandas, quer por intermédio de um browser quer por meio de algum outro programa instalado.
II. Monitorar atividades de um sistema e enviar as informações coletadas para terceiros.

De acordo com cgi.br, I e II são tipos de software categorizados, respectivamente, como
A) trojan e worm.
B) adware e worm.
C) adware e spyware.
D) spyware e trojan.
E) phishing e spam.

34.FCC – TRT – 5ª Região (BA)/Analista Judiciário – TI/2013

Um site de segurança publicou uma notícia informando sobre um tipo de e-mail falso que vem atacando as redes sociais. Trata-se de um falso aviso de segurança informando que a conta será bloqueada caso não seja atualizada. Com aparência semelhante à do Facebook, este tipo de e-mail oferece um link para que a pessoa acesse uma página da rede social para iniciar o processo de atualização dos dados. Na verdade, o que ocorre ao clicar no link é a instalação de um spyware, capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador.

O spyware capaz de realizar o que está sublinhado no texto, de acordo com a cartilha de segurança para internet do CERT.BR, é denominado:
A) Adware.
B) Keylogger.
C) Rootkit.
D) Bot.
E) Trojan.

35.FCC – TCE-GO/Analista de Controle Externo – TI/2014

Ao tentar entrar em alguns sites de comércio eletrônico para comprar produtos de seu interesse, Maria percebeu que estava sendo redirecionada

para sites muito semelhantes aos verdadeiros, mas que não ofereciam conexão segura, nem certificado digital. Pela característica do problema, é mais provável que Maria esteja sendo vítima de
A) vírus.
B) worm.
C) trojan.
D) backdoor.
E) pharming.

36.FCC – TCE-SP/Agente da Fiscalização Financeira – Conhecimento Básicos/2010

Mensagem não solicitada e mascarada sob comunicação de alguma instituição conhecida e que pode induzir o internauta ao acesso a páginas fraudulentas, projetadas para o furto de dados pessoais ou financeiros do usuário. Trata-se especificamente de
A) keylogger.
B) scanning.
C) botnet.
D) phishing.
E) rootkit.

37.FCC – TRE-RR/Analista Judiciário – Análise de Sistemas/2015

Rootkits exploram vulnerabilidades do sistema operacional de um computador e são usados para
A) transformar um computador em zumbi.
B) criar uma conta anônima de e-mail para enviar spam.
C) substituir a página inicial de navegação por uma página de propaganda forçada.
D) esconder e assegurar a presença de invasor ou de malware em um computador comprometido.
E) capturar imagens da tela e de caracteres digitados no teclado do computador.

38.FCC – TRF 3ª Região (SP MS)/Analista Judiciário – Informática/2014

Qualquer ataque planejado para fazer uma máquina ou software ficar indisponível e incapaz de executar sua funcionalidade básica é conhecido como ataque de negação de serviço (Denial of Service − DOS). Há diversos tipos de ataque DOS sendo que, um deles, tira vantagem de redes mal configuradas que possuem um endereço de difusão (broadcast) pelo qual o usuário pode enviar um pacote que é recebido por todos os endereços IP da rede. Este tipo de ataque explora esta propriedade enviando pacotes ICMP com um endereço fonte configurado para o alvo e com um endereço destino configurado para o endereço de difusão da rede.

O tipo de ataque descrito acima é conhecido como
A) sniffing.
B) inundação por SYN.
C) ACK TCP.
D) smurf.
E) falsificação de IP.

39.FCC – TRT – 15ª Região (Campinas-SP)/Técnico Judiciário – TI/2015

O usuário de um computador conectado à internet está se queixando que, repentinamente, começaram a aparecer janelas com anúncios na tela do computador. Considerando a possibilidade de que um malware está atacando o computador do usuário, o sintoma relatado aparenta ser a ação de um malware do tipo
A) Rootkit.
B) Backdoor.
C) Adware.
D) Botnet.
E) Spyware.

40.FCC – TRT – 15ª Região (Campinas-SP)/Técnico Judiciário – TI/2015

Sobre um programa de código malicioso − malware, considere:

I. É notadamente responsável por consumir muitos recursos devido à grande quantidade de cópias de si mesmo que costuma propagar e, como

consequência, pode afetar o desempenho de redes e a utilização de computadores.
II. Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.
III. Diferente do vírus, não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores.

Os itens I, II e III tratam de características de um
A) Trojan Proxy.
B) Keylogger.
C) Scan.
D) Worm.
E) Spoofing.

---

41. FCC – TRT – 15ª Região (Campinas-SP)/Técnico Judiciário – TI/2015

Considere, abaixo, as células assinaladas por um tique, como características de códigos maliciosos.

Como é obtido:	*Vírus*	*Bot*	*Spyware*	I.	II.
Recebido automaticamente pela rede		✔			
Recebido por *e-mail*	✔	✔	✔		
Baixado de *sites* na Internet	✔	✔	✔		
Inserido por um invasor		✔	✔	✔	✔
Ação de outro código malicioso		✔	✔	✔	✔
Como ocorre a instalação:					
Via execução de outro código malicioso				✔	✔
Exploração de vulnerabilidades		✔		✔	✔
Ações maliciosas mais comuns:					
Altera e/ou remove arquivos	✔				✔
Instala outros códigos maliciosos		✔			✔
Possibilita o retorno do invasor				✔	✔

Imagem da Questão

Neste caso, I e II correspondem, correta e respectivamente a
A) Rootkit e Backdoor.
B) Rootkit e Trojan.
C) Trojan e Rootkit.
D) Backdoor e Rootkit.
E) Trojan e Backdoor.

42.FCC – TRT – 13ª Região (PB)/Analista Judiciário – TI/2014

Atualmente existem inúmeras formas pelas quais os malwares (software malicioso) se disseminam e atuam. Por exemplo, o tipo de malware conhecido como Worms é caracterizado
A) pela exibição de anúncios na tela do computador sem autorização.
B) por monitorar as atividades de um sistema e enviar os dados coletados, por meio da rede, para utilização fraudulenta.
C) pela capacidade de se propagar, automaticamente, por meio de redes, enviando cópias de si para outros computadores.
D) pela utilização das falhas no sistema operacional para obter o controle do equipamento infectado.
E) por monitorar as ações de digitação realizada pelos usuários do computador infectado.

43.FCC – MPE-CE/Analista Ministerial – Ciências da Computação/2013

Há diferentes tipos de vírus. Alguns procuram permanecer ocultos, infectando arquivos do disco e executando uma série de atividades sem o conhecimento do usuário. Há outros que permanecem inativos durante certos períodos, entrando em atividade apenas em datas específicas. Alguns dos tipos de vírus mais comuns são apresentados nas afirmativas abaixo. Assinale o que NÃO se trata de um vírus.

A) Propaga-se de celular para celular por meio de bluetooth ou de mensagens MMS. A infecção ocorre quando um usuário permite o recebimento de um arquivo infectado e o executa. Após infectar o celular, pode destruir ou sobrescrever arquivos, remover ou transmitir contatos da agenda, efetuar ligações telefônicas e drenar a carga da bateria.

B) Recebido como um arquivo anexo a um e-mail, que tenta induzir o usuário a clicar sobre este arquivo para que seja executado. Quando entra em ação, infecta arquivos e programas e envia cópias de si mesmo para os e-mails encontrados nas listas de contatos gravadas no computador.

C) Escrito em linguagem de script, recebido ao acessar uma página web ou por e-mail, como um arquivo anexo ou parte do próprio e-mail escrito em HTML. Pode ser automaticamente executado, dependendo da configuração do browser e do leitor de e-mails do usuário.

D) Escrito em linguagem de macro e tenta infectar arquivos manipulados por aplicativos que utilizam esta linguagem como, por exemplo, os que compõem o Microsoft Office.

E) Após infectar um computador, tenta se propagar e continuar o processo de infecção. Para isso, necessita identificar os computadores alvos para os quais tentará se copiar, o que pode ser feito efetuando uma varredura na rede e identificando os computadores ativos.

44.FCC – TRT -14ª Região (RO e AC)/Analista Judiciário – TI/2016

Um atacante introduziu um dispositivo em uma rede para induzir usuários a se conectarem a este dispositivo, ao invés do dispositivo legítimo, e conseguiu capturar senhas de acesso e diversas informações que por ele trafegaram. A rede sofreu um ataque de
(A) varredura.
(B) interceptação de tráfego.
(C) negação de serviço.
(D) força bruta.
(E) personificação.

Facebook: André Castro (Professor)
Twitter e Periscope: @andrehsc

GABARITO

1	2	3	4	5	6	7	8	9	10
C	C	C	E	C	C	C	C	E	C
11	12	13	14	15	16	17	18	19	20
C	E	C	C	C	C	E	E	E	C
21	22	23	24	25	26	27	28	29	30
E	E	C	B	A	B	A	D	A	E
31	32	33	34	35	36	37	38	39	40
C	C	C	B	E	D	D	D	C	D
41	42	43	44	45	46	47	48	49	50
D	C	E	E						