SEGURANÇA DA INFORMAÇÃO VI

DIRETO DO CONCURSO

17. (2024/INSTITUTO VERBENA/TJ AC/ ANALISTA JUDICIÁRIO) Os princípios básicos da segurança da informação são a confidencialidade, a disponibilidade, a integridade e a irretratabilidade. Quais são técnicas utilizadas para se implementar respectivamente os referidos princípios?

a. Backup, criptografia, assinatura digital e hashing.
b. Hashing, assinatura digital, backup e criptografia.
c. Criptografia, backup, hashing e assinatura digital.
d. Assinatura digital, hashing, criptografia e backup.

a. O backup se baseia na cópia de segurança, garantindo a disponibilidade. Já a criptografia não garante disponibilidade.
b. O hashing garante a integridade. A assinatura digital não garante a disponibilidade.
c. A assinatura digital não garante a confidencialidade.

18. (2024/CEBRASPE/CNPq ANALISTA/GESTÃO DE DADOS CORPORATIVOS) Hash é um método criptográfico que, quando aplicado sobre uma informação, gera um resultado único e de tamanho fixo, independentemente do tamanho da informação.

MALWARE

Os malwares, junção de "malicious" e "software" em inglês, são programas maliciosos.

Obs.: é importante que o candidato leia as cartilhas do CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil). É possível encontrá-las em: CET.br/NIC.br

PRINCIPAIS MALWARES

SPYWARE

Spywares são programas espiões que coletam dados indevidamente dados da máquina e os enviam para o atacante.

5m

- Screenlogger: captura imagens da tela por completo ou apenas locais específicos. Do inglês, “screen” (tela) e “logger” (registrador).
- Keylogger: captura as teclas digitadas.
- Adware: apresenta propagandas.

VÍRUS

O vírus é um programa ou parte de um programa de computador que precisa ser executado, necessita de um arquivo hospedeiro e pode criar cópias de si mesmo e se multiplicar, podendo enviá-las por e-mail e contaminar outros arquivos.

- Macro: contamina arquivos que contêm macro, como arquivos do Word, PowerPoint e Excel.
- Boot: contamina o setor responsável pela inicialização operacional. Como é inicializado antes do sistema operacional, é de difícil detecção.
- Worm: não precisa ser executado manualmente, não usa arquivo hospedeiro e se propaga explorando falhas de segurança nos computadores conectados. Em muitos casos, o worm pode causar lentidão na rede.
- Backdoor: em português, significa “porta dos fundos”. Esse programa permite o retorno de um invasor à máquina, inserindo, caso ele queira, outros programas na máquina e a infectando.
- Trojan Horse: em português, significa “cavalo de Troia”. Esse programa é recebido como um presente aparentemente inofensivo, como um cartão virtual, um jogo, entre outros. Muitas vezes, após clicar no “presente”, uma ameaça escondida será instalada. Existem tipos específicos de cavalos de Troia: os que geram cliques em uma página, os que fazem download de arquivos, os que acessam sites de banco etc.

Obs.: para recordar do cavalo de Troia, basta lembrar da guerra entre gregos e troianos. Quando os gregos estavam quase perdendo a guerra, deixaram um cavalo como presente, e a partir desse momento, surgiu a expressão “presente de grego”. Isso porque o cavalo estava recheado de soldados que, uma vez dentro da fortaleza, tinham a intenção de abrir as portas e criar vulnerabilidade.

- Bot: não precisa ser executado manualmente, não usa um arquivo hospedeiro, pode criar cópias de si mesmo e explora vulnerabilidades, assim como o worm. A diferença é que o bot pode ser controlado remotamente. Quando esse controle é feito e bots são instalados em várias redes, pode ser criada uma botnet, que é uma rede de computadores infectados por bots. Esses computadores infectados passam a ser

chamados de computadores zumbis, uma vez que são comandados remotamente por alguém e podem ser utilizados para diversos fins.

- Ransomware: sequestra os dados por meio da criptografia dos dados ou do bloqueio do computador. Existem dois tipos de ransomware: locker, que bloqueia o computador, e crypto, que bloqueia os dados. Normalmente, o atacante coloca uma mensagem automática que aparece pedindo resgate e exigindo pagamento em moedas virtuais.
- Rootkit: no Linux, o root é utilizado como administrador com plenos poderes sobre o sistema. Rootkit é um conjunto de programas e técnicas usados para invadir uma máquina e manter essa invasão oculta, escondendo os programas infiltrados, causando modificações e dificultando a sua detecção. A partir desse momento, o atacante tem acesso à máquina e pode manipulá-la como quiser.
- Rat: é uma combinação de um backdoor com um trojan horse. Ele combina as características desses programas para invadir uma máquina e mantê-la sob invasão.

15m

ATAQUES

Fonte: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf

1. Exploração de vulnerabilidades;

A vulnerabilidade é uma falha de segurança. O spyware, caracterizado como malware, pode ser usado legalmente, conforme previsto na cartilha. Levando em consideração a legislação trabalhista, é necessário um acordo entre patrão e colaborador. A exploração de vulnerabilidades não é necessariamente ilegal, uma vez que pessoas podem ser contratadas para explorar a vulnerabilidade de uma empresa, por exemplo. Em oposição a esse tipo de exploração, esta aula tratará dos ataques de forma negativa.

2. Varredura em redes (Scan);

O scan varre a rede procurando falhas para invadir. Uma dessas falhas pode ser encontrada em redes Wi-Fi que estão abertas ou que não usam criptografia, permitindo a captura dos dados que estão circulando.

3. Falsificação de e-mail (E-mail spoofing);

A falsificação de e-mail é uma alteração no cabeçalho do e-mail para fingir ser de uma pessoa que não é.

4. Interceptação de tráfego (Sniffing) sniffers;

A interceptação de tráfego é feita pela utilização de sniffers, que são programas farejadores. Existe a possibilidade de uso legal desses programas. No entanto, quando utilizados de maneira maliciosa, um sniffer pode ser implementado para capturar os dados da rede. Se o tráfego estiver criptografado, não será compreensível para quem capturou os dados. Por outro lado, se não estiver criptografado, tudo será compreensível, incluindo senhas e dados sigilosos.

5. Força bruta (Brute force);

O ataque de força bruta tenta descobrir uma senha através de tentativa e erro. Dependendo da força da criptografia, é quase impossível que isso ocorra, mas senhas mais simples podem ser quebradas em segundos.

20m

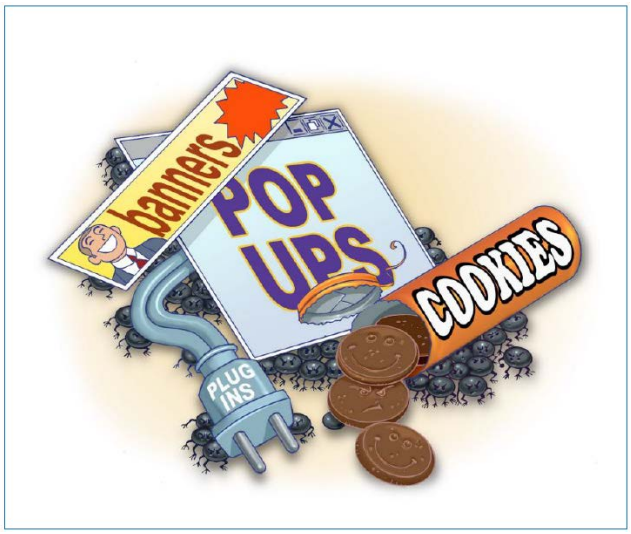
6. Desfiguração de página (Defacement);

A intenção do defacement é desfigurar uma página para alterar o seu propósito.

7. Negação de serviço (DoS e DDoS).

Um ataque de DoS ocorre quando uma única máquina é utilizada para atacar um servidor, ou seja, um contra um. Esse tipo de ataque sobrecarrega a máquina-alvo enviando uma grande quantidade de requisições. Todo servidor possui um limite de requisições que pode atender simultaneamente. Quando esse limite é excedido, o servidor geralmente para de funcionar e outras pessoas não conseguem acessá-lo. O DDoS faz isso utilizando uma botnet, em que várias máquinas trabalham em conjunto para atacar o servidor. Existem mecanismos de proteção para tentar detectar esse tipo de ataque, mas em alguns casos ele pode ser bem-sucedido em derrubar o servidor.

OUTROS RISCOS



Fonte: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf

1) PHISHING (PHISHING SCAM)

O phishing scam é um golpe que tenta enganar alguém para que esta pessoa forneça seus dados pessoais. Pode-se fazer uma analogia com o crime previsto no artigo 171 do Código Penal. Kevin Mitnick inventou o método de persuasão conhecido como engenharia social. Isso pode ser feito através de e-mails que se passam por um banco, informando, por exemplo, que o cartão foi clonado. Outro exemplo pode ser observado a seguir:

Comprovante Nº 002526

Anexo: Deposito002526.doc (103kb)

O dinheiro já foi transferido via transferencia interbancaria para sua conta e já deve ter sido compensado, segue na mensagem o comprovante com os dados e o valor, desculpe o transtorno.

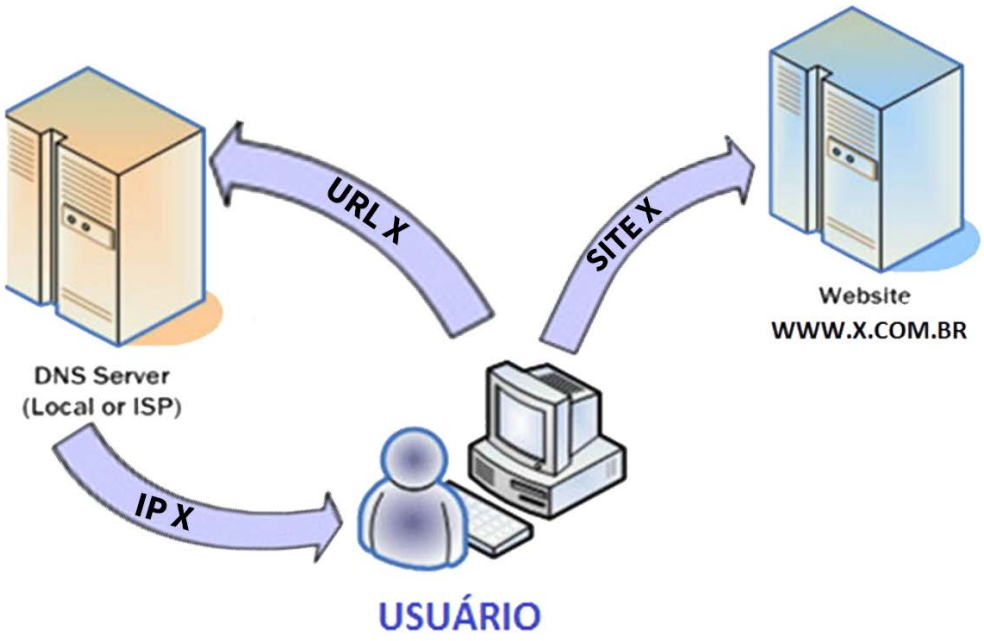
Muito obrigada!

Alice Pacheco Silva

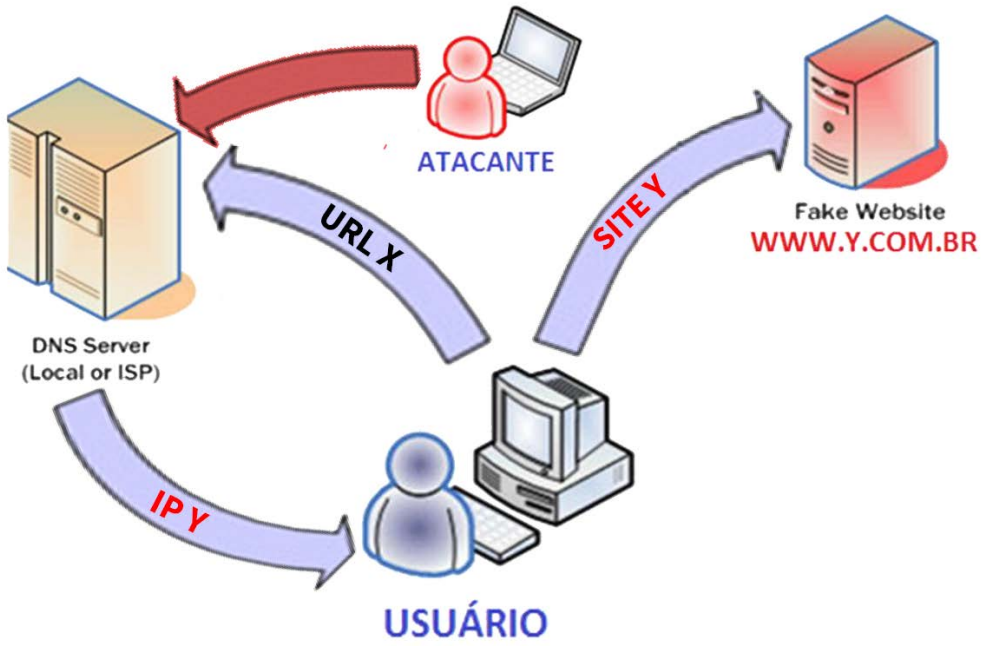
1.1) PHARMING

O pharming é um tipo de phishing. Para entendê-lo, é necessário compreender como ocorre o acesso a um site. O usuário digita uma URL, ou seja, um endereço no navegador. Essa requisição é enviada para o servidor DNS, cujo papel é converter a URL em um endereço IP X, que é o endereço único que identifica as máquinas na internet. Através do IP X, é possível acessar o site X. Na informática, isso é conhecido como "caminho feliz".

25m

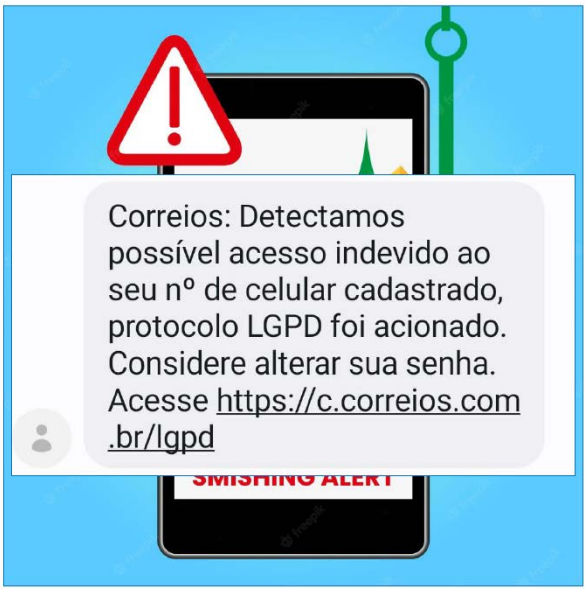


O golpe de pharming ocorre quando o usuário digita o URL X, mas o servidor DNS foi comprometido pelo atacante. Isso é feito pela substituição do IP X desejado pelo IP Y. Com isso, o usuário é redirecionado para o site Y, que é um site falso. Geralmente, é criado um site idêntico ao verdadeiro para capturar dados pessoais, como informações de cartão e senhas. Este golpe é de difícil detecção, porém é raro.



1.2) SMISHING

O smishing é uma tentativa de golpe enviada por SMS, como mostrado no exemplo a seguir.



GABARITO

17. c

18. C