SEGURANÇA DA INFORMAÇÃO E DE REDES

Prof. Milton Palmeira Santana

Sql Injection

- Em um sistema WEB é muito comum ataques do tipo SQL Injection que é um ataque muito simples, que baseia-se na execução de comandos SQL, sejam comandos de manipulação de dados (DML) ou comandos de definição de dados (DDL).

- Esses comandos são executados através das entradas de formulários web, onde são passados comandos SQL que por falhas nas aplicações acabam por resultar em alterações no banco ou acesso indevido à aplicação.

```
$sql = "SELECT * FROM USUARIOS
    WHERE LOGIN = '$login' AND SENHA = '$senha'";
```

Sql Injection

- O comando anterior permite que o usuário insira manualmente comandos SQL e execute os mesmos para simular uma informação e permitir que o código SQL retorne VERDADEIRO na sua consulta.

- Vamos fazer um exemplo prático:
  - Criaremos um banco de dados, uma página HTML e os códigos PHP para realizarmos essa simulação de ataque.

Ameaças à rede – Pessoas

- Há duas visões quando tratamos sobre pessoas em segurança da informação. Algumas delas são os agentes de ameaça, como os crackers e os hackers, bem como os funcionários (insiders) ou mesmo os concorrentes.

- Sobre essas nomenclaturas, vamos conhecer algumas delas:
  - **Hacker**: A definição de hacker é um pouco difusa e já foi usada com múltiplos significados ao longo dos anos. Hoje em dia, a mais aceita é de que um hacker é alguém com amplo conhecimento tecnológico e que gosta de mexer com sistemas de informação. “Hacker”, por si só, é uma palavra neutra, sem julgamento de valor. Conceito mais voltado para pessoas que utilizam seu conhecimento para fins não criminosos.

Ameaças à rede – Pessoas

- **Hacker – White Hat**: ainda sobre os hackers é muito comum encontrar dois termos. O primeiro é o White hat que é um termo específico para os especialistas em segurança da informação. São considerados “hackers do bem”.

- **Hacker – Black Hat**: utilizam vulnerabilidades para obter dados e causar ações criminosas.

- **Hacker – Gray Hat**: Ao encontrar uma vulnerabilidade, ele observa os dados, talvez até divulga alguns, mas procura não cometer crimes nenhum. Também não informa sobre as vulnerabilidades. Fica meio que em cima do muro.

Ameaças à rede – Pessoas

- **Cracker**: Essa palavra sempre gera polêmica. No passado, ela era usada para definir o “hacker do mal”, a pessoa que usava seu conhecimento de tecnologia para o crime. No entanto, o tempo tratou de dar a ela um novo significado. “Crackear”, no jargão digital, é disponibilizar uma versão pirateada de um software (um jogo, por exemplo) na internet após quebrar a proteção que impede o uso de cópias piratas.

- **Script Kiddie:** não possui alvo certo. Normalmente, utilizam ferramentas prontas sem saber muito bem como funcionam.

Ameaças à rede – Pessoas

- **Phreaker:** especialista em telefonia (móvel ou fixa).
- **Exemplos interessantes:** O “pai” dos Phreakers é **John Draper** um hacker americano que descobriu (na época) uma forma de realizar chamadas nacionais e internacionais gratuitamente.

- Era década de 70, e claro, as ligações eram muito caras.

- Um amigo de John percebeu que um **APITO** que vinha em um cereal era capaz de emitir tons a 2600 Hertz.
- Coincidentemente, era a mesma frequência utilizada pela AT & T para indicar que uma linha poderia fazer chamada.

- Com apenas algumas pequenas modificações foi possível criar um pequeno dispositivo que o permitia fazer ligações gratuitas.

Ameaças à rede – Pessoas

- **Phreaker:** MAS E HOJE?

- Não, não adianta tentar comprar diversas caixas de cereal para conseguir achar esse apito porque hoje em dia isso não funciona mais. ☺

- Hoje em dia, com a evolução da tecnologia, existem técnicas e meios para burlar a rede. Exemplos são: clonagem de chips, espionagem de ligações e mensagens, etc.

Ameaças

- As ameaças enfrentadas pela aplicação podem ser categorizadas com base nos objetivos e propósitos dos ataques. A Microsoft adota uma categoria de ameaças conhecida como STRIDE.
  - **Spoofing**: é a falsificação como meio de ganhar acesso a um sistema usando uma identidade falsa. Isso pode ser feito usando credenciais roubadas ou um endereço falso de IP. Após o invasor ter conseguido ganhar acesso como um usuário legítimo ou host, a elevação ou o abuso de privilégios usando a autorização pode ser realizado.
  - **Tampering**: é a manipulação ou modificação não autorizada dos dados, por exemplo, entre dois computadores em rede.

Ameaças

- **Repudiation**: é o repúdio ou a habilidade de usuários (legítimos ou não) de negar que tenham executado ações ou transações específicas.
- **Information disclosure**: é a revelação de informações ou a exposição não autorizada de dados privados. Por exemplo, um usuário visualiza o conteúdo de uma tabela ou arquivo não autorizado, ou monitora dados transmitidos em texto puro através de uma rede.
- **Denial of service**: é a negação de serviço ou o processo que torna um sistema ou aplicação indisponível. Por exemplo, um ataque de negação de serviço pode ser feito por meio do bombardeamento de solicitações que consomem todos os recursos disponíveis do sistema.

Ameaças

- **Elevation of privilege**: é a elevação de privilégio que ocorre quando um usuário com privilégios limitados assume a identidade de um usuário privilegiado para ganhar acesso a uma aplicação. Por exemplo, um invasor com privilégios limitados pode elevar seu nível de privilégio para comprometer e tomar o controle de uma conta ou de processo altamente privilegiado.

- **Keylogger**: é um software criado para gravar tudo que uma pessoa digita em um determinado teclado de um computador.

Ameaças

- **DOS –** os ataques de negação de serviço (Denial of Service, DoS) fazem com que recursos sejam explorados de maneira agressiva, de modo que usuários legítimos ficam impossibilitados de utilizá-los.

- Uma técnica típica é o SYN Flooding, que causa o overflow da pilha de memória por meio do envio de um grande número de pedidos de conexão, que não podem ser totalmente completados e manipulados.

- Outra técnica é o envio de pacotes específicos visando causar a interrupção do serviço, que pode ser exemplificada pelo Smurf.

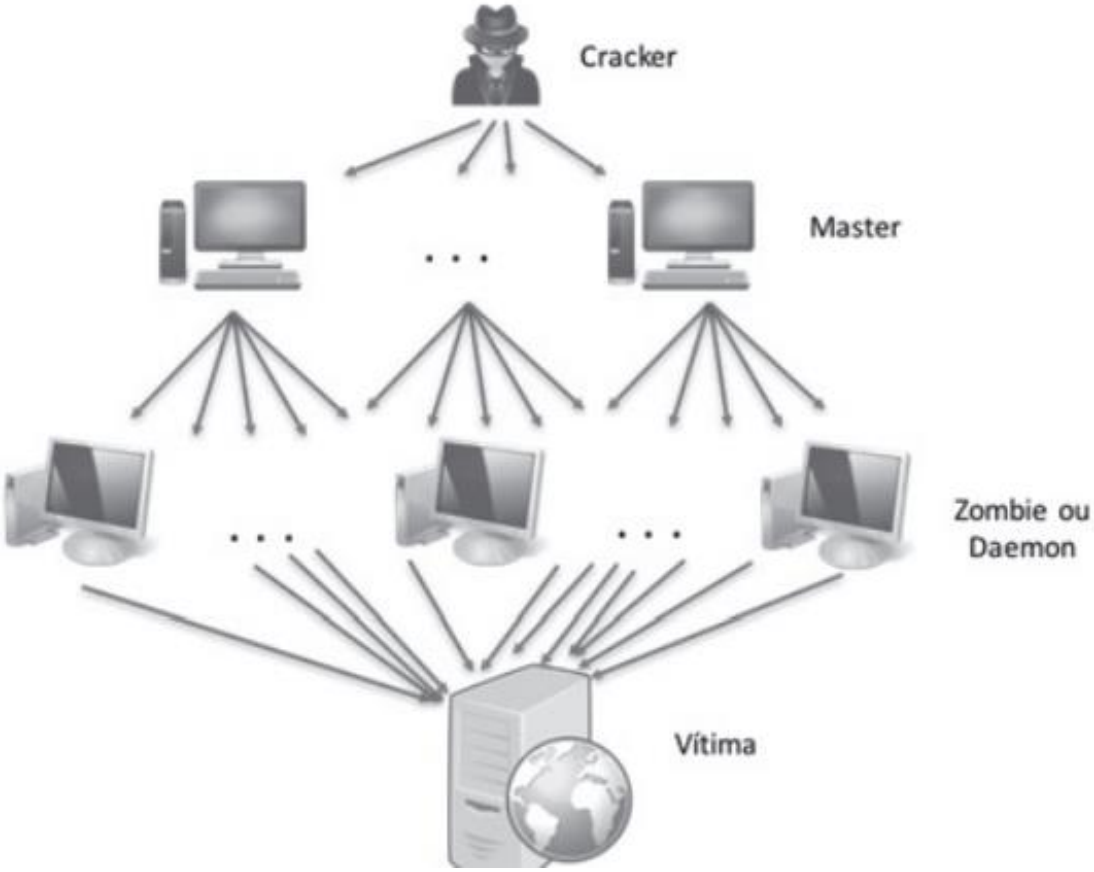
Ameaças

- **DOS –** alguns dos maiores responsáveis pelos ataques de negação de serviços são os próprios desenvolvedores de software. Diversas falhas na implementação e na concepção de serviços, aplicativos, protocolos e sistemas operacionais abrem brechas que podem ser exploradas.

- **Smurf e Fraggle** - Com a intenção de causar a negação de serviço, o Smurf é um ataque simples que gera um grande tráfego na rede, por meio do envio de ping (ICMP Echo) para o endereço IP de broadcast da rede da vítima. A origem do ping é um endereço falsificado com o IP Spoofing, o que faz com que todos os hosts daquela rede respondam ao endereço de origem da requisição ping, que é falsificado. Fraggle é equivalente ao Smurf, mas com uso do UDP Echo ao invés do ICMP Echo.

Ameaças

- **DDoS (Ataques distribuídos e coordenados –** O cracker define alguns sistemas master, que se comunicam com os daemons ou zombies que realizam os ataques à vítima.



Ameaças

- **Malware –** O conceito de malware é interessante por englobar os famosos vírus, worms, cavalos de Troia, ransomware, spyware, backdoor, entre outros. O termo malwarevem do inglês malicious software, ou software malicioso, que causa, intencionalmente, danos à vítima.

- Os malwares mais conhecidos são os vírus e os worms (ou vermes). Apesar de serem similares, há diferenças conceituais importantes entre eles. Os vírus precisam ser executados pelo usuário para contaminarem a vítima. Já os worms se autopropagam com a exploração de vulnerabilidades existentes no ambiente, de modo que não necessitam de ações de usuários.

Ameaças

- Os **cavalos de Troia** ou **trojans** seguem a ideia da Guerra de Troia, quando os gregos conseguiram entrar em Troia dentro de um cavalo, que teria sido um “presente de grego”, o que levou a cidade fortificada à ruína. Os cavalos de Troia, em segurança da informação, executam tarefas legítimas ao mesmo tempo em que atividades ilícitas são realizadas no equipamento da vítima, por exemplo, roubo de informações armazenadas ou envio de tudo o que o usuário digita.

- O **ransomware** tem feito muitas vítimas ultimamente, consiste no sequestro de informações que são recuperadas apenas mediante pagamento de um resgate. Métodos criptográficos são utilizados nesse ataque, no qual o cracker envia a chave para a recuperação das informações após o pagamento do valor estipulado.

Ameaças

- Já o **backdoor** é uma condição que possibilita o acesso remoto ou a execução de comandos com a existência de uma "porta não autorizada" em softwares e hardwares.

- O **phishing** é um ataque que busca capturar informações pessoais enquanto o fraudador se faz passar por uma pessoa ou empresa confiável, com o uso de uma comunicação eletrônica oficial.

- O **Bot** dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção parecido com o Worm, sendo capaz de se propagar automaticamente explorando vulnerabilidades.
- **Botnet** são redes de computadores infectadas com bots.

EXERCÍCIOS

1) O DoS, ou Denial of Service, afeta qual propriedade básica de segurança da informação?

a) Nenhuma.

b) Confidencialidade.

c) Integridade.

d) Disponibilidade.

e) CID.

EXERCÍCIOS

2) O DDoS, ou Distributed Denial of Service, afeta qual propriedade básica de segurança da informação?

a) Nenhuma.

b) Confidencialidade.

c) Integridade.

d) Disponibilidade.

e) CID.

EXERCÍCIOS

3) Um cracker é uma ameaça que afeta qual propriedade básica de segurança da informação?

a) Nenhuma.

b) Confidencialidade.

c) Integridade.

d) Disponibilidade.

e) CID.

EXERCÍCIOS

Pesquise sobre Exploit, Vírus, Worm, Spyware, Rootkit e Adware.

DATA DE ENTREGA: 22/04

REFERÊNCIAS

MACHADO, Felipe Nery Rodrigues. **Segurança da Informação: princípios e controle de ameaças**. [S. l.]: ÉRICA, 2014.

FONTES, Edison. **Segurança da Informação**: O usuário faz a diferença. [S. l.]: SARAIVA, 2007.

SMULDERS, André; BAARS, Hans; HINTZBERGEN, Jule; HINTZBERGEN, Kees. **Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. [S. l.]: BRASPORT, 2018.

BASTA, Alfred; BASTA, Nadine; BROWN, Mary. **Segurança de computadores e teste de invasão**. [S. l.]: Cengage Learning, 2014.

REFERÊNCIAS

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à Segurança de Computadores**. [S. l.]: Bookman Editora, 2013.

STALLINGS, WILLIAM. **Criptografia e Segurança de Redes**: Princípios e práticas. 6. ed. [S. l.]: Pearson Universidades, 2014.

SINGH, Simon. **O livro dos códigos**: A ciência do sigilo – do antigo Egito à criptografia quântica. [S. l.]: Record, 2001.


Anhanguera