Segurança da Informação

ATAQUES V

Professor: Jósis Alves

Técnicas de Ataques

❑ Engenharia Social

Método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

Filme: Prenda-me se for capaz

❑ Session Hijacking (Sequestro de Conexões)

- ✓ Consiste em um ataque ativo que redireciona as conexões TCP para outra máquina (man-in-the-middle).
- ✓ Dribla proteções de protocolos de autenticação como o Kerberos.
- ✓ O atacante descobre o número de sequência de um dos pacotes e cria a partir desse, número de sequência validos.
- ✓ E então, envia pacotes para ambos.

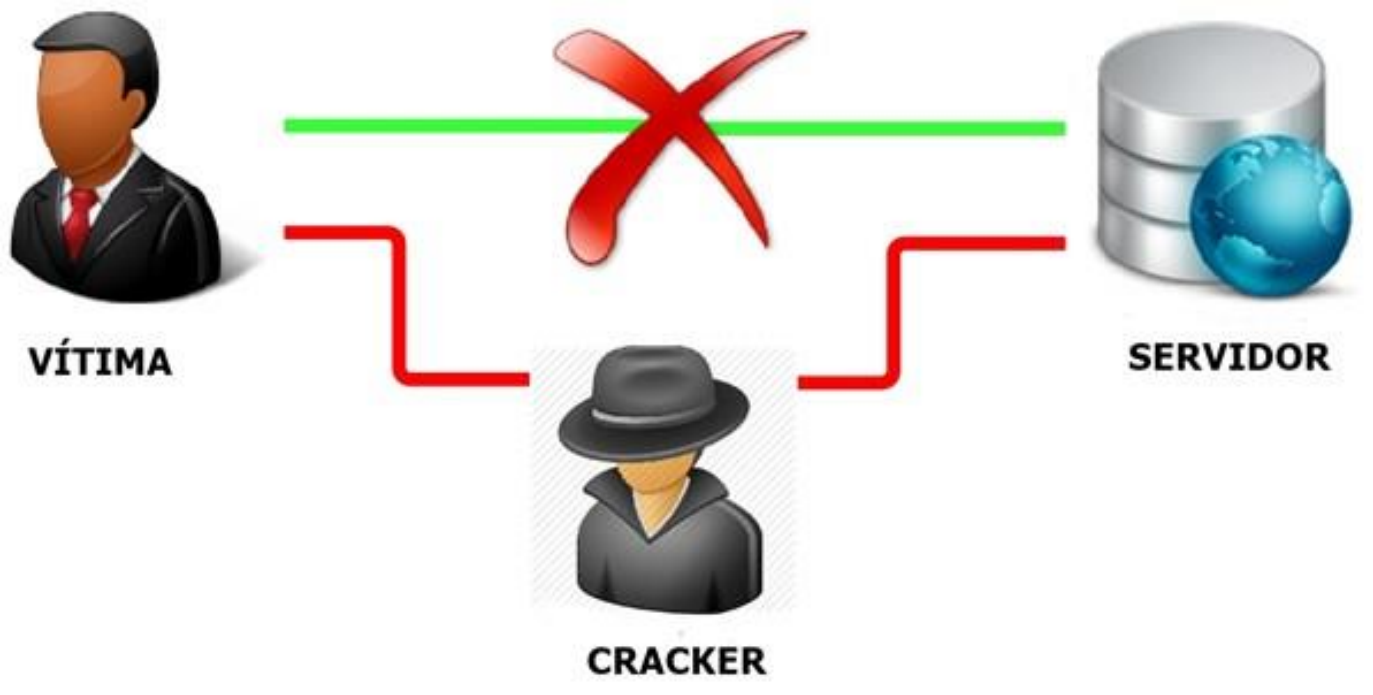
1) Ano: 2016 Banca: IF-SE Órgão: IF-SE Prova: IF-SE - 2016 - IF-SE - Analista de Tecnologia da Informação - Suporte em Infraestrutura e Redes

No mundo das pequenas corrupções, no qual a moral e a ética são afetadas da mesma forma, pessoas vão ao cinema e usam uma carteira de estudante vencida e adulterada ou até mesmo de outra pessoa. Além disso, podem ganhar a confiança de quem está controlando a entrada, obtendo acesso ao cinema como se fossem estudantes. Para a segurança da informação, estas situações são análogas às técnicas:

A) Ping O'Death e Ping Sweep.
B) Varredura Invisível e Syn Flood.
C) IP Spoofing e Engenharia Social.
D) FingerPrint e Engenharia Social.

❑ Ataques Man-in-the-middle

- ✓ O atacante realiza a interceptação da comunicação.
- ✓ Podendo alterar e criar informações.



❑ Ataques a Camada de Aplicação

➢ Funcionam explorando vulnerabilidades em:

✓ Aplicações
✓ Serviços
✓ Protocolos

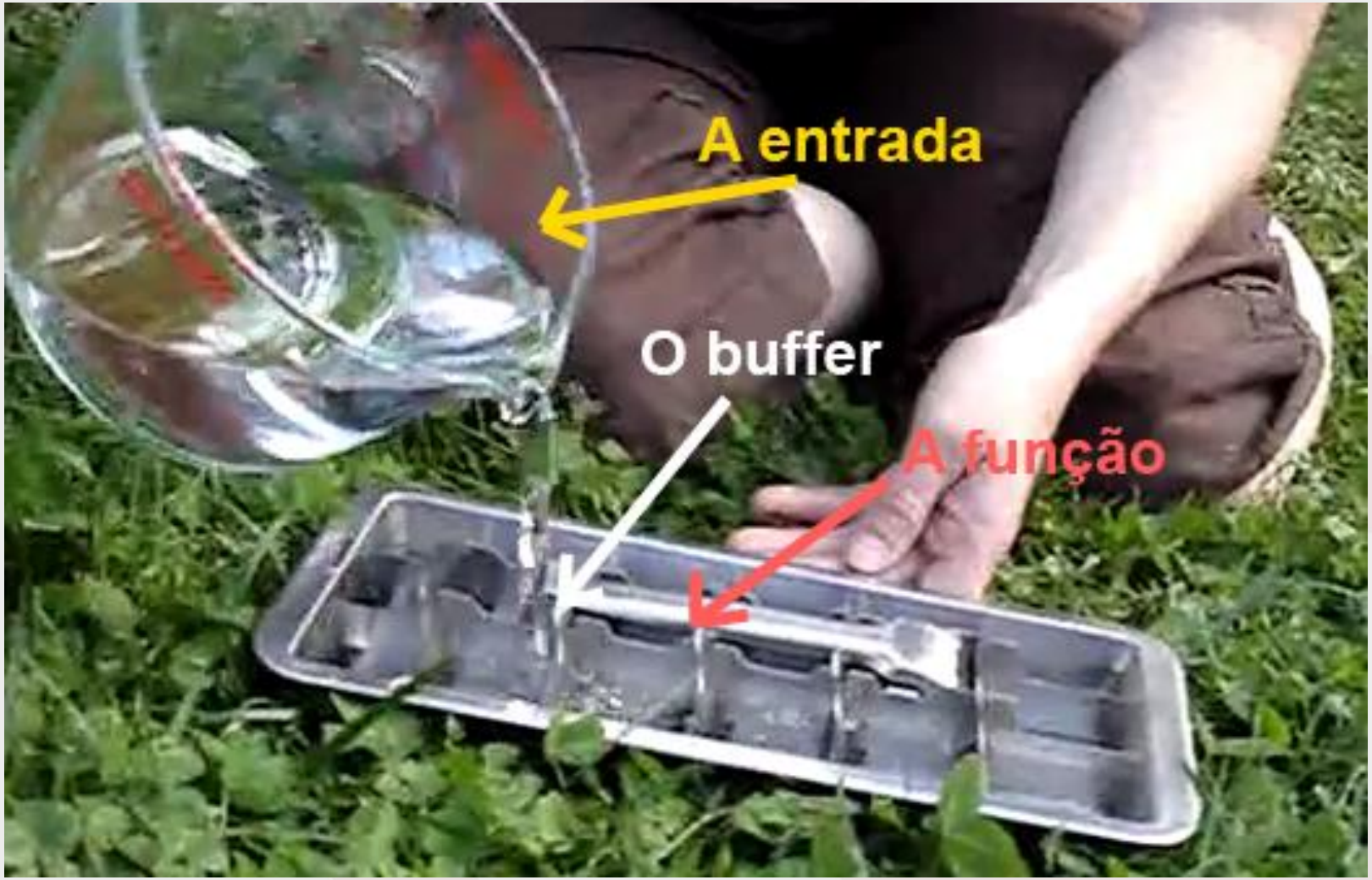
❑ Buffer Overflow (Estouro de buffer)

- ❖ *Buffer =>* região de armazenamento temporário na memória.
- ❖ *Overflow => transbordamento.*

- ➢ As vulnerabilidades referentes ao *buffer overflow* nos sistemas são consideradas as maiores.
- ➢ Envia-se mais dados do que o *buffer* pode manipular, tomando toda a pilha de memória.

- ✓ Usados para execução de códigos arbitrários.
- ✓ Perda ou modificação dos dados.
- ✓ Paralisação de todo sistema.

❑ Buffer Overflow



❑ Buffer Overflow

➢ Podem afetar:

✓ Sistemas Operacionais:
Windows, Unix, MacOS, etc.
✓ Serviços:
E-mail (Exchange), WEB (IIS, Apache, ...), etc.
✓ Protocolos:
FTP, NTP, RPC, etc.

2) Ano: 2015 Banca: FGV Órgão: TCE-SE Prova: FGV - 2015 - TCE-SE - Analista de Tecnologia da Informação-Segurança da Informação

Os ataques relativos à segurança da informação baseiam-se em aspectos técnicos, físicos e/ou humanos. O tipo de ataque que está baseado principalmente no aspecto humano é:

A) Worm;
B) Spoofing;
C) Engenharia social;
D) Negação de serviço;
E) Buffer overflow.

3) Ano: 2019 Banca: UFGD Órgão: UFGD Prova: UFGD - 2019 - UFGD - Técnico de Laboratório – Informática

Uma séria ameaça a lojas virtuais, serviços de armazenamento de arquivos na nuvem, serviços de e-mail, provedores de Internet, dentre outros, é um tipo de ataque que visa a impedir usuários legítimos de acessarem determinado serviço. Esse tipo de ataque torna os sistemas de computador inacessíveis, inundando servidores, redes e inclusive sistemas de usuário final com tráfego basicamente inútil, provindos de um ou diferentes hosts contaminados reunidos para esse fim, causando indisponibilidade do alvo, fazendo com que os usuários reais não consigam acessar o recurso pretendido. Essa ameaça é conhecida como

3) Ano: 2019 Banca: UFGD Órgão: UFGD Prova: UFGD - 2019 - UFGD - Técnico de Laboratório – Informática

A) interceptação de tráfego (Sniffing).
B) negação de serviço (DoS e DDoS).
C) desfiguração de página (Defacement).
D) falsificação de e-mail (E-mail spoofing).
E) força bruta (Brute force).

4) Ano: 2018 Banca: CESPE / CEBRASPE Órgão: STJ Prova: CESPE - 2018 - STJ - Técnico Judiciário - Suporte Técnico

A respeito das técnicas e características de ataques de rede, julgue o item que se segue.

Buffer overflow é um tipo de ataque que, ao explorar falha na implementação de um programa, permite escrita em um endereço de memória diferente do previamente alocado.

( ) certo ( ) errado

❑ SQL Injection (Injeção de SQL)

Consiste no ataque que explora vulnerabilidade na entradas de aplicações.

O ataque insere ou manipula consultas SQL criadas pela aplicação.

Técnica que “engana” formulário de login.

Comandos DML (select, insert, update, delete) ou DDL (create, drop, alter).

Segurança: Validação de entrada de dados

❑ SQL Injection (Injeção de SQL)

5) Ano: 2018 Banca: FGV Órgão: MPE-AL Prova: FGV - 2018 - MPE-AL - Analista do Ministério Público - Desenvolvimento de Sistemas

Na prática de programação segura, a ação que pode ser adotada para mitigar ataques que exploram a inserção de comandos em campos de formulários dos sistemas, especialmente em sistemas web, como o ataque de "SQL Injection", é descrita como

A) codificação dos dados de entrada.
B) criptografia dos dados de entrada.
C) autenticação de usuários.
D) controle de acesso dos dados de entrada.
E) validação dos dados de entrada.

GABARITO
1 - C
2 - C
3 - B
4 - certo
5 - certo