Segurança da Informação

PLANEJAMENTO DO ATAQUE

Professor: Jósis Alves

Planejamento do ataque

❑ Motivações

- ✓ *Script Kiddies*
  - Curiosidade, diversão, etc.
- ✓ *Insiders* ou *Black Hats*
  - Financeira, fama, vingança, espionagem, etc.
- ✓ *Cyberterroristas*
  - Ideológicas, religiosas, etc.

❑ Níveis de Segurança

- Segurança não é importante, muito caro.
- Segurança por Obscuridade.
- Segurança individual.
- Segurança Ampla.

❑ Obtenção de Informações

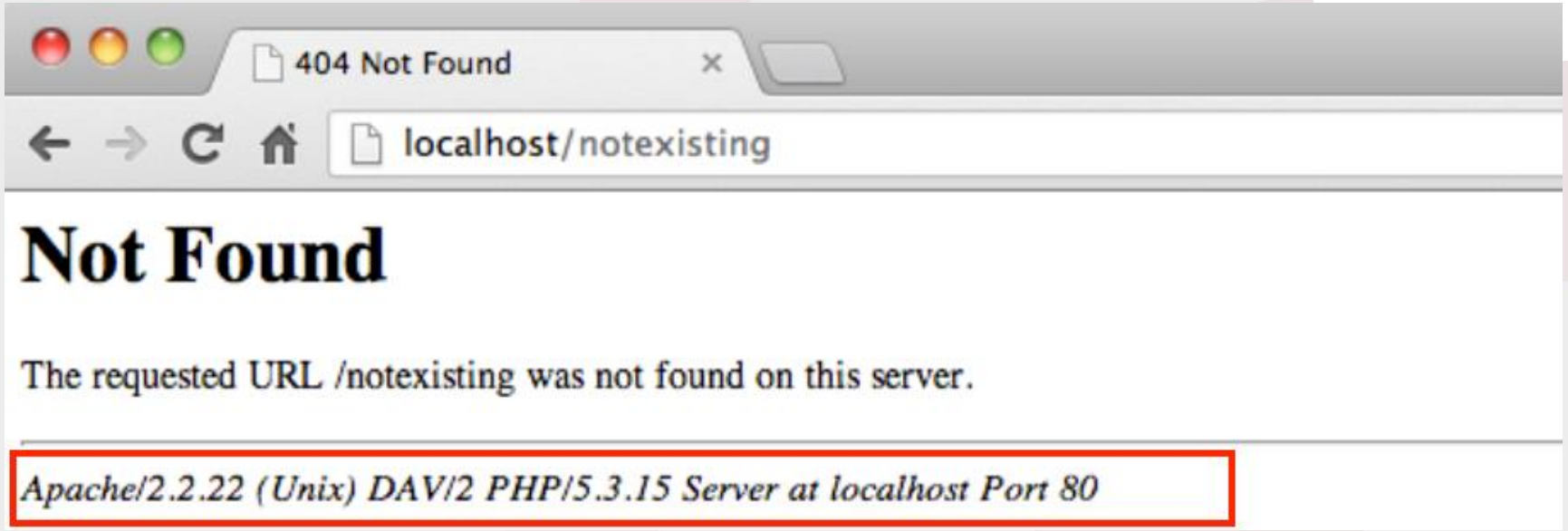
❑ Informações Livres

Não intrusivas, por isso, não podem ser detectadas.

- ✓ Buscas na internet.
- ✓ Consultas a servidores DNS (comando WHOIS).
- ✓ Análise de cabeçalhos de email.
- ✓ Banners com informação de versão de serviços.

❑ Obtenção de Informações

- ❑ **Informações Livres**



❑ Obtenção de Informações

❑ **Footprinting:** é a técnica utilizada para um levantamento de informações sobre alguém ou um alvo.

✓ Levantamento de Informações de Domínios:
- Nomes, responsáveis.

✓ Identificação do SO (Fingerprint).

✓ Descobrir subredes.

✓ Serviços TCP e UDP disponíveis.

✓ Topologia da rede.

❑ Obtenção de Informações

❑ Dumpster Diving ou Trashing

✓ Consiste em verificar lixo.
✓ É legal.

Ex: Procter Gamble e Unilever.

❑ Obtenção de Informações

- **Engenharia Social**

- Enganar, ludibriar.
- Exploração das fraquezas humanas e sociais.
- Simpatia, autoridade, medo, etc.

Ex: Se passar por funcionário de alto escalão que tem problemas de acesso ao sistema.

❑ Obtenção de Informações

❑ ***Packet Sniffing***

Também conhecida como ***Passive Eavesdropping.***

Captura de pacotes pela rede no mesmo segmento de rede.

Conteúdo que trafega em aberto.

Ex: ferramenta *TCPDump.*

1) Ano: 2015 Banca: FGV Órgão: DPE-RO Prova: FGV - 2015 - DPE-RO - Técnico da Defensoria Publica - Técnico em Informática

Uma das formas de ataque à segurança dos dados é o monitoramento de pacotes que passam na rede, procurando por senhas em texto claro, por exemplo. O nome dessa forma de ataque é:

A) Phishing;

B) Scamming;

C) Spoofing;

D) poisoning;

E) sniffing.

2) Ano: 2018 Banca: FADESP Órgão: IF-PA Prova: FADESP - 2018 - IF-PA - Professor - Informática

Em segurança computacional e programação, o ataque que explora a falta de tratamento dos dados de uma entrada do sistema tentando injetar strings maiores que as permitidas no intuito de invadir outras áreas de memória é o

A) Injection sniffing.

B) Buffer overflow.

C) Spoofing.

D) Phishing.

E) SYN Flood.

3) Ano: 2019 Banca: CESPE / CEBRASPE Órgão: CGE - CE Prova: CESPE - 2019 - CGE - CE - Auditor de Controle Interno - Tecnologia da Informação

Após o envio de um email pelo emissor a determinado destinatário, ocorreu uma ação maliciosa e o email foi lido por terceiro.

Nessa situação, a ação maliciosa é do tipo

A) sniffing

B) spoofing

C) brute force

D) defacement

E) denial of service.

4) Ano: 2017 Banca: FGV Órgão: MPE-BA Prova: FGV - 2017 - MPE-BA - Analista Técnico – Tecnologia

Um cibercriminoso envia para sua vítima um e-mail falso, em que se passa por uma instituição conhecida, informando que seu cadastro está irregular e que, para regularizá-lo, é necessário clicar no link presente no corpo do e-mail.

Esse tipo de falsificação de uma comunicação por e-mail é uma técnica conhecida como:

A) Phishing;

B) Sniffing;

C) MAC Spoof;

D) Denial of Service;

E) SQL Injection.

5) Ano: 2018 Banca: IF-TO Órgão: IF-TO Prova: IF-TO - 2018 - IF-TO - Técnico em Tecnologia da Informação

Tem como objetivo tornar inoperante um servidor, serviço ou rede, por meio da sobrecarga do alvo ou de sua infraestrutura. Trata-se de um ataque do tipo

A) SQL Injection

B) DoS (Denial of Service)

C) Phishing

D) Sniffing

E) Backdoors

GABARITO
1 - E
2 - B
3 - A
4 - A
5 - B