Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

- OS fingerprint
- Syn Scan
- TCP Connect (differenze con sys scan)
- Version detection

E la seguente sul target Windows

Os Fingerprint

Produrre un report con le seguenti info:

- IP
- Sistema operativo
- Porte aperte
- Servizi in ascolto con versione

Per iniziare, utilizzando fping, otteniamo la lista dei dispositivi connessi alla rete e la inseriamo in un file di testo:

Andiamo ad individuare i sistemi operativi delle macchine connesse alla rete:

Dove -O ci ritornerà i sistemi operativi degli host connessi, -Pn tratterà tutti gli indirizzi dati come attivi e -iL userà come input gli IP che abbiamo inserito nel file txt.
Tra le varie informazioni che otteniamo, abbiamo questo:

Per la nostra PfSense

Per la Metasploitable

Per Windows XP

Eseguiamo il Syn Scan:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -iL listaip.txt
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 15:35 CEST
Nmap scan report for 192.168.51.1
Host is up (0.0030s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
MAC Address: 08:00:27:BC:4B:F1 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.51.101
Host is up (0.0056s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:BE:2A:6E (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.51.103
Host is up (0.0028s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:5C:8D:1C (Oracle VirtualBox virtual NIC)
```

E TCP Connect:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT -iL listaip.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 15:46 CEST
Nmap scan report for 192.168.51.1
Host is up (0.0053s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
MAC Address: 08:00:27:BC:4B:F1 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.51.101
Host is up (0.0064s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:BE:2A:6E (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.51.103
Host is up (0.0057s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:5C:8D:1C (Oracle VirtualBox virtual NIC)
```

La prima differenza che salta all'occhio è che Syn Scan ha bisogno dei permessi di root, mentre il TCP Connect no.

Teoricamente, il Syn Scan dovrebbe metterci meno tempo, anche se nei vari tentativi, risulta sempre piu lento rispetto al TCP Connect

```
Nmap done: 4 IP addresses (4 hosts up) scanned in 8.07 seconds
```

```
Nmap done: 4 IP addresses (4 hosts up) scanned in 6.58 seconds
```

Eseguiamo poi il version detection su tutto il range di porte (-p-):

```
Nmap scan report for 192.168.51.101
Host is up (0.0080s latency).
Not shown: 65505 closed tcp ports (reset)
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
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
32833/tcp open  status      1 (RPC #100024)
39298/tcp open  java-rmi    GNU Classpath grmiregistry
48700/tcp open  mountd      1-3 (RPC #100005)
53500/tcp open  nlockmgr    1-4 (RPC #100021)
MAC Address: 08:00:27:BE:2A:6E (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.51.103
Host is up (0.0020s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:5C:8D:1C (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
```

Abbiamo quindi una versione dettagliata di IP, versione del sistema operativo, porte aperte e servizi in ascolto.

Sperimentiamo un po’ di script:

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script-help ssh-hostkey
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 16:45 CEST

ssh-hostkey
Categories: safe default discovery
https://nmap.org/nsedoc/scripts/ssh-hostkey.html
  Shows SSH hostkeys.

  Shows the target SSH server's key fingerprint and (with high enough
  verbosity level) the public key itself.  It records the discovered host keys
  in <code>nmap.registry</code> for use by other scripts.  Output can be
  controlled with the <code>ssh_hostkey</code> script argument.

  You may also compare the retrieved key with the keys in your known-hosts
  file using the <code>known-hosts</code> argument.

  The script also includes a postrule that check for duplicate hosts using the
  gathered keys.

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script=ssh-hostkey -p22 192.168.51.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 16:47 CEST
Nmap scan report for 192.168.51.101
Host is up (0.0090s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
```

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script-help http-php-version
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 16:53 CEST

http-php-version
Categories: discovery safe
https://nmap.org/nsedoc/scripts/http-php-version.html
  Attempts to retrieve the PHP version from a web server. PHP has a number
  of magic queries that return images or text that can vary with the PHP
  version. This script uses the following queries:
  * <code>/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42</code>: gets a GIF logo, which changes on April Fool's Day.
  * <code>/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000</code>: gets an HTML credits page.

  A list of magic queries is at http://www.0php.com/php_easter_egg.php.
  The script also checks if any header field value starts with
  <code>"PHP"</code> and reports that value if found.

  PHP versions after 5.5.0 do not respond to these queries.

  Link:
  * http://phpsadness.com/sad/11

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script=http-php-version -p80 192.168.51.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 16:54 CEST
Nmap scan report for 192.168.51.101
Host is up (0.0028s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-php-version: Versions from logo query (less accurate): 5.1.3 - 5.1.6, 5.2.0 - 5.2.17
| Versions from credits query (more accurate): 5.2.3 - 5.2.5, 5.2.6RC3
|_Version from header x-powered-by: PHP/5.2.4-2ubuntu5.10

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script-help http-headers
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 17:01 CEST

http-headers
Categories: discovery safe
https://nmap.org/nsedoc/scripts/http-headers.html
  Performs a HEAD request for the root folder ("/") of a web server and displays the HTTP headers returned.

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script=http-headers -p80 192.168.51.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 17:02 CEST
Nmap scan report for 192.168.51.101
Host is up (0.0053s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-headers:
|   Date: Tue, 10 Sep 2024 11:35:04 GMT
|   Server: Apache/2.2.8 (Ubuntu) DAV/2
|   X-Powered-By: PHP/5.2.4-2ubuntu5.10
|   Connection: close
|   Content-Type: text/html
|
|_  (Request type: HEAD)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

(Purtroppo non ho modo di testare questi)

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script-help quake1-info
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 17:04 CEST

quake1-info
Categories: default discovery safe version
https://nmap.org/nsedoc/scripts/quake1-info.html
  Extracts information from Quake game servers and other game servers
  which use the same protocol.

  Quake uses UDP packets, which because of source spoofing can be used to amplify
  a denial-of-service attack. For each request, the script reports the payload
  amplification as a ratio. The format used is
  <code>response_bytes/request_bytes=ratio</code>

  http://www.gamers.org/dEngine/quake/QDP/qnp.html

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script-help quake3-info
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 17:05 CEST

quake3-info
Categories: default discovery safe version
https://nmap.org/nsedoc/scripts/quake3-info.html
  Extracts information from a Quake3 game server and other games which use the same protocol.

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap --script-help quake3-master-getservers
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 17:05 CEST

quake3-master-getservers
Categories: default discovery safe
https://nmap.org/nsedoc/scripts/quake3-master-getservers.html
  Queries Quake3-style master servers for game servers (many games other than Quake 3 use this same protocol).
```

```
┌──(kali㉿kali)-[~]
└─$ nmap --script-help ssh-brute
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 17:33 CEST

ssh-brute
Categories: brute intrusive
https://nmap.org/nsedoc/scripts/ssh-brute.html
  Performs brute-force password guessing against ssh servers.
```

```
┌──(kali㉿kali)-[~]
└─$ nmap --script=ssh-brute --script-args="userdb=usernames.txt,passdb=passwords.txt" -p22 192.168.51.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 17:34 CEST
NSE: [ssh-brute] Trying username/password pair: user :user
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: msfadmin:msfadmin
NSE: [ssh-brute] Trying username/password pair: user:user
NSE: [ssh-brute] Trying username/password pair: user :
NSE: [ssh-brute] Trying username/password pair: admin:
NSE: [ssh-brute] Trying username/password pair: root:
NSE: [ssh-brute] Trying username/password pair: user :1234
NSE: [ssh-brute] Trying username/password pair: admin:1234
NSE: [ssh-brute] Trying username/password pair: root:1234
NSE: [ssh-brute] Trying username/password pair: user :admin
NSE: [ssh-brute] Trying username/password pair: root:admin
NSE: [ssh-brute] Trying username/password pair: user :password
NSE: [ssh-brute] Trying username/password pair: admin:password
NSE: [ssh-brute] Trying username/password pair: root:password
NSE: [ssh-brute] Trying username/password pair: user :msfadmin
NSE: [ssh-brute] Trying username/password pair: admin:msfadmin
NSE: [ssh-brute] Trying username/password pair: root:msfadmin
NSE: [ssh-brute] Trying username/password pair: user :user
NSE: [ssh-brute] Trying username/password pair: admin:user
NSE: [ssh-brute] Trying username/password pair: root:user
NSE: [ssh-brute] Trying username/password pair: user :pinco
NSE: [ssh-brute] Trying username/password pair: admin:pinco
NSE: [ssh-brute] Trying username/password pair: root:pinco
NSE: [ssh-brute] Trying username/password pair: user :password123
NSE: [ssh-brute] Trying username/password pair: admin:password123
NSE: [ssh-brute] Trying username/password pair: root:password123
Nmap scan report for 192.168.51.101
Host is up (0.0065s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-brute:
|   Accounts:
|     msfadmin:msfadmin - Valid credentials
|     user:user - Valid credentials
|_  Statistics: Performed 28 guesses in 27 seconds, average tps: 1.0

Nmap done: 1 IP address (1 host up) scanned in 26.59 seconds
```