EPICODE

Esercizio
Scansione dei servizi

Traccia: Tecniche di scansione con Nmap

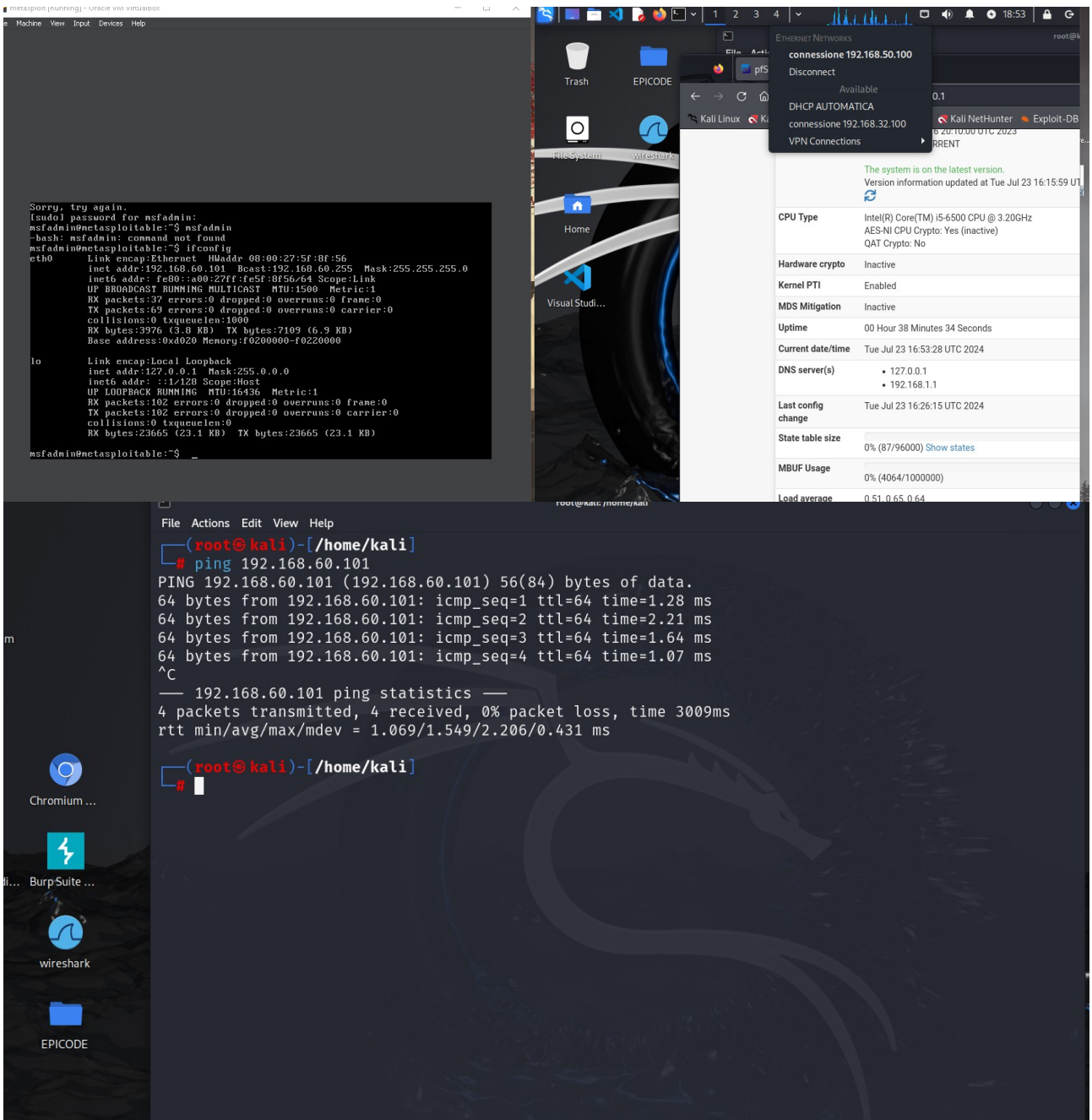
Si richiede allo studente di effettuare le seguenti scansioni sul target **Metasploitable** (target e attaccante devono essere su due reti diverse):

- OS fingerprint
- Syn Scan
- TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
- Version detection

A valle delle scansioni, è prevista la produzione di un **report** contenente le seguenti info (dove disponibili):

- IP
- Sistema Operativo
- Porte Aperte
- Servizi in ascolto con versione
- Descrizione dei servizi

Metasploitable e Kali si trovano su due reti diverse grazie a Pfsense



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.60.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 12:55 EDT
Nmap scan report for 192.168.60.101
Host is up (0.0015s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (97%)
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (97%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.08 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.60.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 12:55 EDT
Nmap scan report for 192.168.60.101
Host is up (0.0021s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 5.11 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.60.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 12:56 EDT
Nmap scan report for 192.168.60.101
Host is up (0.0019s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
53/tcp open  domain  Unbound
80/tcp open  http    nginx

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.01 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.60.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 12:56 EDT
Nmap scan report for 192.168.60.101
Host is up (0.0027s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
```

53/tcp open domain Unbound
80/tcp open http   nginx
|_http-title: pfSense - Login
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (97%)
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (97%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE (using port 80/tcp)
HOP RTT   ADDRESS
1   2.75 ms 192.168.60.101

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 23.44 seconds