Traccia:

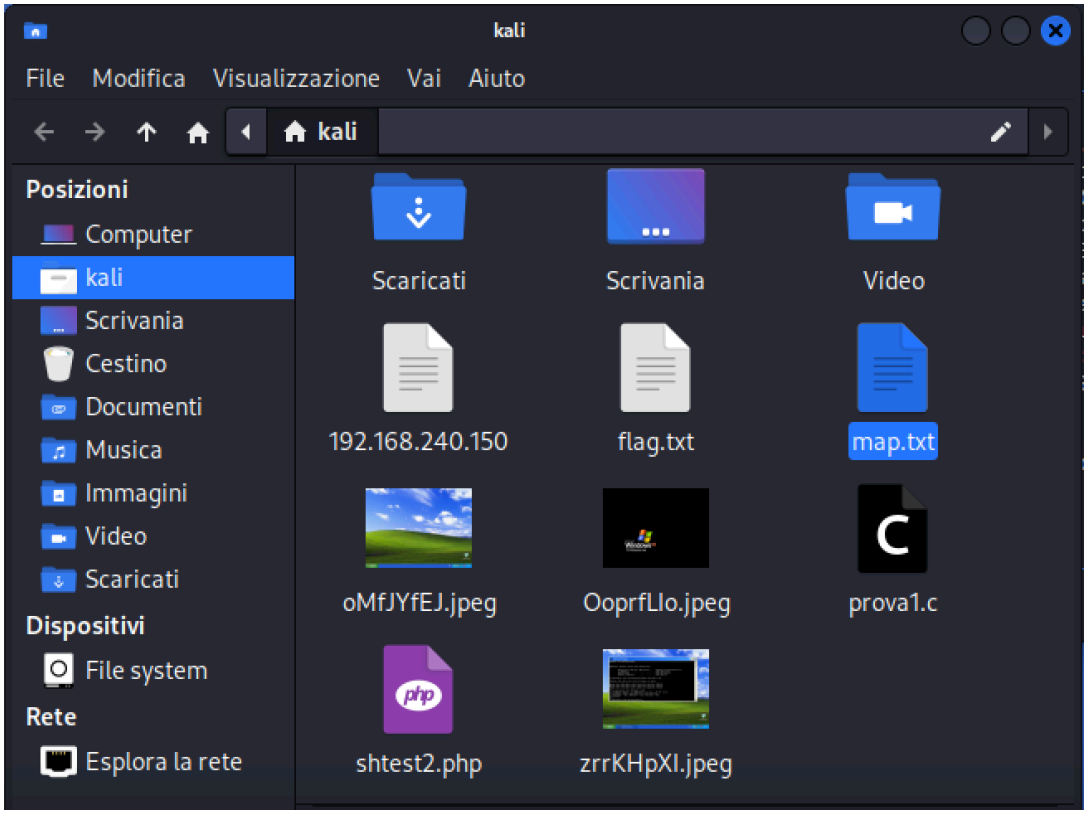
Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall'esterno. Abbiamo visto che a livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato.
La macchina Windows XP che abbiamo utilizzato ha di default il Firewall disabilitato.
L'esercizio di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno. Per questo motivo:

1. Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP
2. Effettuate una scansione con nmapsulla macchina target (utilizzate lo switch–sV, per la service detectione -o nomefilereportper salvare in un file l'output)
3. Abilitare il Firewall sulla macchina Windows XP
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch–sV.
5. Trovare le eventuali differenze e motivarle.

Scansione con firewall disabilitato

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -o map.txt 192.168.240.150
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-05 14:00 CET
Nmap scan report for 192.168.240.150
Host is up (0.0031s latency).
Not shown: 997 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 XP microsoft-ds
MAC Address: 26:8C:1E:D5:C2:63 (Unknown)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows
ws_xp

Service detection performed. Please report any incorrect results at h
.
Nmap done: 1 IP address (1 host up) scanned in 20.62 seconds
```



Scansione con firewall abilitato

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.240.150
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-05 14:12 CET
Nmap scan report for 192.168.240.150
Host is up (0.0014s latency).
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 26:8C:1E:D5:C2:63 (Unknown)

Service detection performed. Please report any incorrect results at htt
.
Nmap done: 1 IP address (1 host up) scanned in 34.91 seconds
```

Le differenze fra le due scansioni sono:

- Il tempo impiegato, dovuto ai maggiori tempi di risposta dovuti alla presenza del firewall
- Le porte mostrate dalla scansione. Nel primo caso ci vengono mostrate le tre porte aperte, mentre nel secondo caso ci dice che lo stato delle porte è ignoto
- Informazioni sul sistema operativo, nel primo caso la scansione ci dice che sulla macchina scansionata è utilizzato il sistema operativo Windows xp, nel secondo invece non abbiamo informazioni a riguardo

La causa è che la scansione che prova a fare nmap sulla macchina windows viene rilevata dal firewall come connessione proveniente dall'esterno e quindi bloccata, inoltre il firewall di windows non permette di effettuare ping verso windows e nmap utilizza dei ping per effettuare la scansione a meno che non si inserisca anche il comando -Pn.