

# Analisi delle Vulnerabilità & Azioni di Rimedio

CSPT0324 Modulo 3



Yilei Wu

29 Settembre 2024

# Indice

<b>INTRODUZIONE ALL'ESERCIZIO</b>	<b>3</b>
TRACCIA	3
CONSEGNA	3
SELEZIONE DELLE VULNERABILITÀ	3
<b>REQUISITI</b>	<b>4</b>
CONFIGURAZIONE DELLA RETE DEL LABORATORIO VIRTUALE	4
<i>Impostare Kali in DHCP</i>	4
<i>Impostare Metasploitable2 in DHCP</i>	5
PFSENSE	5
<i>Premessa: cos'è pfSense</i>	5
<i>Installazione di pfSense</i>	6
<i>Prima configurazione di pfSense</i>	9
<i>Rete 192.168.50.0/24 su pfSense</i>	10
INSTALLAZIONE DI TENABLE NESSUS	12
<i>Download e installazione</i>	12
<i>Avvio del servizio e primo avvio di Nessus</i>	12
<b>ANALISI DELLA RETE</b>	<b>13</b>
RICERCA HOST TARGET METASPLOITABLE2	13
INDIVIDUAZIONE INDIRIZZO IP TARGET	14
<b>ANALISI DELLE VULNERABILITÀ</b>	<b>15</b>
SCANSIONE NMAP	15
SCANSIONE NESSUS	17
<i>Configurazione scan</i>	17
<i>Esportazione report</i>	18
ANALISI DEI RISULTATI	19
<b>AZIONI DI RIMEDIO</b>	<b>21</b>
CREDENZIALI PFSENSE	21
VNC SERVER 'PASSWORD' PASSWORD (TRACCIA - LIVELLO CRITICO)	22
NFS SHARES WORLD READABLE (TRACCIA - LIVELLO ALTO)	23
BIND SHELL BACKDOOR DETECTION (TRACCIA - LIVELLO CRITICO)	24
APACHE TOMCAT SEOL (<= 5.5.x) (LIVELLO CRITICO)	25
SSL VERSION 2 AND 3 PROTOCOL DETECTION (LIVELLO CRITICO)	26
ISC BIND SERVICE DOWNGRADE / REFLECTED DOS (LIVELLO ALTO)	27
CONSIDERAZIONI SULLA SICUREZZA DI METASPLOITABLE2	28
<i>Firewall pfSense</i>	28
<i>Gestione dei servizi non necessari</i>	29
<i>Conclusione</i>	29
<b>SCANSIONE DOPO LE AZIONI DI RIMEDIO</b>	<b>30</b>
<b>CONSIDERAZIONI FINALI</b>	<b>31</b>
<b>DOCUMENTAZIONE ALLEGATA</b>	<b>31</b>

## Introduzione all'esercizio

### Traccia

Effettuare una scansione completa sul target Metasploitable.

Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità **critiche** e provate ad **implementare delle azioni di rimedio**.

N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili.

Vi consigliamo tuttavia di utilizzare magari questo approccio **per non più di una vulnerabilità**.

Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

Ai fini della soluzione, abbiamo scelto le vulnerabilità in giallo nella figura in slide 3.

### Consegna

1. Scansione iniziale dove si vede il grafico con tutte le vulnerabilità e le vulnerabilità da risolvere (tecnico, già riassunto) - **ScansioneInizio.pdf**
2. **Screenshot e spiegazione dei passaggi della remediation - RemediationMeta.pdf**
3. Scansione dopo le modifiche che evidenzia la risoluzione dei problemi/vulnerabilità (il grafico che mostra tutte le vulnerabilità) - **ScansioneFine.pdf**

**Oppure un report unico, a vostra scelta. Penso sia più comodo farne tre comunque.**

**Nota: i report possono essere lasciati in inglese, senza problemi.**

Se risolvete le 4 vulnerabilità, potete risolverne una quinta (a scelta), ad esempio con una regola di firewall

### Selezione delle Vulnerabilità



<input type="checkbox"/>	Sev ▼	Score ▼	Name ▲
<input type="checkbox"/>	CRITICAL	10.0 *	NFS Exported Share Information Disclosure
<input type="checkbox"/>	CRITICAL	10.0 *	rexecd Service Detection
<input type="checkbox"/>	CRITICAL	10.0	Unix Operating System Unsupported Version Detection
<input type="checkbox"/>	CRITICAL	10.0 *	VNC Server 'password' Password
<input type="checkbox"/>	CRITICAL	9.8	Bind Shell Backdoor Detection

## Requisiti

### Configurazione della rete del Laboratorio Virtuale

La rete target del laboratorio virtuale ai fini dell'esercizio è la seguente:

pfSense con la funzione di Server DHCP/ Firewall / Router

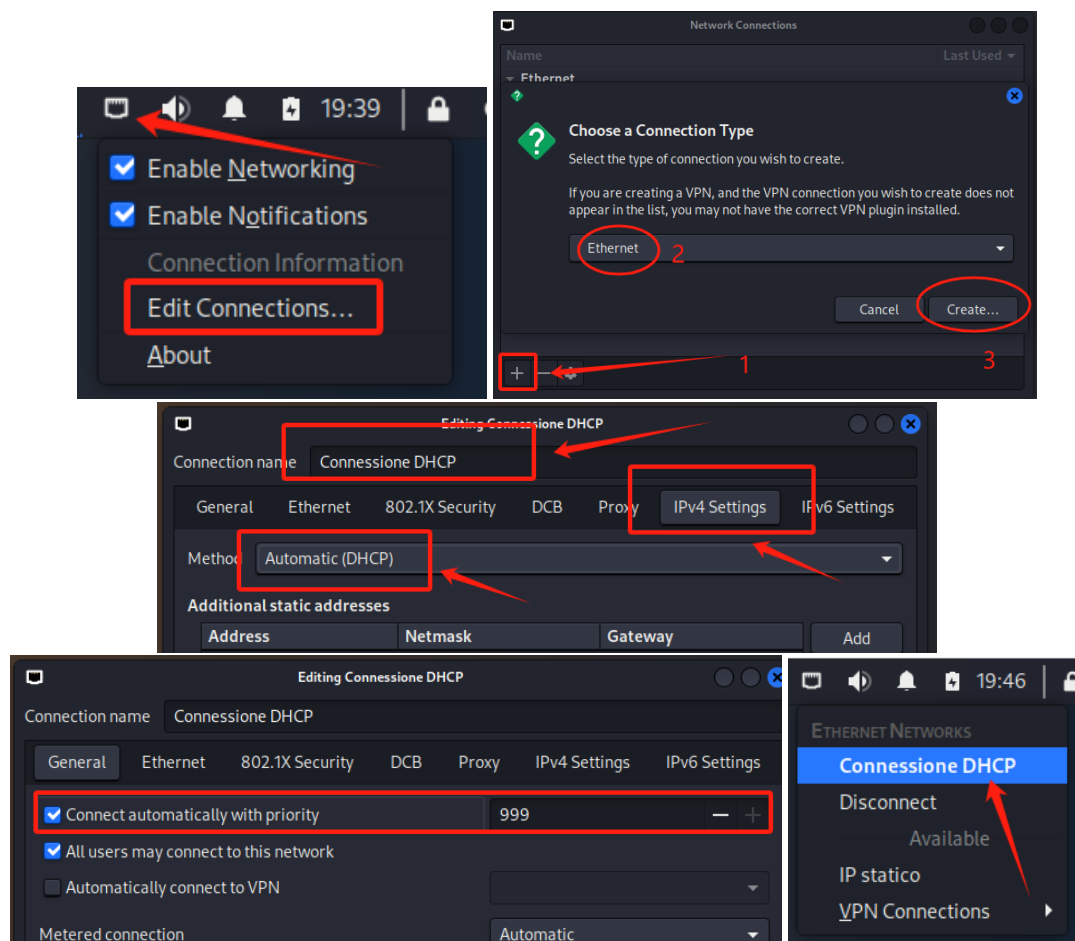
Kali Linux in DHCP su rete 192.168.1.0/24

Metasploitable2 in DHCP su rete 192.168.50.0/24

Interfaces			
WAN	↑	1000baseT <full-duplex>	10.0.2.15
LAN	↑	1000baseT <full-duplex>	192.168.1.1
LAN2	↑	1000baseT <full-duplex>	192.168.50.1

### Impostare Kali in DHCP

Il metodo più semplice per passare in DHCP è click tasto destro del mouse sull'icona di rete > Edit connections

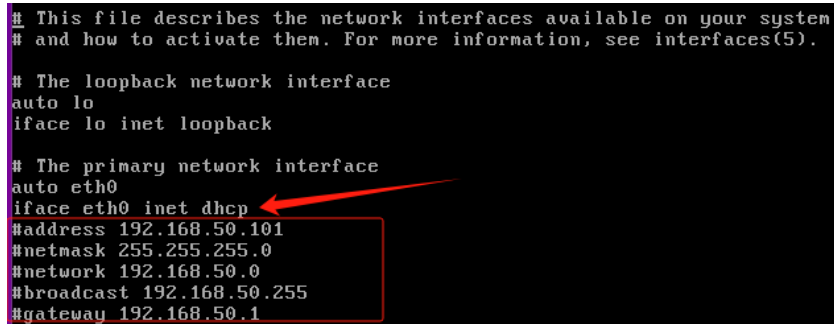


Creare una nuova connessione, mettere priorità massima 999 (cosicché ai prossimi avvii sia in DHCP in automatico), configurare come da immagine la scheda IPv4 e dare un nome personalizzato alla connessione.

Per fare lo switch alla connessione DHCP o STATICA, click sinistro sull'icona di rete e selezionare la rete desiderata.

## Impostare Metasploitable2 in DHCP

Per impostare in DHCP (stato di default della macchina) lanciare il comando **sudo nano /etc/network/interfaces** e modificare dopo inet (vedi freccia) static in **dhcp** (in minuscolo) e commentare con **#** (SHIFT+3 [Layout EN]) o cancellare, ogni riga all'interno del rettangolo rosso.



```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp
#address 192.168.50.101
#netmask 255.255.255.0
#network 192.168.50.0
#broadcast 192.168.50.255
#gateway 192.168.50.1
```

**NB:** Nel corso dell'esercizio, durante i tentativi richiesti, la macchina virtuale Metasploitable2 è stata accidentalmente compromessa e distrutta. Per proseguire con l'attività, è stato quindi importato un backup della macchina effettuato prima degli interventi descritti nei paragrafi successivi. Questo spiega la differenza nell'indirizzo IP: inizialmente Metasploitable2 aveva l'IP 192.168.50.101, che successivamente è diventato 192.168.50.103. Pur trattandosi della stessa macchina con la medesima configurazione, il cambiamento è dovuto all'assegnazione di un nuovo indirizzo IP da parte di pfSense, causata dalla modifica del MAC address.

## pfSense

Premessa: cos'è pfSense

pfSense è un sistema operativo basato su FreeBSD progettato per essere utilizzato come firewall e router. È una soluzione open source e offre una vasta gamma di funzionalità per la gestione della rete. Ecco alcune delle sue caratteristiche principali:

1. **Firewall e Router:** pfSense è principalmente usato per proteggere le reti gestendo il traffico in entrata e in uscita, configurando regole di filtraggio avanzate.
2. **Interfaccia web:** La configurazione e la gestione di pfSense avviene tramite un'interfaccia web intuitiva, rendendolo accessibile anche a utenti non esperti.
3. **VPN (Virtual Private Network):** pfSense supporta diversi tipi di VPN come IPsec, OpenVPN e PPTP, consentendo la connessione sicura tra reti remote.
4. **Traffic Shaping:** Offre funzionalità di "traffic shaping", che permette di prioritizzare determinati tipi di traffico, ad esempio limitando la banda per il download e assicurando che le applicazioni critiche abbiano una connettività ottimale.
5. **Monitoraggio e reportistica:** pfSense fornisce strumenti di monitoraggio del traffico e può generare report dettagliati per analizzare l'attività della rete.
6. **Gestione degli accessi:** Può essere configurato per gestire l'accesso a internet per gli utenti della rete, con funzioni come il blocco di siti specifici o la limitazione della larghezza di banda.
7. **Ridondanza e Failover:** Supporta funzionalità avanzate come la ridondanza e il failover per garantire l'affidabilità e la continuità del servizio.

In sintesi, pfSense è un sistema versatile, utilizzato in contesti aziendali e domestici per la gestione di firewall e rete con elevate prestazioni e flessibilità.

La licenza FreeBSD consente di modificare e utilizzare il codice in progetti chiusi o commerciali, richiedendo solo di dare credito agli autori originali.

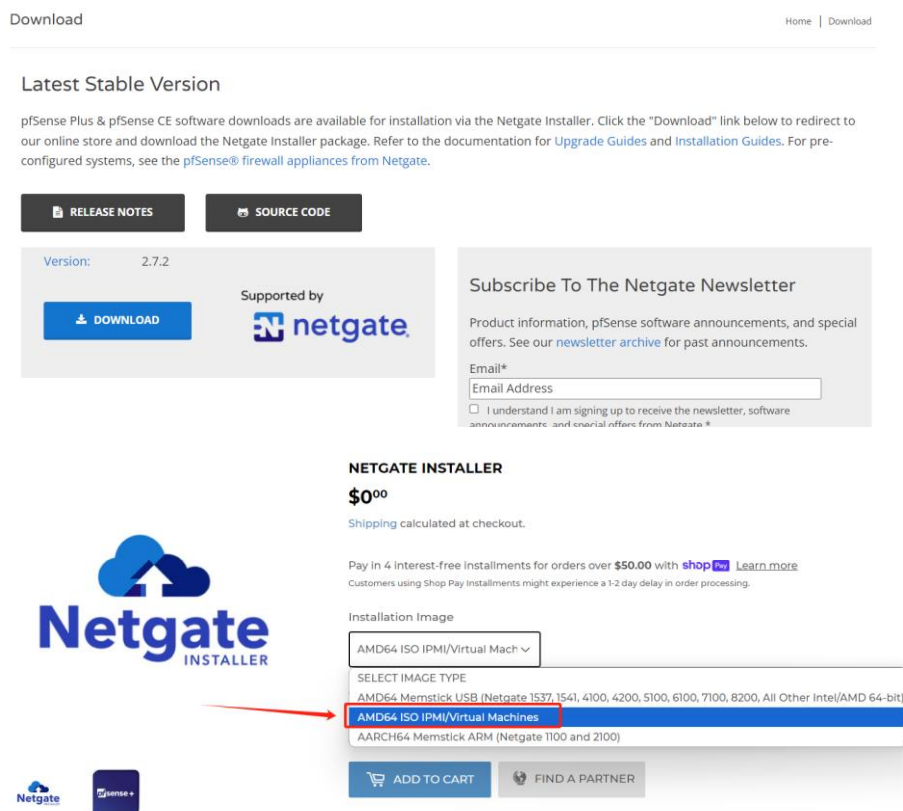
Per una migliore comprensione, il ruolo di pfSense in questo laboratorio virtuale può essere paragonato, per analogia, a quello di un modem/router in una rete domestica, svolgendo funzioni di firewall e gestione del traffico tra le macchine collegate alla rete.

In questo esercizio sarà il ponte di comunicazione tra Kali Linux e Metasploitable2 situate in 2 reti diverse.

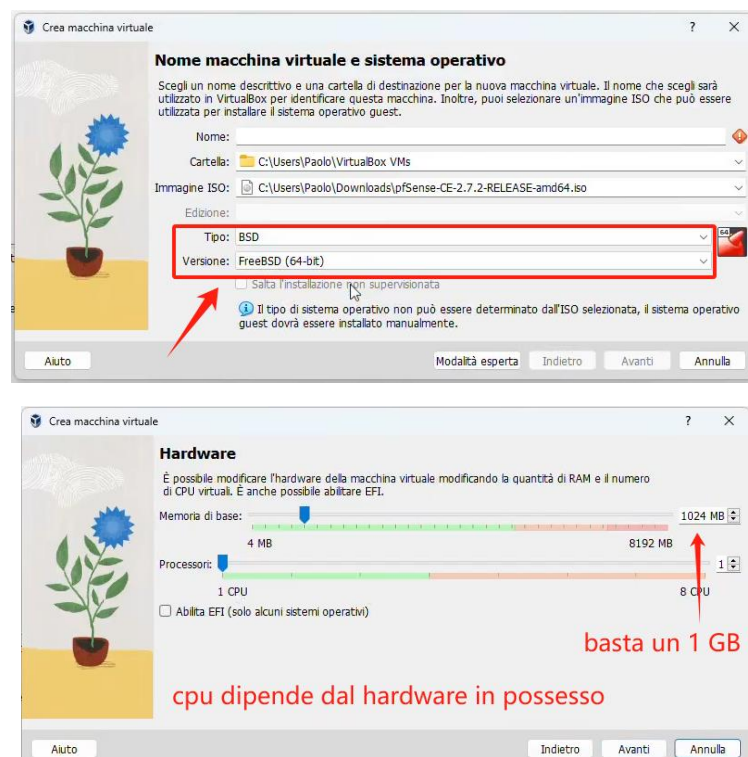


## Installazione di pfSense

Scaricare l'immagine .ISO scegliendo la versione per Virtual Machine dal sito ufficiale <https://www.pfsense.org/download/> e seguire le istruzioni per il download.

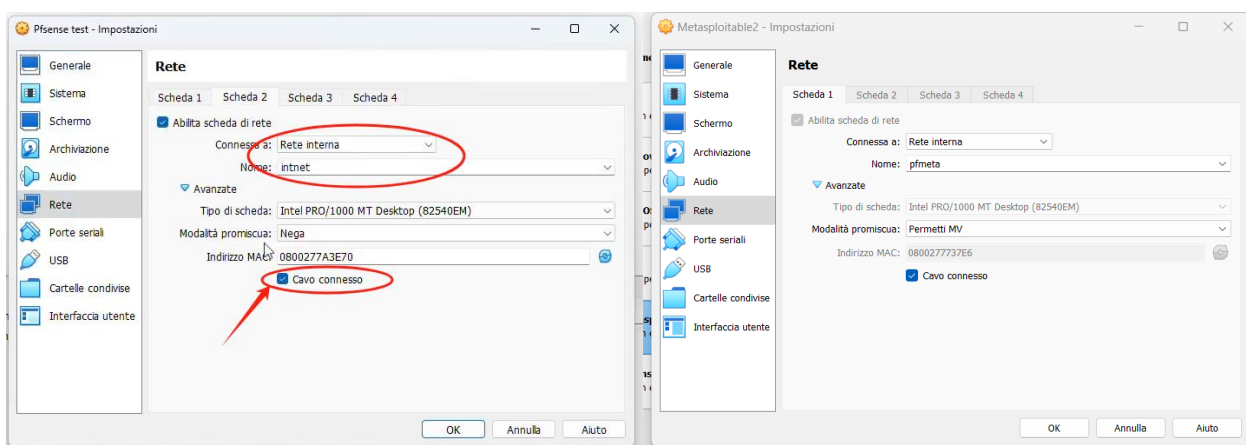


Si richiama il report M1 W1 D3 per le istruzioni sull'installazione di un sistema operativo con Virtual Box. Di seguito si precisano le configurazioni di installazione per pfSense:



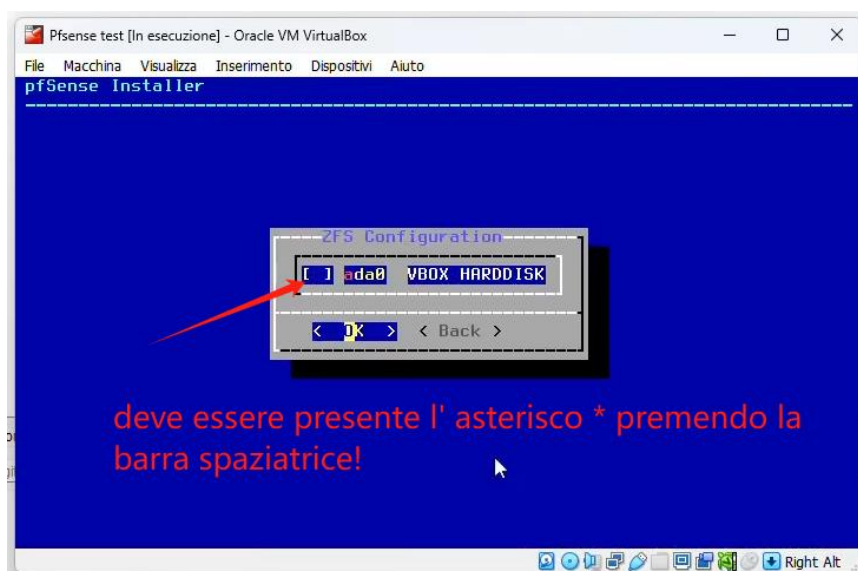


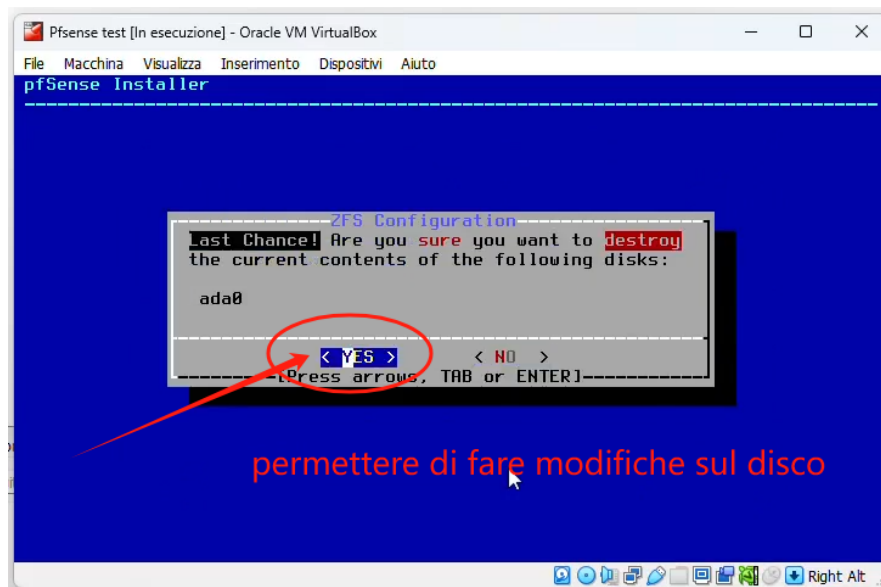
Prima di avviare la VM, è molto importante la configurazione delle schede di rete 1, 2 e 3, abilitate, rispettivamente in **NAT**, **Rete Interna: intnet** e **Rete Interna: pfmeta** sempre in ogni caso con **Cavo connesso**.



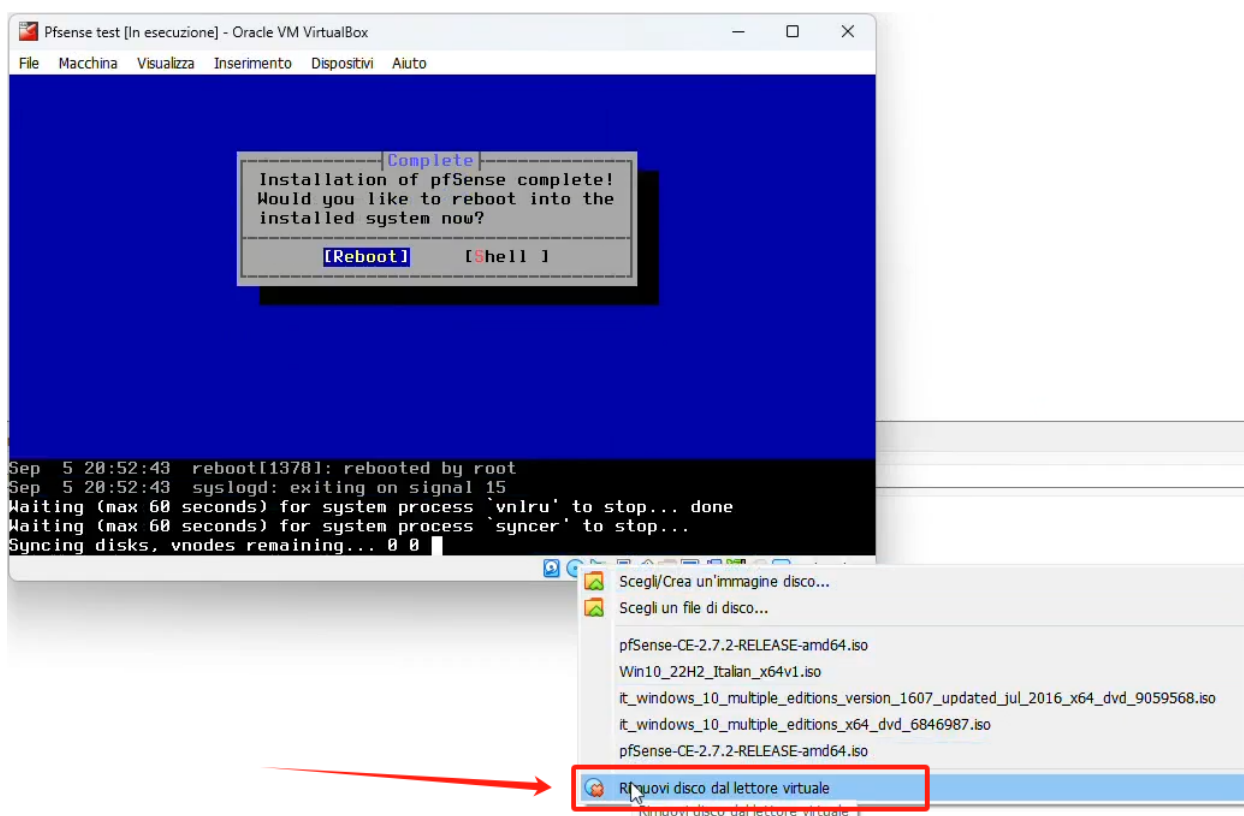
Avviare la macchina virtuale di pfSense e seguire le istruzioni intuitive per l'installazione, procedendo sempre con il tasto Invio.

**Attenzione all'unico passaggio da prestare la massima attenzione per selezionare il disco e dare il permesso alla modifica dello stesso.**





Alla fine del procedimento, riavviare la VM e durante il processo di riavvio, rimuovere il disco virtuale dalla VM per evitare che la macchina avvii il sistema operativo dal disco di installazione (l'ISO scaricata), invece di avviarlo dal disco virtuale.



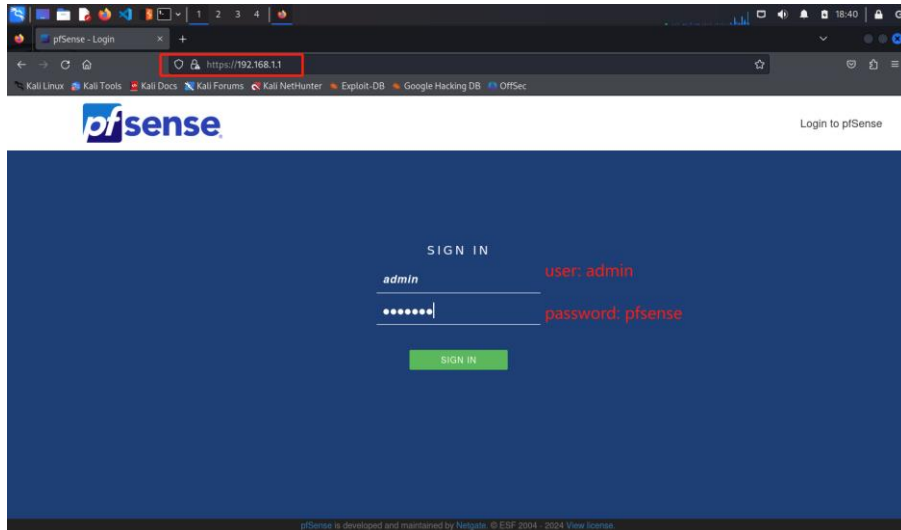


## Prima configurazione di pfSense

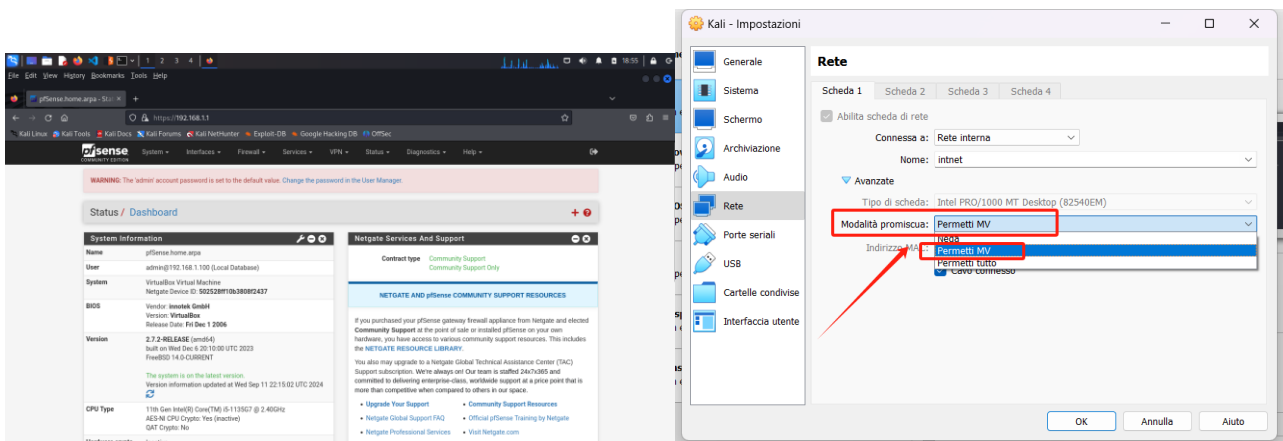
Kali Linux deve avere la configurazione in Virtual Box con la scheda di rete in rete interna con cavo connesso e deve essere in DHCP. Verificare con il comando **ip a** su terminale Kali che sia connessa correttamente alla rete di pfSense.

L'indirizzo di gateway, di default, dovrebbe essere **192.168.1.1** come da immagini a seguire. Pertanto da browser, digitando l'indirizzo IP di gateway appare la pagina di configurazione di pfSense (proseguire lo stesso in caso di avvisi di sicurezza da parte del browser).

Credenziali di default: user **admin** password **pfSense**



Seguire passo passo la configurazione intuitiva di benvenuto.

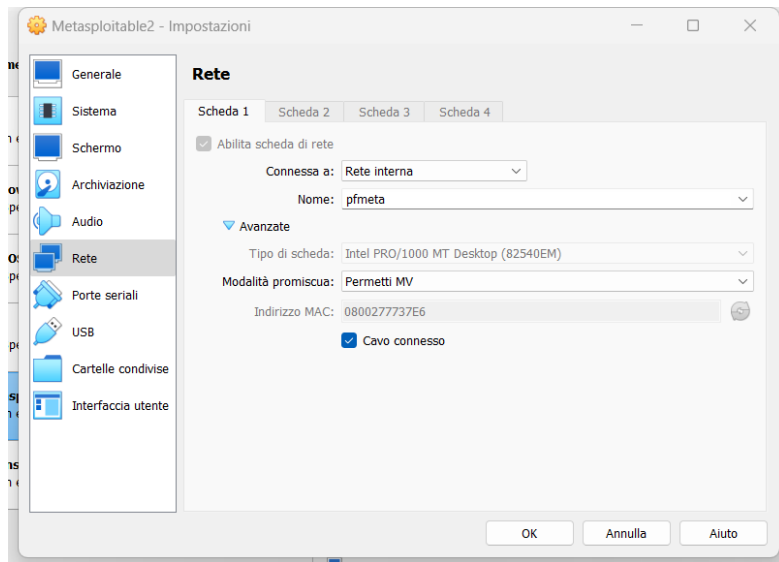


Da questa schermata, la Dashboard si possono effettuare tutte le configurazioni e impostazioni desiderate.

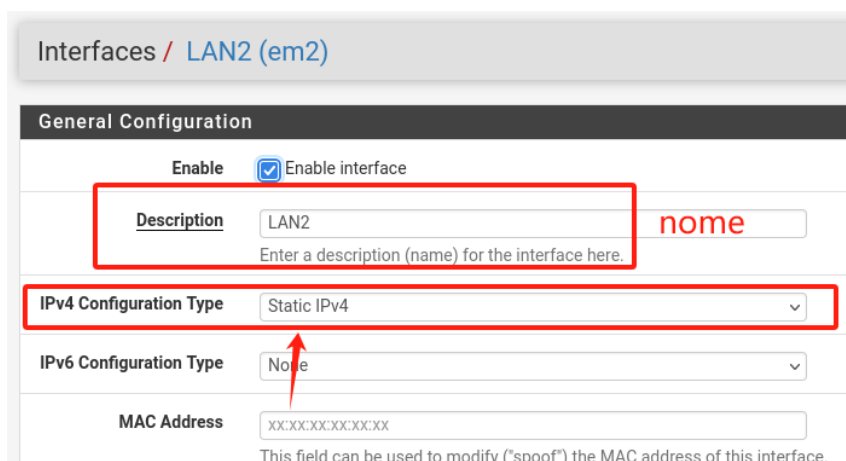
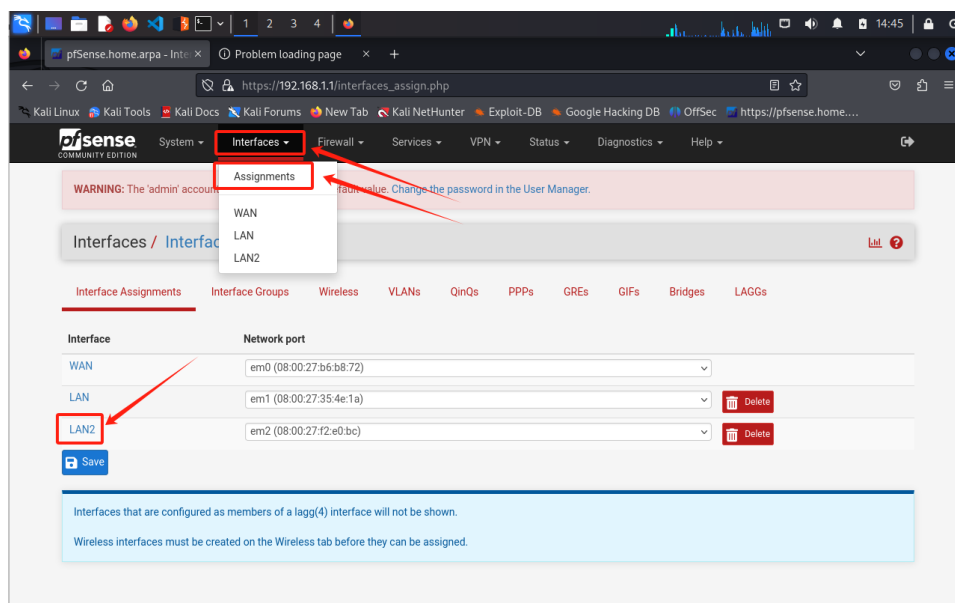
Per assicurarsi di mantenere attivo la connessione a internet, rete esterna, sulla macchina Kali Linux è consigliabile attivare la modalità promiscua. Questa modalità consente alla VM di vedere tutto il traffico sulla rete a cui è connessa, permettendo a pfSense di funzionare correttamente come router. **Attivare pertanto su pfSense tale funzione.**

Rete 192.168.50.0/24 su pfSense

Sulla scheda di configurazione di Virtual Box per la macchina Metasploitable2, cambiare il nome della rete interna a **pfmata** (nome deciso nel paragrafo precedente relativo all'installazione).



Da Kali recarsi nella pagina di configurazione di pfSense su **Interfaces > Assignments** e cliccare su **opt1** (quest'ultimo si potrà modificarlo con un nome personalizzato, LAN2 in questo caso).



**Static IPv4 Configuration**

IPv4 Address: 192.168.50.1 / 24

IPv4 Upstream gateway: None

+ Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface. Gateways can be managed by [clicking here](#).

**Reserved Networks**

Block private networks

Inserire l'indirizzo di gateway, in questo caso il 192.168.50.1 in subnet 24 e salvare.

Attivare il servizio del DHCP Server in **Services > DHCP Server**

Services / DHCP Server / LAN2

ISC DHCP has reached end-of-life and will be removed in a future release.

LAN2

**General DHCP Options**

DHCP Backend: ISC DHCP

Enable DHCP server on LAN2 interface: ☒

BOOTP: ☐ Ignore BOOTP queries

Deny Unknown Clients: ☐ Allow all clients

Ignore Denied Clients: ☐ Ignore denied clients rather than reject

**Primary Address Pool**

Subnet: 192.168.50.0/24

Subnet Range: 192.168.50.1 - 192.168.50.254

Address Pool Range: 192.168.50.100 To 192.168.50.254

The specified range for this pool must not be within the range configured on any other address pool for this interface.

Additional Pools: + Add Address Pool

If additional pools of addresses are needed inside of this subnet outside of the above range, they may be specified here.

Impostare il range di indirizzi IP che il server DHCP potrà assegnare e salvare.

Dopo tale configurazione, avviare Metasploitable2 e lanciare il comando **ip a** o **ifconfig** per ottenere l'indirizzo IP appartenente alla rete 192.168.50.0/24.

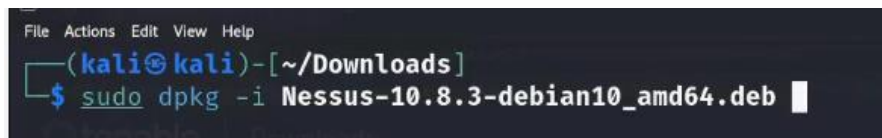
## Installazione di Tenable Nessus

### Download e installazione

Per l'installazione di Tenable Nessus, sulla macchina Kali Linux recarsi sul sito ufficiale <https://www.tenable.com/downloads/nessus?loginAttempted=true> e scaricare la versione per Linux Debian amd64

Terminato il download, aprire il terminale shell nella stessa cartella del file scaricato e lanciare il comando

```
sudo dpkg -i <nome_file.deb>
```



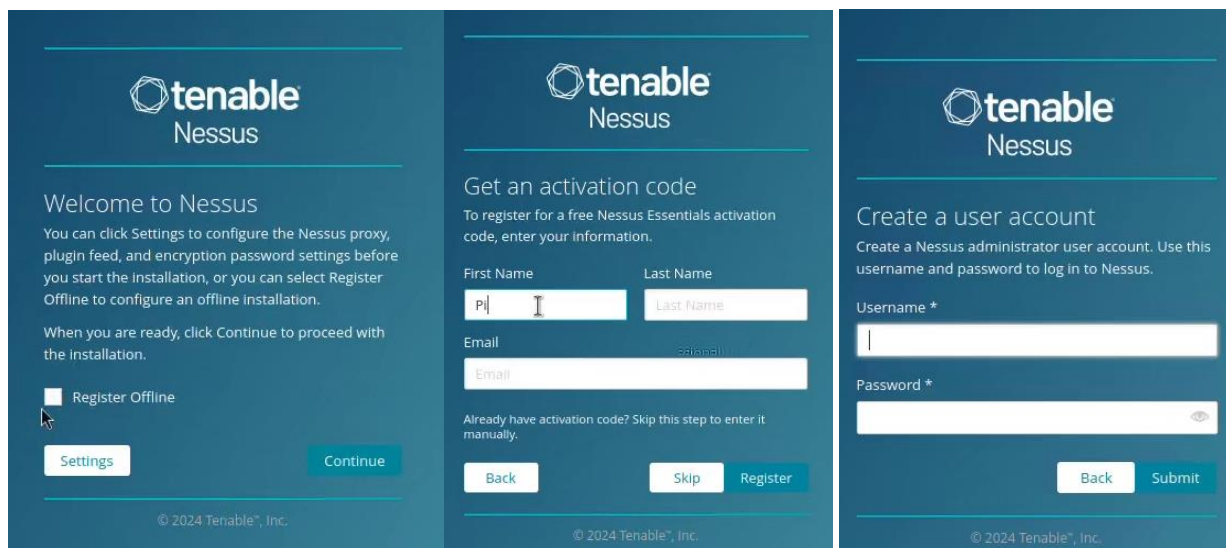
### Avvio del servizio e primo avvio di Nessus

Per avviare il servizio digitare il comando **sudo systemctl start nessusd**

Nel caso servisse chiuderlo, il comando è **sudo systemctl stop nessusd**

Dopo aver avviato il servizio aprire sul browser il link di configurazione:

<https://localhost:8834/> oppure <https://kali:8834/> oppure <https://127.0.0.1:8834/>



**Non selezionare la registrazione offline**, ma continue, creando un account lasciando un indirizzo email valido per ricevere il codice di attivazione e creare username e password.

Successivamente effettuare l'accesso e su richiesta inserire il codice di attivazione ricevuta via email.

Per i futuri accessi:

1. Attivare il servizio **sudo systemctl start nessusd**
2. Aprire la pagina di configurazione <https://127.0.0.1:8834/>
3. Accedere con le credenziali note

Se ci fossero errori di caricamento dei plugin, aggiornarli con il comando:

```
sudo /opt/nessus/sbin/nessuscli update
```

Attendere fino al termine del download di tutti i plugin, se necessario.

## Analisi della rete

### Ricerca host target Metasploitable2

Sebbene si disponga della piena configurazione del laboratorio virtuale, si simula un contesto di tipo black box. Attraverso l'esecuzione del comando **ip a**, è possibile ottenere l'indirizzo IP della macchina Kali Linux, che funge da punto di ingresso nel laboratorio.

```
(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:88:c5:b4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.101/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
        valid_lft 4973sec preferred_lft 4973sec
    inet6 fe80::aadf:3f4f:33a0:c954/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

L'indirizzo IP assegnato alla macchina Kali Linux è **192.168.1.101**, configurato dal gateway di rete con indirizzo IP **192.168.1.1**. Si procede con la scansione della rete **192.168.1.0/24** per identificare gli host attivi. Sono stati utilizzati due metodi di scansione: una scansione Nmap (**-sn** scansione di tipo “ping”) e una scansione ARP (sulla scheda di rete eth0). I comandi eseguiti sono i seguenti:

**nmap -sn 192.168.1.0/24**      **sudo arp-scan --interface=eth0 192.168.1.0/24**

```
(kali@kali)-[~]
$ nmap -sn 192.168.1.0/24

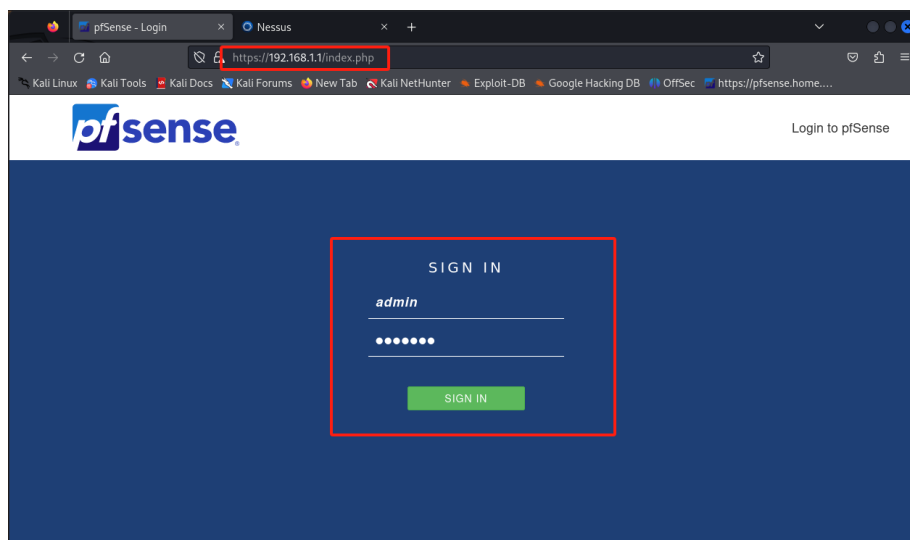
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-27 13:57 EDT
Nmap scan report for pfSense.home.arp (192.168.1.1)
Host is up (0.0011s latency).
MAC Address: 08:00:27:35:4E:1A (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.101
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 1.92 seconds

(kali@kali)-[~]
$ sudo arp-scan --interface=eth0 192.168.1.0/24

[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:88:c5:b4, IPv4: 192.168.1.101
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1      08:00:27:35:4e:1a      (Unknown)




1 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.872 seconds (136.75 hosts/sec). 1 responded
```

I risultati della scansione non mostrano esiti favorevoli: l'indirizzo IP **192.168.1.1** corrisponde al gateway di rete, mentre l'indirizzo IP **192.168.1.101** è associato alla macchina Kali Linux, probabilmente alle limitazioni imposte dal router. Pertanto, si procede con un tentativo di intrusione nella configurazione del router accedendo all'indirizzo del gateway tramite browser, utilizzando l'URL <https://192.168.1.1/>.





In questo caso favorevole, è stato individuato che il router in uso è pfSense e che l'amministratore di rete ha lasciato le credenziali di accesso predefinite, ovvero username: **admin** e password: **pfSense**. Dopo aver effettuato l'accesso, è possibile procedere con la gestione dell'intera rete.

Interfaces			
 WAN	↑	1000baseT <full-duplex>	10.0.2.15
 LAN	↑	1000baseT <full-duplex>	192.168.1.1
 LAN2	↑	1000baseT <full-duplex>	192.168.50.1

Dalla dashboard di pfSense, nella sezione **Interfaces**, si possono visualizzare gli indirizzi delle altre reti: **10.0.2.15** per la WAN e **192.168.50.1** per la LAN2.

Si procede con una scansione di Nmap sulla rete LAN2 per individuare gli host attivi.

```
(kali@kali)-[~]
$ nmap -sn 192.168.50.0/24

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-27 14:24 EDT
Nmap scan report for 192.168.50.1
Host is up (0.0017s latency)
Nmap scan report for 192.168.50.100
Host is up (0.0041s latency)
Nmap done: 256 IP addresses (2 hosts up) scanned in 3.98 seconds
```

## Individuazione indirizzo IP target

Per confermare l'appartenenza dell'indirizzo IP identificato alla macchina target, si procede con l'OS fingerprinting utilizzando Nmap. A tal fine, viene eseguito il seguente comando:

**nmap -O 192.168.50.100**

```
(kali@kali)-[~]
$ nmap -O 192.168.50.100

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-27 14:30 EDT
Nmap scan report for 192.168.50.100
Host is up (0.0034s 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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded), Linux 2.6.29 (Gentoo)
Network Distance: 2 hops
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.16 seconds
```

Dalla scansione effettuata, si conferma con elevata probabilità che il kernel Linux **2.6** appartenga a Metasploitable2, con una distanza di **2 hops**. Inoltre, dalla scansione sono state identificate le porte aperte e i relativi servizi associati.

# Analisi delle Vulnerabilità

## Scansione Nmap

Si procede con una scansione completa utilizzando Nmap e il relativo database. Viene eseguito il seguente comando:

```
TARGET="192.168.50.100"; REPORT="report-$(date +%Y-%m-%d_%H-%M-%S)-${TARGET}"; ;sudo nmap -A -p- --script "all" -oA ${REPORT} -T4 ${TARGET} && xsltproc ${REPORT}.xml -o ${REPORT}.html
```

### Dettagli del Comando

1. **TARGET="192.168.50.100":**
  - Imposta la variabile TARGET all'indirizzo IP dell'host che si desidera scansionare.
2. **REPORT="report-\$(date +%Y-%m-%d\_%H-%M-%S)-\${TARGET}":**
  - Imposta la variabile REPORT per generare un nome di file unico per il report, includendo la data e l'ora attuale.
3. **sudo nmap:**
  - Esegue Nmap con privilegi di superutente, il che è spesso necessario per alcune funzionalità di scansione.
4. **-A:**
  - Abilita il rilevamento aggressivo, che include:
    - Rilevamento del sistema operativo (OS detection).
    - Rilevamento delle versioni dei servizi.
    - Esecuzione di traceroute per mappare il percorso di rete verso l'host target.
    - Rilevamento degli script Nmap.
5. **-p-:**
  - Scansiona tutte le porte, dalla 1 alla 65535, invece delle porte standard (1-1024).
6. **--script "all":**
  - Esegue tutti gli script Nmap disponibili. Questo include vari script per:
    - **Rilevamento delle vulnerabilità.**
    - Controllo della configurazione dei servizi.
    - Esecuzione di test specifici per determinati protocolli e applicazioni.
7. **-oA \${REPORT}:**
  - Salva i risultati della scansione in diversi formati:
    - .nmap: formato testo di Nmap.
    - .xml: formato XML.
    - .gnmap: formato per l'output in griglia.
8. **-T4:**
  - Imposta il livello di velocità della scansione su "4" (Aggressivo), che rende la scansione più veloce, ma con un rischio maggiore di rilevamento da parte di sistemi di intrusione.
9. **&& xsltproc \${REPORT}.xml -o \${REPORT}.html:**
  - Se la scansione Nmap ha successo, converte il file XML generato in un report HTML utilizzando xsltproc, rendendo più facile la lettura e l'analisi dei risultati.

### Cosa Scansiona

- **Tutte le porte (1-65535)** per rilevare servizi attivi.
- **Sistema operativo** in esecuzione sull'host target.
- **Versioni** dei servizi identificati su porte aperte.
- **Traceroute** per identificare il percorso di rete verso l'host.
- **Vulnerabilità** e configurazioni errate attraverso l'esecuzione di script.

```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~$  
[kali@kali]~$ TARGET="192.168.50.100"; REPORT="report-$(date +%Y-%m-%d_%H-%M-%S)-${TARGET}"; sudo nmap -A -p- --script "all" -oA ${REPORT} -T4  
$TARGET 66 xsltproc ${REPORT}.xml -o ${REPORT}.html  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-27 14:40 EDT  
Pre-scan script results:  
| broadcast-listener:  
| ether  
| ARP Request  
| sender ip sender mac target ip  
| 192.168.1.1 08:00:27:35:4e:1a 192.168.1.105  
| udp  
| DHCP  
| srvt ip cli ip mask gw dns vendor  
| 192.168.1.1 192.168.1.103 255.255.255.0 192.168.1.1 192.168.1.1 -  
| 192.168.1.1 192.168.1.105 255.255.255.0 192.168.1.1 192.168.1.1 -  
|_ hostmap-robtext: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtext.com/api/  
|_ http-robtext-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtext.com/api/  
|_ targets-ipv6-multicast-echo:  
| IP: fe80::a00:27ff:fe35:4e1a MAC: 08:00:27:35:4e:1a IFACE: eth0  
| Use --script-args=newtargets to add the results as targets  
|_ broadcast-dhcp-discover:  
| Response 1 of 1:  
| Interface: eth0  
| IP Offered: 192.168.1.105  
| Server Identifier: 192.168.1.1  
| Subnet Mask: 255.255.255.0  
| Router: 192.168.1.1  
| Domain Name Server: 192.168.1.1  
| Domain Name: home.arpa  
|_ targets-asn:  
|_ targets-asn.asn is a mandatory parameter  
|_ leap-info: please specify an interface with -e  
Stats: 0:02:19 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 93.33% done; ETC: 14:42 (0:00:04 remaining)  
Stats: 0:04:07 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 100.00% done; ETC: 14:44 (0:00:00 remaining)  
Stats: 0:07:13 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan  
NSE Timing: About 49.06% done; ETC: 14:50 (0:03:11 remaining)  
Stats: 0:08:08 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan  
NSE Timing: About 87.24% done; ETC: 14:49 (0:00:35 remaining)  
Stats: 0:08:08 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan  
NSE Timing: About 87.24% done; ETC: 14:49 (0:00:35 remaining)  
Stats: 0:09:47 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan  
NSE Timing: About 87.24% done; ETC: 14:50 (0:00:50 remaining)  
Stats: 0:10:19 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan  
NSE Timing: About 87.24% done; ETC: 14:51 (0:00:54 remaining)  
  
Post-scan script results:  
| reverse-index:  
| 21/tcp: 192.168.50.100  
| 22/tcp: 192.168.50.100  
| 23/tcp: 192.168.50.100  
| 25/tcp: 192.168.50.100  
| 53/tcp: 192.168.50.100  
| 80/tcp: 192.168.50.100  
| 111/tcp: 192.168.50.100  
| 139/tcp: 192.168.50.100  
| 445/tcp: 192.168.50.100  
| 512/tcp: 192.168.50.100  
| 513/tcp: 192.168.50.100  
| 514/tcp: 192.168.50.100  
| 1099/tcp: 192.168.50.100  
| 1524/tcp: 192.168.50.100  
| 2049/tcp: 192.168.50.100  
| 2121/tcp: 192.168.50.100  
| 3306/tcp: 192.168.50.100  
| 3632/tcp: 192.168.50.100  
| 5432/tcp: 192.168.50.100  
| 5900/tcp: 192.168.50.100  
| 6000/tcp: 192.168.50.100  
| 6667/tcp: 192.168.50.100  
| 6697/tcp: 192.168.50.100  
| 8009/tcp: 192.168.50.100  
| 8180/tcp: 192.168.50.100  
| 8787/tcp: 192.168.50.100  
| 34181/tcp: 192.168.50.100  
| 40607/tcp: 192.168.50.100  
| 47589/tcp: 192.168.50.100  
| 59950/tcp: 192.168.50.100  
|_ creds-summary:  
| 192.168.50.100:  
| 8180/http:  
| tomcat:tomcat - Valid credentials  
| tomcat:tomcat - Valid credentials  
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 4735.37 seconds  
Warning: program compiled against libxml 212 using older 209
```

La scansione richiede un tempo variabile, potendo impiegare anche diverse ore a seconda della complessità della rete e del numero di porte da esaminare. In questo caso, il processo di scansione ha richiesto 4735.37 secondi, ovvero circa 1 ora e 20 minuti, per essere completato.

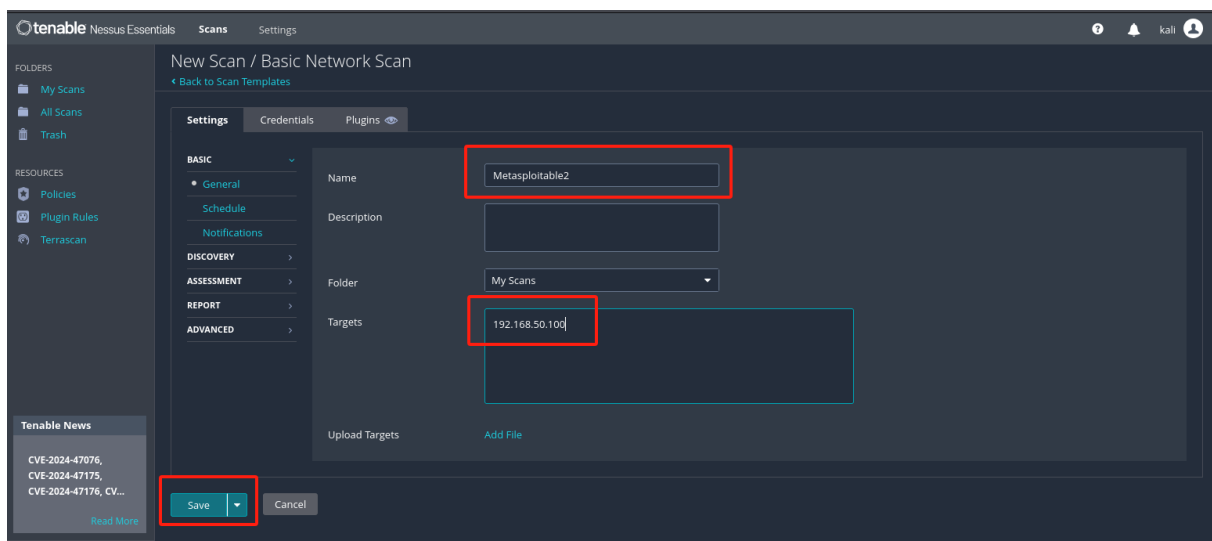
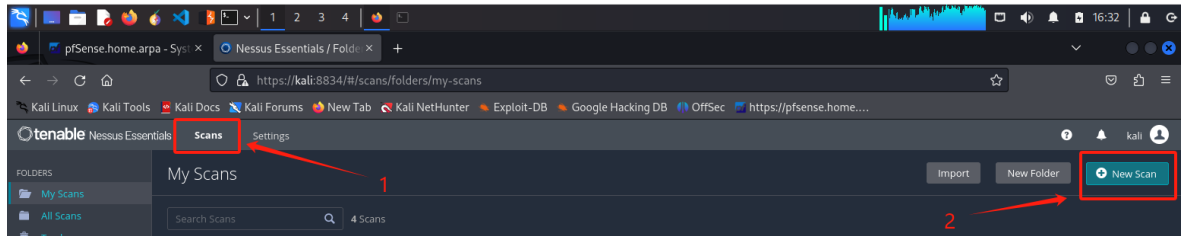
I risultati della scansione sono stati salvati nella cartella **Home** della macchina Kali in diversi formati (xml, html ecc..), mentre il report finale convertito in formato PDF è fornito nell'allegato "**Nmap Scan Report.pdf**".

## Scansione Nessus

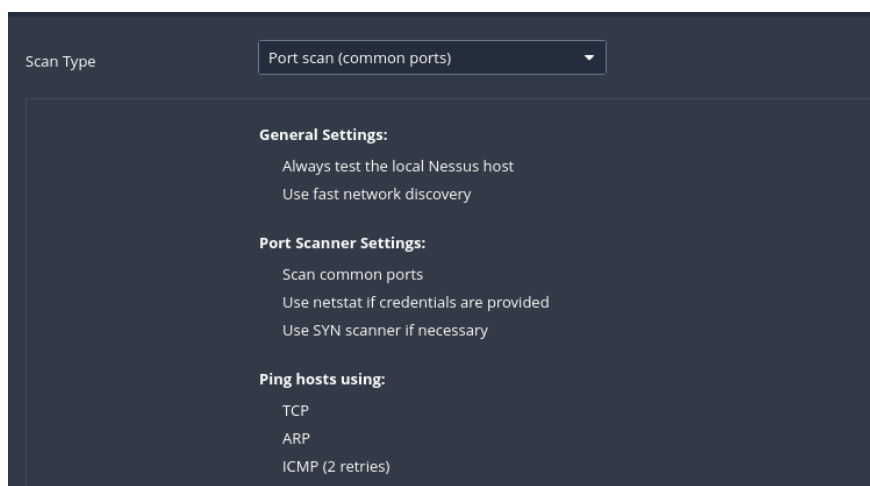
### Configurazione scan

Per avviare Nessus, seguire i passaggi indicati nel paragrafo precedente. Successivamente, eseguire i seguenti passaggi per configurare una nuova scansione:

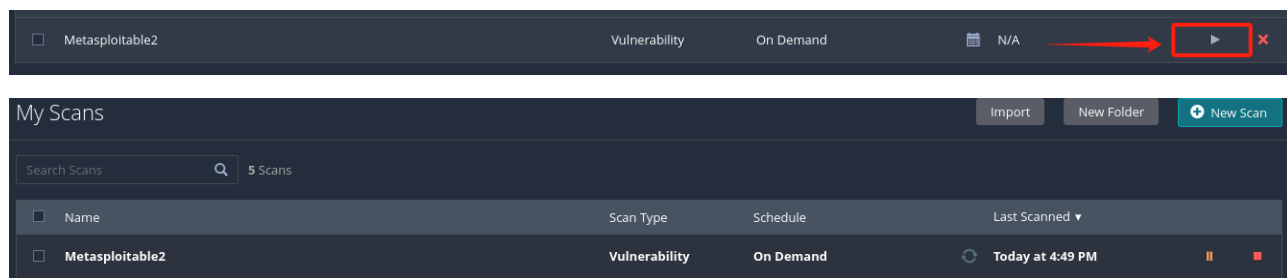
1. Avviare una nuova scansione selezionando **New Scan**.
2. Per questa attività, è stata utilizzata la tipologia di scansione **Basic Network Scan**.
3. Assegnare un nome personalizzato alla scansione.
4. Inserire l'indirizzo IP target: **192.168.50.100**.
5. Salvare la configurazione.



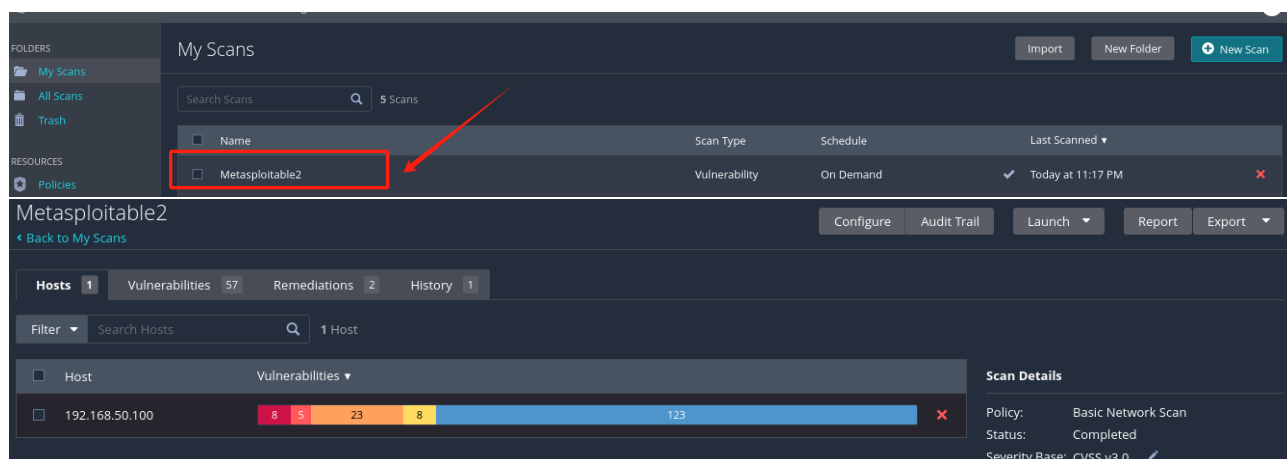
Nella sezione **Discovery** è possibile visualizzare i dettagli su cosa verrà scansionato. Per l'obiettivo dell'esercizio, questa configurazione è considerata sufficiente.



Avviare la scansione appena configurata.

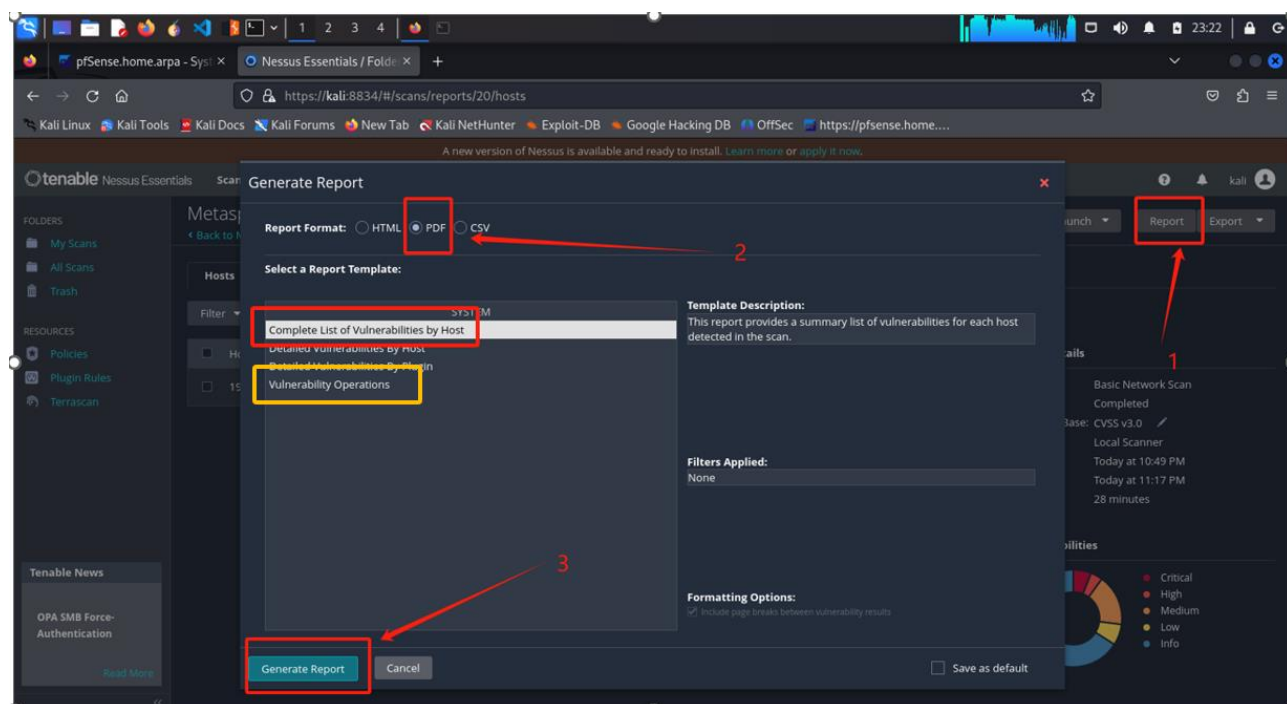


Attendere la fine della scansione, che in questo caso ha impiegato circa mezz'ora.  
Aprire e visualizzare i risultati della scansione.



Esportazione report

Selezionare **Report** e generare il file pdf come da immagine.



Il report generato in pdf è stato salvato nella cartella **Download** della macchina Kali che si fornisce nell'allegato "**Nessus Scan Report.pdf**".

Selezionare l'opzione in giallo per il report tecnico che si fornisce nell'allegato "**Nessus Vuln Report.pdf**"



## Analisi dei risultati

Durante la fase di ricerca dell'indirizzo IP target, è stata riscontrata un'ulteriore vulnerabilità: il router **pfSense** utilizzava le credenziali di default **admin**. Questa configurazione rappresenta un rischio significativo per la sicurezza, poiché le credenziali predefinite sono facilmente reperibili e devono essere prontamente modificate per prevenire accessi non autorizzati.

Sono state eseguite due scansioni per ottenere il maggior numero di informazioni possibili sulla macchina target **Metasploitable2** utilizzando **Nmap** e **Nessus**. L'analisi risultante si focalizza, ai fini dell'esercizio, sulle vulnerabilità rilevate. Ecco un riassunto delle **vulnerabilità critiche** individuate:

### 1. Apache Tomcat Ghostcat (CVE-2020-1938):

- **Nessus:** Questa vulnerabilità permette agli attaccanti di accedere a file sensibili o eseguire codice malevolo sul server tramite il connettore AJP.
- **Nmap:** La scansione ha rilevato che la porta 8009/tcp (utilizzata dal connettore AJP di Apache Tomcat) è aperta, indicando la presenza di Apache Tomcat 5.5.

### 2. Rilevamento dei protocolli SSL Version 2 e 3:

- **Nessus:** L'uso di vecchie versioni di SSL (2.0 e 3.0) rende il sistema vulnerabile ad attacchi come POODLE, che permettono di intercettare o modificare il traffico cifrato.
- **Nmap:** La scansione ha rilevato che le porte 443/tcp (HTTPS) e 993/tcp (IMAPS) supportano SSLv2 e SSLv3, utilizzando cifrari deboli come 3DES e RC4.

### 3. Apache Tomcat SEoL (fino alla versione 5.5.x):

- **Nessus:** Le vecchie versioni di Apache Tomcat consentono agli attaccanti di eseguire codice da remoto.
- **Nmap:** Ha rilevato Apache Tomcat 5.5 sulla porta 8080/tcp (HTTP), associata a questa vulnerabilità.

### 4. Debian OpenSSH/OpenSSL (CVE-2008-0166):

- **Nessus:** Un difetto nel generatore di numeri casuali di Debian rende le chiavi SSH vulnerabili, consentendo agli attaccanti di comprometterle.
- **Nmap:** La porta 22/tcp (SSH) è aperta e utilizza OpenSSH 4.7p1, che è affetta da questa vulnerabilità.

### 5. Debian OpenSSH/OpenSSL (SSL Check):

- **Nessus:** Lo stesso problema del punto precedente si applica anche ai certificati SSL generati, rendendo la crittografia insicura.
- **Nmap:** Le porte 443/tcp (HTTPS) e 993/tcp (IMAPS) utilizzano certificati SSL generati con metodi vulnerabili, esponendo i servizi a compromissioni.

### 6. Password di default per il server VNC:

- **Nessus:** Il server VNC utilizza la password predefinita "password", che permette agli attaccanti di ottenere facilmente l'accesso remoto.
- **Nmap:** La porta 5900/tcp (VNC) è aperta, con il servizio VNC configurato in modo insicuro.

### 7. Apache Tomcat SEoL (fino alla versione 5.5.x):

- **Nessus:** Una seconda vulnerabilità relativa alle versioni obsolete di Apache Tomcat, che permette l'esecuzione remota di codice.
- **Nmap:** Come rilevato in precedenza, la porta 8080/tcp è aperta e associata a questa vulnerabilità.

### 8. Debian OpenSSH/OpenSSL (CVE-2008-0166):

- **Nessus:** La stessa vulnerabilità già menzionata legata al generatore di numeri casuali debole in OpenSSH/OpenSSL.
- **Nmap:** La scansione ha confermato la presenza di OpenSSH 4.7p1 sulla porta 22/tcp, vulnerabile a questo problema.

E un riassunto delle **vulnerabilità di gravità elevata** individuate:

9. **ISC BIND Service Downgrade / Reflected DoS**

- **Nessus:** Criticità 8.6, attacco DoS che sfrutta una vulnerabilità di BIND per eseguire downgrade dei servizi.
- **Nmap:** La scansione ha rilevato BIND esposto su porta **53/tcp** e **53/udp**, con supporto per DNS.

10. **NFS Shares World Readable**

- **Nessus:** Criticità 7.5, NFS (Network File System) permette la lettura pubblica delle condivisioni.
- **Nmap:** La porta **2049/tcp** è aperta, con condivisioni NFS configurate in modo insicuro.

11. **SSL Medium Strength Cipher Suites Supported (SWEET32)**

- **Nessus:** Criticità 7.5, alcune suite di cifrari SSL di media forza sono vulnerabili a SWEET32.
- **Nmap:** La scansione ha rilevato cifrari SSL come **3DES** utilizzati sulle porte **443/tcp** e **993/tcp**.

12. **Samba Badlock Vulnerability**

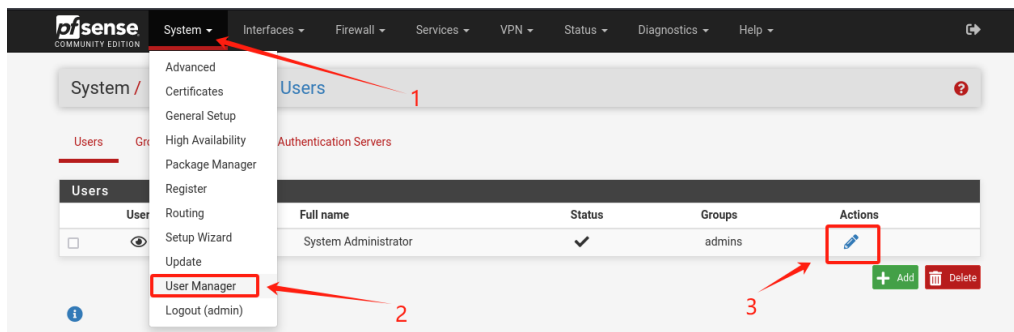
- **Nessus:** Criticità 7.5, vulnerabilità in Samba che permette attacchi man-in-the-middle e denial of service.
- **Nmap:** Ha rilevato la versione vulnerabile di **Samba 3.0.20** esposta su porte **139/tcp** e **445/tcp**.

## Azioni di Rimedio

Le vulnerabilità saranno analizzate secondo due criteri: inizialmente in base alle indicazioni fornite dalla traccia dell'esercizio e successivamente ordinate per livello di criticità.

### Credenziali pfSense

Per modificare le credenziali di pfSense recarsi nella pagina di configurazione come in figura.



Inserire la nuova password e ripeterla, poi salvare.

The screenshot shows the 'User Properties' form in the pfSense web interface. The form is titled 'User Properties' and contains several fields. The 'Username' field is set to 'admin'. The 'Password' field is highlighted with a red box, and the 'Confirm Password' field is also highlighted with a red box. The 'Full name' field is set to 'System Administrator'. The 'Defined by' field is set to 'SYSTEM'. The 'Disabled' checkbox is checked, with the text 'This user cannot login' next to it.

## VNC Server 'password' Password (Traccia - Livello Critico)

Il server VNC utilizza la password predefinita "password", che permette agli attaccanti di ottenere facilmente l'accesso remoto. (Relativo al punto 6 della lista analizzata)

Vulnerabilities 57

CRITICAL VNC Server 'password' Password

< >

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Output

Nessus logged in using a password of "password".  
To see debug logs, please visit individual host

Port	Hosts
5900 / tcp / vnc	192.168.50.100

Plugin Details

Severity: Critical  
ID: 61708  
Version: \$Revision: 1.2 \$  
Type: remote  
Family: Gain a shell remotely  
Published: August 29, 2012  
Modified: September 24, 2015

Risk Information

Risk Factor: Critical  
CVSS v2.0 Base Score: 10.0  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

Default Account: true  
Exploited by Nessus: true

Per modificare la password del server VNC su **Metasploitable2**, aprire un terminale ed eseguire il seguente comando: **vncpasswd**

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Password too short
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
msfadmin@metasploitable:~$
```

Inserire la nuova password desiderata, ad esempio **Epiccode24**, e confermare. La password verrà applicata anche alla modalità "solo lettura".

Accedere nella cartella .vnc al file passwd e modificare la password.

```
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ vncpasswd
-bash: vncpasswd: command not found
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
VNC directory /home/msfadmin/.vnc does not exist, creating.
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
msfadmin@metasploitable:~$ ls -a
.      .distcc  giggio.txt.save  .rhosts
..     .gconf   .mysql_history   .ssh
.bash_history  .gconfd  .profile         .sudo_as_admin_successful
msfadmin@metasploitable:~$ cd .vnc
msfadmin@metasploitable:~/.vnc$ ls
passwd
msfadmin@metasploitable:~/.vnc$ sudo passwd
[sudol password for msfadmin:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
msfadmin@metasploitable:~/.vnc$
```

## NFS Shares World Readable (Traccia - Livello Alto)

La vulnerabilità **NFS Shares World Readable** indica che il server NFS (Network File System) sta esportando una o più condivisioni senza restrizioni di accesso. Ciò significa che chiunque sulla rete può accedere alle condivisioni, il che rappresenta un rischio significativo per la sicurezza, poiché potrebbe consentire a un attaccante di visualizzare o modificare dati sensibili (punto 10 della lista analizzata).

The screenshot shows a vulnerability scanner interface with a dark theme. At the top, it says 'Vulnerabilities 57'. Below that, a red box highlights 'HIGH' and 'NFS Shares World Readable'. The 'Description' section states: 'The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range)'. The 'Solution' section says: 'Place the appropriate restrictions on all NFS shares'. The 'See Also' section provides a link: 'http://www.tdtp.org/HOWTO/NFS-HOWTO/security.html'. The 'Output' section shows: 'The following shares have no access restrictions : / \*'. Below this, there is a table with columns 'Port' and 'Hosts'. The first row shows '2049 /tcp/rpcnfs' and '192.168.50.100'. To the right, the 'Plugin Details' section lists: Severity: High, ID: 42256, Version: 1.12, Type: remote, Family: RPC, Published: October 26, 2009, Modified: February 21, 2024. The 'Risk Information' section shows: Risk Factor: Medium, CVSS v3.0 Base Score: 7.5, and CVSS vectors. The 'Vulnerability Information' section at the bottom shows: Vulnerability Pub Date: January 1, 1985.

1. Accedere a Metasploitable2
2. Modificare la configurazione di esportazione con il comando: **sudo nano /etc/exports**
3. Modificare le righe nel file per limitare l'accesso alle condivisioni NFS consentendo solo a Kali l'accesso: sostituire la riga indicata in figura con **/nfs\_share 192.168.1.101(rw,sync,no\_subtree\_check)**

The screenshot shows a terminal window with the command 'GNU nano 2.0.7 File: /etc/exports'. The file content is displayed, showing the access control list for filesystems. A red box highlights the line: **/\*(rw,sync,no\_root\_squash,no\_subtree\_check)**. Below the terminal window, a new line is shown: **/nfs\_share 192.168.1.101(rw,sync,no\_root\_squash,no\_subtree\_check)**.

4. CTRL + O & CTRL + X per salvare e uscire
5. Riavviare il servizio o riavviare Metasploitable2



## Bind Shell Backdoor Detection (Traccia - Livello Critico)

Una **bind shell** o una **backdoor shell** consente a un attaccante di eseguire comandi sul sistema da remoto senza autenticazione. In questo scenario, la shell è in ascolto su una porta specifica e, se un attaccante si collega a quella porta, può ottenere accesso completo al sistema senza dover autenticarsi.

Vulnerabilities 21

CRITICAL

Bind Shell Backdoor Detection

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Output

Nessus was able to execute the command "id" using the following request :

This produced the following truncated output (limited to 10 lines) :

----- snip -----

root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)

root@metasploitable:/#

----- snip -----

To see debug logs, please visit individual host

Port ▲

Hosts

Plugin Details

Severity: Critical

ID: 51988

Version: 1.10

Type: remote

Family: Backdoors

Published: February 15, 2011

Modified: April 11, 2022

Risk Information

Risk Factor: Critical


CVSS v3.0 Base Score: 9.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/CH:H/H/A/H

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

To see debug logs, please visit individual host

Port ▲	Hosts
1524 / tcp / wild_shell	192.168.50.103 

Il backdoor si trova sulla porta 1524 in tcp. Attraverso il comando **sudo netstat -tulnp**

```
tcp        0      0 0.0.0.0:111          0.0.0.0:*           LISTEN
3684/portmap
tcp        0      0 0.0.0.0:6000        0.0.0.0:*           LISTEN
4617/Xtightvnc
tcp        0      0 0.0.0.0:80          0.0.0.0:*           LISTEN
4576/apache2
tcp        0      0 0.0.0.0:60560       0.0.0.0:*           LISTEN
tcp        0      0 0.0.0.0:8787        0.0.0.0:*           LISTEN
4599/ruby
tcp        0      0 0.0.0.0:8180        0.0.0.0:*           LISTEN
1558/java
tcp        0      0 0.0.0.0:1524        0.0.0.0:*           LISTEN
4462/xinetd
tcp        0      0 192.168.50.103:33  0.0.0.0:*           LISTEN
4057/named
tcp        0      0 0.0.0.0:21          0.0.0.0:*           LISTEN
4462/xinetd
tcp        0      0 127.0.0.1:53        0.0.0.0:*           LISTEN
4057/named
tcp        0      0 0.0.0.0:57399       0.0.0.0:*           LISTEN
4595/rmiregistry
tcp        0      0 0.0.0.0:23          0.0.0.0:*           LISTEN
4462/xinetd
tcp        0      0 0.0.0.0:5432        0.0.0.0:*           LISTEN
```

Spostarsi con **SHIFT+PAGE**. **SU / PAGE**. **GIU** per scorrere la lista e utilizzare il comando **sudo kill -9 4062** (PID associato alla porta oggetto del backdoor). Si è optato l'utilizzo della funzione **SIGKILL** (9) per forzare la chiusura, per avere la certezza che sia chiuso il processo.

Pag. 24

M3 W12 D5

Analisi delle Vulnerabilità & Azioni di Rimedio

Yilei Wu

## Apache Tomcat SEoL (<= 5.5.x) (Livello Critico)

La vulnerabilità **Apache Tomcat SEoL** (Server-Side Execution of Logic) nelle versioni di Apache Tomcat fino alla **5.5.x** consente agli attaccanti di eseguire codice da remoto sul server. Questa vulnerabilità è spesso sfruttata per ottenere accesso non autorizzato, eseguire comandi arbitrari o compromettere il sistema in vari modi. (numero 1 della lista analizzata)

L'utilizzo di una versione vulnerabile di Apache Tomcat espone il server a vari tipi di attacchi, inclusi:

- **Esecuzione remota di codice:** Gli attaccanti possono sfruttare la vulnerabilità per eseguire comandi sul server.
- **Accesso non autorizzato:** Accesso ai dati sensibili o esecuzione di operazioni non autorizzate.

The screenshot shows the Metasploit2 interface for the Apache Tomcat SEoL vulnerability (Plugin #171340). The interface is divided into several sections:

- Vulnerabilities:** A tab showing 57 vulnerabilities, with the current one highlighted as 'CRITICAL'.
- Description:** A text block explaining that Apache Tomcat versions less than or equal to 5.5.x are no longer maintained and may contain security vulnerabilities.
- Solution:** A text block suggesting upgrading to a version of Apache Tomcat that is currently supported.
- See Also:** A link to the Apache Tomcat SEoL page: <https://tomcat.apache.org/tomcat-55-eol.html>.
- Output:** A table showing the results of a scan on a host. The table has columns for 'Port' and 'Hosts'. The output shows a single entry for port 8080 on host 192.168.50.100, indicating the vulnerability is present.
- Plugin Details:** A sidebar on the right providing additional information about the vulnerability, including its severity (Critical), ID (171340), version (1.5), type (combined), family (Web Servers), published date (February 10, 2023), and modified date (May 6, 2024).
- Risk Information:** A section showing the risk factor (Critical) and CVSS scores (CVSS v3.0 Base Score: 10.0, CVSS v2.0 Base Score: 10.0).
- Vulnerability Information:** A section showing the vulnerability name (Apache Tomcat SEoL) and its version (5.5.x).

Per la risoluzione basterebbe semplicemente aggiornare con i comandi:

```
sudo apt-get update
sudo apt-get upgrade
```

Tuttavia, come ben documentato, **Metasploit2** non è un sistema operativo progettato per essere aggiornato, poiché il suo scopo principale è quello di fornire un ambiente vulnerabile per la formazione e la simulazione di attacchi. Pertanto, la soluzione migliore per risolvere la vulnerabilità **Apache Tomcat SEoL (<= 5.5.x)** è, in questo contesto, creare una regola di firewall che blocchi la porta 8080 tramite pfSense.

pfSense > Firewall > Rules e impostare come da immagine sottostante facendo attenzione all'ip assegnato a metasploit2.

<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	*	192.168.50.100	8080	*	none	Apache Tomcat SEoL (fino alla versione 5.5.x)	
--------------------------	-------------------------------------	-------	----------	---	---	----------------	------	---	------	---	--

Per ragioni di test si bloccano tutte le connessioni, ma per ragioni di sicurezza si potrebbe abilitare i permessi agli host autorizzati.

## SSL Version 2 and 3 Protocol Detection (Livello Critico)

La vulnerabilità **SSL Version 2 and 3 Protocol Detection** indica che il server è configurato per utilizzare le versioni obsolete di SSL (Secure Sockets Layer), ovvero SSLv2 e SSLv3. Questi protocolli presentano diverse vulnerabilità note, rendendo la comunicazione insicura e suscettibile a vari tipi di attacchi, tra cui il **POODLE attack** e attacchi **man-in-the-middle**. Utilizzare queste versioni vulnerabili di SSL espone le informazioni trasmesse a rischi significativi. (punto 2 della lista analizzata)

The screenshot shows a Nessus vulnerability report for 'SSL Version 2 and 3 Protocol Detection'. The severity is 'Critical'. The description states that the remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0, which are affected by several cryptographic flaws, including insecure padding schemes and insecure session renegotiation. It also mentions that although SSL/TLS has a secure means for choosing the highest supported version, many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). The solution is to consult the application's documentation to disable SSL 2.0 and 3.0, and use TLS 1.2 (with approved cipher suites) or higher instead. The report also includes a table of hosts and a section for debug logs.

Port	Hosts
5432 / tcp / postgresql	192.168.50.103

Nessus suggerisce di disattivare il servizio: cercare il file di configurazione di apache2: **sudo find / -name "apache2.conf"** e aggiungere **sudo nano** al collegamento dato dalla ricerca.

```
msfadmin@metasploitable:~$ ls /opt
msfadmin@metasploitable:~$ ls /opt/
msfadmin@metasploitable:~$ sudo find / -name "apache2.conf"
/etc/apache2/apache2.conf
msfadmin@metasploitable:~$ sudo nano /etc/apache2/apache2.conf
```

```
GNU nano 2.0.7 File: /etc/apache2/apache2.conf Modified
# Include of directories ignores editors' and dpkg's backup files,
# see README.Debian for details.

# Include generic snippets of statements
Include /etc/apache2/conf.d/

# Include the virtual host configurations:
Include /etc/apache2/sites-enabled/

SSLProtocol All -SSLv2 -SSLv3

[ Wrote 300 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

Aggiungere la riga **SSLProtocol All -SSLv2 -SSLv3** al file **apache2.conf** salvare e uscire CTRL+O, CTRL+X. Inoltre usare il comando **sudo netstat -tuln** per terminalre il processo che apre la porta 5432 e 25 come visto nel caso della backdoor.

## ISC BIND Service Downgrade / Reflected DoS (Livello Alto)

La vulnerabilità **ISC BIND Service Downgrade / Reflected DoS** si riferisce a un attacco che sfrutta vulnerabilità nel servizio DNS fornito da **BIND** (Berkeley Internet Name Domain). Questo tipo di attacco può permettere a un aggressore di inviare richieste di downgrade a un server DNS vulnerabile, costringendolo a utilizzare versioni precedenti meno sicure, o può riflettere attacchi DoS (Denial of Service) attraverso risposte DNS amplificate. (Punto 9 della lista analizzata).

- **Denial of Service:** Un attacco di questo tipo può sovraccaricare il server DNS, rendendolo inaccessibile.
- **Compromissione della Sicurezza:** L'uso di versioni obsolete di DNS può esporre il server a exploit noti.














Per mitigare la vulnerabilità di BIND, si può intervenire su pfSense bloccando il traffico alle porte DNS vulnerabili:

1. Andare su **Firewall > Rules**, seleziona l'interfaccia **LAN2** > Aggiungere nuova regola
2. Configurare in modo da bloccare la porta 53 in TCP e UDP

The top screenshot shows the 'Destination' tab of the pfSense Firewall Rule configuration. The 'Destination' dropdown is set to 'Any'. The 'Destination Port Range' is set to 'DNS (53)' with 'From' and 'To' fields both set to 'Custom'. The 'Description' field contains 'ISC BIND Service Downgrade / Reflected DoS (Livello Alto)'. The 'Log' checkbox is checked. The 'Advanced Options' button is visible.

The bottom screenshot shows the same configuration, but the 'Destination Port Range' dropdown menu is open, showing the 'DNS (53)' option selected.

3. Salvare la configurazione

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	 	0/0 B	IPv4	*	*	*	53 (DNS)	*	none	ISC BIND Service Downgrade / Reflected DoS (Livello Alto)	   
<div> Add  Add  Delete  Toggle  Copy  Save  Separator</div>											

## Considerazioni sulla Sicurezza di Metasploitable2

**Metasploitable2** è un ambiente progettato specificamente per simulare vulnerabilità e testare le tecniche di attacco e difesa. Poiché non è concepito come un sistema sicuro e non può essere aggiornato o corretto come una distribuzione standard di Linux, risolvere le vulnerabilità presenti in esso non è sempre pratico o semplice.

### Firewall pfSense

Di conseguenza, è più sensato intervenire a livello del firewall sul router **pfSense**. Configurando regole specifiche nel firewall, è possibile limitare l'accesso e ridurre la superficie di attacco di **Metasploitable2**, rendendola meno vulnerabile alle minacce esterne.


















































Questa strategia consente di mantenere l'ambiente di test intatto, mentre si garantisce una maggiore sicurezza e protezione contro potenziali exploit.

N°	Vulnerabilità	Porta da Bloccare
1	Apache Tomcat Ghostcat (CVE-2020-1938)	8009/tcp (AJP)
2	Rilevamento dei protocolli SSL Version 2 e 3	443/tcp (HTTPS)
		993/tcp (IMAPS)
3	Apache Tomcat SEoL (fino alla versione 5.5.x)	8080/tcp (HTTP)
4	Debian OpenSSH/OpenSSL (CVE-2008-0166)	22/tcp (SSH)
5	Debian OpenSSH/OpenSSL (SSL Check)	443/tcp (HTTPS)
		993/tcp (IMAPS)
6	Password di default per il server VNC	5900/tcp (VNC)
7	Apache Tomcat SEoL (fino alla versione 5.5.x)	8080/tcp (HTTP)
8	Debian OpenSSH/OpenSSL (CVE-2008-0166)	22/tcp (SSH)
9	ISC BIND Service Downgrade / Reflected DoS	53/tcp (DNS)
		53/udp (DNS)
10	NFS Shares World Readable	2049/tcp (NFS)
11	SSL Medium Strength Cipher Suites Supported (SWEET32)	443/tcp (HTTPS)
		993/tcp (IMAPS)
12	Samba Badlock Vulnerability	139/tcp (NetBIOS)
		445/tcp (SMB)

Tuttavia bloccare tutte queste porte potrebbe rendere il sistema inutilizzabile, soprattutto se alcune di queste porte sono necessarie per il corretto funzionamento delle applicazioni o dei servizi.



La chiave è trovare un equilibrio tra sicurezza e funzionalità. Concentrandosi su misure di sicurezza mirate, è possibile proteggere **Metasploitable2** senza compromettere l'operatività del sistema.

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	 0/0 B	IPv4 TCP	*	*	192.168.50.103	2049	*	none		NFS Shares World Readable	    
<input type="checkbox"/>	 0/0 B	IPv4 TCP	*	*	192.168.50.103	5900 (VNC)	*	none		Password di default per il server VNC	    
<input type="checkbox"/>	 0/0 B	IPv4 TCP	*	*	192.168.50.103	8080	*	none		Apache Tomcat SEoL (fino alla versione 5.5.x)	    
<input type="checkbox"/>	 0/0 B	IPv4 TCP	*	*	192.168.50.103	8009	*	none		Apache Tomcat Ghostcat (CVE-2020-1938)	    
<input type="checkbox"/>	  0/0 B	IPv4 TCP/UDP	*	*	192.168.50.103	53 (DNS)	*	none		ISC BIND Service Downgrade / Reflected DoS (Livello Alto)	    
<input type="checkbox"/>	 0/0 B	IPv4 TCP	*	*	192.168.50.103	1099	*	none		java-rmi GNU Classpath grmiregistry	    
<input type="checkbox"/>	 0/0 B	IPv4 TCP	*	*	192.168.50.103	3306	*	none		mysql MySQL 5.0.51a-3ubuntu5	    
<input type="checkbox"/>	 0/0 B	IPv4 TCP	*	*	192.168.50.103	43856	*	none		java-rmi GNU Classpath grmiregistry	    

### Gestione dei servizi non necessari

Un'altra soluzione praticabile per migliorare la sicurezza del sistema consiste nello spegnere tutti i servizi non necessari, attivandoli solo quando effettivamente richiesti. Seguendo la stessa logica utilizzata per la risoluzione della backdoor, è possibile terminare i processi inutilizzati e riattivarli solo quando necessari, riducendo così la superficie d'attacco. Questo approccio minimizza l'esposizione ai rischi di sicurezza, mantenendo attivi solo i servizi strettamente necessari al momento opportuno.

Pertanto sono state rilevate i servizi attraverso il comando **sudo netstat -tulnp** visualizzando i processi e servizi attivi con le relative porte vulnerabili e attraverso l'utilizzo della funzione **SIGKILL (9)** si è provveduto a terminare forzatamente i servizi e processi non necessari.

### Conclusione

Tenendo conto delle considerazioni riguardanti la configurazione del firewall **pfSense** e la gestione dei servizi non necessari, **Metasploitable2** non è stato reso meno vulnerabile, poiché, come spiegato in precedenza, non è un sistema aggiornabile, anzi con gli aggiornamenti si risolverebbero la quasi totalità delle vulnerabilità. Tuttavia, è stata ridotta sensibilmente la superficie d'attacco.

Queste misure, che includono la disattivazione di servizi superflui e l'applicazione di regole firewall mirate, rappresentano un'azione di rimedio efficace e immediata. Sebbene il sistema rimanga vulnerabile per sua natura, l'intervento ha limitato le opportunità di attacco, un obiettivo considerato raggiunto ai fini di questo esercizio.

In altre parole, partendo da un sistema vulnerabile come **Metasploitable2** e non da una macchina aggiornabile, si è proceduto a mettere delle "toppe" per evitare di far affondare la barca (la macchina stessa). In questo caso, la soluzione definitiva sarebbe cambiare l'intero sistema.

## Scansione dopo le azioni di rimedio

Per un'analisi più approfondita dei risultati della scansione a seguito delle azioni di rimedio, si rimanda agli allegati **“Nessus Last Scan Report.pdf”** e **“Nessus Last Vuln Report.pdf”**. Questi documenti forniscono una panoramica dettagliata delle vulnerabilità identificate e delle misure correttive adottate.

Come evidenziato nelle sezioni precedenti, seguendo le azioni suggerite, è stata eliminata la quasi totalità delle vulnerabilità di gravità elevata. Questi interventi, che hanno incluso la disabilitazione dei protocolli insicuri, la chiusura dei servizi non necessari e la configurazione mirata del firewall, hanno notevolmente ridotto i rischi per la sicurezza del sistema, migliorando così la sua resilienza complessiva.

The screenshot displays the Metasploitable2 web interface. At the top, there are tabs for 'Hosts', 'Vulnerabilities', and 'History'. The 'Hosts' tab is active, showing a list of hosts with a search bar and a filter dropdown. A single host, 192.168.50.103, is listed with a severity level of 1 and a count of 34. To the right, the 'Scan Details' section provides information about the scan: Policy (Basic Network Scan), Status (Completed), Severity Base (CVSS v3.0), Scanner (Local Scanner), Start (Today at 10:11 PM), End (Today at 10:15 PM), and Elapsed (4 minutes). Below this, a 'Vulnerabilities' section features a donut chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (blue), and Info (light blue). The bottom part of the image shows a browser window displaying the Nessus Essentials interface. The browser address bar shows the URL 'https://kali.8834/#/scans/reports/20/hosts/2/vulnerabilities'. The Nessus Essentials interface shows a list of vulnerabilities for the host 192.168.50.103. The table lists vulnerabilities with columns for Severity, CVSS, VPR, EPSS, Family, and Count. The vulnerabilities are categorized by severity: LOW (yellow), INFO (blue), and CRITICAL (red). The table shows 17 vulnerabilities in total. The 'Host Details' section on the right provides information about the host: 192.168.50.103, Linux Kernel 2.6, Start (Today at 10:11 PM), End (Today at 10:15 PM), Elapsed (4 minutes), and a 'Download' link. Below this, a 'Vulnerabilities' section features a donut chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (blue), and Info (light blue).

## Considerazioni finali

Attraverso questo esercizio si è potuto sperimentare nella pratica come eseguire una scansione dettagliata di una rete e/o di una macchina, individuando tutte le vulnerabilità conosciute. Non solo si è proceduto a fornire consigli e suggerimenti attraverso questo report, ma si è anche intervenuti per porre rimedio alle vulnerabilità riscontrate.

Il miglior consiglio resta quello di mantenere i sistemi aggiornati; laddove questo non sia possibile, la soluzione ideale è sostituire il sistema piuttosto che applicare soluzioni temporanee. Quest'ultima tuttavia, sarà oggetto di valutazione dell'amministratore di sistema sul rapporto costi/benefici.

È inoltre essenziale eseguire backup quotidiani dei sistemi. Anche se questo esercizio si svolge in un laboratorio virtuale, nel mondo reale la compromissione di un sistema può avere un impatto non solo economico, ma anche sulla reputazione dell'azienda, comportando una perdita di fiducia da parte dei clienti.

## Documentazione allegata

Lista degli allegati al presente report:

- Nmap Scan Report.pdf
- Nessus Scan Report.pdf
- Nessus Vuln Report.pdf
- Nessus Last Scan Report.pdf
- Nessus Last Vuln Report.pdf