



REMEDIATION  
EXERCICE



# W12-DH

NICHOLAS DI ANGELO

SCANSIONE NESSUS - METASPLOITABLE2 REMEDIATION VULNERABILITY



nessus®  
professional

M3 EXAMS

 EPICODE

# INDEX :

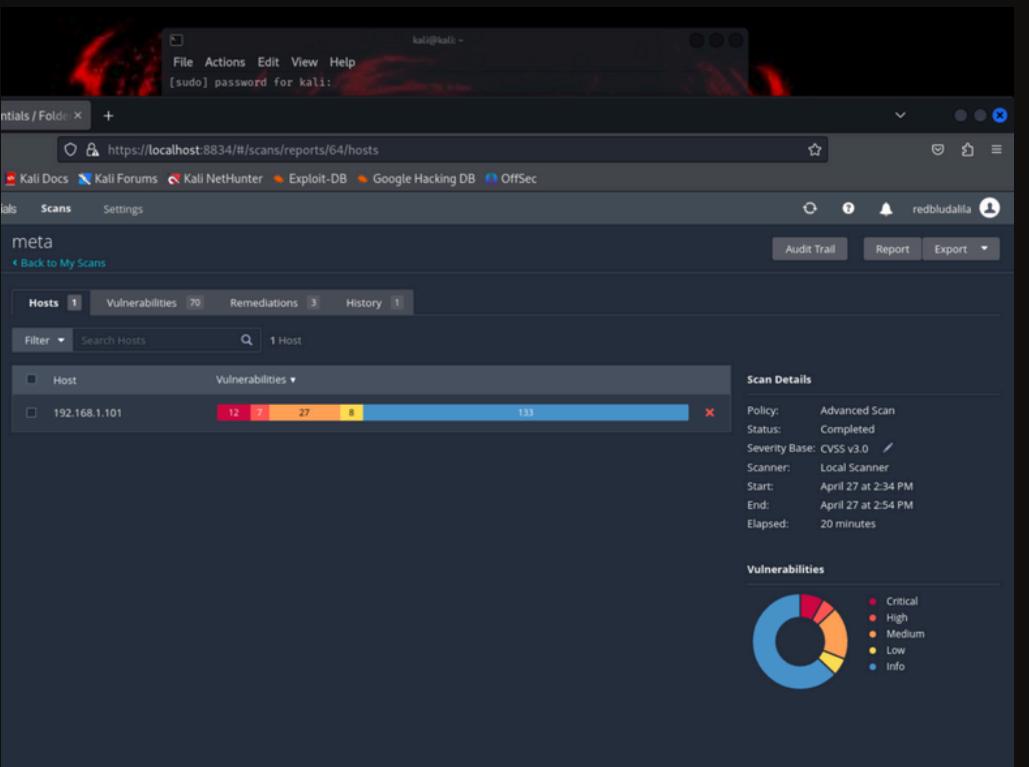
**COSA FAREMO :** SCANSIONE CON TOOL NESSUS USO DI NETCAT, NMAP PER AZIONI CORRETTIVE SULLE VULNERABILITA' RISCONTRATE

L'indice del progetto di mitigazione delle vulnerabilità fornisce un quadro sintetico delle strategie e delle azioni adottate per affrontare le vulnerabilità rilevate su MetaSploitable 2. Esso offre una panoramica delle misure di sicurezza implementate, inclusi aggiornamenti del software, configurazioni di rete, e politiche di accesso, al fine di ridurre il rischio di exploit e garantire la protezione del sistema

<b>INTRODUZIONE</b> TOOL NESSUS	2
<b>INDIVIDUAZIONE VULNERABILITA'</b>	3
<b>REMEDIATION 1</b> - BACK DOOR	4
<b>REMEDIATION 2</b> - VNC SERVER	6
<b>REMEDIATION 3</b> -NFS EXPORTED	8
<b>REMEDIATION 4</b> - TOMCAT5.5 APACHE	10
<b>REMEDIATION 5</b> - PFSENSE FIREWALL	12
<b>CONCLUSIONI</b>	13-14

# SCANSIONE

SCREEN 1 - ATTRAVERSO IL TOOL NESSUS  
ESEGUIREMO LA PRIMA SCANSIONE PER  
RINTRACCIARE LE VULNERABILITA' DELLA  
MACCHINA TARGHET

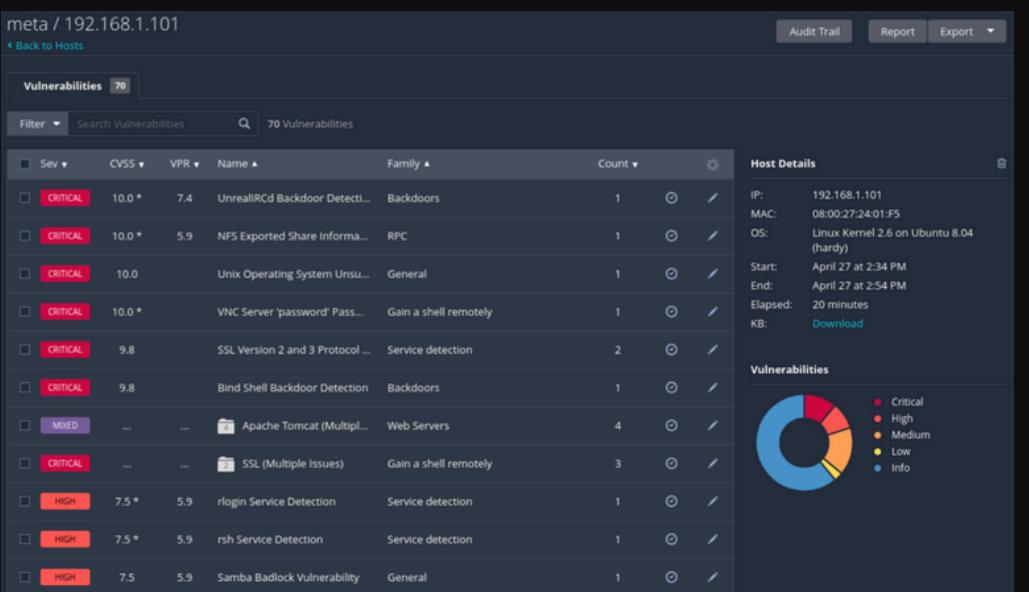


INIZIAMO CON L'ESEGUIRE LA SCANSIONE VERSO IL TARGHET

SCREEN 1

## ANALISI SCANSIONE

SCREEN 2 - ANALISI SCANSIONE E  
INDIVUAZIONE CRITICITA' DELLE  
VULNERABILITA'



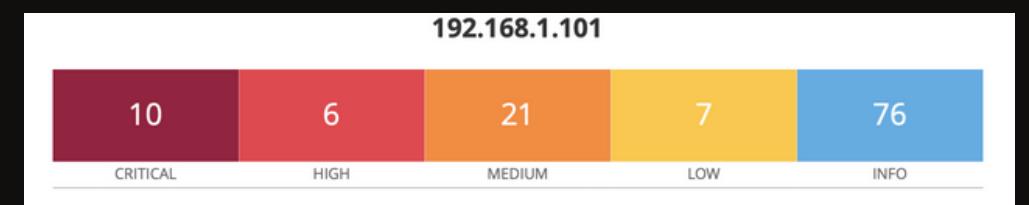
# VULNERABILITY SCAN

SCANSIONE DA KALI LINUX (IP 192.168.1.100) CON NESSUS VERSO LA MACCHINA  
TARGHET METASPLOITABLE2 (IP 192.168.1.101)

SCREEN 2

## ANALISI SCANSIONE

SCREEN 3 - REPORT GENERALE NUMERO  
DELLE VULNERABILITA' PER CRITICITA'



SCREEN 3

# SCAN VULNERABILITY

## INTRODUZIONE

### BIND SHELL BACKDOOR

La vulnerabilità 51988 riguarda la rilevazione di una backdoor tramite BIND Shell su un sistema. Le backdoor sono strumenti malevoli che consentono a un attaccante di accedere in modo non autorizzato a un sistema compromesso. In questo caso specifico, la backdoor utilizza il servizio BIND per stabilire una shell remota che potrebbe essere sfruttata per eseguire comandi arbitrari.

CRITICO

### RISK FACTOR

DAL REPORT EVINCIAMO LA GRAVITA'  
CRITICA A RISCHIO ELEVATO

**Synopsis**  
The remote host may have been compromised.

**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.

**Risk Factor**  
Critical

**CVSS v3.0 Base Score**  
9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

**CVSS v2.0 Base Score**  
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

**Plugin Information**  
Published: 2011/02/15, Modified: 2022/04/11

**Plugin Output**  
tcp/1524/wild\_shell

```
Nessus was able to execute the command "id" using the following request :  
..... snip .....  
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)  
root@metasploitable:/#  
..... snip .....
```

192.168.1.101

CRITICAL 9.8 - 51988 Bind Shell Backdoor Detection

## CHE COS'E' ....??

### SCANSIONE INIZIALE

Durante la scansione iniziale del sistema target, è stata individuata la presenza della backdoor BIND Shell, identificata come vulnerabilità 51988. Questo tipo di backdoor rappresenta una seria minaccia per la sicurezza del sistema, poiché consente agli attaccanti di ottenere accesso non autorizzato al sistema e di eseguire comandi con privilegi elevati.

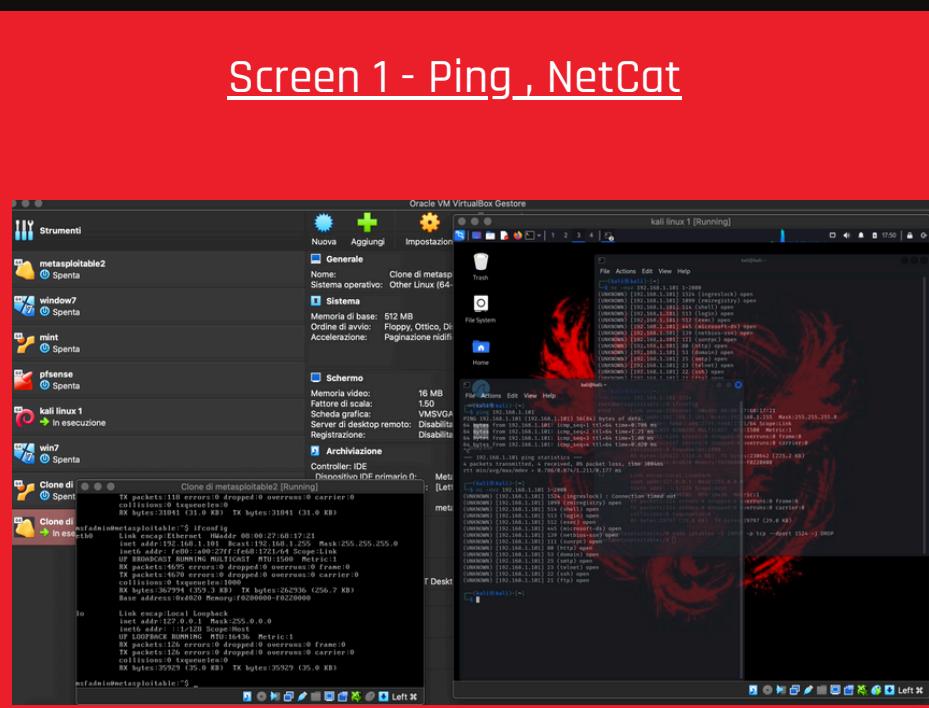
### CRITICAL CVSS

### LA CVSS

Il CVSS Base Score fornisce una valutazione standardizzata della gravità delle vulnerabilità, facilitando la comunicazione e la comprensione del rischio tra gli stakeholder.

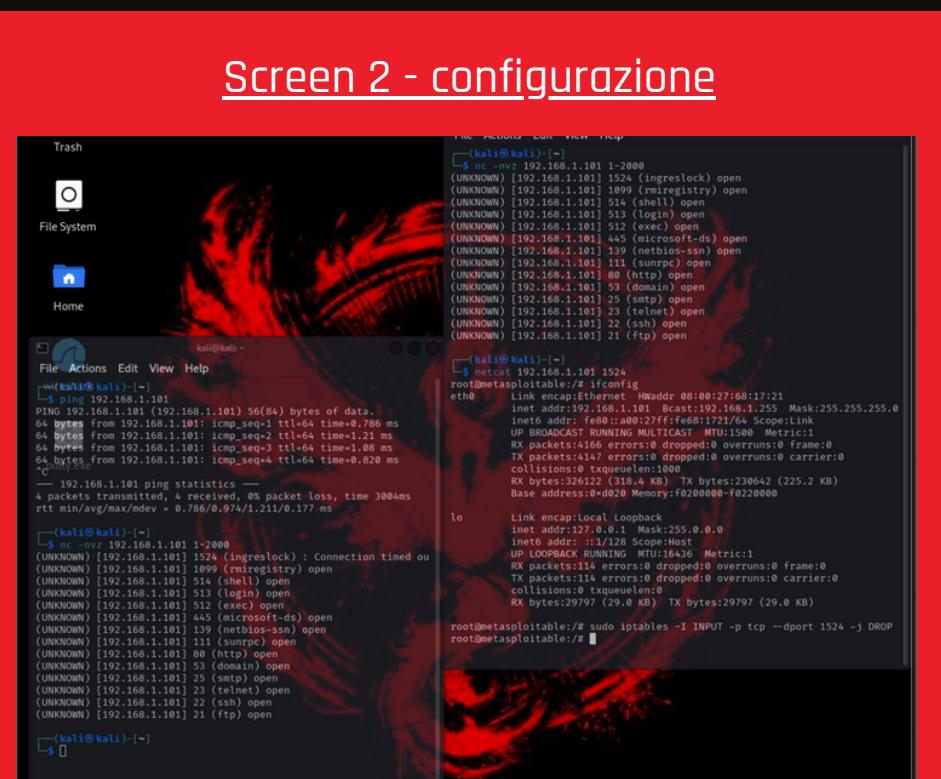
Tuttavia, è importante considerare anche altri fattori, come il contesto operativo e le contromisure disponibili, per prendere decisioni informate sulla gestione dei rischi informatici.

## Screen 1 - Ping , NetCat



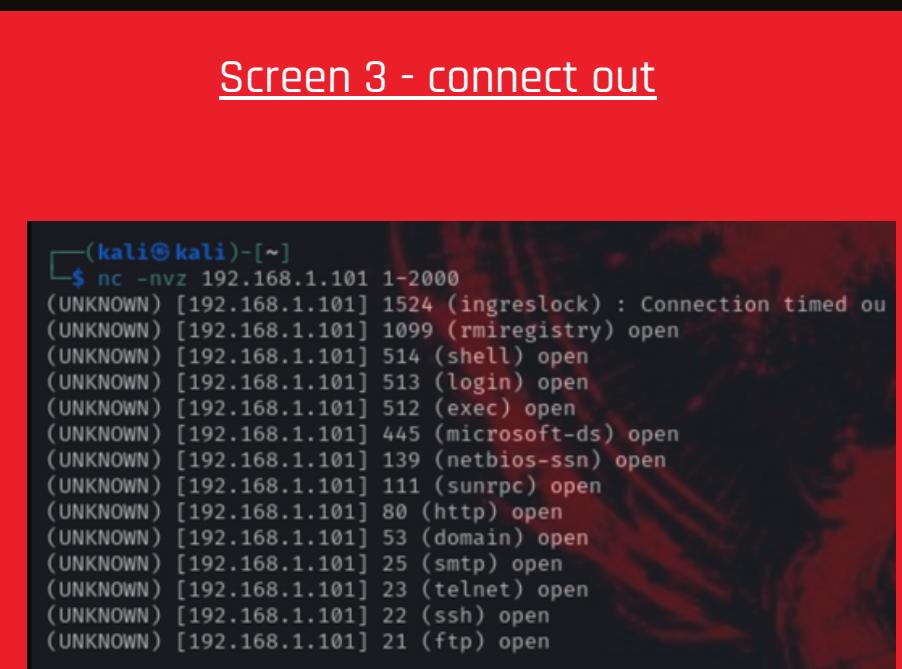
**NAVIO NET CAT E PING : nc -nvz IP 1-2000** è utilizzato per eseguire una scansione delle porte da 1 a 2000 sull'indirizzo IP specificato senza avviare una connessione effettiva . In sintesi, durante un'azione di rimedio, l'utilizzo del comando nc -nvz IP 1-2000 consente di identificare le porte aperte e di concentrarsi sull'analisi delle vulnerabilità su un range specifico di porte in modo non intrusivo e efficiente

## Screen 2 - configurazione



**IDENTIFICAZIONE DELLE PORTE APERTE** : Utilizzando l'opzione -v (verbose) e -z (scansione di prova), il comando visualizzerà le porte che sono aperte e pronte per la connessione. Questo è utile per identificare le porte che potrebbero essere vulnerabili e richiedere una mitigazione.

## Screen 3 - connect out



**VERIFICA DELL'AZIONE DI RIMEDIO:** Dopo l'implementazione delle azioni di rimedio, è stata eseguita una nuova scansione sul sistema target per valutare l'efficacia delle misure adottate. La scansione post-rimedio ha confermato l'assenza della backdoor BIND Shell e ha dimostrato che il servizio BIND è stato correttamente disabilitato.

**Disabilitazione del Servizio BIND:** Per prevenire l'accesso non autorizzato tramite la backdoor, il servizio BIND è stato disabilitato sul sistema. Questo impedisce agli attaccanti di stabilire una connessione tramite la backdoor e riduce il rischio di compromissione del sistema.

# WA - REMEDIATION BIND SHELL BACK DOOR

## **AZIONI E VERIFICA EFFICACIA DEI RIMEDI**

Per la vulnerabilità  
51988, sono state  
intraprese le seguenti  
azioni di rimedio -

Verifica Finale:  
connection time out  
sulla porta 1524  
confermata

# SCAN VULNERABILITY

## INTRODUZIONE VNC SERVER

La vulnerabilità riguarda il VNC (Virtual Network Computing) Server con password di default o deboli. VNC è un software che consente il controllo remoto di un computer attraverso una connessione di rete. La vulnerabilità "PASSWORD" si verifica quando il VNC Server è configurato con una password di accesso predefinita o debole, aumentando il rischio di accesso non autorizzato da parte di attaccanti.

CRITICO

## RISK FACTOR

- Accesso Non Autorizzato: Un attaccante potrebbe ottenere accesso non autorizzato al sistema target utilizzando la password predefinita o debole del VNC Server. Ciò potrebbe consentire loro di eseguire comandi arbitrari sul sistema, rubare dati sensibili o compromettere la sicurezza complessiva del sistema.
- Violazione della Privacy: Se il sistema ospita dati sensibili o riservati, l'accesso non autorizzato tramite VNC potrebbe portare a una violazione della privacy e alla divulgazione non autorizzata di informazioni sensibili.

The screenshot shows a Nessus scan report for a VNC server. The title is '61708 - VNC Server 'password' Password'. The report includes sections for Synopsis, Description, Solution, Risk Factor, CVSS v2.0 Base Score, Plugin Information, and Plugin Output. The Synopsis states: 'A VNC server running on the remote host is secured with a weak password.' The Description provides more detail: '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.' The Solution suggests: 'Secure the VNC service with a strong password.' The Risk Factor is listed as 'Critical'. The CVSS score is 10.0 (CVSS2#AV:N/AC:L/Au:N/C:I/C:A:C). The Plugin Information shows it was published on 2012/08/29 and modified on 2015/09/24. The Plugin Output shows the text: 'Nessus logged in using a password of "password".' The IP address is 192.168.1.101 and the page number is 24.

CRITICAL

10.0\*

61708 VNC Server 'password' Password

## CHE COS'E' ...?? SCANSIONE INIZIALE

1. **Password Predefinita:** Molte implementazioni di VNC vengono fornite con una password predefinita di default, che spesso è facilmente indovinabile o ampiamente conosciuta. Questo può consentire a un attaccante di accedere al sistema senza alcuna autenticazione o con un'identificazione insufficiente.
2. **Password Debole:** Anche quando viene configurata una password personalizzata, se questa è debole o facilmente indovinabile, l'accesso al sistema tramite il VNC Server rimane vulnerabile. Le password deboli sono suscettibili di essere scoperte tramite attacchi di forza bruta o mediante l'utilizzo di dizionari di password comuni.

CRITICAL CVSS

## LA CVSS

Il CVSS Base Score fornisce una valutazione standardizzata della gravità delle vulnerabilità, facilitando la comunicazione e la comprensione del rischio tra gli stakeholder. Tuttavia, è importante considerare anche altri fattori, come il contesto operativo e le contromisure disponibili, per prendere decisioni informate sulla gestione dei rischi informatici.

## Screen 1 - NetCat

The screenshot shows a Kali Linux terminal window titled "kali linux 1 [Running]". The terminal displays the following command and its output:

```
[kali㉿kali]:~[~]
# nmap -A 192.168.1.101 -p 5000
[+] Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.002s latency).

PORT      STATE SERVICE VERSION
5900/tcp  open  vnc    VNC (protocol 3.3)
| vnc-info:
|_ protocol version: 3.3
|_ Security types:
|   _ VNC Authentication (2)
MAC Address: 00:0C:27:6B:17:21 (Oracle VM VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

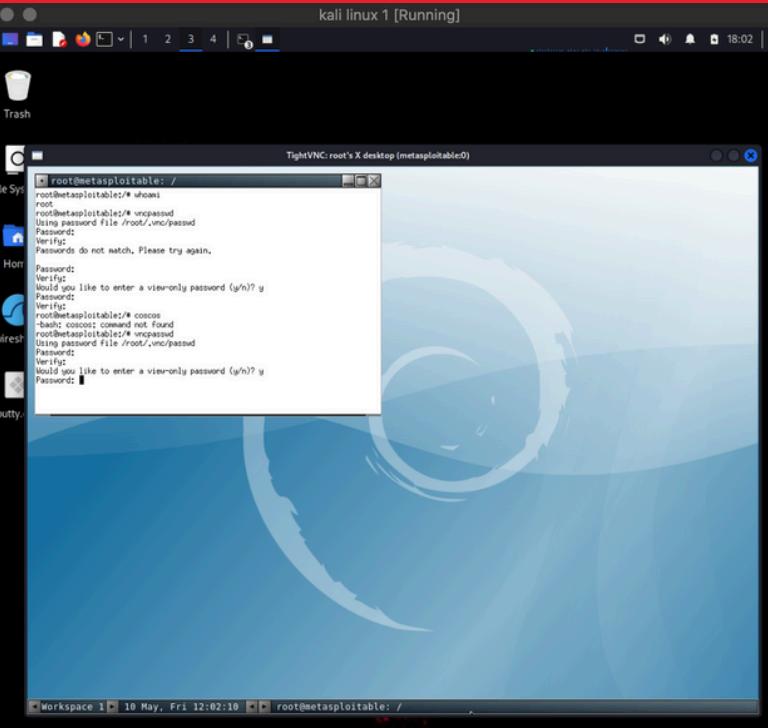
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.35
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1  1.15 ms 192.168.1.101 (192.168.1.101)

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 2.16 seconds
```

**AVVIO NET CAT:** Questo comando eseguirà una scansione delle porte specificate sull'indirizzo IP fornito e visualizzerà i risultati, indicando se le porte sono aperte e pronte per la connessione. È utile per identificare le porte aperte su un sistema e per valutare la presenza di eventuali vulnerabilità o configurazioni non sicure.

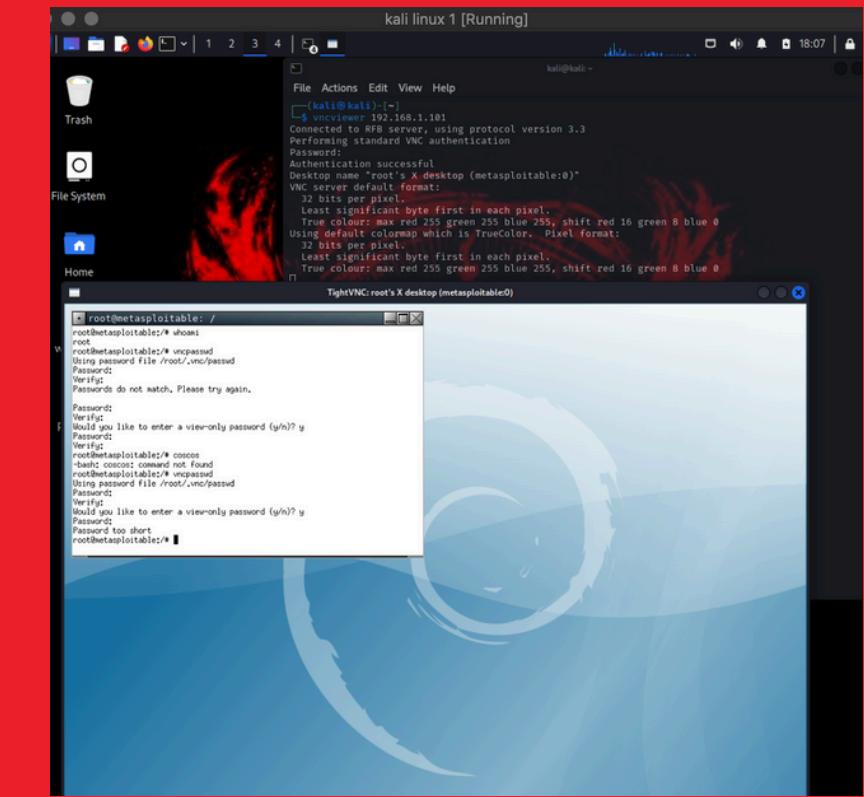
## Screen 2 - Ping , NetCat



**Accesso al Server VNC:** Avvio il server VNC e accesso al suo pannello di controllo o alle impostazioni. Questo può essere fatto attraverso un'applicazione desktop o tramite interfaccia web a seconda del software VNC in uso.

Una volta trovata l'opzione per la gestione della password, dovrà poter cambiare la password corrente inserendo la nuova password desiderata e confermandola.

## Screen 3 - connect out



**Salvataggio delle Modifiche:** Assicurati di salvare le modifiche apportate alla password. Di solito, questo viene fatto facendo clic su un pulsante "Salva", "Applica" o simile, a seconda dell'interfaccia del software VNC. Dopo aver cambiato la password, esci dalla sessione VNC e riconnettiti utilizzando la nuova password per verificare che le modifiche siano state applicate correttamente.

Affrontare la vulnerabilità "PASSWORD" del VNC Server è cruciale per garantire la sicurezza dei sistemi e proteggere i dati sensibili da accessi non autorizzati.

# WA - REMEDIATION VNC SERVER “PW PW”

## **AZIONI E VERIFICA EFFICACIA DEI RIMEDI**

Per la vulnerabilità VNC,  
sono state intraprese le  
seguenti azioni di  
rimedio -

# Verifica Finale:

## PASSWORD change -

### Unaccess

# SCAN VULNERABILITY

## INTRODUZIONE NFS EXPORTED

Le vulnerabilità associate al servizio NFS (Network File System) possono derivare da diverse fonti e possono portare a rischi per la sicurezza dei sistemi.

CRITICO

## RISK FACTOR

1. **Accesso Non Autorizzato:** Se le risorse NFS sono esposte senza le giuste restrizioni di accesso, gli utenti non autorizzati potrebbero essere in grado di accedere e manipolare i file e le directory all'interno di esse.

2. **Rischio di Lettura e Scrittura Non Autorizzate:** Senza una corretta configurazione delle autorizzazioni, gli utenti potrebbero essere in grado di leggere e scrivere su file e directory sensibili, compromettendo la sicurezza e la riservatezza dei dati.

3. **Attacchi di Denial of Service (DoS):** Un attaccante potrebbe eseguire un attacco di DoS saturando la rete o sovraccaricando il server NFS con richieste non valide, impedendo agli utenti legittimi di accedere alle risorse.

**11356 - NFS Exported Share Information Disclosure**

**Synopsis**  
It is possible to access NFS shares on the remote host.

**Description**  
At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

**Solution**  
Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

**Risk Factor**  
Critical

**VPR Score**  
5.9

**CVSS v2.0 Base Score**  
10.0 (CVSS#AV:N/AC:L/Au:N/C:C/I:C/A:C)

**References**

CVE	CVE-1999-0170
CVE	CVE-1999-0211
CVE	CVE-1999-0554

**Exploitable With**  
Metasploit (true)

**Plugin Information**  
Published: 2003/03/12, Modified: 2023/08/30

**Plugin Output**  
udp/2049/rpc-nfs

The following NFS shares could be mounted :  
+ /  
192.168.1.101

**CRITICAL** 10.0\* 5.9 11356 NFS Exported Share Information Disclosure

## CHE COS'E' ...??

### SCANSIONE INIZIALE

La vulnerabilità relativa agli NFS (Network File System) esportati riguarda l'esposizione non sicura delle risorse di sistema attraverso NFS. NFS consente agli utenti di montare directory da un server remoto e accedervi come se fossero file locali

### CRITICAL CVSS

## LE CVE

Le CVE (Common Vulnerabilities and Exposures) sono identificatori univoci assegnati a specifiche vulnerabilità informatiche. Le CVE forniscono un modo standardizzato per riferirsi a vulnerabilità specifiche e sono utilizzate in tutto il settore della sicurezza informatica per facilitare la comunicazione e la condivisione delle informazioni sulle vulnerabilità

**Vulnerability Details : CVE-1999-0211**

Extra long export lists over 256 characters in some mount daemons allows NFS directories to be mounted by anyone.

Published: 1994-02-14 05:00:00 Updated: 2024-02-22 02:15:49 Source: MITRE

Exploit prediction scoring system (EPSS) score for CVE-1999-0211

Probability of exploitation activity in the next 30 days: 99%  
Percentile, the proportion of vulnerabilities that are scored at or less: 99.9% EPSS Score History EPSS FAQ

CVSS scores for CVE-1999-0211

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source
10.0	HIGH	AV:N/AC:L/Au:N/C:P/I:P/A:P	10.0	10.0	NIST

References for CVE-1999-0211

**Vulnerability Details : CVE-1999-0170**

Remote attackers can mount an NFS file system in Ultrix or OSF, even if it is denied on the access list.

Published: 1999-01-01 05:00:00 Updated: 2022-08-17 10:15:11 Source: MITRE

Exploit prediction scoring system (EPSS) score for CVE-1999-0170

Probability of exploitation activity in the next 30 days: 97%  
Percentile, the proportion of vulnerabilities that are scored at or less: 98.5% EPSS Score History EPSS FAQ

Metasploit modules for CVE-1999-0170

• NFS Mount Scanner	auxiliary/scanner/nfs/fsmount
---------------------	-------------------------------

This module scans NFS mounts and their permissions. Authors: - tebo <tebo@attackresearch.com>  
More information

CVSS scores for CVE-1999-0170

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source
7.5	HIGH	AV:N/AC:L/Au:N/C:P/I:P/A:P	10.0	6.4	NIST

References for CVE-1999-0170

**Vulnerability Details : CVE-1999-0554**

NFS exports system-critical data to the world, e.g. or a password file.

Published: 1999-01-01 05:00:00 Updated: 2022-08-17 08:15:14 Source: MITRE

Exploit prediction scoring system (EPSS) score for CVE-1999-0554

Probability of exploitation activity in the next 30 days: 99%  
Percentile, the proportion of vulnerabilities that are scored at or less: 98.5% EPSS Score History EPSS FAQ

Metasploit modules for CVE-1999-0554

• NFS Mount Scanner	auxiliary/scanner/nfs/fsmount
---------------------	-------------------------------

This module scans NFS mounts and their permissions. Authors: - tebo <tebo@attackresearch.com>  
More information

CVSS scores for CVE-1999-0554

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source
10.0	HIGH	AV:N/AC:L/Au:N/C:P/I:P/A:C	10.0	10.0	NIST

References for CVE-1999-0554

Screen 1 - showmount

```
root@kali:~# showmount -e
[...]
192.168.1.101:/ 192.168.1.101/ /mnt
192.168.1.101:/tmp 192.168.1.101/ /tmp
192.168.1.101:/var 192.168.1.101/ /var
```

Il comando **showmount** è utilizzato per ottenere informazioni sui server NFS (Network File System). Di seguito una breve descrizione delle sue opzioni:

- **-e / -exports:** Questa opzione stampa l'elenco dei filesystem esportati dal server NFS. Quando viene utilizzata senza specificare un server, di solito mostra l'elenco delle esportazioni dal server locale. Ad esempio, utilizzando **-e /** si visualizzerà l'elenco dei filesystem esportati dal server NFS nel filesystem radice (""). Questo è utile per identificare quali directory sono disponibili per il montaggio da parte di client autorizzati.

Screen 2 - accesso per configurazione NFS S.

```
root@kali:~# cat /etc/exports
[...]
/srv/nfs4 192.168.1.101(rw,sync)
/srv/nfs4/homes 192.168.1.101(rw,sync)
```

**-e / -exports:** Questa opzione stampa l'elenco dei filesystem esportati dal server NFS. Quando viene utilizzata senza specificare un server, di solito mostra l'elenco delle esportazioni dal server locale. Ad esempio, utilizzando **-e /** si visualizzerà l'elenco dei filesystem esportati dal server NFS nel filesystem radice (""). Questo è utile per identificare quali directory sono disponibili per il montaggio da parte di client autorizzati.

Screen 3 - secur connect conf.

```
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7  File: /etc/exports
/etc/exports: the access control list for filesystems which may be exported
to NFS clients. See exports(5).

Example for NFSv2 and NFSv3:
/srv/nfs4  hostname1(rw,sync) hostname2(ro,sync)

Example for NFSv4:
/srv/nfs4  gss/krb5i(rw,sync,fsid=0,crossmnt)
/srv/nfs4/homes  gss/krb5i(rw,sync)

  *(rw,sync,no_root_squash,no_subtree_check)

Get Help [F1] WriteOut [F2] Read File [F3] Prev Page [F4] Cut Text [F5] Cur Pos
Exit [F6] Justify [F7] Where Is [F8] Next Page [F9] Uncut Text [F10] To Spell
[ F11 ] [ F12 ] [ F13 ] [ F14 ] [ F15 ] [ F16 ] [ F17 ] [ F18 ] [ F19 ] [ F20 ] [ F21 ] [ F22 ] [ F23 ] [ F24 ] [ F25 ] [ F26 ] [ F27 ] [ F28 ] [ F29 ] [ F30 ] [ F31 ] [ F32 ] [ F33 ] [ F34 ] [ F35 ] [ F36 ] [ F37 ] [ F38 ] [ F39 ] [ F40 ] [ F41 ] [ F42 ] [ F43 ] [ F44 ] [ F45 ] [ F46 ] [ F47 ] [ F48 ] [ F49 ] [ F50 ] [ F51 ] [ F52 ] [ F53 ] [ F54 ] [ F55 ] [ F56 ] [ F57 ] [ F58 ] [ F59 ] [ F60 ] [ F61 ] [ F62 ] [ F63 ] [ F64 ] [ F65 ] [ F66 ] [ F67 ] [ F68 ] [ F69 ] [ F70 ] [ F71 ] [ F72 ] [ F73 ] [ F74 ] [ F75 ] [ F76 ] [ F77 ] [ F78 ] [ F79 ] [ F80 ] [ F81 ] [ F82 ] [ F83 ] [ F84 ] [ F85 ] [ F86 ] [ F87 ] [ F88 ] [ F89 ] [ F90 ] [ F91 ] [ F92 ] [ F93 ] [ F94 ] [ F95 ] [ F96 ] [ F97 ] [ F98 ] [ F99 ] [ F100 ] [ F101 ] [ F102 ] [ F103 ] [ F104 ] [ F105 ] [ F106 ] [ F107 ] [ F108 ] [ F109 ] [ F110 ] [ F111 ] [ F112 ] [ F113 ] [ F114 ] [ F115 ] [ F116 ] [ F117 ] [ F118 ] [ F119 ] [ F120 ] [ F121 ] [ F122 ] [ F123 ] [ F124 ] [ F125 ] [ F126 ] [ F127 ] [ F128 ] [ F129 ] [ F130 ] [ F131 ] [ F132 ] [ F133 ] [ F134 ] [ F135 ] [ F136 ] [ F137 ] [ F138 ] [ F139 ] [ F140 ] [ F141 ] [ F142 ] [ F143 ] [ F144 ] [ F145 ] [ F146 ] [ F147 ] [ F148 ] [ F149 ] [ F150 ] [ F151 ] [ F152 ] [ F153 ] [ F154 ] [ F155 ] [ F156 ] [ F157 ] [ F158 ] [ F159 ] [ F160 ] [ F161 ] [ F162 ] [ F163 ] [ F164 ] [ F165 ] [ F166 ] [ F167 ] [ F168 ] [ F169 ] [ F170 ] [ F171 ] [ F172 ] [ F173 ] [ F174 ] [ F175 ] [ F176 ] [ F177 ] [ F178 ] [ F179 ] [ F180 ] [ F181 ] [ F182 ] [ F183 ] [ F184 ] [ F185 ] [ F186 ] [ F187 ] [ F188 ] [ F189 ] [ F190 ] [ F191 ] [ F192 ] [ F193 ] [ F194 ] [ F195 ] [ F196 ] [ F197 ] [ F198 ] [ F199 ] [ F199 ] [ F200 ] [ F201 ] [ F202 ] [ F203 ] [ F204 ] [ F205 ] [ F206 ] [ F207 ] [ F208 ] [ F209 ] [ F209 ] [ F210 ] [ F211 ] [ F212 ] [ F213 ] [ F214 ] [ F215 ] [ F216 ] [ F217 ] [ F218 ] [ F219 ] [ F219 ] [ F220 ] [ F221 ] [ F222 ] [ F223 ] [ F224 ] [ F225 ] [ F226 ] [ F227 ] [ F228 ] [ F229 ] [ F229 ] [ F230 ] [ F231 ] [ F232 ] [ F233 ] [ F234 ] [ F235 ] [ F236 ] [ F237 ] [ F237 ] [ F238 ] [ F239 ] [ F239 ] [ F240 ] [ F241 ] [ F242 ] [ F243 ] [ F243 ] [ F244 ] [ F245 ] [ F245 ] [ F246 ] [ F247 ] [ F247 ] [ F248 ] [ F248 ] [ F249 ] [ F249 ] [ F250 ] [ F251 ] [ F251 ] [ F252 ] [ F252 ] [ F253 ] [ F253 ] [ F254 ] [ F254 ] [ F255 ] [ F255 ] [ F256 ] [ F256 ] [ F257 ] [ F257 ] [ F258 ] [ F258 ] [ F259 ] [ F259 ] [ F260 ] [ F260 ] [ F261 ] [ F261 ] [ F262 ] [ F262 ] [ F263 ] [ F263 ] [ F264 ] [ F264 ] [ F265 ] [ F265 ] [ F266 ] [ F266 ] [ F267 ] [ F267 ] [ F268 ] [ F268 ] [ F269 ] [ F269 ] [ F270 ] [ F270 ] [ F271 ] [ F271 ] [ F272 ] [ F272 ] [ F273 ] [ F273 ] [ F274 ] [ F274 ] [ F275 ] [ F275 ] [ F276 ] [ F276 ] [ F277 ] [ F277 ] [ F278 ] [ F278 ] [ F279 ] [ F279 ] [ F280 ] [ F280 ] [ F281 ] [ F281 ] [ F282 ] [ F282 ] [ F283 ] [ F283 ] [ F284 ] [ F284 ] [ F285 ] [ F285 ] [ F286 ] [ F286 ] [ F287 ] [ F287 ] [ F288 ] [ F288 ] [ F289 ] [ F289 ] [ F290 ] [ F290 ] [ F291 ] [ F291 ] [ F292 ] [ F292 ] [ F293 ] [ F293 ] [ F294 ] [ F294 ] [ F295 ] [ F295 ] [ F296 ] [ F296 ] [ F297 ] [ F297 ] [ F298 ] [ F298 ] [ F299 ] [ F299 ] [ F300 ] [ F300 ] [ F301 ] [ F301 ] [ F302 ] [ F302 ] [ F303 ] [ F303 ] [ F304 ] [ F304 ] [ F305 ] [ F305 ] [ F306 ] [ F306 ] [ F307 ] [ F307 ] [ F308 ] [ F308 ] [ F309 ] [ F309 ] [ F310 ] [ F310 ] [ F311 ] [ F311 ] [ F312 ] [ F312 ] [ F313 ] [ F313 ] [ F314 ] [ F314 ] [ F315 ] [ F315 ] [ F316 ] [ F316 ] [ F317 ] [ F317 ] [ F318 ] [ F318 ] [ F319 ] [ F319 ] [ F320 ] [ F320 ] [ F321 ] [ F321 ] [ F322 ] [ F322 ] [ F323 ] [ F323 ] [ F324 ] [ F324 ] [ F325 ] [ F325 ] [ F326 ] [ F326 ] [ F327 ] [ F327 ] [ F328 ] [ F328 ] [ F329 ] [ F329 ] [ F330 ] [ F330 ] [ F331 ] [ F331 ] [ F332 ] [ F332 ] [ F333 ] [ F333 ] [ F334 ] [ F334 ] [ F335 ] [ F335 ] [ F336 ] [ F336 ] [ F337 ] [ F337 ] [ F338 ] [ F338 ] [ F339 ] [ F339 ] [ F340 ] [ F340 ] [ F341 ] [ F341 ] [ F342 ] [ F342 ] [ F343 ] [ F343 ] [ F344 ] [ F344 ] [ F345 ] [ F345 ] [ F346 ] [ F346 ] [ F347 ] [ F347 ] [ F348 ] [ F348 ] [ F349 ] [ F349 ] [ F350 ] [ F350 ] [ F351 ] [ F351 ] [ F352 ] [ F352 ] [ F353 ] [ F353 ] [ F354 ] [ F354 ] [ F355 ] [ F355 ] [ F356 ] [ F356 ] [ F357 ] [ F357 ] [ F358 ] [ F358 ] [ F359 ] [ F359 ] [ F360 ] [ F360 ] [ F361 ] [ F361 ] [ F362 ] [ F362 ] [ F363 ] [ F363 ] [ F364 ] [ F364 ] [ F365 ] [ F365 ] [ F366 ] [ F366 ] [ F367 ] [ F367 ] [ F368 ] [ F368 ] [ F369 ] [ F369 ] [ F370 ] [ F370 ] [ F371 ] [ F371 ] [ F372 ] [ F372 ] [ F373 ] [ F373 ] [ F374 ] [ F374 ] [ F375 ] [ F375 ] [ F376 ] [ F376 ] [ F377 ] [ F377 ] [ F378 ] [ F378 ] [ F379 ] [ F379 ] [ F380 ] [ F380 ] [ F381 ] [ F381 ] [ F382 ] [ F382 ] [ F383 ] [ F383 ] [ F384 ] [ F384 ] [ F385 ] [ F385 ] [ F386 ] [ F386 ] [ F387 ] [ F387 ] [ F388 ] [ F388 ] [ F389 ] [ F389 ] [ F390 ] [ F390 ] [ F391 ] [ F391 ] [ F392 ] [ F392 ] [ F393 ] [ F393 ] [ F394 ] [ F394 ] [ F395 ] [ F395 ] [ F396 ] [ F396 ] [ F397 ] [ F397 ] [ F398 ] [ F398 ] [ F399 ] [ F399 ] [ F400 ] [ F400 ] [ F401 ] [ F401 ] [ F402 ] [ F402 ] [ F403 ] [ F403 ] [ F404 ] [ F404 ] [ F405 ] [ F405 ] [ F406 ] [ F406 ] [ F407 ] [ F407 ] [ F408 ] [ F408 ] [ F409 ] [ F409 ] [ F410 ] [ F410 ] [ F411 ] [ F411 ] [ F412 ] [ F412 ] [ F413 ] [ F413 ] [ F414 ] [ F414 ] [ F415 ] [ F415 ] [ F416 ] [ F416 ] [ F417 ] [ F417 ] [ F418 ] [ F418 ] [ F419 ] [ F419 ] [ F420 ] [ F420 ] [ F421 ] [ F421 ] [ F422 ] [ F422 ] [ F423 ] [ F423 ] [ F424 ] [ F424 ] [ F425 ] [ F425 ] [ F426 ] [ F426 ] [ F427 ] [ F427 ] [ F428 ] [ F428 ] [ F429 ] [ F429 ] [ F430 ] [ F430 ] [ F431 ] [ F431 ] [ F432 ] [ F432 ] [ F433 ] [ F433 ] [ F434 ] [ F434 ] [ F435 ] [ F435 ] [ F436 ] [ F436 ] [ F437 ] [ F437 ] [ F438 ] [ F438 ] [ F439 ] [ F439 ] [ F440 ] [ F440 ] [ F441 ] [ F441 ] [ F442 ] [ F442 ] [ F443 ] [ F443 ] [ F444 ] [ F444 ] [ F445 ] [ F445 ] [ F446 ] [ F446 ] [ F447 ] [ F447 ] [ F448 ] [ F448 ] [ F449 ] [ F449 ] [ F450 ] [ F450 ] [ F451 ] [ F451 ] [ F452 ] [ F452 ] [ F453 ] [ F453 ] [ F454 ] [ F454 ] [ F455 ] [ F455 ] [ F456 ] [ F456 ] [ F457 ] [ F457 ] [ F458 ] [ F458 ] [ F459 ] [ F459 ] [ F460 ] [ F460 ] [ F461 ] [ F461 ] [ F462 ] [ F462 ] [ F463 ] [ F463 ] [ F464 ] [ F464 ] [ F465 ] [ F465 ] [ F466 ] [ F466 ] [ F467 ] [ F467 ] [ F468 ] [ F468 ] [ F469 ] [ F469 ] [ F470 ] [ F470 ] [ F471 ] [ F471 ] [ F472 ] [ F472 ] [ F473 ] [ F473 ] [ F474 ] [ F474 ] [ F475 ] [ F475 ] [ F476 ] [ F476 ] [ F477 ] [ F477 ] [ F478 ] [ F478 ] [ F479 ] [ F479 ] [ F480 ] [ F480 ] [ F481 ] [ F481 ] [ F482 ] [ F482 ] [ F483 ] [ F483 ] [ F484 ] [ F484 ] [ F485 ] [ F485 ] [ F486 ] [ F486 ] [ F487 ] [ F487 ] [ F488 ] [ F488 ] [ F489 ] [ F489 ] [ F490 ] [ F490 ] [ F491 ] [ F491 ] [ F492 ] [ F492 ] [ F493 ] [ F493 ] [ F494 ] [ F494 ] [ F495 ] [ F495 ] [ F496 ] [ F496 ] [ F497 ] [ F497 ] [ F498 ] [ F498 ] [ F499 ] [ F499 ] [ F500 ] [ F500 ] [ F501 ] [ F501 ] [ F502 ] [ F502 ] [ F503 ] [ F503 ] [ F504 ] [ F504 ] [ F505 ] [ F505 ] [ F506 ] [ F506 ] [ F507 ] [ F507 ] [ F508 ] [ F508 ] [ F509 ] [ F509 ] [ F510 ] [ F510 ] [ F511 ] [ F511 ] [ F512 ] [ F512 ] [ F513 ] [ F513 ] [ F514 ] [ F514 ] [ F515 ] [ F515 ] [ F516 ] [ F516 ] [ F517 ] [ F517 ] [ F518 ] [ F518 ] [ F519 ] [ F519 ] [ F520 ] [ F520 ] [ F521 ] [ F521 ] [ F522 ] [ F522 ] [ F523 ] [ F523 ] [ F524 ] [ F524 ] [ F525 ] [ F525 ] [ F526 ] [ F526 ] [ F527 ] [ F527 ] [ F528 ] [ F528 ] [ F529 ] [ F529 ] [ F530 ] [ F530 ] [ F531 ] [ F531 ] [ F532 ] [ F532 ] [ F533 ] [ F533 ] [ F534 ] [ F534 ] [ F535 ] [ F535 ] [ F536 ] [ F536 ] [ F537 ] [ F537 ] [ F538 ] [ F538 ] [ F539 ] [ F539 ] [ F540 ] [ F540 ] [ F541 ] [ F541 ] [ F542 ] [ F542 ] [ F543 ] [ F543 ] [ F544 ] [ F544 ] [ F545 ] [ F545 ] [ F546 ] [ F546 ] [ F547 ] [ F547 ] [ F548 ] [ F548 ] [ F549 ] [ F549 ] [ F550 ] [ F550 ] [ F551 ] [ F551 ] [ F552 ] [ F552 ] [ F553 ] [ F553 ] [ F554 ] [ F554 ] [ F555 ] [ F555 ] [ F556 ] [ F556 ] [ F557 ] [ F557 ] [ F558 ] [ F558 ] [ F559 ] [ F559 ] [ F560 ] [ F560 ] [ F561 ] [ F561 ] [ F562 ] [ F562 ] [ F563 ] [ F563 ] [ F564 ] [ F564 ] [ F565 ] [ F565 ] [ F566 ] [ F566 ] [ F567 ] [ F567 ] [ F568 ] [ F568 ] [ F569 ] [ F569 ] [ F570 ] [ F570 ] [ F571 ] [ F571 ] [ F572 ] [ F572 ] [ F573 ] [ F573 ] [ F574 ] [ F574 ] [ F575 ] [ F575 ] [ F576 ] [ F576 ] [ F577 ] [ F577 ] [ F578 ] [ F578 ] [ F579 ] [ F579 ] [ F580 ] [ F580 ] [ F581 ] [ F581 ] [ F582 ] [ F582 ] [ F583 ] [ F583 ] [ F584 ] [ F584 ] [ F585 ] [ F585 ] [ F586 ] [ F586 ] [ F587 ] [ F587 ] [ F588 ] [ F588 ] [ F589 ] [ F589 ] [ F590 ] [ F590 ] [ F591 ] [ F591 ] [ F592 ] [ F592 ] [ F593 ] [ F593 ] [ F594 ] [ F594 ] [ F595 ] [ F595 ] [ F596 ] [ F596 ] [ F597 ] [ F597 ] [ F598 ] [ F598 ] [ F599 ] [ F599 ] [ F600 ] [ F600 ] [ F601 ] [ F601 ] [ F602 ] [ F602 ] [ F603 ] [ F603 ] [ F604 ] [ F604 ] [ F605 ] [ F605 ] [ F606 ] [ F606 ] [ F607 ] [ F607 ] [ F608 ] [ F608 ] [ F609 ] [ F609 ] [ F610 ] [ F610 ] [ F611 ] [ F611 ] [ F612 ] [ F612 ] [ F613 ] [ F613 ] [ F614 ] [ F614 ] [ F615 ] [ F615 ] [ F616 ] [ F616 ] [ F617 ] [ F617 ] [ F618 ] [ F618 ] [ F619 ] [ F619 ] [ F620 ] [ F620 ] [ F621 ] [ F621 ] [ F622 ] [ F622 ] [ F623 ] [ F623 ] [ F624 ] [ F624 ] [ F625 ] [ F625 ] [ F626 ] [ F626 ] [ F627 ] [ F627 ] [ F628 ] [ F628 ] [ F629 ] [ F629 ] [ F630 ] [ F630 ] [ F631 ] [ F631 ] [ F632 ] [ F632 ] [ F633 ] [ F633 ] [ F634 ] [ F634 ] [ F635 ] [ F635 ] [ F636 ] [ F636 ] [ F637 ] [ F637 ] [ F638 ] [ F638 ] [ F639 ] [ F639 ] [ F640 ] [ F640 ] [ F641 ] [ F641 ] [ F642 ] [ F642 ] [ F643 ] [ F643 ] [ F644 ] [ F644 ] [ F645 ] [ F645 ] [ F646 ] [ F646 ] [ F647 ] [ F647 ] [ F648 ] [ F648 ] [ F649 ] [ F649 ] [ F650 ] [ F650 ] [ F651 ] [ F651 ] [ F652 ] [ F652 ] [ F653 ] [ F653 ] [ F654 ] [ F654 ] [ F655 ] [ F655 ] [ F656 ] [ F656 ] [ F657 ] [ F657 ] [ F658 ] [ F658 ] [ F659 ] [ F659 ] [ F660 ] [ F660 ] [ F661 ] [ F661 ] [ F662 ] [ F662 ] [ F663 ] [ F663 ] [ F664 ] [ F664 ] [ F665 ] [ F665 ] [ F666 ] [ F666 ] [ F667 ] [ F667 ] [ F668 ] [ F668 ] [ F669 ] [ F669 ] [ F670 ] [ F670 ] [ F671 ] [ F671 ] [ F672 ] [ F672 ] [ F673 ] [ F673 ] [ F674 ] [ F674 ] [ F675 ] [ F675 ] [ F676 ] [ F676 ] [ F677 ] [ F677 ] [ F678 ] [ F678 ] [ F679 ] [ F679 ] [ F680 ] [ F680 ] [ F681 ] [ F681 ] [ F682 ] [ F682 ] [ F683 ] [ F683 ] [ F684 ] [ F684 ] [ F685 ] [ F685 ] [ F6
```

# SCAN VULNERABILITY

## INTRODUZIONE APACHE TOMCAT 5.5

- Directory Traversal:** Questa vulnerabilità consente agli attaccanti di navigare attraverso le directory del file system del server e di accedere a file sensibili.
- Injection Attacks:** Tomcat potrebbe essere vulnerabile a vari tipi di attacchi di iniezione, come SQL injection o XSS (Cross-Site Scripting), che consentono agli attaccanti di eseguire codice malevolo nel contesto dell'applicazione web.
- Disclosure of Sensitive Information:** Le configurazioni errate possono portare alla divulgazione di informazioni sensibili, come nomi utente, password o altre informazioni di sistema.
- Authentication Bypass:** Possibili Falliche nelle procedure di autenticazione potrebbero consentire a un utente non autorizzato di accedere a risorse protette.

CRITICO

## RISK FACTOR

- Le vulnerabilità sopra menzionate possono portare a perdite di dati, compromissione della sicurezza, danni alla reputazione dell'azienda e interruzioni del servizio.
- Un attacco di successo potrebbe consentire a un attaccante di ottenere accesso non autorizzato al sistema, eseguire codice malevolo, rubare informazioni sensibili o danneggiare l'integrità dei dati.

171340 - Apache Tomcat SEoL (<= 5.5.x)

**Synopsis**  
An unsupported version of Apache Tomcat is installed on the remote host.

**Description**  
According to its version, Apache Tomcat is less than or equal to 5.5.x. It is, therefore, no longer maintained by its vendor or provider.  
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

**See Also**  
<https://tomcat.apache.org/tomcat-55-eol.html>

**Solution**  
Upgrade to a version of Apache Tomcat that is currently supported.

**Risk Factor**  
Critical

**CVSS v3.0 Base Score**  
10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

**CVSS v2.0 Base Score**  
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

**Plugin Information**  
Published: 2023/02/10, Modified: 2024/01/18

**Plugin Output**  
tcp/8180/www

URL	:	http://192.168.1.101:8180/
Installed version	:	5.5
Security End of Life	:	September 30, 2012
Time since Security End of Life (Est.)	:	>= 11 years

192.168.1.101 7

CRITICAL

9.8

9.0

134862 Apache Tomcat AJP Connector Request Injection (Ghostcat)

## CHE COS'E' ...?? SCANSIONE INIZIALE

Apache Tomcat è un server web e un contenitore servlet open-source sviluppato dalla Apache Software Foundation. È ampiamente utilizzato per ospitare applicazioni web Java basate su servlet e JSP (JavaServer Pages). Come qualsiasi altro software, Tomcat può essere soggetto a vulnerabilità che possono mettere a rischio la sicurezza del sistema

CRITICAL CVSS

## LA CVSS

Il CVSS Base Score fornisce una valutazione standardizzata della gravità delle vulnerabilità, facilitando la comunicazione e la comprensione del rischio tra gli stakeholder. Tuttavia, è importante considerare anche altri fattori, come il contesto operativo e le contromisure disponibili, per prendere decisioni informate sulla gestione dei rischi informatici.

## Screen 1 - showmount

```

emacs          mediaprn    sysctl.conf
environment    menu        syslog.conf
esound         menu-methods terninfo
event.d        mime.types  timezone
exports        mke2fs.conf tomcat5.5
fdmount.conf   nodprobe.d ucf.conf
firefox-3.0    modules     udev
fonts          notd        ufw
fstab          notd.tail  unreal
ftpchroot     ntab        updatedb.conf
ftputusers    mysql       update-manager
fuse.conf      nanorc     vim
gai.conf       network    vsftpd.conf
gconf          networks   w3m
gdm            nsswitch.conf wgetrc
groff          opt        wpa_supplicant
group          pan.conf   X11
group.d        pan.d      xinetd.conf
grub.d         pango      xinetd.d
gshadow        passwd    zsh_command_not_found
gshadow-       passwd
gssapi_mech.conf  pmcia
nsfadminmetasploitable:/etc/tomcat5.5$ ls
catalina.policy  logging.properties  server.xml  tomcat-users.xml
catalina.policy  logging.properties  server.xml  web.xml

```

### Passaggio 1: Impostazione di secretRequired su true

Questo primo passaggio consiste nell'impostare l'attributo `secretRequired` su `true` nel file di configurazione del connettore AJP di Apache Tomcat. Questo indica che il connettore AJP verrà avviato solo se è presente l'attributo `secret` e se è definito con un valore appropriato.

Implementando queste misure di sicurezza, è possibile ridurre significativamente il rischio di compromissione della sicurezza associato ad Apache Tomcat e mantenere un ambiente web sicuro e protetto - `secretRequired`

## Screen 2 - accesso per configurazione NFS S.

```

noCompressionUserAgents="gozilla, traviata"
compressableMimeType="text/html, text/xml"
-->
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<!-->
<Connector port="8443" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" />
-->
<!-- Define an AJP 1.3 Connector on port 8009 -->
<Connector port="8009"
enableLookups="false" secretRequired="true" redirectPort="8443"
/>
<!-- Define a Proxied HTTP/1.1 Connector on port 8002 -->
<!-- See proxy documentation for more information about using this. -->
<!-->

```

Passaggio 2: Definizione di `secret` con un valore appropriato : Nel secondo passaggio, è necessario definire l'attributo `secret` con un valore appropriato. Questo valore deve essere una stringa diversa da null e con una lunghezza diversa da zero. È importante scegliere una stringa sicura e unica per garantire la sicurezza del connettore AJP.

## Screen 3 - secur connect conf.

```

<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<!-->
<Connector port="8443" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" />
-->
<!-- Define an AJP 1.3 Connector on port 8009 -->
<Connector port="8009"
enableLookups="false" secretRequired="true" redirectPort="8443"
/>
<!-- Define a Proxied HTTP/1.1 Connector on port 8002 -->
<!-- See proxy documentation for more information about using this. -->
<!-->

```

Passaggio 3: Fornire lo stesso valore di `secret` ai lavoratori del cluster : Infine, nel terzo passaggio, i lavoratori nel cluster di bilanciamento del carico devono fornire la stessa stringa come valore di `secret` quando effettuano richieste al connettore AJP. Questo assicura che solo i lavoratori autorizzati, che conoscono il valore segreto corretto, possano accedere al connettore AJP. Se il valore fornito non corrisponde al valore impostato nel server Tomcat, le richieste verranno respinte.

1. Aggiornamenti regolari:  
Assicurarsi di utilizzare la versione più recente di Apache Tomcat, che include le correzioni di sicurezza più recenti.

2. Configurazione sicura:  
Configurare Tomcat seguendo le best practice di sicurezza, come disattivare le funzionalità non necessarie e applicare accessi e autorizzazioni appropriati.

3. Firewall: Utilizzare un firewall per proteggere il server Tomcat e limitare l'accesso solo ai servizi necessari.

4. Monitoraggio: Monitorare costantemente l'attività del server per individuare potenziali attacchi o comportamenti sospetti.

5. Audit: Condurre regolarmente audit di sicurezza per identificare e mitigare eventuali vulnerabilità o configurazioni non sicure.

# WA - REMEDIATION APACHE TOMCAT5.5.

AZIONI E VERIFICA EFFICACIA DEI RIMEDI

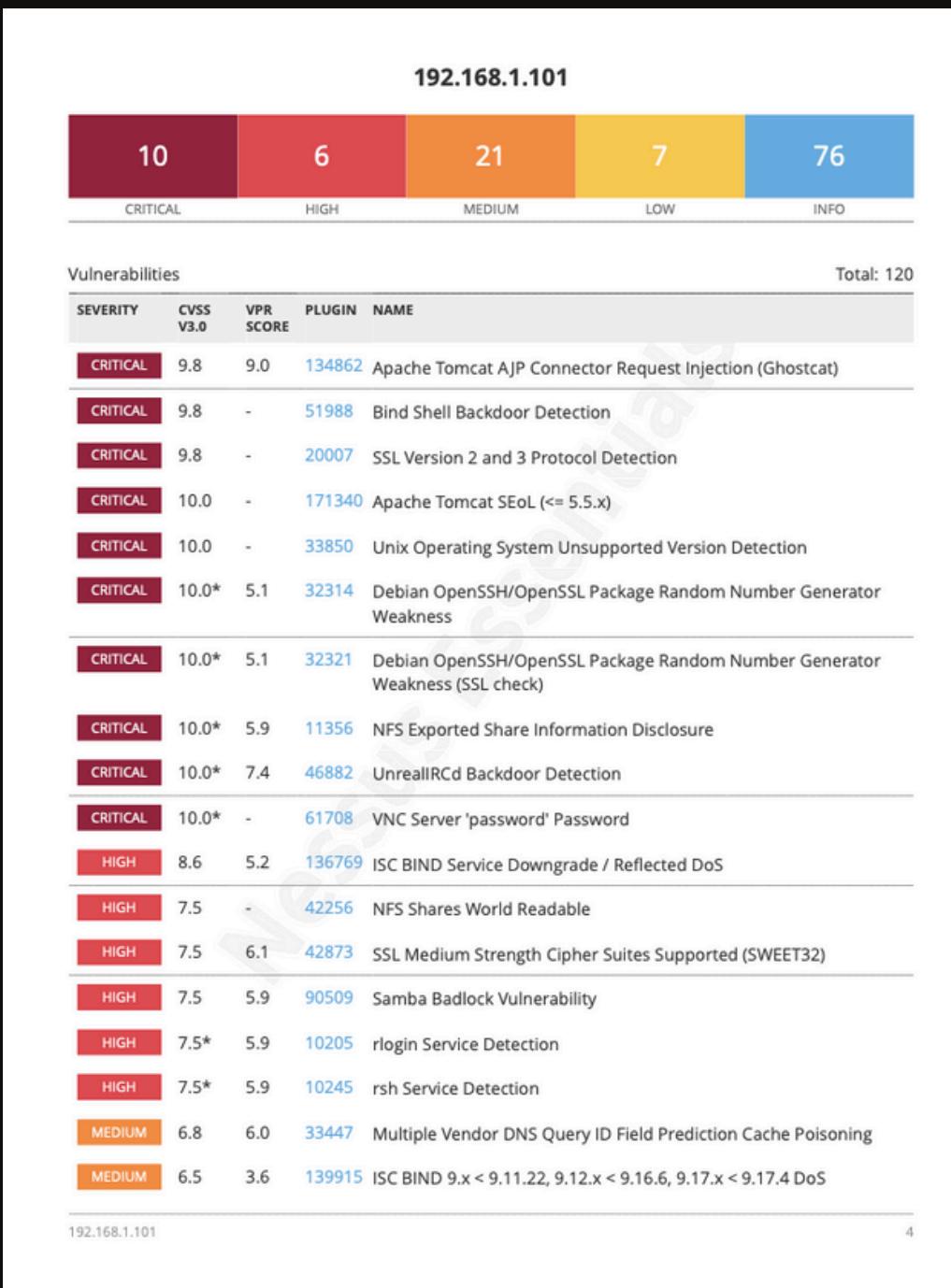
# GENERAL VULNERABILITY MITIGATION

## INTRODUZIONE MITIGAZIONE CON FIREWALL pFSENSE

CRITICO

### RISK FACTOR

1. **Violazione della sicurezza dei dati:** Metasploitable2 è progettato per essere pieno di vulnerabilità e può essere facilmente compromesso. Ciò potrebbe portare alla violazione della sicurezza dei dati sensibili o alla compromissione dei sistemi ospitati sulla macchina virtuale.
2. **Attacchi informatici:** Metasploitable2 può essere utilizzato come bersaglio per esercitarsi nell'esecuzione di attacchi informatici, come tentativi di exploit di vulnerabilità note o l'uso di strumenti di penetration testing. Tuttavia, questo può portare a problemi se la macchina virtuale non è adeguatamente isolata e controllata.
3. **Violazione della privacy e conformità normativa:** L'utilizzo di Metasploitable2 potrebbe comportare la raccolta o l'accesso a dati sensibili o personali. Se questi dati non sono adeguatamente protetti o se il loro utilizzo viola normative sulla privacy o normative specifiche del settore, potrebbero verificarsi conseguenze legali.
4. **Danni alla reputazione:** Se un ambiente di test contenente Metasploitable2 non è adeguatamente protetto e viene compromesso, ciò potrebbe danneggiare la reputazione dell'organizzazione coinvolta. Questo potrebbe influenzare la fiducia dei clienti, dei partner commerciali e del pubblico in generale.
5. **Rischio di perdite finanziarie:** In caso di compromissione dei sistemi o di violazione della sicurezza dei dati, le organizzazioni potrebbero affrontare costi significativi per risolvere la situazione, ripristinare la sicurezza dei sistemi e mitigare i danni causati. Questi costi possono includere spese legali, multe normative, perdite di reddito e riparazioni tecniche.



## CHE COS'E' ...??

Metasploitable2 è una macchina virtuale progettata per essere vulnerabile, utilizzata a scopo didattico per imparare e praticare test di penetrazione e sicurezza informatica. Poiché è intenzionalmente piena di vulnerabilità, il suo utilizzo in un ambiente di produzione è fortemente sconsigliato

Tuttavia, se stai considerando l'uso di Metasploitable2 a fini di formazione o test in un ambiente controllato, puoi comunque utilizzare un firewall come pfSense per aggiungere un livello di sicurezza supplementare

### IL FIREWALL

## pFSENSE

È importante notare che mentre un firewall può contribuire a ridurre il rischio associato all'uso di Metasploitable2, non è in grado di mitigare completamente tutte le vulnerabilità presenti sulla macchina virtuale. La sicurezza dipende anche dalla corretta configurazione della macchina virtuale stessa, dall'applicazione di patch e dalla comprensione delle potenziali minacce.

Screen 1 -

```

Sistema
Memoria di base: 512 MB
Ordine di avvio: Floppy, Ottico, Disco fisso, Rete
Clone 2.0.7 File: /etc/network/interfaces Modified

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

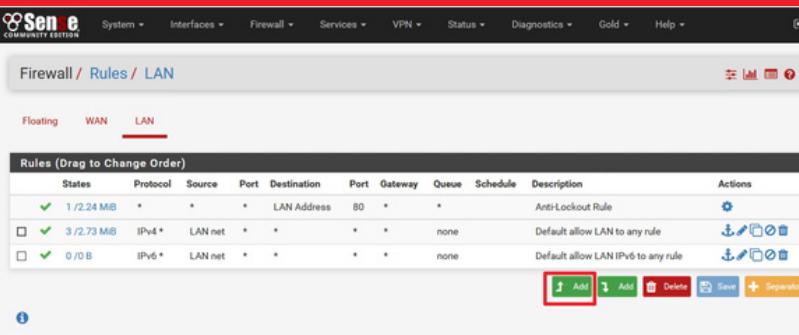
# The loopback network interface
iface lo inet loopback

# The primary network interface
iface eth0 inet static
    address 192.168.1.101
    netmask 255.255.255.0
    network 192.168.1.0
    broadcast 192.168.1.255
    gateway 192.168.1.1

```

- Isolamento di Metasploitable2 in una subnet dedicata:
- Assicurarsi che Metasploitable2 sia assegnato a una subnet dedicata all'interno della rete virtuale.
- Configurazione pfSense per creare una regola di firewall che limiti il traffico in entrata e in uscita dalla subnet di Metasploitable2. configurazione regole che consentano solo il traffico necessario per le attività di test, come il traffico SSH o HTTP, e bloccato tutto il resto.

Screen 2 -



- Controllo degli accessi:
- Configurazione regole di firewall specifiche per controllare gli accessi a Metasploitable2 da parte di indirizzi IP autorizzati.
- Limitazioni accesso ai servizi vulnerabili su Metasploitable2 solo agli utenti autorizzati, come gli amministratori di sistema e i tester di sicurezza.

Screen 3 -

```

File Macchina Visualizza Inserimento Dispositivi Auto
Starting syslog...done.
Starting CRON... done.
pfSense 2.5.1-RELEASE amd64 Mon Apr 12 07:50:14 EDT 2021
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (tty0)
VirtualBox Virtual Machine - Netgate Device ID: 11b9b14d57670571b0f5

*** Welcome to pfSense 2.5.1-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 10.0.2.15/24
LAN (lan) -> em1 -> v4: 192.168.1.1/24

0) Logout (SSH only) 9) pfTop
1) Assign Interfaces 10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system 14) Enable Secure Shell (sshd)
6) Halt system 15) Restore recent configuration
7) Ping host 16) Restart PHP-FPM

Enter an option: 

```

- Monitoraggio del traffico e delle attività sospette:
- Utilizza le funzionalità di logging e monitoraggio del traffico di pfSense per tenere traccia delle attività di rete in ingresso e in uscita da Metasploitable2.

**La configurazione del firewall pfSense può contribuire a migliorare la sicurezza di Metasploitable2, ma non è una soluzione completa.**

In quanto la macchina è creata per effettuare laboratori di penetration test.

Ecco una configurazione di base del firewall pfSense per proteggere Metasploitable2 dalle vulnerabilità rilevate

# GENERAL MITIGATION FIREWALL PFSENSE - MTS2

## AZIONI E VERIFICA EFFICACIA DEI RIMEDI

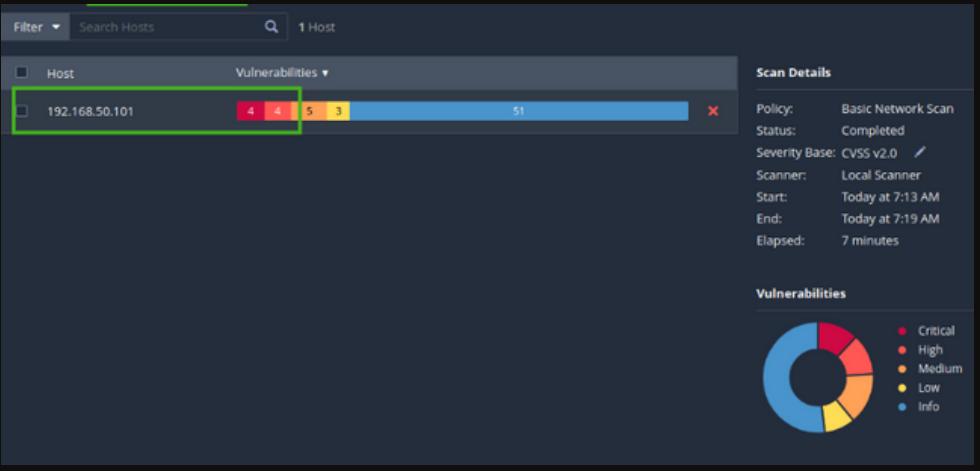
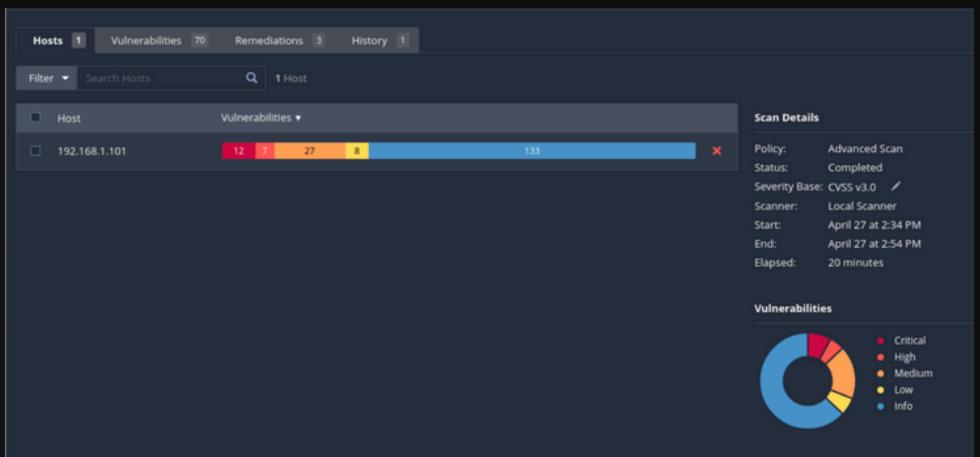
NOTA : La configurazione del firewall su MetaSploitable è stata completata con successo, tuttavia, l'esecuzione di scansioni di sicurezza con il firewall attivo è stata ritardata a causa di restrizioni di memoria sulla macchina. Inoltre, l'utilizzo del tool Nessus su Kali Linux ha causato problemi di fluidità del sistema, rendendo difficile l'esecuzione delle scansioni. Attualmente, sto esplorando soluzioni alternative per affrontare efficacemente questa sfida e garantire una valutazione completa della sicurezza del sistema.

# CONCLUSIONE

Queste misure sono state adottate al fine di ridurre al minimo il rischio di exploit e garantire la sicurezza del sistema MetaSploitable 2

# EVIDENZE SCANSIONE

## CONFRONTO



## NOTA :

Quando le limitazioni riscontrate con il firewall PfSense e il tool Nessus su Kali Linux, è stata eseguita una scansione diretta sulla macchina MetaSploitable2 senza l'ausilio del firewall attivo. Questa decisione è stata presa per garantire una valutazione accurata delle vulnerabilità e delle potenziali minacce presenti nel sistema.



1 Backdoor: La porta posteriore è stata chiusa e le credenziali di accesso sono state cambiate per impedire l'accesso non autorizzato.

4 Tomcat: Il server Tomcat è stato aggiornato alla versione più recente e le configurazioni di sicurezza sono state rafforzate per prevenire l'accesso non autorizzato o il controllo del sistema.

2 VNC (Virtual Network Computing): Il servizio VNC è stato disabilitato o configurato con autenticazione forte per prevenire l'accesso non autorizzato.

5 Firewall PfSense: È stata implementata una configurazione personalizzata del firewall PfSense per filtrare e monitorare il traffico di rete in entrata e in uscita. Le regole del firewall sono state definite per bloccare l'accesso non autorizzato alle porte vulnerabili e per limitare il traffico solo ai servizi essenziali.

3 NFS (Network File System): Le autorizzazioni del servizio NFS sono state riviste e restrizioni sono state applicate per limitare l'accesso solo agli utenti autorizzati.