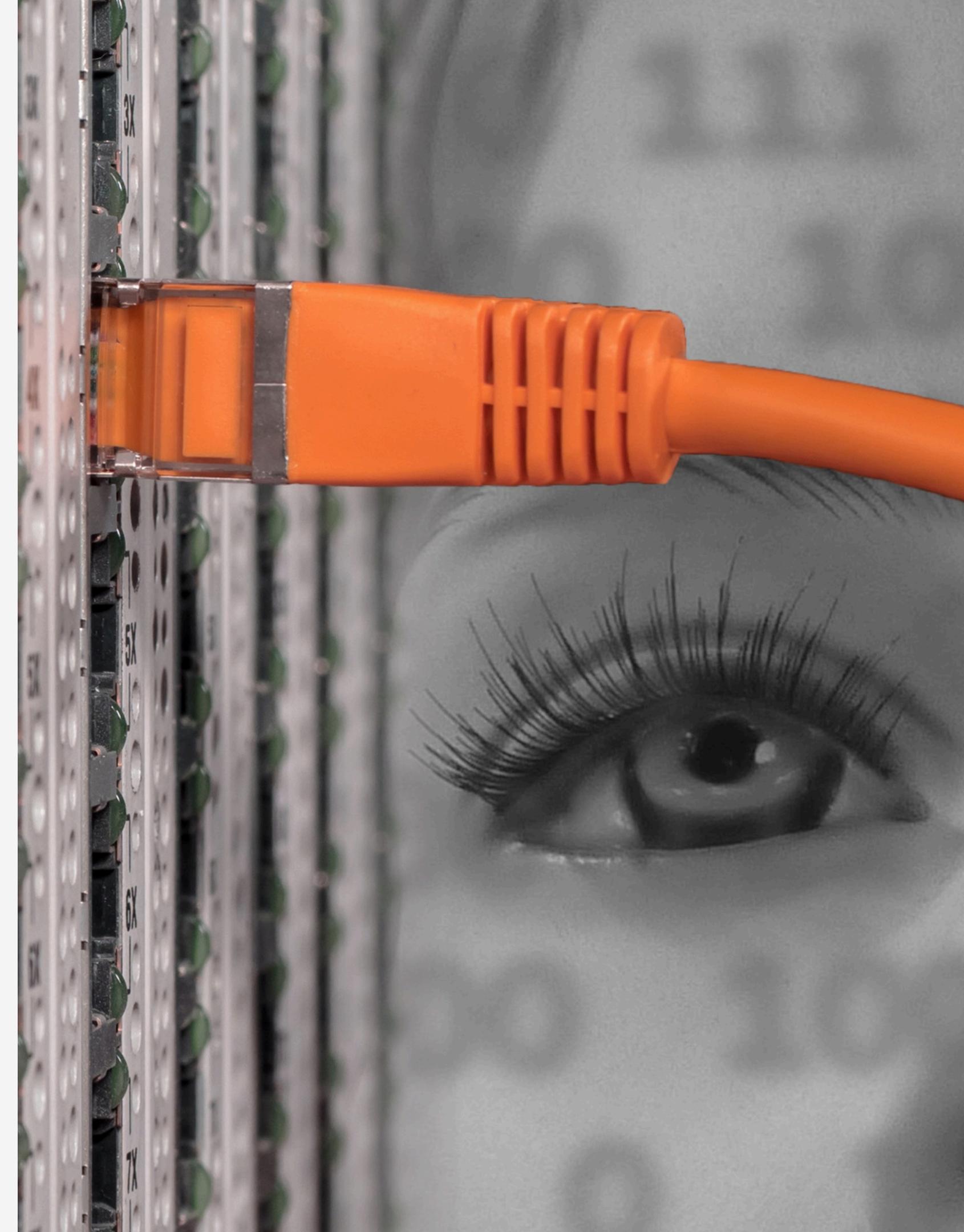


# S5/L5

NESSUS TO  
METASPLOITABLE



# INDICE

---

1. ESERCIZIO
2. VULNERABILITÀ
3. V.CRITICHE
4. ANALISI DELLE V/ SOLUZIONE





# ESERCIZIO

---

## TRACCIA

Consiste nell'effettuare una scansione completa sul target METASPLOITABLE. Dove visto le tante vulnerabilità presentate da questa macchina virtuale, la traccia richiedeva di concentrarci sulle vulnerabilità critiche

# VULNERABILITÀ

## Host Details

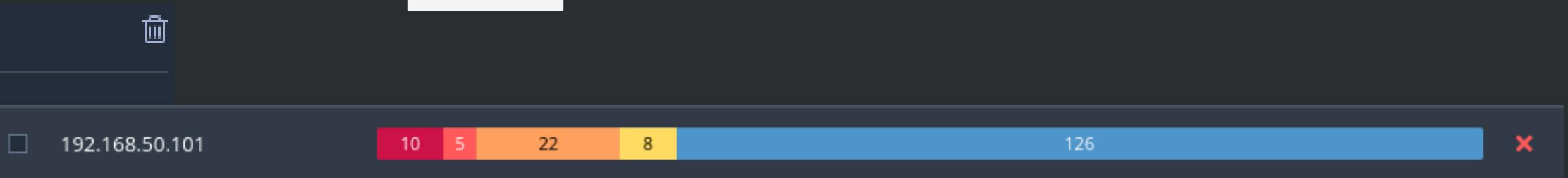
IP: 192.168.50.101  
MAC: 08:00:27:CF:71:97  
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)  
Start: Today at 2:21 PM  
End: Today at 2:52 PM  
Elapsed: 32 minutes  
KB: Download

## Vulnerabilities

- Critical
- High
- Medium
- Low
- Info



HLTRH



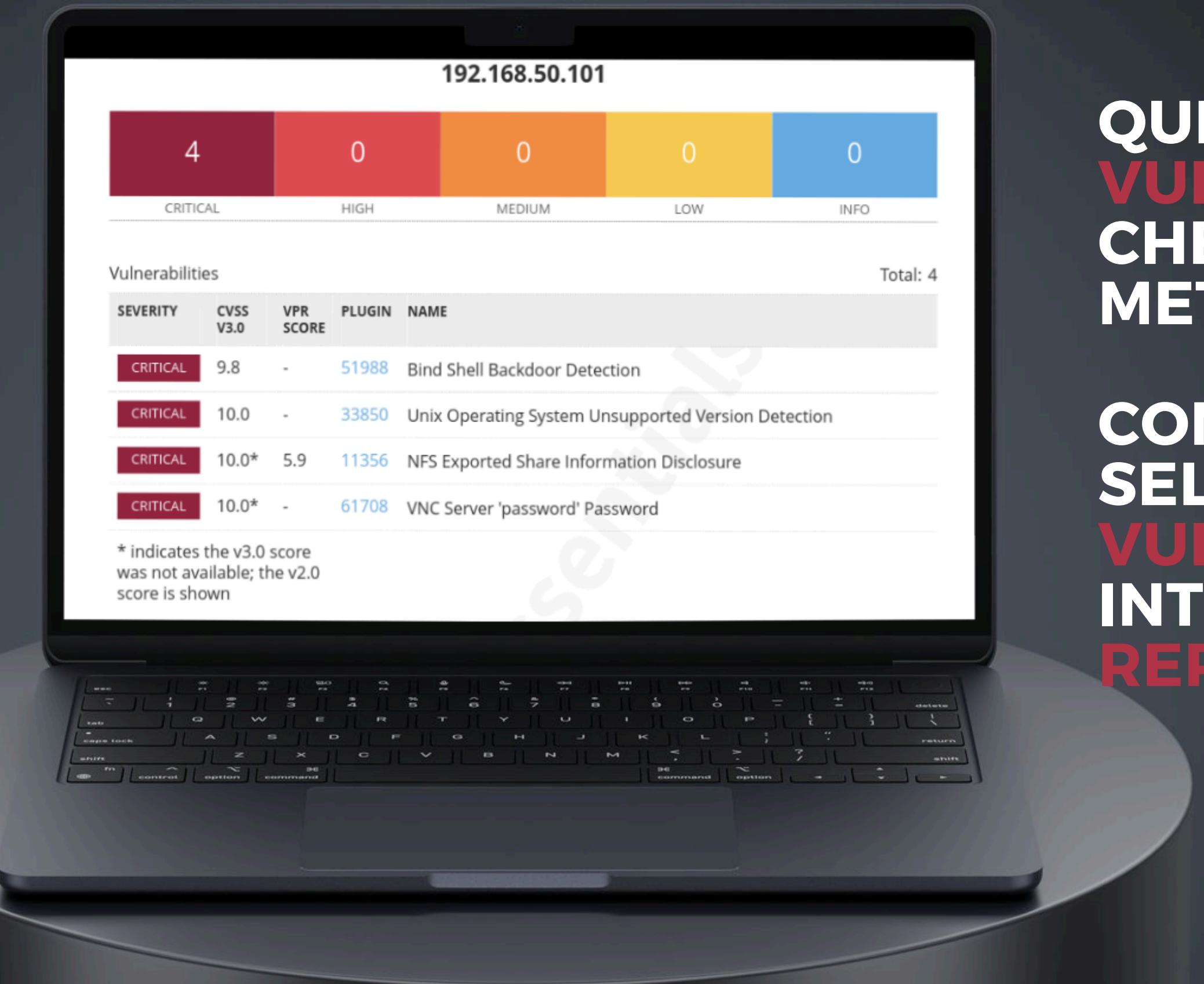
**VEDIAMO UNA PANORAMICA GENERALE DI TUTTE LE VULNERABILITÀ CHE NESSUS HA TOVATO SU METASPLOITABLE.**

**ANDANDO ALL'INTERNO DELLE VULNERABILITÀ NESSUS CI DA UNA DESCRIZIONE DELLA VULNERABILITÀ, E ANCHE UNA SOLUZIONE.**

Sev ▾	CVSS ▾	VPR ▾	Name ▾	Family ▾
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection ...	Web Servers
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely

NEXT

# VULNERABILITÀ CRITICHE



QUESTE SONO LE  
**VULNERABILITÀ CRITICHE**  
CHE PRESENTA  
**METASPLOITABLE.**

COME VEDIAMO NEXUS CI FA  
SELEZIONARE LE  
**VULNERABILITÀ CHE CI**  
**INTERESSANO E CI CREA UN**  
**REPORT SULLE STESE**

NEXT



# ANALISI DELLE V.



CRITICAL

10.0 \*

5.9

NFS Exported Share Information Disclosure



■ Network File System, o NFS, consente agli host remoti di montare sistemi/directory su una rete. Un server NFS può esportare una directory che può essere montata su una macchina Linux remota. Ciò consente all'utente di condividere i dati centralmente su tutte le macchine della rete. Il risultato della scansione della porta mostra che la porta 2049 è aperta e su di essa è in esecuzione il servizio nfs. Quindi : L'aggressore può ottenere privilegi di root sulla macchina compromessa, può utilizzare la macchina come punto cardine per attaccare ulteriormente la rete, compromettendola notevolmente

■ Impostazioni come la limitazione degli indirizzi IP che possono montare le condivisioni esposte e l'utilizzo della funzione "root\_squash" possono restringere la superficie di attacco. Quando "root\_squash" è abilitato su un'esportazione NFS, qualsiasi richiesta di accesso ai file effettuata dal super utente (root) su un client NFS viene "schiacciata" o ridotta a un utente non privilegiato (solitamente "nobody" o "nfsnobody"). Ciò significa che il root sul client NFS non ha privilegi di root quando accede ai file condivisi tramite NFS.

# ANALISI DELLE V.



CRITICAL

10.0

Unix Operating System Unsupported Version Det...



- Il sistema operativo in esecuzione sull'host remoto non è più supportato. Secondo il numero di versione riportato, il sistema operativo Unix in esecuzione sull'host remoto non è più supportato. La mancanza di supporto implica che il fornitore non rilascerà alcuna nuova patch di sicurezza per il prodotto. Di conseguenza, è probabile che contenga vulnerabilità di sicurezza.

- Esegui l'upgrade a una versione del sistema operativo Unix attualmente supportata.

# ANALISI DELLE V.



CRITICAL

10.0 \*

VNC Server 'password' Password



- Un server VNC (Virtual Network Computing) è un software che consente agli utenti di controllare e visualizzare il desktop di un computer remoto attraverso una connessione di rete.
- In sostanza, il server VNC consente di eseguire il mirroring o il controllo remoto del desktop di un computer da un altro computer o dispositivo.
- Se un server VNC in esecuzione sull'host remoto è protetto da una password debole, ciò può costituire un rischio per la sicurezza. Una password debole su un server VNC aumenta il rischio di accesso non autorizzato, violazione della privacy e compromissione del sistema. Gli attaccanti potrebbero facilmente indovinare o scoprire la password, ottenendo così accesso completo al desktop remoto e la possibilità di manipolare dati sensibili.

- Importante utilizzare una password sicura e complessa per proteggere il server VNC. La password dovrebbe essere lunga, casuale e includere una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali.
- Infine, è importante mantenere il software del server VNC aggiornato con le patch di sicurezza più recenti per proteggere contro le vulnerabilità conosciute.

```
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$ vncpasswd  
Using password file /home/msfadmin/.vnc/passwd  
VNC directory /home/msfadmin/.vnc does not exist, creating.  
Password: _
```

# ANALISI DELLE V.



CRITICAL

9.8

Bind Shell Backdoor Detection



■ Quando una shell è in ascolto su una porta remota senza richiedere autenticazione, significa che un servizio di shell remota è attivo e in esecuzione su quella porta, è configurato per consentire connessioni senza autenticazione. Questo può rappresentare un rischio significativo per la sicurezza del sistema, poiché un utente malintenzionato può connettersi alla porta remota utilizzando un client di rete, come ad esempio Telnet o netcat, e inviare direttamente comandi al sistema.

■ Per mitigare questo rischio, è importante implementare misure di sicurezza appropriate, come l'autenticazione forte e la crittografia dei canali di comunicazione, per garantire che solo utenti autorizzati possano accedere alla shell remota e inviare comandi al sistema. Inoltre, è consigliabile monitorare attentamente l'attività di rete e configurare adeguatamente le politiche di sicurezza per prevenire e rilevare eventuali attività sospette o non autorizzate sulla rete.

# SOLUZIONE BACKDOOR

Per avere la certezza della presenza di una backdoor, dal nostro terminale kali, ci connettiamo alla porta che nessus ci ha indicato “1524”.

‘nc 192.168.50.101 1524, vediamo che siamo root, quindi andiamo a vedere quale processo permette questo, apriamo i processi, da root, usiamo il comando ‘lsof -i :1534’, e vediamo che il pd è il 4550, per eliminarlo facciamo sudo kill 4550, e vediamo che non c’è più nessun pd in ascolto.

```
(kali㉿kali)-[~]
└─$ nc 192.168.50.101 1524
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/# whoami
root
root@metasploitable:/# lsof -i :1534
COMMAND PID USER FD TYPE DEVICE SIZE NODE NAME
xinetd 4550 root 12u IPv4 12245      TCP *:ingreslock (LISTEN)
bash 9173 root 0u IPv4 26009      TCP 192.168.50.101:ingreslock
bash 9173 root 1u IPv4 26009      TCP 192.168.50.101:ingreslock
bash 9173 root 2u IPv4 26009      TCP 192.168.50.101:ingreslock
bash 9173 root 255u IPv4 26009      TCP 192.168.50.101:ingreslock
lsof 9227 root 0u IPv4 26009      TCP 192.168.50.101:ingreslock
lsof 9227 root 1u IPv4 26009      TCP 192.168.50.101:ingreslock
lsof 9227 root 2u IPv4 26009      TCP 192.168.50.101:ingreslock
root@metasploitable:/# sudo kill 4550
root@metasploitable:/# sudo lsof -i :1524
COMMAND PID USER FD TYPE DEVICE SIZE NODE NAME
bash 9173 root 0u IPv4 26009      TCP 192.168.50.101:ingreslock
bash 9173 root 1u IPv4 26009      TCP 192.168.50.101:ingreslock
bash 9173 root 2u IPv4 26009      TCP 192.168.50.101:ingreslock
bash 9173 root 255u IPv4 26009      TCP 192.168.50.101:ingreslock
lsof 9257 root 0u IPv4 26009      TCP 192.168.50.101:ingreslock
lsof 9257 root 1u IPv4 26009      TCP 192.168.50.101:ingreslock
lsof 9257 root 2u IPv4 26009      TCP 192.168.50.101:ingreslock
root@metasploitable:/#
```



**HLTRH**

**THANK YOU**

---

*Thanks!*