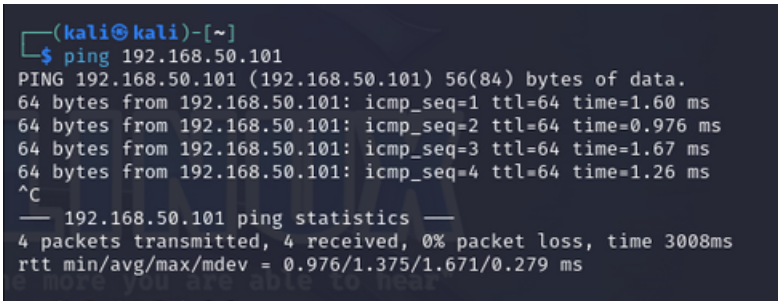
# Report Nessus e remediation actions

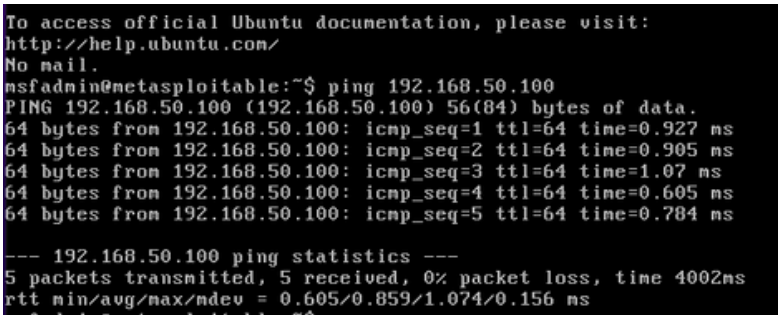
Traccia: Effettuare una scansione completa sul target Metasploitable. Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio. N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate 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.

**Target:**

Metasploitable (IP 192.168.50.101)

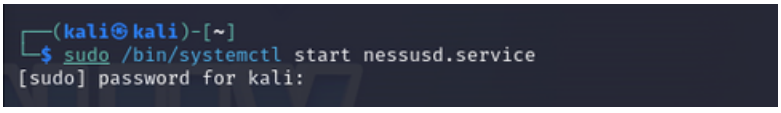
**Verifico comunicazione tra Kali e Meta:**




**Avvio Nessus**

Dopo aver verificato che le macchine comunicano tra di loro faccio partire il servizio con il comando:




e procedo avviando una nuova scansione.

**Scansione iniziale:** Tra le vulnerabilità critical e high ci sono:

| SEVERITY | CVSS V3.0 | VPR SCORE | PLUGIN | NAME |
|---|---|---|---|---|
| CRITICAL | 9.8 | 9.0 | 134862 | Apache Tomcat AJP Connector Request Injection (Ghostcat) |
| CRITICAL | 9.8 | - | 51988 | Bind Shell Backdoor Detection |
| CRITICAL | 9.8 | - | 20007 | SSL Version 2 and 3 Protocol Detection |
| CRITICAL | 10.0 | - | 33850 | Unix Operating System Unsupported Version Detection |
| CRITICAL | 10.0* | 7.4 | 32314 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness |
| CRITICAL | 10.0* | 7.4 | 32321 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) |
| CRITICAL | 10.0* | 5.9 | 11356 | NFS Exported Share Information Disclosure |
| CRITICAL | 10.0* | - | 61708 | VNC Server 'password' Password |
| HIGH | 8.6 | 5.2 | 136769 | ISC BIND Service Downgrade / Reflected DoS |
| HIGH | 7.5 | - | 42256 | NFS Shares World Readable |
| HIGH | 7.5 | 6.1 | 42873 | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| HIGH | 7.5 | 6.7 | 90509 | Samba Badlock Vulnerability |

**Vulnerabilità scelte:**

| | | | | |
|---|---|---|---|---|
| CRITICAL | 9.8 | - | 51988 | Bind Shell Backdoor Detection |
| CRITICAL | 10.0* | 5.9 | 11356 | NFS Exported Share Information Disclosure |
| CRITICAL | 10.0* | - | 61708 | VNC Server 'password' Password |
| HIGH | 7.5 | 6.7 | 90509 | Samba Badlock Vulnerability |

## Prima Vulnerabilità: Bind Shell Backdoor Detection

Con una scansione nmap su Kali avente come target l'ip di Meta vedo su quale porta sia in ascolto il servizio.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-28 23:50 CET
Nmap scan report for 192.168.50.101
Host is up (0.00063s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:99:2A:16 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Una bind shell backdoor è un tipo di backdoor che ascolta attivamente su una specifica porta del sistema compromesso. Quando un utente remoto si connette a questa porta, la backdoor consente l'accesso al sistema, solitamente fornendo un prompt della shell. Questo tipo di backdoor è spesso utilizzato per mantenere l'accesso a un sistema dopo l'effettuazione di un attacco iniziale.

**Remediation action:**

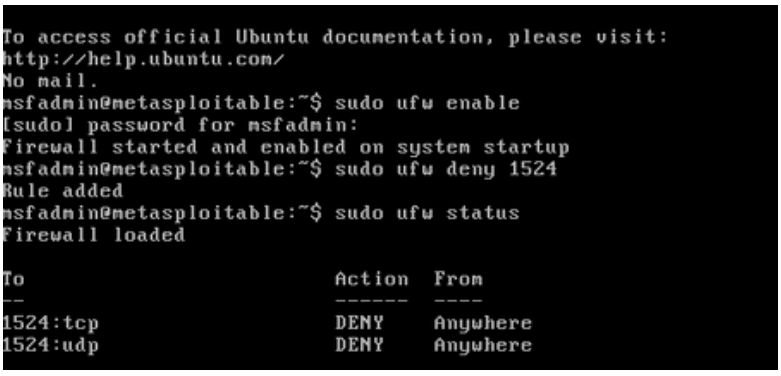
Controllo lo stato di UFW per assicurarmi che sia installato e attivo con il comando
**sudo ufw status**

Nel caso in cui UFW non sia attivo è possibile attivarlo con il comando
**sudo ufw enable**

Per bloccare tutto il traffico in entrata verso la porta 1524 ed impedire il funzionamento della backdoor aggiungo una regola firewall con il comando
**sudo ufw deny 1524**

Dopo aver aggiunto la regola verifico che sia stata aggiunta correttamente  verificando lo stato eseguendo nuovamente il comando
**sudo ufw status**

tenendo conto che se necessario è possibile riavviare il servizio UFW con il comando
**sudo ufw reload**




## Seconda vulnerabilità: NFS Exported Share Information Disclosure

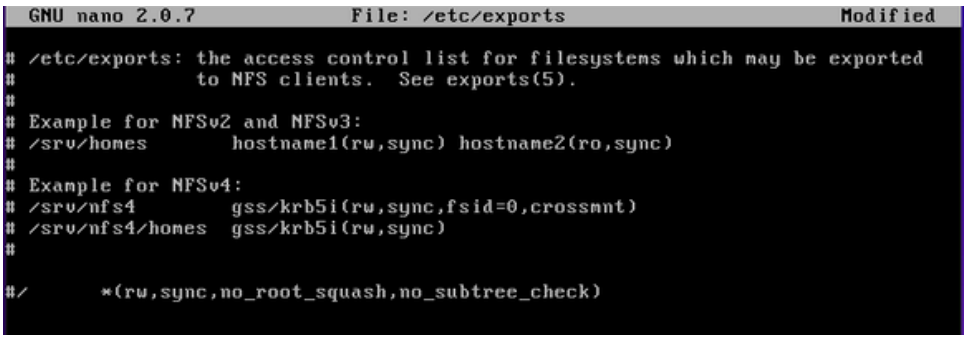
La vulnerabilità "NFS Exported Share Information Disclosure" riguarda i sistemi che utilizzano il Network File System (NFS). NFS è un protocollo utilizzato per la condivisione di file su una rete. La vulnerabilità si verifica quando le condivisioni NFS sono configurate in modo improprio, permettendo a utenti non autorizzati di accedere alle informazioni contenute nelle condivisioni.

**Remediation action:**

Per mitigare una potenziale vulnerabilità nel servizio Network File System (NFS), posso intervenire sul file di configurazione delle esportazioni NFS, situato in **/etc/exports**.
L'ultima riga del file di esportazione rappresenta una configurazione particolarmente insicura che, se attivata, potrebbe permettere ad un attaccante di accedere e modificare i file condivisi con elevati privilegi.
Ognuno dei parametri della riga presa in questione allenta le restrizioni di sicurezza del servizio NFS:

- *: permette l'accesso alla condivisione da qualsiasi host sulla rete.
- rw: concede permessi di lettura e scrittura a tutti gli utenti.
- sync: assicura che le operazioni di scrittura siano completate prima di rispondere, ma non implica restrizioni di sicurezza.
- no_root_squash: consente all'utente root di un client NFS di mantenere i propri privilegi anche quando accede alla condivisione, esponendo il sistema a gravi rischi in caso di accesso da parte di utenti malintenzionati.
- no_subtree_check: disabilita i controlli sulle sottodirectory, che possono migliorare le prestazioni ma potenzialmente esporre a rischi di sicurezza.

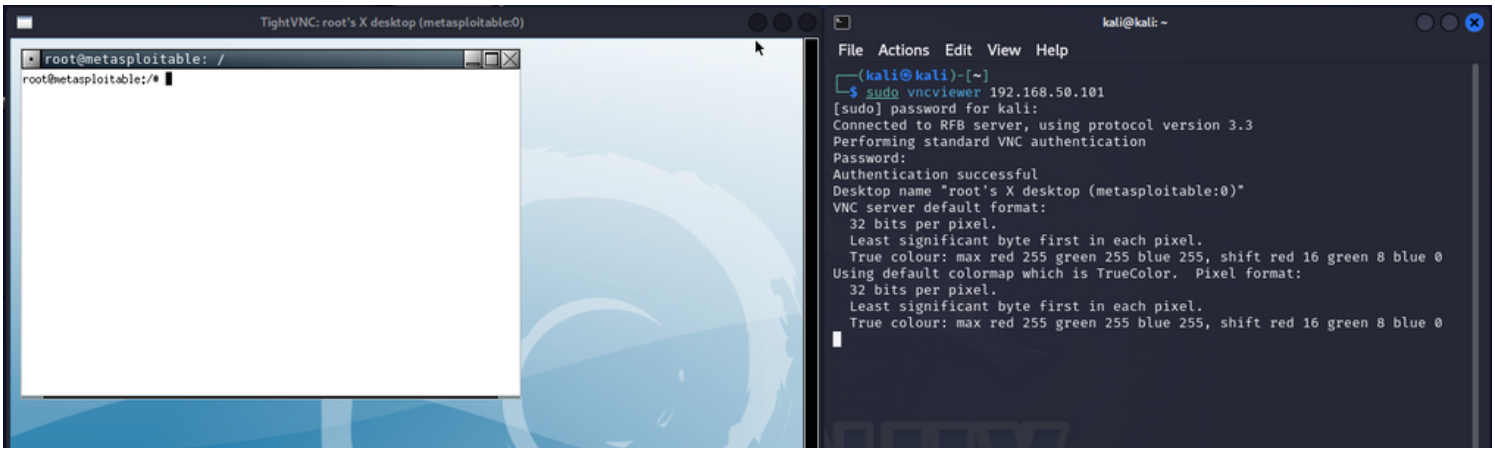
Commentare questa riga previene l'attivazione di tale configurazione, migliorando la sicurezza del sistema. Il server NFS non applicherà più queste opzioni insicure, e di conseguenza, i file condivisi non saranno esposti a rischi derivanti da accesso incontrollato o da privilegi elevati concessi a client non affidabili.




## Terza vulnerabilità: VNC Server “password” Password

Tale vulnerabilità fa riferimento a una debolezza nella gestione delle password da parte del server VNC, che può permettere ad attaccanti di accedere in modo non autorizzato ai sistemi. VNC (Virtual Network Computing) è un sistema di condivisione desktop remoto che consente di controllare un computer da remoto attraverso un altro dispositivo.

In particolare da terminale Kali posso connettermi al visualizzatore VNC usando il comando **sudo vncviewer 192.168.50.101**
autenticandomi con successo usando “password” come Password




**Remediation action:**

Dopo aver avuto accesso ai privilegi amministrativi imposto una password più “forte” usando prima il comando
**vncpasswd**

Infine rispondo “no” per l’opzione di una password di sola lettura.


Per verificare la corretta configurazione della nuova password provo nuovamente ad utilizzare “password” come password per autenticarmi dopo aver lanciato su Kali il comando
**sudo vncviewer 192.168.50.101**

Ottengo come risultato che usando “password” l’autenticazione è fallita.

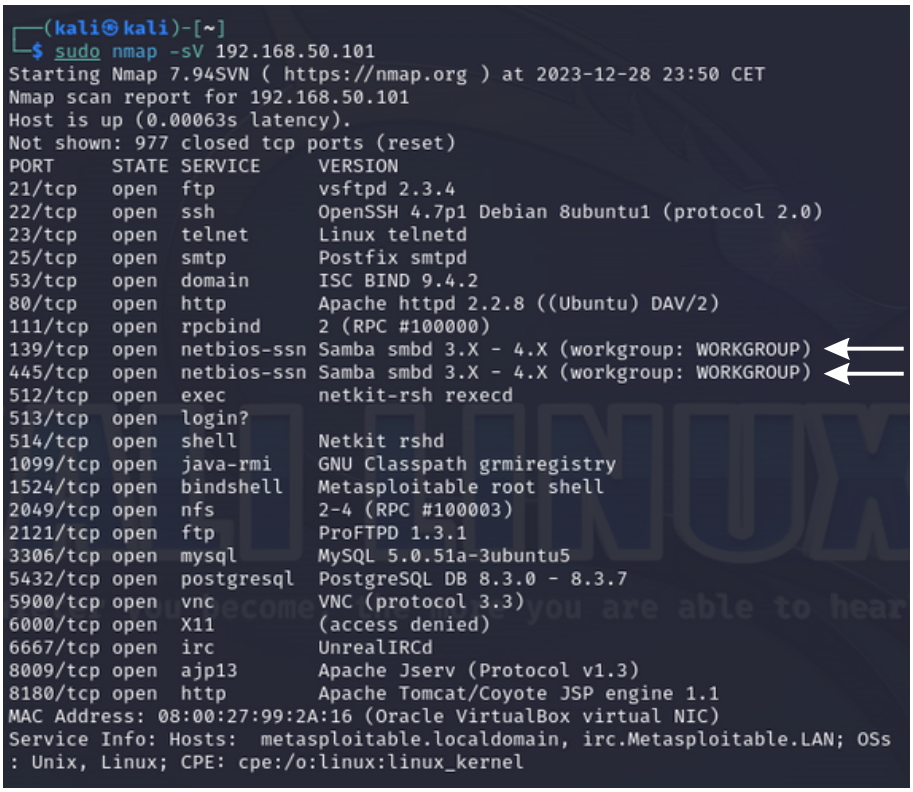

## Quarta vulnerabilità: Samba Badlock Vulnerability

La vulnerabilità Badlock in Samba rappresenta un serio problema di sicurezza in un ambiente informatico. Badlock affligge il protocollo SMB/CIFS (Server Message Block/Common Internet File System), che è un componente chiave per la condivisione di file e stampanti nelle reti.

Questa vulnerabilità si manifesta principalmente attraverso la possibilità di manomissione dei dati. Gli aggressori possono alterare i dati trasmessi attraverso il protocollo SMB, mettendo a rischio informazioni sensibili. Il pericolo si estende anche agli attacchi Man-in-the-Middle, dove un aggressore può intercettare e modificare il traffico tra client e server. Questo tipo di attacco non solo espone a rischi di sicurezza ma può anche condurre alla compromissione della sessione di rete, permettendo agli aggressori di accedere a risorse protette senza autorizzazione.

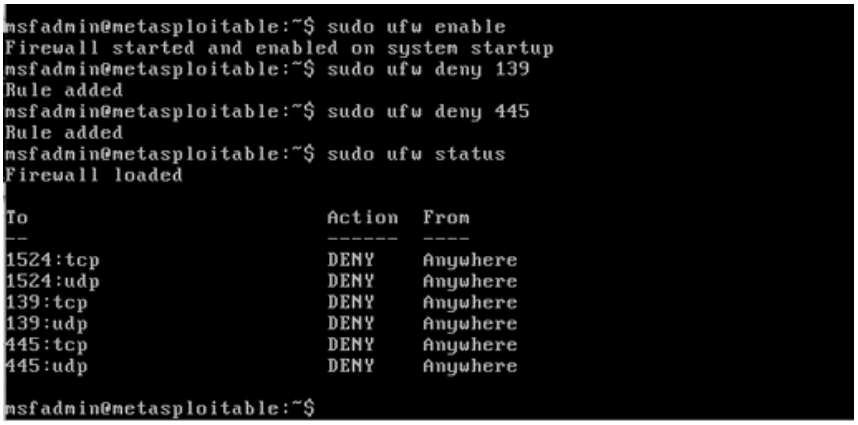
**Remediation action:**

Dalla precedente scansione Nmap su Kali, avente come target l'IP di Meta, posso vedere su quali porte siano in ascolto i servizi interessati.

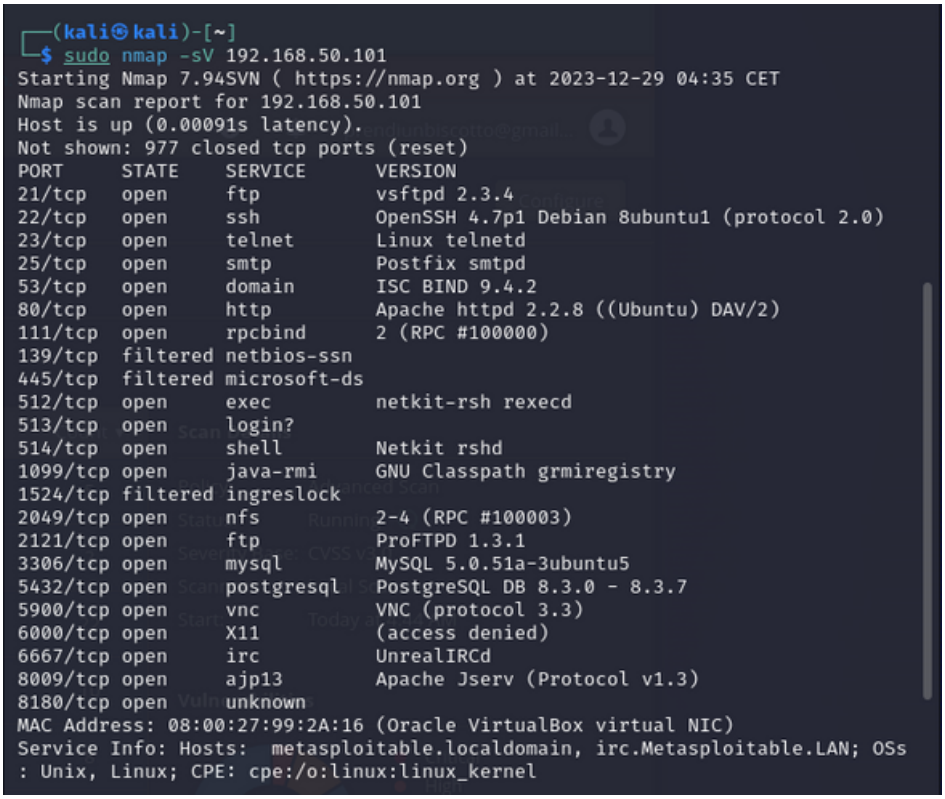



Per bloccare tutto il traffico in entrata verso le porte 139 e 445 ed impedire a qualsiasi servizio di utilizzare queste porte, considerando la possibilità di interrompere la normale condivisione di file e stampanti in rete, uso i comandi
**sudo ufw deny 139**
**sudo ufw deny 445**

Dopo aver aggiunto le regole verifico che siano state aggiunte correttamente verificando lo stato eseguendo nuovamente il comando
**sudo ufw status**



**Effettuando una scansione Nmap prima di procedere con la scansione finale su Nessus** noto che le porte per le quali si applicano le regole firewall appaiono come “filtered”.
Nel contesto della scansione di rete, le porte "filtered" (filtrate) sono quelle per le quali lo scanner non è in grado di determinare se la porta sia aperta o meno perché  a causa delle regole firewall i filtri dei pacchetti impediscono alle sue sonde di raggiungere la porta.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-29 04:35 CET
Nmap scan report for 192.168.50.101
Host is up (0.00091s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          vsftpd 2.3.4
22/tcp   open     ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open     telnet       Linux telnetd
25/tcp   open     smtp         Postfix smtpd
53/tcp   open     domain       ISC BIND 9.4.2
80/tcp   open     http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open     rpcbind      2 (RPC #100000)
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
512/tcp  open     exec         netkit-rsh rexecd
513/tcp  open     login?
514/tcp  open     shell        Netkit rshd
1099/tcp open     java-rmi     GNU Classpath grmiregistry
1524/tcp filtered ingreslock
2049/tcp open     nfs          2-4 (RPC #100003)
2121/tcp open     ftp          ProFTPD 1.3.1
3306/tcp open     mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp open     postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open     vnc          VNC (protocol 3.3)
6000/tcp open     X11          (access denied)
6667/tcp open     irc          UnrealIRCd
8009/tcp open     ajp13        Apache Jserv (Protocol v1.3)
8180/tcp open     unknown
MAC Address: 08:00:27:99:2A:16 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

**Scansione finale:** Tra le vulnerabilità critical e high non ci sono più le vulnerabilità risolte:

| SEVERITY | CVSS V3.0 | VPR SCORE | PLUGIN | NAME |
|---|---|---|---|---|
| CRITICAL | 9.8 | 9.0 | 134862 | Apache Tomcat AJP Connector Request Injection (Ghostcat) |
| CRITICAL | 9.8 | - | 20007 | SSL Version 2 and 3 Protocol Detection |
| CRITICAL | 10.0 | - | 33850 | Unix Operating System Unsupported Version Detection |
| CRITICAL | 10.0* | 7.4 | 32314 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness |
| CRITICAL | 10.0* | 7.4 | 32321 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) |
| HIGH | 8.6 | 5.2 | 136769 | ISC BIND Service Downgrade / Reflected DoS |
| HIGH | 7.5 | 6.1 | 42873 | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| MEDIUM | 6.5 | 3.6 | 139915 | ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS |
| MEDIUM | 6.5 | - | 51192 | SSL Certificate Cannot Be Trusted |