CSPT0524

Esercitazione Analisi delle vulnerabilità e azioni di rimedio M3 W12 D4

INFORMAZIONI DEL DOCUMENTO

1.	**Autore**	Giovanni D'Abrosca
2.	**Nome Documento**	Analisi delle vulnerabilità e azioni di rimedio M3 W12 D4
3.	**Data Emissione**	10/02/2025

Traccia esercizio:

Esercizio Traccia e requisiti Effettuare una scansione completa sul target Metasploitable2.

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.

Screenshot e spiegazione dei passaggi della remediation

In prima analisi ho preso la vulnerabilità OpenSSH 4.7.1 che girava sulla porta 22 e ho proceduto a disinstallare la stessa. Questa particolare vulnerabilità permetteva potenzialmente agli attaccanti di ottenere un accesso non autorizzato al sistema, compromettendo così la sicurezza dell'intero ambiente. L'azione di disinstallazione ha rimosso il servizio vulnerabile, eliminando il rischio associato. Dopo aver completato questo passaggio, ho eseguito una nuova scansione sul target per verificare l'efficacia dell'azione di rimedio.

```
root@metasploitable:/home/msfadmin# apt-get remove --purge openssh-server -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
  openssh-server*
0 upgraded, 0 newly installed, 1 to remove and 138 not upgraded.
After this operation, 668kB disk space will be freed.
(Reading database ... 37634 files and directories currently installed.)
Removing openssh-server ...
 * Stopping OpenBSD Secure Shell server sshd                            [ OK ]
Purging configuration files for openssh-server ...
```

Di seguito è riportato lo screenshot dei risultati della scansione effettuata con nmap:

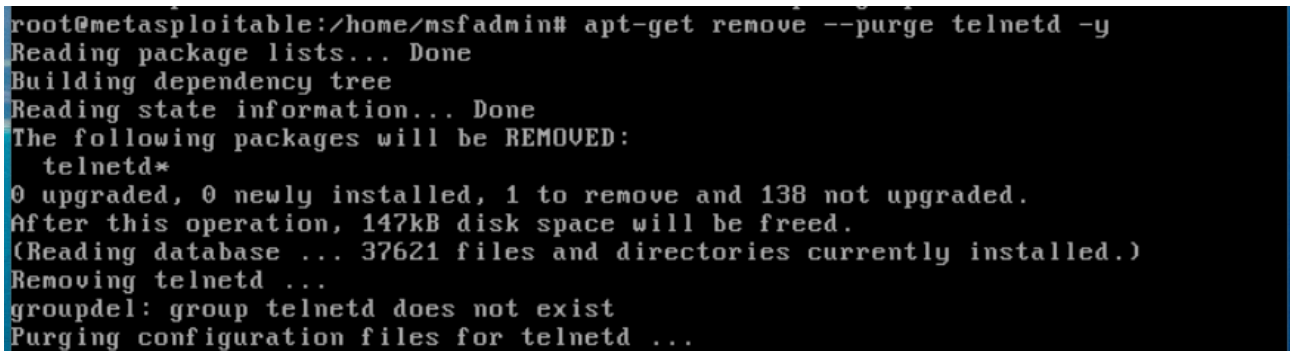
Dalla scansione si può osservare che la porta 22, precedentemente occupata dal servizio OpenSSH 4.7.1 vulnerabile, risulta ora chiusa, confermando così l'efficacia della disinstallazione eseguita.

```
└─$ nmap -sV -p- 192.168.51.120
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-09 23:58 CET
Nmap scan report for 192.168.51.120
Host is up (0.00087s latency).
Not shown: 65506 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
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  tcpwrapped
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
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
37186/tcp open  nlockmgr    1-4 (RPC #100021)
48481/tcp open  mountd      1-3 (RPC #100005)
54229/tcp open  java-rmi    GNU Classpath grmiregistry
56134/tcp open  status      1 (RPC #100024)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 131.46 seconds
```

In seconda analisi, ho preso il servizio telnet che girava sulla porta 23 e ho proceduto a disinstallare il servizio e a modificare il file di configurazione nella directory /etc/inetd.conf. Questa vulnerabilità poteva permettere agli attaccanti di intercettare comunicazioni non criptate, esponendo dati sensibili. Dopo aver rimosso il servizio telnet, ho eseguito una nuova scansione sul target per verificare l'efficacia delle azioni di rimedio.

Di seguito è riportato lo screenshot della disinstallazione del servizio telnet.

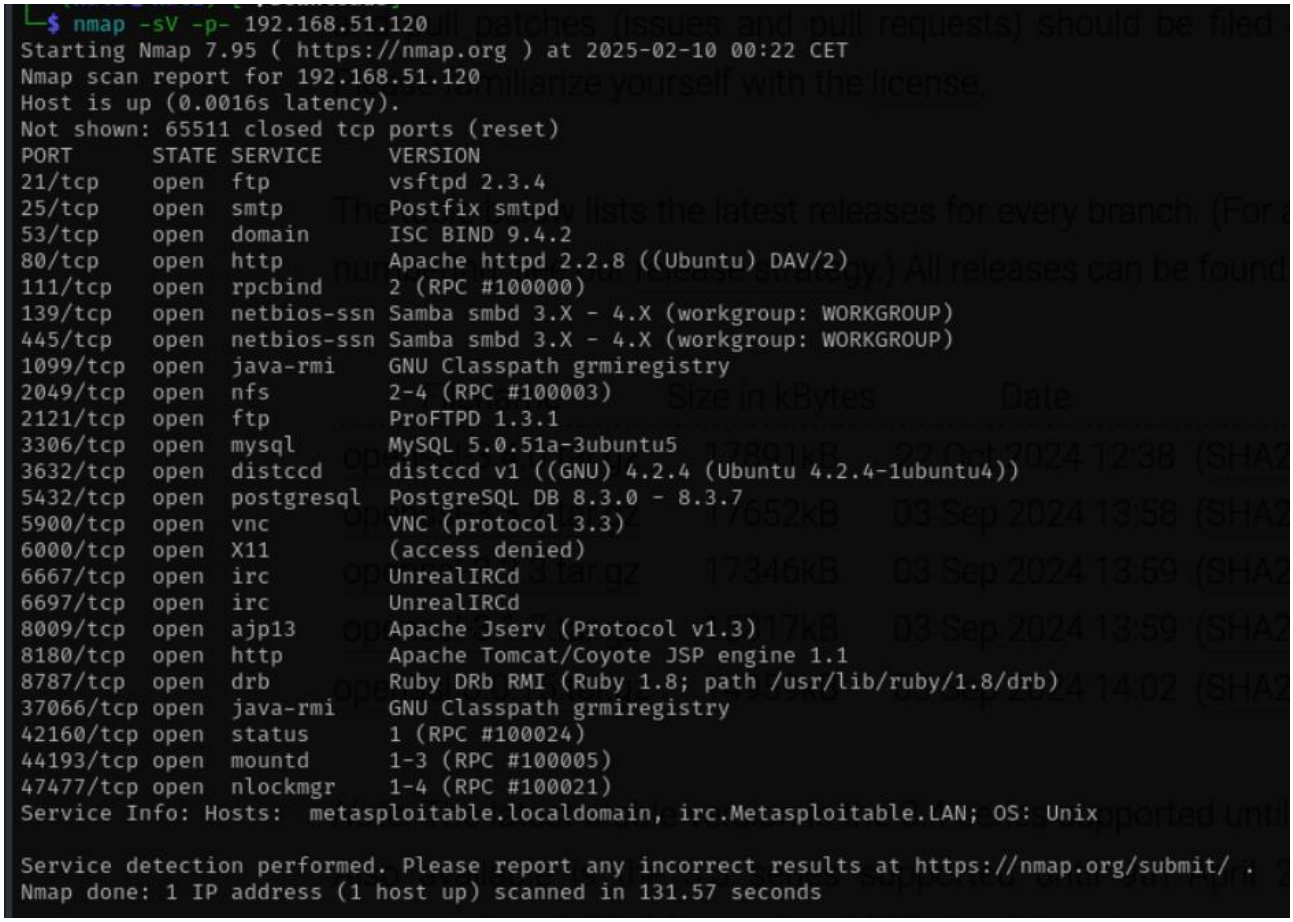


Di seguito è la modifica effettuata al file di configurazione nella directory /etc/inetd.conf:

Questa modifica ha garantito che il servizio telnet non venga più avviato, prevenendo così le intercettazioni di comunicazioni non crittografate.

Successivamente, ho eseguito una nuova scansione con nmap per verificare l'efficacia delle modifiche. Lo screenshot dei risultati della scansione mostra che la porta 23, precedentemente utilizzata dal servizio telnet vulnerabile, risulta ora chiusa, confermando l'efficacia della disinstallazione e della modifica del file di configurazione.

Ecco lo screenshot della scansione effettuata con nmap:



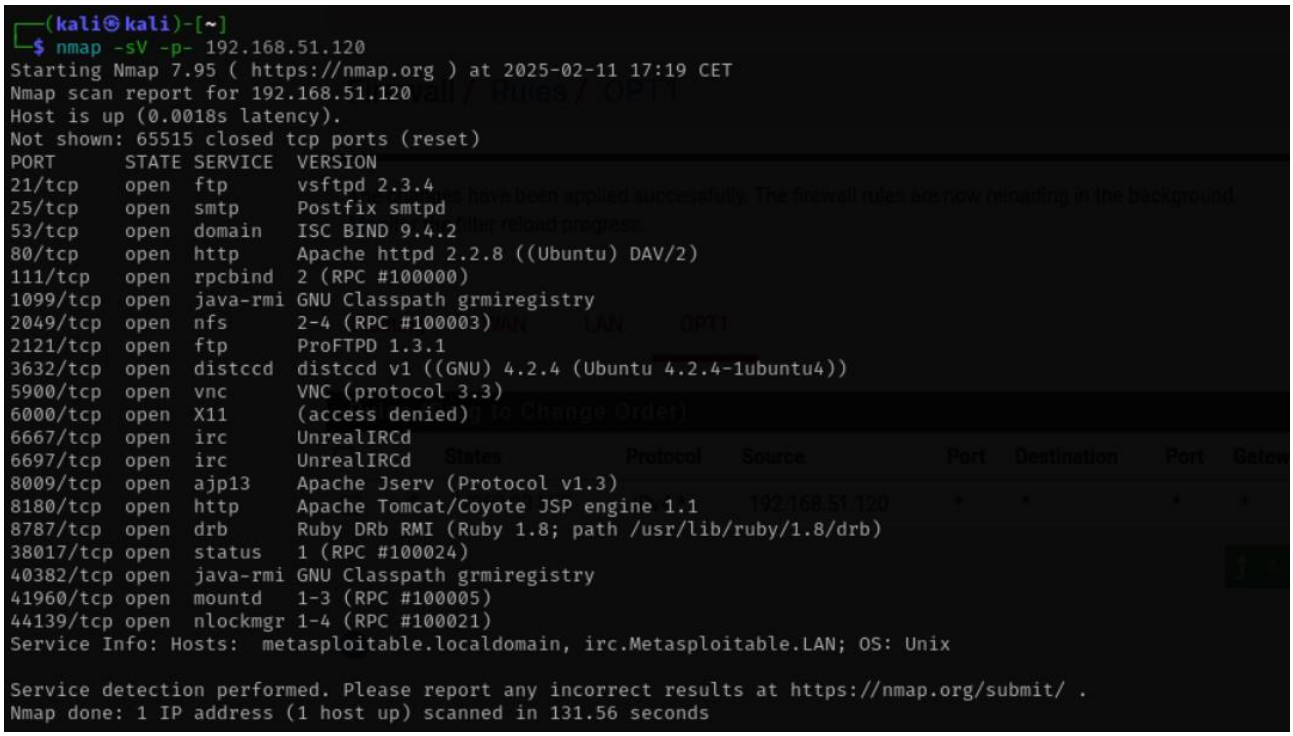
In terza analisi, ho affrontato la chiusura di ulteriori porte vulnerabili su Metasploitable2, assicurandomi che fossero completamente disabilitate e che il sistema fosse protetto contro possibili attacchi. Le porte interessate erano le seguenti: 139, 445, 3306, 5432, 37066, 42160, 44193 e 47477.

Per ciascuna di queste porte, ho proceduto alla disinstallazione dei relativi servizi vulnerabili. Ad esempio, le porte 139 e 445 erano utilizzate dal servizio SMB (Server Message Block), noto per essere vulnerabile a diverse tipologie di attacchi. Dopo aver disinstallato il servizio SMB, ho applicato delle regole firewall tramite iptables per garantire che le porte rimanessero chiuse e inaccessibili.

La porta 3306, utilizzata dal database MySQL, e la porta 5432, relativa al database PostgreSQL, erano entrambe esposte a potenziali exploit che potevano compromettere l'integrità dei dati. Ho disinstallato i servizi MySQL e PostgreSQL e configurato iptables per bloccare l'accesso a queste porte.

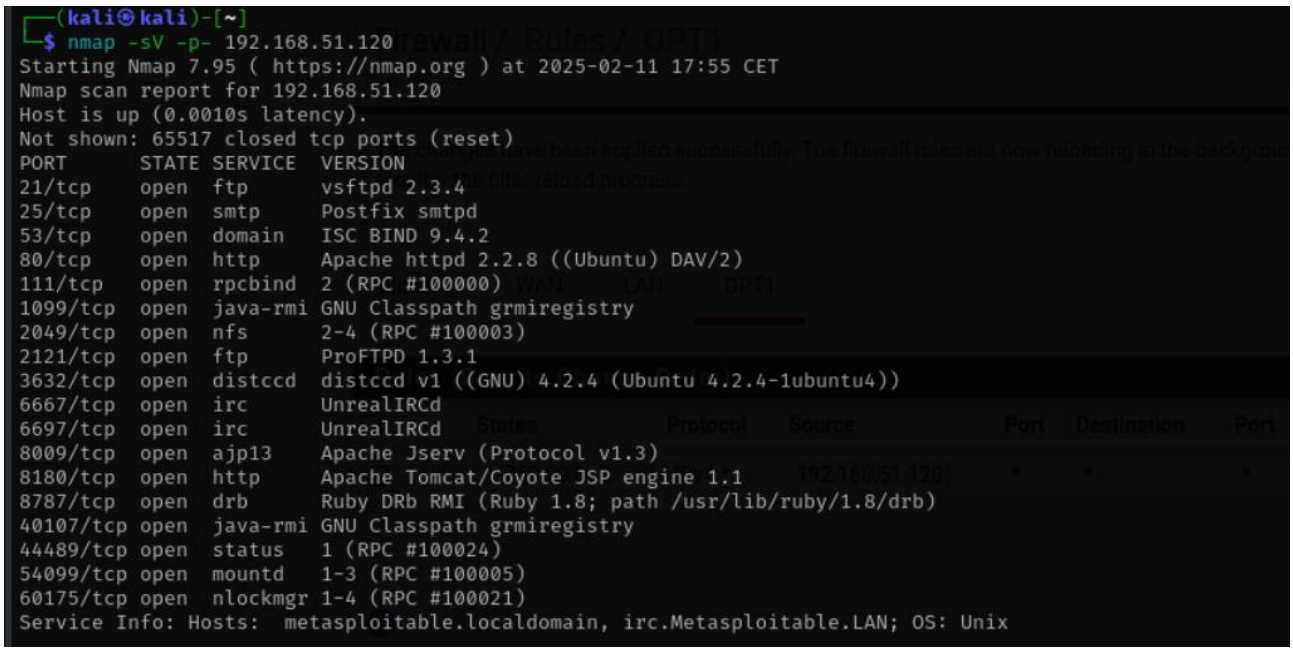
Le porte 37066, 42160, 44193 e 47477 erano utilizzate da servizi meno comuni, ma comunque vulnerabili. Ho proceduto alla loro disinstallazione e ho applicato regole firewall specifiche per prevenire qualsiasi accesso futuro attraverso queste porte.

Dopo aver completato questi passaggi, ho eseguito una scansione completa con nmap per verificare l'efficacia delle disinstallazioni e delle regole firewall. I risultati della scansione confermano che tutte le porte menzionate risultano ora chiuse, garantendo così un ambiente di sistema più sicuro e protetto da potenziali attacchi.



Infine, come quarto caso, ho affrontato la disinstallazione del servizio VNC su Metasploitable2. Il servizio VNC, noto per essere vulnerabile a diverse tipologie di attacchi, rappresentava un rischio significativo per la sicurezza del sistema. Procedendo con la disinstallazione di VNC, ho eliminato una potenziale via di accesso per gli aggressori, garantendo un ulteriore livello di protezione per il sistema.

Di seguito lo screen di una nuova scansione con nmap:



In conclusione, secondo il mio parere, disinstallare i servizi non rappresenta una vera e propria remediation. Idealmente, avrei preferito aggiornare il sistema Metasploitable2 aggiungendo i link aggiornati nella sources.list di Metasploitable. Tuttavia, questo tentativo si è rivelato infruttuoso poiché Metasploitable2 si basa su un sistema obsoleto, "Ubuntu 8.04". Di conseguenza, non sono riuscito ad aggiornare i vari servizi disinstallati, limitando le possibilità di migliorare la sicurezza del sistema attraverso aggiornamenti più recenti e sicuri. Questa situazione evidenzia l'importanza di operare su piattaforme supportate e aggiornate per garantire una protezione efficace contro le minacce più recenti.