Esercizio W12D4

Studente: Roberto Bella

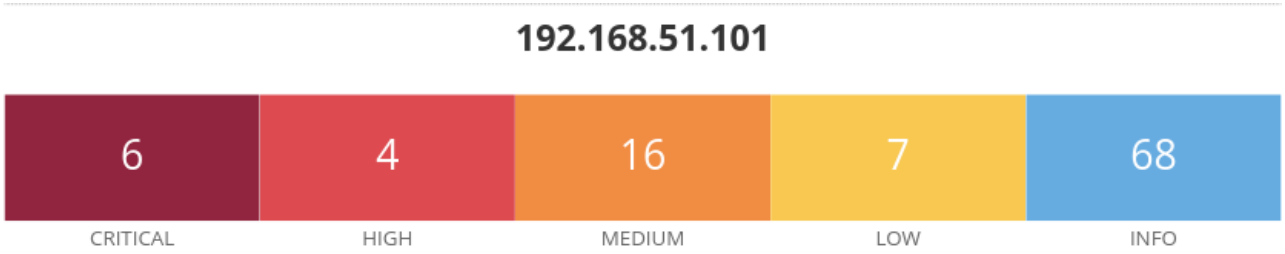
VM scansionata: Metasploitable (192.168.51.101)

Software utilizzato: Tenable Nessus 10.8.3

VM utilizzata: Kali Linux

Viene eseguita la scansione delle vulnerabilità tramite il tool Nessus sulla VM Metasploitable.

La scansione iniziale, come ben sappiamo, evidenzia numerose vulnerabilità presenti sulla VM Metasploitable, rilvando un totale di 33 vulnerabilità e 68 informative così disposte:



Ampliando la ricerca sulle vulnerabilità critiche vengono mostrate quanto segue:

Vulnerabilities Total: 101

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	-	-	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*	-	-	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	-	-	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password

In questo caso andremo ad analizzare e risolvere le vulnerabilità di seguito elencate:

1. CRITICAL 10.0* - - 61708 VNC Server 'password' Password
2. CRITICAL 9.8 - - 51988 Bind Shell Backdoor Detection
3. CRITICAL 9.8 - - 134862 Apache Tomcat AJP Connector Request Injection (Ghostcat)

134862 (1) - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Synopsis

There is a vulnerable AJP connector listening on the remote host.

Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

Solution

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

- Update to the latest version of Apache Tomcat. Apache Tomcat has released versions 9.0.31, 8.5.51, and 7.0.100 to fix this vulnerability.
- Red Hat recommends disabling the Apache JServ Protocol (AJP) connector in Tomcat if not used, or binding it to localhost port, since most of AJP's use is in cluster environments, and the 8009 port should never be exposed on the internet without strict access-control lists. The AJP connector is enabled by default on all Tomcat servers
- If the Apache JServ Protocol (AJP) service is not required, disable it on the host.
- If the AJP service does not need to be publicly accessible, ensure that access is filtered.
- If your Linux distribution or apps include Tomcat, watch for updates from your vendor and apply them.

RISOLUZIONE

Per la risoluzione di questa vulnerabilità viene consigliato di aggiornare il server Tomcat alla versione più recente e di disattivare il servizio qualora non venga utilizzato.

Per disattivare il servizio AJP bisogna recarsi nella cartella di configurazione Tomcat ed editare il file server.xml disattivando il servizio AJP inserendo un commento:

```
msfadmin@metasploitable:/$ cd /usr/share/tomcat5.5/conf
msfadmin@metasploitable:/usr/share/tomcat5.5/conf$ ls
Catalina              logging.properties  server.xml.2025-02-07.06-07-41
catalina.policy       policy.d            tomcat5.5
catalina.properties   server-minimal.xml  tomcat-users.xml
context.xml           server.xml          web.xml
```

Figura 1 Metasploitable, selezione cartella Tomcat

```
<!--<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />-->
```

Figura 2 Commento da aggiungere per disattivare il servizio AJP

51988 (1) - Bind Shell Backdoor Detection

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

Per verificare questa vulnerabilità, ho utilizzato una scansione con Nmap sul target vittima, mostrando la porta 1524 aperta:

```
1524/tcp open  bindshell    Metasploitable root shell
```

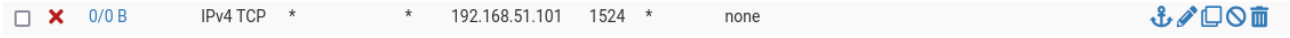
Utilizzando netcat sulla porta 1524 sono riuscito ad utilizzare la shell come root

```
└─$ nc 192.168.51.101 1524
root@metasploitable:/# whoami
root
root@metasploitable:/#
```

RISOLUZIONE

Per risolvere questa vulnerabilità bisogna chiudere la porta 1524 tramite firewall.

Viene, dunque, creata una regola sul firewall al quale la macchina è collegata, in questo caso pfsense, che blocca tale porta.



Utilizzando nuovamente la scansione Nmap viene mostrato che la porta risulta filtrata

```
└─$ sudo nmap -sV -p 1524 192.168.51.101 -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-07 11:20 CET
Nmap scan report for 192.168.51.101
Host is up (0.0035s latency).

PORT     STATE    SERVICE    VERSION
1524/tcp filtered ingreslock
```

```
└─$ nc 192.168.51.101 1524 -v
192.168.51.101: inverse host lookup failed: Host name lookup failure
```

61708 (1) - VNC Server 'password' Password

Synopsis

A VNC server running on the remote host is secured with a weak 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.

Risk Factor

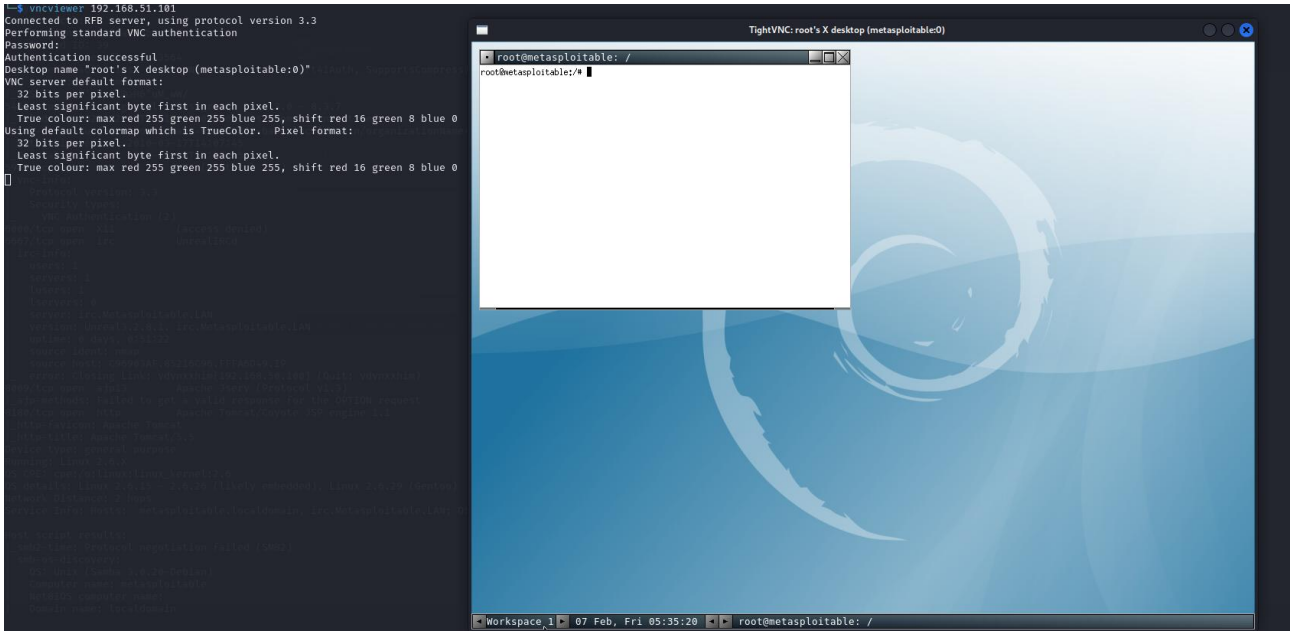
Critical

La vulnerabilità in oggetto mostra come ci sia un problema relativa alla debolezza della password del server VNC.

Utilizzando il software Nmap, viene mostrata la porta del servizio:

```
5900/tcp open  vnc          VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
```

Utilizzando il tool vncviewer si riesce ad ottenere l'accesso alla GUI della macchina utilizzando la password di default (*password*) mostrata da Nessus:



RISOLUZIONE

Per mitigare questa criticità viene consigliato di:

- utilizzare una password più robusta ed attivare l'autenticazione a più fattori.
- Disattivare il servizio se non viene utilizzato.
- Se il servizio viene utilizzando è importante impostare delle regole nel firewall per permettere la connessione solo a determinati indirizzi IP.

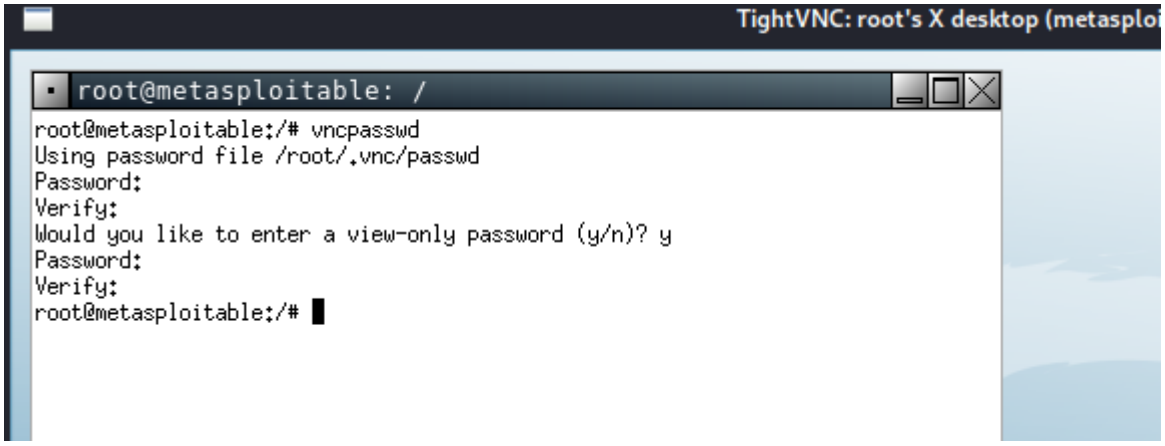


Figura 3 Modifica della password del servizio VNC

Eseguendo una nuova scansione tramite il software Nessus, le vulnerabilità sopra trattate sono state risolte:

192.168.51.101

3	4	16	7	67
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 97

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0*	-	-	32314	Debian OpenSSH/OpenSSL Package Random Number Gener Weakness
CRITICAL	10.0*	-	-	32321	Debian OpenSSH/OpenSSL Package Random Number Gener Weakness (SSL check)
HIGH	8.6	-	-	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	-	42256	NFS Shares World Readable
HIGH	7.5	-	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)

Anche utilizzando una scansione con il tool Nmap le vulnerabilità sopra trattate non vengono più rilevate:

```
└─$ sudo nmap -sV 192.168.51.101 -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-07 12:27 CET
Warning: 192.168.51.101 giving up on port because retransmission cap hit (2).
Stats: 0:01:03 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 90.00% done; ETC: 12:28 (0:00:04 remaining)
Stats: 0:01:40 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.00% done; ETC: 12:28 (0:00:04 remaining)
Nmap scan report for 192.168.51.101
Host is up (0.0051s latency).
Not shown: 953 closed tcp ports (reset), 27 filtered tcp ports (no-response)
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
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ccproxy-ftp?
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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Si allegano le scansioni pre e post risoluzione.