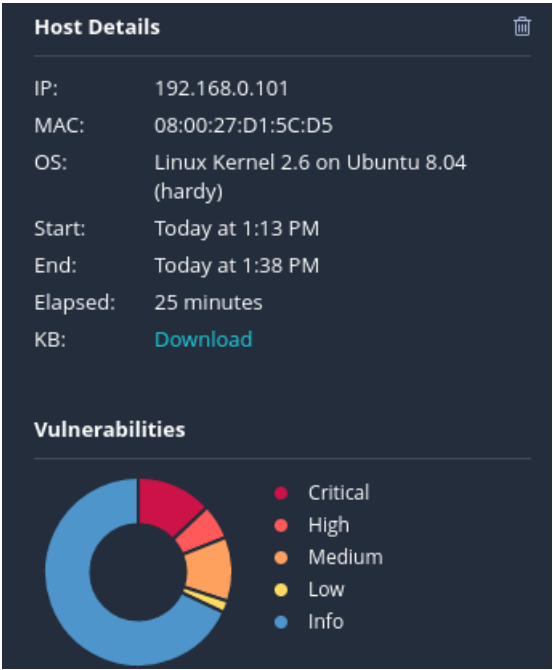


Nell'esercizio di oggi abbiamo eseguito una scansione dell'IP di Metasploitable usando il vulnerability scanner Nessus.

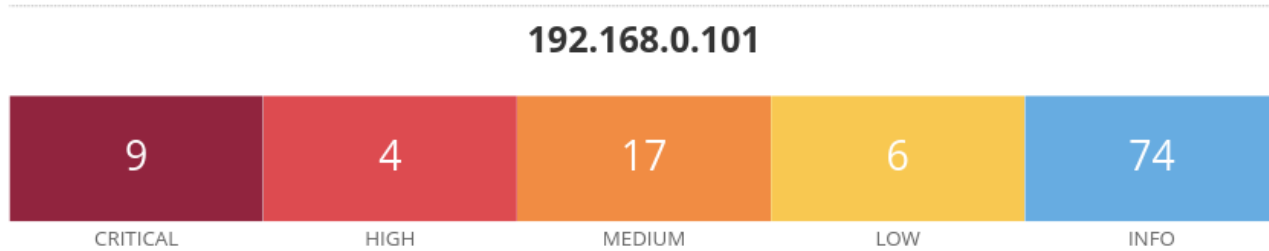
Vulnerabilities 63					
Filter	Search Vulnerabilities				
Sev	CVSS	VPR	Name		Family
<input type="checkbox"/> CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure		RPC
<input type="checkbox"/> CRITICAL	10.0		Unix Operating System Unsupported Version Detection		General
<input type="checkbox"/> CRITICAL	10.0 *		VNC Server 'password' Password		Gain a shell remotely
<input type="checkbox"/> CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)		Web Servers
<input type="checkbox"/> CRITICAL	9.8		Bind Shell Backdoor Detection		Backdoors
<input type="checkbox"/> MIXED	...	...	DNS (Multiple Issues)		DNS
<input type="checkbox"/> CRITICAL	...	...	SSL (Multiple Issues)		Gain a shell remotely
<input type="checkbox"/> MIXED	...	...	SSL (Multiple Issues)		Service detection
<input type="checkbox"/> HIGH	7.5		NFS Shares World Readable		RPC
<input type="checkbox"/> HIGH	7.5	6.7	Samba Badlock Vulnerability		General
<input type="checkbox"/> MIXED	...	...	SSL (Multiple Issues)		General

Vediamo che Nessus ha rilevato 63 vulnerabilità in Metasploitable, alcune non gravi (il 66%) altre di gravità crescente da media a critica.



Nessus può generare report più o meno dettagliati delle vulnerabilità riscontrate.

Prendiamo ad esempio il report meno dettagliato.



Vulnerabilities

Total: 110

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	9.1	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
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

Le criticità più pericolose sono quelle con il numero CVSS più alto (vediamo che ne abbiamo 4 a livello 10.0).

La prima vulnerabilità che incontriamo riguarda NFS Share, un protocollo che gestisce lo stoccaggio e il recupero di dati da parte di dispositivi di storage su rete (in pratica un file system di rete).

**CRITICAL** NFS Exported Share Information Disclosure

**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.

Nessus ci informa che almeno uno degli NFS può essere attaccato e i file in esso contenuti letti o persino riscritti.

La soluzione che ci viene proposta è di mettere al sicuro gli NFS configurando una regola che permetta solo a determinati host di accedervi (potrebbe essere fatto tramite una regola di firewall).

La seconda vulnerabilità è piuttosto comune e riguarda l'intero sistema operativo.

**CRITICAL** **Unix Operating System Unsupported Version Detection**

**Description**

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

**Solution**

Upgrade to a version of the Unix operating system that is currently supported.

La versione del sistema operativo è obsoleta e non è più supportata (di conseguenza no vengono più rilasciate patch per risolvere errori e vulnerabilità). La soluzione più ovvia è quella di fare l'upgrade ad una versione del sistema operativo più recente e supportata.

La terza vulnerabilità è un'altra di quelle più comuni, cioè la sicurezza della password.

**CRITICAL** **VNC Server 'password' 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.

**Output**

```
Nessus logged in using a password of "password".
```

La password settata è proprio “password”, una delle parole chiave più vulnerabili; è una situazione molto facilmente sfruttabile da un black hat e l'unica soluzione possibile è impostare una password più forte, fatta di almeno 8 caratteri (possibilmente di più) e composta da lettere minuscole, maiuscole, numeri e caratteri speciali.

Infine abbiamo una vulnerabilità riscontrata sul web server, sul protocollo AJP.

**CRITICAL** Apache Tomcat AJP Connector Request Injection (Ghostcat)

**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.

**See Also**

- <http://www.nessus.org/u?8ebe6246>
- <http://www.nessus.org/u?4e287adb>
- <http://www.nessus.org/u?cbc3d54e>
- <https://access.redhat.com/security/cve/CVE-2020-1745>
- <https://access.redhat.com/solutions/4851251>
- <http://www.nessus.org/u?dd218234>
- <http://www.nessus.org/u?dd772531>
- <http://www.nessus.org/u?2a01d6bf>
- <http://www.nessus.org/u?3b5af27e>
- <http://www.nessus.org/u?9dab109f>
- <http://www.nessus.org/u?5eafc70>

Un attaccante potrebbe sfruttare questa vulnerabilità per accedere a file presenti nel web server o persino caricare malware (o file contenenti malware) nel server stesso.

In questo caso Nessus ci propone due soluzioni: cambiare la configurazione del protocollo AJP in modo che sia necessaria un'autorizzazione per accedere al server o aggiornare ad una versione più recente il server stesso.