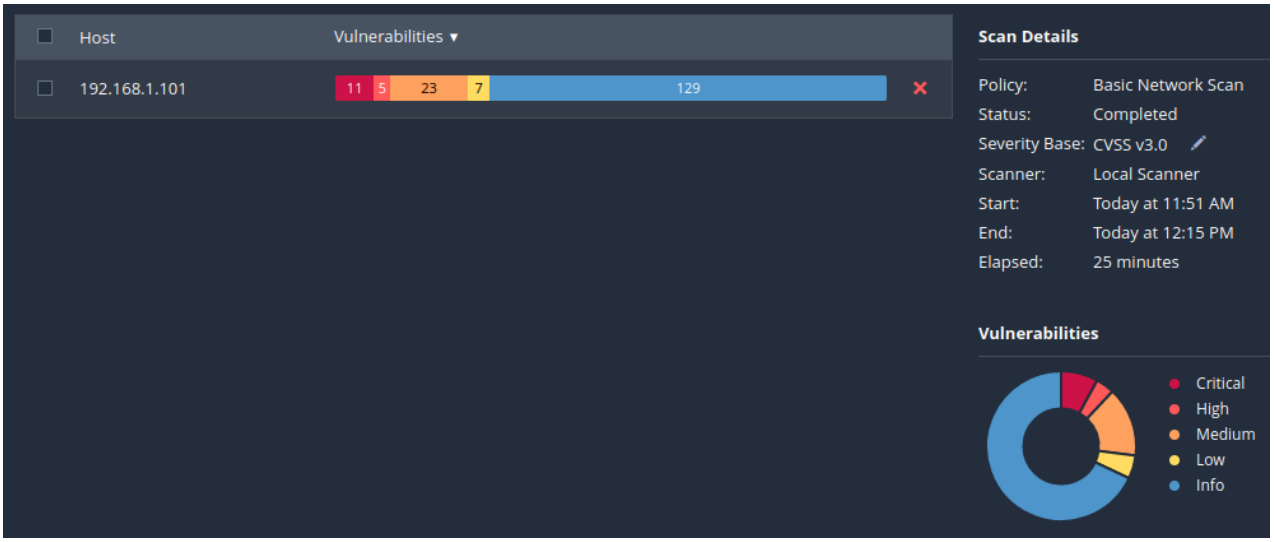
Vulnerability Assessment: Nessus

Scopo dell'esercizio di oggi è quello di effettuare un **vulnerability assessment** su macchina virtuale Metasploitable usando il software **Nessus**, elencare i risultati e proporre eventuali soluzioni.

Essendo Metasploitable una macchina virtuale progettata per essere particolarmente vulnerabile, la quantità di vulnerabilità trovata è molto alta: come da immagine seguente, Nessus ha trovato ben 11 vulnerabilità critiche, 5 alte, 23 medie e 7 basse. A scopo didattico (e per brevità), analizzeremo le prime quattro vulnerabilità critiche riportate proponendo per ognuna di esse una soluzione.



In particolare, le quattro che andremo ad analizzare sono le seguenti, come proposte dal report finale dello stesso Nessus.

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

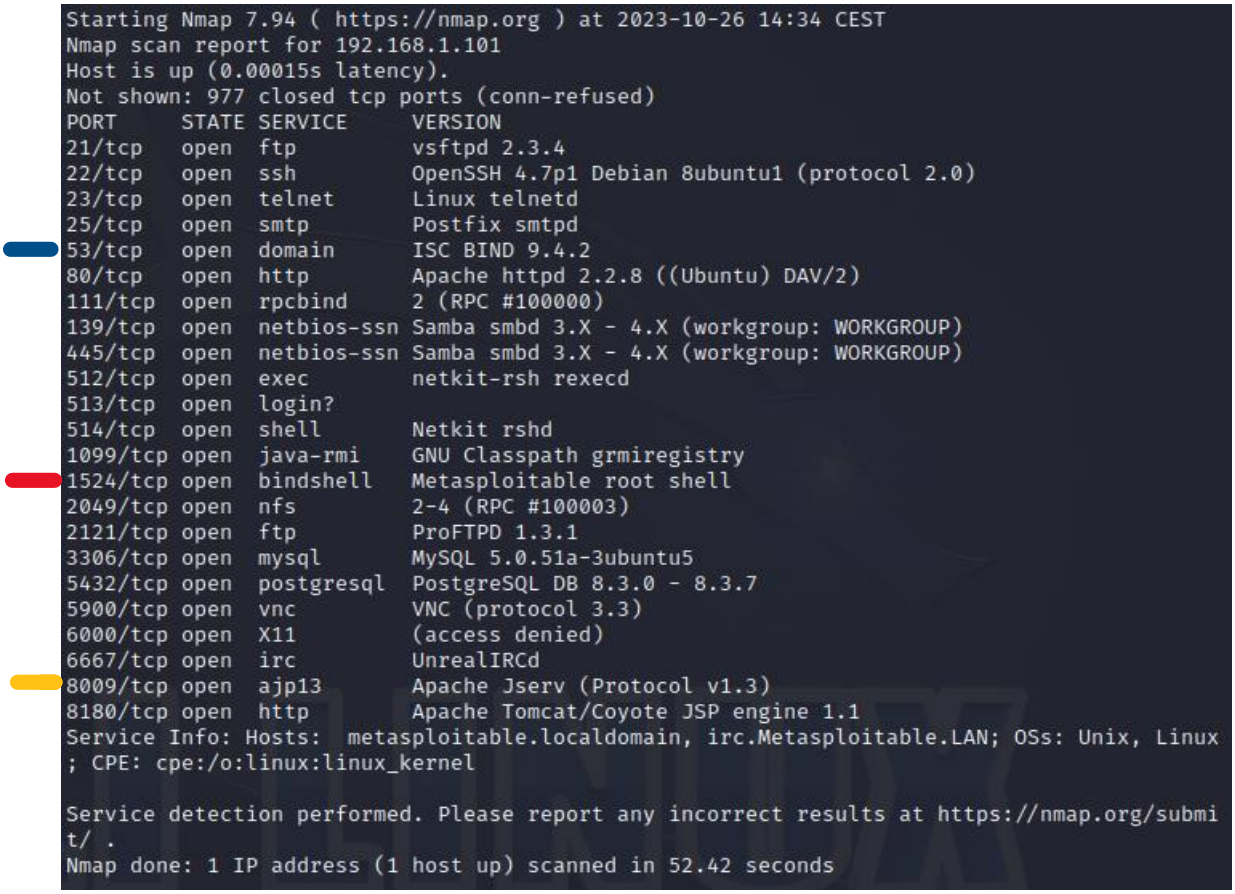
Vulnerabilità e loro possibili soluzioni

AJP Connector

La prima vulnerabilità riguarda il protocollo **Apache Tomcat AJP Connector**, il quale si occupa di facilitare e "alleggerire" dal lato macchina la comunicazione tra un web server ed un application server, anche se questi hanno protocolli diversi, come ad esempio uno HTTP e l'altro Java. In particolare, un attaccante potrebbe usare questa vulnerabilità per iniettare codice malevolo sul server e lanciarlo. In questo caso, possiamo risolvere il problema aggiornando la configurazione ad una versione più recente, in quanto la vulnerabilità nota era presente su versioni più vecchie. La porta di riferimento su cui Nessus ha trovato il problema è evidenziata in giallo nell'immagine successiva (porta 8009).

Bind shell backdoor

Nessus ci informa della presenza di uno **shell** in ascolto su una porta del nostro sistema, specificando che tale shell non necessita di credenziali per essere lanciato. Effettuando una scansione con Nmap, notiamo che in particolare la porta interessata è la 1524 (evidenziata in rosso).



```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-26 14:34 CEST
Nmap scan report for 192.168.1.101
Host is up (0.00015s latency).
Not shown: 977 closed tcp ports (conn-refused)
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
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/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 52.42 seconds
```

Questo potrebbe permettere ad un attaccante di entrare facilmente nella nostra macchina e inviarle istruzioni. Come soluzione, dobbiamo prima di tutto assicurarci che il nostro host non sia già compromesso, nel caso reinstallando il sistema, e successivamente implementare un sistema di credenziali per bloccarne l'accesso o addirittura chiudere la porta interessata.

SSL versioni 2.0 e 3.0

Nessus ha rilevato che la macchina accetta comunicazioni utilizzanti i protocolli di criptazione **SSL versione 2 e 3**. Tali protocolli hanno vulnerabilità note per cui un attaccante potrebbe decriptare i pacchetti e usare attacchi MITM e, per questo, non sono più considerati standard nella comunicazione criptata. Come soluzione, si consiglia di passare al protocollo di criptazione **TLS 1.2** o versioni successive.

Assegnazione porte DNS

Nessus ha riscontrato che quando la macchina effettua **richieste DNS** a server di terze parti non usa porte randomiche. Un attaccante potrebbe sfruttare questa vulnerabilità per divergere il traffico verso siti scelti da lui. Abbiamo evidenziato in blu la porta interessata, ossia la 53. Come soluzione, sarebbe necessario contattare il proprio provider DNS per chiedere una correzione.