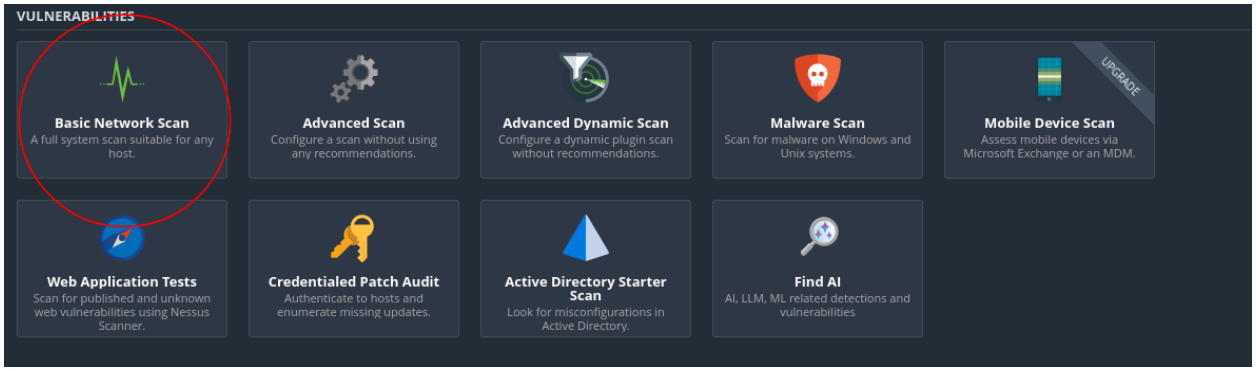
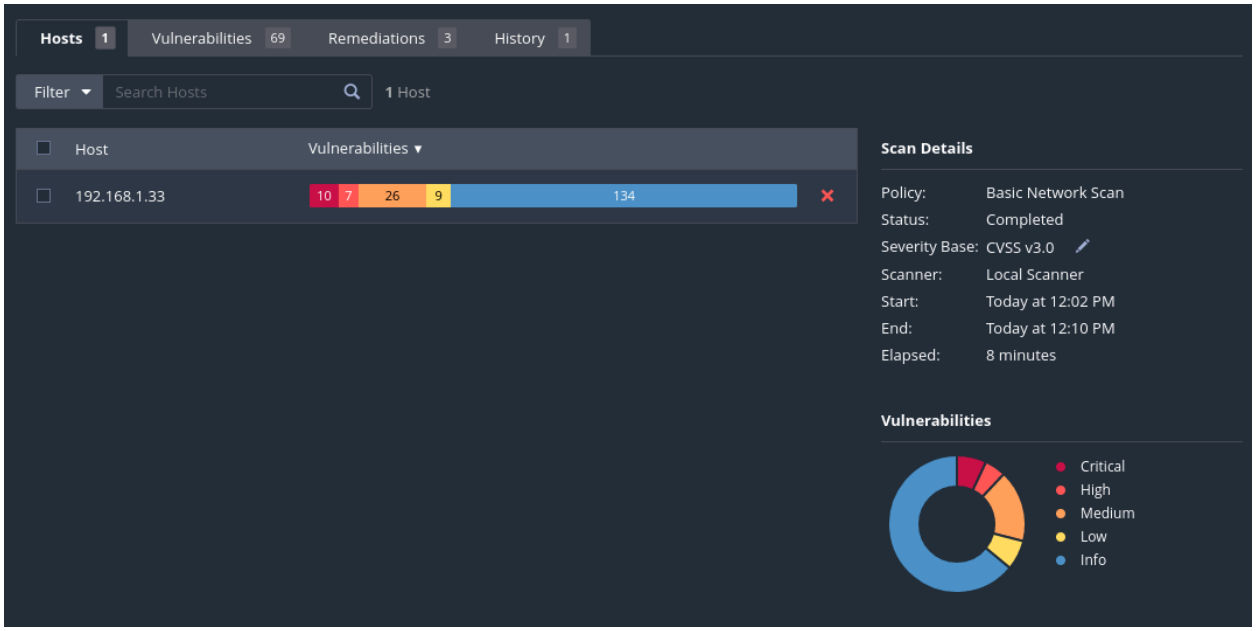
S5 - L3 NESSUS

Come ben sappiamo **Nessus** è un *Vulnerability Scanner*, ovvero è un software che ci permette di poter scansionare gli indirizzi IP di una rete fornendoci dei report esaustivi sulle vulnerabilità presenti.

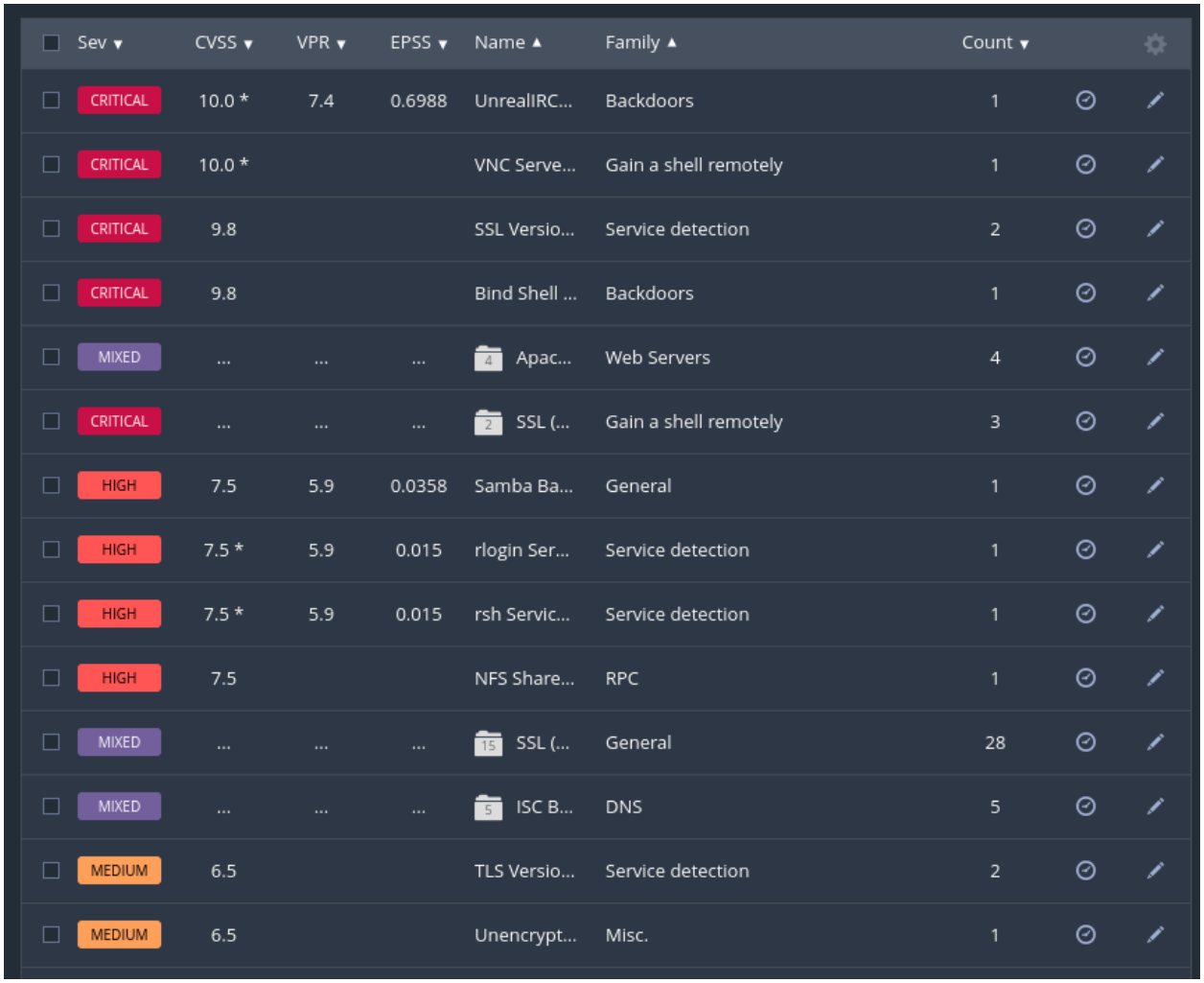
In questo specifico caso ho effettuato una scansione di tutte le porte note sulla macchina target **Metasploitable** che ha il seguente indirizzo IP: **192.168.1.33,** utilizzando il Template di Scansione Base.



Nel risultato seguente possiamo vedere come Nessus ci riporta le vulnerabilità trovatee le divide per Criticità, rispettivamente: Rosso (Critical), Rosso Chiaro (High), Arancione (Medium), Giallo (Low), Azzurro (Info).



Entrando nel dettaglio vediamo per ogni singola vulnerabilità trovata una serie di informazioni utili a capire il tipo di falla e come risolverla.



Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *	7.4	0.6988	UnrealIRC...	Backdoors	1
CRITICAL	10.0 *			VNC Serve...	Gain a shell remotely	1
CRITICAL	9.8			SSL Versio...	Service detection	2
CRITICAL	9.8			Bind Shell ...	Backdoors	1
MIXED	...	...	...	4 Apac...	Web Servers	4
CRITICAL	...	...	...	2 SSL (...	Gain a shell remotely	3
HIGH	7.5	5.9	0.0358	Samba Ba...	General	1
HIGH	7.5 *	5.9	0.015	rlogin Ser...	Service detection	1
HIGH	7.5 *	5.9	0.015	rsh Servic...	Service detection	1
HIGH	7.5			NFS Share...	RPC	1
MIXED	...	...	...	15 SSL (...	General	28
MIXED	...	...	...	5 ISC B...	DNS	5
MEDIUM	6.5			TLS Versio...	Service detection	2
MEDIUM	6.5			Unencrypt...	Misc.	1

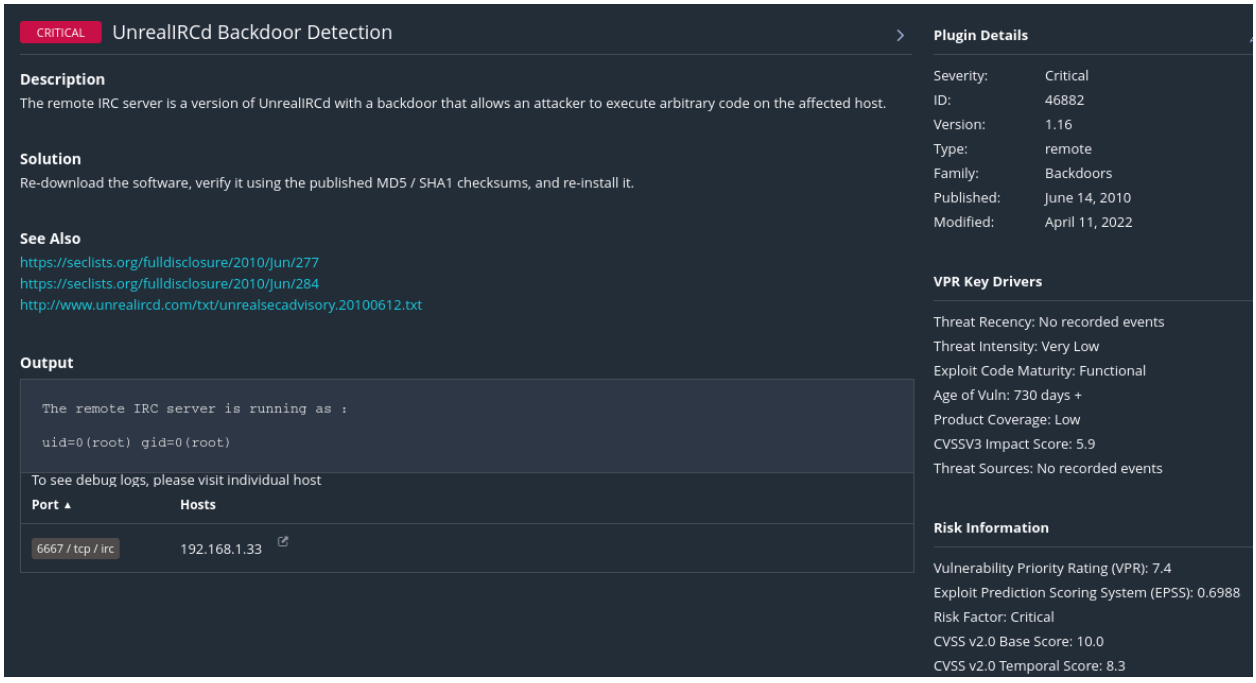
Mi concentro per ovvi motivi sulle vulnerabilità critiche.

Nella schermata seguente vediamo il dettaglio di una delle vulnerabilità critiche trovate.

- **Description**: in questa sezione Nessus ci descrive il tipo di vulnerabilità, in questo caso abbiamo una vulnerabilità sul servizio IRC.
- **Solution**: Nessus ci da una soluzione per risolvere il problema, qui possiamo semplicemente riscaricare il software, verificare che utilizzi MD5/SHA1 e reinstallarlo.

Inoltre ci mette a disposizione dei **Link** che riportano in maniera più dettagliata il tipo di vulnerabilità e servono come approfondimento per avere piena coscienza di cosa stiamo "vedendo".

Nell'**output** invece come si può notare abbiamo l'host e la porta su cui è stata trovata la vulnerabilità.



Una volta che ho effettuato la scansione Nessus ci permette di estrapolare diversi tipi di report ho scelto il report “breve” che riporta semplicemente una lista di tutte le vulnerabilità in ordine di criticità per gli host scansionati e il report “dettagliato” che ci riporta i dettagli, come abbiamo visto sopra, di tutte le vulnerabilità trovate per l’host scansionato, di seguito uno screenshot di entrambi.

- REPORT DETTAGLIATO

171340 - Apache Tomcat SEoL (<= 5.5.x)

Synopsis

An unsupported version of Apache Tomcat is installed on the remote host.

Description

According to its version, Apache Tomcat is less than or equal to 5.5.x. It is, therefore, no longer maintained by its vendor or provider.

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

See Also

https://tomcat.apache.org/tomcat-55-eol.html

Solution

Upgrade to a version of Apache Tomcat that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information

Published: 2023/02/10, Modified: 2024/05/06

Plugin Output

tcp/8180/www

```
URL                                : http://192.168.1.33:8180/
Installed version                  : 5.5
Security End of Life               : September 30, 2012
Time since Security End of Life (Est.) : >= 12 years
```

- REPORT “BREVE”

192.168.1.33

8	6	20	8	77
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 119

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	0.9728	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	-	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0*	5.1	0.1175	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.1175	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	7.4	0.6988	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	0.0164	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	-	42256	NFS Shares World Readable
HIGH	7.5	5.1	0.0053	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	0.0358	90509	Samba Badlock Vulnerability
HIGH	7.5*	5.9	0.015	10205	rlogin Service Detection
HIGH	7.5*	5.9	0.015	10245	rsh Service Detection

CONCLUSIONI

Come si può notare dal report tra le vulnerabilità di livello critico abbiamo:

- Apache Tomcat AJP
- Bind Shell Backdoor
- SSL v2 e v3
- Debian OpenSSH/OpenSSL
- UnrealIRCd Backdoor
- VNC Server

In allegato il report dettagliato di queste vulnerabilità.

Analizzato questo siamo in grado ora di capire quali sono le vulnerabilità trovate, come poterle risolvere e soprattutto avere un quadro ben chiaro di quelle che sono le falle riscontrate nella rete.

Nessus inoltre, come citato prima, ci fornisce per ogni vulnerabilità ulteriori fonti di approfondimento è ovviamente buona pratica approfondirle.