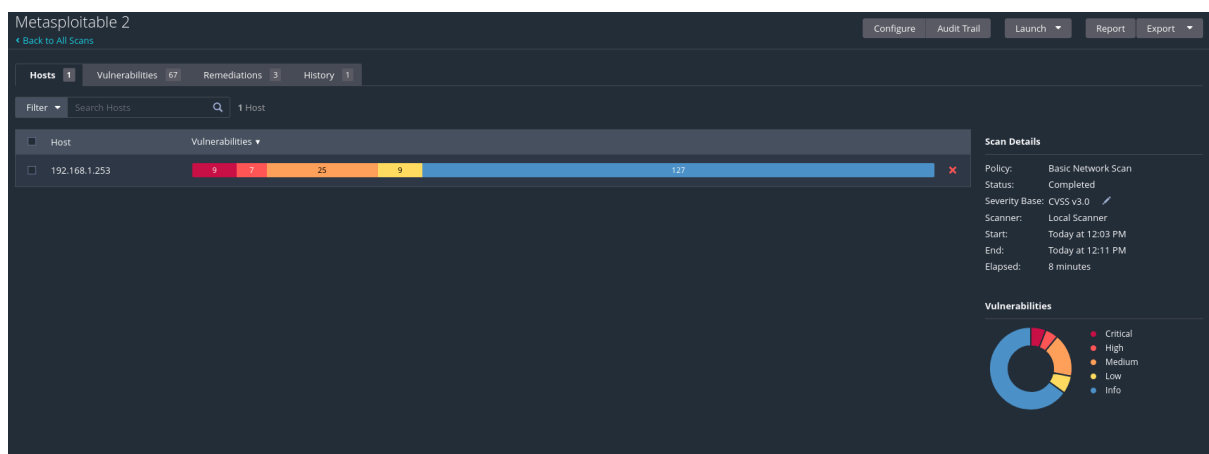


NESSUS

L'azienda mi ha chiesto di scansionare la sua macchina per verificare le vulnerabilità presenti su di essa.

Per farlo ho utilizzato il programma Nessus, installato precedentemente su Kali Linux.



Nessus è uno strumento essenziale per la sicurezza informatica, utile per aziende e professionisti che desiderano proteggere i propri sistemi e dati da minacce e attacchi. La sua capacità di identificare e segnalare vulnerabilità consente di adottare misure preventive efficaci.

Funziona:

1. Manda un pacchetto TCP (syn syn-ack ack)
2. Guarda i sistemi operativi, Password, scansione porte, versione dei protocolli
3. Guarda che applicazioni utilizza la macchina
4. Guarda i registri e gli aggiornamenti installati
5. Controlla nel suo database e mette a confronto le informazioni con le versioni in una tabella
6. Utilizzando la informazioni prova ad attaccare la macchina (Es Attacco al database) utilizzando Exploit
7. Fornisce un report con le vulnerabilità

VULNERABILITA' ANALIZZATE

Filter	Search Vulnerabilities		67 Vulnerabilities				
Sev	CVSS	VPR	EPSS	Name	Family	Count	
<div>CRITICAL</div>	10.0 *	7.4	0.6988	UnrealIRCd Backdoor Detection	Backdoors	1	<div></div> <div></div>
<div>CRITICAL</div>	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1	<div></div> <div></div>
<div>CRITICAL</div>	9.8	9.0	0.9728	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	<div></div> <div></div>
<div>CRITICAL</div>	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2	<div></div> <div></div>
<div>CRITICAL</div>	9.8			Bind Shell Backdoor Detection	Backdoors	1	<div></div> <div></div>
<div>CRITICAL</div>	<div></div> SSL (Multiple Issues)	Gain a shell remotely	3	<div></div> <div></div>
<div>HIGH</div>	7.5	5.9	0.0358	Samba Badlock Vulnerability	General	1	<div></div> <div></div>
<div>HIGH</div>	7.5 *	5.9	0.015	rlogin Service Detection	Service detection	1	<div></div> <div></div>
<div>HIGH</div>	7.5 *	5.9	0.015	rsh Service Detection	Service detection	1	<div></div> <div></div>
<div>HIGH</div>	7.5			NFS Shares World Readable	RPC	1	<div></div> <div></div>
<div>MIXED</div>	<div></div> SSL (Multiple Issues)	General	28	<div></div> <div></div>
<div>MIXED</div>	<div></div> ISC Bind (Multiple Issues)	DNS	5	<div></div> <div></div>
<div>MEDIUM</div>	6.5			TLS Version 1.0 Protocol Detection	Service detection	2	<div></div> <div></div>

Finita la scansione Nessus ci fornirà di un elenco di vulnerabilità in una scala da 0 a 10 (10 vulnerabilità critica e 1 vulnerabilità bassa).

Punteggio	Livello di Criticità	Descrizione
0 - 3.9	Basso	Vulnerabilità di basso rischio e impatto limitato.
4.0 - 6.9	Medio	Rischio moderato con possibilità di sfruttamento.
7.0 - 8.9	Alto	Vulnerabilità serie con impatto significativo.
9.0 - 10.0	Critico	Vulnerabilità estremamente gravi e facili da sfruttare.

Per ogni vulnerabilità Nessus ti trova una soluzione ed i possibili exploit che vengono utilizzati per attaccare questo protocollo

Analizziamo la prima vulnerabilità della scansione:

Vulnerabilities
67

CRITICAL
UnrealIRCd Backdoor Detection

Description
The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution
Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

See Also
<https://seclists.org/fulldisclosure/2010/Jun/277>
<https://seclists.org/fulldisclosure/2010/Jun/284>
<http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt>

Output

```
The remote IRC server is running as :
uid=0(root) gid=0(root)
```

To see debug logs, please visit individual host

Port ▲	Hosts
6667 / tcp / irc	192.168.1.253

Spiegazione del Backdoor in UnrealIRCd

UnrealIRCd è un software di server IRC (Internet Relay Chat) molto diffuso. Tuttavia, una vulnerabilità è stata scoperta in alcune versioni di questo software, che include un backdoor

L'attaccante può sfruttare la backdoor per “rubare o manipolare” le informazioni della macchina

Questa è la seconda ed ultima analisi

Vulnerabilities 67

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".
```

To see debug logs, please visit individual host

Port ▲	Hosts
5900 / tcp / vnc	192.168.1.253 

Spiegazione VNC Server Password (Password)

In questa vulnerabilità la password del server VNC è molto debole un attaccante potrebbe sfruttare questa debolezza per entrare nella macchina e prenderne il controllo

Il restante delle vulnerabilità sarà sul secondo file, da me caricato che mostra un report molto più dettagliato