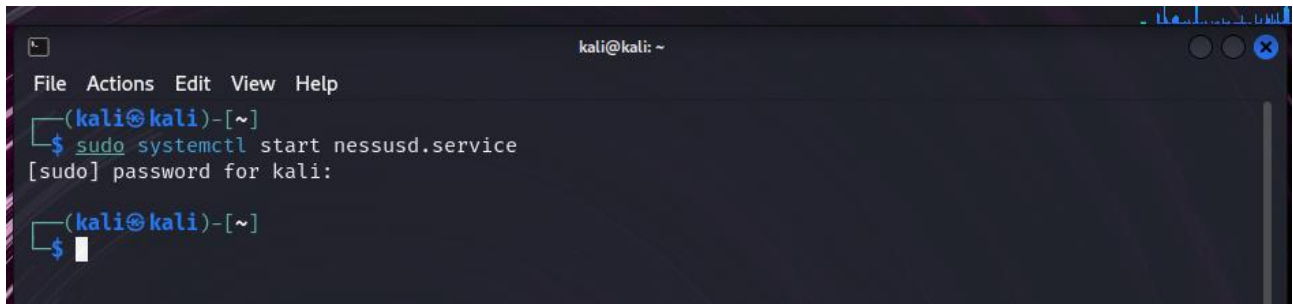


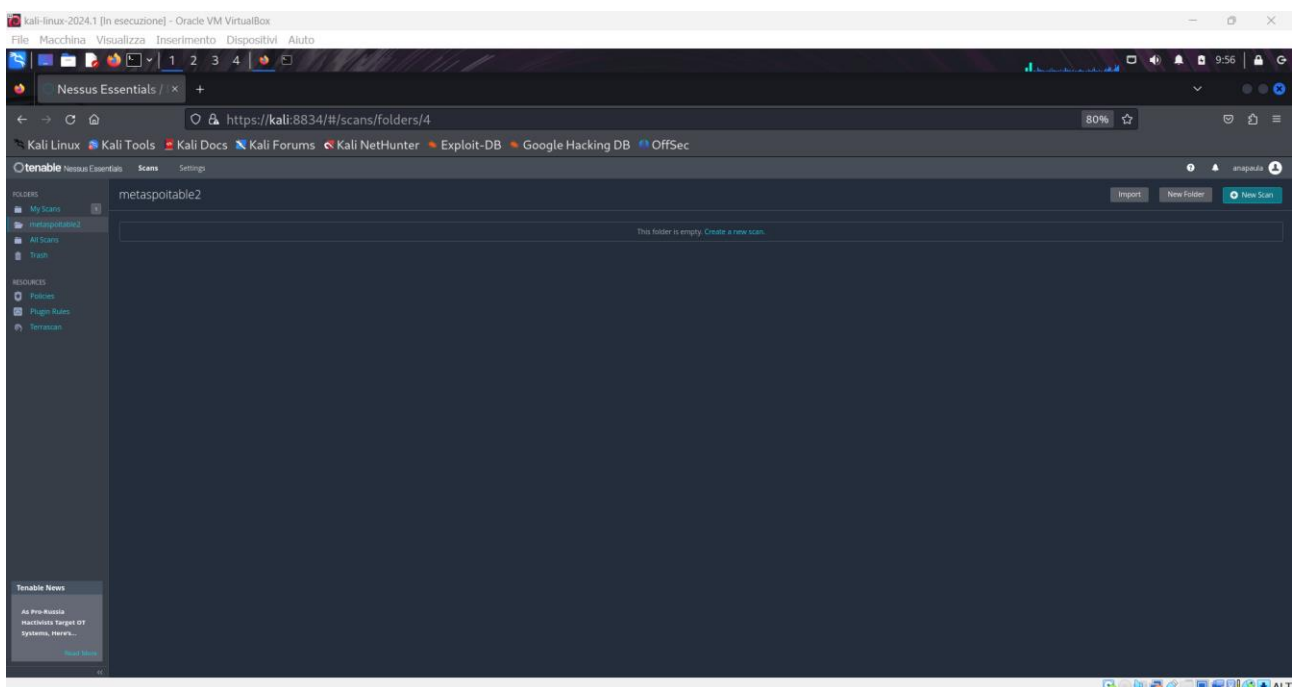
S5-L4 Traccia: Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni (potete scegliere come scansione il «basic network scan», o l’advanced e poi configurarlo).

(dopo l’installazione) Prima d’iniziare dobbiamo avviare Nessus dalla terminale di kali

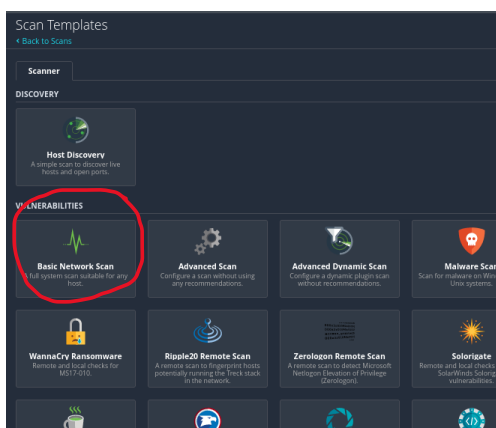


```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo systemctl start nessusd.service  
[sudo] password for kali:  
(kali@kali)-[~]  
$
```

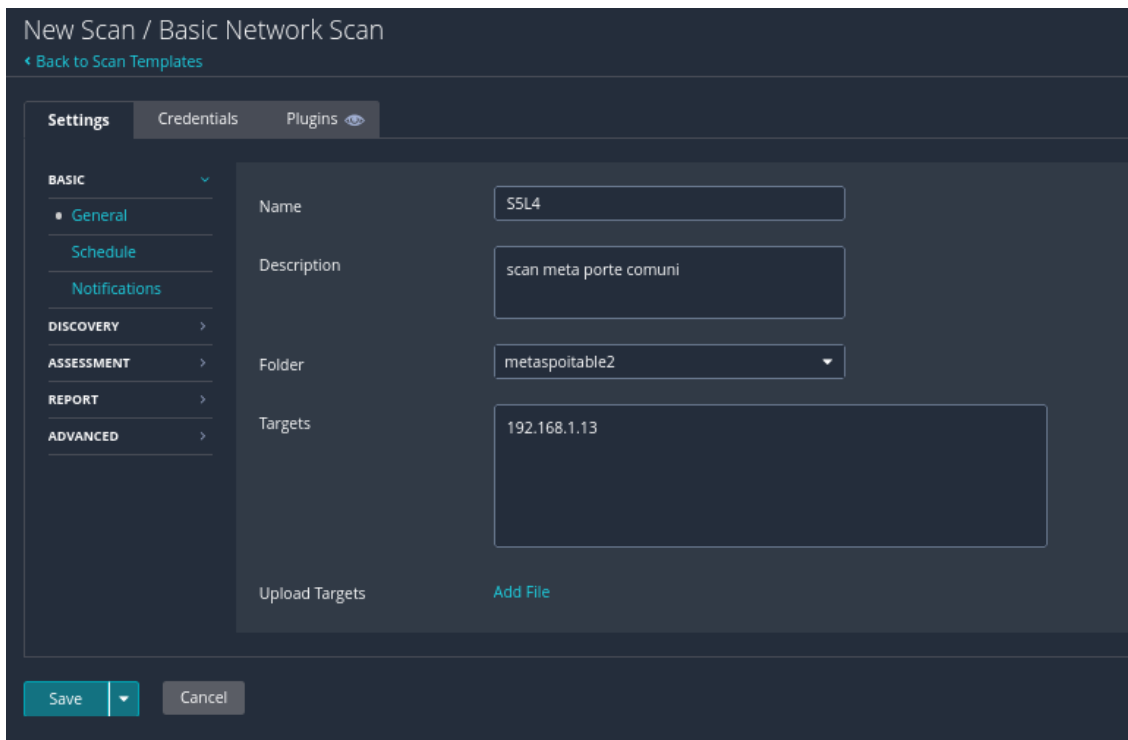
Dopo possiamo andare al browser e collegarci a <https://kali:8834> inseriamo le credenziali



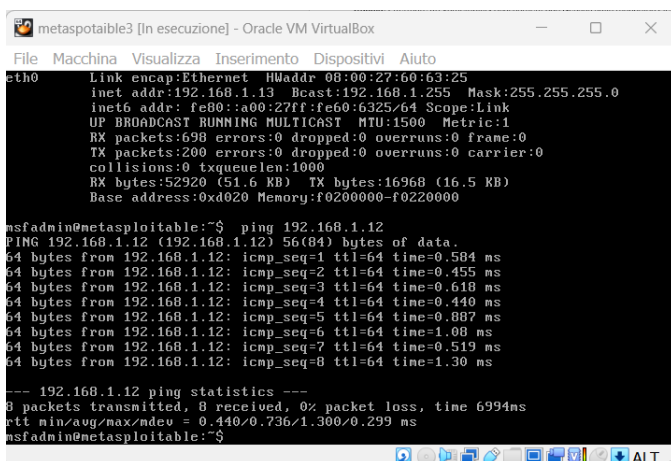
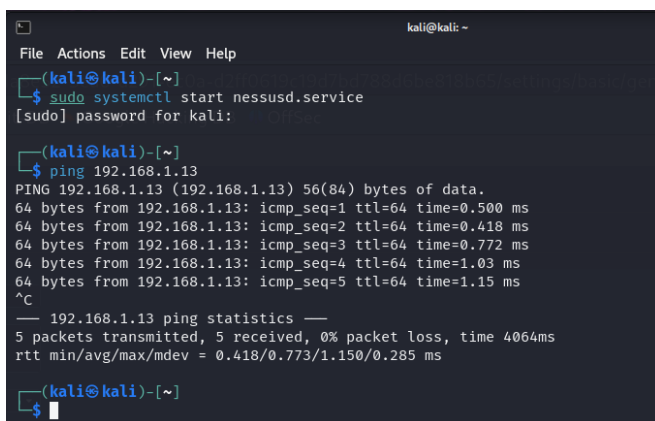
Una volta dentro dobbiamo effettuare un VA sulla macchina Metasploitable indicando solo le porte comuni (**common ports**) in questo caso sceglierò la scansione “basic network scan”



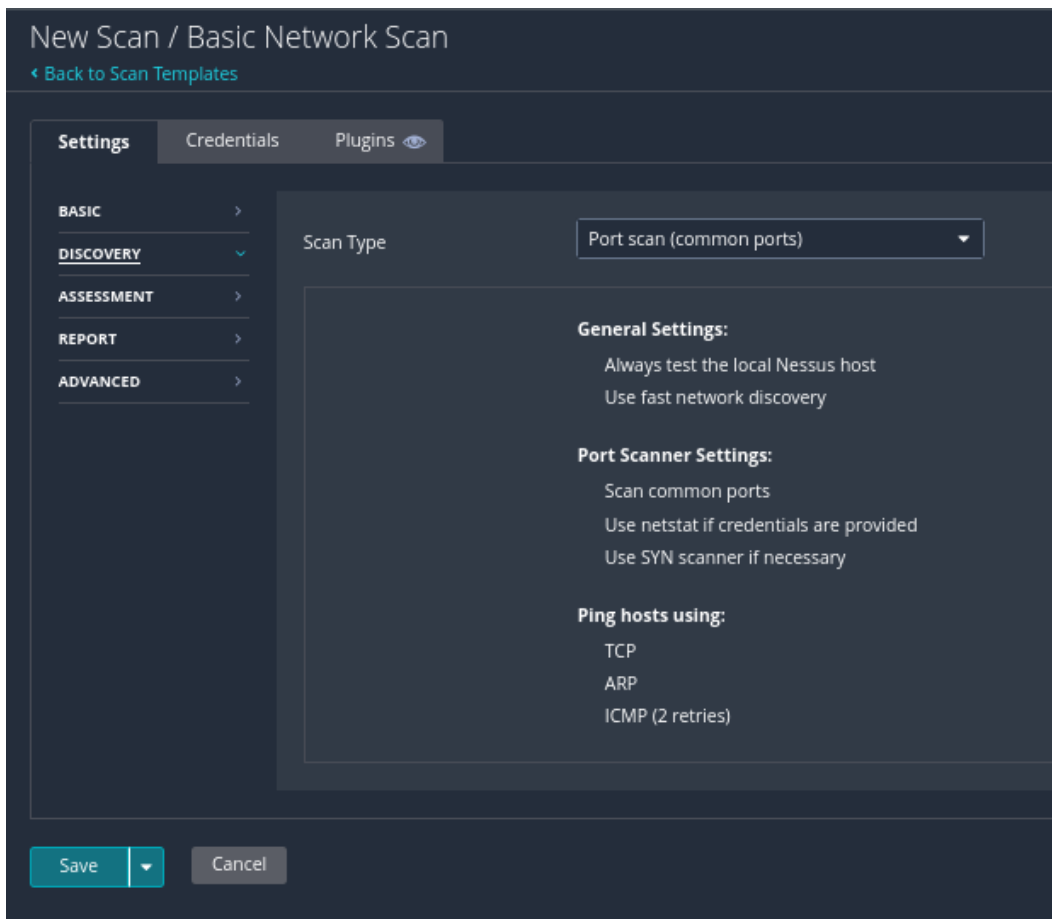
Iniziamo a configurare Nessus



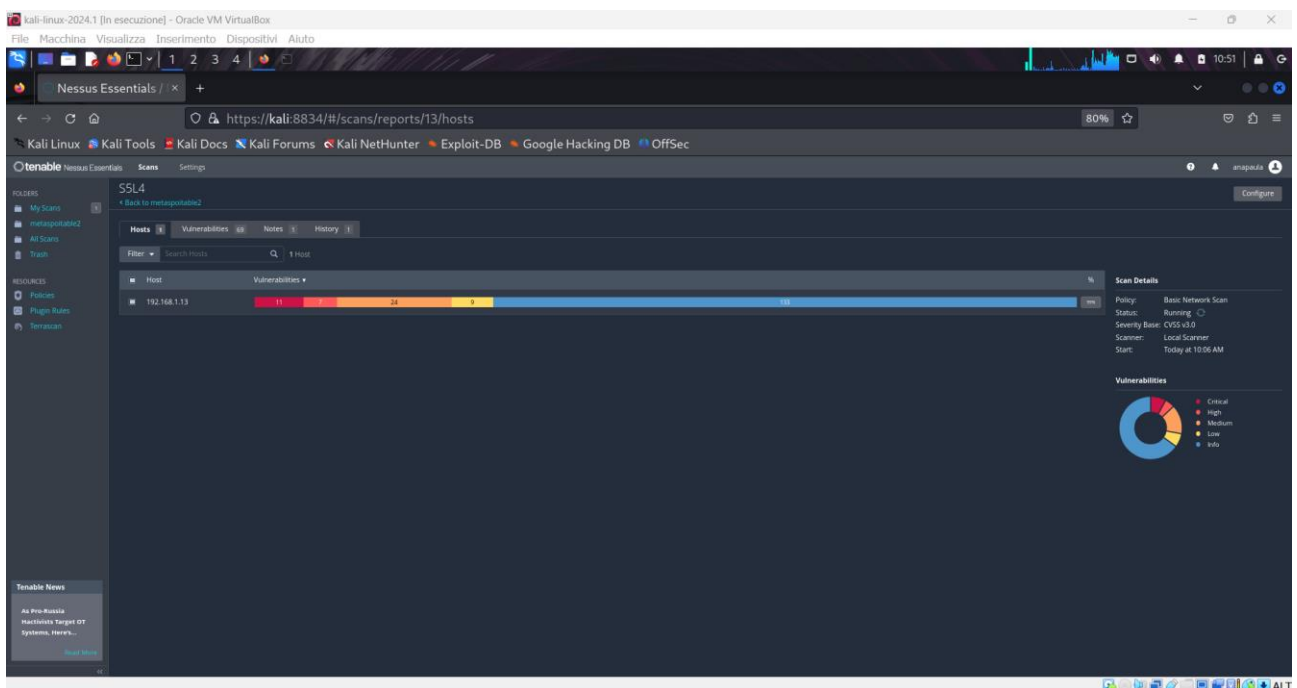
Nel target inseriamo l'ip della macchina Metasploitable (dobbiamo assicurarci che kali e Meta abbiano comunicazione tra di loro)



Nella parte Discovery mettiamo come opzione “Common ports” (richiesto dalla traccia)



Dopo di che salviamo e possiamo premere Launch per iniziare la scansione.



kali-linux-2024.1 [in esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Nessus Essentials / x

https://kali:8834/#scans/reports/13/vulnerabilities 80%

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

tenable Nessus Essentials Scans Settings

ROLES My Scans metaspotable2 All Scans Trash

RESOURCES Policies Plugin Rules TenableScan

Tenable News

SSL4

Back to metaspotable2

Configure Audit Trail Launch Report Export

Hosts Vulnerabilities Remediations Notes History

Filter Search Vulnerabilities 70 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
<input type="checkbox"/> CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1	✓
<input type="checkbox"/> CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	✓
<input type="checkbox"/> CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1	✓
<input type="checkbox"/> CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	✓
<input type="checkbox"/> CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1	✓
<input type="checkbox"/> MEDIUM	Apache Tomcat (Multiple Issues)	Web Servers	4	✓
<input type="checkbox"/> CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	✓
<input type="checkbox"/> MEDIUM	7.5 *	5.9	rhttp Service Detection	Service detection	1	✓
<input type="checkbox"/> MEDIUM	7.5 *	5.9	rsh Service Detection	Service detection	1	✓
<input type="checkbox"/> MEDIUM	7.5	5.9	Samba Badlock Vulnerability	General	1	✓
<input type="checkbox"/> MEDIUM	7.5		NFS Shares World Readable	RPC	1	✓
<input type="checkbox"/> MEDIUM	SSL (Multiple Issues)	General	28	✓
<input type="checkbox"/> MEDIUM	ISC Bind (Multiple Issues)	DNS	5	✓
<input type="checkbox"/> MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2	✓
<input type="checkbox"/> MEDIUM	6.5		Unencrypted Telnet Server	Misc.	1	✓
<input type="checkbox"/> MEDIUM	5.9	4.4	SSL Anonymous Exported Session Transactions	Service detection	1	✓

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:56 AM
End: Today at 10:51 AM
Elapsed: an hour

Vulnerabilities

Legend: Critical, High, Medium, Low, Info

E queste sono le vulnerabilità trovate sulla macchina Metaspotable che è intenzionalmente vulnerabile usata per esercitarsi nella cybersecurity.