Indice

Traccia dell'esercizio principale

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)

A valle del completamento della scansione**, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web.**

Gli obiettivi dell'esercizio sono:

- **Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni**
- **Familiarizzare con alcune delle vulnerabilità note che troverete spesso sul vostro percorso da penetration tester**

Consegna

- Report PDF per «tecnico»

Report tecnico è inteso come "quasi completo" che va ad indicare sia le porte che la vulnerabilità che la risoluzione, in modo da poter intervenire.

- Suggerimento: fare traduzione in italiano della descrizione e/o remediation

Traccia dell'esercizio facoltativo

- Analisi/studio delle vulnerabilità (PDF) - servirà sia per exploit che remediation
- Report PDF per «dirigente»: Inteso come riassunto che va presentato ai dirigenti per l'approvazione a livello finanziario ecc. Non contiene troppi dettagli tecnici ma soltanto l'indicazione della vulnerabilità e soprattutto i grafici con la pericolosità delle varie vulnerabilità riscontrate

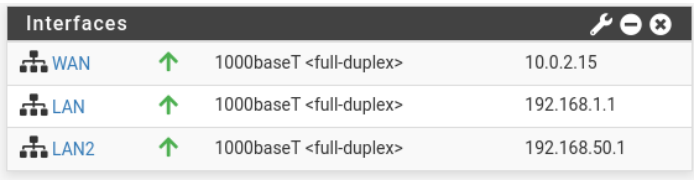
Configurazione laboratorio virtuale

La configurazione è impostata seguendo la logica del report M3 W9 D5

pfSense come Server DHCP

Kali Linux su rete 192.168.1.0/24

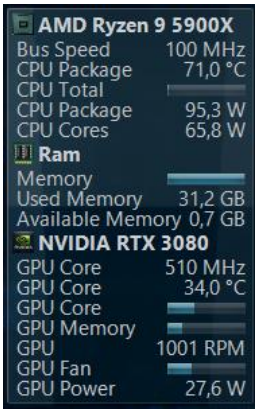
Tutte le altre macchine su rete 192.168.50.0/24



Per questo esercizio è stato utilizzato un hardware abbastanza potente, tenendo attivo numerose macchine virtuali, di seguito la lista delle macchine con indirizzo IP assegnato da pfSense:

Metasploitable2 192.168.50.103; Windows 7 192.168.50.104; Windows Vista 192.168.50.105; Linux Mint 192.168.50.106; Ubuntu 192.168.50.107; Windows 10 (versione con vulnerabilità) 192.168.50.108; Parrot OS 192.168.50.109

Infatti dalle analisi si nota il consumo quasi totale della Ram da 32 gb.



Installazione di Tenable Nessus

Download e installazione

Per l'installazione di Tenable Nessus, dalla macchina Kali Linux recarsi sul sito ufficiale https://www.tenable.com/downloads/nessus?loginAttempted=true e scaricare la versione per Linux Debian amd64

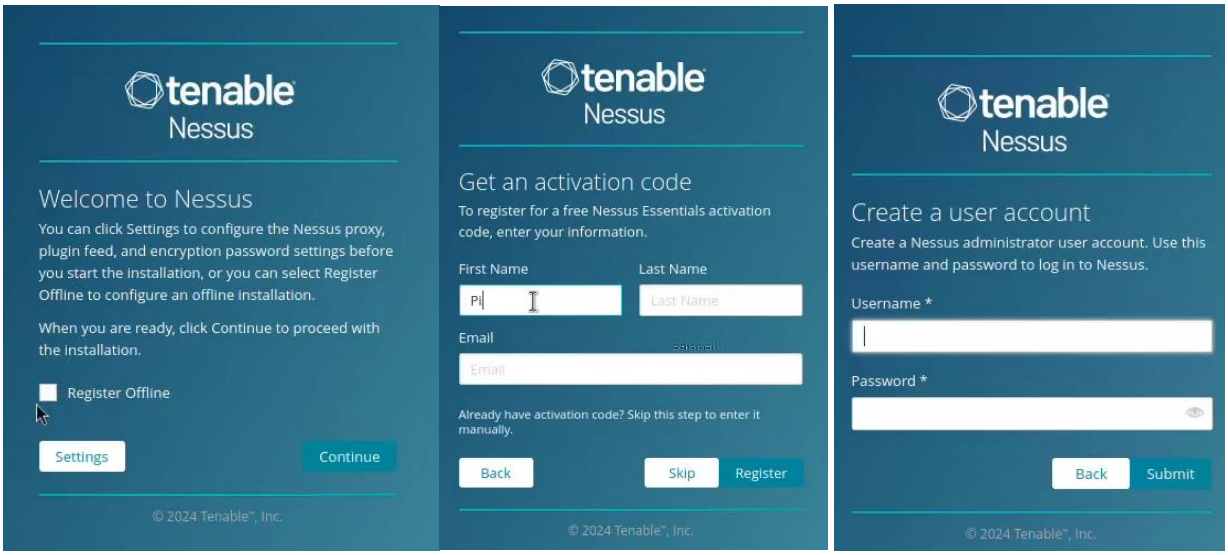
Finito il download, aprire il terminale shell nella stessa cartella del file scaricato e lanciare il comando

sudo dpkg -i <nome_file.deb>

Avvio del servizio e primo avvio di Nessus

Per avviare il servizio digitare il comando **sudo systemctl start nessusd**
Nel caso servisse chiuderlo, il comando è **sudo systemctl stop nessusd**

Dopo aver avviato il servizio aprire sul browser il link di configurazione:
https://localhost:8834/ oppure https://kali:8834/ oppure https://127.0.0.1:8834/



Non selezionare la registrazione offline, ma continua, creando un account lasciando un indirizzo email valido per ricevere il codice di attivazione e creare username e password.

Successivamente effettuare l'accesso e su richiesta inserire il codice di attivazione ricevuta via email.

Per i futuri accessi:

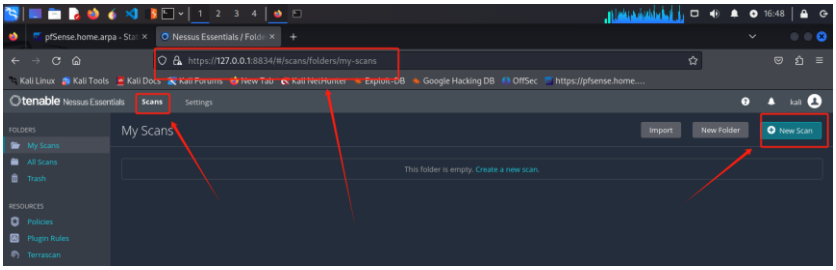
1. Attivare il servizio **sudo systemctl start nessusd**
2. Aprire la pagina di configurazione https://127.0.0.1:8834/
3. Accedere con le credenziali note

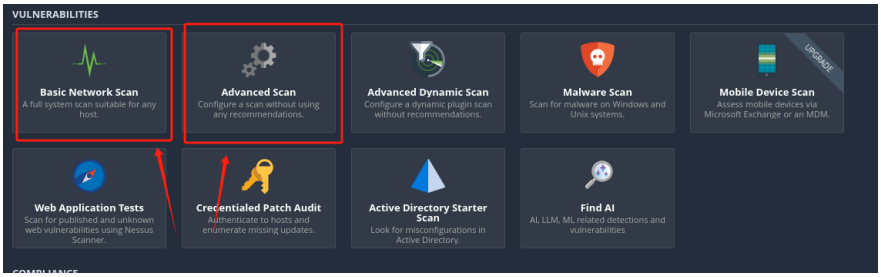
Se ci fossero errori di caricamento dei plugin, aggiornarli con il comando **sudo /opt/nessus/sbin/nessuscli update**

Svolgimento traccia principale

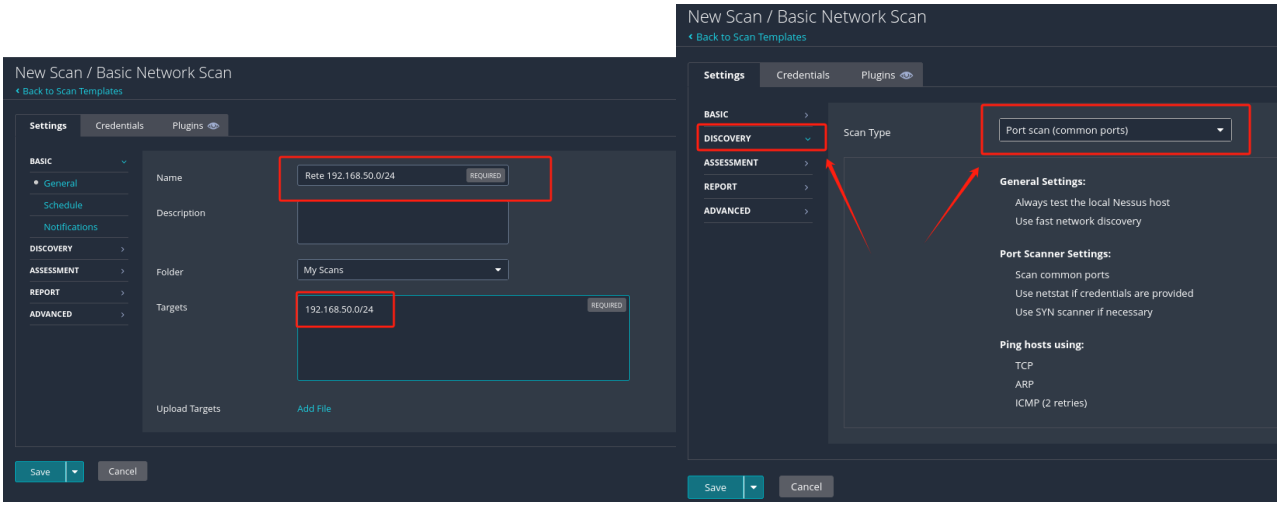
Scansione della rete

L'interfaccia è molto intuitiva, per effettuare una scansione recarsi su **Scans>New Scan**
Ai fini dell'esercizio si possono scegliere la tipologia di scan preferita.





Importante inserire nome della scansione e rete e/o ip target, in questo caso la rete dove si trova Metasploitable2 con indirizzo IP **192.168.50.103** è **192.168.50.0/24**



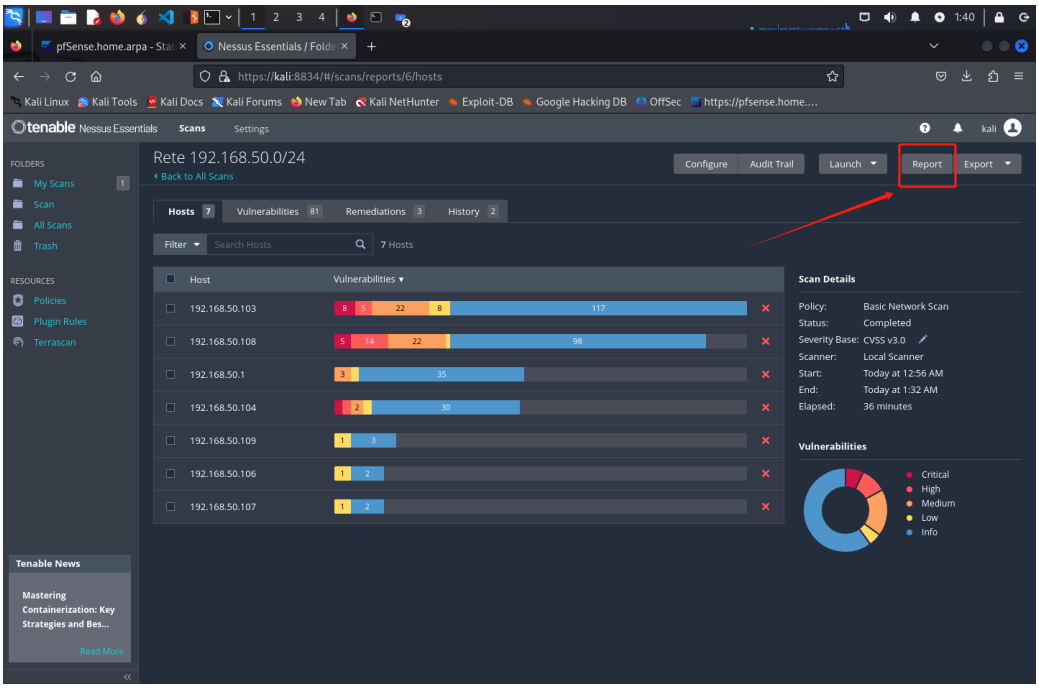
L'esercizio prevede la scansione delle porte comuni **Discovery> Port scan (common ports)**

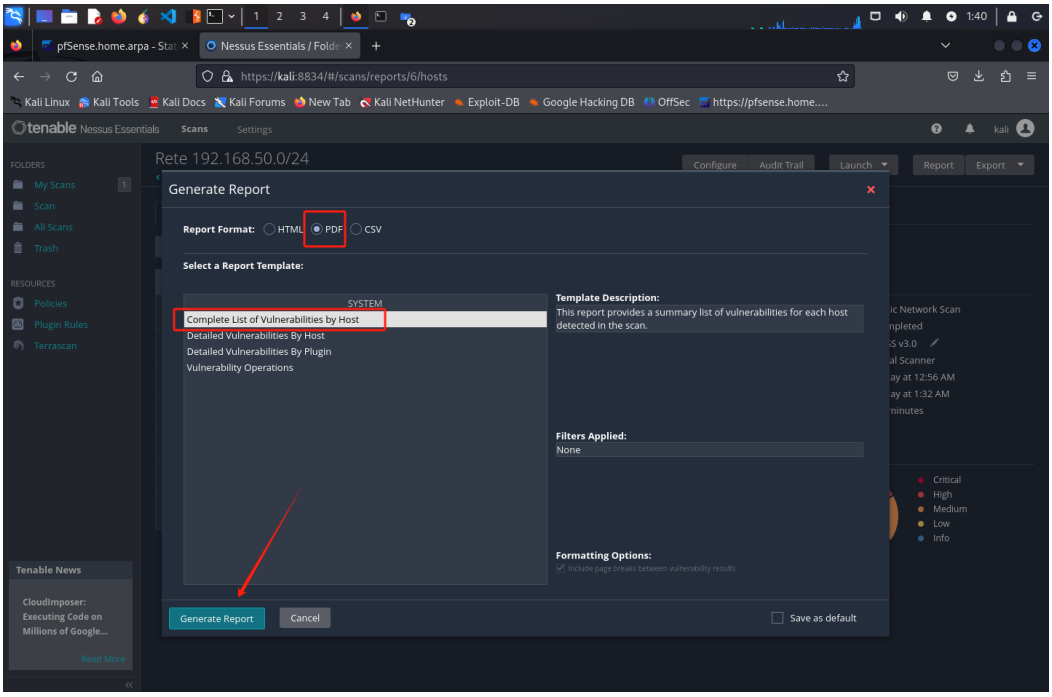
Poi salvare con **Save** e **Launch**

Anche se scansionare l'intera rete, invece di scansionare la singola macchina Metasploitable2, impiega più tempo, tuttavia in compenso si ha una panoramica completa delle macchine di tutta la rete.

Risultati della scansione

Si può esportare il report in formato PDF intuitivamente come da immagini sottostanti.





Il risultato completo della scansione è nel file allegato al presente report "**Rete 192_168_50_0_24.pdf**"

Rete 192_168_50_0_24.pdf che può essere consegnato al tecnico.

Svolgimento esercizio facoltativo

Report di Sicurezza- Host 192.168.50.103 Metasploitable 2

Vulnerabilità Critiche:

1. **Apache Tomcat AJP Connector Injection (Ghostcat)**
   - **Rischio**: Accesso remoto non autorizzato a file e codice.
   - **Azione**: Aggiornare Tomcat, disabilitare AJP se non necessario.
2. **Bind Shell Backdoor Detection**
   - **Rischio**: Accesso remoto completo tramite shell aperta.
   - **Azione**: Rimuovere la backdoor e analizzare compromissioni.
3. **SSL Version 2 e 3 Detection**
   - **Rischio**: Protocolli obsoleti vulnerabili ad attacchi crittografici.
   - **Azione**: Disabilitare SSL v2/v3, abilitare solo TLS 1.2/1.3.
4. **Debian OpenSSH/OpenSSL Weakness**
   - **Rischio**: Chiavi crittografiche prevedibili.
   - **Azione**: Aggiornare OpenSSL/OpenSSH, rigenerare le chiavi.
5. **VNC Server 'password' di Default**
   - **Rischio**: Accesso remoto non autenticato.
   - **Azione**: Cambiare immediatamente la password.

Vulnerabilità Alte:

1. **ISC BIND Service Downgrade/DoS**
   - **Rischio**: Possibilità di attacchi DoS sul servizio DNS.
   - **Azione**: Aggiornare BIND.
2. **NFS Shares World Readable**
   - **Rischio**: Accesso globale ai file condivisi.
   - **Azione**: Limitare accesso NFS solo agli utenti autorizzati.
3. **SSL Medium Strength Cipher Suites (SWEET32)**
   - **Rischio**: Suite crittografiche vulnerabili a decifrazione.
   - **Azione**: Disabilitare le suite deboli.
4. **Samba Badlock Vulnerability**
   - **Rischio**: Attacchi MITM su Samba.
   - **Azione**: Aggiornare Samba.

Raccomandazioni:

- **Aggiornamenti**: Patch immediate per software vulnerabile.
- **Monitoraggio**: Implementare monitoraggio continuo.
- **Hardening**: Rivedere e migliorare le configurazioni di sicurezza.

Intervenire con urgenza sulle criticità evidenziate per ridurre il rischio di compromissioni.

Vulnerabilities — Total: 98

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*	5.1	0.0967	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.0967	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
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

Report per dirigente

Report di Sicurezza: Host 192.168.50.103 (Metasploitable 2)

Vulnerabilità Critiche

Vulnerabilità	Rischio	Azione Raccomandata
Apache Tomcat AJP Connector Injection (Ghostcat)	Accesso remoto non autorizzato a file e codice	Aggiornare Tomcat, disabilitare AJP se non necessario
Bind Shell Backdoor Detection	Accesso remoto completo tramite shell aperta	Rimuovere la backdoor e analizzare compromissioni
SSL Version 2 e 3 Detection	Protocolli obsoleti vulnerabili ad attacchi crittografici	Disabilitare SSL v2/v3, abilitare solo TLS 1.2/1.3
Debian OpenSSH/OpenSSL Weakness	Chiavi crittografiche prevedibili	Aggiornare OpenSSL/OpenSSH, rigenerare le chiavi
VNC Server 'password' di Default	Accesso remoto non autenticato	Cambiare immediatamente la password

Vulnerabilità Alte

Vulnerabilità	Rischio	Azione Raccomandata
ISC BIND Service Downgrade/DoS	Possibilità di attacchi DoS sul servizio DNS	Aggiornare BIND
NFS Shares World Readable	Accesso globale ai file condivisi	Limitare accesso NFS solo agli utenti autorizzati
SSL Medium Strength Cipher Suites (SWEET32)	Suite crittografiche vulnerabili a decifrazione	Disabilitare le suite deboli
Samba Badlock Vulnerability	Attacchi MITM su Samba	Aggiornare Samba

Raccomandazioni Strategiche

- **Aggiornamenti**: Eseguire patch immediate per il software vulnerabile.
- **Monitoraggio**: Implementare un sistema di monitoraggio continuo.
- **Hardening**: Rivedere e migliorare le configurazioni di sicurezza per ridurre il rischio.

Conclusione

È fondamentale intervenire con urgenza sulle vulnerabilità critiche per proteggere l'infrastruttura e ridurre il rischio di compromissioni.