REPORT S5/L3

Vulnerability Scanning

Traccia

Lo studente effettuerà un Vulnerability Scanning sulla macchina Metasploitable utilizzando Nessus, concentrandosi sulle porte comuni. Questo esercizio ha lo scopo di fare pratica con lo strumento Nessus, la configurazione delle scansioni, e di familiarizzare con alcune delle vulnerabilità note.

Svolgimento

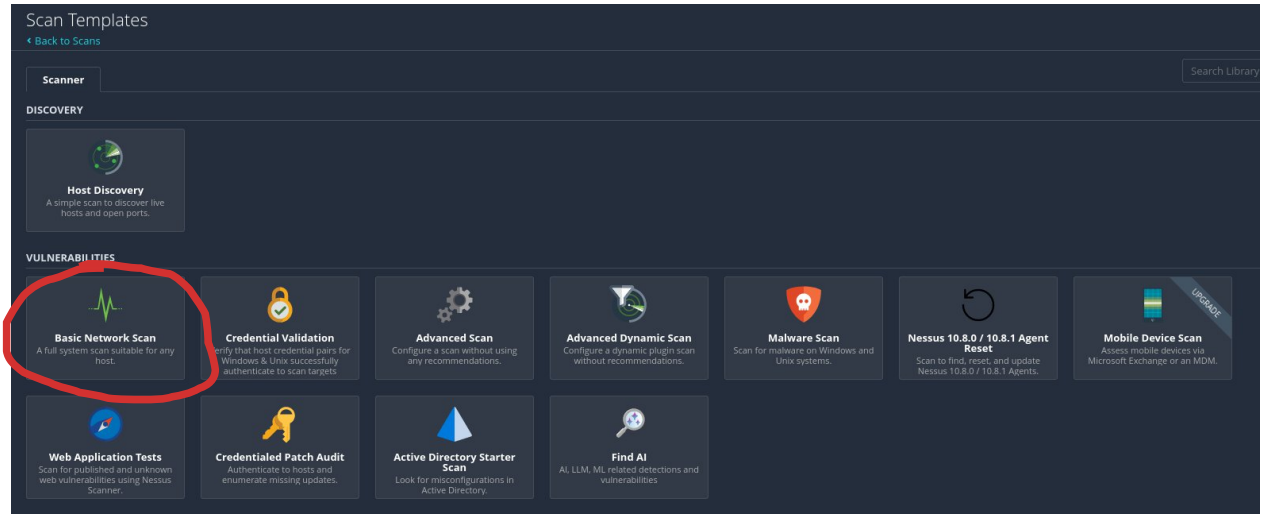
Dopo aver installato Nessus, provvediamo alle impostazioni di rete, facendo in modo che Kali e Metasploitable siano sulla stessa rete.

Per questo asssegniamo gli indirizzi IP:

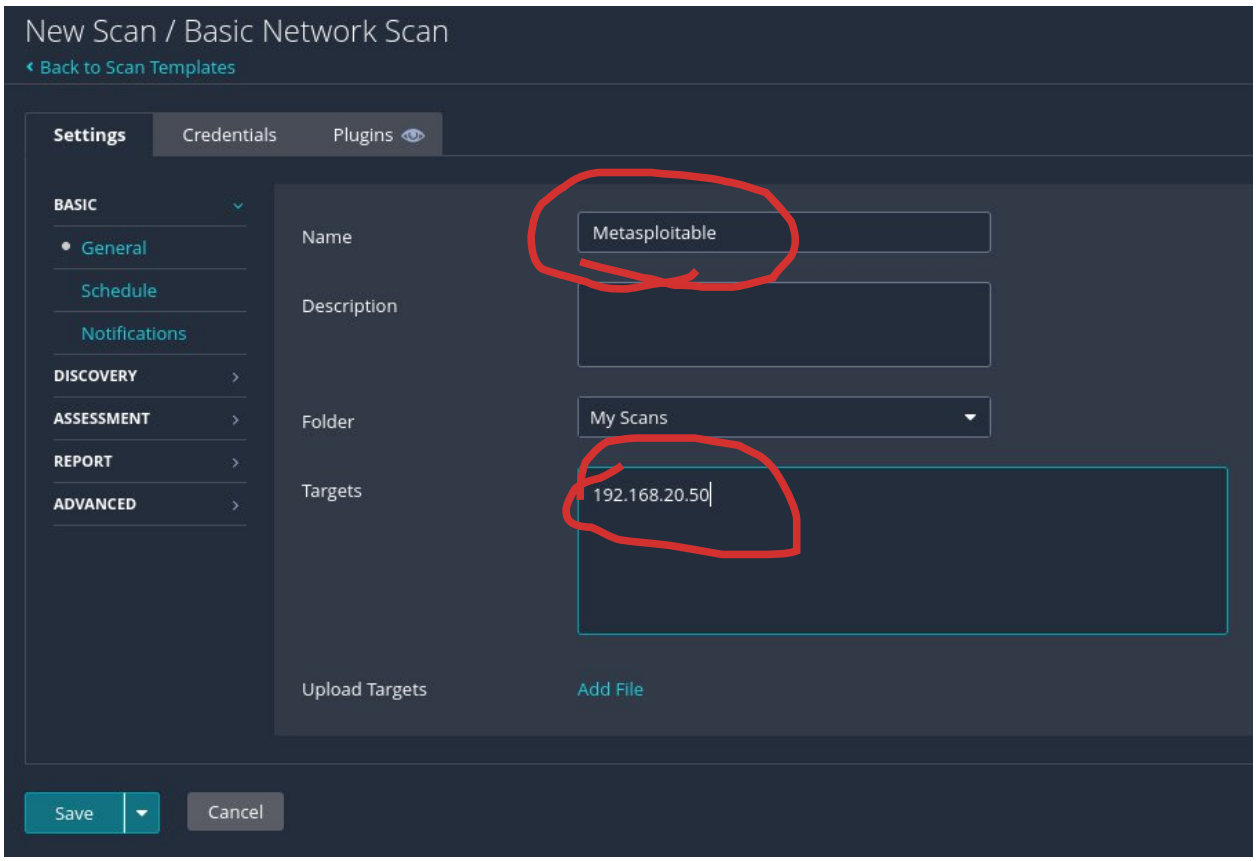
- 192.168.20.30 a Kali
- 192.168.20.50 a Metasploitable

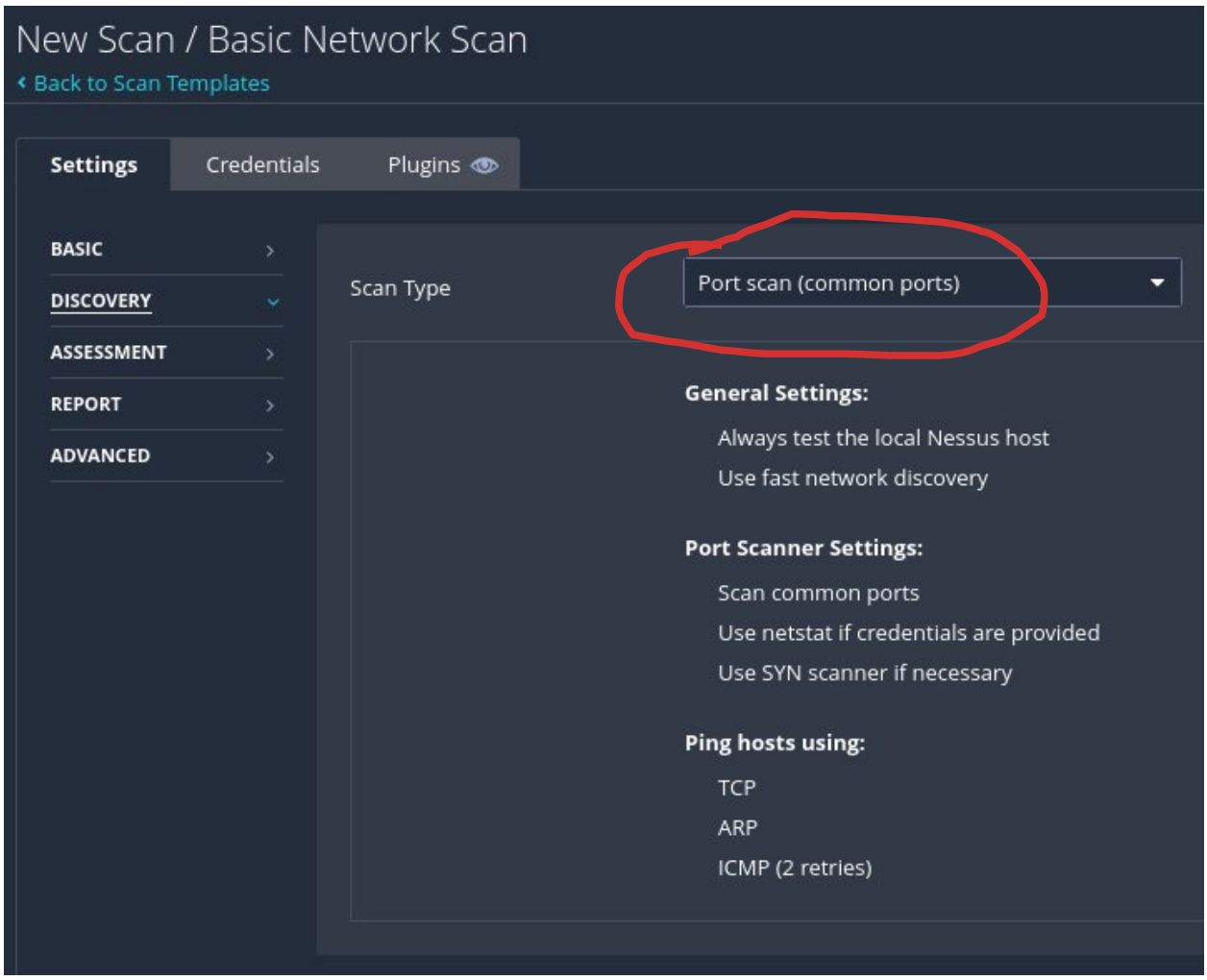
Effettuiamo un ping per controllare che le macchine comunichiano, poi avviamo il demone di Nessus con il comando: *sudo systemctl start nessusd.service*.

Apriamo Nessus tramite browser andando sull'indirizzo *http://kali:8834* e spostiamoci nella scheda *Scans*.

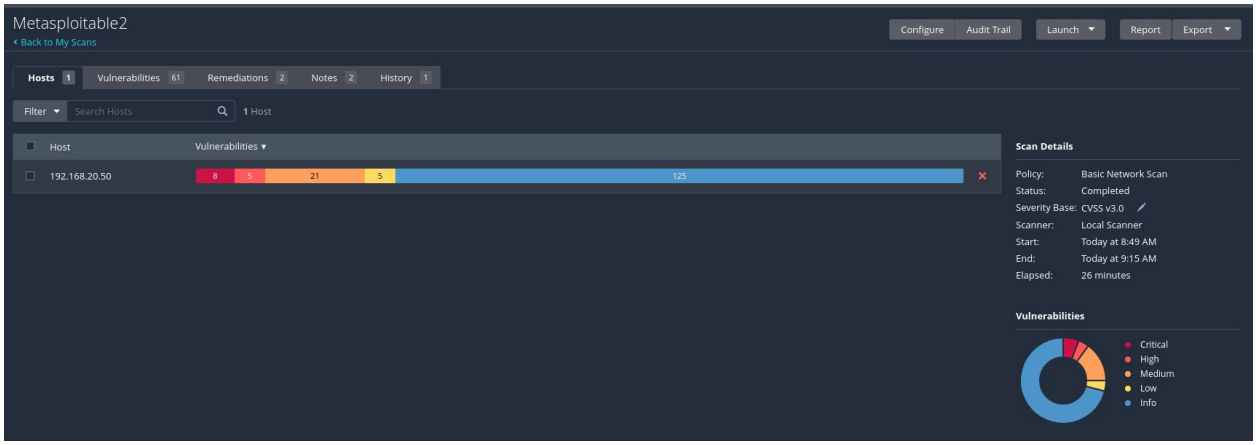


Da qui creiamo una nuova scansione dove andremo a selezionare le impostazioni suggerite nella traccia dell'esercizio. Pertiamo impostiamo l'indirizzo IP da scansionare (192.168.20.50) e dalla scheda *Discovery* selezioniamo l'opzione *Common Ports*, così da concentrare la nostra scansione sulle porte (es. 21, 22, 23, 25, 80, 110, 139, 443, 445, 3389, ecc..) più usate dai vari servizi.


New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Metasploitable
Description
Folder
My Scans
Targets
192.168.20.50
Upload Targets
Add File
Save
Cancel


New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Scan Type
Port scan (common ports)
General Settings:
Always test the local Nessus host
Use fast network discovery
Port Scanner Settings:
Scan common ports
Use netstat if credentials are provided
Use SYN scanner if necessary
Ping hosts using:
TCP
ARP
ICMP (2 retries)

Fatte le dovute impostazioni, salviamo e lanciamo la scansione, al termine della quale andremo ad analizzarne i risultati.



Dall'immagine in alto possiamo vedere come sono state individuate 8 vulnerabilità critiche, 5 alte, 21 medie e 5 basse.

Di seguito elencheremo le varie vulnerabilità e le soluzioni date da Nessus, dove presenti altrimenti cercheremo un'alternativa.

Vulnerabilità critiche:

Vulnerabilità	**Soluzione**
There is a vulnerable A JP connector listening on the remote host.	Update the A JP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.
Bind Shell Backdoor Detection	Verify if the remote host has been compromised, and reinstall the system if necessary.
The remote SSH host keys are weak.	Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.
The remote SSL certificate uses a weak key.	Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.
The remote service encrypts traffic using a protocol with known weaknesses.	Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.
A VNC server running on the remote host is secured with a weak password.	Secure the VNC service with a strong password.

Vulnerabilità alte:

Vulnerabilità	Soluzione
ISC BIND Service Downgrade / Reflected DoS	Upgrade to the ISC BIND version referenced in the vendor advisory.
NFS Shares World Readable	Place the appropriate restrictions on all NFS shares.
SSL Medium Strength Cipher Suites Supported (SWEET32)	Reconfigure the affected application if possible to avoid use of medium strength ciphers.
Samba Badlock Vulnerability	Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

Vulnerabilità medie:

Vulnerabilità	Soluzione
HTTP TRACE / TRACK Methods Allowed	Disable these HTTP methods.
ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS	Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.
ISC BIND Denial of Service	Upgrade to the patched release most closely related to your current version of BIND.
SMB Signing not required	Enforce message signing in the host's configuration.
SMTP Service STARTTLS Plaintext Command Injection	Contact the vendor to see if an update is available.
SSL Anonymous Cipher Suites Supported	Reconfigure the affected application if possible to avoid use of weak ciphers.
SSL Certificate Cannot Be Trusted	Purchase or generate a proper SSL certificate for this service.
SSL Certificate Expiry	Purchase or generate a proper SSL certificate for this service.
SSL Certificate with Wrong Hostname	Purchase or generate a proper SSL certificate for this service.
SSL DROWN Attack Vulnerability	Disable SSLv2 and export grade cryptography cipher suites.
SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.
SSL Self-Signed Certificate	Purchase or generate a proper SSL certificate for this service.
SSL Weak Cipher Suites Supported	Reconfigure the affected application, if possible to avoid the use of weak ciphers.
SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	Reconfigure the service to remove support for EXPORT_RSA cipher suites.
TLS Version 1.0 Protocol Detection	Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.
TLS Version 1.0 Protocol Detection	Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Vulnerabilità basse:

Vulnerabilità	**Soluzione**
ICMP Timestamp Request Remote Date Disclosure	Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).
SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)	Reconfigure the service to remove support for EXPORT_DHE cipher suites.
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	Disable SSLv3.
X Server Detection	Restrict access to this port. If the X11 client/server facility is not used, disable TCP support in X11 entirely (-nolisten tcp).

Nell’elenco riportato le vulnerabilità sono inferiori rispetto a quelle indicate numericamente, questo perchè sono state riscontrate uguali, ma su più porte.