

Obiettivo dell'esercizio:

Lo scopo dell'esercizio è effettuare una scansione di vulnerabilità sulla macchina Metasploitable utilizzando Nessus, focalizzandosi solo sulle porte comuni.

Configurazione della scansione:

- **Target:** 192.168.20.10 (Macchina Metasploitable)
- **Porte scansionate:** 21 (FTP), 22 (SSH), 23 (Telnet), 25 (SMTP), 80 (HTTP), 110 (POP3), 139 (NetBIOS), 443 (HTTPS), 445 (SMB), 3389 (RDP)
- **Tipo di scansione:** Basic Network Scan (profilo predefinito di Nessus)

Procedimento:

- Abbiamo avviato il servizio di nessus tramite il comando:
`/bin/systemctl start nessusd.service`
- Aperto l'interfaccia web tramite <https://kali:8834>
- Configurata una scansione "Basic network scan" dal bottone "new scan"

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: 192.168.20.10

Upload Targets [Add File](#)

Save Cancel

- Abbiamo avviato la scansione e al termine scaricato il report in formato PDF.

Analisi delle vulnerabilit  riscontrate:

Nome vulnerabilit�	Descrizione
Apache tomcat ghostcat	permette l'accesso a file interni e possibile esecuzione di codice.
backdoor bind shell	indica la presenza di una backdoor in ascolto che consente l'accesso remoto.
SSL v2/v3 enabled	supporta protocolli SSL obsoleti e insicuri vulnerabili ad attacchi
debian openssl RNG weakness	generazione di chiavi crittografiche prevedibili
VNC 'password' password	il server VNC � accessibile con una password debole: 'password'
samba badlock	vulnerabilit� nei protocolli SMB/samba che consente DoS o escalation di privilegi
SMB signing not required	consente attacchi MITM nei protocolli SMB perche' la firma non � obbligatoria.
TLS 1.0 detected	versione obsoleta di TLS ancora in uso, vulnerabile ad attacchi crittografici
SSL FREAK attack	supporto a cifrari EXPORT_RSA deboli, esposti a attacchi di decifrazione
HTTP TRACE/TRACK enabled	metodi HTTP abilitati che possono rivelare informazioni sensibili
SSL SWEET32	supporto a cifrari CBC a 64 bit che possono permettere decifrazioni di sessioni
openssh weak algorithms	algoritmi crittografici deboli abilitati in SSH

Conclusione:

La scansione condotta ha evidenziato numerose vulnerabilit  di livello critico e alto, tra cui backdoor attive, protocolli di cifratura obsoleti e configurazioni deboli nei servizi SSH, VNC e HTTP.