Traccia: Esercizio Scansione dei servizi

Si richiede allo studente di effettuare le scansioni dell’esercizio precedente con Nmap sul target Windows con Windows Firewall abilitato e disabilitato.

Elencare tutti i passaggi compiuti ed i tipi di scansione, con i relativi risultati, durante la fase di scrittura report.

Report con Firewall attivo:

Immagine che contiene testo, schermata, software, Software multimediale

Il contenuto generato dall'IA potrebbe non essere corretto.

Scansione Nmap

Autore: Cosimo

Sistema operativo: Kali Linux

Comando eseguito: Nmap 192.168.50.102

Informazioni generali sul target:

• Indirizzo IP: 192.168.50.102

• Stato host: attivo

• MAC Address: 08:00:27:AD:53:B8

• Vendor MAC: PCS Systemtechnik / Oracle VirtualBox

Avviso DNS:

"Unable to determine any DNS servers. Reverse DNS is disabled."

Nmap non è riuscito a risolvere il nome DNS inverso del target. Questo può indicare una rete isolata o la mancanza di configurazione DNS.

Risultati della scansione delle porte:

Sono state analizzate le 1000 porte piu comuni.

996 porte senza risposta

Le seguenti 10 porte risultano aperte:

• Porta 22/tcp: SSH (accesso remoto sicuro)

• Porta 80/tcp: HTTP (server web attivo)

• Porta 135/tcp: MSRPC (servizi RPC di Windows)

• Porta 139/tcp: NetBIOS-SSN (condivisione file Windows)

• Porta 445/tcp: Microsoft-DS (SMB su TCP/IP)

• Porta 3306/tcp: MySQL (database attivo)

• Porta 3389/tcp: MS-WBT-Server (Remote Desktop Protocol)

• Porta 5985/tcp: WSMan (Windows Remote Management)

• Porta 8080/tcp: HTTP-Proxy (proxy o servizio web alternativo)

• Porta 9001/tcp: Tor-Orport (porta di comunicazione nodo Tor)

Considerazioni:

• Il sistema presenta servizi critici come SSH, RDP, SMB e MySQL, che sono spesso bersagliati da attacchi.

• La presenza della porta Tor (9001) suggerisce l’uso della rete Tor.

• Le porte 135, 139 e 445 indicano un sistema Windows, potenzialmente vulnerabile a exploit noti.

• WSMan (5985) è usato per la gestione remota via PowerShell, utile ma rischioso se non protetto.

• La porta 8080 potrebbe ospitare un’applicazione web secondaria o un proxy.

Immagine che contiene testo, schermata

Il contenuto generato dall'IA potrebbe non essere corretto.

Nmap completo

Comando eseguito: Nmap -sS -sV -O -A -T4 -p- 192.168.50.102

• -sS(TCP SYN Scan):

È la modalità di scansione più comune e stealth.

Invia pacchetti SYN (come per iniziare una connessione TCP) e analizza la risposta.

Non completa la connessione, quindi è meno rilevabile da sistemi di logging.

• -sV (Version Detection):

Cerca di identificare la versione esatta dei servizi in esecuzione sulle porte aperte.

Utile per sapere se un servizio è aggiornato o vulnerabile.

• - O (OS Detection):

Tenta di determinare il sistema operativo dell’host target.

Si basa su fingerprinting TCP/IP e altre tecniche di analisi.

• -A (Aggressive Scan):

Attiva automaticamente diverse opzioni: OS detection (), version detection (), script scanning () e traceroute.

È molto utile per una panoramica completa, ma può essere invasiva.

• -T4 (Timing Template):

Imposta la velocità della scansione su “rapida”.

Riduce i tempi di attesa tra i pacchetti, ma aumenta la probabilità di essere rilevati da sistemi IDS/IPS.

• -p- (Scan tutte le porte):

Scansiona tutte le 65535 porte TCP, non solo quelle più comuni.

È utile per trovare servizi nascosti o non convenzionali.

Di seguito una sintesi dettagliata dei risultati ottenuti:

Risoluzione DNS

È stato utilizzato il comando dig per interrogare il server DNS di OpenDNS (208.67.222.222) alla ricerca dell'indirizzo IP pubblico del sistema tramite il dominio “myip.opendns.com”. Il risultato ha restituito correttamente l'indirizzo IP pubblico:

IP pubblico rilevato: “98.169.244.14”

Questo conferma che il sistema è correttamente connesso a Internet e che la risoluzione DNS funziona come previsto.

Interfacce di rete

Il comando ip a ha mostrato le interfacce di rete attive e virtuali presenti sul sistema. Ecco un riepilogo:

lo (loopback): Interfaccia interna con IP 127.0.0.1

eth0: Interfaccia principale connessa alla rete locale, con indirizzo IP assegnato

virbr0 / virbr0-nic / vnet0: Interfacce virtuali, probabilmente utilizzate da macchine virtuali o ambienti di virtualizzazione come KVM/QEMU

Ogni interfaccia è correttamente configurata con indirizzi MAC e IP.

Interfacce virtuali: Instradamenti dedicati per “virbr0”, utili per la comunicazione tra host e guest virtuali

La configurazione appare coerente con un ambiente che utilizza sia rete fisica che virtuale.

Conclusione:

La scansione ha rivelato un sistema attivo con diversi servizi esposti, alcuni dei quali potenzialmente vulnerabili. La configurazione suggerisce un ambiente di test o una macchina virtuale Windows con servizi di rete e database attivi. È fondamentale procedere con cautela e rispettare le policy di autorizzazione prima di qualsiasi test intrusivo.

Report con Firewall disattivo:

Immagine che contiene testo, software, Pagina Web, schermata

Il contenuto generato dall'IA potrebbe non essere corretto.

Comando Nmap:

Immagine che contiene testo, schermata

Il contenuto generato dall'IA potrebbe non essere corretto.

Comparazione con il firewall attivo:

Firewall disattivato

Sono state rilevate 19 porte TCP aperte, tutte associate a servizi noti e comuni.

I servizi visibili includono:  
ftp, ssh, telnet, smtp, http, https, pop3, imap, mysql, postgresql, http-proxy, https-alt, ecc.

Sono presenti anche servizi di posta sicura come smtps, submission, imaps, pop3s.

La macchina risponde liberamente a tutte le richieste, senza alcun tipo di filtraggio.

Questo comportamento indica chiaramente che non è presente alcuna protezione firewall: tutte le porte sono accessibili e visibili dall’esterno.

Firewall attivo

Sono state rilevate 18 porte TCP aperte, ma molte sono porte di test o legacy come: echo, discard, daytime, chargen.

Alcune porte risultano "unknown", come 49152, 49153, 49154.

Mancano completamente i servizi di posta (imap, pop3, smtp sicuro), database (postgresql) e proxy (http-proxy, https-alt).

Sono visibili solo alcuni servizi Microsoft (msrpc, microsoft-ds, ms-wbt-server) e mysql.

Questo comportamento suggerisce che il firewall è attivo e sta filtrando molte richieste, impedendo la visibilità di servizi comuni.

La prima scansione mostra un sistema completamente esposto, con tutti i servizi visibili: questo è tipico di una macchina senza firewall.  
La seconda scansione, invece, mostra un sistema più chiuso, con porte limitate e alcune non identificate: questo è indice di un firewall attivo che blocca o filtra le connessioni in ingresso.

Nmap completo

Comando eseguito: Nmap -sS -sV -O -A -T4 -p- 192.168.50.102Immagine che contiene testo, schermata

Il contenuto generato dall'IA potrebbe non essere corretto.

La seconda scansione (ovvero questo qui sopra) mostra più porte aperte, tra cui servizi web e di gestione remota. Sono visibili dettagli sul sistema operativo, hostname, dominio e persino il titolo della pagina web. Questo indica che il firewall è disattivato o molto permissivo, perché lascia passare molte richieste.

La seconda scansione è molto più chiusa: si vedono solo tre porte aperte (135, 139, 445), tutte legate ai servizi base di Windows. Non ci sono servizi web né informazioni dettagliate. Questo significa che il firewall è attivo e sta bloccando la maggior parte delle connessioni.