Nmap

Tecniche di scansione con e senza 3-way handshake

Denisa D.
Epicode

Indice

Introduzione

1.1 Contesto dell'esercizio e obiettivi

L'esercizio proposto si concentra sull'utilizzo di Nmap, uno strumento ampiamente utilizzato per la scansione della rete su piattaforme Linux, per acquisire familiarità con le tecniche di scansione di un host. Si eseguiranno scansioni su un host utilizzando Nmap, sia con che senza il completamento del 3-way handshake, al fine di comprendere le differenze nei risultati ottenuti e l'importanza del completamento del 3-way handshake durante le scansioni di rete.

L'obiettivo principale è permettere di acquisire competenze pratiche nell'utilizzo di Nmap e comprendere le implicazioni delle diverse tecniche di scansione sulla precisione e sulla completezza dei risultati ottenuti.

1.2 Importanza delle Tecniche di Scansione con Nmap

Le tecniche di scansione con Nmap rivestono un'importanza cruciale nel contesto della sicurezza informatica e della gestione delle reti. Nmap consente agli amministratori di rete di identificare dispositivi connessi alla rete, scoprire porte aperte e servizi in esecuzione su tali porte, nonché valutare la sicurezza complessiva della rete.

Metodologia

2.1 Descrizione delle Tecniche di Scansione con Nmap

- Scansione SYN (-sS): Questa tecnica, nota anche come scansioni stealth, invia pacchetti SYN per determinare lo stato delle porte senza stabilire una connessione completa, fornendo una rapida indicazione delle porte aperte.
- Scansione Version Detection (-sV): Questa tecnica identifica le versioni dei servizi in esecuzione sulle porte aperte, inviando specifici pacchetti di richiesta per ottenere informazioni sulle versioni dei servizi.
- Scansione UDP (-sU): Utilizzata per individuare servizi e porte UDP aperti, che sono comunemente utilizzati per servizi di rete come DNS e DHCP.
- Identificazione del Sistema Operativo (-O): Questa tecnica tenta di identificare il sistema operativo del target, analizzando le risposte del sistema a determinati pacchetti di prova.

2.2 Spiegazione dei Comandi Utilizzati nell'Esercizio

Durante l'esercizio sono stati utilizzati i seguenti comandi Nmap:

- nmap -sS: scansione SYN per individuare le porte aperte. Invia pacchetti SYN ai dispositivi target e analizzando le risposte per determinare lo stato delle porte (aperte, chiuse o filtranti) È una tecnica stealth in quanto non completa la connessione TCP.
- nmap -sV: scansione di versione per identificare le versioni dei servizi. Invia specifici pacchetti di richiesta ai servizi per ottenere informazioni sulle versioni.
- nmap -sV -oN file.txt: scansione di versione e salva i risultati in un file di testo. È utile per archiviare e analizzare i risultati della scansione in un secondo momento.
- nmap -sS -p 8080: scansione SYN solo sulla porta 8080.
- nmap -sS -p: scansione SYN su tutte le porte.
- nmap -sU -r -v: scansione UDP con routing e output verbose per visualizzare maggiori dettagli.
- nmap -O: scansione del sistema operativo.
- nmap -F: scansione veloce, esaminando solo le porte più comuni.
- nmap -PR: scansione ARP ping per individuare host attivi e scoprire i loro indirizzi MAC.
- nmap -sP: scansione ping per individuare host attivi.
- nmap -PN: scansione senza ping per tutti gli host, è utile quando si desidera eseguire una scansione su dispositivi che potrebbero non rispondere ai ping.

Scansione di un Host senza completamento del 3-way handshake

3.1 Risultati della scansione di un host senza completamento del 3-way handshake

- **nmap -sS nmap -sS -P nmap -PN**

Numero Porta	Stato	Servizio
135/tcp	aperta	MSRPC (Microsoft Remore Procedure Call)
139/tcp	aperta	NetBIOS-SSN (NetBIOS Session Service)
445/tcp	aperta	Microsoft-DS (Microsoft Directory Services)

Stato sistema: Windows
Indirizzo MAC: 08:00:27:D8:C3:D7

- **nmap -PR** e **nmap -sP**
  non hanno fornito risultati utili all'indagine, probabilmente a causa di firewall attivo o di una sua regola.

3.2 Analisi dei risultati ottenuti

La scansione nmap -sS mostra che l'host è attivo e rivela diverse porte aperte, tra cui 135/tcp (msrpc), 139/tcp (netbios-ssn), 445/tcp (microsoft-ds).
La scansione nmap -sS -P conferma che l'host è attivo e risponde al ping. Le stesse porte aperte sono state rilevate come nei precedenti risultati.
La scansione nmap -PN riporta i risultati precedentemente elencati.
La scansione -PR non ha riportato informazioni utili.

Scansione di un Host con completamento del 3-way handshake

4.1 Risultati della scansione di un host con completamento del 3-way handshake

- **nmap -sV**
- **nmap -sV -oN file.txt**
- **nmap -sS -p 8080**
- **nmap -sU -r -v**
- **nmap -O**
- **nmap -F**

Numero Porta	Stato	Servizio
135/tcp	aperta	MSRPC (Microsoft Remore Procedure Call)
139/tcp	aperta	NetBIOS-SSN (NetBIOS Session Service)
445/tcp	aperta	Microsoft-DS (Microsoft Directory Services)
8080/tcp	filtrata	http-proxy
137/udp	aperta	Netbios-ns

Sistema Operativo: Windows
Indirizzo MAC: 08:00:27:D8:C3:D7
Porta http-proxy: potrebbe essere aperta, ma non accessibile dall'esterno

4.2 Analisi dei risultati ottenuti

L'host sembra essere un sistema Windows attivo sulla rete. Le porte aperte rilevate indicano l'utilizzo di servizi comuni associati a Windows, come msrpc, netbios-ssn e microsoft-ds. Tuttavia alcune porte specifiche, come la 8080/tcp, sembrano essere filtrate o non accessibili, suggerendo che potrebbero essere soggette a restrizioni di rete. L'identificazione del sistema operativo tramite la scansione -O non è stata conclusiva, ma suggerisce fortemente l'utilizzo di un sistema Windows.

Inoltre, l'utilizzo di diverse opzioni di scansione, come -oN per salvare i risultati su un file di testo e -v per aumentare il livello di dettaglio nella scansione DP, fornisce una panoramica più completa della topologia e dei servizi attivi sull'host.

Conclusioni

5.1 Sintesi dei risultati ottenuti

Le scansioni effettuate utilizzando diverse opzioni di Nmap hanno fornito una panoramica dettagliata dello stato e delle caratteristiche dell'host. Sono state identificate le porte aperte e sono stati ottenuti alcuni dettagli sui servizi in esecuzione, incluso il sistema operativo utilizzato, in alcuni casi. Tuttavia, è emerso che l'host sembra non rispondere alle richieste di ping in alcune scansioni, mentre in altre risulta attivo e raggiungibile.

5.2 Riflessioni sull'utilità delle tecniche di scansione con Nmap

Le tecniche di scansione con Nmap si sono dimostrate estremamente utili per ottenere informazioni dettagliate sull'host di destinazione. Questo strumento è fondamentale per gli amministratori di rete e gli esperti di sicurezza per identificare le risorse di rete, rilevare eventuali vulnerabilità e monitorare la sicurezza complessiva del sistema. Tuttavia, è importante notare che l'accuratezza dei risultati può variare a seconda delle condizioni di rete e delle impostazioni di configurazione dell'host. Pertanto, è consigliabile utilizzare Nmap in modo responsabile e in conformità con le normative sulla sicurezza informatica.