S5L3 Scansione dei servizi con Nmap

Traccia: Tecniche di scansione con Nmap Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

● OS fingerprint.

● Syn Scan.

● TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?

● Version detection.

E la seguente sul target Windows 7:

● OS fingerprint.

A valle delle scansioni è prevista la produzione di un report contenente le seguenti info (dove disponibili):

● IP.

● Sistema Operativo.

● Porte Aperte.

● Servizi in ascolto con versione. Quesito extra (al completamento dei quesiti sopra): Quale potrebbe essere una valida ragione per spiegare il risultato ottenuto dalla scansione sulla macchina Windows 7? Che tipo di soluzione potreste proporre per continuare le scansioni?

Scansioni su Metasploitable:

*OS Fingerprint:* È la tecnica di scansione che ci fornirà informazioni sull'identificazione del sistema operativo. Lo eseguiremmo con seguente commando *nmap -O 172.20.10.13*

*Syn Scan*: È la tecnica di scansione per eseguire una scansione SYN per identificare le porte aperte. Lo eseguiremmo con seguente commando nmap -sS *172.20.10.13*

*TCP Connect:* È la tecnica di scansione che confrontera i risultati di questa scansione con quelli della scansione SYN per trovare eventuali differenze. Lo eseguiremmo con seguente commando *nmap -sT 172.20.10.13*

*Version Detection:* Questo comando identificherà le versioni dei servizi in ascolto sulle porte aperte. Lo eseguiremmo con seguente commando *nmap -sV 172.20.10.13*

**Scansione su Windows 7:**

*OS Fingerprint:* Lo eseguiremmo con seguente commando *nmap -O 192.168.1.11*

**Report:**

*Os Fingerprint*:

Il comando *nmap -O 192.168.1.50*, è utilizzato per la rilevazione del sistema operativo sull'host di destinazione con l'indirizzo IP 192.168.1.50. Vediamo nel dettaglio l'output:

Une image contenant texte, capture d’écran, Police, information

Description générée automatiquement

Starting Nmap 7.94SVN: Questa riga indica la versione di Nmap utilizzata per la scansione.

Nmap scan report for Host-007.lan (192.168.1.50): Nmap ha identificato l'host di destinazione come "Host-007.lan" con l'indirizzo IP 192.168.1.50.

Host is up (0.000061s latency): La scansione ha determinato che l'host di destinazione è online, con una latenza molto bassa di 0.000061 secondi.

All 1000 scanned ports on Host-007.lan (192.168.1.50) are in ignored states: Questo suggerisce che le porte scansionate sono in uno stato "ignorato", il che significa che Nmap non è riuscito a determinare lo stato aperto o chiuso di queste porte. Ciò potrebbe essere dovuto a varie ragioni, come regole del firewall o filtraggio dei pacchetti.

Not shown: 1000 closed tcp ports (reset): Nmap indica di aver trovato 1000 porte TCP chiuse sull'host di destinazione. "Not shown" significa che queste porte non vengono visualizzate nell'output per ridurre la verbosità. La menzione di "(reset)" suggerisce che Nmap ha determinato che le porte erano chiuse in base alle risposte di reset ricevute.

Too many fingerprints match this host to give specific OS details: Nmap ha incontrato molteplici possibili impronte del sistema operativo per l'host di destinazione, rendendo difficile fornire dettagli specifici sul sistema operativo. Ciò potrebbe essere dovuto a vari fattori, come l'host che esegue servizi multipli o l'uso di tecniche per offuscare il proprio sistema operativo.

Network Distance: 1 hop: Ciò indica che l'host di destinazione è a un salto di rete dallo scanning host.

OS detection performed. Please report any incorrect results at https://nmap.org/submit/.: Questo è un promemoria per segnalare eventuali risultati errati sulla rilevazione del sistema operativo al progetto Nmap per ulteriore analisi e miglioramento.

Nmap done: 1 IP address (1 host up) scanned in 1.79 seconds: La scansione è completa e ha richiesto circa 1.79 secondi per scansionare l'host di destinazione.

In sintesi, la scansione Nmap ha cercato di rilevare il sistema operativo dell'host di destinazione ma ha incontrato sfide a causa di molteplici impronte corrispondenti. Lo stato aperto/chiuso delle porte non è stato chiaramente determinato per le porte scansionate. Se sono necessari dettagli più specifici sul sistema operativo, potrebbero essere esplorate opzioni o tecniche aggiuntive di Nmap.

*Syn Scan*:

Il tuo comando Nmap ha eseguito una scansione SYN sull'indirizzo IP specificato 192.168.1.50. Vediamo nel dettaglio l'output ricevuto:

Une image contenant texte, Police, capture d’écran, information

Description générée automatiquement

Starting Nmap 7.94SVN: Questo fornisce l'informazione sulla versione di Nmap che stai utilizzando.

Nmap scan report for Host-007.lan (192.168.1.50): Nmap riporta di aver eseguito la scansione sull'host specificato con indirizzo IP 192.168.1.50. Il nome "Host-007.lan" può essere ottenuto attraverso la risoluzione DNS inversa o una ricerca di hostname locale.

Host is up (0.0000050s latency): Nmap ha determinato che l'host al 192.168.1.50 è online, e il tempo di latenza è molto basso, 0,0000050 secondi, indicando una risposta molto rapida.

All 1000 scanned ports on Host-007.lan (192.168.1.50) are in ignored states: Similarmente al tuo primo comando, questo indica che Nmap non è stato in grado di determinare lo stato delle porte scansionate. L'espressione "ignored states" suggerisce che Nmap non è riuscito a determinare in modo affidabile se le porte sono aperte, chiuse o filtrate.

Not shown: 1000 closed tcp ports (reset): Nmap non ha mostrato lo stato delle 1000 porte TCP scansionate, e assume che siano chiuse. La parte "(reset)" indica che le porte chiuse hanno restituito un segnale di reset.

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds: Questa è una sintesi della scansione Nmap. Indica che Nmap ha scansionato con successo un indirizzo IP (192.168.1.50) e ha trovato un host online. La scansione è stata completata in 0,15 secondi.

In sostanza non è stato in grado di determinare in modo affidabile lo stato delle porte scansionate. Questo potrebbe essere dovuto a fattori come le impostazioni del firewall o altre condizioni di rete.

*Tcp Connect*:

Nel comando *nmap -sT 192.168.1.50*, l'opzione -sT specifica una scansione TCP connect. Analizziamo l'output ricevuto:

Une image contenant texte, capture d’écran, Police, information

Description générée automatiquement

Starting Nmap 7.94SVN: Questo è solo l'informazione sulla versione dello strumento Nmap che stai utilizzando.

Nmap scan report for Host-007.lan (192.168.1.50): Nmap segnala di aver eseguito la scansione dell'host specificato, che ha l'indirizzo IP 192.168.1.50. Il nome "Host-007.lan" è probabilmente ottenuto tramite reverse DNS o una ricerca di hostname locale.

Host is up (0.00043s latency): Nmap ha determinato che l'host al 192.168.1.50 è online e ha impiegato 0,00043 secondi per ricevere una risposta.

All 1000 scanned ports on Host-007.lan (192.168.1.50) are in ignored states: L'output suggerisce che Nmap non è stato in grado di determinare lo stato delle porte scansionate. Il termine "ignored states" di solito indica che Nmap non è riuscito a rilevare in modo affidabile se le porte sono aperte, chiuse o filtrate.

Not shown: 1000 closed tcp ports (conn-refused): Nmap non ha mostrato lo stato delle 1000 porte TCP che ha scansionato e assume che siano chiuse. La parte "(conn-refused)" indica che le porte chiuse hanno restituito un messaggio di connessione rifiutata.

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds: Questa è una sintesi della scansione Nmap. Indica che Nmap ha scansionato con successo un indirizzo IP (192.168.1.50) e ha trovato un host online. La scansione è stata completata in 0,12 secondi.

In sintesi, il comando Nmap ha cercato di eseguire una scansione TCP connect sull'indirizzo IP specificato (192.168.1.50), ma non è stato in grado di determinare in modo affidabile lo stato delle porte scansionate. Questo potrebbe essere dovuto a vari motivi, come le impostazioni del firewall o altre condizioni di rete.

Version Detection:

Il comando Nmap nmap -sV 192.168.1.50 include la scansione dei servizi. Di seguito una spiegazione dell'output:

Une image contenant texte, Police, nombre, capture d’écran

Description générée automatiquement

Starting Nmap 7.94SVN: Fornisce l'informazione sulla versione di Nmap in uso.

Nmap scan report for Host-007.lan (192.168.1.50): Nmap riporta di aver eseguito la scansione sull'host specificato con indirizzo IP 192.168.1.50. Il nome "Host-007.lan" può essere ottenuto attraverso la risoluzione DNS inversa o una ricerca di hostname locale.

Host is up (0.0000050s latency): Nmap ha determinato che l'host al 192.168.1.50 è online, e il tempo di latenza è molto basso, 0,0000050 secondi, indicando una risposta molto rapida.

All 1000 scanned ports on Host-007.lan (192.168.1.50) are in ignored states: Ancora una volta, Nmap non è stato in grado di determinare in modo affidabile lo stato delle porte scansionate. L'espressione "ignored states" suggerisce che Nmap non è riuscito a determinare se le porte sono aperte, chiuse o filtrate.

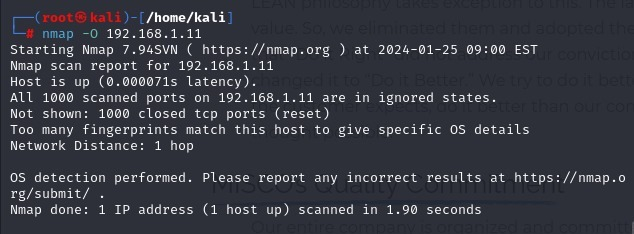
Not shown: 1000 closed tcp ports (reset): Nmap non ha mostrato lo stato delle 1000 porte TCP scansionate, presumendo che siano chiuse. La parte "(reset)" indica che le porte chiuse hanno restituito un segnale di reset.

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ : Questo indica che Nmap ha anche eseguito la rilevazione dei servizi, cercando di identificare i servizi in esecuzione sulle porte scansionate.

Nmap done: 1 IP address (1 host up) scanned in 0.71 seconds: Questa è una sintesi della scansione Nmap. Indica che Nmap ha scansionato con successo un indirizzo IP (192.168.1.50) e ha trovato un host online. La scansione, questa volta, è stata più lunga, completata in 0,71 secondi a causa della rilevazione dei servizi.

In conclusione, il comando Nmap ha eseguito una scansione dei servizi sull'indirizzo IP specificato, ma ancora una volta non è stato in grado di determinare in modo affidabile lo stato delle porte scansionate. Può essere dovuto a fattori come le impostazioni del firewall o altre condizioni di rete.

Scansione Window 7



Il comando Nmap nmap -O 192.168.1.11 è stato utilizzato per eseguire una scansione di rilevamento del sistema operativo. Di seguito una spiegazione dell'output:

Starting Nmap 7.94SVN: Fornisce l'informazione sulla versione di Nmap che stai utilizzando.

Nmap scan report for 192.168.1.11: Nmap riporta di aver eseguito la scansione sull'indirizzo IP specificato, che è 192.168.1.11.

Host is up (0.000071s latency): Nmap ha determinato che l'host al 192.168.1.11 è online, e il tempo di latenza è molto basso, 0,000071 secondi, indicando una risposta molto rapida.

All 1000 scanned ports on 192.168.1.11 are in ignored states: Nmap ancora una volta non è stato in grado di determinare in modo affidabile lo stato delle porte scansionate. L'espressione "ignored states" suggerisce che Nmap non è riuscito a determinare se le porte sono aperte, chiuse o filtrate.

Not shown: 1000 closed tcp ports (reset): Nmap non ha mostrato lo stato delle 1000 porte TCP scansionate, presumendo che siano chiuse. La parte "(reset)" indica che le porte chiuse hanno restituito un segnale di reset.

Too many fingerprints match this host to give specific OS details: Nmap ha rilevato molteplici fingerprint che corrispondono a questo host, rendendo difficile fornire dettagli specifici sul sistema operativo.

Network Distance: 1 hop: Indica che l'host è raggiungibile direttamente, a una distanza di un hop di rete.

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ : Questo suggerisce che Nmap ha eseguito la rilevazione del sistema operativo, cercando di identificare il sistema operativo in esecuzione sull'host.

Nmap done: 1 IP address (1 host up) scanned in 1.90 seconds: Questa è una sintesi della scansione Nmap. Indica che Nmap ha scansionato con successo un indirizzo IP (192.168.1.11) e ha trovato un host online. La scansione è stata completata in 1,90 secondi.

In conclusione, il comando Nmap ha eseguito una scansione di rilevamento del sistema operativo sull'indirizzo IP specificato, ma la presenza di molteplici fingerprint ha reso difficile fornire dettagli specifici sul sistema operativo.

Metasploitable:

IP: 192.168.1.50

Sistema Operativo identificato:

Porte aperte: Stato non preciso

Servizi in ascolto con versione

Windows 7:

IP 192.168.1.11

Sistema Operativo identificato

Quesito Extra

Risultato della scansione su Windows 7: Potrebbe essere che il firewall di Windows 7 blocca le risposte alle richieste di scansione, influenzando i risultati.

Soluzione proposta per continuare le scansioni:

Disabilitare il Firewall: Temporaneamente disabilitare il firewall su Windows 7 e rieseguire la scansione per verificare se ci sono differenze nei risultati.

Regole del Firewall: Configurare regole specifiche nel firewall di Windows 7 per consentire la scansione senza disabilitarlo completamente.

Modalità di Sicurezza del Sistema: Controllare se il sistema ha un software di sicurezza che potrebbe interferire con la scansione e considerare la modifica delle impostazioni o la temporanea disattivazione per scopi di test.