REPORT

Enumerazione e scansione OS e servizi

Denisa D.

Epicode

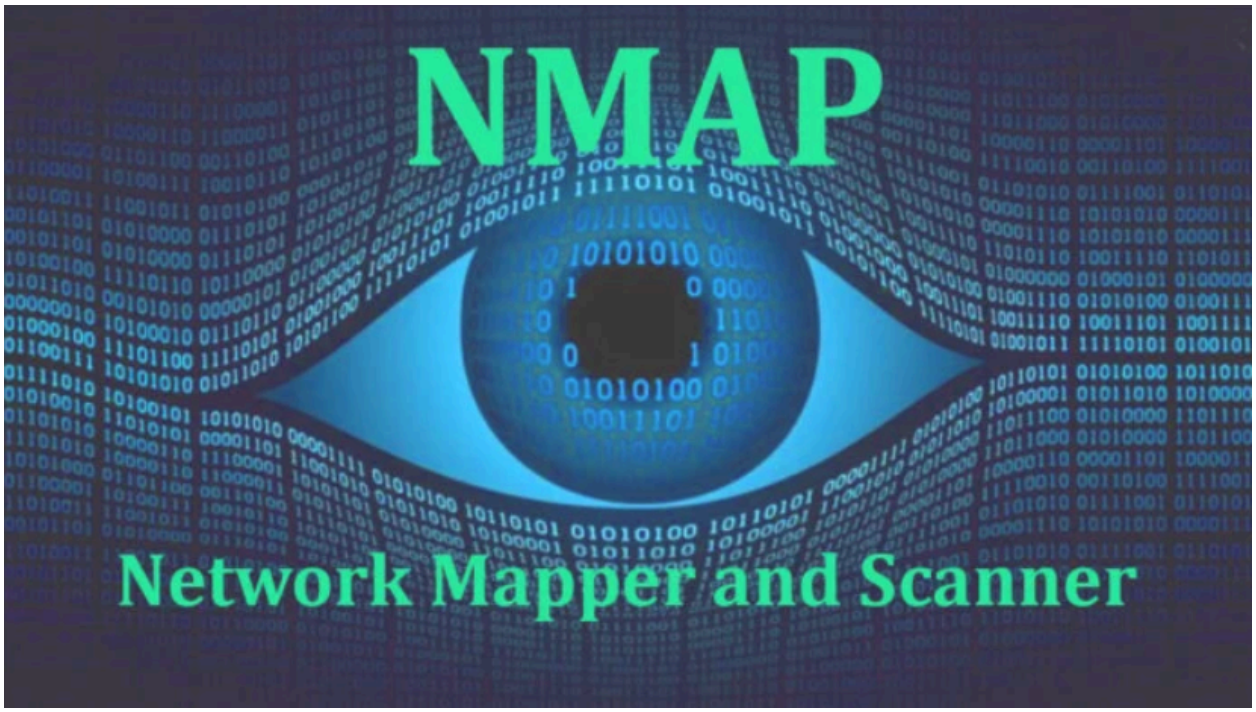
Indice

Traccia

Tecniche di scansione nmap

Si richiede allo studente di effettuare le seguenti scansioni sul target Windows 7:

1. OS fingerprint
2. Syn Scan
3. Version detection



Metodologia

La seguente sezione delinea la metodologia impiegata per condurre le scansioni sul target Windows 7, utilizzando lo strumento Nmap.

1.1 Descrizione delle tecniche e degli argomenti utilizzati in Nmap

Per condurre le scansioni sul sistema target, sono state adottate diverse tecniche supportate da Nmap:

- **OS Fingerprinting**: Questa tecnica mira a identificare il sistema operativo in esecuzione sul target analizzando le risposte alle richieste di scansione inviate. Nmap confronta i comportamenti delle risposte con un database di firme per determinare il sistema operativo più probabile.
- **Syn Scan**: Questa tecnica di scansione utilizza pacchetti TCP SYN per determinare lo stato delle porte sul sistema target. È una scansione veloce ed efficiente in grado di individuare le porte aperte senza completare la connessione TCP.
- **Version Detection**: Questa tecnica mira a identificare le versioni specifiche dei servizi in esecuzione sulle porte aperte del sistema target. Nmap invia richieste appositamente progettate per ottenere risposte che includono informazioni sulla versione del software.

1.2 Parametri e opzioni specificate nello scan

Durante le scansioni, è essenziale specificare parametri e opzioni pertinenti per ottenere i risultati desiderati e limitare il tempo e le risorse impiegate. Alcuni dei parametri e delle opzioni utilizzate in Nmap includono:

- **-O** (OS Detection): Utilizzato per attivare il riconoscimento del sistema operativo durante lo scan.
- **-sS** (Synscan): Specifica l'uso della scansione Syn per esaminare lo stato delle porte.
- **-sV** (Version Detection): Abilita la rilevazione delle versioni dei servizi sulle porte aperte.

L'accurata selezione di questi parametri e opzioni assicura un'analisi dettagliata del sistema target, consentendo di identificare le sue caratteristiche e vulnerabilità con precisione.

Enumerazione di Porte

2.1 Risultati dello scan porte aperte/chiuse

L'analisi delle porte effettuate tramite i comandi **-O**, **-sS**, **-sV** riporta i seguenti risultati:

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)

2.2 Analisi delle porte e dei servizi trovati

La presenza delle porte 135/tcp, 139/tcp e 445/tcp indica la disponibilità dei servizi MSRPC, NetBIOS-SSN e Microsoft-DS su sistema target. Questi servizi sono comuni in ambienti Windows e sono utilizzati per varie funzionalità di rete, tra cui la condivisione di file e risorse.

La presenza di questi servizi e porte aperte, insieme all'indirizzo MAC del dispositivo, conferma che il target è probabilmente un dispositivo Windows, come confermato dalle specifiche rilevate con -O:"Microsoft Windows Embedded Standard 7" o "Microsoft Windows Phone 7.7 or 8.0".

Scansione dei servizi

3.1 Dettagli sulla versione e le informazioni rilevate sui servizi

Ulteriori dettagli e informazioni rilevati sui servizi individuati includono:

- Porta 135/tcp: il servizio MSRPC è associato a Microsoft Windows netbios-ssn. Non sono stati forniti dettagli sulla versione specifica.
- Porta 139/tcp: il servizio NetBIOS-SSN è associato a Microsoft Windows netbios-ssn. Non sono stati forniti dettagli sulla versione specifica.
- Porta 445/tcp: il servizio Microsoft-DS è associato a Microsoft Windows 7-10 microsoft-ds. Questo fornisce un'indicazione sulla possibile versione del sistema operativo ospitante.

Questi dettagli sui servizi forniscono informazioni utili per comprendere meglio il contesto e le specifiche versioni dei servizi.

Identificazione di Sistemi Operativi

4.1 Risultati ottenuti riguardo alla determinazione del sistema operativo

Le scansioni con Nmap utilizzando i comandi “-O”, “-sS”, “-sV” hanno fornito i seguenti risultati riguardo alla determinazione del sistema operativo target.

Il sistema operativo target è stato identificato come un dispositivo Windows, con alcune ipotesi sulla possibile versione del SO:

- Descrizione del Sistema Operativo: Microsoft Windows Embedded Standard 7 o Microsoft Windows Phone 7.5 o 8.0.

Questi risultati indicano chiaramente che il sistema target è un dispositivo Windows, con ulteriori dettagli sulla possibile versione del SO ospitante.

4.2 Ipotesi basate sui dati raccolti

Basandosi sui dati raccolti durante le scansioni, è possibile formulare alcune ipotesi riguardo al sistema operativo ospitante:

- Il SO potrebbe essere una versione di Windows Embedded Standard 7, un’edizione di Windows progettata per dispositivi embedded e applicazioni specializzate.
- Alternativamente, il sistema potrebbe essere un dispositivo Windows Phone con una versione compresa tra 7.5 e 8.0, utilizzata per dispositivi mobili.

Tuttavia, è importante notare che l'identificazione precisa del sistema operativo potrebbe essere influenzata da variabili come la configurazione di rete e le politiche di sicurezza del target, e quindi, queste ipotesi dovrebbero essere considerate come indicazioni preliminari soggette a conferma ulteriore.

Analisi di vulnerabilità

5.1 Individuazione di Possibili Vulnerabilità

Dalle scansioni eseguite utilizzando Nmap utilizzando i comandi “-O”, “-sS”, “-sV”, è possibile individuare alcune potenziali vulnerabilità o aree di rischio nel sistema target:

- Porte aperte esposte: Le porte aperte rilevate nelle scansioni (porta 135/tcp per MSRPC, porta 139/tcp per NetBIOS-SSN e porta 445/tcp per Microsoft-DS) potrebbero esporre il sistema a potenziali attacchi come exploitation dei servizi, attacchi di forza bruta o tentativi di accesso non autorizzato.

5.2 Considerazioni sulla Vulnerabilità e sulle Potenziali Contromisure

Considerando le possibili vulnerabilità individuate, è importante adottare misure preventive per mitigare i rischi associati:

- Patch e Aggiornamenti: assicurarsi che il sistema target sia aggiornato con le porte patch di sicurezza più recenti per ridurre l’esposizione a vulnerabilità conosciute.
- Firewall e Filtraggio del Traffico: configurare un firewall per limitare l’accesso alle porte aperte solo a utenti autorizzati e applicare filtri per mitigare potenziali attacchi.
- Monitoraggio del Traffico di Reti: implementare un sistema di monitoraggio del traffico di rete per individuare attività sospette o anomalie che potrebbero indicare un potenziale attacco.

Inoltre, è consigliabile condurre regolarmente scansioni di vulnerabilità e test di penetrazione per identificare e risolvere eventuali debolezze nel sistema.

Conclusioni

6.1 Sintesi dei risultati ottenuti

Le scansioni condotte utilizzando Nmap hanno fornito una visione dettagliata dello stato e delle caratteristiche del sistema target. Di seguito sono riassunti i principali risultati:

- Identificazione del Sistema Operativo: Il sistema target è stato identificato come un dispositivo Windows, con possibili indicazioni sulla versione del sistema operativo.
- Enumerazione delle Porte: Sono state individuate diverse porte aperte, tra cui le porte 135/tcp, 139/tcp e 445/tcp, che ospitano servizi tipici di un ambiente Windows.
- Analisi di Vulnerabilità: Sono state identificate alcune potenziali vulnerabilità legate alle porte aperte e ai servizi esposti, che potrebbero essere oggetto di attacchi o intrusioni.

6.2 Raccomandazioni per Eventuali Azioni Future

Basandosi sui risultati ottenuti, si consiglia di prendere in considerazione le seguenti azioni future:

- Aggiornamenti di Sicurezza: Assicurarsi che il sistema target sia aggiornato con le ultime patch di sicurezza per ridurre l'esposizione a vulnerabilità note.
- Configurazione del Firewall: Implementare regole di firewall per limitare l'accesso alle porte aperte solo a utenti autorizzati e monitorare il traffico di rete per rilevare attività sospette.
- Scansioni Periodiche di Vulnerabilità: Condurre regolarmente scansioni di vulnerabilità e test di penetrazione per identificare e risolvere eventuali debolezze nel sistema.
- Formazione e Consapevolezza: Fornire formazione e consapevolezza sulla sicurezza informatica agli utenti e al personale per promuovere comportamenti sicuri e prevenire attacchi informatici.

Implementando queste raccomandazioni, si può migliorare la sicurezza complessiva del sistema e ridurre il rischio di compromissione della sicurezza e delle informazioni sensibili.