Cyber Security Analyst

PROJECT REPORT

SIMULAZIONE FASE DI RACCOLTA parte 2

In risposta all'esercizio su: (vedi consegna nella pag. seguente)

Prepared by

Fulvio Zalateu

Security Rookies

Consegna:

Info Gathering
https://www.yeahhub.com/15-most-useful-host-scanning-commands-kalilinux/
Utilizzare alcuni di questi strumenti per raccogliere informazioni sulla macchina metasploitable e produrre un report.
Nel report indicare sopra l’esecuzione degli strumenti e nella parte finale un riepilogo delle informazioni trovate

Svolgimento

Individuare la rete a cui si è connessi, se la macchina target si trovi nella stessa rete. Ai fini dell'esercizio, l'autore conosce già l'indirizzo IP target, tuttavia si fa una simulazione come se non si conoscesse l'indirizzo IP. Lanciare il comando ip a su terminale Kali.

Scansione rete ed individuazione IP target

Dall'indirizzo IP 192.168.1.101/24 si deduce che il gateway è 192.168.1.1 e pertanto si può eseguire una scansione della rete 192.168.1.1 con il comando sudo nmap -A 192.168.1.0/24 o in alternativa utilizzare netdiscover netdiscover -r 192.168.1.0/24

Non ci sono informazioni utili rilevanti, tuttavia tramite questa scansione si scopre che pfSense è il gateway.
Pertanto si può procedere alla pagina di configurazione di pfSense per scoprire quali reti sono state configurate e/o collegate. Conosciamo le credenziali di accesso alla pagina di configurazione di pfSense all'indirizzo IP 192.168.1.1 avviandolo da browser da Kali. Si scopre che c'è un'altra rete collegata 192.168.50.1 con subnet /24
Pertanto si prosegue con il comando per la scansione di nmap sul nuovo indirizzo IP sudo nmap -A 192.168.50.0/24
Individuato una macchina con indirizzo ip 192.168.50.100 che è l'unica macchina collegata alla rete.

Non ci sono informazioni utili rilevanti, tuttavia tramite questa scansione si scopre che pfSense è il gateway.
Pertanto si può procedere alla pagina di configurazione di pfSense per scoprire quali reti sono state configurate e/o collegate. Conosciamo le credenziali di accesso alla pagina di configurazione di pfSense all'indirizzo IP 192.168.1.1 avviandolo da browser da Kali. Si scopre che c'è un'altra rete collegata 192.168.50.1 con subnet /24
Pertanto si prosegue con il comando per la scansione di nmap sul nuovo indirizzo IP sudo nmap -A 192.168.50.0/24
Individuato una macchina con indirizzo ip 192.168.50.100 che è l'unica macchina collegata alla rete.

Conferma che l’IP target appartenga a Metasploitable2

Per accertare che sia l’indirizzo IP di Metasploitable2 utilizzare sudo nmap -A 192.168.50.100
Il flag -A in nmap è considerato invasivo. Attivando -A, nmap esegue una scansione approfondita che include: • Rilevamento del sistema operativo: Prova a determinare il sistema operativo del target. • Rilevamento delle versioni dei servizi: Identifica le versioni dei servizi in esecuzione. • Rilevamento degli script: Esegue vari script di scansione per raccogliere informazioni aggiuntive. • Rilevamento degli host: Scansiona per identificare gli host attivi nella rete

Raccolta dati con gli strumenti consigliati

1. nmap -sn -PE <target>

Esegue una scansione di tipo ping per verificare se l'host è online usando pacchetti ICMP Echo Request. nmap -sn -PE 192.168.50.100

- -sn: Questo flag sta per "Scan No Port". Indica a nmap di eseguire una scansione di tipo "Ping" senza eseguire una scansione delle porte. Questo comando è utile per determinare se un host è attivo o meno senza esaminare le porte aperte.
- -PE: Questo flag specifica che nmap deve utilizzare i pacchetti ICMP Echo Request (i classici "ping") per verificare se l'host è raggiungibile. È uno dei metodi che nmap utilizza per effettuare un ping agli host.

2. netdiscover -r <target>

Scansiona la rete 192.168.50.0/24 per scoprire dispositivi attivi. sudo netdiscover -r 192.168.50.0/24

-r 192.168.50.0/24

Specifica l'intervallo di indirizzi IP da scansionare. In questo caso, 192.168.50.0/24 indica una rete con maschera di sottorete 255.255.255.0, che include tutti gli indirizzi IP da 192.168.50.1 a 192.168.50.254.

3. crackmapexec <target>

Esegue una scansione SMB per raccogliere informazioni sul target. crackmapexec smb 192.168.50.100

crackmapexec: È uno strumento di post-exploitation e di gestione della rete utilizzato per eseguire vari tipi di scansioni e test di penetrazione su reti e servizi. SMB 192.168.50.100 445 METASPLOITABLE: Indica che è stato rilevato un servizio SMB in esecuzione sull'indirizzo IP 192.168.50.100 sulla porta 445, e il nome del computer è METASPLOITABLE

4. nmap <target> –top-ports 10 –open

Scansiona le 10 porte più comuni sul target e mostra solo quelle aperte: nmap 192.168.50.100 --top□ports 10 –open

5. nmap <target> -p- -sV –reason –dns-server ns

Nota: per continuare con questo comando, a causa dei limiti imposti da pfSense, da questo punto in poi, le due macchine saranno configurate nella stessa rete interna. Meta 192.168.1.100 Scansionare tutte le porte e identificare i servizi e le versioni. Mostrare il motivo per cui una porta è in uno stato particolare. Utilizzare un server DNS specifico: nmap 192.168.1.100 -p- -sV --reason -- dns-servers 192.168.1.1 in questo caso si è utilizzato il DNS di pfSense. ▪ -p-: Scansiona tutte le porte (da 1 a 65535). ▪ -sV: Rileva le versioni dei servizi in esecuzione sulle porte aperte. ▪ --reason: Mostra il motivo per cui Nmap ha classificato una porta come aperta, chiusa o filtrata. ▪ --dns-servers : Specifica quali server DNS utilizzare per la risoluzione dei nomi durante la scansione.

6. us -mT -Iv <target> :a -r 3000 -R 3 && us -mU -Iv :a -r 3000 -R 3 Nota: dopo il punto precedente la configurazione di Meta mantiene IP a 192.168.1.100 us -mT -Iv 192.168.1.100:a -r 3000 -R 3 && us -mU -Iv 192.168.1.100:a -r 3000 -R 3 Questo comando esegue due scansioni separate sul target con l'indirizzo IP 192.168.1.100 utilizzando lo strumento us. Di seguito è fornita una spiegazione dettagliata di ciascun flag e parametro utilizzato:

I. us: Il nome dello strumento di scansione utilizzato. Non è uno strumento standard, quindi il suo comportamento specifico dipende dalla sua implementazione.

II. -mT: a. -m: Indica il tipo di scansione o protocollo da utilizzare. b. T: Specifica che la scansione deve essere eseguita utilizzando il protocollo TCP.

III. -mU: a. -m: Come sopra, indica il tipo di scansione o protocollo. b. U: Specifica che la scansione deve essere eseguita utilizzando il protocollo UDP.

IV. -Iv: a. -I: Richiede che lo strumento fornisca informazioni dettagliate o approfondite durante la scansione. b. -v: Abilita la modalità verbose, che fornisce informazioni aggiuntive sullo stato e sui risultati della scansione.

V. 192.168.1.100:a: a. 192.168.1.100: L'indirizzo IP del target della scansione. b. :a: Indica che devono essere scansionate tutte le porte disponibili sul target.

VI. -r 3000: a. -r: Specifica un parametro aggiuntivo che potrebbe essere un intervallo di porte, un timeout, o una configurazione di scansione. Il valore 3000 rappresenta il parametro assegnato, il cui significato preciso dipende dalle specifiche dello strumento.

VII. -R 3: a. -R: Definisce un ulteriore parametro configurabile. Potrebbe rappresentare il numero di tentativi, un livello di dettaglio, o un altro valore specifico. b. 3: Il valore assegnato a questo parametro, che indica il numero di tentativi o un altro aspetto della configurazione della scansione.

VIII. &&: Operatore di concatenamento di comandi che esegue il secondo comando solo se il primo comando è completato con successo. Sintesi: Il comando esegue due scansioni sul target 192.168.1.100: • La prima scansione utilizza il protocollo TCP (-mT), mostrando informazioni dettagliate e verbose (-lv), e scansiona tutte le porte (:a), con un intervallo o timeout di 3000 (-r 3000) e un parametro di configurazione 3 (-R 3). • La seconda scansione utilizza il protocollo UDP (-mU), con le stesse opzioni di verbose e dettagli, e gli stessi parametri di intervallo e configurazione. Si ottengono le seguenti informazioni: Lista delle porte TCP e UDP aperte, Versioni dei servizi e Stato delle porte

7. nmap -sS -sV -T4 <target>

nmap -sS -sV -T4 192.168.1.100 • La scansione SYN (-sS) scopre quali porte TCP sono aperte sul target senza completare il processo di handshake TCP completo, rendendo la scansione relativamente discreta. • Il flag version detection (-sV) fornisce informazioni dettagliate sui servizi attivi su ciascuna porta aperta, inclusa la loro versione. • Il flag -T4 velocizza la scansione (più basso è e più stealth)

8. hping3 –scan known <target>

Comando hping3 --scan known 192.168.1.100
hping3 è uno strumento di rete avanzato usato per generare pacchetti TCP/IP personalizzati e condurre varie operazioni di scansione e test di rete. È comunemente usato per eseguire scansioni di porte, test di connettività e verificare la risposta dei sistemi target a specifici pacchetti. --scan: Il flag --scan indica che si vuole eseguire una scansione delle porte sul target. hping3 supporta diversi tipi di scansione, come la scansione di porte specifiche o intervalli di porte. known: Questo parametro, quando associato al flag --scan, specifica che la scansione deve essere limitata alle porte conosciute (well-known ports), che sono le porte numerate da 0 a 1023. Queste porte sono comunemente assegnate a servizi standard (ad esempio, HTTP sulla porta 80, SSH sulla porta 22, etc.)
Il risultato mostra le porte conosciute che non hanno risposto durante la scansione.

9. nc -nvz <target> 1-1024

Utilizzo di Netcat per scansionare le porte 1-1024 e verificare quali sono aperte: nc -nvz 192.168.1.100 1-1024 • -n: Evita la risoluzione DNS, lavorando direttamente con gli indirizzi IP. • -v: Attiva la modalità verbose, fornendo informazioni dettagliate sullo stato di ciascuna porta. • -z: Abilita la modalità zero-I/O, controllando semplicemente se le porte sono aperte o chiuse senza trasferire dati.

10.nc -nv <target> 22

Verificare se la porta 22 è aperta su un target specifico: nc -nv 192.168.1.100 22

11.nmap -sV <target>

Rilevare i servizi in esecuzione su un target specifico: nmap -sV 192.168.1.100

12.db_import <file.xml> (For Metasploit Framework)

Per testare questo comando, bisogna salvare u file una precedente scansione, che potrebbe eseguire con nmap -sV -oX nmap_results.xml 192.168.1.100 il quale salva in xml la scansione del punto 11. -oX nmap_results.xml: Salva i risultati della scansione in formato XML con il nome nmap_results.xml.

Con il comando ls si ritrova il file generato che bisogna importarlo nel framework di Meta. Avviare la modalità di super utente con sudo su e avviare il database PostgreSQL sudo service postgresql start e per la configurazione msfdb init Avviare il framework Metasploit con msfconsole Importare il file xml db_import nmap_results.xml Una volta importato si possono cercare vulnerabilità e/o consultare il documento, che in questo report non si analizzerà.

13.nmap -f –mtu=512

Questo comando è utilizzato per mascherare le scansioni e superare le restrizioni basate sulla dimensione dei pacchetti. nmap -f --mtu=512 192.168.1.100 • -f: Frammenta i pacchetti IP inviati, utile per eludere IDS e firewall. • --mtu=512: Imposta la dimensione massima dei pacchetti a 512 byte

14.masscan <network> -p80 –banners –source-ip <target>

Questo comando è utilizzato per scoprire server HTTP su una rete e raccogliere informazioni sui banner dei servizi, con un IP di origine specifico: masscan 192.168.1.0/24 -p80 --banners -- source-ip 192.168.1.100 • -p80: Scansiona solo la porta 80 (HTTP). • --banners: Rileva e mostra banner dei servizi sui target.

GRAZIE