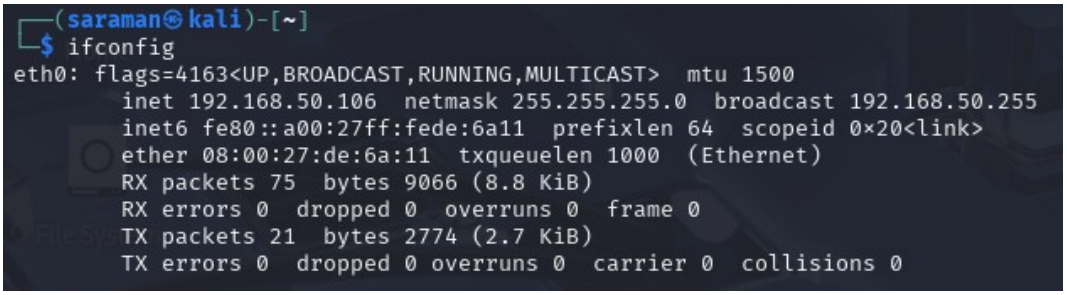
Report esercitazione tecniche di scansione con Nmap W11D1

In questo esercizio dovremo eseguire delle scansioni dalla macchina Kali tramite Nmap con target la macchina Metasploitable 2, le due macchine dovranno essere su reti diverse ed utilizzeremo PfSense come gateway per permettere la comunicazione.

Prerequisiti:

- Configurazione di PfSense:

- Configurazione di Kali:



- Configurazione di Metasploitable 2:

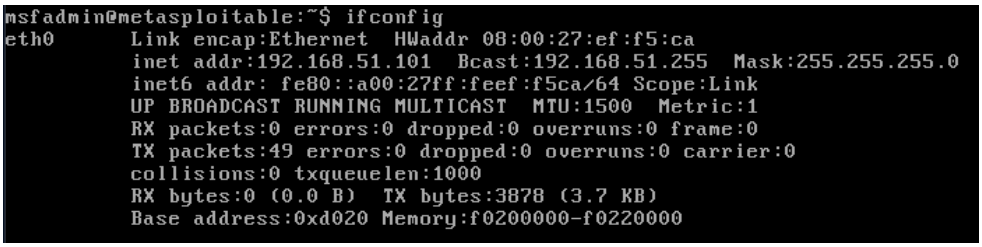


Tabella riassuntiva delle scansioni

Metasploitable 2 IP=192.168.51.101				
Tipo di scansione	Comando eseguito	Scopo scansione	Dettagli	Tempo scansione (secondi)
OS fingerprinting	nmap -O <IP target>	Trovare dettagli sul s.o. del target	23 porte aperte dettagli sul s.o. del target (2 hop compiuti)	19
SYN scan	nmap -sS <IP target>	Esegue una scansione SYN sul target	23 porte aperte	16.74
TCP scan	nmap -sT <IP target>	Esegue una scansione TCP sul target	23 porte aperte	16.89
Version scan	nmap -sV <IP target>	Esegue una scansione TCP sul target specificando la versione dei servizi	23 porte aperte e relativi servizi	189.35

Tabella dettagliata delle scansioni

Metasploitable 2 IP=192.168.51.101			
Sistema operativo=Linux 2.6.X			
N. Porta	Servizio in ascolto	Versione servizio	Descrizione servizio
21	FTP	Vsftp 2.3.4	Trasferimento file
22	SSH	Open SSH 4.7p1 debian 8ubuntu1 (protocol 2.0)	Accesso remoto (cifrato)
23	Telnet	Linux telnetd	Accesso remoto (non cifrato)
25	SMTP	Postfix smtpd	Invio mail
53	DNS	ISC BIND 9.4.2	Risoluzione nome dominio
80	HTTP	Apache httpd 2.2.8 ((ubuntu) dav/2)	Trasferimento dati sul web (non cifrato)
111	RPCbind	2 (RPC #100000)	Binding di servizi RPC alle porte
139	Netbios-SSN	Samba smbd 3.X – 4.X (workgroup: WORKGROUP)	Gestisce sessioni di rete tra macchine Windows per la condivisione di risorse (tramite Netbios)
445	Microsoft-DS	Samba smbd 3.X – 4.X (workgroup: WORKGROUP)	Gestisce sessioni di rete tra macchine Windows per la condivisione di risorse (tramite Microsoft-DS)
512	Exec	Netkit-rsh rexecd	Esecuzione comandi da remoto tramite RSH
513	Login		Accesso remoto ad un terminale tramite Rlogin
514	Shell	Netkit rshd	Accesso remoto ad un terminale tramite RSH
1099	RMIregistry	GNU Classpath grmiregistry	Registra oggetti remoti e permette ai client di trovarli tramite nome (framework Java)
1524	Ingreslock	Metasploitable root shell	Aiuta a gestire operazione concorrenti per evitare modifiche non sincronizzate (database Ingres)
2049	NFS	2-4 (RPC #100003)	Accesso remoto a file e directories tra computer su una rete
2121	CCproxy-FTP		Gestione traffico FTP tramite server proxy

3306	MySQL	MySQL 5.0.51a-3ubuntu5	Database per gestione dati tramite linguaggio SQL
5432	PostgresQL	PostgreSQL DB 8.3.0 - 8.3.7	Database per gestione dati tramite linguaggio SQL (anche dati non strutturati)
5900	VNC	VNC (protocol 3.3)	Desktop remoto tramite rete
6000	X11	(access denied)	Gestione app grafiche su sistemi Unix e simili
6667	IRC	UnrealIRCd	Comunicazione tramite messaggistica istantanea
8009	AJP13	Apache Jserv (protocol v1.3)	Comunicazione tra server web e applicativo per facilitare la gestione richieste HTTP
8180	Unknown (HTTP)	Apache Tomcat/Coyote JSP engine 1.1	Accesso a web app su Apache Tomcat tramite HTTP

Facoltativo

Ripetere le scansioni ma questa volta le due macchine dovranno essere sulla stessa rete, annotare le differenze trovate in una tabella.

Differenze scansioni		
Tipo scansione	Stessa rete: Meta=192.168.50.101 Kali=192.168.50.106	Reti diverse: Meta=192.168.51.101 Kali=192.168.50.106
-O	Tempo impiegato: 14.74 sec. 1 hop Latenza: 0.0035 sec Info MAC address	Tempo impiegato: 19 sec. 2 hop Latenza: 0,043 sec
-sS	Tempo impiegato: 13.39 sec Latenza: 0.004 sec Info MAC address	Tempo impiegato: 16.74 sec Latenza: 0.11 sec
-sT	Tempo impiegato: 13.31 sec Latenza: 0.017 sec Info MAC address	Tempo impiegato: 16.89 sec Latenza: 0.045 sec
-sV	Tempo impiegato: 65.84 sec Latenza: 0.0063 sec Info MAC address Trovata versione protocollo porta 2121-ProFTPD 1.3.1	Tempo impiegato: 189.35 sec Latenza: 0.21 sec