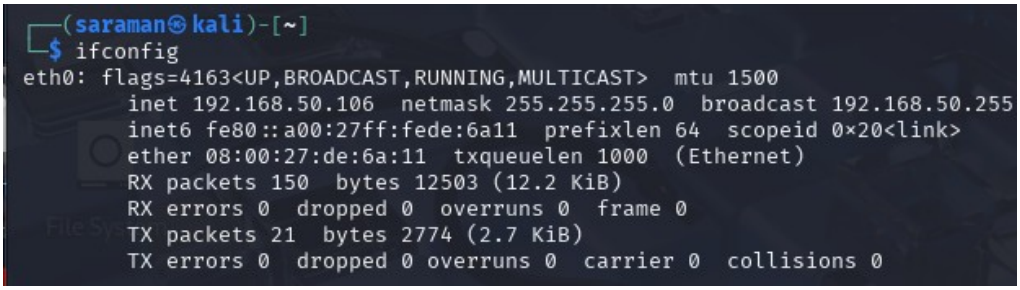
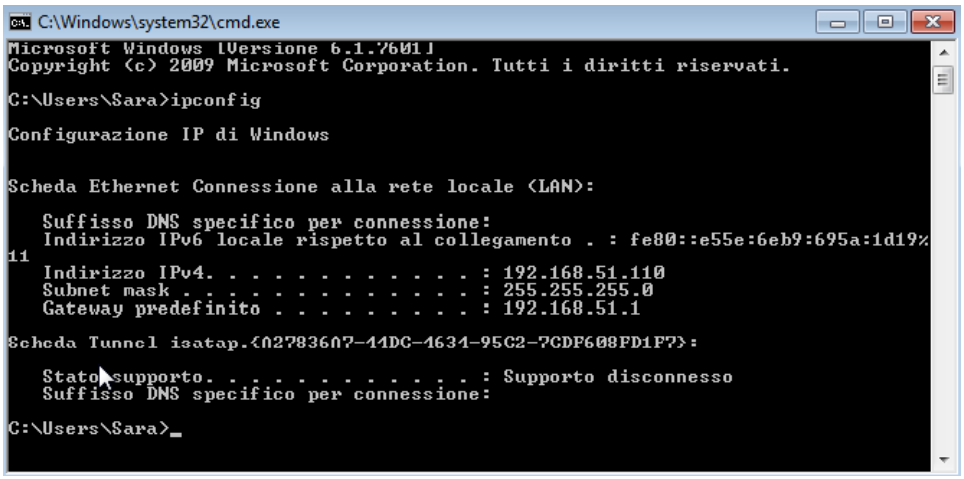
Report scansione con Nmap di Windows 7 W11D4

In questo esercizio dovremo effettuare delle scansioni sulla macchina di Windows 7 tramite comandi Nmap lanciati dalla macchina Kali, le due VM saranno su reti diverse e comunicheranno grazie a PfSense.
Dovremo prima scansionare con il firewall di Windows 7 abilitato e poi ripeteremo le scansioni a firewall disabilitato, annoteremo tutti i rilevamenti in delle tabelle riassuntive.

Configurazione di Kali:



Configurazione di Windows:



Configurazione di PfSense:

Scansione con firewall Windows abilitato

Windows 7 IP=192.168.51.110				
Tipo di scansione	Comando eseguito	Scopo scansione	Dettagli	Tempo scansione (secondi)
OS fingerprinting	nmap -O <IP target>	Trovare dettagli sul s.o. del target	Target non visibile	3.79
SYN scan	nmap -sS <IP target>	Esegue una scansione SYN sul target	Target non visibile	4.01
TCP scan	nmap -sT <IP target>	Esegue una scansione TCP sul target	Target non visibile	3.21
Version scan	nmap -sV <IP target>	Esegue una scansione TCP sul target specificando la versione dei servizi	Target non visibile	5.11

Scansione con firewall Windows disabilitato

Windows 7 IP=192.168.51.110				
Tipo di scansione	Comando eseguito	Scopo scansione	Dettagli	Tempo scansione (secondi)
OS fingerprinting	nmap -O <IP target>	Trovare dettagli sul s.o. del target	13 porte aperte Dettagli S.O. 2 hops	19.36
SYN scan	nmap -sS <IP target>	Esegue una scansione SYN sul target	13 porte aperte	16.68
TCP scan	nmap -sT <IP target>	Esegue una scansione TCP sul target	13 porte aperte	18.24
Version scan	nmap -sV <IP target>	Esegue una scansione TCP sul target specificando la versione dei servizi	13 porte aperte e relativi servizi Info hostname Info S.O.	143.98

Dettaglio scansioni con firewall Windows disabilitato

Windows 7 IP=192.168.51.110			
Sistema operativo=Microsoft Windows server 2008/ 7 /Vista			
Host info=SARA-PC OS=Windows CPE=cpe:/o:microsoft:windows			
N. Porta	Servizio in ascolto	Versione servizio	Descrizione servizio
135	MSRPC	Microsoft Windows RPC	Permette a programmi Windows di comunicare tra loro o con altre macchine in rete eseguendo comandi o servizi da remoto
139	netbios-SSN	Microsoft Windows netbios-SSN	Gestisce sessioni di rete tra macchine Windows per la condivisione di risorse (tramite Netbios)
445	Microsoft-DS	Microsoft Windows 7-10 Microsoft-DS	Gestisce sessioni di rete tra macchine Windows per la condivisione di risorse (tramite Microsoft-DS)
554	RTSP	-	Controlla lo streaming di contenuti multimediali in tempo reale
2869	HTTP	Microsoft HTTPAPI HTTPD 2.0	Trasferimento dati sul web (non cifrato)
5357	HTTP	Microsoft HTTPAPI HTTPD 2.0	Trasferimento dati sul web (non cifrato)
10243	HTTP	Microsoft HTTPAPI HTTPD 2.0	Trasferimento dati sul web (non cifrato)
49152	MSRPC	Microsoft Windows RPC	Microsoft remote procedure call
49153	MSRPC	Microsoft Windows RPC	Microsoft remote procedure call
49154	MSRPC	Microsoft Windows RPC	Microsoft remote procedure call
49155	MSRPC	Microsoft Windows RPC	Microsoft remote procedure call
49156	MSRPC	Microsoft Windows RPC	Microsoft remote procedure call
49159	MSRPC	Microsoft Windows RPC	Microsoft remote procedure call

Facoltativo

Ripetere le scansioni nelle modalità viste in precedenza, ma spostando entrambe le macchine sulla stessa rete.
Evidenziare le eventuali differenze in una tabella.

Windows 7 IP=192.168.50.110		
Comando	Firewall abilitato	Firewall disabilitato
nmap -O	Dettagli MAC address 1 hop 1000 porte senza risposta 47.47 sec	Dettagli MAC address 1 hop 9 porte aperte trovate 16.26 sec Dettagli S.O.
nmap -sS	Dettagli MAC address 1000 porte senza risposta 45.51 sec	Dettagli MAC address 9 porte aperte trovate 13.70 sec
nmap -sT	Dettagli MAC address 1000 porte senza risposta 45.98 sec	Dettagli MAC address 9 porte aperte trovate 14.36 sec
nmap -sV	Dettagli MAC address 1000 porte senza risposta 43.63 sec	Dettagli MAC address 9 porte aperte trovate con relative versioni dei servizi 73.95 sec

Dettaglio scansioni con firewall Windows disabilitato (VM sulla stessa rete)

Windows 7 IP=192.168.50.110			
Sistema operativo=Microsoft Windows Vista/ 7/ Server 2008/ 8.1			
Host info=SARA-PC OS=Windows CPE=cpe:/o:microsoft:windows			
N. Porta	Servizio in ascolto	Versione servizio	Descrizione servizio
135	MSRPC	Microsoft Windows RPC	Permette a programmi Windows di comunicare tra loro o con altre macchine in rete eseguendo comandi o servizi da remoto
139	netbios-SSN	Microsoft Windows netbios-SSN	Gestisce sessioni di rete tra macchine Windows per la condivisione di risorse (tramite Netbios)
445	Microsoft-DS	Microsoft Windows 7-10 Microsoft-DS	Gestisce sessioni di rete tra macchine Windows per la condivisione di risorse (tramite Microsoft-DS)
5357	HTTP	Microsoft HTTPAPI HTTPD 2.0	Trasferimento dati sul web (non cifrato)
49152	MSRPC	Microsoft Windows RPC	Microsoft remote procedure call
49153	MSRPC	Microsoft Windows RPC	Microsoft remote procedure call
49154	MSRPC	Microsoft Windows RPC	Microsoft remote procedure call
49155	MSRPC	Microsoft Windows RPC	Microsoft remote procedure call
49156	MSRPC	Microsoft Windows RPC	Microsoft remote procedure call