Report di Scansione Nmap su Windows 7

Informazioni Generali

- **IP Target**: 192.168.50.102
- **IP Source**: 192.168.50.100
- **Scopo della Scansione**: Identificazione e valutazione delle misure di sicurezza, determinazione del sistema operativo, e rilevamento di porte aperte e servizi.

Risultati della Scansione

1. **Indirizzo IP**
    - IP Target: **192.168.50.102**
    - IP Source: 192.168.50.100
2. **Sistema Operativo**
    - Tentativi di determinazione tramite OS fingerprinting sono stati inconcludenti a causa delle porte filtrate che hanno impedito una determinazione accurata.
3. **Porte Aperte**
    - Non sono state rilevate porte aperte. Tutte le scansioni hanno mostrato le porte come "filtered" o non hanno ricevuto risposta, indicativo di un firewall.
4. **Servizi in Ascolto con Versione**
    - Non è stato possibile identificare servizi specifici o le loro versioni a causa delle restrizioni imposte sulle porte.
5. **Descrizione dei Servizi**
    - A causa delle porte filtrate e dell'assenza di risposta, non è stato possibile raccogliere dettagli sui servizi in esecuzione sul target.

Dettaglio delle Scansioni Effettuate

Ogni comando Nmap è seguito da una descrizione dettagliata del suo scopo e dei risultati ottenuti.

Scansione TCP SYN

- **Comando**: **sudo nmap -sS -T4 -Pn 192.168.50.102**
- **Descrizione**: Utilizzata per identificare rapidamente porte aperte senza completare la connessione TCP.
- **Risultato**: Nessuna porta aperta rilevata; tutte risultano "filtered".

OS Fingerprinting

- **Comando**: **sudo nmap -O 192.168.50.102**
- **Descrizione**: Tentativo di determinare il sistema operativo del host tramite caratteristiche specifiche delle risposte ai pacchetti.

- **Risultato**: Fallito a causa delle porte filtrate che hanno bloccato le risposte necessarie per l'analisi.

ACK Scan

- **Comando**: **sudo nmap -sA 192.168.50.102**
- **Descrizione**: Utilizzata per mappare le regole di filtraggio del firewall verificando come vengono trattati i pacchetti TCP ACK.
- **Risultato**: Conferma che tutte le porte sono filtrate.

Scansione con Pacchetti Frammentati

- **Comando**: **sudo nmap --mtu 24 --badsum 192.168.50.102**
- **Descrizione**: Scansione progettata per eludere i firewall che filtrano basandosi su caratteristiche specifiche dei pacchetti.
- **Risultato**: Nessun successo, tutte le porte continuano a risultare filtrate.

Scansione mirata su Porte Critiche

- **Comando**: **sudo nmap -p 445,3389,1433 192.168.50.102**
- **Descrizione**: Concentrata su porte note per essere usate da servizi critici come SMB, RDP, e SQL Server.
- **Risultato**: Tutte filtrate, indicando una protezione specifica su queste porte ad alto rischio.

Utilizzo degli Script NSE per Vulnerabilità

- **Comando**: **sudo nmap --script "vuln" 192.168.50.102**
- **Descrizione**: Esegue script per identificare vulnerabilità note nei servizi rilevati.
- **Risultato**: Nessuna vulnerabilità trovata a causa della mancanza di risposta delle porte.

Conclusioni

Le misure di sicurezza del target sono robuste, con tutte le porte che appaiono come filtrate e nessuna risposta significativa ottenuta dalle scansioni. Questo suggerisce la presenza di un firewall configurato per non rispondere a scansioni non autorizzate, rendendo molto difficile qualsiasi forma di rilevamento a distanza del sistema operativo, delle porte aperte, o dei servizi in esecuzione.

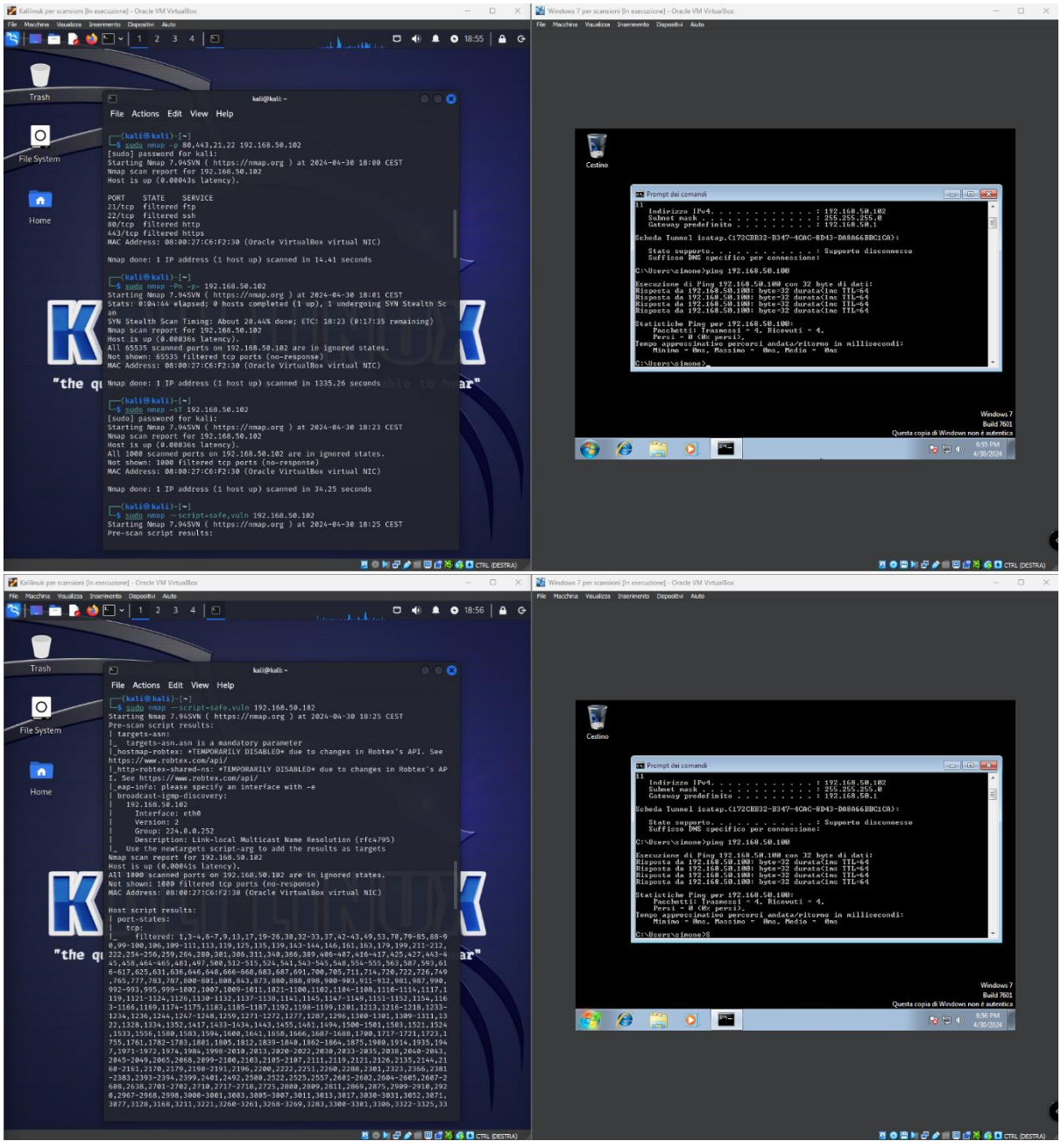
Soluzioni Proposte per Continuare le Scansioni

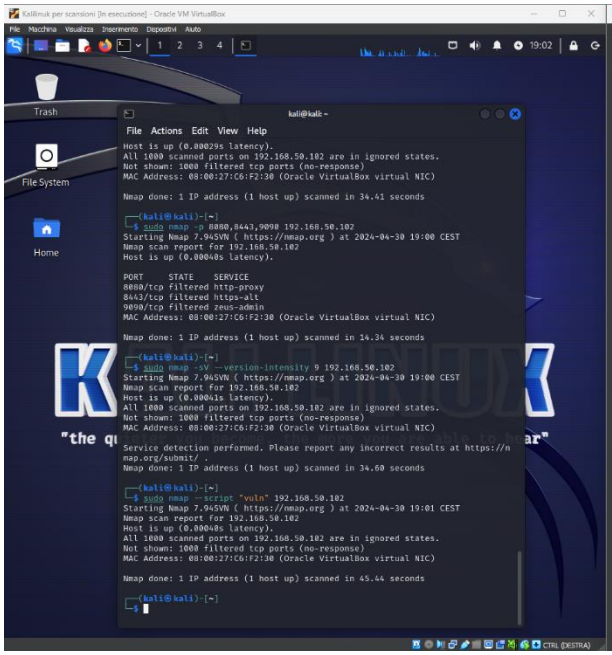
- **Scansione Passiva**: Utilizzare strumenti come Wireshark per catturare traffico passivo e identificare comunicazioni non filtrate.

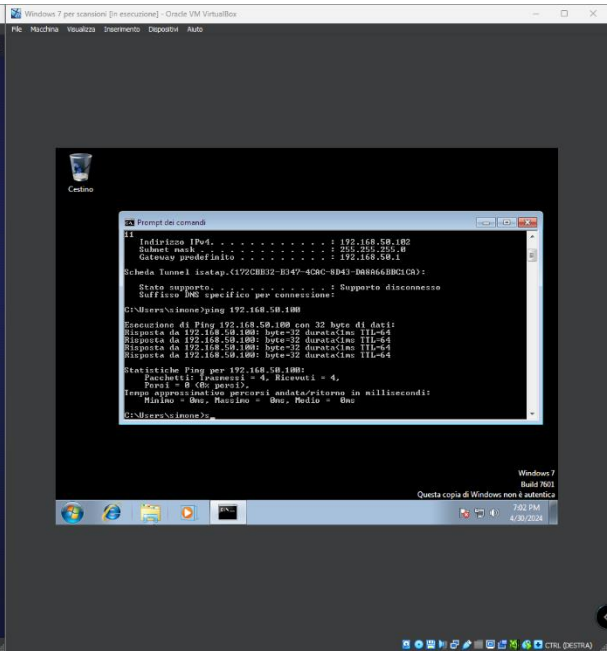
Usare scansioni più stealth:

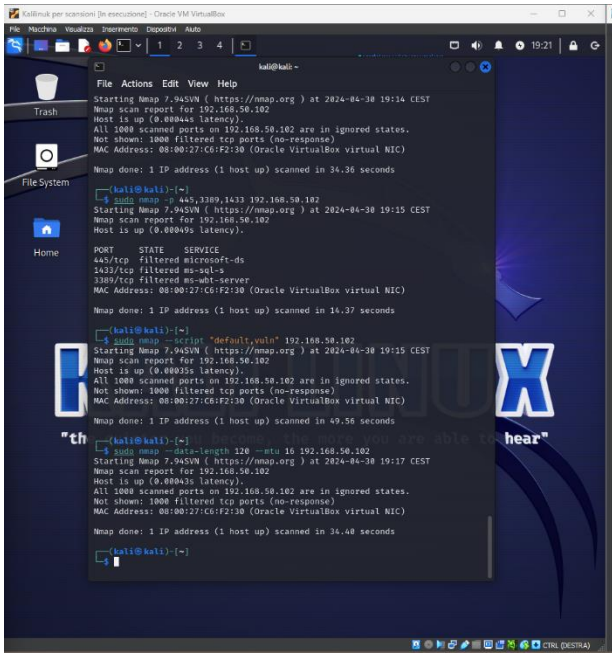
- sudo nmap -p 80,443,21,22 192.168.50.102
- sudo nmap --script=safe,vuln 192.168.50.102
- sudo nmap -p 8080,8443,9090 192.168.50.102
- sudo nmap -p 445,3389,1433 192.168.50.102

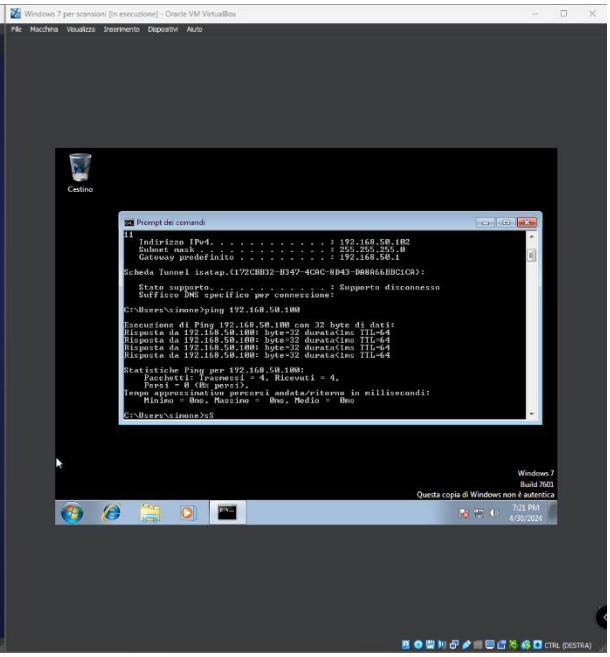
Screenshot


Kalilinuk per scansioni [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo nmap -p 80,443,21,22 192.168.50.102
[sudo] password for kali:
Starting Nmap 7.94SVN (https://nmap.org) at 2024-04-30 18:00 CEST
Nmap scan report for 192.168.50.102
Host is up (0.00043s latency).
PORT STATE SERVICE
21/tcp filtered ftp
22/tcp filtered ssh
80/tcp filtered http
443/tcp filtered https
MAC Address: 08:00:27:C6:F2:30 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 14.41 seconds
(kali㉿kali)-[~]
$ sudo nmap -Pn -sF 192.168.50.102
Starting Nmap 7.94SVN (https://nmap.org) at 2024-04-30 18:01 CEST
Stats: 0:04:44 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 20.44% done; ETC: 18:23 (0:17:35 remaining)
Nmap scan report for 192.168.50.102
Host is up (0.00036s latency).
All 65535 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 65535 filtered tcp ports (no-response)
MAC Address: 08:00:27:C6:F2:30 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 1335.26 seconds
(kali㉿kali)-[~]
$ sudo nmap -sI 192.168.50.102
[sudo] password for kali:
Starting Nmap 7.94SVN (https://nmap.org) at 2024-04-30 18:23 CEST
Nmap scan report for 192.168.50.102
Host is up (0.00036s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:C6:F2:30 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 34.25 seconds
(kali㉿kali)-[~]
$ sudo nmap --script=safe,vuln 192.168.50.102
Starting Nmap 7.94SVN (https://nmap.org) at 2024-04-30 18:25 CEST
Pre-scan script results:
Windows 7 per scansioni [In esecuzione] - Oracle VM VirtualBox
Cestino
Prompt dei comandi
Indirizzo IPv4. . . . . : 192.168.50.102
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.50.1
Scheda Tunnel isatap.{172CBB32-B347-4CAC-8D43-D88A66BBC1CA}:
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:
C:\Users\simone>ping 192.168.50.100
Esecuzione di Ping 192.168.50.100 con 32 byte di dati:
Risposta da 192.168.50.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.50.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.50.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.50.100: byte=32 durata<1ms TTL=64
Statistiche Ping per 192.168.50.100:
Pacchetti: Trasmessi = 4, Ricevuti = 4,
Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo = 0ms, Massimo = 0ms, Media = 0ms
C:\Users\simone>_
Windows 7
Build 7601
Questa copia di Windows non è autentica
6:55 PM
4/30/2024
CTRL (DESTRA)
Kalilinuk per scansioni [In esecuzione] - Oracle VM VirtualBox
Starting Nmap 7.94SVN (https://nmap.org) at 2024-04-30 18:25 CEST
Pre-scan script results:
| targets-asn:
|_ targets-asn.asn is a mandatory parameter
| hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
|_eap-info: please specify an interface with -e
| broadcast-igmp-discovery:
| 192.168.50.102
| Interface: eth0
| Version: 2
| Group: 224.0.0.252
| Description: Link-local Multicast Name Resolution (rfc4795)
|_ Use the newtargets script-arg to add the results as targets
Nmap scan report for 192.168.50.102
Host is up (0.00041s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:C6:F2:30 (Oracle VirtualBox virtual NIC)
Host script results:
| port-states:
| tcp:
|_ filtered: 1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,280,301,306,311,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,500,512-515,524,541,543-545,548,554-555,563,587,593,616-617,625,631,636,646,648,666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,843,873,880,888,898,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-1011,1021-1100,1102,1104-1108,1110-1114,1117,1119,1121-1124,1126,1130-1132,1137-1138,1141,1145,1147-1149,1153-1154,1163-1166,1169,1174-1175,1183,1185-1187,1192,1198-1199,1201,1213,1216-1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,1277,1287,1296,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1500-1501,1503,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,1666,1687-1688,1700,1717-1721,1723,1755,1761,1782-1783,1801,1805,1812,1839-1840,1862-1864,1875,1900,1914,1935,1947,1971-1972,1974,1984,1998-2010,2013,2020-2022,2030,2033-2035,2038,2040-2043,2045-2049,2065,2068,2099-2100,2103,2105-2107,2111,2119,2121,2126,2135,2144,2160-2161,2170,2179,2190-2191,2196,2200,2222,2251,2260,2288,2301,2323,2366,2381-2383,2393-2394,2399,2401,2492,2500,2522,2525,2557,2601-2602,2604-2605,2607-2608,2638,2701-2702,2710,2717-2718,2725,2800,2809,2811,2869,2875,2909-2910,2920,2967-2968,2998,3000-3001,3003,3005-3007,3011,3013,3017,3030-3031,3052,3071,3077,3128,3168,3211,3221,3260-3261,3268-3269,3283,3300-3301,3306,3322-3325,33
Windows 7 per scansioni [In esecuzione] - Oracle VM VirtualBox
Cestino
Prompt dei comandi
Indirizzo IPv4. . . . . : 192.168.50.102
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.50.1
Scheda Tunnel isatap.{172CBB32-B347-4CAC-8D43-D88A66BBC1CA}:
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:
C:\Users\simone>ping 192.168.50.100
Esecuzione di Ping 192.168.50.100 con 32 byte di dati:
Risposta da 192.168.50.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.50.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.50.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.50.100: byte=32 durata<1ms TTL=64
Statistiche Ping per 192.168.50.100:
Pacchetti: Trasmessi = 4, Ricevuti = 4,
Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo = 0ms, Massimo = 0ms, Media = 0ms
C:\Users\simone>^C
Windows 7
Build 7601
Questa copia di Windows non è autentica
6:56 PM
4/30/2024
CTRL (DESTRA)


Kalilinux per scansioni [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:C6:F2:30 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 34.41 seconds
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p 8080,8443,9090 192.168.50.102
Starting Nmap 7.945VN (https://nmap.org) at 2024-04-30 19:00 CEST
Nmap scan report for 192.168.50.102
Host is up (0.00064s latency).
PORT STATE SERVICE
8080/tcp filtered http-proxy
8443/tcp filtered https-alt
9090/tcp filtered zeus-admin
MAC Address: 08:00:27:C6:F2:30 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 14.34 seconds
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV --version-intensity 9 192.168.50.102
Starting Nmap 7.945VN (https://nmap.org) at 2024-04-30 19:00 CEST
Nmap scan report for 192.168.50.102
Host is up (0.00041s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:C6:F2:30 (Oracle VirtualBox virtual NIC)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.60 seconds
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script "vuln" 192.168.50.102
Starting Nmap 7.945VN (https://nmap.org) at 2024-04-30 19:01 CEST
Nmap scan report for 192.168.50.102
Host is up (0.00040s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:C6:F2:30 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 45.44 seconds
┌──(kali㉿kali)-[~]
CTRL (DESTRA)


Windows 7 per scansioni [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Cestino
Prompt dei comandi
Indirizzo IPv4. . . . . : 192.168.50.102
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.50.1
Scheda Tunnel isatap.{172CBB32-B347-4C8C-8D43-D88A66BBC1CA}:
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:
C:\Users\simone>ping 192.168.50.100
Esecuzione di Ping 192.168.50.100 con 32 byte di dati:
Risposta da 192.168.50.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.50.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.50.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.50.100: byte=32 durata<1ms TTL=64
Statistiche Ping per 192.168.50.100:
Pacchetti: Inviati = 4, Ricevuti = 4,
Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo = 0ms, Massimo = 0ms, Medio = 0ms
C:\Users\simone>s_
Windows 7
Build 7601
Questa copia di Windows non è autentica
7:02 PM
4/30/2024
CTRL (DESTRA)


Kalilinux per scansioni [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
Starting Nmap 7.945VN (https://nmap.org) at 2024-04-30 19:14 CEST
Nmap scan report for 192.168.50.102
Host is up (0.00044s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:C6:F2:30 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 34.36 seconds
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p 445,3389,1433 192.168.50.102
Starting Nmap 7.945VN (https://nmap.org) at 2024-04-30 19:15 CEST
Nmap scan report for 192.168.50.102
Host is up (0.00049s latency).
PORT STATE SERVICE
445/tcp filtered microsoft-ds
1433/tcp filtered ms-sql-s
3389/tcp filtered ms-wbt-server
MAC Address: 08:00:27:C6:F2:30 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 14.37 seconds
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script "default,vuln" 192.168.50.102
Starting Nmap 7.945VN (https://nmap.org) at 2024-04-30 19:15 CEST
Nmap scan report for 192.168.50.102
Host is up (0.00035s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:C6:F2:30 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 49.56 seconds
┌──(kali㉿kali)-[~]
└─$ sudo nmap --data-length 120 --mtu 16 192.168.50.102
Starting Nmap 7.945VN (https://nmap.org) at 2024-04-30 19:17 CEST
Nmap scan report for 192.168.50.102
Host is up (0.00043s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:C6:F2:30 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 34.40 seconds
┌──(kali㉿kali)-[~]
CTRL (DESTRA)


Windows 7 per scansioni [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Cestino
Prompt dei comandi
Indirizzo IPv4. . . . . : 192.168.50.102
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.50.1
Scheda Tunnel isatap.{172CBB32-B347-4C8C-8D43-D88A66BBC1CA}:
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:
C:\Users\simone>ping 192.168.50.100
Esecuzione di Ping 192.168.50.100 con 32 byte di dati:
Risposta da 192.168.50.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.50.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.50.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.50.100: byte=32 durata<1ms TTL=64
Statistiche Ping per 192.168.50.100:
Pacchetti: Inviati = 4, Ricevuti = 4,
Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo = 0ms, Massimo = 0ms, Medio = 0ms
C:\Users\simone>s
Windows 7
Build 7601
Questa copia di Windows non è autentica
7:21 PM
4/30/2024
CTRL (DESTRA)

Sintassi per comandi più aggressivi

-f; --mtu <val>: fragment packets (optionally w/given MTU)

-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys

-S <IP_Address>: Spoof source address

-e <iface>: Use specified interface

-g/--source-port <portnum>: Use given port number

--proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies

--data <hex string>: Append a custom payload to sent packets

--data-string <string>: Append a custom ASCII string to sent packets

--data-length <num>: Append random data to sent packets

--ip-options <options>: Send packets with specified ip options

--ttl <val>: Set IP time-to-live field

--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address

--badsum: Send packets with a bogus TCP/UDP/SCTP checksum

nmap -p 445 --script smb-vuln-ms17-010 <target_ip>

nmap -sS -e vmnet 8 -s "ip falso" "ip target" -p21,990

nmap -sS vmnet8 -S 192.168.1.10 -p 21,990 192.168.1.4 192.168.1.8

nmap -T4 -A -V "iptarget"

Nmap -n -PN -sT -sU -p- "iptarget"

sudo nmap -sU -sS --script smb-enum-shares.nse -p U:137,T:139 192.168.50.101

sudo nmap -sS -O -S 192.168.0.210 -Pn 192.168.0.120 -e eth0 -p 21,990

sudo nmap -sS -O -S 192.168.0.210 -Pn 192.168.0.120 -e eth0 -p 21,990

sistema target **192.168.50.102**:

1. Scansione Aggressiva con OS e Servizi Detection

Questo comando combina la rilevazione del sistema operativo, la versione dei servizi, gli script Nmap e il traceroute per una visione approfondita:

bash

Copy code

sudo nmap -sS -A -T4 -v -Pn 192.168.50.102

- **-sS**: Scansione SYN stealth.
- **-A**: Abilita OS detection, version detection, script scanning e traceroute.
- **-T4**: Imposta il timing template a "aggressive" per velocizzare la scansione.
- **-v**: Aumenta la verbosità per dettagli aggiuntivi sui processi di scansione.
- **-Pn**: Disabilita la scoperta host, assumendo che il target sia up.

2. Scansione con Tecniche di Evasione Firewall

Se sospetti che il firewall stia bloccando scansioni attive, usa tecniche di evasione come il frammentamento dei pacchetti e lo spoofing dell'IP:

bash

Copy code

sudo nmap -sS -f --mtu 24 -D RND:10 -S 192.168.50.100 -Pn -T4 192.168.50.102

- **-f** e **--mtu 24**: Frammenta i pacchetti per bypassare i firewall.
- **-D RND:10**: Utilizza 10 decoy per mascherare l'origine della scansione.
- **-S 192.168.50.100**: Spoofing dell'IP sorgente, usando il tuo indirizzo Kali come sorgente.
- **-T4**: Usa un template di timing aggressivo.

3. Scansione di Porte Specifiche con Verbose e Debugging

Se desideri concentrarti su porte specifiche che possono essere critiche:

bash

Copy code

sudo nmap -sV -p 21,22,80,443,139,445,3389 -v -d -Pn 192.168.50.102

- **-sV**: Prova a determinare la versione dei servizi in esecuzione sulle porte aperte.
- **-p 21,22,80,443,139,445,3389**: Specifica le porte comuni di interesse.
- **-v** e **-d**: Aumentano verbosità e debugging per dettagli più tecnici.

4. Scansione Completa delle Porte

Per una mappatura completa delle porte TCP aperte:

bash

Copy code

sudo nmap -p 1-65535 -sS -T4 -A -v -Pn 192.168.50.102

- **-p 1-65535**: Scansiona tutte le porte TCP da 1 a 65535.
- **-sS**, **-A**, **-T4**, **-v**, **-Pn**: Come sopra, per una scansione dettagliata e aggressiva.

Scansione con Evasione Avanzata

Utilizza tecniche di evasione più avanzate per tentare di bypassare il firewall o i filtri IDS/IPS:

bash

Copy code

sudo nmap -sS -T4 --script "firewalk" --badsum -Pn 192.168.50.102

--script "firewalk": Questo script tenta di scoprire quali porte sono filtrate utilizzando una tecnica simile al tracerouting.

--badsum: Invia pacchetti con un checksum TCP/UDP/SCTP errato per confondere gli IDS passivi.

Scansione Intensiva di OS Detection

Una scansione più intensa del sistema operativo potrebbe rivelare qualche informazione aggiuntiva non rilevata da scansioni più superficiali:

bash

Copy code

sudo nmap -O --osscan-guess --osscan-limit -Pn 192.168.50.102

--osscan-guess: Fa supposizioni più aggressive su quale OS potrebbe essere.

--osscan-limit: Limita la scansione OS ai target più probabili di rispondere.

Scansione Stealth Modificata

Combina tecniche stealth con scansione aggressiva dei servizi:

bash

Copy code

sudo nmap -sS -sV --version-intensity 9 -Pn -T2 192.168.50.102

--version-intensity 9: Imposta l'intensità della scansione dei servizi al massimo per ottenere il maggior numero di dettagli possibile.

-T2: Riduce la velocità della scansione per evitare di innescare i sensori di sicurezza.

Utilizzo di Nmap Scripts per Scansione Avanzata

Usa NSE (Nmap Scripting Engine) per eseguire script che potrebbero rivelare vulnerabilità o configurazioni:

bash

Copy code

sudo nmap --script "vuln" -p 445,139 192.168.50.102

--script "vuln": Esegue tutti gli script di vulnerabilità disponibili su porte specifiche.

1. Scansione Aggressiva con Evasione IDS

Questa scansione utilizza diverse tecniche di evasione per tentare di bypassare l'IDS e il firewall:

bash

Copy code

sudo nmap -sS -T4 --min-rate 100 --max-retries 1 --defeat-rst-ratelimit --reason -Pn --script "(safe or default) and not broadcast" 192.168.50.102

- **-sS**: Utilizza una scansione TCP SYN stealth.
- **-T4**: Aumenta la velocità della scansione.
- **--min-rate 100**: Imposta un minimo di 100 pacchetti al secondo per accelerare la scansione.
- **--max-retries 1**: Riduce i tentativi di riconnessione a 1 per ridurre le tracce.
- **--defeat-rst-ratelimit**: Cerca di eludere i limiti imposti dai firewall sugli RST.
- **--reason**: Mostra il motivo per cui una porta è in uno stato specifico.
- **-Pn**: Assume che l'host sia online, disabilitando la scoperta host.
- **--script**: Utilizza script NSE che sono considerati "sicuri" o "default", escludendo gli script che si comportano come un broadcast.

2. Scansione di Vulnerabilità e Configurazione

Utilizzare gli script NSE per cercare specifiche vulnerabilità e configurazioni sbagliate:

bash

Copy code

sudo nmap -p 1-65535 -sV --version-intensity 9 --script=vulners --script-args mincvss=5.0 192.168.50.102

- **-p 1-65535**: Scansiona tutte le porte.
- **-sV --version-intensity 9**: Esegue una scansione approfondita della versione dei servizi.
- **--script=vulners**: Utilizza lo script "vulners" per cercare vulnerabilità note basate sulle versioni dei servizi identificate.
- **--script-args mincvss=5.0**: Filtra le vulnerabilità segnalate con un punteggio CVSS minimo di 5.0.

3. Scansione Stealth Modificata per Evasione

Utilizzare una combinazione di tecniche stealth per ridurre la possibilità di rilevamento:

bash

Copy code

sudo nmap -sS -T2 --data-length 200 --badsum -f --randomize-hosts 192.168.50.102

- **-sS**: Scansione SYN stealth.

- **-T2**: Diminuisce la velocità della scansione per essere meno aggressivi e più difficili da rilevare.
- **--data-length 200**: Aggiunge 200 byte di dati casuali ai pacchetti per confondere gli IDS.
- **--badsum**: Invia pacchetti con checksum TCP/UDP/SCTP invalidi.
- **-f**: Frammenta i pacchetti.
- **--randomize-hosts**: Randomizza l'ordine di scansione degli host se più target sono specificati.

4. Scansione con Autenticazione

Se hai credenziali valide, puoi utilizzarle per effettuare scansioni più approfondite:

bash

Copy code

sudo nmap -sU -sS --script auth,brute,exploit -p 20-25,80,443,3389 192.168.50.102

- **-sU -sS**: Combinazione di scansioni TCP SYN e UDP.
- **--script**: Specifica script per autenticazione, attacchi brute force e tentativi di exploit.
- **-p 20-25,80,443,3389**: Specifica le porte di interesse.