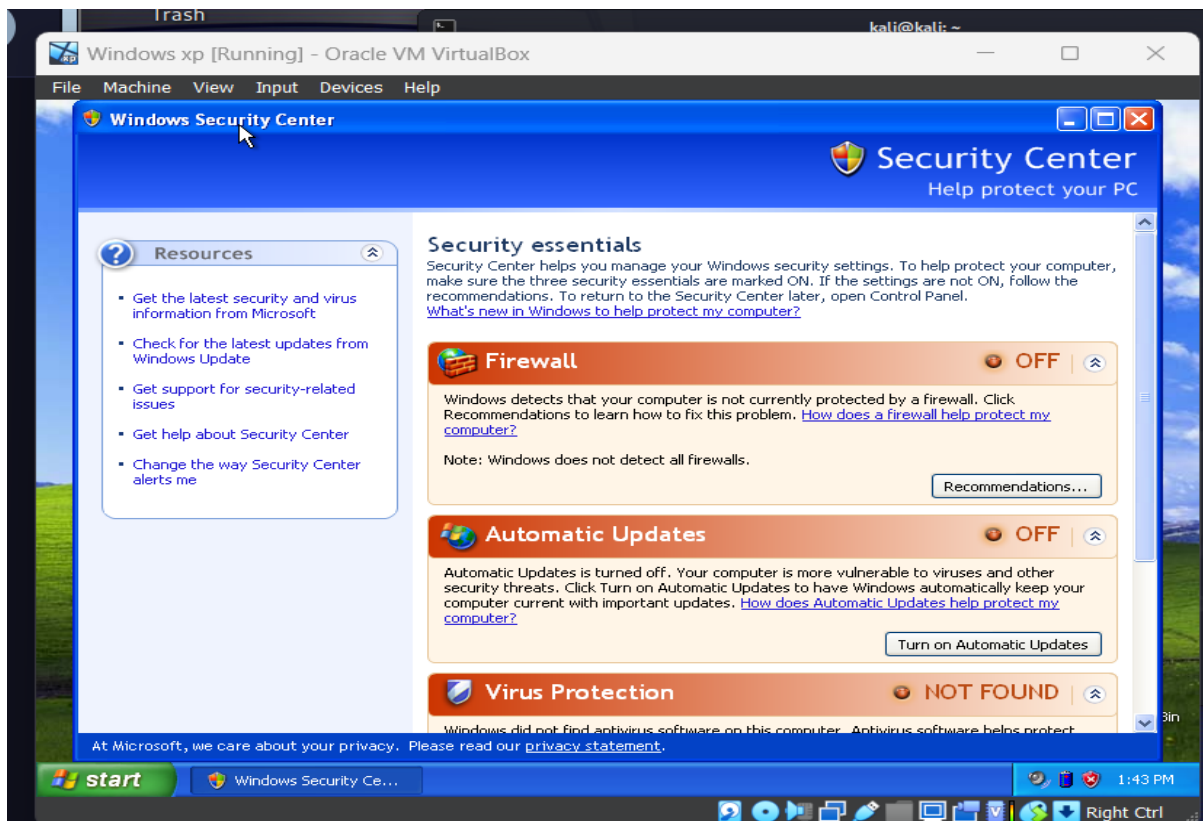


Scansione di rete con NMap con salvataggio del file(txt) di report in output

NMap è un tool che ci consente di scansionare/mappare la rete o la rete di un determinato target, nell'esercizio assegnatoci veniva richiesto di scansionare il target Windows xp utilizzando il tool NMap da Kali Linux, configurando gli ip delle due macchine virtuali sulla subnet 192.168.240 per poi avere l'ip 192.168.240.100 assegnato alla macchina Linux, mentre per la macchina Windows xp avremo l'ip 192.168.240.150. Eseguendo una prima scansione con NMap sul bersaglio windows xp noteremo che non riusciremo a scansionare le porte perché sono filtrate, in quanto abbiamo un servizio che ce lo impedisce, possiamo dedurre che si tratti di un servizio di sicurezza in questo caso un FIREWALL, andando ad investigare con un semplice ping scopriremo infatti che le macchine non comunicano affatto. Una volta disattivato il FIREWALL su Windows le macchine daranno un esito positivo con il ping infatti possiamo notare che i pacchetti sono stati trasmessi correttamente senza nessun loss, possiamo quindi iniziare la scansione. Useremo quindi gli switch di NMap per avere più informazioni possibili sulla rete della macchina bersaglio in particolare per osservare lo stato delle porte di quest'ultima per poi salvarle in output come un file.txt, ciò ci permette di poter analizzare la rete in un secondo momento anche al di fuori del prompt come di poter condividere il file per vari altri scopi, il comando che ci permetterà di fare ciò digitandolo sul prompt quindi sarà `nmap -sV 192.168.240.150 -o nomefile.txt`, ma ci sono anche molti altri switch: `-oN`-`oX`-`oG`-`oA`-`oS` ed anche `-stats-every` con i secondi in seguito per avere una scansione di rete continua, esempio `-stats-every 2s`, si possono ottenere anche file in xml. Avendo eseguito le varie scansioni ed avendo salvato i file come root, troveremo i report salvati nella cartella root alla quale accederemo lanciando il comando `"sudo su"` nel prompt seguito dal comando `"thunar"`.



```
kali@kali: ~  
File Actions Edit View Help  
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=0.997 ms  
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=1.21 ms  
64 bytes from 192.168.240.150: icmp_seq=5 ttl=128 time=0.929 ms  
64 bytes from 192.168.240.150: icmp_seq=6 ttl=128 time=0.925 ms  
^C  
— 192.168.240.150 ping statistics —  
6 packets transmitted, 6 received, 0% packet loss, time 5010ms  
rtt min/avg/max/mdev = 0.925/2.463/6.637/2.179 ms  
  
(kali@kali)-[~]  
$ nmap 192.168.240.150 -sV -o  
nmap: option requires an argument -- 'o'  
See the output of nmap -h for a summary of options.  
  
(kali@kali)-[~]  
$ nmap 192.168.240.150 -sV  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 08:46 EDT  
Nmap scan report for 192.168.240.150  
Host is up (0.0012s latency).  
Not shown: 997 closed tcp ports (conn-refused)  
PORT      STATE SERVICE        VERSION  
135/tcp   open  msrpc          Microsoft Windows RPC  
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn  
445/tcp   open  microsoft-ds   Microsoft Windows XP microsoft-ds  
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 19.88 seconds  
  
(kali@kali)-[~]  
$
```

```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# nmap -oN /root/Desktop/metascan.txt 192.168.240.150  
Failed to open normal output file /root/Desktop/metascan.txt for writing: No such file  
or directory (2)  
(root@kali)-[~]  
# nmap -oN/root/Desktop/metascan.txt 192.168.240.150  
You are using a deprecated option in a dangerous way. Did you mean: -oN /root/Desktop/  
metascan.txt  
QUITTING!  
(root@kali)-[~]  
# nmap -oN/Desktop/metascan.txt 192.168.240.150  
You are using a deprecated option in a dangerous way. Did you mean: -oN /Desktop/metascan.txt  
QUITTING!  
(root@kali)-[~]  
# nmap -oN scan.txt 192.168.240.150  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 09:10 EDT  
Nmap scan report for 192.168.240.150  
Host is up (0.00053s latency).  
Not shown: 997 closed tcp ports (reset)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
MAC Address: 08:00:27:A2:69:E6 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 14.44 seconds  
(root@kali)-[~]  
#
```

```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# nmap -oN scan.txt 192.168.240.150  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 09:10 EDT  
Nmap scan report for 192.168.240.150  
Host is up (0.00053s latency).  
Not shown: 997 closed tcp ports (reset)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
MAC Address: 08:00:27:A2:69:E6 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 14.44 seconds  
(root@kali)-[~]  
# cat scan.txt  
# Nmap 7.94SVN scan initiated Mon Mar 18 09:10:07 2024 as: nmap -oN scan.txt 192.168.240.150  
Nmap scan report for 192.168.240.150  
Host is up (0.00053s latency).  
Not shown: 997 closed tcp ports (reset)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
MAC Address: 08:00:27:A2:69:E6 (Oracle VirtualBox virtual NIC)  
  
# Nmap done at Mon Mar 18 09:10:21 2024 -- 1 IP address (1 host up) scanned in 14.44 seconds  
(root@kali)-[~]  
#
```

```
root@kali: ~  
File Actions Edit View Help  
  
(root@kali)-[~]  
# cat scan.txt  
# Nmap 7.94SVN scan initiated Mon Mar 18 09:10:07 2024 as: nmap -oN scan.txt 192.168.240.150  
Nmap scan report for 192.168.240.150  
Host is up (0.00053s latency).  
Not shown: 997 closed tcp ports (reset)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
MAC Address: 08:00:27:A2:69:E6 (Oracle VirtualBox virtual NIC)  
  
# Nmap done at Mon Mar 18 09:10:21 2024 -- 1 IP address (1 host up) scanned in 14.44 seconds  
  
(root@kali)-[~]  
# nmap -oX scan.xml 192.168.240.150  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 09:14 EDT  
Nmap scan report for 192.168.240.150  
Host is up (0.0011s latency).  
Not shown: 997 closed tcp ports (reset)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
MAC Address: 08:00:27:A2:69:E6 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds  
  
(root@kali)-[~]  
#
```

```
(root@kali)-[~]  
# cat scan.xml  
<?xml version="1.0" encoding="UTF-8"?>  
<!DOCTYPE nmaprun>  
<?xml-stylesheet href="file:///usr/bin/.. /share/nmap/nmap.xml" type="text/xml"?>  
<nmaprun scanner="nmap" args="nmap -oX scan.xml 192.168.240.150" start="1710767648" startstr="Mon Mar 18 09:14:08 2024" version="7.94SVN" xmloutputversion="1.05">  
<scaninfo type="syn" protocol="tcp" numservices="1000" services="1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,280,301,306,311,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,500,512-515,524,541,543-545,548,554-555,563,587,593,616-617,625,631,636,646,648,666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,843,873,880,888,898,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-1011,1021-1100,1102,1104-1108,1110-1114,1117,1119,1121-1124,1126,1130-1132,1137-1138,1141,1145,1147-1149,1151-1152,1154,1163-1166,1169,1174-1175,1183,1185-1187,1192,1198-1199,1201,1213,1216-1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,1277,1287,1296,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1500-1501,1503,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,1666,1687-1688,1700,1717-1721,1723,1755,1761,1782-1783,1801,1805,1812,1839-1840,1862-1864,1875,1900,1914,1935,1947,1971-1972,1974,1984,1998-2010,2013,2020-2022,2030,2033-2035,2038,2040-2043,2045-2049,2065,2068,2099-2100,2103,2105-2107,2111,2119,2121,2126,2135,2144,2160-2161,2170,2179,2190-2191,2196,2200,2222,2251,2260,2288,2301,2323,2366,2381-2383,2393-2394,2399,2401,2492,2500,2522,2525,2557,2601-2602,2604-2605,2607-2608,2638,2701-2702,2710,2717-2718,2725,2800,2809,2811,2869,2875,2909-2910,2920,2967-2968,2998,3000-3001,3003,3005-3007,3011,3013,3017,3030-3031,3052,3071,3077,3128,3168,3211,3221,3260-3261,3268-3269,3283,3300-3301,3306,3322-3325,3333,3351,3367,3369-3372,3389-3390,3404,3476,3493,3517,3527,3546,3551,3580,3659,3689-3690,3703,3737,3766,3784,3800-3801,3809,3814,3826-3828,3851,3869,3871,3878,3880,3889,3905,3914,3918,3920,3945,3971,3986,3995,3998,4000-4006,4045,4111,4125-4126,4129,4224,4242,4279,4321,4343,4443-4446,4449,4550,4567,4662,4848,4899-4900,4998,5000-5004,5009,5030,5033,5050-5051,5054,5060-5061,5080,5087,5100-5102,5120,5190,5200,5214,5221-5222,5225-5226,5269,5280,5298,5357,5405,5414,5431-5432,5440,5500,5510,5544,5550,5555,5560,5566,5631,5633,5666,5678-5679,5718,5730,5800-5802,5810-5811,5815,5822,5825,5850,5859,5862,5877,5900-5904,5906-5907,5910-5911,5915,5922,5925,5950,5952,5959-5963,5987-5989,5998-6007,6009,6025,6059,6100-6101,6106,6112,6123,6129,6156,6346,6389,6502,6510,6543,6547,6565-6567,6580,6646,6666-6669,6689,6692,6699,6779,6788-6789,6792,6839,6881,6901,6969,7000-7002,7004,7007,7019,7025,7070,7100,7103,7106,7200-7201,7402,7435,7443,7496,7512,7625,7627,7676,7741,7777-7778,7800,7911,7920-7921,7937-7938,7999-8002,8007-8011,8021-8022,8031,8042,8045,8080-8090,8093,8099-8100,8180-8181,8192-8194,8200,8222,8254,8290-8292,8300,8333,8383,8400,8402,8443,8500,8600,8649,8651-8652,8654,8701,8800,8873,8888,8899,8994,9000-9003,9009-9011,9040,9050,9071,9080-9081,9090-9091,9099-9103,9110-9111,9200,9207,9220,9290,9415,9418,9485,9500,9502-9503,9535,9575,9593-9595,9618,9666,9876-9878,9898,9900,9917,9929,9943-9944,9968,9998-10004,10009-10010,10012,10024-10025,10082,10180,10215,10243,10566,10616-10617,10621,10626,10628-10629,10778,11110-11111,11967,12000,12174,12265,12345,13456,13722,13782-13783,14000,14238,14441-14442,15000,15002-15004,15660,15742,16000-16001,16012,16016,16018,16080,16113,16992-16993,17877,17988,18040,18101,18988,19101,19283,19315,19350,19780,19801,19842,200
```



```
File Actions Edit View Help
80,49152-49161,49163,49165,49167,49175-49176,49400,49999-50003,50006,50300,50389,50500
,50636,50800,51103,51493,52673,52822,52848,52869,54045,54328,55055-55056,55555,55600,5
6737-56738,57294,57797,58080,60020,60443,61532,61900,62078,63331,64623,64680,65000,651
29,65389"/>
<verbose level="0"/>
<debugging level="0"/>
<hosthint><status state="up" reason="arp-response" reason_ttl="0"/>
<address addr="192.168.240.150" addrtype="ipv4"/>
<address addr="08:00:27:A2:69:E6" addrtype="mac" vendor="Oracle VirtualBox virtual NIC
"/>
<hostnames>
</hostnames>
</hosthint>
<host starttime="1710767662" endtime="1710767663"><status state="up" reason="arp-respo
nse" reason_ttl="0"/>
<address addr="192.168.240.150" addrtype="ipv4"/>
<address addr="08:00:27:A2:69:E6" addrtype="mac" vendor="Oracle VirtualBox virtual NIC
"/>
<hostnames>
</hostnames>
<ports><extraports state="closed" count="997">
<extrareasons reason="reset" count="997" proto="tcp" ports="1,3-4,6-7,9,13,17,19-26,30
,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,143-144,146,161,16
3,179,199,211-212,222,254-256,259,264,280,301,306,311,340,366,389,406-407,416-417,425,
427,443-444,458,464-465,481,497,500,512-515,524,541,543-545,548,554-555,563,587,593,61
6-617,625,631,636,646,648,666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,
783,787,800-801,808,843,873,880,888,898,900-903,911-912,981,987,990,992-993,995,999-10
02,1007,1009-1011,1021-1100,1102,1104-1108,1110-1114,1117,1119,1121-1124,1126,1130-113
2,1137-1138,1141,1145,1147-1149,1151-1152,1154,1163-1166,1169,1174-1175,1183,1185-1187
,1192,1198-1199,1201,1213,1216-1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,1277,
1287,1296,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1
500-1501,1503,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,1666,1687-1688,1700,17
17-1721,1723,1755,1761,1782-1783,1801,1805,1812,1839-1840,1862-1864,1875,1900,1914,193
5,1947,1971-1972,1974,1984,1998-2010,2013,2020-2022,2030,2033-2035,2038,2040-2043,2045
-2049,2065,2068,2099-2100,2103,2105-2107,2111,2119,2121,2126,2135,2144,2160-2161,2170,
2179,2190-2191,2196,2200,2222,2251,2260,2288,2301,2323,2366,2381-2383,2393-2394,2399,2
401,2492,2500,2522,2525,2557,2601-2602,2604-2605,2607-2608,2638,2701-2702,2710,2717-27
18,2725,2800,2809,2811,2869,2875,2909-2910,2920,2967-2968,2998,3000-3001,3003,3005-300
7,3011,3013,3017,3030-3031,3052,3071,3077,3128,3168,3211,3221,3260-3261,3268-3269,3283
,3300-3301,3306,3322-3325,3333,3351,3367,3369-3372,3389-3390,3404,3476,3493,3517,3527,
3546,3551,3580,3659,3689-3690,3703,3737,3766,3784,3800-3801,3809,3814,3826-3828,3851,3
869,3871,3878,3880,3889,3905,3914,3918,3920,3945,3971,3986,3995,3998,4000-4006,4045,41
11,4125-4126,4129,4224,4242,4279,4321,4343,4443-4446,4449,4550,4567,4662,4848,4899-490
0,4998,5000-5004,5009,5030,5033,5050-5051,5054,5060-5061,5080,5087,5100-5102,5120,5190
,5200,5214,5221-5222,5225-5226,5269,5280,5298,5357,5405,5414,5431-5432,5440,5500,5510,
5544,5550,5555,5560,5566,5631,5633,5666,5678-5679,5718,5730,5800-5802,5810-5811,5815,5
822,5825,5850,5859,5862,5877,5900-5904,5906-5907,5910-5911,5915,5922,5925,5950,5952,59
59-5963,5987-5989,5998-6007,6009,6025,6059,6100-6101,6106,6112,6123,6129,6156,6346,638
9,6502,6510,6543,6547,6565-6567,6580,6646,6666-6669,6689,6692,6699,6779,6788-6789,6792
,6839,6881,6901,6969,7000-7002,7004,7007,7019,7025,7070,7100,7103,7106,7200-7201,7402,
7435,7443,7496,7512,7625,7627,7676,7741,7777-7778,7800,7911,7920-7921,7937-7938,7999-8
```

```
File Actions Edit View Help
9,6502,6510,6543,6547,6565-6567,6580,6646,6666-6669,6689,6692,6699,6779,6788-6789,6792
,6839,6881,6901,6969,7000-7002,7004,7007,7019,7025,7070,7100,7103,7106,7200-7201,7402,
7435,7443,7496,7512,7625,7627,7676,7741,7777-7778,7800,7911,7920-7921,7937-7938,7999-8
002,8007-8011,8021-8022,8031,8042,8045,8080-8090,8093,8099-8100,8180-8181,8192-8194,82
00,8222,8254,8290-8292,8300,8333,8383,8400,8402,8443,8500,8600,8649,8651-8652,8654,870
1,8800,8873,8888,8899,8994,9000-9003,9009-9011,9040,9050,9071,9080-9081,9090-9091,9099
-9103,9110-9111,9200,9207,9220,9290,9415,9418,9485,9500,9502-9503,9535,9575,9593-9595,
9618,9666,9876-9878,9898,9900,9917,9929,9943-9944,9968,9998-10004,10009-10010,10012,10
024-10025,10082,10180,10215,10243,10566,10616-10617,10621,10626,10628-10629,10778,1111
0-11111,11967,12000,12174,12265,12345,13456,13722,13782-13783,14000,14238,14441-14442,
15000,15002-15004,15660,15742,16000-16001,16012,16016,16018,16080,16113,16992-16993,17
877,17988,18040,18101,18988,19101,19283,19315,19350,19780,19801,19842,20000,20005,2003
1,20221-20222,20828,21571,22939,23502,24444,24800,25734-25735,26214,27000,27352-27353,
27355-27356,27715,28201,30000,30718,30951,31038,31337,32768-32785,33354,33899,34571-34
573,35500,38292,40193,40911,41511,42510,44176,44442-44443,44501,45100,48080,49152-4916
1,49163,49165,49167,49175-49176,49400,49999-50003,50006,50300,50389,50500,50636,50800,
51103,51493,52673,52822,52848,52869,54045,54328,55055-55056,55555,55600,56737-56738,57
294,57797,58080,60020,60443,61532,61900,62078,63331,64623,64680,65000,65129,65389"/>
</extraports>
<port protocol="tcp" portid="135"><state state="open" reason="syn-ack" reason_ttl="128
"/><service name="msrpc" method="table" conf="3"/></port>
<port protocol="tcp" portid="139"><state state="open" reason="syn-ack" reason_ttl="128
"/><service name="netbios-ssn" method="table" conf="3"/></port>
<port protocol="tcp" portid="445"><state state="open" reason="syn-ack" reason_ttl="128
"/><service name="microsoft-ds" method="table" conf="3"/></port>
</ports>
<times srtt="1080" rttvar="750" to="100000"/>
</host>
<runstats><finished time="1710767663" timestr="Mon Mar 18 09:14:23 2024" summary="Nmap
done at Mon Mar 18 09:14:23 2024; 1 IP address (1 host up) scanned in 14.40 seconds"
elapsed="14.40" exit="success"/><hosts up="1" down="0" total="1"/>
</runstats>
</nmaprun>
```

```
</nmaprun>

(root@kali)~#
# nmap -oG scantron.txt 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 09:17 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00084s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:A2:69:E6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.47 seconds

(root@kali)~#
# grep "microsoft" scantron.txt
Host: 192.168.240.150 ()      Ports: 135/open/tcp//msrpc///, 139/open/tcp//netbios-ssn///, 445/open/tcp//microsoft
-ds/// Ignored State: closed (997)

(root@kali)~#
# nmap -oA scan2 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 09:21 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00047s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:A2:69:E6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.47 seconds

(root@kali)~#
# ls -l scan2.*
-rw-r--r-- 1 root root 363 Mar 18 09:22 scan2.gnmap
-rw-r--r-- 1 root root 450 Mar 18 09:22 scan2.nmap
-rw-r--r-- 1 root root 9539 Mar 18 09:22 scan2.xml

(root@kali)~#
```

```
(root@kali)~#
# nmap -oA scan2 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 09:21 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00047s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:A2:69:E6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.47 seconds

(root@kali)~#
# ls -l scan2.*
-rw-r--r-- 1 root root 363 Mar 18 09:22 scan2.gnmap
-rw-r--r-- 1 root root 450 Mar 18 09:22 scan2.nmap
-rw-r--r-- 1 root root 9539 Mar 18 09:22 scan2.xml

(root@kali)~#
# nmap --stats-every 2s 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 09:25 EDT
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:04 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:06 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:08 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:10 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:12 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 54.35% done; ETC: 09:26 (0:00:01 remaining)
Nmap scan report for 192.168.240.150
Host is up (0.0011s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:A2:69:E6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.43 seconds

(root@kali)~#
```

```

(root@kali)-[~]
# nmap --stats-every 2s 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 09:25 EDT
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:04 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:06 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:08 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:10 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:12 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 54.35% done; ETC: 09:26 (0:00:01 remaining)
Nmap scan report for 192.168.240.150
Host is up (0.0011s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:A2:69:E6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.43 seconds

```

```

(root@kali)-[~]
# nmap -oS kiddie.txt 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 09:29 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00077s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:A2:69:E6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.41 seconds

```

```

(root@kali)-[~]
#

```

```

(root@kali)-[~]
# nmap -oS kiddie.txt 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 09:29 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00077s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:A2:69:E6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.41 seconds

```

```

(root@kali)-[~]
# cat kiddie.txt
StArt|nG Nmap 7.94$VN ( httpz://nmap.0Rg ) aT 2024-03-18 09:29 EDT
Nmap scan rep0rt f0r 192.168.240.150
H0$t Iz up (0.00077s Lat3ncy).
n0t $hOwn: 997 cl0seD tcp p0rTS (r3$Et)
P0RT      sTAT3 $eRVIC3
135/tcP    0peN    M$Rpc
139/tcP    op3n    n3Tb|0z-$n
445/tcP    opEn    m|Cr0$0ft-Dz
M4C 4ddr3$z: 08:00:27:42:69:e6 (oRacl3 V!rtuaLb0x virtual niC)

NmaP donE: 1 Ip AddrEsz (1 ho$t uP) $Cann3d in 14.41 S3c0ndz

```

