Temat 02.4 Techniki skanowania hostów i portów

Wykonał(a): Bartosz Miazga
Stanowisko: 14

Zadanie 1 - Skanowanie metodą połączeniową (*TCP connect scan)*

1.1 (poniżej) Obraz okna wiersza poleceń z linią polecenia i raportem programu *nmap* ze skanowania metodą
połączeniową

```
C:\Users\Administrator>nmap -p 130-140 -PN -sT 192.168.79.55 -scan-delay 2s
Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-06 11:13 Central European Standard Time
Nmass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns o
Specify valid servers with --dns-servers
Nmap scan report for 192.168.79.55
Host is up (0.72s latency).

PORT    STATE  SERVICE
130/tcp closed cisco-fna
131/tcp closed cisco-tna
132/tcp closed cisco-sys
133/tcp closed statsrv
134/tcp closed ingres-net
135/tcp open   msrpc
136/tcp closed profile
137/tcp closed netbios-ns
138/tcp closed netbios-dgm
139/tcp open   netbios-ssn
140/tcp closed emfis-data

Nmap done: 1 IP address (1 host up) scanned in 23.34 seconds
```

1.2 (poniżej) Obraz okna sniffera uzyskany podczas skanowania metodą połączeniową. Kolorem zielonym zaznaczono pojedynczą sekwencję pakietów związaną z wykrywaniem jednego portu otwartego. Kolorem czerwonym zaznaczono pojedynczą sekwencję pakietów związaną z wykrywaniem jednego portu zamkniętego.

Wkleić obraz okna

15	224.652102	Vmware_86:45:9c	Vmware_8a:a7:3f	ARP	42 192.168.214.56 is at 00:0c:29:86:45:9c
16	224.652599	192.168.79.55	192.168.214.56	TCP	66 135 → 49808 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=…
17	224.652640	192.168.214.56	192.168.79.55	TCP	54 49808 → 135 [ACK] Seq=1 Ack=1 Win=65536 Len=0
18	224.666437	192.168.214.56	192.168.79.55	TCP	54 49808 → 135 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19	226.650914	192.168.214.56	192.168.79.55	TCP	66 49809 → 139 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PE…
20	226.651398	192.168.79.55	192.168.214.56	TCP	66 139 → 49809 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=…
21	226.651427	192.168.214.56	192.168.79.55	TCP	54 49809 → 139 [ACK] Seq=1 Ack=1 Win=525568 Len=0
22	226.666423	192.168.214.56	192.168.79.55	TCP	54 49809 → 139 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	228.650968	192.168.214.56	192.168.79.55	TCP	66 49810 → 136 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PE…
24	228.651481	192.168.79.55	192.168.214.56	TCP	60 136 → 49810 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	229.166553	192.168.214.56	192.168.79.55	TCP	66 [TCP Retransmission] 49810 → 136 [SYN] Seq=0 Win=8192 Len=0 MS…
26	229.167202	192.168.79.55	192.168.214.56	TCP	60 136 → 49810 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	229.682056	192.168.214.56	192.168.79.55	TCP	62 [TCP Retransmission] 49810 → 136 [SYN] Seq=0 Win=8192 Len=0 MS…
28	229.682516	192.168.79.55	192.168.214.56	TCP	60 136 → 49810 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29	230.666662	192.168.214.56	192.168.79.55	TCP	66 49811 → 134 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PE…
30	230.667164	192.168.79.55	192.168.214.56	TCP	60 134 → 49811 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31	231.182073	192.168.214.56	192.168.79.55	TCP	66 [TCP Retransmission] 49811 → 134 [SYN] Seq=0 Win=8192 Len=0 MS…
32	231.182580	192.168.79.55	192.168.214.56	TCP	60 134 → 49811 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	231.697660	192.168.214.56	192.168.79.55	TCP	62 [TCP Retransmission] 49811 → 134 [SYN] Seq=0 Win=8192 Len=0 MS…
34	231.698149	192.168.79.55	192.168.214.56	TCP	60 134 → 49811 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Charakterystyka metody połączeniowej i ocena poprawności uzyskanych wyników

m.in. dokładny opis wszelkich możliwych wariantów sekwencji pakietów wymienianych pomiędzy komputerami, w przypadku skanowania portu otwartego i zamkniętego (nawet jeżeli nie zaobserwowano ich podczas realizacji ćwiczenia).

Jeżeli podczas nawiązywania połączenia serwer odpowie pakietem z flagami SYN/ACK to port jest **otwarty** w trybie nasłuchu. Pakiet z flagami RST/ACK może wskazywać na zamknięty port, ale na etapie skanowania nie jesteśmy w stanie tego jednoznacznie określić, ponieważ ruch na porcie może być filtrowany. Skanowanie kończy wysłanie pakietu z flagą RST.

Wady: Wady tej metody to łatwość wykrycia i zablokowania.

Zalety: Zaletą tej metody jest jej szybkość oraz fakt ,że może zostać wykonana przez każdego użytkownika

Sekwencja portu otwartego:

[SYN]
[SYN,ACK]
[ACK]
[RST,ACK]

Sekwencja portu zamkniętego(filtrowanego):
[SYN]
[RST,ACK]

Zadanie 2 - Skanowanie metodą półotwartą (*TCP SYN scan)*

2.1 (poniżej) Obraz okna wiersza poleceń z linią polecenia i raportem programu *nmap* ze skanowania metodą półotwartą.

```
C:\Users\Administrator>nmap -p 130-140 -PN -sS 192.168.79.55 -scan-delay 2s
Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-06 11:18 Central European Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-d
cify valid servers with --dns-servers
Nmap scan report for 192.168.79.55
Host is up (0.00s latency).

PORT    STATE  SERVICE
130/tcp closed cisco-fna
131/tcp closed cisco-tna
132/tcp closed cisco-sys
133/tcp closed statsrv
134/tcp closed ingres-net
135/tcp open   msrpc
136/tcp closed profile
137/tcp closed netbios-ns
138/tcp closed netbios-dgm
139/tcp open   netbios-ssn
140/tcp closed emfis-data
MAC Address: 00:0C:29:8A:A7:3F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 26.39 seconds

C:\Users\Administrator>
```

2.2 (poniżej) Obraz okna sniffera uzyskany podczas skanowania metodą półotwartą. Kolorem zielonym zaznaczono pojedynczą sekwencję pakietów związanych z wykrywaniem jednego portu otwartego. Kolorem czerwonym zaznaczono pojedynczą sekwencję pakietów związanych z wykrywaniem jednego portu zamkniętego.

7	42.491164	Vmware_86:45:9c	Broadcast	ARP	42 Who has 192.168.79.55? Tell 192.168.214.56
8	42.491713	Vmware_8a:a7:3f	Vmware_86:45:9c	ARP	60 192.168.79.55 is at 00:0c:29:8a:a7:3f
9	44.584620	192.168.214.56	192.168.79.55	TCP	58 48901 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10	44.585136	192.168.79.55	192.168.214.56	TCP	60 139 → 48901 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
11	44.585179	192.168.214.56	192.168.79.55	TCP	54 48901 → 139 [RST] Seq=1 Win=0 Len=0
12	46.600337	192.168.214.56	192.168.79.55	TCP	58 48901 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13	46.600851	192.168.79.55	192.168.214.56	TCP	60 135 → 48901 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
14	46.600902	192.168.214.56	192.168.79.55	TCP	54 48901 → 135 [RST] Seq=1 Win=0 Len=0
16	48.616371	192.168.79.55	192.168.214.56	TCP	60 140 → 48901 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17	49.265760	Vmware_8a:a7:3f	Vmware_86:45:9c	ARP	60 Who has 192.168.214.56? Tell 192.168.79.55
18	49.265771	Vmware_86:45:9c	Vmware_8a:a7:3f	ARP	42 192.168.214.56 is at 00:0c:29:86:45:9c
19	50.631634	192.168.214.56	192.168.79.55	TCP	58 48901 → 133 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	50.632186	192.168.79.55	192.168.214.56	TCP	60 133 → 48901 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	52.647679	192.168.79.55	192.168.214.56	TCP	60 134 → 48901 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	54.662788	192.168.214.56	192.168.79.55	TCP	58 48901 → 131 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24	54.663267	192.168.79.55	192.168.214.56	TCP	60 131 → 48901 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	56.678430	192.168.214.56	192.168.79.55	TCP	58 48901 → 132 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
26	56.678952	192.168.79.55	192.168.214.56	TCP	60 132 → 48901 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	58.694114	192.168.214.56	192.168.79.55	TCP	58 48901 → 138 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
28	58.694642	192.168.79.55	192.168.214.56	TCP	60 138 → 48901 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29	60.709706	192.168.214.56	192.168.79.55	TCP	58 48901 → 137 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
30	60.710181	192.168.79.55	192.168.214.56	TCP	60 137 → 48901 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31	62.725423	192.168.214.56	192.168.79.55	TCP	58 48901 → 130 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
32	62.725961	192.168.79.55	192.168.214.56	TCP	60 130 → 48901 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	64.740926	192.168.214.56	192.168.79.55	TCP	58 48912 → 140 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
34	64.741457	192.168.79.55	192.168.214.56	TCP	60 140 → 48912 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
35	66.756650	192.168.214.56	192.168.79.55	TCP	58 48901 → 136 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
36	66.757086	192.168.79.55	192.168.214.56	TCP	60 136 → 48901 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
37	71.266062	Vmware_8a:a7:3f	Vmware_86:45:9c	ARP	60 Who has 192.168.214.56? Tell 192.168.79.55
38	71.266087	Vmware_86:45:9c	Vmware_8a:a7:3f	ARP	42 192.168.214.56 is at 00:0c:29:86:45:9c

Charakterystyka metody półotwartej i ocena poprawności uzyskanych wyników

m.in. dokładny opis wszelkich możliwych wariantów sekwencji pakietów wymienianych pomiędzy komputerami, w przypadku skanowania portu otwartego i zamkniętego (nawet jeżeli nie zaobserwowano ich podczas realizacji ćwiczenia).

System docelowy dostarcza informacji o statusie portu już podczas trwania procesu nawiązywania połączenia po nadesłaniu odpowiedzi na pakiet SYN. Technika półotwartego skanowania wykorzystuje właśnie ten fakt. Polega ona na wysłaniu pakietu z flagą RST po otrzymaniu w drugiej fazie połączenia pakietu z flagami SYN/ACK lub RST/ACK. Wykrywanie portów zamkniętych działa na tej samej zasadzie co w metodzie połączeniowej, czyli nie jesteśmy w stanie jednoznacznie ocenić czy port jest zamknięty czy filtrowany otrzymując pakiet RST/ACK.

Wykrywanie portów otwartych również działa w ten sam sposób co w metodzie połączeniowej- jeżeli w trakcie nawiązywania połączenia serwer odpowie pakietem z flagami SYN/ACK to port jest otwarty.
Wady: Konieczność posiadania uprawnień superużytkownika w syst. Linux
Zalety: Kiedyś utrudniona wykrywalność metody

Sekwencja portu otwartego:
[SYN]
[SYN,ACK]
[RST]

Sekwencja portu zamkniętego(filtrowanego):
[SYN]
[RST,ACK]

Zadanie 3 - Skanowanie metodą UDP (*UDP scan)*

3.1 (poniżej) Obraz okna wiersza poleceń z linią polecenia i raportem programu *nmap* ze skanowania metodą UDP.

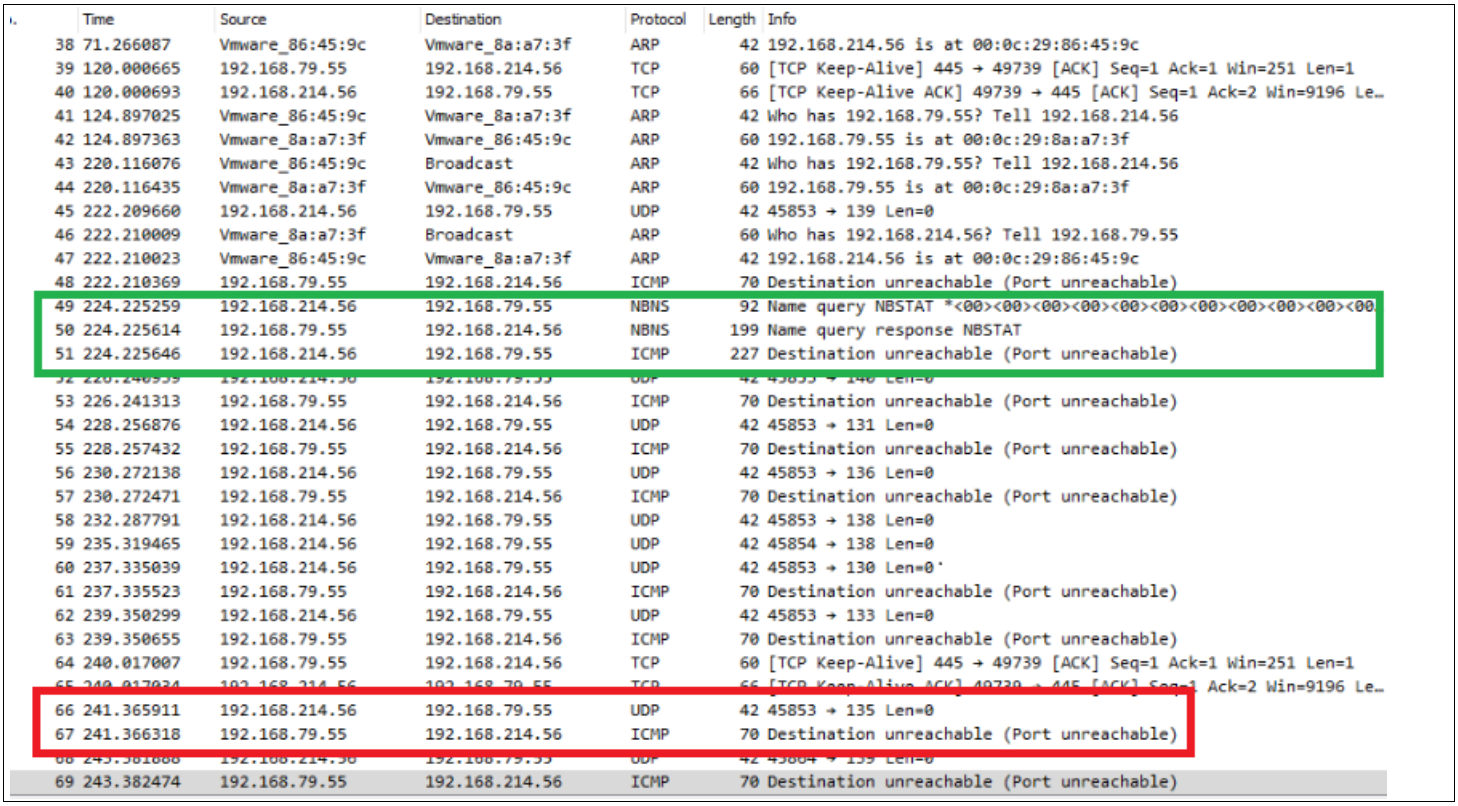
```
C:\Users\Administrator>nmap -p 130-140 -PN -sU 192.168.79.55 -scan-delay 2s
Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-06 11:21 Central European Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns o
cify valid servers with --dns-servers
Nmap scan report for 192.168.79.55
Host is up (0.00s latency).

PORT    STATE         SERVICE
130/udp closed        cisco-fna
131/udp closed        cisco-tna
132/udp closed        cisco-sys
133/udp closed        statsrv
134/udp closed        ingres-net
135/udp closed        msrpc
136/udp closed        profile
137/udp open          netbios-ns
138/udp open|filtered netbios-dgm
139/udp closed        netbios-ssn
140/udp closed        emfis-data
MAC Address: 00:0C:29:8A:A7:3F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 29.45 seconds

C:\Users\Administrator>
```

3.2 (poniżej) Obraz okna sniffera uzyskany podczas skanowania metodą UDP. Kolorem zielonym zaznaczono pojedynczą sekwencję pakietów związanych z wykrywaniem jednego portu otwartego. Kolorem czerwonym zaznaczono pojedynczą sekwencję pakietów związanych z wykrywaniem jednego portu zamkniętego.



	Time	Source	Destination	Protocol	Length	Info
38	71.266087	Vmware_86:45:9c	Vmware_8a:a7:3f	ARP	42	192.168.214.56 is at 00:0c:29:86:45:9c
39	120.000665	192.168.79.55	192.168.214.56	TCP	60	[TCP Keep-Alive] 445 → 49739 [ACK] Seq=1 Ack=1 Win=251 Len=1
40	120.000693	192.168.214.56	192.168.79.55	TCP	66	[TCP Keep-Alive ACK] 49739 → 445 [ACK] Seq=1 Ack=2 Win=9196 Le…
41	124.897025	Vmware_86:45:9c	Vmware_8a:a7:3f	ARP	42	Who has 192.168.79.55? Tell 192.168.214.56
42	124.897363	Vmware_8a:a7:3f	Vmware_86:45:9c	ARP	60	192.168.79.55 is at 00:0c:29:8a:a7:3f
43	220.116076	Vmware_86:45:9c	Broadcast	ARP	42	Who has 192.168.79.55? Tell 192.168.214.56
44	220.116435	Vmware_8a:a7:3f	Vmware_86:45:9c	ARP	60	192.168.79.55 is at 00:0c:29:8a:a7:3f
45	222.209660	192.168.214.56	192.168.79.55	UDP	42	45853 → 139 Len=0
46	222.210009	Vmware_8a:a7:3f	Broadcast	ARP	60	Who has 192.168.214.56? Tell 192.168.79.55
47	222.210023	Vmware_86:45:9c	Vmware_8a:a7:3f	ARP	42	192.168.214.56 is at 00:0c:29:86:45:9c
48	222.210369	192.168.79.55	192.168.214.56	ICMP	70	Destination unreachable (Port unreachable)
49	224.225259	192.168.214.56	192.168.79.55	NBNS	92	Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00
50	224.225614	192.168.79.55	192.168.214.56	NBNS	199	Name query response NBSTAT
51	224.225646	192.168.214.56	192.168.79.55	ICMP	227	Destination unreachable (Port unreachable)
53	226.241313	192.168.79.55	192.168.214.56	ICMP	70	Destination unreachable (Port unreachable)
54	228.256876	192.168.214.56	192.168.79.55	UDP	42	45853 → 131 Len=0
55	228.257432	192.168.79.55	192.168.214.56	ICMP	70	Destination unreachable (Port unreachable)
56	230.272138	192.168.214.56	192.168.79.55	UDP	42	45853 → 136 Len=0
57	230.272471	192.168.79.55	192.168.214.56	ICMP	70	Destination unreachable (Port unreachable)
58	232.287791	192.168.214.56	192.168.79.55	UDP	42	45853 → 138 Len=0
59	235.319465	192.168.214.56	192.168.79.55	UDP	42	45854 → 138 Len=0
60	237.335039	192.168.214.56	192.168.79.55	UDP	42	45853 → 130 Len=0
61	237.335523	192.168.79.55	192.168.214.56	ICMP	70	Destination unreachable (Port unreachable)
62	239.350299	192.168.214.56	192.168.79.55	UDP	42	45853 → 133 Len=0
63	239.350655	192.168.79.55	192.168.214.56	ICMP	70	Destination unreachable (Port unreachable)
64	240.017007	192.168.79.55	192.168.214.56	TCP	60	[TCP Keep-Alive] 445 → 49739 [ACK] Seq=1 Ack=1 Win=251 Len=1
66	241.365911	192.168.214.56	192.168.79.55	UDP	42	45853 → 135 Len=0
67	241.366318	192.168.79.55	192.168.214.56	ICMP	70	Destination unreachable (Port unreachable)
69	243.382474	192.168.79.55	192.168.214.56	ICMP	70	Destination unreachable (Port unreachable)

Charakterystyka metody UDP i ocena poprawności uzyskanych wyników

m.in. dokładny opis wszelkich możliwych wariantów sekwencji pakietów wymienianych pomiędzy komputerami, w przypadku skanowania portu otwartego i zamkniętego (nawet jeżeli nie zaobserwowano ich podczas realizacji ćwiczenia).

UDP to protokół bezpołączeniowy, jeżeli aktywny system otrzyma datagram UDP na zamknięty port , powinien odpowiedzieć komunikatem ICMP Destination Unreachable (typ 3), a dokładniej ICMP Port Unreachable (typ 3 , kod 3). Jeżeli port jest otwarty , nie należy się spodziewać odpowiedzi , gdyż w przypadku UDP nie występuje potwierdzenie odebrania pakietu. Jednakze należy pamiętać ,że brak odpowiedzi nie identyfikuje jednoznacznie portu otwartego gdyż datagram UDP może zostać odfiltrowany. Czasami odbierane są odpowiedzi z portu otwartego, jeżeli serwer próbuje odpowiedzieć na domniemane żądanie. Zależy to jednak od konstrukcji serwera i budowy pakietów skanujących.

Wady: Technika nie należy do najskuteczniejszych, wiele bramek w tym np. ściany ogniowe odfiltrowuje datagramy UDP skierowane na inne porty niż 53

Sekwencja portu zamkniętego:
[komunikat UDP]
[komunikat ICMP Port Unreachable]
Sekwencja portu otwartego:
[komunikat UDP]
[komunikat od portu otwartego]
[komunikat ICMP Port Unreachable]
Sekwencja portu otwartego(filtrowanego):
[komunikat UDP]

Zadanie 4 - Skanowanie metodą FIN (TCP *FIN)*

4.1 (poniżej) Obraz okna wiersza poleceń z linią polecenia i raportem programu *nmap* ze skanowania metodą FIN.

```
C:\Users\Administrator>nmap -p 130-140 -PN -sF 192.168.79.55 -scan-delay 2s
Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-06 11:27 Central European Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns o
cify valid servers with --dns-servers
Nmap scan report for 192.168.79.55
Host is up (0.00s latency).

PORT    STATE  SERVICE
130/tcp closed cisco-fna
131/tcp closed cisco-tna
132/tcp closed cisco-sys
133/tcp closed statsrv
134/tcp closed ingres-net
135/tcp closed msrpc
136/tcp closed profile
137/tcp closed netbios-ns
138/tcp closed netbios-dgm
139/tcp closed netbios-ssn
140/tcp closed emfis-data
MAC Address: 00:0C:29:8A:A7:3F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 26.39 seconds

C:\Users\Administrator>
```

4.2 (poniżej) Obraz okna sniffera uzyskany podczas skanowania metodą FIN. Kolorem zielonym zaznaczono pojedynczą sekwencję pakietów związanych z wykrywaniem jednego portu otwartego. Kolorem czerwonym zaznaczono pojedynczą sekwencję pakietów związanych z wykrywaniem jednego portu zamkniętego.

not tcp.analysis.retransmission

	Time	Source	Destination	Protocol	Length	Info
82	480.019160	192.168.79.55	192.168.214.56	TCP	60	[TCP Keep-Alive] 445 → 49739 [ACK] Seq=1 Ack=1 Win=25…
83	480.019186	192.168.214.56	192.168.79.55	TCP	66	[TCP Keep-Alive ACK] 49739 → 445 [ACK] Seq=1 Ack=2 Wi…
84	484.891315	Vmware_86:45:9c	Vmware_8a:a7:3f	ARP	42	Who has 192.168.79.55? Tell 192.168.214.56
85	484.891702	Vmware_8a:a7:3f	Vmware_86:45:9c	ARP	60	192.168.79.55 is at 00:0c:29:8a:a7:3f
86	579.782176	Vmware_86:45:9c	Broadcast	ARP	42	Who has 192.168.79.55? Tell 192.168.214.56
87	579.782682	Vmware_8a:a7:3f	Vmware_86:45:9c	ARP	60	192.168.79.55 is at 00:0c:29:8a:a7:3f
88	581.875712	192.168.214.56	192.168.79.55	TCP	54	50987 → 135 [FIN] Seq=1 Win=1024 Len=0
89	581.876218	Vmware_8a:a7:3f	Broadcast	ARP	60	Who has 192.168.214.56? Tell 192.168.79.55
90	581.876233	Vmware_86:45:9c	Vmware_8a:a7:3f	ARP	42	192.168.214.56 is at 00:0c:29:86:45:9c
91	581.876703	192.168.79.55	192.168.214.56	TCP	60	135 → 50987 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
92	583.891407	192.168.214.56	192.168.79.55	TCP	54	50987 → 139 [FIN] Seq=1 Win=1024 Len=0
93	583.891767	192.168.79.55	192.168.214.56	TCP	60	139 → 50987 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
94	585.907086	192.168.214.56	192.168.79.55	TCP	54	50987 → 138 [FIN] Seq=1 Win=1024 Len=0
95	585.907604	192.168.79.55	192.168.214.56	TCP	60	138 → 50987 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
96	587.922657	192.168.214.56	192.168.79.55	TCP	54	50987 → 140 [FIN] Seq=1 Win=1024 Len=0
97	587.923150	192.168.79.55	192.168.214.56	TCP	60	140 → 50987 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
98	589.938373	192.168.214.56	192.168.79.55	TCP	54	50987 → 130 [FIN] Seq=1 Win=1024 Len=0
99	589.938899	192.168.79.55	192.168.214.56	TCP	60	130 → 50987 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
100	591.954122	192.168.214.56	192.168.79.55	TCP	54	50987 → 137 [FIN] Seq=1 Win=1024 Len=0
101	591.954720	192.168.79.55	192.168.214.56	TCP	60	137 → 50987 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
102	593.969497	192.168.214.56	192.168.79.55	TCP	54	50987 → 136 [FIN] Seq=1 Win=1024 Len=0
103	593.969964	192.168.79.55	192.168.214.56	TCP	60	136 → 50987 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
104	595.985480	192.168.214.56	192.168.79.55	TCP	54	50987 → 131 [FIN] Seq=1 Win=1024 Len=0
105	595.986200	192.168.79.55	192.168.214.56	TCP	60	131 → 50987 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
106	598.000856	192.168.214.56	192.168.79.55	TCP	54	50987 → 133 [FIN] Seq=1 Win=1024 Len=0
107	598.001400	192.168.79.55	192.168.214.56	TCP	60	133 → 50987 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
108	600.016391	192.168.214.56	192.168.79.55	TCP	54	50987 → 132 [FIN] Seq=1 Win=1024 Len=0
109	600.016891	192.168.79.55	192.168.214.56	TCP	60	132 → 50987 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
110	600.019721	192.168.79.55	192.168.214.56	TCP	60	[TCP Keep-Alive] 445 → 49739 [ACK] Seq=1 Ack=1 Win=25…
111	600.019738	192.168.214.56	192.168.79.55	TCP	66	[TCP Keep-Alive ACK] 49739 → 445 [ACK] Seq=1 Ack=2 Wi…
112	602.032084	192.168.214.56	192.168.79.55	TCP	54	50998 → 135 [FIN] Seq=1 Win=1024 Len=0
113	602.032588	192.168.79.55	192.168.214.56	TCP	60	135 → 50998 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
114	604.047686	192.168.214.56	192.168.79.55	TCP	54	50987 → 134 [FIN] Seq=1 Win=1024 Len=0
115	604.048182	192.168.79.55	192.168.214.56	TCP	60	134 → 50987 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0

Charakterystyka metody FIN i ocena poprawności uzyskanych wyników

m.in. dokładny opis wszelkich możliwych wariantów sekwencji pakietów wymienianych pomiędzy komputerami, w przypadku skanowania portu otwartego i zamkniętego (nawet jeżeli nie zaobserwowano ich podczas realizacji ćwiczenia).

Skanowanie miało pierwotnie na celu utrudnienie wykrycia faktu skanowania. Metody specjalne wykorzystują zasadę zapisaną w RFC 793 mówiącą o tym ,że system powinien odpowiedzieć pakietem RST na każdy pakiet niezgodny z kolejnością nawiązywania połączenia TCP, jeżeli jest on kierowany do portu zamkniętego. Otwarty port nie wysyła żadnego pakietu zwrotnego.

Niektóre systemy , w tym system Windows są odporne na te techniki , zwracają one pakiet RST również w przypadku skanowania portu otwartego. Doprowadza to do błędu detekcji przez program nmap.

Ja taki błąd detekcji podczas ćwiczenia otrzymałem, zaobserwowałem ,że nmap wskazuje wszystkie porty jako zamknięte . Natomiast wiem z poprzednich skanowań innymi metodami ,że port 135 jest otwarty (dlatego zaznaczyłem go na zielono mimo, że sekwencja flag była taka sama jak dla portu zamkniętego.

Sekwencja portu otwartego:
[FIN]

Sekwencja portu zamkniętego(filtrowanego):
[FIN]
[RST,ACK]

Zadanie 5 - Detekcja metod skanowania

5.1a (poniżej) Obraz okna wiersza poleceń z linią polecenia i raportem programu nsc1.exe

Wkleić obraz okna

5.1b (poniżej) Obraz okna sniffera uzyskany podczas skanowania programem *nsc1*. Zaznaczono pojedynczą sekwencję pakietów charakterystyczną dla stosowanej metody skanowania.

Wkleić obraz okna

Charakterystyka metody wykorzystanej przez program *nsc1.exe*
(nazwa metody i uzasadnienie decyzji)
.....
.....

5.2a (poniżej) Obraz okna wiersza poleceń z linią polecenia i raportem programu *nsc2.exe*

Wkleić obraz okna

5.2b (poniżej) Obraz okna sniffera uzyskany podczas skanowania programem *nsc2.exe*. Zaznaczono pojedynczą sekwencję pakietów charakterystyczną dla stosowanej metody skanowania.

Wkleić obraz okna

Charakterystyka metody wykorzystanej przez program *nsc2.exe*
(nazwa metody i uzasadnienie decyzji)
.....
.....

5.3a (poniżej) Obraz okna wiersza poleceń z linią polecenia i raportem programu n*sc3.exe*

Wkleić obraz okna

5.3b (poniżej) Obraz okna sniffera uzyskany podczas skanowania programem *nsc3.exe*. Zaznaczono pojedynczą sekwencję pakietów charakterystyczną dla stosowanej metody skanowania.

Wkleić obraz okna

Charakterystyka metody wykorzystanej przez program *nsc3.exe*
(nazwa metody i uzasadnienie decyzji)
.....
.....

5.4 – wycofane

5.5a (poniżej) Obraz okna wiersza poleceń z linią polecenia i raportem programu *nsc5.exe*

Wkleić obraz okna

5.5b (poniżej) Obraz okna sniffera uzyskany podczas skanowania programem *nsc5.exe*. Zaznaczono pojedynczą sekwencję pakietów charakterystyczną dla stosowanej metody skanowania.

Wkleić obraz okna

Charakterystyka metody wykorzystanej przez program *nsc5.exe*
(nazwa metody i uzasadnienie decyzji)
.....
.....

5.6a (poniżej) Obraz okna wiersza poleceń z linią polecenia i raportem programu *nsc6.exe*

Wkleić obraz okna

5.6b (poniżej) Obraz okna sniffera uzyskany podczas skanowania programem *nsc6.exe*. Zaznaczono pojedynczą sekwencję pakietów charakterystyczną dla stosowanej metody skanowania.

Wkleić obraz okna

Charakterystyka metody wykorzystanej przez program *nsc6.exe*

(nazwa metody i uzasadnienie decyzji)

.....

.....

5.7a (poniżej) Obraz okna wiersza poleceń z linią polecenia i raportem programu *nsc7.exe*

Wkleić obraz okna

5.7b (poniżej) Obraz okna sniffera uzyskany podczas skanowania programem *nsc7.exe*. Zaznaczono pojedynczą sekwencję pakietów charakterystyczną dla stosowanej metody skanowania.

Wkleić obraz okna

Charakterystyka metody wykorzystanej przez program *nsc7.exe*

(nazwa metody i uzasadnienie decyzji)

.....

.....

5.8a (poniżej) Obraz okna wiersza poleceń z linią polecenia i raportem programu *nsc8.exe*

Wkleić obraz okna

5.8b (poniżej) Obraz okna sniffera uzyskany podczas skanowania programem *nsc8.exe*. Zaznaczono pojedynczą sekwencję pakietów charakterystyczną dla stosowanej metody skanowania.

Wkleić obraz okna

Charakterystyka metody wykorzystanej przez program *nsc8.exe*

(nazwa metody i uzasadnienie decyzji)

.....

.....

Własne uwagi, wnioski i propozycje dotyczące przebiegu ćwiczenia, mające na celu polepszenie procesu kształcenia:

.....

.....

.....