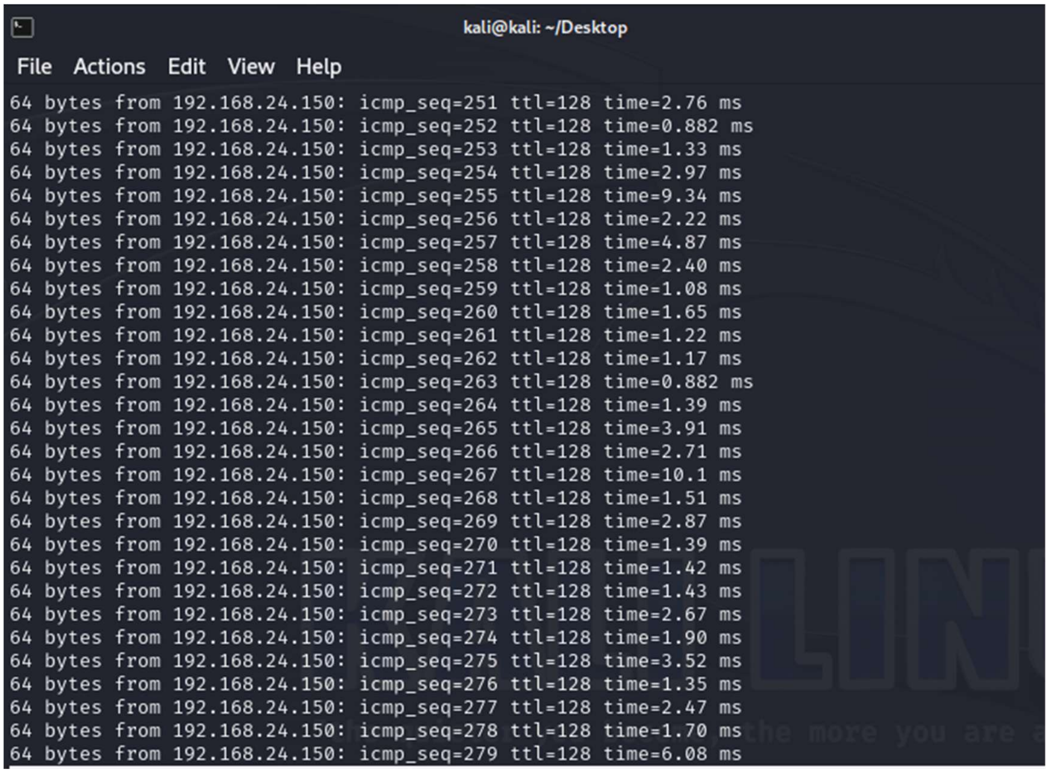
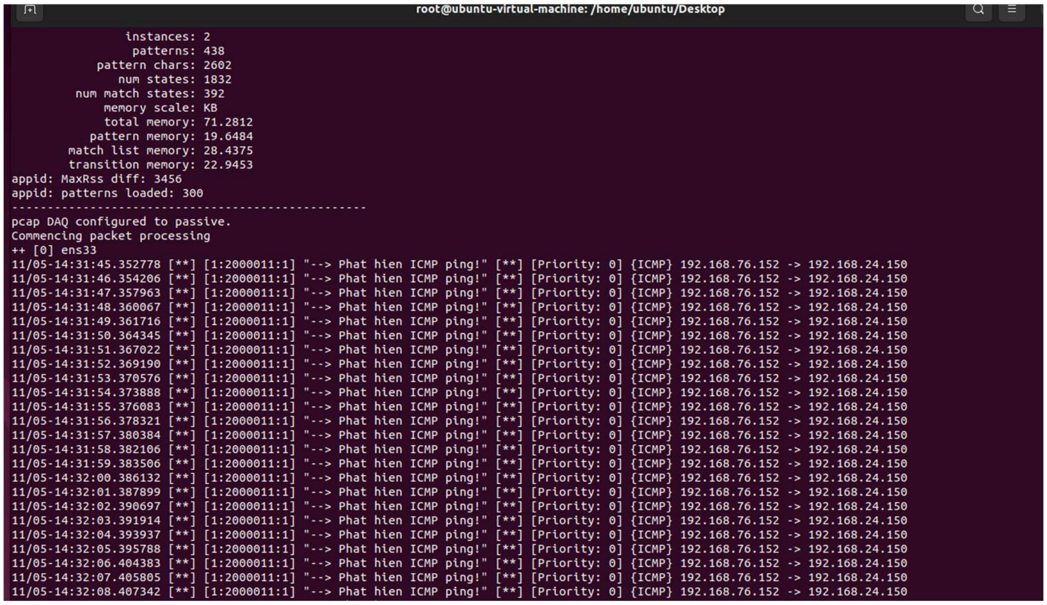
IP attacker: 192.168.76.152
IP victim: 192.168.25.150

1.

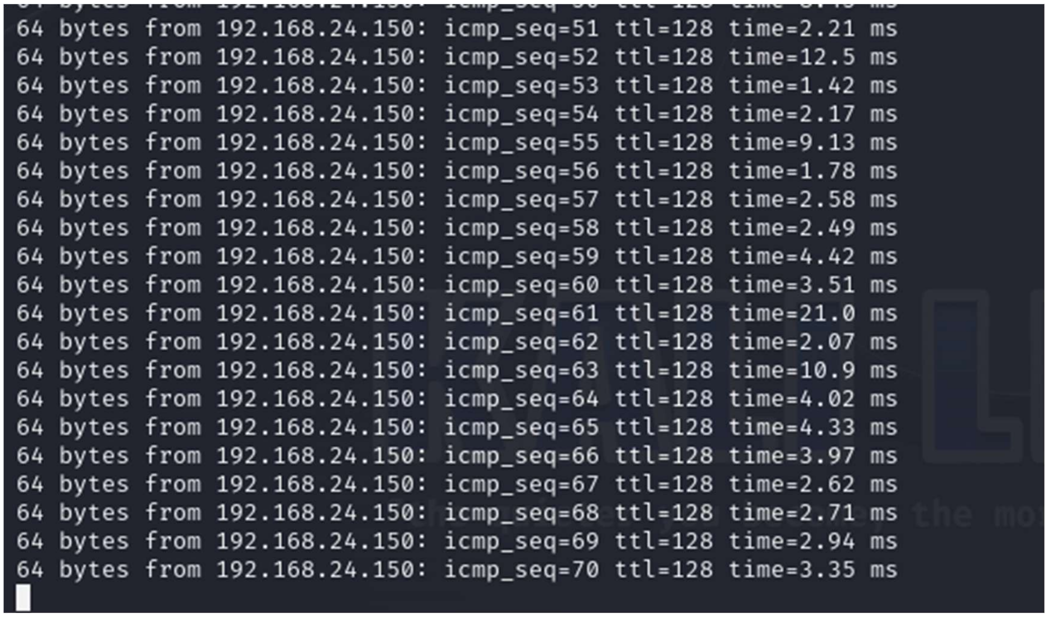


```
64 bytes from 192.168.24.150: icmp_seq=251 ttl=128 time=2.76 ms
64 bytes from 192.168.24.150: icmp_seq=252 ttl=128 time=0.882 ms
64 bytes from 192.168.24.150: icmp_seq=253 ttl=128 time=1.33 ms
64 bytes from 192.168.24.150: icmp_seq=254 ttl=128 time=2.97 ms
64 bytes from 192.168.24.150: icmp_seq=255 ttl=128 time=9.34 ms
64 bytes from 192.168.24.150: icmp_seq=256 ttl=128 time=2.22 ms
64 bytes from 192.168.24.150: icmp_seq=257 ttl=128 time=4.87 ms
64 bytes from 192.168.24.150: icmp_seq=258 ttl=128 time=2.40 ms
64 bytes from 192.168.24.150: icmp_seq=259 ttl=128 time=1.08 ms
64 bytes from 192.168.24.150: icmp_seq=260 ttl=128 time=1.65 ms
64 bytes from 192.168.24.150: icmp_seq=261 ttl=128 time=1.22 ms
64 bytes from 192.168.24.150: icmp_seq=262 ttl=128 time=1.17 ms
64 bytes from 192.168.24.150: icmp_seq=263 ttl=128 time=0.882 ms
64 bytes from 192.168.24.150: icmp_seq=264 ttl=128 time=1.39 ms
64 bytes from 192.168.24.150: icmp_seq=265 ttl=128 time=3.91 ms
64 bytes from 192.168.24.150: icmp_seq=266 ttl=128 time=2.71 ms
64 bytes from 192.168.24.150: icmp_seq=267 ttl=128 time=10.1 ms
64 bytes from 192.168.24.150: icmp_seq=268 ttl=128 time=1.51 ms
64 bytes from 192.168.24.150: icmp_seq=269 ttl=128 time=2.87 ms
64 bytes from 192.168.24.150: icmp_seq=270 ttl=128 time=1.39 ms
64 bytes from 192.168.24.150: icmp_seq=271 ttl=128 time=1.42 ms
64 bytes from 192.168.24.150: icmp_seq=272 ttl=128 time=1.43 ms
64 bytes from 192.168.24.150: icmp_seq=273 ttl=128 time=2.67 ms
64 bytes from 192.168.24.150: icmp_seq=274 ttl=128 time=1.90 ms
64 bytes from 192.168.24.150: icmp_seq=275 ttl=128 time=3.52 ms
64 bytes from 192.168.24.150: icmp_seq=276 ttl=128 time=1.35 ms
64 bytes from 192.168.24.150: icmp_seq=277 ttl=128 time=2.47 ms
64 bytes from 192.168.24.150: icmp_seq=278 ttl=128 time=1.70 ms
64 bytes from 192.168.24.150: icmp_seq=279 ttl=128 time=6.08 ms
```

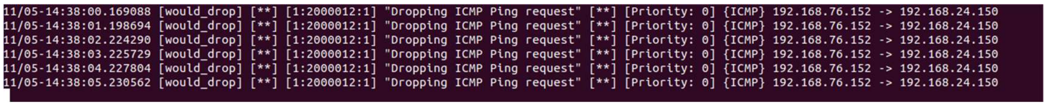


```
                instances: 2
                 patterns: 438
            pattern chars: 2602
               num states: 1832
         num match states: 392
             memory scale: KB
             total memory: 71.2812
           pattern memory: 19.6484
        match list memory: 28.4375
        transition memory: 22.9453
appid: MaxRss diff: 3456
appid: patterns loaded: 300
--------------------------------------------------
pcap DAQ configured to passive.
Commencing packet processing
++ [0] ens33
11/05-14:31:45.352778 [**] [1:2000011:1] "--> Phat hien ICMP ping!" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:31:46.354206 [**] [1:2000011:1] "--> Phat hien ICMP ping!" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:31:47.357963 [**] [1:2000011:1] "--> Phat hien ICMP ping!" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:31:48.360067 [**] [1:2000011:1] "--> Phat hien ICMP ping!" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:31:49.361716 [**] [1:2000011:1] "--> Phat hien ICMP ping!" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:31:50.364345 [**] [1:2000011:1] "--> Phat hien ICMP ping!" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:31:51.367022 [**] [1:2000011:1] "--> Phat hien ICMP ping!" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:31:52.369190 [**] [1:2000011:1] "--> Phat hien ICMP ping!" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:31:53.370576 [**] [1:2000011:1] "--> Phat hien ICMP ping!" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:31:54.373888 [**] [1:2000011:1] "--> Phat hien ICMP ping!" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:31:55.376083 [**] [1:2000011:1] "--> Phat hien ICMP ping!" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:31:56.378321 [**] [1:2000011:1] "--> Phat hien ICMP ping!" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:31:57.380384 [**] [1:2000011:1] "--> Phat hien ICMP ping!" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:31:58.382106 [**] [1:2000011:1] "--> Phat hien ICMP ping!" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:31:59.383506 [**] [1:2000011:1] "--> Phat hien ICMP ping!" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:32:00.386132 [**] [1:2000011:1] "--> Phat hien ICMP ping!" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:32:01.387899 [**] [1:2000011:1] "--> Phat hien ICMP ping!" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:32:02.390697 [**] [1:2000011:1] "--> Phat hien ICMP ping!" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:32:03.391914 [**] [1:2000011:1] "--> Phat hien ICMP ping!" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:32:04.393937 [**] [1:2000011:1] "--> Phat hien ICMP ping!" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:32:05.395788 [**] [1:2000011:1] "--> Phat hien ICMP ping!" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:32:06.404383 [**] [1:2000011:1] "--> Phat hien ICMP ping!" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:32:07.405805 [**] [1:2000011:1] "--> Phat hien ICMP ping!" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:32:08.407342 [**] [1:2000011:1] "--> Phat hien ICMP ping!" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
```

2.

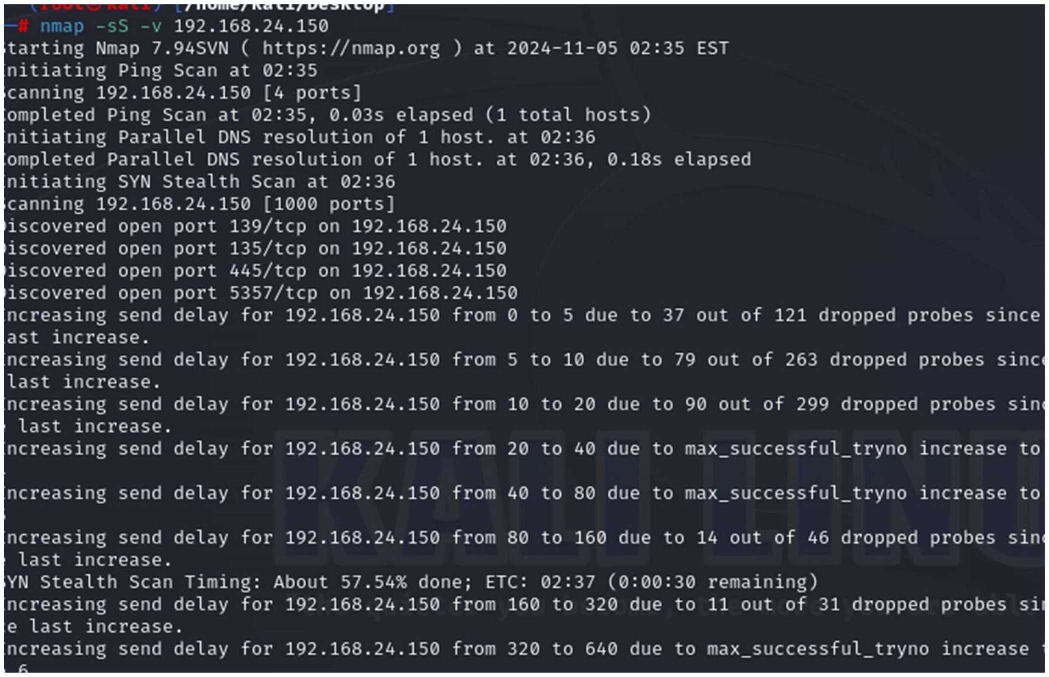


```
64 bytes from 192.168.24.150: icmp_seq=51 ttl=128 time=2.21 ms
64 bytes from 192.168.24.150: icmp_seq=52 ttl=128 time=12.5 ms
64 bytes from 192.168.24.150: icmp_seq=53 ttl=128 time=1.42 ms
64 bytes from 192.168.24.150: icmp_seq=54 ttl=128 time=2.17 ms
64 bytes from 192.168.24.150: icmp_seq=55 ttl=128 time=9.13 ms
64 bytes from 192.168.24.150: icmp_seq=56 ttl=128 time=1.78 ms
64 bytes from 192.168.24.150: icmp_seq=57 ttl=128 time=2.58 ms
64 bytes from 192.168.24.150: icmp_seq=58 ttl=128 time=2.49 ms
64 bytes from 192.168.24.150: icmp_seq=59 ttl=128 time=4.42 ms
64 bytes from 192.168.24.150: icmp_seq=60 ttl=128 time=3.51 ms
64 bytes from 192.168.24.150: icmp_seq=61 ttl=128 time=21.0 ms
64 bytes from 192.168.24.150: icmp_seq=62 ttl=128 time=2.07 ms
64 bytes from 192.168.24.150: icmp_seq=63 ttl=128 time=10.9 ms
64 bytes from 192.168.24.150: icmp_seq=64 ttl=128 time=4.02 ms
64 bytes from 192.168.24.150: icmp_seq=65 ttl=128 time=4.33 ms
64 bytes from 192.168.24.150: icmp_seq=66 ttl=128 time=3.97 ms
64 bytes from 192.168.24.150: icmp_seq=67 ttl=128 time=2.62 ms
64 bytes from 192.168.24.150: icmp_seq=68 ttl=128 time=2.71 ms
64 bytes from 192.168.24.150: icmp_seq=69 ttl=128 time=2.94 ms
64 bytes from 192.168.24.150: icmp_seq=70 ttl=128 time=3.35 ms
```



```
11/05-14:38:00.169088 [would_drop] [**] [1:2000012:1] "Dropping ICMP Ping request" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:38:01.198694 [would_drop] [**] [1:2000012:1] "Dropping ICMP Ping request" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:38:02.224290 [would_drop] [**] [1:2000012:1] "Dropping ICMP Ping request" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:38:03.225729 [would_drop] [**] [1:2000012:1] "Dropping ICMP Ping request" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:38:04.227804 [would_drop] [**] [1:2000012:1] "Dropping ICMP Ping request" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
11/05-14:38:05.230562 [would_drop] [**] [1:2000012:1] "Dropping ICMP Ping request" [**] [Priority: 0] {ICMP} 192.168.76.152 -> 192.168.24.150
```

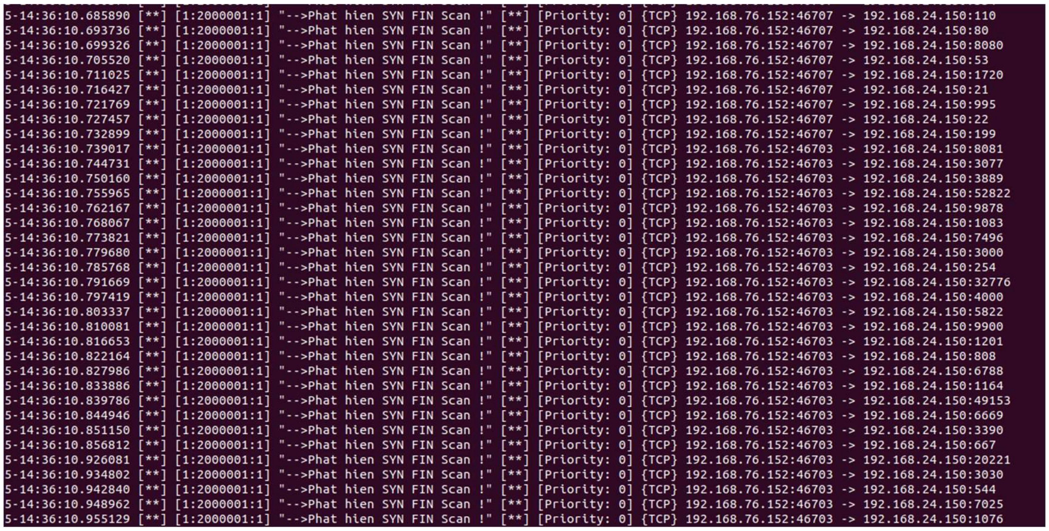
3.



```
 (root㉿kali)-[/home/kali/Desktop]
─# nmap -sS -v 192.168.24.150
tarting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-05 02:35 EST
nitiating Ping Scan at 02:35
canning 192.168.24.150 [4 ports]
ompleted Ping Scan at 02:35, 0.03s elapsed (1 total hosts)
nitiating Parallel DNS resolution of 1 host. at 02:36
ompleted Parallel DNS resolution of 1 host. at 02:36, 0.18s elapsed
nitiating SYN Stealth Scan at 02:36
canning 192.168.24.150 [1000 ports]
iscovered open port 139/tcp on 192.168.24.150
iscovered open port 135/tcp on 192.168.24.150
iscovered open port 445/tcp on 192.168.24.150
iscovered open port 5357/tcp on 192.168.24.150
ncreasing send delay for 192.168.24.150 from 0 to 5 due to 37 out of 121 dropped probes since
ast increase.
ncreasing send delay for 192.168.24.150 from 5 to 10 due to 79 out of 263 dropped probes sinc
last increase.
ncreasing send delay for 192.168.24.150 from 10 to 20 due to 90 out of 299 dropped probes sin
 last increase.
ncreasing send delay for 192.168.24.150 from 20 to 40 due to max_successful_tryno increase to

ncreasing send delay for 192.168.24.150 from 40 to 80 due to max_successful_tryno increase to

ncreasing send delay for 192.168.24.150 from 80 to 160 due to 14 out of 46 dropped probes sin
 last increase.
YN Stealth Scan Timing: About 57.54% done; ETC: 02:37 (0:00:30 remaining)
ncreasing send delay for 192.168.24.150 from 160 to 320 due to 11 out of 31 dropped probes si
e last increase.
ncreasing send delay for 192.168.24.150 from 320 to 640 due to max_successful_tryno increase
 6
```



```
5-14:36:10.685890 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46707 -> 192.168.24.150:110
5-14:36:10.693736 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46707 -> 192.168.24.150:80
5-14:36:10.699326 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46707 -> 192.168.24.150:8080
5-14:36:10.705520 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46707 -> 192.168.24.150:53
5-14:36:10.711025 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46707 -> 192.168.24.150:1720
5-14:36:10.716427 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46707 -> 192.168.24.150:21
5-14:36:10.721769 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46707 -> 192.168.24.150:995
5-14:36:10.727457 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46707 -> 192.168.24.150:22
5-14:36:10.732899 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46707 -> 192.168.24.150:199
5-14:36:10.739017 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:8081
5-14:36:10.744731 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:3077
5-14:36:10.750160 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:3889
5-14:36:10.755965 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:52822
5-14:36:10.762167 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:9878
5-14:36:10.768067 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:1083
5-14:36:10.773821 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:7496
5-14:36:10.779680 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:3000
5-14:36:10.785768 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:254
5-14:36:10.791669 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:32776
5-14:36:10.797419 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:4000
5-14:36:10.803337 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:5822
5-14:36:10.810081 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:9900
5-14:36:10.816653 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:1201
5-14:36:10.822164 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:808
5-14:36:10.827986 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:6788
5-14:36:10.833886 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:1164
5-14:36:10.839786 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:49153
5-14:36:10.844946 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:6669
5-14:36:10.851150 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:3390
5-14:36:10.856812 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:667
5-14:36:10.926081 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:20221
5-14:36:10.934802 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:3030
5-14:36:10.942840 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:544
5-14:36:10.948962 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:7025
5-14:36:10.955129 [**] [1:2000001:1] "-->Phat hien SYN FIN Scan !" [**] [Priority: 0] {TCP} 192.168.76.152:46703 -> 192.168.24.150:1076
```