The following images are the screenshots of the result of TcpAttck script using Wireshark, what I did was trying to scan for open ports for TCP protocol between port 440 to port 443 of the target address 128.46.4.92(the ECN machine public IP address) and perform a SYN flood attack to port 443(it's not actually an effective attack since I only send 10 SYN packets for testing, which won't influence the machine very much). I choose port 443 because by default the machine use port 443 for HTTPS(I also test the port 80 for HTTP and port 22 for SSH which result the similar thing that I didn't include here). As the screenshots shows the SYN packets were successfully sent out to the correct port and only port 443 is open, so another 10 SYN packets then send out to the port 443. All the grey highline content in the screenshots are the packets send out by my local machine, I have filter out all the packets related to other address or ports so everything in the screenshots are only between my local machine and the target address and target port.

addr == 128, 46, 4, 9	2 and tep. port in {440, 441, 442,	, 443, 444, 445, 446, 447, 448, 449,	450}	X □
Time	Source	Destination	Protocol	Length Info
462 9.154768	172.16.20.125	128.46.4.92	TCP	66 1596 → 440 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
463 9.187132	128.46.4.92	172.16.20.125	ICMP	94 Destination unreachable (Host administratively prohibited)
483 9.670814	172.16.20.125	128.46.4.92	TCP	66 1597 → 441 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
486 9.699415	128.46.4.92	172.16.20.125	ICMP	94 Destination unreachable (Host administratively prohibited)
503 10.177528	3 172.16.20.125	128.46.4.92	TCP	66 1598 → 442 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
505 10.229791	1 128.46.4.92	172.16.20.125	ICMP	94 Destination unreachable (Host administratively prohibited)
528 10.683166	5 172.16.20.125	128.46.4.92	TCP	66 1599 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
533 10.710352	2 128.46.4.92	172.16.20.125	TCP	66 443 → 1599 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM
534 10.710562	2 172.16.20.125	128.46.4.92	TCP	54 1599 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
535 10.710839	9 172.16.20.125	128.46.4.92	TCP	54 1599 → 443 [FIN, ACK] Seq=1 Ack=1 Win=65536 Len=0
536 10.711189	9 172.16.20.125	128.46.4.92	TCP	66 1600 → 444 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
539 10.739761	1 128.46.4.92	172.16.20.125	TCP	60 443 → 1599 [ACK] Seq=1 Ack=2 Win=29312 Len=0
540 10.740769	9 128.46.4.92	172.16.20.125	ICMP	94 Destination unreachable (Host administratively prohibited)
541 10.744648	3 128.46.4.92	172.16.20.125	TCP	60 443 → 1599 [FIN, ACK] Seq=1 Ack=2 Win=29312 Len=0
542 10.744819	9 172.16.20.125	128.46.4.92	TCP	54 1599 → 443 [ACK] Seq=2 Ack=2 Win=65536 Len=0
560 11.222773	3 172.16.20.125	128.46.4.92	TCP	66 1601 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
575 11.728425	5 172.16.20.125	128.46.4.92	TCP	66 1603 → 446 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
58 1 11. 757371	1 128.46.4.92	172.16.20.125	ICMP	94 Destination unreachable (Host administratively prohibited)
612 12.234999	9 172.16.20.125	128.46.4.92	TCP	66 1604 → 447 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
613 12.263786	0 128.46.4.92	172.16.20.125	ICMP	94 Destination unreachable (Host administratively prohibited)
636 12.742633	3 172.16.20.125	128.46.4.92	TCP	66 1605 → 448 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
642 12.772131	1 128.46.4.92	172.16.20.125	ICMP	94 Destination unreachable (Host administratively prohibited)
664 13.249373	3 172.16.20.125	128.46.4.92	TCP	66 1606 → 449 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
666 13.278002	2 128.46.4.92	172.16.20.125	ICMP	94 Destination unreachable (Host administratively prohibited)
679 13.758482	2 172.16.20.125	128.46.4.92	TCP	66 1607 → 450 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
685 13.789382	2 128.46.4.92	172.16.20.125	ICMP	94 Destination unreachable (Host administratively prohibited)
ma 717. 60 h	utoc on wino (100 hitc	A hytoc contuned	(100 hi+c) a	n intenface \Davice\\NDE [D703031E 7CAC ADCC ADEC 303630EA33AA] id a
642 12.772131		172.16.20.125	ICMP	94 Destination unreachable (Host administratively prohibited)
664 13.249373		128.46.4.92	TCP	66 1606 → 449 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
666 13.278002		172.16.20.125	ICMP	94 Destination unreachable (Host administratively prohibited)
679 13.758482		128.46.4.92	TCP	66 1607 → 450 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
685 13.789382		172.16.20.125	ICMP	94 Destination unreachable (Host administratively prohibited)
727 14.268219		128.46.4.92	TCP	66 1609 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
728 14.296923		172.16.20.125	TCP	66 443 → 1609 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM
729 14.297157		128.46.4.92	TCP	54 1609 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
733 14.307868		128.46.4.92	TCP	54 62194 → 443 [SYN] Seq=0 Win=8192 Len=0
734 14.309804		128.46.4.92	TCP	54 35766 → 443 [SYN] Seq=0 Win=8192 Len=0
735 14.311816		128.46.4.92	TCP	54 142 → 443 [SYN] Seq=0 Win=8192 Len=0
736 14.313828	3 172.16.20.125	128.46.4.92	TCP	54 5734 → 443 [SYN] Seq=0 Win=8192 Len=0
727 14 216404	4 70 45 20 425		TOD	

642 12.772131	128.46.4.92	172.16.20.125	ICMP	94 Destination unreachable (Host administratively prohibited)	
664 13.249373	172.16.20.125	128.46.4.92	TCP	66 1606 → 449 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1	
666 13.278002	128.46.4.92	172.16.20.125	ICMP	94 Destination unreachable (Host administratively prohibited)	
679 13.758482	172.16.20.125	128.46.4.92	TCP	66 1607 → 450 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1	
685 13.789382	128.46.4.92	172.16.20.125	ICMP	94 Destination unreachable (Host administratively prohibited)	
727 14.268219	172.16.20.125	128.46.4.92	TCP	66 1609 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1	
728 14.296923	128.46.4.92	172.16.20.125	TCP	66 443 → 1609 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=	
729 14.297157	172.16.20.125	128.46.4.92	TCP	54 1609 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0	
733 14.307868	172.16.20.125	128.46.4.92	TCP	54 62194 → 443 [SYN] Seq=0 Win=8192 Len=0	
734 14.309804	172.16.20.125	128.46.4.92	TCP	54 35766 → 443 [SYN] Seq=0 Win=8192 Len=0	
735 14.311810	172.16.20.125	128.46.4.92	TCP	54 142 → 443 [SYN] Seq=0 Win=8192 Len=0	
736 14.313828	172.16.20.125	128.46.4.92	TCP	54 5734 → 443 [SYN] Seq=0 Win=8192 Len=0	
737 14.316404	172.16.20.125	128.46.4.92	TCP	54 13565 → 443 [SYN] Seq=0 Win=8192 Len=0	
738 14.318821	172.16.20.125	128.46.4.92	TCP	54 9826 → 443 [SYN] Seq=0 Win=8192 Len=0	
739 14.321245	172.16.20.125	128.46.4.92	TCP	54 29394 → 443 [SYN] Seq=0 Win=8192 Len=0	
741 14.324088	172.16.20.125	128.46.4.92	TCP	54 2638 → 443 [SYN] Seq=0 Win=8192 Len=0	
742 14.326390	172.16.20.125	128.46.4.92	TCP	54 56345 → 443 [SYN] Seq=0 Win=8192 Len=0	
743 14.328722	172.16.20.125	128.46.4.92	TCP	54 1672 → 443 [SYN] Seq=0 Win=8192 Len=0	
744 14.331368	172.16.20.125	128.46.4.92	TCP	54 1609 → 443 [FIN, ACK] Seq=1 Ack=1 Win=65536 Len=0	
745 14.336495	128.46.4.92	172.16.20.125	TCP	60 443 → 62194 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460	
747 14.338386	128.46.4.92	172.16.20.125	TCP	60 443 → 35766 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460	
748 14.338796	128.46.4.92	172.16.20.125	TCP	60 443 → 142 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460	
749 14.340947	128.46.4.92	172.16.20.125	TCP	60 443 → 5734 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460	
750 14.344179	128.46.4.92	172.16.20.125	TCP	60 443 → 13565 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460	
751 14.345957	128.46.4.92	172.16.20.125	TCP	60 443 → 9826 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460	
752 14.349892	128.46.4.92	172.16.20.125	TCP	60 443 → 29394 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460	
7. FARM 736, FA hydrog on vine (A22 hits) FA hydrog continued (A22 hits) on intenface \Device\NDF (D703D24F 766 ABCC ABCC ABCC ABCC ABCC ABCC ABCC AB					

751 14.345957	128.46.4.92	172.16.20.125	TCP	60 443 → 9826 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
752 14.349892	128.46.4.92	172.16.20.125	TCP	60 443 → 29394 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
753 14.351317	128.46.4.92	172.16.20.125	ТСР	60 443 → 2638 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
754 14.354848	128.46.4.92	172.16.20.125	TCP	60 443 → 56345 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
755 14.356332	128.46.4.92	172.16.20.125	TCP	60 443 → 1672 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
756 14.360031	128.46.4.92	172.16.20.125	TCP	60 443 → 1609 [ACK] Seg=1 Ack=2 Win=29312 Len=0
757 14.361150	128.46.4.92	172.16.20.125	TCP	60 443 → 1609 [FIN, ACK] Seq=1 Ack=2 Win=29312 Len=0
758 14.361226	172.16.20.125	128.46.4.92	TCP	54 1609 → 443 [ACK] Seq=2 Ack=2 Win=65536 Len=0
831 15.537764	128.46.4.92	172.16.20.125	TCP	60 [TCP Retransmission] 443 → 2638 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=
832 15.537903	128.46.4.92	172.16.20.125	TCP	60 [TCP Retransmission] 443 → 142 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
833 15.537903	128.46.4.92	172.16.20.125	TCP	60 [TCP Retransmission] 443 → 13565 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len
834 15.539144	128.46.4.92	172.16.20.125	TCP	60 [TCP Retransmission] 443 → 35766 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len
838 15.737658	128.46.4.92	172.16.20.125	TCP	60 [TCP Retransmission] 443 → 9826 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=
839 15.737928	128.46.4.92	172.16.20.125	TCP	60 [TCP Retransmission] 443 → 5734 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=
840 15.739270	128.46.4.92	172.16.20.125	TCP	60 [TCP Retransmission] 443 → 62194 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len
856 15.937661	128.46.4.92	172.16.20.125	TCP	60 [TCP Retransmission] 443 → 1672 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=
857 15.938991	128.46.4.92	172.16.20.125	TCP	60 [TCP Retransmission] 443 → 56345 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len
858 15.939129	128.46.4.92	172.16.20.125	TCP	60 [TCP Retransmission] 443 → 29394 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len
930 17.538032	128.46.4.92	172.16.20.125	TCP	60 [TCP Retransmission] 443 → 13565 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len
931 17.538232	128.46.4.92	172.16.20.125	TCP	60 [TCP Retransmission] 443 → 142 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
932 17.538232	128.46.4.92	172.16.20.125	TCP	60 [TCP Retransmission] 443 → 2638 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=
933 17.539214	128.46.4.92	172.16.20.125	TCP	60 [TCP Retransmission] 443 → 35766 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len
948 17.738278	128.46.4.92	172.16.20.125	TCP	60 [TCP Retransmission] 443 → 5734 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=
949 17.738416	128.46.4.92	172.16.20.125	TCP	60 [TCP Retransmission] 443 → 9826 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=
950 17.739491	128.46.4.92	172.16.20.125	TCP	60 [TCP Retransmission] 443 → 62194 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len
959 17.937861	128.46.4.92	172.16.20.125	TCP	60 [TCP Retransmission] 443 → 1672 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=

Forms 752. 50 histor on wins (400 hits) 60 histor contined (400 hits) on intenfers (Doubles) NDE (D7070715 7646 ADEC ADEC 2036305423AA) 34 A

The following is the content in the logfile:

New message log:

1

From li3402@purdue.edu Sat Mar 26 16:54:02 2022

Subject: ece 404 hw9 test

Folder: my404Folder 6154

New message log:

2

procmail: Couldn't determine implicit lockfile from "/usr/sbin/sendmail"

From li3402@purdue.edu Sat Mar 26 17:00:50 2022

Subject: Test No. 2

Folder: /usr/sbin/sendmail -oi li3402@purdue.edu 6703

New message log:

3

procmail: Couldn't determine implicit lockfile from "/usr/sbin/sendmail"

From li3402@purdue.edu Sat Mar 26 17:06:08 2022

Subject: Test to Transfer File

Folder: /usr/sbin/sendmail -oi li3402@purdue.edu 115093

New message log:

4

procmail: Couldn't determine implicit lockfile from "/usr/sbin/sendmail"

From li3402@purdue.edu Sat Mar 26 17:07:45 2022

Subject: Test to Send mail Again

Folder: /usr/sbin/sendmail -oi li3402@purdue.edu 6385

New message log:

5

procmail: Couldn't determine implicit lockfile from "/usr/sbin/sendmail"

From li3402@purdue.edu Sat Mar 26 17:18:20 2022

Subject:

Folder: /usr/sbin/sendmail -oi li3402@purdue.edu 6875

New message log:

6

From bounces+14629914-d697-ece404l3=ecn.purdue.edu@u14629914.wl165.sendgrid.net Sat Mar 26 17:23:55 2022

Subject: Please confirm your subscription

Folder: spamFolder 8317