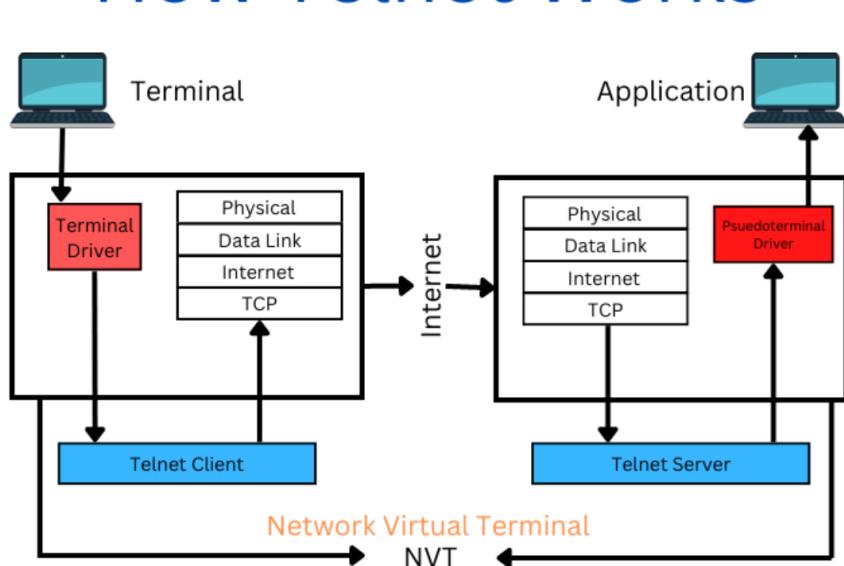


Strange Telnet & UDP Connections

When we look for strange traffic, we should always consider telnet and UDP traffic. After all, these can be overlooked, but can especially reveal during our traffic analysis efforts.

Telnet



Telnet is a network protocol that allows a bidirectional interactive communication session between two devices over a network. This protocol was developed in the 1970s and was defined in RFC 854. As of recent years, its usage has decreased significantly as opposed to SSH.

In many older cases, such as our Windows NT like machines, they may still utilize telnet to provide remote command and control to microsoft terminal services.

However, we should always watch for weird and strange telnet communications as it can also be used by attackers for malicious purposes such as data exfiltration and tunneling.

Finding Traditional Telnet Traffic Port 23

Related PCAP File(s):

- [telnet_tunneling_23.pcapng](#)

Suppose we were to open Wireshark, we might notice some telnet communications originating from Port 23. In this case, we can always inspect this traffic further.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.10.5	192.168.10.7	TCP	74	59694 → 23 [SYN] Seq=0 Win=64240 Len=0 TSeq=1460 SACK_PERM TSeqval=3668950072 TSecr=0 WS=128
2	0.000148	192.168.10.7	192.168.10.5	TCP	74	23 → 59694 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 NSS=1460 SACK_PERM TSeqval=256665246 TSecr=3668950072 WS=128
3	0.000242	192.168.10.5	192.168.10.7	TCP	66	59694 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSeqval=3668950072 TSecr=256665246
4	3.899331	192.168.10.5	192.168.10.7	TELNET	74	Telnet Data ...

Table of Contents

Introduction

- Intermediate Network Traffic Analysis Overview

Link Layer Attacks

- ARP Spoofing & Abnormality Detection
- ARP Scanning & Denial-of-Service
- 802.11 Denial-of-Service
- Rogue Access Point & Evil-Twin Attacks

Detecting Network Abnormalities

- Fragmentation Attacks
- IP Source & Destination Spoofing Attacks
- IP Time-to-Live Attacks
- TCP Handshake Abnormalities
- TCP Connection Resets & Hijacking
- ICMP Tunneling

Application Layer Attacks

- HTTP/HTTPs Service Enumeration Detection
- Strange HTTP Headers
- Cross-Site Scripting (XSS) & Code Injection Detection
- SSL Renegotiation Attacks
- Peculiar DNS Traffic
- Strange Telnet & UDP Connections

Skills Assessment

- Skills Assessment

My Workstation

3 3.891093	192.168.10.7	192.168.10.5	TCP	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 23 Telnet Data ...
6 15.945673	192.168.10.5	192.168.10.7	TELNET	66 23 + 59694 [ACK] Seq=1 Ack=71 Win=65152 Len=0 TSval=25668966627	66 23 Telnet Data ...
7 15.946957	192.168.10.7	192.168.10.5	TCP	66 23 + 59694 [ACK] Seq=1 Ack=71 Win=65152 Len=0 TSval=25668966627	66 23 + 59694 [ACK] Seq=1 Ack=74 Win=65152 Len=0 TSval=25668970198
8 20.107981	192.168.10.5	192.168.10.7	TELNET	66 23 + 59694 [ACK] Seq=1 Ack=74 Win=65152 Len=0 TSval=25668970198	66 23 + 59694 [ACK] Seq=1 Ack=74 Win=65152 Len=0 TSval=25668970198
9 20.108158	192.168.10.7	192.168.10.5	TCP	66 23 + 59694 [ACK] Seq=1 Ack=74 Win=65152 Len=0 TSval=25668970198	66 23 + 59694 [ACK] Seq=1 Ack=74 Win=65152 Len=0 TSval=25668970198
10 20.108159	192.168.10.5	192.168.10.7	TELNET	66 23 + 59694 [ACK] Seq=1 Ack=74 Win=65152 Len=0 TSval=25668970198	66 23 + 59694 [ACK] Seq=1 Ack=74 Win=65152 Len=0 TSval=25668970198
11 20.399897	192.168.10.7	192.168.10.5	TCP	66 23 + 59694 [ACK] Seq=1 Ack=77 Win=65152 Len=0 TSval=25668970482	66 23 + 59694 [ACK] Seq=1 Ack=77 Win=65152 Len=0 TSval=25668970482
12 20.685781	192.168.10.5	192.168.10.7	TELNET	69 Telnet Data	69 Telnet Data
13 20.689823	192.168.10.7	192.168.10.5	TCP	66 23 + 59694 [ACK] Seq=1 Ack=80 Win=65152 Len=0 TSval=25668970768	66 23 + 59694 [ACK] Seq=1 Ack=80 Win=65152 Len=0 TSval=25668970768
14 20.962655	192.168.10.5	192.168.10.7	TELNET	69 Telnet Data	69 Telnet Data
15 20.962935	192.168.10.7	192.168.10.5	TCP	66 23 + 59694 [ACK] Seq=1 Ack=83 Win=65152 Len=0 TSval=256686208 TSecr=3668971045	66 23 + 59694 [ACK] Seq=1 Ack=83 Win=65152 Len=0 TSval=256686208 TSecr=3668971045
16 21.242599	192.168.10.5	192.168.10.7	TELNET	69 Telnet Data	69 Telnet Data
17 21.242792	192.168.10.7	192.168.10.5	TCP	66 23 + 59694 [ACK] Seq=1 Ack=86 Win=65152 Len=0 TSval=256686488 TSecr=3668971325	66 23 + 59694 [ACK] Seq=1 Ack=86 Win=65152 Len=0 TSval=256686488 TSecr=3668971325
18 21.538623	192.168.10.5	192.168.10.7	TELNET	69 Telnet Data	69 Telnet Data
19 21.538625	192.168.10.7	192.168.10.5	TCP	66 23 + 59694 [ACK] Seq=1 Ack=89 Win=65152 Len=0 TSval=256686784 TSecr=3668971622	66 23 + 59694 [ACK] Seq=1 Ack=89 Win=65152 Len=0 TSval=256686784 TSecr=3668971622
20 21.829445	192.168.10.5	192.168.10.7	TELNET	69 Telnet Data	69 Telnet Data

OFFLINE

Start Instance

∞ / 1 spawns left

Fortunately for us, telnet traffic tends to be decrypted and easily inspectable, but like ICMP, DNS, and other tunneling methods, attackers may encrypt, encode, or obfuscate this text. So we should always be careful.

```
> Frame 6: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface \Device\NPF_{CCC4B960-1E92-4BD5-BBF3-11E2DFD12FE1}, id 0
> Ethernet II, Src: PcsCompu_53:0c:ba (00:00:27:53:0c:ba), Dst: Micro-5t_95:68:2a (44:8a:5b:95:68:2a)
> Internet Protocol Version 4, Src: 192.168.10.5, Dst: 192.168.10.7
> Transmission Control Protocol, Src Port: 59694, Dst Port: 23, Seq: 9, Ack: 1, Len: 62
Telnet
Data: telnet is unencrypted, so we can find things a little easier\r\n
```

Unrecognized TCP Telnet in Wireshark

Related PCAP File(s):

- [telnet_tunneling_9999.pcapng](#)

Telnet is just a communication protocol, and as such can be easily switched to another port by an attacker. Keeping an eye on these strange port communications can allow us to find potentially malicious actions. Lets take the following for instance.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.10.5	192.168.10.7	TCP	74	56378 + 9999 [SYN] Seq=0 Win=64348 Len=0 MSS=1468 SACK_PERM TSval=3668729713 TSecr=0 WSz=128
2	0.000263	192.168.10.7	192.168.10.5	TCP	74	9999 + 56276 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1468 SACK_PERM TSval=356444999 TSecr=3668729713 WSz=128
3	8.000379	192.168.10.5	192.168.10.7	TCP	66	56276 + 9999 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3668729713 TSecr=256444999
4	13.763743	192.168.10.5	192.168.10.7	TCP	82	56276 + 9999 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=16 TSval=3668743483 TSecr=256444999
5	13.763883	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=1 Ack=17 Win=65152 Len=0 TSval=256458762 TSecr=3668743483
6	17.849089	192.168.10.5	192.168.10.7	TCP	69	56276 + 9999 [PSH, ACK] Seq=17 Ack=1 Win=64256 Len=3 TSval=3668747571 TSecr=256458762
7	17.849232	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=1 Ack=18 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
8	18.668918	192.168.10.5	192.168.10.7	TCP	66	56276 + 9999 [ACK] Seq=18 Ack=19 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
9	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=19 Ack=20 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=20 Ack=21 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=21 Ack=22 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=22 Ack=23 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=23 Ack=24 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=24 Ack=25 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=25 Ack=26 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=26 Ack=27 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=27 Ack=28 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=28 Ack=29 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=29 Ack=30 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=30 Ack=31 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=31 Ack=32 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=32 Ack=33 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=33 Ack=34 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=34 Ack=35 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=35 Ack=36 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=36 Ack=37 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=37 Ack=38 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=38 Ack=39 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=39 Ack=40 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=40 Ack=41 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=41 Ack=42 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=42 Ack=43 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=43 Ack=44 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=44 Ack=45 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=45 Ack=46 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=46 Ack=47 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=47 Ack=48 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=48 Ack=49 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=49 Ack=50 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=50 Ack=51 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=51 Ack=52 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=52 Ack=53 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=53 Ack=54 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=54 Ack=55 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=55 Ack=56 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=56 Ack=57 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=57 Ack=58 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=58 Ack=59 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=59 Ack=60 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=60 Ack=61 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=61 Ack=62 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=62 Ack=63 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=63 Ack=64 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=64 Ack=65 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=65 Ack=66 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=66 Ack=67 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.5	192.168.10.7	TCP	66	9999 + 56276 [ACK] Seq=67 Ack=68 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10	18.669396	192.168.10.7	192.168.10.5	TCP	66	9999 + 56276 [ACK] Seq=68 Ack=69 Win=65152 Len=0 TSval=256458762 TSecr=3668747571
10</						

Doing so can allow us to inspect potentially malicious actions.

Telnet Protocol through IPv6

Related PCAP File(s):

- telnet_tunneling_ipv6.pcapng

After all, unless our local network is configured to utilize IPv6, observing IPv6 traffic can be an indicator of bad actions within our environment. We might notice the usage of IPv6 addresses for telnet like the following.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000	fe80::c9c8:ed3:1b10..	fe80::468a:5bff:fe9..	TELNET	89	Telnet Data ...
2	0.0000218	fe80::468a:5bff:fe9..	fe80::c9c8:ed3:1b10..	TCP	86	23 → 51222 [ACK] Seq=1 Ack=4 Win=503 Len=0 TSval=579109237 TSecr=3911462172
3	0.327967	fe80::c9c8:ed3:1b10..	fe80::468a:5bff:fe9..	TELNET	89	Telnet Data ...
4	0.328161	fe80::468a:5bff:fe9..	fe80::c9c8:ed3:1b10..	TCP	86	23 → 51222 [ACK] Seq=1 Ack=7 Win=503 Len=0 TSval=579109565 TSecr=3911462500
5	0.630079	fe80::c9c8:ed3:1b10..	fe80::468a:5bff:fe9..	TELNET	89	Telnet Data ...
6	0.630258	fe80::468a:5bff:fe9..	fe80::c9c8:ed3:1b10..	TCP	86	23 → 51222 [ACK] Seq=10 Ack=10 Win=503 Len=0 TSval=579109867 TSecr=3911462802
7	0.939934	fe80::c9c8:ed3:1b10..	fe80::468a:5bff:fe9..	TELNET	89	Telnet Data ...
8	0.940118	fe80::468a:5bff:fe9..	fe80::c9c8:ed3:1b10..	TCP	86	23 → 51222 [ACK] Seq=1 Ack=13 Win=503 Len=0 TSval=579110177 TSecr=3911463112
9	1.272028	fe80::c9c8:ed3:1b10..	fe80::468a:5bff:fe9..	TELNET	89	Telnet Data ...
10	1.272207	fe80::468a:5bff:fe9..	fe80::c9c8:ed3:1b10..	TCP	86	23 → 51222 [ACK] Seq=1 Ack=16 Win=503 Len=0 TSval=579110509 TSecr=3911463444
11	2.219247	fe80::c9c8:ed3:1b10..	fe80::468a:5bff:fe9..	TELNET	89	Telnet Data ...
12	2.219476	fe80::468a:5bff:fe9..	fe80::c9c8:ed3:1b10..	TCP	86	23 → 51222 [ACK] Seq=1 Ack=19 Win=503 Len=0 TSval=579111457 TSecr=3911464392
13	5.083361	fe80::468a:5bff:fe9..	fe80::c9c8:ed3:1b10..	ICMPv6	86	Neighbor Solicitation for fe80::c9c8:ed3:1b10::f10b from 44:8a:5b:95:68:2a
14	5.083564	fe80::c9c8:ed3:1b10..	fe80::468a:5bff:fe9..	ICMPv6	78	Neighbor Advertisement fe80::c9c8:ed3:1b10::f10b (sol)
15	11.093126	fe80::c9c8:ed3:1b10..	fe80::468a:5bff:fe9..	TELNET	130	Telnet Data ...

We can narrow down our filter in Wireshark to only show telnet traffic from these addresses with the following filter.

```
• ((ipv6.src_host == fe80::c9c8:ed3:1b10:f10b) or (ipv6.dst_host == fe80::c9c8:ed3:1b10:f10b)) and telnet
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000	fe80::c9c8:ed3:1b10..	fe80::468a:5bff:fe9..	TELNET	89	Telnet Data ...
3	0.327967	fe80::c9c8:ed3:1b10..	fe80::468a:5bff:fe9..	TELNET	89	Telnet Data ...
5	0.630079	fe80::c9c8:ed3:1b10..	fe80::468a:5bff:fe9..	TELNET	89	Telnet Data ...
7	0.939934	fe80::c9c8:ed3:1b10..	fe80::468a:5bff:fe9..	TELNET	89	Telnet Data ...
9	1.272028	fe80::c9c8:ed3:1b10..	fe80::468a:5bff:fe9..	TELNET	89	Telnet Data ...
11	2.219247	fe80::c9c8:ed3:1b10..	fe80::468a:5bff:fe9..	TELNET	89	Telnet Data ...
15	11.093126	fe80::c9c8:ed3:1b10..	fe80::468a:5bff:fe9..	TELNET	130	Telnet Data ...
17	19.777904	fe80::c9c8:ed3:1b10..	fe80::468a:5bff:fe9..	TELNET	89	Telnet Data ...
19	20.191486	fe80::c9c8:ed3:1b10..	fe80::468a:5bff:fe9..	TELNET	89	Telnet Data ...
21	20.643738	fe80::c9c8:ed3:1b10..	fe80::468a:5bff:fe9..	TELNET	89	Telnet Data ...
23	21.032943	fe80::c9c8:ed3:1b10..	fe80::468a:5bff:fe9..	TELNET	89	Telnet Data ...
25	21.443061	fe80::c9c8:ed3:1b10..	fe80::468a:5bff:fe9..	TELNET	89	Telnet Data ...
27	21.862009	fe80::c9c8:ed3:1b10..	fe80::468a:5bff:fe9..	TELNET	89	Telnet Data ...
29	22.246044	fe80::c9c8:ed3:1b10..	fe80::468a:5bff:fe9..	TELNET	89	Telnet Data ...

Likewise, we can inspect the contents of these packets through their data field, or by following the TCP stream.

```
> Frame 15: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface \Device\NPF_{CCC4B960-1E92-4BD5-BBF3-11E2DFD12FE1}, id 0
> Ethernet II, Src: PcsCompu_53:0c:ba (08:00:27:53:0c:ba), Dst: Micro-St_95:68:2a (44:8a:5b:95:68:2a)
> Internet Protocol Version 6, Src: fe80::c9c8:ed3:1b10:f10b, Dst: fe80::468a:5bff:fe9:682a
> Transmission Control Protocol, Src Port: 51222, Dst Port: 23, Seq: 19, Ack: 1, Len: 44
` Telnet
  Data: ipv6 also can be used for telnet tunneling\r\n
```

Watching UDP Communications

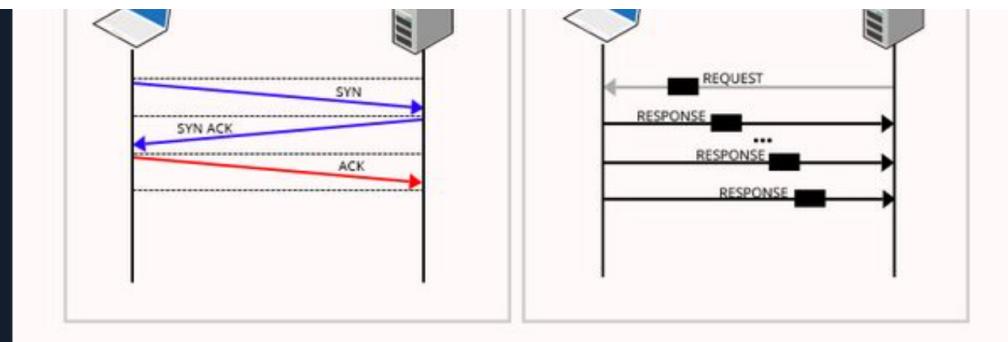
Related PCAP File(s):

- udp_tunneling.pcapng

On the other hand, attackers might opt to use UDP connections over TCP in their exfiltration efforts.

TCP Vs UDP Communication





One of the biggest distinguishing aspects between TCP and UDP is that UDP is connectionless and provides fast transmission. Let's take the following traffic for instance.

No.	Time	Source	Destination	Protocol	Length	Info
15	10.178286	192.168.10.5	192.168.10.7	UDP	60	46678 → 12345 Len=2
16	10.864737	192.168.10.5	192.168.10.7	UDP	60	46678 → 12345 Len=2
17	11.595531	192.168.10.5	192.168.10.7	UDP	60	46678 → 12345 Len=2
18	12.082710	192.168.10.5	192.168.10.7	UDP	60	46678 → 12345 Len=2
19	12.706286	192.168.10.5	192.168.10.7	UDP	60	46678 → 12345 Len=2
20	13.584752	192.168.10.5	192.168.10.7	UDP	60	46678 → 12345 Len=2
21	13.997879	192.168.10.5	192.168.10.7	UDP	60	46678 → 12345 Len=2
22	14.703007	192.168.10.5	192.168.10.7	UDP	60	46678 → 12345 Len=2
23	21.214295	192.168.10.5	192.168.10.7	UDP	60	46678 → 12345 Len=2
24	21.819600	192.168.10.5	192.168.10.7	UDP	60	46678 → 12345 Len=2
25	22.826006	192.168.10.5	192.168.10.7	UDP	60	46678 → 12345 Len=2
26	24.276725	192.168.10.5	192.168.10.7	UDP	60	46678 → 12345 Len=2
27	26.929886	192.168.10.5	192.168.10.7	UDP	60	46678 → 12345 Len=2
28	27.328421	192.168.10.5	192.168.10.7	UDP	60	46678 → 12345 Len=2
29	27.692619	192.168.10.5	192.168.10.7	UDP	60	46678 → 12345 Len=2
30	28.033756	192.168.10.5	192.168.10.7	UDP	60	46678 → 12345 Len=2
31	28.372636	192.168.10.5	192.168.10.7	UDP	60	46678 → 12345 Len=2
32	28.695390	192.168.10.5	192.168.10.7	UDP	60	46678 → 12345 Len=2

We will notice that instead of a SYN, SYN/ACK, ACK sequence, the communications are immediately sent over to the recipient. Like TCP, we can follow UDP traffic in Wireshark, and inspect its contents.

9

10

UDP can be superb for exfil especially in the case of quick connections, unlike TCP, which is super monitored. Hence why we attackers like it

Common Uses of UDP

UDP although less reliable than TCP provides quicker connections through its connectionless state. As such, we might find legitimate traffic that uses UDP like the following:

Step	Description
1. Real-time Applications	Applications like streaming media, online gaming, real-time voice and video communications
2. DNS (Domain Name System)	DNS queries and responses use UDP
3. DHCP (Dynamic Host Configuration Protocol)	DHCP uses UDP to assign IP addresses and configuration information to network devices.
4. SNMP (Simple Network Management Protocol)	SNMP uses UDP for network monitoring and management
5. TFTP (Trivial File Transfer Protocol)	TFTP uses UDP for simple file transfers, commonly used by older Windows systems and others.



Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK

139ms

⚠️ Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...



Enable step-by-step solutions for all questions ⓘ ⚡

Questions

Answer the question(s) below to complete this Section and earn cubes!

+ 1 🎁 Inspect the telnet_tunneling_ipv6.pcapng file, part of this module's resources, and enter the hidden flag as your answer. Answer format: HTB(____) (Replace all spaces with underscores)

HTB(Ipv6_is_my_best_friend)

Submit

◀ Previous

Next ▶

✓ Mark Complete & Next

Powered by  HACKTHEBOX 