Packet Info tcpdump

1. Advanced tcpdump for TLS Analysis

Option 1: Detailed tcpdump with ASCII output

```
# Capture with full packet details and ASCII representation
sudo tcpdump -i lo -A -s 0 port 8443 -nn
```

Option 2: Hex dump format

```
# Show raw packet data in hex format
sudo tcpdump -i lo -X -s 0 port 8443 -nn
```

Option 3: Save to file for later analysis

```
# Capture to pcap file
sudo tcpdump -i lo -s 0 port 8443 -w packets.pcap
```

```
tshark -r packets.pcap -Y "ssl.handshake"
```

```
tshark -nr packets.pcap -Y "ssl.handshake.ciphersuite" -T fields -e
ssl.handshake.ciphersuit
```

Let me demonstrate with a practical example. First, let me start a packet capture and then make a connection:

```
sudo timeout 10 tcpdump -i lo -A -s 0 port 8443 -nn &
```

Now let me start the server and make a connection to capture the TLS handshake:

```
./CrowApp &
```

```
sleep 2 && curl -k https://192.168.1.10:8443/ && sleep 2
```

Complete toolkit for TLS handshake analysis from command line:

1. tcpdump - Basic Packet Capture

```
# Capture TLS handshake with full packet content
sudo tcpdump -i lo -X -s 0 'port 8443 and (tcp[20:1] = 0x16 or tcp[20:1] =
0x14 or tcp[20:1] = 0x15)'

# Save to file for analysis
sudo tcpdump -i lo -s 0 port 8443 -w tls_capture.pcap
```

```
# Show only TLS handshake packets
sudo tcpdump -i lo -X 'port 8443 and tcp[((tcp[12:1] & 0xf0) >> 2):1] =
0x16'
```

---

2. tshark - Wireshark Command Line

```
which tshark
```

```
sudo timeout 8 tshark -i lo -f "port 8443" -Y "tls.handshake.type" &
```

```
sleep 2 && curl -k https://192.168.1.10:8443/ && sleep 3
```

Advanced

---

1. tshark - Advanced TLS Analysis

```
# Show only TLS handshake messages
sudo tshark -i lo -f "port 8443" -Y "tls.handshake.type"

# Detailed TLS handshake with cipher info
sudo tshark -i lo -f "port 8443" -Y "tls" -V

# Show TLS certificate details
sudo tshark -i lo -f "port 8443" -Y "tls.handshake.certificate"

# Export TLS session info
sudo tshark -i lo -f "port 8443" -T fields -e tls.handshake.type -e
tls.handshake.version
```

2. OpenSSL for TLS Connection Analysis

```
# Test TLS connection and show certificate
openssl s_client -connect 192.168.1.10:8443 -showcerts

# Check specific TLS version
openssl s_client -connect 192.168.1.10:8443 -tls1_2

# Show cipher suites
openssl s_client -connect 192.168.1.10:8443 -cipher
```

Openssl demo

```
echo "GET /" | timeout 5 openssl s_client -connect 192.168.1.10:8443 -
showcerts
```