Packet Master

Analyze your Network Packets

K-Secure
IT Security Services

The skill of analyzing packets is the most essential skill required if you are a pentester / ethical hacker, a network or security administrator, intrusion analyst, forensic analyst, application security tester, researcher of vulnerabilities, or you deploy or audit firewalls and IDS, or you write custom IDS signatures. If you already acquired the skill to analyze packets using IPv4, then you surely need to upgrade your skills for IPv6.

Duration

3 Days

Who Should Attend

Anyone who has anything to do with networks. See the introduction above

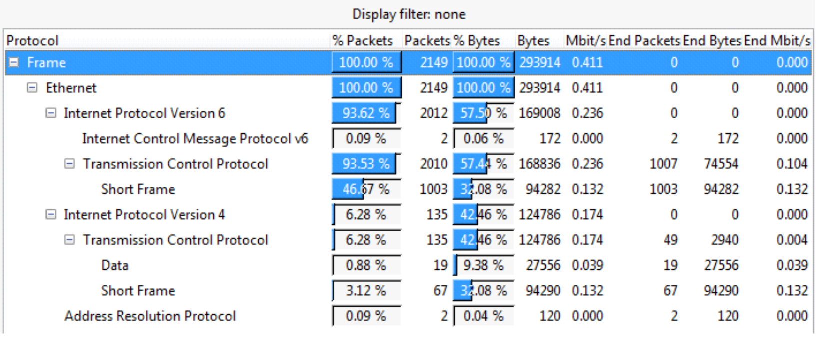
Prerequisites

Knowledge and experience with TCP/IP networks and applications

.

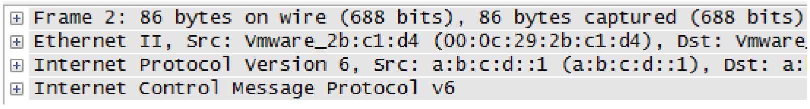
Requirements

To be able to do the exercises, participants need to bring a laptop with VMware Workstation. USB port is needed for sharing files required for the exercises



Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
⊟ Frame	100.00 %	2149	100.00 %	293914	0.411	0	0	0.000
⊟ Ethernet	100.00 %	2149	100.00 %	293914	0.411	0	0	0.000
⊟ Internet Protocol Version 6	93.62 %	2012	57.50 %	169008	0.236	0	0	0.000
Internet Control Message Protocol v6	0.09 %	2	0.06 %	172	0.000	2	172	0.000
⊟ Transmission Control Protocol	93.53 %	2010	57.44 %	168836	0.236	1007	74554	0.104
Short Frame	46.67 %	1003	32.08 %	94282	0.132	1003	94282	0.132
⊟ Internet Protocol Version 4	6.28 %	135	42.46 %	124786	0.174	0	0	0.000
⊟ Transmission Control Protocol	6.28 %	135	42.46 %	124786	0.174	49	2940	0.004
Data	0.88 %	19	9.38 %	27556	0.039	19	27556	0.039
Short Frame	3.12 %	67	32.08 %	94290	0.132	67	94290	0.132
Address Resolution Protocol	0.09 %	2	0.04 %	120	0.000	2	120	0.000



```
⊞ Frame 2: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
⊞ Ethernet II, Src: Vmware_2b:c1:d4 (00:0c:29:2b:c1:d4), Dst: Vmware_
⊞ Internet Protocol Version 6, Src: a:b:c:d::1 (a:b:c:d::1), Dst: a:
⊞ Internet Control Message Protocol v6
```

What you will learn

Day 1 - The Basics

The course starts with the very basics of computing i.e. the bits and bytes and the binary, hex and decimal numbers. It is important to understand the OSI and TCP/IP models before diving deep into the network packets, hence we cover the basics of these layered models. There is no doubt that you understand IPv4 well but it would be great if you also look at the new IPv6 as well, so we explain the basic features of IPv6 here.

Topics

- Overview of numbering systems (Hex / Binary / Decimal)
- Review TCP/IP networks
- Capturing packets from network using tcpdump
- Capturing packets from network using Wireshark
- Introduction to IPv6

Hands on Exercises

- Number conversion exercises
- Capture the packets using tcpdump
- Capture the packets using Wireshark
- Examine protocol layers in captured packets
- Create an IPv6 environment

Packet Master

Analyze your Network Packets

K-SECURE
IT Security Services

```
0000   00 00 01 00 00 00 fe ff   20 00 01 00 08 00 45 00
0010   05 8c c0 a2 40 00 2f 06   2c 2e 41 d0 e4 df 91 fe
0020   a0 ed 00 50 0d 2c 11 4c   71 b8 38 af ff f3 50 18
0030   19 20 e1 35 00 00 22 66   74 70 3a 2f 2f 66 74 70
0040   2e 70 6c 61 6e 65 74 6d   69 72 72 6f 72 2e 63 6f
0050   6d 2f 70 75 62 2f 65 74   68 65 72 65 61 6c 2f 22
0060   3e 41 75 73 74 72 61 6c   69 61 3c 2f 61 3e 0a 3c
0070   61 20 68 72 65 66 3d 22   66 74 70 3a 2f 2f 66 74
0080   70 2e 6d 69 72 72 6f 72   73 2e 77 69 72 65 74 61
0090   70 70 65 64 2e 6e 65 74   2f 70 75 62 2f 73 65 63
```

Day 2 - Protocol Headers

We go straight into the packets and see the headers of the most vital protocols like IP/ARP/ICMP/ICMPv6/TCP/UDP

Topics

- IP Header (v4 and v6)
- ARP Header
- ICMP & ICMPv6 Header
- UDP / TCP Header
- NDP, DNS and more
- Application protocols (HTTP/FTP/Telnet)
- Creating packets using hping2

Hands on Exercises

- Examine normal IPv4 / IPv6 packets
- Analyzing all above protocol headers
- Inspecting the Application Layer
- Creating malformed packets using hping2
- Checking reaction of hosts to malformed packets

Day 3 - Advanced Analysis

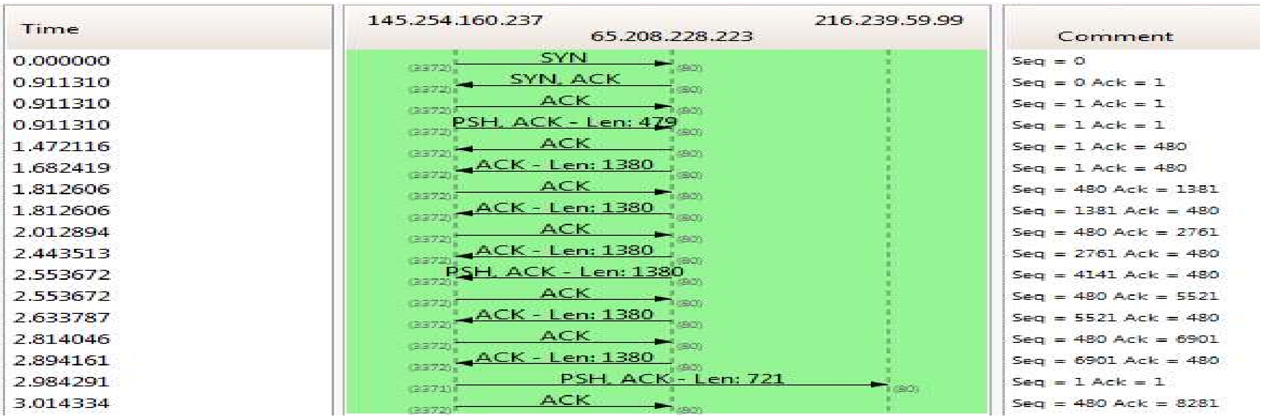
With all the knowledge acquire in 2 days, you now start doing analysis of the traffic you captured by filtering out unwanted packets and focusing on the interesting packets. You also use the high level statistics to get a view of the activities in your network

Topics

- Capture filters (BPF)
- Wireshark display filters
- PCAP files—capturing and reading
- Splitting and merging capture files
- Pattern matching in network traffic
- Analysis using Wireshark

Hands on Exercises

- Using tcpdump filters
- Using Wireshark capture and display filters
- Capturing packets with specific strings using ngrep
- Using Wireshark Statistics Options
- Practice assignments



Time	145.254.160.237 65.208.228.223 216.239.59.99	Comment
0.000000	SYN	Seq = 0
0.911310	SYN, ACK	Seq = 0 Ack = 1
0.911310	ACK	Seq = 1 Ack = 1
0.911310	PSH, ACK - Len: 479	Seq = 1 Ack = 1
1.472116	ACK	Seq = 1 Ack = 480
1.682419	ACK - Len: 1380	Seq = 1 Ack = 480
1.812606	ACK	Seq = 480 Ack = 1381
1.812606	ACK - Len: 1380	Seq = 1381 Ack = 480
2.012894	ACK	Seq = 480 Ack = 2761
2.443513	ACK - Len: 1380	Seq = 2761 Ack = 480
2.553672	PSH, ACK - Len: 1380	Seq = 4141 Ack = 480
2.553672	ACK	Seq = 480 Ack = 5521
2.633787	ACK - Len: 1380	Seq = 5521 Ack = 480
2.814046	ACK	Seq = 480 Ack = 6901
2.894161	ACK - Len: 1380	Seq = 6901 Ack = 480
2.984291	PSH, ACK - Len: 721	Seq = 1 Ack = 1
3.014334	ACK	Seq = 480 Ack = 8281