Eduva Tech

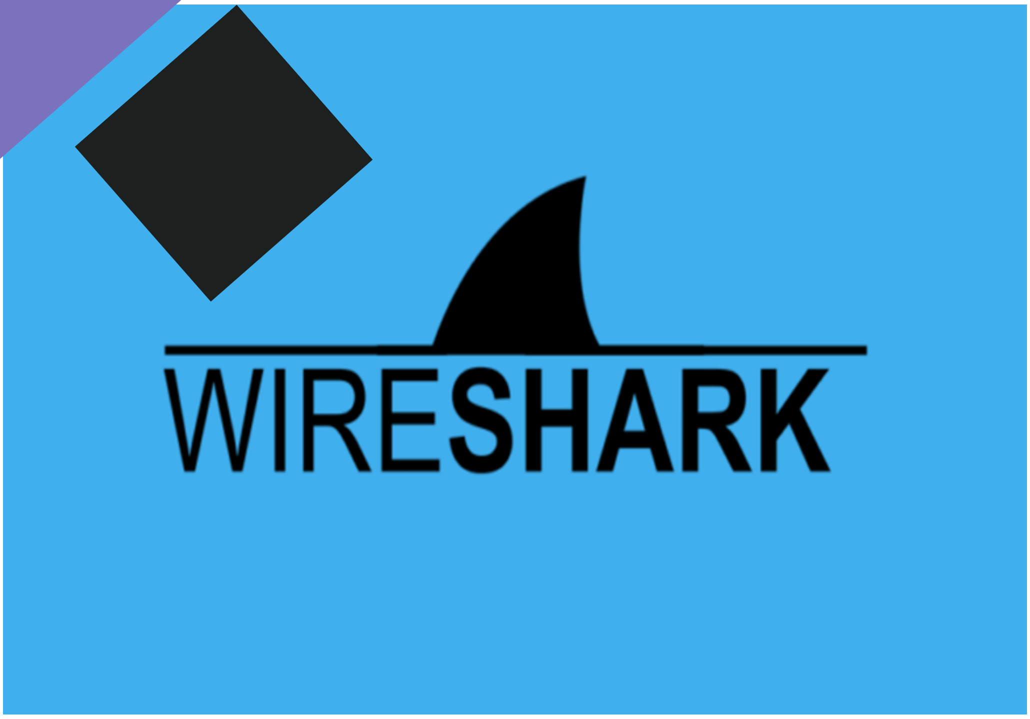
WIRESHARK

SYLLABUS

Prepared For :
Eduva Tech

Contact Us:

info@eduvatech.com
Call/Whatsapp: +91 9315519124

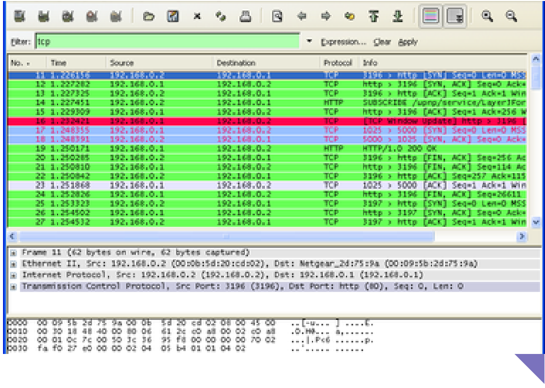


Course Outline

NETWORK ANALYSIS OVERVIEW

- DEFINE THE PURPOSE OF NETWORK ANALYSIS
- LIST TROUBLESHOOTING TASKS FOR THE NETWORK ANALYST
- LIST SECURITY TASKS FOR THE NETWORK ANALYST
- LIST OPTIMIZATION TASKS FOR THE NETWORK ANALYST
- LIST APPLICATION ANALYSIS TASKS FOR THE NETWORK ANALYST
- DEFINE LEGAL ISSUES OF LISTENING TO NETWORK TRAFFIC
- UNDERSTAND GENERAL NETWORK TRAFFIC FLOWS
- REVIEW A CHECKLIST OF ANALYSIS TASKS

Eduva Tech



Filter: tcp

```
No.   Time      Source       Destination  Protocol Info
   11 1.226156  192.168.0.2  192.168.0.1  TCP      3196 > http [SYN] Seq=0 Len=0 MSS
   12 1.227282  192.168.0.1  192.168.0.2  TCP      http > 3196 [SYN, ACK] Seq=0 Ack=
   13 1.227325  192.168.0.2  192.168.0.1  TCP      3196 > http [ACK] Seq=1 Ack=1 Win
   14 1.227451  192.168.0.2  192.168.0.1  HTTP     SUBSCRIBE /upnp/service/Layer3For
   15 1.229309  192.168.0.1  192.168.0.2  TCP      http > 3196 [ACK] Seq=1 Ack=256 W
   16 1.232421  192.168.0.1  192.168.0.2  TCP      [TCP Window Update] http > 3196 [
   17 1.248355  192.168.0.1  192.168.0.2  TCP      1025 > 5000 [SYN] Seq=0 Len=0 MSS
   18 1.248391  192.168.0.2  192.168.0.1  TCP      5000 > 1025 [SYN, ACK] Seq=0 Ack=
   19 1.250171  192.168.0.1  192.168.0.2  HTTP     HTTP/1.0 200 OK
   20 1.250285  192.168.0.2  192.168.0.1  TCP      3196 > http [FIN, ACK] Seq=256 Ac
   21 1.250810  192.168.0.1  192.168.0.2  TCP      http > 3196 [FIN, ACK] Seq=114 Ac
   22 1.250842  192.168.0.2  192.168.0.1  TCP      3196 > http [ACK] Seq=257 Ack=115
   23 1.251868  192.168.0.1  192.168.0.2  TCP      1025 > 5000 [ACK] Seq=1 Ack=1 Win
   24 1.252826  192.168.0.1  192.168.0.2  TCP      http > 3196 [FIN, ACK] Seq=26611
   25 1.253323  192.168.0.2  192.168.0.1  TCP      3197 > http [SYN] Seq=0 Len=0 MSS
   26 1.254502  192.168.0.1  192.168.0.2  TCP      http > 3197 [SYN, ACK] Seq=0 Ack=
   27 1.254532  192.168.0.2  192.168.0.1  TCP      3197 > http [ACK] Seq=1 Ack=1 Win

⊞ Frame 11 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)
⊞ Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
⊞ Transmission Control Protocol, Src Port: 3196 (3196), Dst Port: http (80), Seq: 0, Len: 0

0000  00 09 5b 2d 75 9a 00 0b  5d 20 cd 02 08 00 45 00   ..[-u... ] .....E.
0010  00 30 18 48 40 00 80 06  61 2c c0 a8 00 02 c0 a8   .0.H@... a,......
0020  00 01 0c 7c 00 50 3c 36  95 f8 00 00 00 00 70 02   ...|.P<6 ......p.
0030  fa f0 27 e0 00 00 02 04  05 b4 01 01 04 02         ..'..... ......
```

INTRODUCTION TO WIRESHARK

- DESCRIBE WIRESHARK'S PURPOSE
- KNOW HOW TO OBTAIN THE LATEST VERSION OF WIRESHARK
- CAPTURE PACKETS ON WIRED
- DESCRIBE HOW WIRESHARK PROCESSES PACKETS
- DEFINE THE ELEMENTS OF THE START PAGE
- NAVIGATE WIRESHARK'S MAIN MENU
- USE THE MAIN TOOLBAR FOR EFFICIENCY
- FOCUS FASTER WITH THE FILTER TOOLBAR
- ACCESS OPTIONS THROUGH RIGHT-CLICK FUNCTIONALITY
- DEFINE THE FUNCTIONS OF THE MENUS AND TOOLBARS

CAPTURE TRAFFIC

- KNOW WHERE TO TAP INTO THE NETWORK
- KNOW WHEN TO RUN WIRESHARK LOCALLY
- IDENTIFY THE MOST APPROPRIATE CAPTURE INTERFACE
- CAPTURE ON MULTIPLE ADAPTERS SIMULTANEOUSLY
- CAPTURE TRAFFIC REMOTELY
- AUTOMATICALLY SAVE PACKETS TO ONE OR MORE FILES
- OPTIMIZE WIRESHARK TO AVOID DROPPING PACKETS

CREATE AND APPLY CAPTURE FILTERS

- DESCRIBE THE PURPOSE OF CAPTURE FILTERS
- BUILD AND APPLY A CAPTURE FILTER TO AN INTERFACE
- FILTER BY A PROTOCOL
- CREATE MAC/IP ADDRESS OR HOST NAME CAPTURE FILTERS
- CAPTURE ONE APPLICATION'S TRAFFIC ONLY
- USE OPERATORS TO COMBINE CAPTURE FILTERS
- CREATE CAPTURE FILTERS TO LOOK FOR BYTE VALUES
- SHARE CAPTURE FILTERS WITH OTHERS

DEFINE GLOBAL AND PERSONAL PREFERENCES

- FIND YOUR CONFIGURATION FOLDERS
- SET GLOBAL AND PERSONAL CONFIGURATIONS
- CUSTOMIZE YOUR USER INTERFACE SETTINGS
- DEFINE YOUR CAPTURE PREFERENCES
- DEFINE HOW WIRESHARK AUTOMATICALLY RESOLVES IP AND MAC NAMES
- PLOT IP ADDRESSES ON A WORLD MAP WITH GEOIP
- RESOLVE PORT NUMBERS (TRANSPORT NAME RESOLUTION)
- RESOLVE SNMP INFORMATION
- CONFIGURE FILTER EXPRESSIONS
- CONFIGURE STATISTICS SETTINGS
- DEFINE ARP, TCP, HTTP/HTTPS AND OTHER PROTOCOL SETTINGS
- CONFIGURE PROTOCOL SETTINGS WITH RIGHT-CLICK

COLORIZE TRAFFIC

- USE COLORS TO DIFFERENTIATE TRAFFIC
- DISABLE ONE OR MORE COLORING RULES
- SHARE AND MANAGE COLORING RULES
- IDENTIFY WHY A PACKET IS A CERTAIN COLOR
- COLOR CONVERSATIONS TO DISTINGUISH THEM
- TEMPORARILY MARK PACKETS OF INTEREST

DEFINE TIME VALUES AND INTERPRET SUMMARIES

- USE TIME TO IDENTIFY NETWORK PROBLEMS
- UNDERSTAND HOW WIRESHARK MEASURES PACKET TIME
- CHOOSE THE IDEAL TIME DISPLAY FORMAT
- IDENTIFY DELAYS WITH TIME VALUES
- CREATE ADDITIONAL TIME COLUMNS
- MEASURE PACKET ARRIVAL TIMES WITH A TIME REFERENCE
- IDENTIFY CLIENT, SERVER AND PATH DELAYS
- CALCULATE END-TO-END PATH DELAYS
- LOCATE SLOW SERVER RESPONSES

WIRESHARK

INTERPRET BASIC TRACE FILE STATISTICS

- LAUNCH WIRESHARK STATISTICS
- IDENTIFY NETWORK PROTOCOLS AND APPLICATIONS
- IDENTIFY THE MOST ACTIVE CONVERSATIONS
- LIST ALL IPV4/IPV6 ADDRESSES IN THE TRAFFIC
- LIST ALL DESTINATIONS IN THE TRAFFIC
- GRAPH THE FLOW OF TRAFFIC
- GATHER YOUR HTTP STATISTICS

CREATE AND APPLY DISPLAY FILTERS

- UNDERSTAND THE PURPOSE OF DISPLAY FILTERS
- CREATE DISPLAY FILTERS USING AUTO-COMPLETE
- APPLY SAVED DISPLAY FILTERS
- MAKE DISPLAY FILTERS QUICKLY USING RIGHT-CLICK FILTERING
- COMBINE DISPLAY FILTERS WITH COMPARISON OPERATORS
- FILTER ON SPECIFIC BYTES IN A PACKET

TCP/IP ANALYSIS OVERVIEW

- DEFINE BASIC TCP/IP FUNCTIONALITY
- FOLLOW THE MULTISTEP RESOLUTION PROCESS
- DEFINE PORT NUMBER RESOLUTION
- DEFINE NETWORK NAME RESOLUTION
- DEFINE ROUTE RESOLUTION FOR A LOCAL TARGET
- DEFINE LOCAL MAC ADDRESS RESOLUTION FOR A TARGET
- DEFINE ROUTE RESOLUTION FOR A REMOTE TARGET
- DEFINE LOCAL MAC ADDRESS RESOLUTION FOR A GATEWAY

Eduva Tech

ANALYZE DOMAIN NAME SYSTEM (DNS) TRAFFIC

- DEFINE THE PURPOSE OF DNS
- ANALYZE NORMAL DNS QUERIES/RESPONSES
- ANALYZE DNS PROBLEMS
- FILTER ON THE DNS/MDNS TRAFFIC

ANALYZE ADDRESS RESOLUTION PROTOCOL (ARP) TRAFFIC

- DEFINE THE PURPOSE OF ARP TRAFFIC
- ANALYZE NORMAL ARP REQUESTS/RESPONSES
- ANALYZE ARP PROBLEMS
- FILTER ON ARP TRAFFIC

ANALYZE INTERNET PROTOCOL (IPV4/IPV6) TRAFFIC

- DEFINE THE PURPOSE OF IP
- ANALYZE NORMAL IPV4 TRAFFIC
- ANALYZE IPV4 PROBLEMS
- FILTER ON IPV4/IPV6 TRAFFIC
- SANITIZE IPV4 ADDRESSES IN A TRACE FILE

ANALYZE INTERNET CONTROL MESSAGE PROTOCOL (ICMPV4/ICMPV6) TRAFFIC

- DEFINE THE PURPOSE OF ICMP
- ANALYZE NORMAL ICMP TRAFFIC
- ANALYZE ICMP PROBLEMS
- FILTER ON ICMP AND ICMPV6 TRAFFIC

ANALYZE USER DATAGRAM PROTOCOL (UDP) TRAFFIC

- DEFINE THE PURPOSE OF UDP
- ANALYZE NORMAL UDP TRAFFIC
- ANALYZE UDP PROBLEMS
- FILTER ON UDP TRAFFIC

ANALYZE TRANSMISSION CONTROL PROTOCOL (TCP) TRAFFIC

- DEFINE THE PURPOSE OF TCP
- ANALYZE NORMAL TCP COMMUNICATIONS
- DEFINE THE ESTABLISHMENT OF TCP CONNECTIONS
- DEFINE HOW TCP-BASED SERVICES ARE REFUSED
- DEFINE HOW TCP CONNECTIONS ARE TERMINATED
- TRACK TCP PACKET SEQUENCING
- DEFINE HOW TCP RECOVERS FROM PACKET LOSS
- IMPROVE PACKET LOSS RECOVERY WITH SELECTIVE ACKNOWLEDGMENTS
- DEFINE TCP FLOW CONTROL
- ANALYZE TCP PROBLEMS
- FILTER ON TCP TRAFFIC
- SET TCP PROTOCOL PARAMETERS

ANALYZE DYNAMIC HOST CONFIGURATION PROTOCOL (DHCPV4/DHCPV6) TRAFFIC

- DEFINE THE PURPOSE OF DHCP
- ANALYZE NORMAL DHCP TRAFFIC
- ANALYZE DHCP PROBLEMS
- FILTER ON DHCPV4/DHCPV6 TRAFFIC
- DISPLAY BOOTP-DHCP STATISTICS

ANALYZE HYPERTEXT TRANSFER PROTOCOL (HTTP) TRAFFIC

- DEFINE THE PURPOSE OF HTTP
- ANALYZE NORMAL HTTP COMMUNICATIONS
- ANALYZE HTTP PROBLEMS
- DISSECT HTTP PACKET STRUCTURES
- FILTER ON HTTP OR HTTPS TRAFFIC
- EXPORT HTTP OBJECTS
- DISPLAY HTTP STATISTICS
- GRAPH HTTP TRAFFIC FLOWS
- ANALYZE HTTPS COMMUNICATIONS
- ANALYZE SSL/TLS HANDSHAKE
- ANALYZE TLS ENCRYPTED ALERTS
- DECRYPT HTTPS TRAFFIC
- EXPORT SSL KEYS

ANALYZE FILE TRANSFER PROTOCOL (FTP) TRAFFIC

- DEFINE THE PURPOSE OF FTP
- ANALYZE NORMAL FTP COMMUNICATIONS
- ANALYZE PASSIVE MODE CONNECTIONS
- ANALYZE ACTIVE MODE CONNECTIONS
- ANALYZE FTP PROBLEMS
- FILTER ON FTP TRAFFIC

ANALYZE EMAIL TRAFFIC

- ANALYZE NORMAL SMTP COMMUNICATION
- ANALYZE SMTP PROBLEMS
- FILTER ON SMTP TRAFFIC

VOICE OVER IP (VOIP) ANALYSIS FUNDAMENTALS

- DEFINE VOIP TRAFFIC FLOWS
- ANALYZE SESSION BANDWIDTH AND RTP PORT DEFINITION
- ANALYZE VOIP PROBLEMS
- ANALYZE SIP TRAFFIC AND RTP
- PLAY BACK VOIP CONVERSATIONS
- DECIPHER RTP PLAYER MARKER DEFINITIONS
- FILTER ON VOIP TRAFFIC

NETWORK FORENSICS OVERVIEW

- COMPARE HOST TO NETWORK FORENSICS
- GATHER EVIDENCE
- AVOID DETECTION
- HANDLE EVIDENCE PROPERLY
- RECOGNIZE UNUSUAL TRAFFIC PATTERNS
- COLOR UNUSUAL TRAFFIC PATTERNS

ADVANCE

- DECRYPTING WIRELESS TRAFFIC
- SPOT SUSPICIOUS OR UNAUTHORIZED PACKETS FROM YOUR NETWORK
- CONFIGURE FIREWALL ACCORDING TO WIRESHARK TRAFFIC
- SSH TUNNELING THROUGH WIRESHARK

WIRESHARK CLI & COMMANDS

- TSHARK
- START CAPTURING
- SAVE A FILE
- STOP THE CAPTURING AFTER A PARTICULAR PERIOD OF TIME
- SPLITS CAPTURING INTO DIFFERENT FILES ACCORDING TO THE SIZE OF THE FILE
- CAPTURE FILTERS & DISPLAY FILTERS IN CLI
- FILTER THE OUTPUT FILE TO SEE SPECIFIC RESULTS