Wireshark Security (NI306)

40 Hours

Outline

Wireshark Security relates to the analysis of network traffic for the purposes of identifying intrusions or anomalous activity. Compared to computer forensics, where evidence is usually preserved on disk, network data is more volatile and unpredictable, and therefore requires a different approach. This course sets the groundwork for understanding networks and the investigation process on them. Students will master the Wireshark deep and advanced capabilities in order to conduct analysis in a network environment. The course will incorporate demonstrations and lab exercises to reinforce hands-on capabilities.

Target Audience

The course targets participants with basic knowledge in IT or networking, who wish to have a deeper understanding of cyber investigations on the network. Primarily:

- Incident Responders & Intelligence corps
- Computer investigators
- IT/network security personnel
- Junior cyber forensics analysts

Prerequisites

Basic knowledge in IT or networking

Objectives

Mastering Wireshark :

- Detecting various types of computer and network incidents
- Analyzing artifacts left on a compromised system
- Understanding alerts and advisories
- Responding to incidents
- Performing network traffic monitoring and analyzing logs

Contents

Module 1: Introduction to networking

During this module, participants will study the basics of network infrastructures, common network types, network layers and communications between protocols, communication between network devices from different layers and network anonymity methods.

1. Network infrastructure
2. Network implementation
    - Wide area network
    - Local area network
    - Wireless networks
3. OSI layers model and TCP/IP model
    - Application
    - Presentation
    - Session
    - Transport
    - Network
    - Data-Link
    - Physical
4. Common protocols by layers
5. Common network devices
    - Switch vs. Hub
    - Router
    - Bridge
6. Working with network services
    - Run and configure web service
    - Network file sharing services
    - Network devices remote management services

7. Remote networking
    - VPN
    - Proxy
8. World Wide Web
    - ISP
    - Web
    - Hosting
9. Hands-on session:
    - Packet tracer lab
    - The command line and networking

Module 2: Wireshark Basics

During this module, students will become familiar with the key features for network analysis and will construct machines that will serve them during the course. The various commands and capabilities covered in this module are a crucial asset for every network forensics investigator.

1. What is a packet?
2. Capture packets with Wireshark
3. Troubleshooting network applications
4. Top filters
5. The right approach for long-term capture
6. Information Gathering
7. Diving into Transmission Control Protocol (TCP) packets:
    - TCP Structure
    - TCP Handshake
    - Understanding flags
    - TCP Streams and objects
    - Packet loss detection
    - Follow TCP Streams
8. Expressions
9. Divining into User Datagram Protocol (UDP)
    - UDP overview
    - UDP packet structure
    - Filtering UDP traffic
    - Analyzing problems with UDP traffic
    - Follow UDP streams
10. Internet Control Message Protocol
    - ICMP overview
    - ICMP packet structure

- Filtering ICMP traffic
- Analyzing problems with ICMP traffic

11. Address Resolution Protocol
12. Internet Protocol
13. Understanding DHCP behavior using Wireshark
14. Domain Name System
    - DNS overview
    - DNS packet structure
    - Filtering DNS traffic
    - Analyzing problems with DNS traffic
15. Extracting data from Social Networks using Wireshark
16. TCP flow control

Module 3: Wireshark for Security

During this module, participants will learn how to read packets of data, perform "file carving" and identify suspicious activity on the network. They will get an insight into how an attack on the network is carried out and how it can be identified. Later on, students will be tasked with constructing basic defensive tools that will raise alerts when the system is attacked.

1. Identifying open ports using Wireshark
2. Identifying attacks:
    - MiTM attack
    - Brute Force attack
    - DDoS
    - Trojans
3. Finding system exploits with Wireshark
4. Wireless sniffing
5. Packet Analysis on LLMNR
6. Catching SMB errors with Wireshark
7. HTTP authentication review with Wireshark
8. Identifying Application signatures
9. Broadcast Analysis
10. Advanced Wireshark display filters
11. Catching Beacons
12. IoCs :
    - Detection
    - False Positive
    - Verification
13. Sniffing packets with usernames and passwords

14. Regex with Wireshark
15. Finding suspicious traffic
16. Using Wireshark CLI for Automation
17. PCAP files manipulation
18. Packet structure and analysis
19. Internet traffic analysis
20. Network forensics investigation process

Module 4: Network Log Analysis

Throughout this module, students will analyze logs – computer generated records that contain useful data - and get to know where information is stored on Windows and Linux operating systems. They will also understand how to identify logs that have been tempered, using basic and advanced tools.

1. Log analysis process
    - Generating logs
    - Collecting logs
    - Normalizing logs
    - Filtering logs
2. Log sources
    - IDS
    - Firewalls/IPS
    - Network bandwidth
    - Applications
3. Log analysis tools
    - P0f – passive network scanning
    - Snort – basic uses
4. Common string manipulation
5. Windows event viewer
6. Bro analysis
    - Learning to use Bro
    - Using Bro-Cut for special needs
    - Extracting sensitive information
    - Filtering Big-Data