NET400

TCP/IP FUNDAMENTALS

NET400 - TCP/IP Fundamentals studies traffic analysis and concepts of creating defensive measures based on analyst findings. This course covers collection of network traffic, analysis of individual packets, and setup and configuration of open-source intrusion detection systems (IDS).

Additionally covered are the procedures required for network exploitation analysts to implement traffic statistics methodology, intrusion sensors deployment and report generation utilized by management and administrators.

TARGET AUDIENCE

Professionals with UNIX command line familiarity who are looking to enhance their knowledge of collecting and analyzing network traffic

OBJECTIVE

Provide an understanding of TCP/IP fundamentals including where/how to capture and analyze network traffic for summary reporting based on findings and observations

CYBRScore™

DAY 1

Students will learn to understand the packet analysis methodology and how network analysts fit into that methodology. Students will use commands native to Linux and Windows to gain an understanding of network characterization as well as working with files, directories, and network interfaces.

Topics List

- Linux Fundamentals
- Working with Files and Directories
- Working with Network Interface
- Installing Software
- Access Control
- Network Fundamentals
- Network Design
- Port Mirroring
- IDS/IPS Architecture
- Snort and Snorby

DAY 2

Students will examine number systems, general networking terminology and protocol encapsulation. Students will learn to interpret protocol diagrams to make sense of network protocols including Ethernet, IPv4, IPv6, ARP, TCP, ICMP and UDP using network analysis tools.

Topics List

- Packet Deconstruction
- Wireshark
- Tcpdump
- Application Layer Protocols

DAY 3

Students learn how an actor can enumerate a network through completely benign interactions. Students will learn how search engines are used to find security holes exposed in web servers and networking devices.

Topics List

- TCP Scans (SYN, SYN/ACK, FIN, Frag, Idle)
- Well-Known Application Ports
- ICMP Time-to Live (TTL)
- OSINT
- Google Operators
- Introduction to Attacks
- Kali and Metasploit Framework

DAY 4

Students will learn best practices to gain visibility into different parts of a network. Students will examine techniques that prevent an attacker from gaining control and reduce the impact of a compromise. Students will study the IDS architecture and learn to use the Snort IDS/IPS to discover anomalous network traffic.

Topics List

- Defense
- Monitoring Networks
- Windows Event Logs
- Linux Syslog Logs
- DHCP Logs
- DNS Logs and Capture Filters

DAY 5

Students participate in an intense hands-on activity that requires the use of the information learned over the entire course to test the student in the analysis and characterization of anomalous activity transmitted on a live network.

Capstone Exercise

- Analyze network traffic as it is being transmitted live “across the wire”
- Determine the extent and severity of attacks underway
- Analyze attacks and identify potential mitigations

NET400

TCP/IP FUNDAMENTALS

CYBRScore™

