Certified Network Pentesting Professional (CNPP)

This comprehensive Active Directory training will not only cover the most common exploits that attackers use to infiltrate networks but also provide you with the necessary steps to fix and patch these vulnerabilities. You will acquire practical skills and knowledge that can be directly applied to enhance the security of your environment.

Module 1

- Introduction to networking
- TCP/IP Packet Analysis
- Port and Protocols Analysis
- Windows Lab Setup
- Linux Lab Setup

Module 2

- Network Analysis
- Packet analysis's significance
- Network traffic capture
- Promiscuous mode
- Wireshark introduction
- Filtering and decoding of traffic
- Physical data-link layer
- Network internet layer

Module 3

- Detecting Live Systems with ICMP
- Detecting Live Systems with TCP
- ICMP Packet Analysis
- Traceroute

Module 4

- Packet Analysis with Tshark
- Tshark introduction
- Traffic capture
- Promiscuous mode
- Packet count
- File read and write;
- Output formats

Module 5

- Hydra
- Medusa
- Crunch
- CeWL
- cUPP
- Online Attacks

Module 6

- Telnet Penetration Testing
- Introduction & Lab Setup
- Banner Grabbing/Banner Hiding
- Port Redirection
- Brute Force & Password Cracking
- Remote Port Forwarding
- Pivoting

Tools :

Nmap, Zenmap, Currports, Fing, Netdiscover, Angryipscanner, Nessus, Nuclei, Metasploit, Ettercap, Xerosploit, Hydra, Medusa, Responder, Smbwalk