Learnsoft
ENTERPRISE TRAINING

Cybersecurity Boot camp- 5 Days

Length: 5 Days

Learning Outcomes:

- Core Components of Building a Defensible Network infrastructure and properly securing your routers, switches, and other network infrastructure
- Formal methods to perform vulnerability assessment and penetration testing to find weaknesses on your enterprise network
- Methods to detect advanced attacks against your network and indicators of compromise on deployed systems, including the forensically sound collection of artifacts and what you can learn from them
- How to respond to an incident using the six-step process of incident response: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned
- Approaches to analyzing malware, ranging from fully automated techniques to the manual analysis of static properties, interactive behavior, and code reversing

At the completion of this course students will be able to:

- Identify network security threats against infrastructure and build defensible networks that minimize the impact of attacks
- Utilize tools to analyze a network to prevent attacks and detect the adversary
- Decode and analyze packets using various tools to identify anomalies and improve network defenses
- Understand how the adversary compromises systems and how to respond to attacks using the six-step incident handling process
- Perform penetration testing against an enterprise to determine vulnerabilities and points of compromise
- Use various tools to identify and remediate malware across your enterprise

COURSE CONTENT

Features dozens of immersive hands-on lab exercises that will show you how to:

• Build a defensible network architecture by auditing router configurations, launching successful attacks against them, hardening devices to withstand those same attacks, and using active defense tools to detect an attack and generate an alert

• Perform detailed analysis of traffic using various sniffers and protocol analyzers, and automate attack detection by creating and testing new rules for detection systems

• Identify and track attacks and anomalies in network packets

• Use various tools to assess systems and web applications for known vulnerabilities, and exploit those vulnerabilities using penetration testing frameworks and toolsets

• Analyze Windows systems during an incident to identify signs of a compromise

• Find, identify, analyze, and clean up malware such as Ransomware using a variety of techniques, including monitoring the malware as

it executes and manually reversing its code to discover its secrets