CybersCool Defcon Inc.

Syllabus - SOC Analyst

Course Outline:

I. BOOTCAMP INTRODUCTION

Topic Covered:

- Introduction, goals, and values of the Bootcamp.
- Prerequisites required and mindset for success.
- Program structure and types of assignment.
- Overview of key topics and objectives.
- What's in It for Me? What does cybersecurity have to do with this?
- Tool Introductions: Familiarize with essential cybersecurity tools.
- Fast Forward: Quick tips and important highlights for upcoming labs.
- Lab Solution Videos: Step-by-step guides for the lab exercises.
- Emphasis on the growth mindset.
- Strategies for effective learning.
- Problem-solving and adaptability in learning.
- Guidance on navigating the Bootcamp for success.
- Information on available Bootcamp, technical, and peer support.

II. PRE-PROGRAM

Topics Covered:

- Understand Information Technology's role in cybersecurity.
- Learn key cybersecurity concepts and the function of analyst.
- Basics of Network Administration and security.
- Lay the foundations of computers and how they work.
- Explore what operating systems are and perform you first practice in the Windows and Linux Operating systems.
- Explore how AI revolutionizes industries and learn about GenAI.
- Learn how to use AI to enhance your Bootcamp learning experience.

TOOLS: Wireshark, Putty

III. NETOWRK ADMINISTRATION

Topic Covered:

- Learn different network types, topologies, and how devices connect.
- Discover the roles of various network devices and security measures.
- Understand network design and the importance of address.
- Learn the structure and function of each OSI layer.
- Explore important protocols and their OSI layers.
- Understand how these concepts apply in real cybersecurity scenarios.
- Discover what network sniffers are and their role in cybersecurity.
- Introduction and guide to using the Wireshark tool.
- Perform three hands-on labs to analyze network traffic on Wireshark.
- Understand the differences between OSI and TCP/IP.
- Learn about the four layers of the TCP/IP model.
- Compare OSI and TCP/IP layers and their practical uses.
- Uncover the essentials and duties of Network Administration.
- Explore the synergy between Network Administration and Cybersecurity.
- Dive into the role of Network Guardians in safeguarding networks.
- Learn the steps for designing, setting up, and maintaining a network.
- Discover the best practices for network expansion and scalability.
- Learn network management basics and simulate scenarios using Packet Tracer
- Get started with Packer Tracker, exploring its interface and main functions.
- Practice with Packet Tracer labs to simulate and troubleshoot network setups.
- Dive into switch configurations, including basic Cisco switch settings.
- Network operation essentials and routing fundamentals.
- Review IP Addressing and Advanced subnetting (VLSM, CIDR)
- Learn DNS functions and conduct router configuration labs.
- Understand VPN basics, types, and protocols.
- Introduction to using OpenVPN for secure connections.
- Explore traffic monitoring principles and technologies.
- Learn monitoring strategies and the role of SNMP.

TOOLS: Cisco Packet Tracer, Nmap, OpenVPN, Windows PowerShell

IV. CYBERSECURITY FUNDAMENTALS

Topic Covered:

- Explore Cybersecurity fundamentals and types, understand cybercrime, and learn about internal vs. external attackers.
- Review cybersecurity procedures and strategies for effective defense.
- Stay updated with the latest Cyber News.
- NIST and NICE Frameworks for Structured Cybersecurity Approaches.
- Master the steps: Identify, Protect, Detect, Respond, Recover.
- Utilize CyberSeek for cybersecurity career guidance.
- MITRE ATT&CK Framework's tactical phases from Initial Access to impact.
- Apply framework concepts in cybersecurity scenarios.
- Identify different types of Threat Actors and their tactics.
- Examine Cyberthreats: social engineering, phishing, malware.
- Study Vulnerabilities, Exploits, and defense strategies.

V. NETWORK AND APPLICATION SECURITY

Topic Covered:

- Understand the CIO Triad, privacy concepts, and security principles.
- Explore Defense in Depth 9DID) and the Zero Trust model.
- Delve into network security design and threat management strategies.
- Introduction to Cryptography and its role in cybersecurity.
- Learn about encryption/decryption processes and types of cryptography.
- Practice file encryption/decryption in lab exercise.
- Discover what hashing is, and its cybersecurity uses.
- Learn about hashing algorithms and their applications.
- Engage in lab practice focusing on hash functions.
- Examine Access Control principles and the Three A's.
- Understand different authentication methods and protocols.
- Explore types of Access Control: DAC, MAC, RBAC, and Active Directory.
- Conduct lab practice on installing and configuring Active Directory.
- Learn Firewall Foundations, operation principles, and types.

- Practice creating Windows Firewall rules and configuring iptables in Linux.
- Compare Host-based and Network-based Firewalls and apply lab practices for network-based firewall rules.
- Understand IDS & IPS Foundations, their functions, and approaches.
- Dive into NIDS & HIDS differences and explore the Snort intrusion detection system.
- Engage with Snort through tool introduction, rules, modes, and lab practices, including Nmap integration.
- Basics of SIEM, its architecture, and how it operates.
- Learn about SIEM alert structure, correlation rules, and objectives.
- Explore Splunk as a SIEM tool, its features, components, and interface through lab practice and real-life scenario exercises.

TOOLS: Kali Linux, Splunk, Snort IDS, Active Directory, Nmap, OpenVPN, Windows Firewall, Linux, Iptables

VI. INCIDENT HANDLING

Topic Covered:

- Understand HTTP Headers, their types, and core functions.
- Master incident handling principles: identify events, manage alerts, and understand attack vectors.
- Learn about SOC teams: roles, importance, deployment models.
- Explore types of Web Attacks: DoS, SQL Injection, XSS, and others.
- Practice incident analysis and detection techniques, using Splunk labs.
- Apply mitigation strategies and lab practices for various web attacks.
- Discover Domain Attacks: Typosquatting, Domain Hijacking, and more.
- Conduct lab practices for analyzing and responding to domain incidents.
- Implement prevention and response strategies for domain-related attacks.
- Understand Ransomware, Viruses, Worms, Trojans, Adware.
- Introduction to Virus Total, functionality, usage.
- Scenario analysis, report drafting techniques.
- Key components, SOC integration of EDR.
- Phases from detection to remediation in EDR.
- Compare EDR with AV and SIEM.

- Explore Wazuh's capabilities including hands-on application.

TOOLS: Splunk, In-House SIEM

VII. **FINAL EXAM (Theoretical)**

Here's are the of component needed in hosting cybersecurity learning platform via Cloud Services.

1. **Server Infrastructure:**
    - Webservers: Apache Nginx for hosting the platform
    - Database Servers: MySQL, PostgreSQL, MongoDB for storing user data, courses, and progress.
2. **Networking Equipment:**
    - Routers switched and firewalls to manage network security.
    - Load balancers for distributing incoming traffic across multiple servers.
3. **Security Software:**
    - Intrusion Detection Systems (IDS) and Intrusion Prevention System (IPS) to monitor and protect against cyber threats.
    - Anti-malware and antivirus software to scan for and remove malicious software.
    - Security information and event management (SIEM) software for aggregating and analyzing security logs.
4. **Authentication and Authorization Systems:**
    - Single Sign-On (SSO) solutions for seamless login across multiple services.
    - Role-based access control (RBAC) for managing user permissions within the platform.
5. **Encryption Tools:**
    - SSL/TLS certificates for encrypting data transmitted between servers and clients.
    - Encryption protocols (e.g., AUS) for securing stored data.
6. **Monitoring and Logging Tools:**
    - Monitoring tools for tracking system performance, uptime, and resource usage.
    - Logging tools for recording user activity system events, and security incidents.
7. **Content Delivery Systems:**
    - Content Delivery Network (CDNs) for delivering course materials and multimedia content quickly and reliably.

8. **Virtualization and Containerization Platforms:**
    - Virtual machines (VMs) or containers for isolating and running application services.
    - Orchestration tools like Kubernetes or Dockers Swarm for managing containerized applications.
9. **Backup and Disaster Recovery Solutions:**
    - Regular backups of data to prevent data loss in case of system failure or cyber-attacks.
    - Disaster recovery plans and procedures to restore services quickly in the event of a major outage.
10. **Development and testing Environments:**
    - Development frameworks and tools for building and testing new features.
    - Continuous Integration/Continuous Deployment (CI/DC) pipelines for automating software deployment.
11. **User Interface and Experience Tools:**
    - Fronted frameworks like React.js or Angular for building responsive and interactive user interfaces.
    - Design tools for creating visually appealing and intuitive user experiences.
12. **Compliance and Regulatory Tools:**
    - Tools for ensuring compliance with data protection regulations (e.g., GDPR, HIPAA).
    - Vulnerability scanning tools for identifying and addressing security weaknesses.
13. **Customer Support and Communication Tools:**
    - Helpdesk software for managing user inquiries and support tickets.
    - Communication tools like email, chat, and collaboration.
14. **Education Content Creation Tools:**
    - Authoring tools for creating and editing educational materials, such as videos, presentations, and quizzes.
    - Learning management system (LMS) for organizing and delivering course content to users.

15. **User Analytics and Feedback Systems:**
    - Analytics tools for tracking user engagement, course completion rates, and other key metrics.
    - Feedback mechanics for collecting user opinions and suggestions for improving the platform.
16. **Legal and Compliance Support:**
    - Legal consultation for ensuring compliance with intellectual property laws, terms of service, and privacy policies.
    - Cyber insurance to protect against potential legal liabilities and financial losses from security incidents.
17. **Training and Support for Staff:**
    - Training programs for platform administrators, instructors, and support staff on cybersecurity best practices and platform usage.
    - Technical support for troubleshooting issues and resolving user concerns.
18. **Internet Bandwidth:**
    - The required amount will depend on factors such as the numbers of users accessing the platform simultaneously, the type of content being served (e.g., test, images, videos), and any streaming of interactive features.