CyberDefense Fundamentals: Web Application Security, threat intelligence, SIEM and Firewall

Duration: 40 hrs

Introduction to Web Application Security

- Understanding the web application architecture
- Common web application vulnerabilities
- Introduction to Burp Suite and its features

Automated Vulnerability Scanning with Burp Suite Scanner

- Introduction to Burp Suite Scanner module
- Understanding the importance of automated vulnerability scanning
- Configuring and customizing scanning options in Burp Suite

Configuring Burp Suite Intruder:

- Introduction to Burp Suite Intruder
- Understanding the Sniper attack
- Configuring the target and payload positions
- Brute-forcing login credentials using username and password lists

Exploring Burp Suite Repeater Features

- Introduction to Burp Suite Repeater
- Understanding the purpose and benefits of using Repeater
- Sending individual HTTP requests for manual testing and analysis
- Modifying request data and observing the impact on server behavior

Understanding Burp Suite Decoder

- Introduction to Burp Suite Decoder
- Base64 encoding and decoding
- URL encoding and decoding
- Using the Decoder to analyze and modify encoded data within requests and responses

Introduction to Threat Intelligence and Threat Hunting

- Overview of Threat Intelligence and Threat Hunting
- Importance of open-source tools in the modern cybersecurity landscape
- Indicators of Compromise (IoCs)
- TTPs (Tactics, Techniques, and Procedures)
- Threat intelligence lifecycle

Open-Source Threat Intelligence Platforms (TIPs)

- Introduction to MISP (Malware Information Sharing Platform)
- Configuring MISP for receiving and sharing threat intelligence
- Open-Source Threat Intelligence Tools

Malware Analysis and Threat Intelligence Platforms

- YARA
    - Understanding YARA rules for malware identification
    - Writing YARA rules and detecting malware

Data Collection and Analysis

- Introduction to ELK Stack
- ELK Stack for log management and analysis

- Setting up the ELK Stack for log ingestion, filtering, and visualization

MITRE ATT&CK Framework for Threat Hunting

- Understanding MITRE ATT&CK Framework
- Using MITRE ATT&CK Framework its applications in threat hunting

Integrating Threat Intelligence and Threat Hunting

- Leveraging Threat Intelligence to guide threat hunting

Introduction To The Dark Web

- Understanding the Dark Web: Definition, Purpose, and Misconceptions
- Differentiating between the Dark Web, Deep Web, and Surface Web
- Understanding the Dark Web: Definition, Purpose, and Key Features
- Overview of Dar Web Protocols (e.g., Tor, I2P) and Their Significance

Dark Web Infrastructure

- Setting up and Configuring Tor Browser for Safe Dark Web Browsing
- Introduction to I2P and other Alternative Dark Web Networks
- Identifying and Accessing Dark Web Gateways and Hidden Services

Deep Web Intelligence Gathering

- OSINT Techniques Specific to the Dark Web
- Extracting Valuable Intelligence from Dark Web Forums and Communities
- Dark Web Content Analysis: Identifying Trends, Threats, and Actor
- Dark Web Reconnaissance: Collecting Information on Marketplaces,

Forums and Individuals

Dark Web Enumeration

- Exploring the Dark Web for Finding Organization Information
- Finding Employee Information on Dark Web
- Finding the Behavior of APTs and Their TTP
- Detecting Exposed Credentials

Introduction to Security Information and Event Management and Tools

- Overview of SIEM Concepts and Importance
- Overview of AlienVault OSSIM
- Key Features and Capabilities
- Understanding OSSIM Architecture and Components
- Exploring the OSSIM interface

Data Collection and Log Management

- Setting Up Data Sources and Collection
- Log Management and Parsing in OSSIM
- Overview of Syslog and Plugin Configuration
- Configuring and managing data sources

Creating and Managing Alerts

- Overview of Threat Detection and Alerts in OSSIM
- Creating Custom Alerts and Rules
- Configuring Notification Channels

- Creating and customizing an alert
- Setting up and testing notification channels

Building Dashboards and Reporting

- Overview of Dashboards in OSSIM
- Customizing Dashboards for Monitoring
- Configuring Reports for Security Operations

Introduction to Web Application Firewalls (WAFs)

- Overview of WAFs and their role in web application security.

Understanding How WAFs Work

- **Rule-Based Filtering**: Defining and applying static rules to block malicious traffic.
- **Anomaly Detection**: Identifying unusual traffic patterns and potential threats.

Understanding OWASP Top 10 and CWE Top 25

- Detailed insights into the most critical security vulnerabilities.

Simulating Common Web Attacks

- Practical exercises on attacks like:
  - SQL Injection
  - Cross-Site Scripting (XSS)
  - Broken Access Control
  - Cross-Site Request Forgery (CSRF)

Other OWASP Top 10 threats.

Introduction to Firewalls

- What is a Firewall?
- Types of Firewalls (Packet Filtering, Stateful Inspection, Proxy Firewalls, etc.)
- Overview of Key Firewall Tools (e.g., pfSense)
- Importance of Firewalls in Network Security

Setting Up Firewalls

- Installing and Configuring an Open-Source Firewall (pfSense)
- Understanding Firewall Rules and Policies
- Traffic Flow Management: Controlling Incoming and Outgoing Traffic
- Best Practices for Initial Configuration

Core Firewall Use Cases

Configuring a Proxy Server

- Proxy Server Basics
- Using a Firewall as a Proxy
- Benefits of Proxy Configuration

DMZ (Demilitarized Zone) Configuration

- Purpose of a DMZ
- Securing Web and Email Servers in a DMZ

Firewall Rules for DMZ

IDS/IPS Configuration

- Intrusion Detection Systems (IDS) vs. Intrusion Prevention Systems (IPS)
- Configuring IDS/IPS in a Firewall
- Detecting and Blocking Malicious Traffic

Blocking Websites

- URL Filtering
- Configuring Firewalls to Block Specific Websites or Categories

Zero Trust Implementation

- Principles of Zero Trust Architecture

Firewall Management and Monitoring

- Monitoring Logs and Traffic Reports
- Identifying and Resolving Configuration Issues