BİLİŞİM ACADEMY

Bilişim Academy
Cyber Security Expertise
Curriculum

Bilişim Academy
Cyber Security Expertise Curriculum

CONTENT

1 | NETWORK CURRICULUM

2 | PENTEST CURRICULUM

3 | SOC CURRICULUM

4 | OFFLINE CURRICULUM

- Adli Bilişim Uzmanlığı
- Bulut Bilişim Uzmanlığı
- Malware Analysis
- KVKK (GDPR)
- ISO 27001
- Elastic Stack

BİLİŞİM ACADEMY

NETWORK CURRICULUM

NETWORKING FUNDAMENTALS

1.1 Basic Switch, Router and End Device Configuration

1.2 Protocols and Models (OSI-TCP/IP)

1.3 Network topologies and network types

1.4 Cables and connectors

1.5 Common ports and protocols

1.6 Number Systems

1.7 Ethernet Switching

1.8 Address Resolution-ICMP

1.9 IPv4 Addressing

1.10 IPv6 Addressing

NETWORK IMPLEMENTATIONS

2.1 Switching Concepts

2.2 VLANs-Inter-VLAN Routing

2.3 STP Concepts

2.4 EtherChannel

2.5 SLAAC and Network Service (DHCP-DNS-NTP)

2.6 FHRP Concepts

2.7 Wireless LAN Concepts and Configuration

2.8 Static and Dynamic Routing (RIP, E/IGRP, BGP, OSPF)

2.9 ACL Concepts

2.10 NAT for IPv4

2.11 QoS Concepts

NETWORK OPERATIONS

3.1 Organizational Documents and Policies

3.2 High Availability-Cloud Concepts

3.3 Network Management and Monitoring (SNMP, CDP, LLDP, SYSLOG, Netflow)

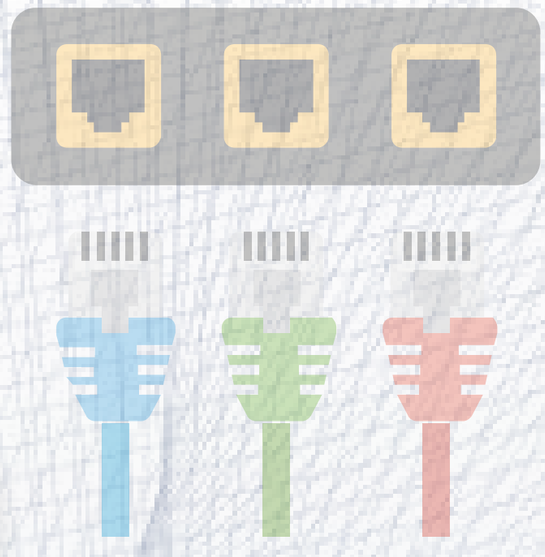
3.4 Network Virtualization and Automation

NETWORK SECURITY CONCEPTS

4.1 Common types of attacks

4.2 Network hardening techniques

4.3 VPN and IPsec Concepts



NETWORK TROUBLESHOOTING

5.1 Network Troubleshooting

BİLİŞİM ACADEMY

PENTEST CURRICULUM

SECTION 1: ETHICAL HACKING INTRODUCTION

1.1 Definition and Scope of Ethical Hacking

1.2 Ethical and Legal Principles

1.3 The Importance of Ethical Hacking

SECTION 2: FOOTPRINTING AND DISCOVERY

2.1 Passive Exploration Techniques

2.2 Active Discovery Techniques

2.3 Open Source Intelligence (OSINT)

SECTION 3: NETWORK SCANNING

3.1 Network Scanning Basics

3.2 Network Scanning Techniques

3.3 Vulnerability Scanning

SECTION 4: ENUMARATION

4.1 Enumeration Techniques

4.2 Enumeration Application

4.3 Web Server

SECTION 5: VULNERABILITY ANALYSIS

5.1 Vulnerability Lifecycle
5.2 Vulnerability Assessment Tools

SECTION 6: SYSTEM HACKING

6.1 System Hacking Techniques
6.2 System Attack Tools and Frameworks

SECTION 7: MALWARE

7.1 Types of Malware
7.2 Malware Analysis

SECTION 8: NETWORK LISTENING

8.1 Network Listening Concepts
8.2 Network Listening Tools

SECTION 9: SOCIAL ENGINEERING

9.1 Social Engineering Methods
9.2 Social Engineering Toolkits

SECTION 10: DENIAL OF SERVICE (DDoS)

10.1 Denial of Service Techniques
10.2 Distributed Denial of Service attacks

SECTION 11: SESSION HIJACKING

11.1 Session Hijacking Techniques

11.2 Session Pinning

SECTION 12: IDS, FIREWALL AND HONEYPOT AVOIDANCE

12.1 IDS/IPS Evasion

12.2 Firewall Avoidance

12.3 Honeypot Avoidance

SECTION 13: HACKING WEB SERVERS

13.1 Web Server Architecture

13.2 Web Server Attacks

SECTION 14: HACKING WEB APPLICATIONS

14.1 Web Application Architecture

14.2 Web Application Vulnerabilities

SECTION 15: SQL INJECTION

15.1 SQL Injection Techniques

15.2 SQL Injection Tools

SECTION 16: HACKING WIRELESS NETWORKS

16.1 Wireless Security Fundamentals

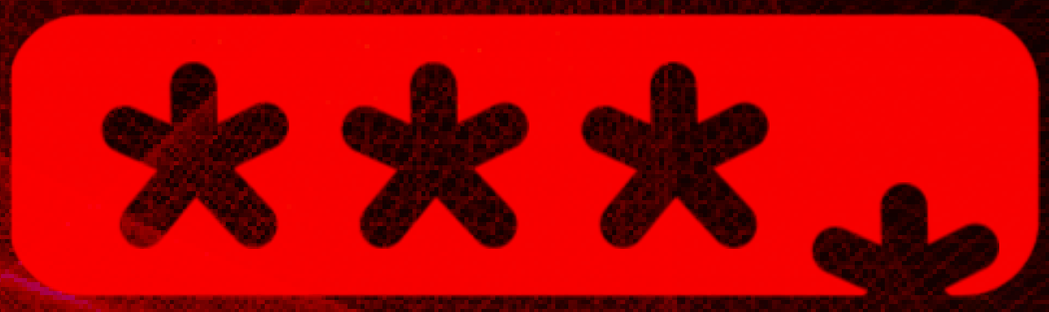
16.2 Wireless Attack Techniques

SECTION 17: HACKING MOBILE PLATFORMS
17.1 Mobile Security Fundamentals
17.2 Mobile attack Techniques

SECTION 18: IOT AND OT HACKING
18.1 IoT and OT Security Fundamentals
18.2 Attacking IoT and OT Devices

SECTION 19: CLOUD SECURITY
19.1 Cloud Security Fundamentals
19.2 Cloud Attack Techniques

SECTION 20: ENCRYPTION
20.1 Encryption Basics
20.2 Password Cracking Techniques



SECTION 21: RESULTS AND APPLICATIONS
21.1 Post-Attack Activities
21.2 Reporting and Communication
21.3 Protection Strategies

C|EH™ Certified Ethical Hacker

CompTIA PenTest+

BİLİŞİM ACADEMY

SOC CURRICULUM

SECTION 1 - INTRODUCION TO BLUE TEAM

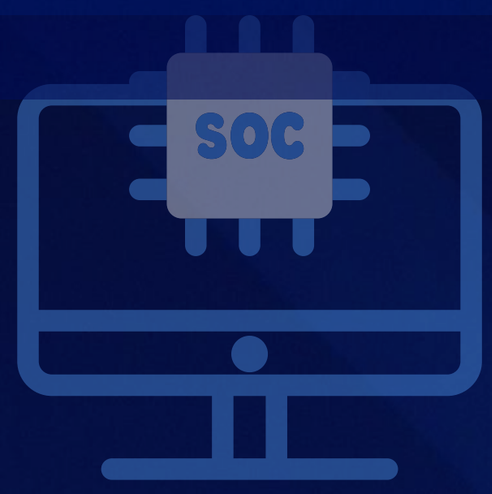
- SOC Structure
- Threat Actors
- Attack Types
- Personal Data and GDPR
- What are SOAR and SIEM?

SECTION 2 - WINDOWS OPERATING SYSTEM

SECTION 3 - CRYPTOGRAPHY

SECTION 4 - QRADAR / THE HIVE

- General SIEM Logic and QRadar Introduction
- Interface Introduction
- Dashboard Creation
- Report Creation
- Log Activity
- Offense -1
- Offense-2
- Offense-3
- AQL Writing / CRE / Building Block / Rules



SECTION 5 - SPLUNK

- Introduction to Splunk
- Spl Explanation and Correlation Writing
- Attacks
- Splunk Forwarder

SECTION 6 - CROWDSTRIKE

SECTION 7 - FIREWALL - FORTINET

- What is Next Generation Firewall?
- How it functions?
- Netwroking in Firewall
- Security Profiles
- Firewall Policy
- Eve-ng Topology for FW

SECTION 8 - WIRESHARK NETWORK ANALYSIS

SECTION 9 - COMPTIA SA+ (SLIDE REVIEW - QUESTION SOLUTION)

1.Modül

2.Modül

3.Modül

CISCO CERTIFIED CCNA

C|EH CERTIFIED ETHICAL HACKER

CompTIA Cybersecurity Analyst+

CompTIA Network+

CompTIA PenTest+

CISCO CERTIFIED CyberOps Associate

CompTIA Security+