Network Defense Essentials

Provider: EC-Council (Coursera/edX)
Completion Date: May 3, 2025

Overview

This course provided a structured introduction to defending organizational networks through layered controls. It covered host-based and network-based firewalls, intrusion detection systems (IDS/IPS), honeypots, VPNs, and related defensive tools. The labs were hands-on and emphasized practical setup and troubleshooting, though some limitations in the virtual lab environment required adaptation.

Key Topics Covered

- Host-based firewall configuration in Linux using iptables
- Windows Firewall rules for inbound and outbound traffic
- pfSense firewall implementation for blocking websites and insecure ports
- Role of access control policies across Windows, Linux, and Windows Admin Center
- Host-based intrusion detection using Wazuh HIDS
- Network-based intrusion detection using Suricata IDS integrated with Splunk
- Traffic analysis and monitoring through tcpdump, Wireshark, and HoneyBOT
- Establishing secure tunnels using SoftEther VPN
- IoT security basics using MQTT Broker and TLS/SSL for encrypted device communication
- Disk encryption, data backup, and recovery as part of defense in depth
- PKI fundamentals including self-signed certificates and HTTPS setup

Practical Applications

The labs demonstrated how defensive tools work in practice. I configured host-based firewalls on both Linux and Windows, blocked traffic through pfSense, and applied access control rules in both Active Directory and Windows Admin Center. IDS functionality was explored through Wazuh and Suricata, though Suricata failed to execute properly due to a configuration error. In those cases, I documented the issue and referenced instructor-side outputs to confirm expected results. Honeypots and VPN exercises showed how malicious traffic can be detected and how secure communication can be established across untrusted networks. IoT communication was configured with MQTT Broker, though traffic

verification failed in Wireshark, which blocked the TLS/SSL steps. Additional labs demonstrated cryptography basics, including hashing with HashCalc and HashMyFiles, and disk encryption with VeraCrypt. Backup and recovery labs reinforced the importance of restoring data after failures.

Personal Reflection

This course highlighted both the strengths and challenges of applied network defense. The labs reinforced my ability to configure firewalls, intrusion detection systems, and secure communication channels. At the same time, the environment often lacked real-time error feedback, meaning that mistakes were only discovered at the final outcome. For a beginner, this created extra troubleshooting steps and occasional incomplete labs, but I adapted by restarting timed sessions, documenting failures transparently, and verifying expected outcomes with provided resources. Overall, I strengthened my understanding of layered defenses and developed confidence in applying defensive tools across different environments, from enterprise networks to IoT devices.