Security Essentials

Week 1: Security Foundations: Understanding Threats and Defenses

- Information Security and Cybersecurity Frameworks
- BlueTeam VS RedTeam
- CIA Triangle
- Access Control Lists
- Security Controls
- Threat Actors
- Attack Surfaces
- Social Engineering
- Cryptographic Concepts.
- Symmetric Encryption and Asymmetric Encryption.
- Hashing (MD5, SHA)
- Encoding (Base64, HEX, URL)
- Compression (Lossless VS Lossy)
- Digital Signatures.

Week 2: Networking

- Network Protocols
- OSI Model & TCP/IP Model
- Internet Protocol
- Subnetting
- Link Layer Protocols and Devices
- Routing and Switching
- TCP and UDP

0xMekawy

- ICMP, DHCP, ARP and DNS

- SMB and NFS

- SNMP and SMTP

- Firewalls (Packet Filtering, Stateful Inspection and WAF)

- Network Defenses Devices

- Proxys

- Wireshark

Week 3: Revealing Linux Operating System

- What's Linux and its Distributions

- Linux File System Structure

- Linux Users, Groups and Permissions

- Linux Command Line – Navigation

- Linux Command Line - Working with Files and Directories

- Linux Command Line - Standard I/O/E

- Linux Command Line - Working with Data

- Linux Command Line - Base64

- Linux Command Line - Hex

- Linux Processes

- Piping and Redirection

- Linux Networking

- What are INodes?

- Symbolic Links

- Linux Run Levels

- Linux Logs

0xMekawy

Week 4: Revealing Windows Operating System

- Windows Basics
- Windows Registries
- Windows File System
- Windows Logs
- Windows Permission Management
- Windows Networking and Sharing
- Windows PE Files and DLLs
- Windows Server Setup
- Active Directory Basics
- Active Directory Services
- PowerShell Scripting

Week 5: Dealing With Programming

- What's a Compiler
- What's an Interpreter
- What's a Linker
- Programming with C++
- Intro To Assembly
- Programming with Python
- HTML, Javascript
- PHP, MySQL

Week 6: Recon and Exploitation

- What's Reconnaissance
- Passive Recon (Shodan, WHOIS,etc..)
- Google Hacking

0xMekawy

- Active recon (Port scanning, DNS, Nikto, Dirb, Sparta, Banner Grabbing)

- Vulnerability Scanners

- Misconfigurations

- Metasploit

- Cross Site Scripting (XSS)

- SQL Injection

- IDOR

Week 7: Network Attacks

- Authentication Bruteforce

- Windows Shares

- Null Sessions

- ARP Poisoning

- Exploit (FTP, SMTP, SNMP)

Week 8: System Attacks

- Password Attacks

- Active Directory Attacks

- Making A Simple Malware

0xMekawy