Program Overview:

Introduction into the exciting world of careers in Cyber Security. This program will take you in many directions highlighting roles as an analyst, penetration tester, systems administrator and computer crime investigator. You will learn priceless skills in this program to help keep you, your family and eventual employer safe on the internet for many years to come.

Certification Alignments:

CompTIA IT Fundamentals (FC0-U61)
CSX Cyber Security Fundamentals
CompTIA Security+ (SYS-501)
AccessData Certified Examiner

Curriculum:

TestOut IT Fundamentals
TestOut Security Pro
Marcraft Cyber Security Essentials
Marcraft Digital Forensics
Palo Alto Academy
Udemy Courses
TestOut Ethical Hacker Pro

Units:

Year 1 - For All Students to Complete
IT Fundamentals - Year 1

- PC Basics
    - Hardware
    - Operating Systems
- Networks
    - Cabling
    - Protocols
    - Services
    - IP Addressing
    - Devices
- Applications and Software
    - Business needs
    - DevOps needs
    - Databases
- Security Basics

        - Attack types
        - Introduce CIA triad
        - Business best practices
            - Phishing tests

Security Pro - Year 1

- Business Policies
    - Risk Management
    - Availability
    - Tabletop Exercises
    - Business Continuity
    - Industry Compliance
- Physical Security
    - Device Protection
    - Building Protection
    - Device Placement
- Network Perimeter
    - External Recon
    - UTM Configuration
    - VPN Access
    - DMZ
    - Wireless Attacks
- Internal Network
    - NAC
    - VLANs
    - ACLs
    - IDS/IPS
    - Zero-Trust Principle
- Host Security
    - Managed AV
    - GPOs
    - Log management
    - Audits
    - ICS/SCADA
- Application
    - AAA
    - Active Directory
- Data
    - File and Disk Encryption
    - PKI
    - Hashing and Integrity
    - DLP
    - Backup and Restore

Year 2 - students will pick 3 of these topics to study more in depth

Marcraft Cyber Security Essentials - Year 2 Choice

- Infrastructure Security
    - Access Controls
    - Badges
    - Intrusion Detection
    - Video Surveillance
- Local Host Security
    - Local Policies
    - Hardening Endpoints
- Local Network Security
    - Network shares
    - Network audits
    - Vulnerability scanning
- Cyber Security
    - NAT
    - Cryptography
    - Commands
    - Attack vectors
- Enterprise Network Security
    - Network Segmentation
    - Honeypots
    - Risk Management
    - Employee Training
- Industrial Cyber Security Systems
    - ICS
    - Protocols
    - Policies
    - SCADA Systems
- Medical Network Security
    - Medical Record Security
    - Data Retention and Destruction
    - IoT
- Introduction to Ethical Hacking
    - Recon
    - Social Engineering
    - Pen Testing

Digital Forensics - Year 2 Choice

- Basics
- Investigative Procedures
    - Investigative Model

    - Searches
- Data Storage
    - HDD Analysis
    - Discover Deleted Files
    - File Carving
- Storage Media and HW Devices
    - Safe Handling
    - Interfaces
    - Order of Volatility
- Passwords
    - Cracking Techniques
- Forensic Tools
- Steganography
- Static and Live Data Acquisition
- Mobile Device Data Acquisition
- Network Data Acquisition

Palo Alto Academy - Year 2 Choice

- Cyber Security Foundation
- Cyber Security Gateway
- Cyber Security Essentials

Python Programming - Year 2 Choice

- *Udemy Course*
- *Udemy Course*

PenTest+ - Year 2 Choice

- *TestOut Ethical Hacker Pro*

Cloud Security - Year 2 Choice

- *Udemy AWS Course*
- *Udemy Azure Course*

Practical Skills Over Both Years:

Identity Access Management

- 2FA
- Password Managers
- Permissions and Rights
    - Windows
    - Linux

Operating Systems/Hypervisors

- Windows Desktop and Server
    - Active Directory
    - Certificate Services
- Linux Desktop and Server
    - SSH
    - Secure File Systems
    - Run Open Source UTM
    - User Management
    - FreeRADIUS
- VMware Professional Workstation
    - Run simulated network
    - Pen test in secure environment

Confidentiality

- File encryption vs Full Disk
- Site to Site VPN configuration
- Dial up VPN configuration
- Using PKI for email and SmartCards
- Digital Certificates with Let's Encrypt
- 802.1x wired and wireless

Availability

- Configure Backup LAN and Cloud
- Test a Disaster Recovery Plan
- Configure NAC with PacketFence
- Build Applocker Rules in Windows
- Backup Network Device Configuration and Restore
- Endpoint Protection and Hardening
- IDS/IPS with OSSEC

Integrity

- Digital Signatures

- Password hashing and salting
- Configure file/folder audits
- SIEM with Security Onion and SGUIL
- Detect Anomalies with Files
- Write-blocking during forensic analysis

Incident Response and Pen Testing in simulated VM environment

Simulated Tabletop Exercises for Different Businesses

Cloud Services and Security Best Practice
- Azure
- Amazon AWS

Participation in multiple CTF competitions

Job Roles from NIST Framework:

SP->RSK Risk Management
Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new information technology (IT) systems meet the organization's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.

OM->NET Network Services
Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.

OV->TEA Cyber Instructor
Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs.

AN -> Threat Analysis
Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber threat/warning assessments

PR->CIR Cyber Defense Incident Responder
Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.

IN->FOR Cyber Defense Forensic Analyst
Conducts detailed investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.