PURDUE UNIVERSITY
Cyber Apprenticeship Program

Cybersecurity Analyst
(16 week)

Cybersecurity Foundations (CF)

Enterprise Security (ES)

Vulnerability Management (VM)

Ethical Hacking (EH)

Coursework developed through Purdue University cyberTap.

PURDUE UNIVERSITY
Cyber Apprenticeship Program

CF

40 hours

Cybersecurity Foundations

PURDUE UNIVERSITY
Cyber Apprenticeship Program

Cybersecurity Foundations (CF)

40 Content Hours

Description: Learn the basic principles of cyber and information security. Topics covered include general cyber domain knowledge, key security concepts, risk & vulnerability management, cryptography basics, and identity access management.

Audience:
- Those interested in learning about cybersecurity.
- Those interested in pursuing a career in information technology or cybersecurity.

Assessment and Credential:
- Successful completion through 70% or higher total grade in weighted deliverables including: Theory Exam (40%), Assignments (30%), Lab Quizzes (30%).
- Test Out Option Available

Recommendation Before You Begin:
- General Interest in Cybersecurity
- STEM or IT background helpful

PURDUE UNIVERSITY
Cyber Apprenticeship Program

Cybersecurity Foundations (CF)

40 Content Hours

Course Outline

Cybersecurity Principles
- CIA and Parkerian Hexad
- Access Control
- Auditing
- Data Structure
- Password Practices
- Attack Overviews

Risk Management
- Risk Assessment
- Types of Risk
- Security Policy
- Baseline Controls
- IT Security Management
- Risk Analysis
- Threat and Vulnerability Identification

Cryptography
- Encryption (Symmetric & Asymmetric)
- Algorithms used in Encryption
- Encryption Attacks
- Cryptosystems
- Hashing
- Cryptographic Tools

Identity and Access Management
- Basics of Identity and Access Management
- Identity Management
- IAM Lifecycle
- IAM Attacks
- IAM Methods
- IAM Technologies

Technical Tools

Self-paced virtual environment providing hands on application with:
- Windows Active Directory
- Microsoft Server Manager
- Windows Active Directory
- Terminal/Shell
- GnuPG
- WinSCP
- vi Editor
- icacls.exe
- PowerShell

Coursework developed through Purdue University cyberTap.

Cybersecurity Foundations (CF)

40 Content Hours

Learning Objectives

- Describe the history, context, problem statement and evolving nature of information security threats and controls as well as cybersecurity professional roles associated with each.
- Describe how cybersecurity and information security are the same, different, and interrelated .
- Classify security controls as technical, administrative, or physical.
- Explain the components of the CIA triad (Confidentiality, Integrity, & Availability).
- Explain the Parkerian Hexad Model and how it enhances C.I.A. with applicable use .
- Define and differentiate between authentication, authorization, and nonrepudiation.
- Explain the methods by which current authentication can occur and give examples of each.
- Describe attacks on different authentication mechanisms.
- Justify best practice guidelines for strong password development.
- Explain auditing methodologies and their necessity for authentication systems.
- Define and differentiate threats, vulnerabilities, attacks, events, and impacts, and how they relate.

(continued next page)

Cybersecurity Foundations (CF)

40 Content Hours

Learning Objectives

- Summarize risk planning with specific articulation of risk identification, transference, acceptance, and remediation.
- Discuss reputational impact of cyber risks.
- Compare and contrast risk analyses methodologies.
- Define and Analyze the relationship between continuity planning and cybersecurity risk management.
- Describe the fundamental laws, principles, and best practices of strong cryptosystems.
- Explain Kerckhoff's Principle & Perfect Secrecy using examples. Discuss how best practices assist in enforcing these laws/principles.
- Describe and differentiate secret-key encryption primitives.
- Explain and apply public key cryptography with emphasis on how aspects of applied PKI systems enforce the confidentiality, and availability of data and the system itself.
- Describe the key concepts of data integrity in system design by applying hash functions.
- Identify correct applications of various cryptographic techniques.
- Identify the vulnerabilities of the implementation of various cryptographic designs.

(continued next page)

Cybersecurity Foundations (CF)

40 Content Hours

Learning Objectives

- Define and differentiate identity and digital identity.
- Define access management models and methods associated with digital identity .
- Describe the digital identity lifecycle.
- Summarize NIST 800-63, Digital Identity Guidelines.
- Describe how database access control concepts differ from other access controls (system, file, etc).
- Compare and contrast common authentication solutions like RADIUS, TACACS, Kerberos, LDAP, etc.
- Define single sign-on (including Federated Identity Management) and common requirements for implementation.
- Identify common access control attacks along with possible counters for those attacks.

ES

40 hours

Enterprise Security

PURDUE UNIVERSITY
Cyber Apprenticeship Program

Enterprise Security (ES)

40 Content Hours

Description: Learn what it takes to create, implement, and manage enterprise level security efforts. Topics include security frameworks, network architecture, protocols, wireless security, monitoring, virtualization and cloud, basics of malware, data protection, and more.

Audience:
- Those interested in learning about cybersecurity.
- Those interested in pursuing a career in information technology or cybersecurity.

Assessment and Credential:
- Successful completion through 70% or higher total grade in weighted deliverables including: Theory Exam (40%), Assignments (30%), Lab Quizzes (30%).
- Test Out Option Available

Recommendation Before You Begin:
- Cybersecurity Foundations Completion, or
- 6+ months cybersecurity background

PURDUE UNIVERSITY
Cyber Apprenticeship Program

Enterprise Security (ES)

40 Content Hours

Course Outline

Security Programs and Architecture
- Enterprise Systems Architecture
- Risk Management Architecture
- Enterprise Security Architecture
- Standards & Frameworks
- Layered Defenses

Network Security Fundamentals
- Network Topologies
- Ethernet Protocol Standard
- Area Networks
- Networking & Protocols
- Wireless Security
- Access Control
- Designing Security into Networks
- Designing Networks for Security

Enterprise Concepts
- Endpoint Security
- Endpoint Vulnerabilities
- Controls
- Malware

Cloud Concepts and Virtualization
- Virtualization
- Virtualization Security
- Cloud-based Services
- Cloud Deployment Models
- Cloud Characteristics
- Cloud Migration Risks
- Cloud Security
- Securing IaaS

Industrial Control Systems
- Where they are found
- Security Functions
- Components
- SCADA
- Potential Attacks against ICS

The Internet of Things
- IoT and the Cloud
- Applications
- Protocols & Paths

Technical Tools

Self-paced virtual environment providing hands on application with:
- Wireshark
- pfSense Firewall
- Oracle VM VirutalBox

Enterprise Security (ES)

40 Content Hours

Learning Objectives

- Describe current and common architectures and frameworks for enterprise security programs.
- Describe underlying tools and technologies in the enterprise framework stack and associate them with appropriate discipline.
- Compare and contrast OSI and TCP/IP network models and the TCP/IP networking protocols suites.
- List and define common network topologies.
- Identify design requirements of TCP/IP networks based on various types of communication needs.
- Articulate secure network principles and apply that thinking to network design.
- Understand IP networking and Network Address Translation including IPV4 & IPV6
- Investigate security features of switches including the application of VLANs.
- Investigate security protocols in network routing management. (BGP, IS-IS, OSPF, etc.)
- Understand IEEE 802.1x network access controls, their role in network management, and how they can be applied.
- Compare and contrast wireless networking standards and security protocols.

(continued next page)

Enterprise Security (ES)

40 Content Hours

Learning Objectives

- Understand and apply strong authentication and access control methods to secure WLAN design.
- Identify network monitoring tools and techniques and explain their role in network security management.
- Describe how network traffic visualization and security monitoring systems expand the network monitoring horizon.
- Identify and differentiate cloud service models, platforms, architectures, and providers.
- Describe virtualization components and architecture designs.
- Compare and contrast security architecture of virtual and physical environments.
- Summarize threats and vulnerabilities unique to virtual environments.
- Demonstrate the implementation and use of virtual firewalls, IPS, proxies, and other security technologies.
- Describe the general architecture of cyber physical systems and the role of an ICS in different domains including public infrastructure and healthcare.
- Describe control mechanisms and communication protocols in ICS and IoT devices.
- Describe how software, endpoints, and network design are interdependent for data protection.
- Describe nature and severity of cyber-attacks and their detection and defense mechanisms.

PURDUE UNIVERSITY
Cyber Apprenticeship Program

VM

40 hours

Vulnerability Management

PURDUE UNIVERSITY
Cyber Apprenticeship Program

Vulnerability Management (VM)

40 Content Hours

Description: Learn about the basics of vulnerability concepts and analysis. Topics covered include threat hunting, vulnerability scanning & reporting, incident response, disaster recovery, application security, and more.

Audience:
- Those interested in learning about cybersecurity.
- Those interested in pursuing a career in information technology or cybersecurity.

Assessment and Credential:
- Successful completion through 70% or higher total grade in weighted deliverables including: Theory Exam (40%), Assignments (30%), Lab Quizzes (30%).
- Test Out Option Available

Recommendation Before You Begin:
- Cybersecurity Foundations Completion, or
- 6+ months cybersecurity background

PURDUE UNIVERSITY
Cyber Apprenticeship Program

Vulnerability Management (VM)

40 Content Hours

Course Outline

Vulnerability Assessment
- Security Testing
- Vulnerability Assessment Methodologies
- Documentation Review
- Target Identification & Analysis Techniques
- Vulnerability Scanners
- Target Vulnerability Validation Techniques
- Penetration Testing
- Threat Hunting

Incident Response
- Defining Terms
- Breach, Event, Incident, etc.
- Phases of Incident Response
- Incident Response Fundamentals
- The Cyber Kill Chain
- Incident Response Practice
- Disaster Recovery

Technical Tools

Self-paced virtual environment providing hands on application with:
- Windows Task Manager
- Windows Computer Management
- Microsoft Baseline Security Analyzer
- Damn Vulnerable Web Application (DVWA)
- PuTTY
- RATS
- skipfish
- vi Editor

Vulnerability Management (VM)

40 Content Hours

Learning Objectives

- Identify various computer security issues and relate suitable framework to evaluate security policies and procedures.
- Compare and contrast various network and computer security assessment methods.
- Explain the use, scope, and scale of vulnerability assessment activities and tools.
- Define baselining and its relationship to cybersecurity.
- Employ scanning tool to identify host, application, and network vulnerabilities.
- Practice monitoring, capturing, and analyzing network traffic to identify possible security threats/attacks.
- Describe and create a vulnerability assessment report and remediation plan.
- Define red, blue, and purple team scope and activities.
- Understand and apply various offensive network security techniques, including penetration testing, to select and/or recommend appropriate security controls.
- Articulate the role of a Threat Hunter.
- Summarize different types of threat hunting and their associated hunting teams.

(continued next page)

Vulnerability Management (VM)

40 Content Hours

Learning Objectives

- Understand what tools a threat hunter would use and why.
- Define the six stages of incident response: preparation, identification, containment, eradication, recovery, and lessons learned.
- Compare and contrast incident, breach, and compromise.
- Summarize NIST 800-61r2 incident response framework.
- Prepare incident response plan based on NIST 800-61r2.
- Explain how disaster recovery is different than incident response.
- Respond to a simulated security incident and execute incident response plan.
- Identify common code and developer introduced vulnerabilities, as seen in OWASP.
- Understand implications of common code and developer introduced application vulnerabilities.
- Understand application security best practices to avoid and remediate OWASP top 10 web application issues.
- Understand the differences between static and dynamic analysis of code; practice each.

EH

40 hours

Ethical Hacking

PURDUE UNIVERSITY
Cyber Apprenticeship Program

Ethical Hacking (EH)

40 Content Hours

Description: Learn the foundations for ethical hacking through videos, readings, and labs. Topis covered include the basics of ethical hacking, network and systems enumeration, vulnerability scanning, system attacks, sniffing, and social engineering.

Audience:
- Those interested in learning about cybersecurity.
- Those interested in pursuing a career in information technology or cybersecurity.

Recommendation Before You Begin:
- Cybersecurity Foundations (CF), Enterprise Security (ES), and Vulnerability Management (VM) Completion, or
- 1+ year cybersecurity experience

Assessment and Credential:
- Successful completion through 70% or higher total grade in weighted deliverables including: Theory Exam (40%), Assignments (30%), Lab Quizzes (30%).
- Test Out Option Available

PURDUE UNIVERSITY
Cyber Apprenticeship Program

Ethical Hacking (EH)

40 Content Hours

Course Outline

Disclaimer and Basics
- Role of Ethical Hacking
- Reconnaissance
- Tool Identification

Network Scanning
- Port Scanning, Ping Sweeps, etc.
- Packet Crafting
- Evasion Techniques

Enumeration
- Record Keeping
- Exploits vs. Compromise
- Using Metasploit

System Hacking
- Acquiring Exploits
- Passwords
- Post-exploitation Techniques

Sniffing
- Frame Capture and Analysis
- Port Mirroring/Spanning
- Common Spoofing Attacks

Social Engineering
- Purpose and principles
- Vishing, Phishing, Smishing
- Common Exploits

Technical Tools

Self-paced virtual environment providing hands on application with:
- Google Advanced Search
- Maltego
- theHarvester
- WHOIS
- Armitage
- Metasploit
- Nessus
- Nmap
- Wireshark
- Zenmap
- John the Ripper
- Meterpreter
- Egress Buster
- Windows Defender

Coursework developed through Purdue University cyberTap.

Ethical Hacking (EH)

40 Content Hours

Learning Objectives

- Disclaimer about techniques.
- Define an ethical hacker (white hat hacker).
- Describe the role of exploitation in ethical hacking, both as a proof of concept and as an information gathering step.
- Understand the importance of reconnaissance to later stages of an attack.
- Recognize the utility of open intelligence sources: SEC EDGAR, Romain and Regional Internet Registrars, Social Networking sites, etc.
- Utilize DNS intelligence tools and methods such as: host, Nslookup, dig, zone transfers, dnsrecon, etc.
- Obtain and Interpret web/http responses.
- Perform complex and context-appropriate Google searches using dorks.
- Recognize the utility of Shodan and Fing for ICS and IoT intelligence.
- Compare and Contrast currently implemented wireless security schemes: WEP, WPA, WPA2
- Identify the tools for sniffing wireless networks

(continued next page)

Ethical Hacking (EH)

40 Content Hours

Learning Objectives

- Differentiate how ping sweeps, port scanning, and vulnerability scanning play a role in ethical hacking vs. vulnerability management.
- Utilize nmap and Zenmap for port scanning activities.
- Contrast vulnerability identification and validation
- Define packet crafting and manipulation
- Explain how packet crafting and manipulation can be used in ethical hacking
- Identify scenarios where crafting packets is desirable, together with tools for doing so.
- Describe various evasion techniques and their uses (hide/obscure data, alterations, fragmentation, overlaps, malformed data, low and slow, resource consumption, screen blindness, tunneling, etc.)
- Define and describe enumeration
- Describe the importance of record-keeping activities in attacks.
- Differentiate between system exploit and system compromise.
- Use Nmap to determine the service versions

(continued next page)

Ethical Hacking (EH)

40 Content Hours

Learning Objectives

- Use RPCs, RMIs, and directory services to obtain remote information.
- Understand the place of Server Message Block (SMB) in Windows environments.
- Use Metasploit to perform common enumeration tasks.
- List methods of safely acquiring new exploits.
- Explain how password gathering and password cracking are related yet different.
- Define and describe when each of these post-exploitation techniques might be used: privilege escalation, pivoting, persistence, command & control, and covering tracks.
- Use Wireshark to capture and analyze frames.
- Use port mirroring/spanning to obtain frames for/from other interfaces.

PURDUE UNIVERSITY
Cyber Apprenticeship Program

Purdue Cyber Apprenticeship Program
Cybersecurity Analyst Price Sheet

	Hours	*Price*
	160	**$2,000.00**
Cyber Foundations	40	$500.00
Enterprise Security	40	$500.00
Vulnerability Management	40	$500.00
Ethical Hacking	40	$500.00

Optional

Industry CERT	Cost
CompTIA Security	$2,900.00
ECC CEH	$2,995.00
CISSP	$3,750.00