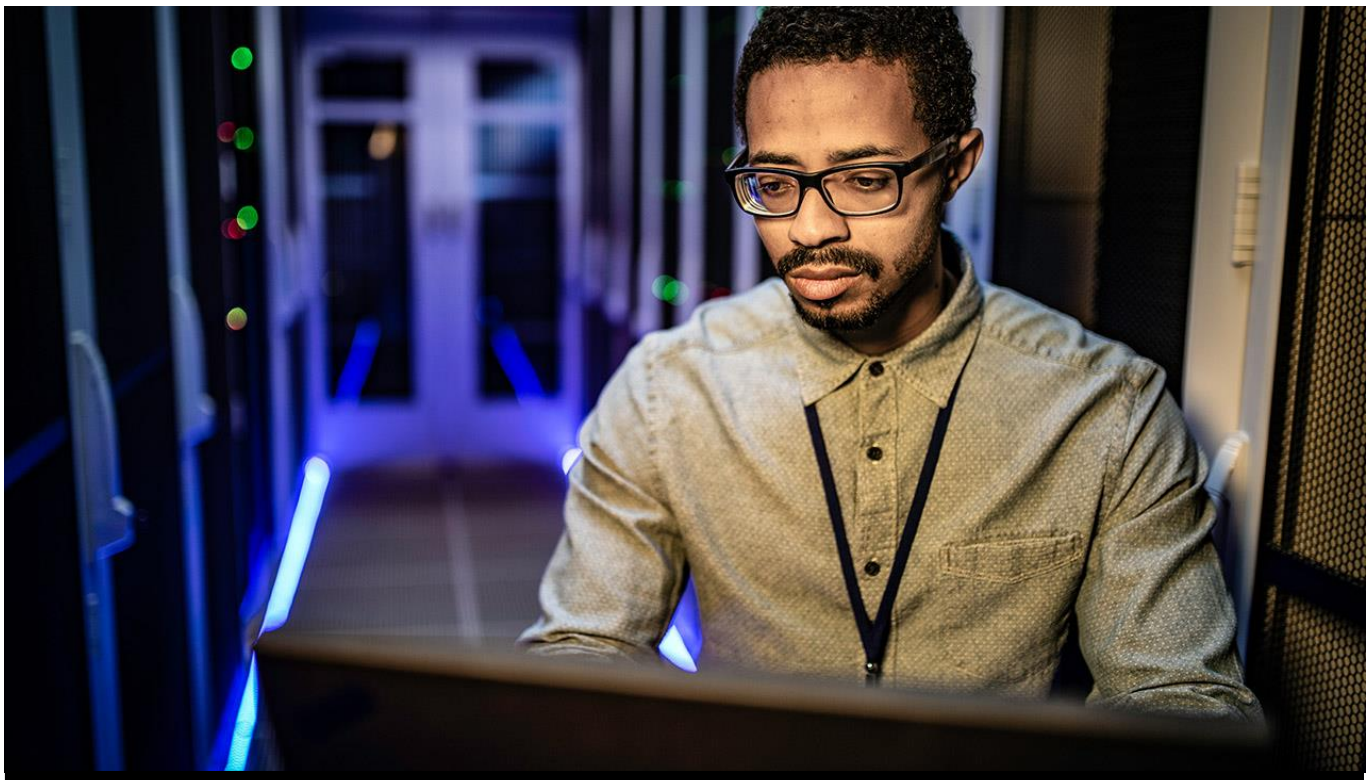


Penetration Tester to SpecOps Engineer

SKILLSOFT ASPIRE JOURNEY

skillsoft | percipio

Tracks

Track 1: Penetration Tester

In this Skillsoft Aspire track of the Penetration Tester to SecOps Engineer journey, the focus will be on Penetration Testing fundamentals, security measures, end-user behavior, physical and Wi-Fi pen ...

View More

Explore | 8 courses | 10h 21m 43s | 1 lab | 8h

Track 2: Incident Response Leader

In this Skillsoft Aspire track of the Penetration Tester to SecOps Engineer journey, the focus will be on incident response, preemptive troubleshooting, securing network appliances, monitoring system...

View More

Explore | 8 courses | 9h 55m 43s | 1 lab | 8h

Track 3: Ethical Hacker

In this Skillsoft Aspire track of the Penetration Tester to SecOps Engineer journey, the focus will be on Ethical Hacking.

Explore | 8 courses | 5h 43m 41s | 1 lab | 8h

Track 4: SecOps Engineer

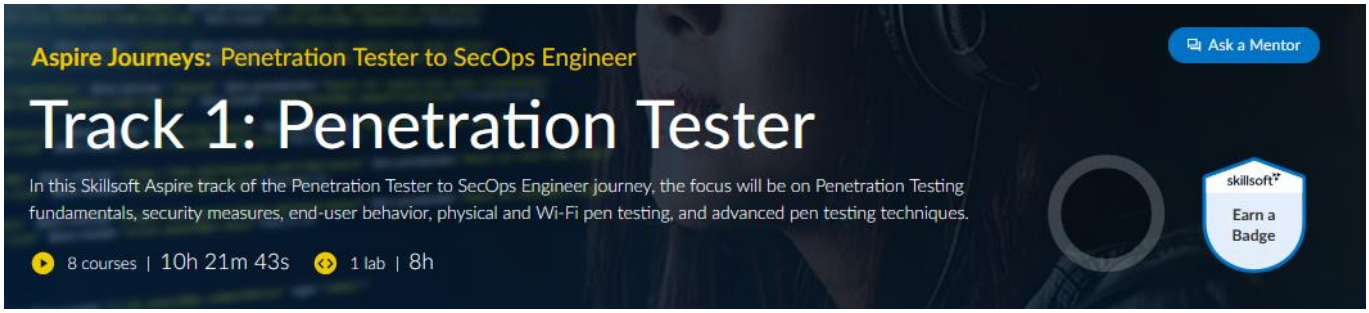
In this Skillsoft Aspire track of the Penetration Tester to SecOps Engineer journey, the focus will be on SecOps Engineering.

Explore | 6 courses | 4h 48m 48s | 1 lab | 8h

Prerequisites

We recommend the following prerequisite skills:

- Familiar with Penetration Testing
- Familiar with Ethical Hacking



Penetration Testing Fundamentals

Objectives:

- describe what penetration testing is and why it is important to the organization
- describe the common types of penetration and the importance of testing each type
- describe passive information gathering and methods for collecting information
- describe active information gathering along with methods and techniques for collecting information
- compare vulnerability to penetration testing and describe the function of each
- describe the cause of buffer overflow and how this exploit can be used for attacks
- describe user privilege escalation and methods that can be used to protect your system from security attacks
- describe common client-side attacks such as Cross-Site Scripting attacks and methods to help prevent them
- describe common web cyberattacks and countermeasures to prevent these attacks
- describe common password attacks and methods for preventing them
- describe port forwarding and how it can be used as an exploit
- describe the purpose of network tunneling and why it is important for penetration testing

Pen Testing Awareness: Results Management

Objectives:

- describe how to set expectations and why it is important
- describe black box penetration testing and why it may be used
- describe white box penetration testing and why it may be used
- describe grey box penetration testing and why it may be used
- describe the rules of engagement and how they are used
- describe the importance of setting stopping points and when to stop a penetration test
- describe what should be documented during a penetration test and why it is important
- describe the different categories of findings
- describe organizational risk tolerance and why it is important
- describe the importance of aligning recommendations to corporate culture, policies, and procedures
- describe how to communicate changes to lay persons and executives
- describe the importance of working with management to conduct further testing after recommendations are implemented

Security Measures: Implementing Security Controls

Objectives:

- describe security controls in relation to the overall NIST Cybersecurity Framework and how security controls are relevant in SecOps
- describe the major security control types and the components of a security control
- describe various areas where security controls are commonly used
- describe defensive and quick win controls for the major control types, how they are compromised, and steps for root cause analysis
- describe the CIS critical security controls and how they are implemented
- describe when to use security controls and how they are enforced
- describe various complex security controls and how they are implemented, including industrial and government security controls and baselines
- describe various controls for assessment and monitoring
- describe how to assess security controls, including establishing security metrics for risk management framework and reporting
- investigate security controls when one fails and describe how to mitigate the outcome
- describe processes of auditing security controls, including how to conduct an audit on control policies
- describe potential risk scenarios and how to mitigate and respond using security controls, including how to test the controls to effectively respond

Pen Testing: End-user Behavior

Objectives:

- identify penetration testing types and describe their reliance on end-user behavior
- describe the limitations of penetration testing and challenges for organizations
- identify the role of human error in causing data breaches
- describe the role of end-user awareness in preventing cybersecurity attacks and during penetration testing
- describe user behavior analytics and why it is important during penetration testing
- identify tools for performing user behavior analytics
- identify how to translate penetration testing results into a formalized report that can be used for the end-user awareness program
- recognize social engineering attacks and how to they relate to penetration testing
- describe how to perform social engineering penetration testing
- describe the goals of social engineering penetration tests
- describe tips and tricks for preventing social engineering attacks
- describe the role of human behavior in penetration testing

Physical Penetration Testing

Objectives:

- describe the importance of physical penetration testing and why organizations must perform penetration testing
- describe the steps necessary to implement a physical penetration testing program and the phases of penetration testing
- identify different lock pick tools and why lock picking is important in cybersecurity
- describe how to protect sensitive data with security testing and the five penetration testing rules of engagement
- describe penetration testing tools that are used by professional hackers
- identify the types of penetration testing and common terminology
- describe electromagnetic security vulnerabilities and devices that can help prevent this method of attack
- describe the purpose and results of dumpster diving and how to protect against this form of attack
- identify how to recognize and prevent tailgating and recognize the risks that it exposes
- describe how to document the findings of physical penetration testing and the key components of the report
- identify web application security testing methodologies and the five stages of OPSEC
- perform penetration testing using the Gruyere demo web site

Wi-Fi Penetration Testing

Objectives:

- identify the business need to provide Wi-Fi access for internal employees and external partners and recognize the categories of wireless threats that can compromise networks
- recognize the built in sniffing capabilities of Wi-Fi used for penetration testing
- step through the process to perform rough AP analysis
- identify the vulnerabilities and processes used to undermine an unsecured Wi-Fi hotspot
- describe the processes used to undermine a Wi-Fi client's vulnerabilities
- list the vulnerabilities of WEP security and identify how they can be exploited
- outline the steps used to perform a Denial of Service attack against a wireless network
- describe the technique of Wi-Fi fuzzing as a method to discover bugs over a wireless network
- list the vulnerabilities of WPA pre-shared key security and identify how they can be exploited
- identify best practices for taking Wi-Fi pen testing results and integrating them into security protocols and end-user education programs

Advanced Pen Testing Techniques

Objectives:

- describe how to find a vulnerability using scanners and other techniques
- capture and analyze network traffic using Wireshark
- recognize wireless security technologies such as WEP, WPA/2/3, and the vulnerabilities they have that could be exploited
- describe cryptography and its four goals
- differentiate between symmetric and asymmetric cryptography
- recognize how to choose a password cracking technique
- differentiate between malware types and recognize some of the consequences of using targeted malware
- differentiate between scanning and enumeration
- recognize the benefits of using Python to build scripts and deliver exploits
- perform Linux privilege escalation via writeable /etc/passwd file
- perform Windows privilege escalation to exploit a Windows system using the AlwaysInstallElevated technique
- use PowerShell to perform pen testing tasks such as reporting on all USB devices installed, killing processes, and using PSDrive to view objects in Windows

Final Exam: Penetration Tester

Objectives:

- capture and analyze network traffic using Wireshark
- compare vulnerability to penetration testing and describe the function of each
- describe active information gathering along with methods and techniques for collecting information
- describe black box penetration testing and why it may be used
- describe common client-side attacks such as Cross-Site Scripting attacks and methods to help prevent them
- describe common web cyber attacks and countermeasures to prevent these attacks
- describe cryptography and its four goals
- describe defensive and quick win controls for the major control types, how they are compromised, and steps for root cause analysis
- describe grey box penetration testing and why it may be used
- describe how to assess security controls, including establishing security metrics for risk management framework and reporting
- describe how to find a vulnerability using scanners and other techniques
- describe how to perform social engineering penetration testing
- describe how to protect sensitive data with security testing and the five penetration testing rules of engagement
- describe how to set expectations and why it is important
- describe passive information gathering and methods for collecting information
- describe penetration testing tools that are used by professional hackers
- describe security controls in relation to the overall NIST Cybersecurity Framework and how security controls are relevant in SecOps
- describe the cause of buffer overflow and how this exploit can be used for attacks
- describe the CIS critical security controls and how they are implemented
- describe the common types of penetration and the importance of testing each type
- describe the different categories of findings
- describe the goals of social engineering penetration tests
- describe the importance of physical penetration testing and why organizations must perform penetration testing
- describe the importance of setting stopping points and when to stop a penetration test
- describe the importance of working with management to conduct further testing after recommendations are implemented
- describe the limitations of penetration testing and challenges for organizations
- describe the major security control types and the components of a security control
- describe the processes used to undermine a Wi-Fi client's vulnerabilities
- describe the purpose and results of dumpster diving and how to protect against this form of attack
- describe the role of end-user awareness in preventing cybersecurity attacks and during penetration testing
- describe the rules of engagement and how they are used
- describe the steps necessary to implement a physical penetration testing program and the phases of penetration testing
- describe tips and tricks for preventing social engineering attacks
- describe user privilege escalation and methods that can be used to protect your system from security attacks
- describe various areas where security controls are commonly used
- describe various complex security controls and how they are implemented, including industrial and government security controls and baselines
- describe what penetration testing is and why it is important to the organization
- describe what should be documented during a penetration test and why it is important
- describe when to use security controls and how they are enforced
- describe white box penetration testing and why it may be used
- differentiate between malware types and recognize some of the consequences of using targeted malware

- differentiate between scanning and enumeration
- differentiate between symmetric and asymmetric cryptography
- identify different lock pick tools and why lock picking is important in cybersecurity
- identify how to recognize and prevent tailgating and recognize the risks that it exposes
- identify how to translate penetration testing results into a formalized report that can be used for the end-user awareness program
- identify penetration testing types and describe their reliance on end-user behavior
- identify the business need to provide Wi-Fi access for internal employees and external partners and recognize the categories of wireless threats that can compromise networks
- identify the role of human error in causing data breaches
- identify the types of penetration testing and common terminology
- identify the vulnerabilities and processes used to undermine an unsecured Wi-Fi hotspot
- identify web application security testing methodologies and the five stages of OPSEC
- investigate security controls when one fails and describe how to mitigate the outcome
- list the vulnerabilities of WEP security and identify how they can be exploited
- outline the steps used to perform a Denial of Service attack against a wireless network
- recognize how to choose a password cracking technique
- recognize social engineering attacks, and how to they relate to penetration testing
- recognize the built-in sniffing capabilities of Wi-Fi used for penetration testing
- recognize wireless security technologies such as WEP, WPA/2/3, and the vulnerabilities they have that could be exploited
- step through the process to perform rough AP analysis

Penetration Tester

Objectives:

- In this lab, you will perform Penetration Tester tasks such as performing network, service, vulnerability and automated scans. Then, test your skills by answering assessment questions after using Metasploit and third party exploits, as well as scanning websites and conducting brute force attacks.

Policy & Governance: Incident Response

Objectives:

- describe elements of an incident response policy and how it governs an incident response team
- describe the incident phases that an incident policy must address and the six stages in an incident response policy
- describe the tools available in incident response strategies including the three As in incident response and the OODA Loop
- describe how incident response is managed across various enterprise organizations, providing examples of cases where incident response policies are managed
- describe how an incident response plan is created and what to include in it, including planning scenarios and recovery objectives
- describe the concept of a Computer Security Incident Response Team, what a team is compromised of, models and their purpose, and the benefits of outsourcing and having a CSIRT internally
- recognize what roles to assign to each member of an incident response team and describe how team members would be engaged in various scenarios
- describe different incidence response scenarios and how an organization should respond with their incident response team
- describe governance policy, roles and responsibilities, and them purpose of incident response planning
- describe ISO 27001 and other various compliance standards, as well as how they are applied in incident response
- use governance policies to effectively create policies in incident response
- describe best practices and scenarios for establishing an incident response governance policy for several business and information sectors

Planning Measures: Incident Response Planning

Objectives:

- identify the purpose of an incident response plan and the costs of not having one in place
- list the steps to create incident response policies, plans, and procedures
- recognize when to create a CSIRT and who should be on that team
- identify the different purposes of the different roles on a CSIRT
- describe the elements of an incident response policy
- describe how the incident response plan will be used in practice

Preemptive Troubleshooting: Concepts & Strategies

Objectives:

- discover the key concepts covered in this course
- describe preemptive troubleshooting and how it applies to security and SecOps
- recognize how preemptive troubleshooting is different than intrusion detection systems
- describe policies and procedures for keeping systems secure in preemptive troubleshooting
- use tools to troubleshoot hardware and policies to prevent security compromise
- use password policies to enforce compliance
- update software and recognize the importance of doing so
- update hardware and recognize the importance of doing so
- describe how indicators of compromise can help reduce exploits in an environment
- identify how a security operations center can be a vital asset to an organization
- recognize how threat hunters can help spot threats before they occur
- differentiate between being preemptive and reactive in troubleshooting
- demonstrate how training can keep an organization secure

Security Best Practices: Network Appliance Security

Objectives:

- recognize the importance of securing network appliances and the top network security risks
- recognize best security practices for the Internet of Things
- describe the security risks and best practices for transitioning to the cloud
- recognize traditional infrastructure deficiencies, such as perimeter exploitation and de-perimeterization as a result of moving to the cloud
- recognize concerns of moving to the security first mindset and de-perimeterization problems
- describe Collaboration-oriented Architecture and how it can be used to deal with de-perimeterization
- recognize various security architecture models such as the Zero Trust Model, the intrusion kill chain, and the diamond model of intrusion analysis
- recognize the impact of software defined networking, virtual networking, and micro-segmentation to network security
- recognize the best security places for network devices such as Next Generation Firewalls, Network Intrusion Detection and Prevention Systems, and Distributed Denial of Service Attacks
- describe the Zero Trust Architecture and how to apply to the Zero Trust Model
- recognize Zero Trust challenges, problems, and concerns
- recognize and employ best practices for using the Zero Trust Architecture

Monitoring & Securing System Configuration

Objectives:

- describe the configuration management process and how it can influence securing system configuration for incident response
- describe tools and software available to monitor systems and their advantages for incident response
- describe continuous monitoring in risk management, including the three-tier approach and how it relates to monitoring system configuration
- recognize the process of minor, major, and unknown configuration changes, including what it means to an organization in terms of incident response and how they are prioritized in an incident strategy
- recognize the importance of securing the CM process in the SDLC for preventing security impacts
- recognize methods for identifying common high probability items, such as identifying default or weak credentials
- describe the process of implementing a secure system configuration monitoring program
- assess the monitoring process and perform a security configuration evaluation
- recognize methods of monitoring releases and deliveries throughout the software development lifecycle
- describe security controls for monitoring system configuration in a cyber framework
- recognize challenges organizations face today in monitoring system configuration and how they can be overcome
- recognize how monitoring system configuration is important in today's enterprise SDLC

Patch Management Strategies

Objectives:

- define patch management for incident response and describe how patch management affects the incident response team and the Security Operations Center
- describe the benefits and importance of a patch management strategy
- prioritize and rate the importance of patches for the software development environment
- describe the baselining, hardening, and how to develop a backout plan
- describe testing and configuration management in patch management
- describe vendor patches and how to implement them
- recognize the open source and commercially available tools that are used for patch management
- describe the process of rolling out patches in a patch management program and patch update policies
- recognize the various tools and techniques for automating patch implementations in organizations and the benefits they provide
- describe patch management in an Agile environment
- describe patching for serverless systems and the benefits of patching strategies using serverless systems
- recognize proper organizational patching strategies, how they are implemented, and the benefits of the implementation methods

Regulation Conformance for Incident Response

Objectives:

- describe regulation conformance and its importance in both an organization and for incident response
- describe examples of internal and external incidents and breaches, as well as how conformance applies to a DevOps environment
- describe the relationship between Agile and DevOps and regulation conformance complexities
- describe the importance of documenting incidents for compliance and incident response management, as well as how to apply best practices
- describe the various cybersecurity frameworks and compliance regulations that relate to an organization
- apply tips and tricks to keep up-to-date with rapidly changing laws and standards
- recognize the business needs that a conformance program addresses and the process for setting the groundwork to create a conformance program
- recognize and apply the techniques used to identify and calculate risk for a conformance program
- describe the importance of using external experts to assist with your conformance program
- recognize situations where legal communication or internal communication is necessary when handling incidents
- recognize the actions that should be taken when a incident occurs and where to find specific requirements within different regulations and standards
- recognize the need for a conformance program and describe how it assists the incident response leader with handling incidents

Final Exam: Incident Response Leader

Objectives:

- Define patch management for incident response. Describe the concept of patch management and how it affects the incident response team and the Security Operations Center (SOC)
- Demonstrate challenges organizations face today in monitoring systems configurations and how they can be overcome
- Demonstrate examples of internal and external incidents and breaches and how conformance in each example applies to a DevOps environment
- Demonstrate how to assess the monitoring process and how to perform a security configuration evaluation
- Demonstrate how to prioritize and rate the importance of patches for the software development environment.
- Demonstrate situations where an incident occurs for the need of legal communication or when Internal communication is necessary when handling incidents
- Demonstrate the actions taken when a incident occurs with regards to regulation conformance
- Demonstrate the methods in monitoring releases and deliveries throughout the Software Development Lifecycle (SDLC)
- Demonstrate the open source and Commercially available tools that are used for patch management
- Demonstrate the process of minor, major, and unknown configuration changes. What it means to an organization with unknown or minor changes for incident response and how its prioritized in an incident strategy
- Demonstrate the relation of patch management in an Agile environment
- Demonstrate the techniques used to identify and calculate risk with regards to a conformance program
- Demonstrate tips and tricks to keep up to date with rapidly changing laws and how to keep staff informed as change is implemented
- Describe briefly the Configuration Management process and how it can possess an influence in securing systems configuration for incident response

- Describe continuous monitoring in risk management including the three tier approach and how it relates to monitoring systems configuration
- describe different incidence response scenarios and how an organization should respond with their incident response team
- describe elements of an incident response policy and how it governs an incident response team
- describe governance policy, roles and responsibilities, and them purpose of incident response planning
- describe how an incident response plan is created and what to include in it, including planning scenarios and recovery objectives
- describe how incident response is managed across various enterprise organizations, providing examples of cases where incident response policies are managed
- describe how indicators of compromise can help reduce exploits in an environment
- describe policies and procedures for keeping systems secure in preemptive troubleshooting
- describe preemptive troubleshooting and how it applies to security and SecOps
- Describe regulation conformance and its importance in an organization and incident response
- Describe testing, and configuration management in patch management
- Describe the benefits of a patch management strategy and why its important
- describe the concept of a Computer Security Incident Response Team, what a team is compromised of, models and their purpose, and the benefits of outsourcing and having a CSIRT internally
- Describe the concept of patching for serverless systems and benefits of patching strategies using serverless systems
- Describe the importance of using external experts to assist with your conformance program
- describe the incident phases that an incident policy must address and the six stages in an incident response policy
- Describe the process in implementing a secure systems configurations monitoring program
- Describe the Process of Baselining, hardening, and how to develop a backout plan
- Describe the process of rolling out patches in a patch management program and the polices for patch updates
- Describe the security controls for monitoring systems configurations in the cyber framework
- describe the security risks and best practices for transitioning to the cloud
- Describe the steps to creating the appropriate conformance program for an organization
- describe the tools available in incident response strategies including the three As in incident response and the OODA Loop
- Describe the various cybersecurity frameworks and which regulations relate to an organization
- Describe the various tools and software available to monitor systems and their advantages for incident response
- describe the Zero Trust Architecture and how to apply to the Zero Trust Model
- discuss the elements of an incident response policy
- identify how a security operations center can be a vital asset to an organization
- identify the different purposes of the different roles on a CSIRT
- identify the purpose of an incident response plan and the costs of not having one in place
- list the steps to create incident response policies, plans, and procedures
- recognize best security practices for the Internet of Things
- recognize concerns of moving to the security first mindset and de-perimeterization problems
- recognize how preemptive troubleshooting is different than intrusion detection systems
- recognize the best security places for network devices such as Next-Generation Firewalls, Network Intrusion Detection and Prevention Systems, and Distributed Denial of Service Attacks
- recognize the impact of software-defined networking, virtual networking, and micro-segmentation to network security

- recognize the importance of securing network appliances and the top network security risks
- recognize traditional infrastructure deficiencies, such as perimeter exploitation and de-perimeterization as a result of moving to the cloud
- recognize various security architecture models such as the Zero Trust Model, the intrusion kill chain, and the diamond model of intrusion analysis
- recognize what roles to assign to each member of an incident response team and describe how team members would be engaged in various scenarios
- recognize when to create a CSIRT and who should be on that team
- recognize Zero Trust challenges, problems, and concerns
- update hardware and recognize the importance of doing so
- update software and recognize the importance of doing so
- use password policies to enforce compliance
- use tools to troubleshoot hardware and policies to prevent security compromise

Incident Response Leader

Objectives:

- In this lab, you will perform tasks commonly completed by Incident Response Leaders tasks such as implementing data governance, deploying software and hardware patches, and implementing monitoring, controls and backups. Then, test your skills by answering assessment questions after responding to an active threat and performing a root cause analysis on an active threat on both a Windows system and a cloud based system.

Ethical Hacker: Risk Assessment

Objectives:

- calculate risk levels in a quantitative manner
- identify and implement specific responses to risk
- assess security vulnerabilities using CVSS
- utilize the CIA triangle and the McCumber cube to assess risks and threats
- apply risk management standards according to NIST 800-37
- evaluate security in accordance with ISO/IEC 18045
- describe the COBIT 5 standard
- describe and use DREAD, PASTA, and other risk models

Ethical Hacker: Incident Response

Objectives:

- describe incident response concepts
- properly classify and describe different types of incidents
- create a response plan for physical incidents
- create a response plan for cyber incidents
- describe and apply basic incident response forensics includikng evidence handling and basic techniques
- apply basic incident response forensics including imaging a drive and basic legal standards
- conduct recovery and remediation activities
- conduct an after action review of incident response

Ethical Hacker: Security Standards

Objectives:

- describe secure software concepts
- properly apply filtering and data validation
- apply the NSA-IAM to ethical hacking to plan, execute, and report on your ethical hacking project
- apply the PTES to ethical hacking to plan, execute, and report on your ethical hacking project
- describe PCI-DSS standards and integrate them into ethical hacking
- describe and implement ISO 27001
- interpret and apply NIST 800-12
- employ NIST 800-26 standards to manage IT security
- describe NIST 800-14 security protocols

Ethical Hacker: Secure Technology & Applications

Objectives:

- describe security devices and how they relate to ethical hacking
- correctly deploy firewall solutions and describe their relevance to ethical hacking
- describe the usage of SIEM and deploy SIEM systems
- describe and utilize IDS/IPS and describe its relation to ethical hacking
- describe antivirus concepts and implement an AV strategy
- configure the firewall in Windows 10 and Windows Server 2019
- configure Windows Defender
- implement basic Snort IDS

Ethical Hacker: Account Creation

Objectives:

- recognize account creation concepts
- describe and implement MAC, DAC, and RBAC
- describe ABAC and its advantages over standard access control
- design access control and account management processes

Ethical Hacker: Scanning

Objectives:

- describe NMAP and how it can be used
- use NMAP to scan a target system or network
- use OWASP ZAP to scan a target web site
- use Vega to scan a target web site
- describe the Shodan search engine, its purpose and usage, and the role it plays in ethical hacking and penetration testing
- use Shodan to gather information about vulnerabilities
- use multiple informational web sites to gain information about a target
- apply specialized Google searches to find information for ethical hacking

Ethical Hacker: Hacking Techniques

Objectives:

- describe SQL injection and variations
- execute basic SQL Injection
- describe cross-site scripting
- describe malware threats
- recognize and describe types of malware
- implement an innocuous virus in penetration testing
- recognize types of DoS and associated counter measures
- describe how steganography works
- use common steganography tools
- recall the basics of Metasploit
- execute basic Metasploit commands
- use common Windows hacking techniques

Final Exam: Ethical Hacker

Objectives:

- apply basic incident response forensics including imaging a drive and basic legal standards
- apply risk management standards according to NIST 800-37
- apply the NSA-IAM to ethical hacking to plan, execute, and report on your ethical hacking project
- apply the PTES to ethical hacking to plan, execute, and report on your ethical hacking project
- assess security vulnerabilities using CVSS
- calculate risk levels in a quantitative manner
- conduct an after-action review of incident response
- conduct recovery and remediation activities
- configure the firewall in Windows 10 and Windows Server 2019
- configure Windows Defender
- correctly deploy firewall solutions and describe their relevance to ethical hacking
- create a response plan for cyber incidents
- create a response plan for physical incidents
- describe ABAC and its advantages over standard access control
- describe and apply basic incident response forensics including evidence handling and basic techniques
- describe and implement ISO 27001
- describe and implement MAC, DAC, and RBAC
- describe and use DREAD, PASTA, and other risk models
- describe antivirus concepts and implement an AV strategy
- describe cross-site scripting
- describe how steganography works
- describe IDS/IPS and describe its relation to ethical hacking
- describe incident response concepts
- describe malware threats
- describe NIST 800-14 security protocols
- describe NMAP and how it can be used
- describe PCI-DSS standards and integrate them into ethical hacking
- describe secure software concepts
- describe security devices and how they relate to ethical hacking
- describe SQL injection and variations
- describe the COBIT 5 standard
- describe the Shodan search engine, its purpose and usage, and the role it plays in ethical hacking and penetration testing
- describe the usage of SIEM and deploy SIEM systems
- describe types of malware
- design access control and account management processes
- employ NIST 800-26 standards to manage IT security
- evaluate security in accordance with ISO/IEC 18045
- execute basic Metasploit commands
- execute basic SQL Injection
- identify and implement specific responses to risk
- implement basic Snort IDS
- interpret and apply NIST 800-12
- properly apply filtering and data validation
- properly classify and describe different types of incidents
- recall the basics of Metasploit
- recognize account creation concepts
- recognize NMAP and how it can be used
- recognize SQL injection and variations
- recognize types of DoS and associated countermeasures
- recognize types of malware
- use common steganography tools
- use common Windows hacking techniques
- use multiple informational web sites to gain information about a target

- use NMAP to scan a target system or network
- use OWASP ZAP to scan a target web site
- use Shodan to gather information about vulnerabilities
- use Vega to scan a target web site
- use web sites to gain information about a target
- utilize IDS/IPS and describe its relation to ethical hacking
- utilize the CIA triangle and the McCumber cube to assess risks and threats

Ethical Hacker

Objectives:

- In this lab, you will perform tasks commonly completed by Ethical Hackers such as disaster recovery configuration and testing, digital forensics, and data exfiltration. Then, test your skills by answering assessment questions after scanning websites and conducting SQL injections, as well as employing common hacking techniques to gain access to Windows and Linux machines.

SecOps Engineer: System Infrastructure Security

Objectives:

- describe SecOps engineering concepts
- apply infrastructure hardening
- harden operating systems to mitigate threats
- analyze issues with Windows 10 and harden a Windows 10 PC
- describe and utilize security devices
- describe and utilize IDS/IPS
- describe and implement proper server hardening
- apply hardening to Windows 10
- harden a Windows 10 server
- describe firewalls and how to properly place them
- describe honeypots and utilize and deploy them effectively

SecOps Engineer: Secure Coding

Objectives:

- describe secure coding concepts
- apply filtering and data validation
- describe the importance of and how to apply practices from the CERT Top 10 list including validating input, paying attention to compiler warnings, secure design, coding for simplicity, and the principle of default deny
- describe the importance of and how to apply practices from the CERT Top 10 list including the principle of least privileges, sanitizing data, defense in depth, implementing quality assurance, and adhering to standards
- deploy software in a safe and secure manner
- apply delivery in a secure manner on an ongoing or continuous basis
- implement security verification and validation in software projects
- describe and utilize metrics appropriate for software security
- recognize and analyze C# examples of secure code
- recognize and analyze Python examples of secure code
- recognize and analyze Java examples of secure code

SecOps Engineer: Security Engineering

Objectives:

- discover the key concepts covered in this course
- describe security modeling techniques, including the CIA Triangle and the McCumber Cube
- describe and implement security engineering techniques
- use the Security Modeling Language
- analyze and utilize appropriate security metrics
- describe essential failure analysis
- apply failure analysis techniques to cybersecurity
- integrate systems engineering into cybersecurity operations
- acquire and analyze security requirements by applying requirements engineering techniques

SecOps Engineer: Cloud & IoT security

Objectives:

- discover the key concepts covered in this course
- describe cloud and IoT concepts and how they impact security
- describe common threats to IoT and cloud
- describe cloud architecture, types of clouds, and the use of cloud technology
- apply cloud security methods and techniques
- describe IoT concepts and usage
- implement IoT security for a wide range of IoT devices

SecOps Engineer: Threat Mitigation

Objectives:

- describe and integrate threat mitigation concepts into security operations
- analyze and mitigate malware threats
- describe approaches to ransomware mitigation
- describe threats to websites
- respond effectively to DoS attacks
- analyze the danger of insider threats and take mitigating steps
- integrate mitigation for social engineering into security operations
- describe the threats posed by phishing and integrate mitigation steps into security operations
- describe the threat of using insecure protocols and how to mitigate that threat
- use cyberthreat intelligence and integrate it into mitigation strategies
- use cyberthreat intelligence resources effectively

Final Exam: SecOps Engineer

Objectives:

- analyze and mitigate malware threats
- analyze and utilize appropriate security metrics
- analyze malware threats
- analyze the danger of insider threats and take mitigating steps
- apply cloud security methods and techniques
- apply common cyberthreat intelligence resources
- apply delivery in a secure manner on an ongoing or continuous basis
- apply failure analysis techniques to cybersecurity
- apply filtering and data validation
- apply hardening to Windows 10
- apply infrastructure hardening
- deploy software in a safe and secure manner
- describe and implement proper server hardening
- describe and implement security engineering techniques
- describe and integrate threat mitigation concepts into security operations
- describe and utilize IDS/IPS
- describe and utilize metrics appropriate for software security
- describe and utilize security devices
- describe approaches to ransomware mitigation
- describe cloud and IoT concepts and how they impact security
- describe cloud architecture, types of clouds, and the use of cloud technology
- describe common threats to IoT and cloud
- describe essential failure analysis
- describe firewalls and how to place them properly
- describe honeypots and utilize and deploy them effectively
- describe IoT concepts and usage
- describe SecOps engineering concepts
- describe secure coding concepts
- describe security modeling techniques, including the CIA Triangle and the McCumber Cube
- describe the importance of and how to apply practices from the CERT Top 10
- describe the threat of using insecure protocols and how to mitigate that threat
- describe the threats posed by phishing and integrate mitigation steps into security operations
- describe threats to web sites
- gather security requirements by applying requirements engineering techniques
- harden a Windows 10 server
- harden operating systems
- harden operating systems to mitigate threats
- identify and analyze Python examples of secure code
- identify approaches to ransomware mitigation
- identify cloud architecture, types of clouds, and the use of cloud technology
- identify common threats to IoT and cloud
- identify practices from the CERT Top 10 list
- identify SecOps engineering concepts
- identify security modeling techniques, including the CIA Triangle and the McCumber Cube
- identify threats to web sites
- implement infrastructure hardening
- implement IoT security for a wide range of IoT devices
- implement practices from the CERT Top 10 list
- implement security verification and validation in software projects
- integrate mitigation for social engineering into security operations
- integrate systems engineering into cybersecurity operations
- mitigate malware threats
- recognize and analyze C# examples of secure code
- recognize and analyze Java examples of secure code
- recognize and analyze Python examples of secure code

- recognize security requirements by applying requirements engineering techniques
- recognize the importance of practices from the CERT Top 10 list
- recognize threat mitigation concepts
- respond effectively to DoS attacks
- use the Security Modeling Language

SecOps Engineer

Objectives:

- In this lab, you will perform tasks commonly completed by SecOps Engineers such as configuring intrusion detection and prevention, Windows and network hardening, and creating and monitoring a honeypot. Then, test your skills by answering assessment questions after configuring items to protect against ransomware and denial of service attacks, configure auditing to detect insider threats, and implement controls to protect insecure and legacy systems.

Productivity Tools for SecOps Engineer

Optional

COURSE

Signing in & Setting up a Team

5

COURSE

Using the Conversation Tools

4

COURSE

Creating & Managing Projects

5

COURSE

Finding & Sharing Items

4

COURSE

Running Reports & Configuring Projects

4

COURSE

Signing In & Setting Up

5

COURSE

Using the Team Communication Tools

29

COURSE

Setting Up & Tracking Projects

2

COURSE

Managing your Project Tasks & Assets

6

COURSE

Using the Calendar Tools

4

COURSE

Using Basecamp for iOS

2

COURSE

Sign-in & Setup

1

COURSE

Communication Tools

3

COURSE

Working with Groups

1

COURSE

Creating, Finding, & Sharing Information

2

COURSE

Configuring Convo

2

COURSE

The Convo iOS App

1

COURSE

Introducing the JIRA Platform

111

COURSE

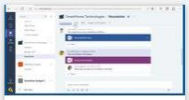
Leveraging the JIRA Platform for Development Projects

68

COURSE

Sign-in & Setup

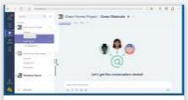
165



COURSE

Teams & Channels

149



COURSE

Conversation Tools

108

COURSE

Creating, Finding, & Sharing Information

103

COURSE

Call & Meeting Tools

95

COURSE

Signing in & Setting Up

19

COURSE

Using Channels

11

COURSE

Private Messaging & Communication Tools

16

COURSE

Creating, Finding & Sharing Information

6

COURSE

Configuring Slack

23

COURSE

Using the iOS App

3

COURSE

Sign-in & Setup

12

COURSE

Creating Teams & Boards

11

COURSE

Managing Cards

4

COURSE

Finding & Sharing Information

8

COURSE

Setting Up

32

COURSE

Posting & Reacting to Status Updates

22

COURSE

Using Groups

4

COURSE

Collaborating & Communicating

36

COURSE

Configuring Networks

14

Bookshelf

Optional

BOOK

Penetration Testing Essentials

12

BOOK

Security Controls Evaluation, Testing, and Assessment...

10

BOOK

Advanced Penetration Testing: Hacking the World'...

6

BOOK

Computer Incident Response Planning Handbook:...

1

BOOK

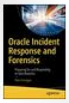
Security Patch Management, Second Edition

3

BOOK

Incident Response & Computer Forensics, Third...

2



BOOK

Oracle Incident Response and Forensics: Preparing fo...

BOOK

Computer Incident Response and Forensics Team...

6

BOOK

CEH Certified Ethical Hacker Practice Exams, Fourth...

6

BOOK

CEH Certified Ethical Hacker All-in-One Exam Guide,...

13

BOOK

Gray Hat Hacking: The Ethical Hacker's Handbook,...

6

BOOK

CEH v10 Certified Ethical Hacker Study Guide

17

BOOK

Securing DevOps: Security in the Cloud

3

BOOK

Introduction to Network Security: Theory and Practice

BOOK

From Hacking to Report Writing: An Introduction to...

2

BOOK

Penetration Testing Basics: A Quick-Start Guide to...

2

BOOK

Ethical Hacking and Penetration Testing Guide

43

BOOK

Coding for Penetration Testers: Building Better...

BOOK

Hacking and Penetration Testing with Low Power...

5

BOOK

Penetration Tester's Open Source Toolkit, Fourth...

6

BOOK

Professional Penetration Testing: Creating and...

17

BOOK

The Basics of Hacking and Penetration Testing: Ethical...

33

BOOK

Violent Python: A Cookbook for Hackers, Forensic...

30

BOOK

Wireless Reconnaissance in Penetration Testing

BOOK

Penetration Testing: Protecting Networks and...

8

BOOK

Professional Red Teaming: Conducting Successful...

1

BOOK

Metasploit: The Penetration Tester's Guide

55

BOOK

Penetration Testing: A Hands-On Introduction to...

31

BOOK

The Car Hacker's Handbook: A Guide for the Penetration...

9

BOOK

CompTIA PenTest+ Certification All-in-One...

3

BOOK

CompTIA PenTest+ Certification Practice Exam...

BOOK

Black Hat Python: Python Programming for Hackers...

18

BOOK

CompTIA PenTest+ Study Guide: Exam PT0-001

8

BOOK

Gray Hat C#: A Hacker's Guide to Creating and...

1

BOOK

Gray Hat Python: Python Programming for Hackers...

9

BOOK

The IoT Hacker's Handbook: A Practical Guide to Hackin...

1

BOOK

Beginning Ethical Hacking with Kali Linux...

2

BOOK

Beginning Ethical Hacking with Python

9

BOOK

Hands-On Ethical Hacking and Network Defense

32

BOOK

Attacking Network Protocols: A Hacker's Guid...

2

BOOK

Hacking with Kali: Practical Penetration Testing...

24

BOOK

Practical Information Security Management: A...

4

BOOK

Network Programming with Go: Essential Skills for Usin...

4

BOOK

Fundamentals of Information Systems Security, Second...

BOOK

Cryptography and Network Security: A Practical...

20

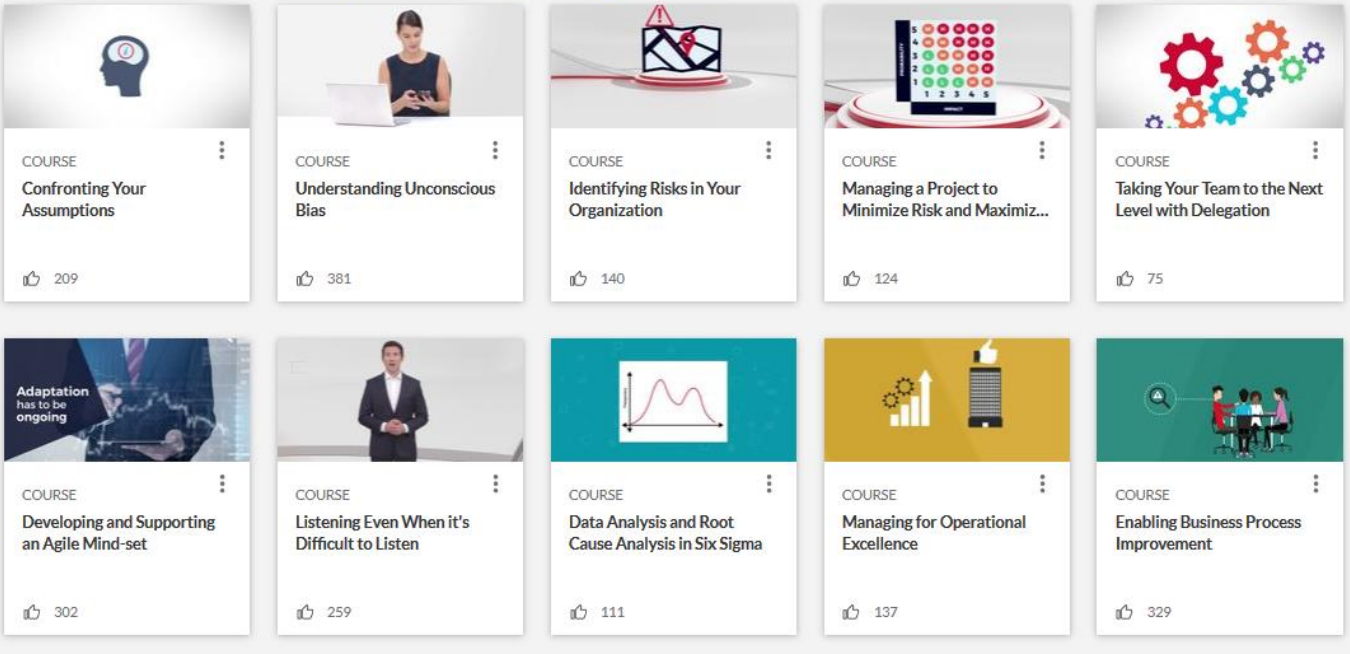
BOOK

Network Security and Cryptography: A Self-...

1

Business & Leadership for SecOps Engineer

Optional



FOLLOW US ON:

www.skilltech.pl

email: biuro@skilltech.pl

tel. +48 22 44 88 827

SkillTech

Technology hired for excellence