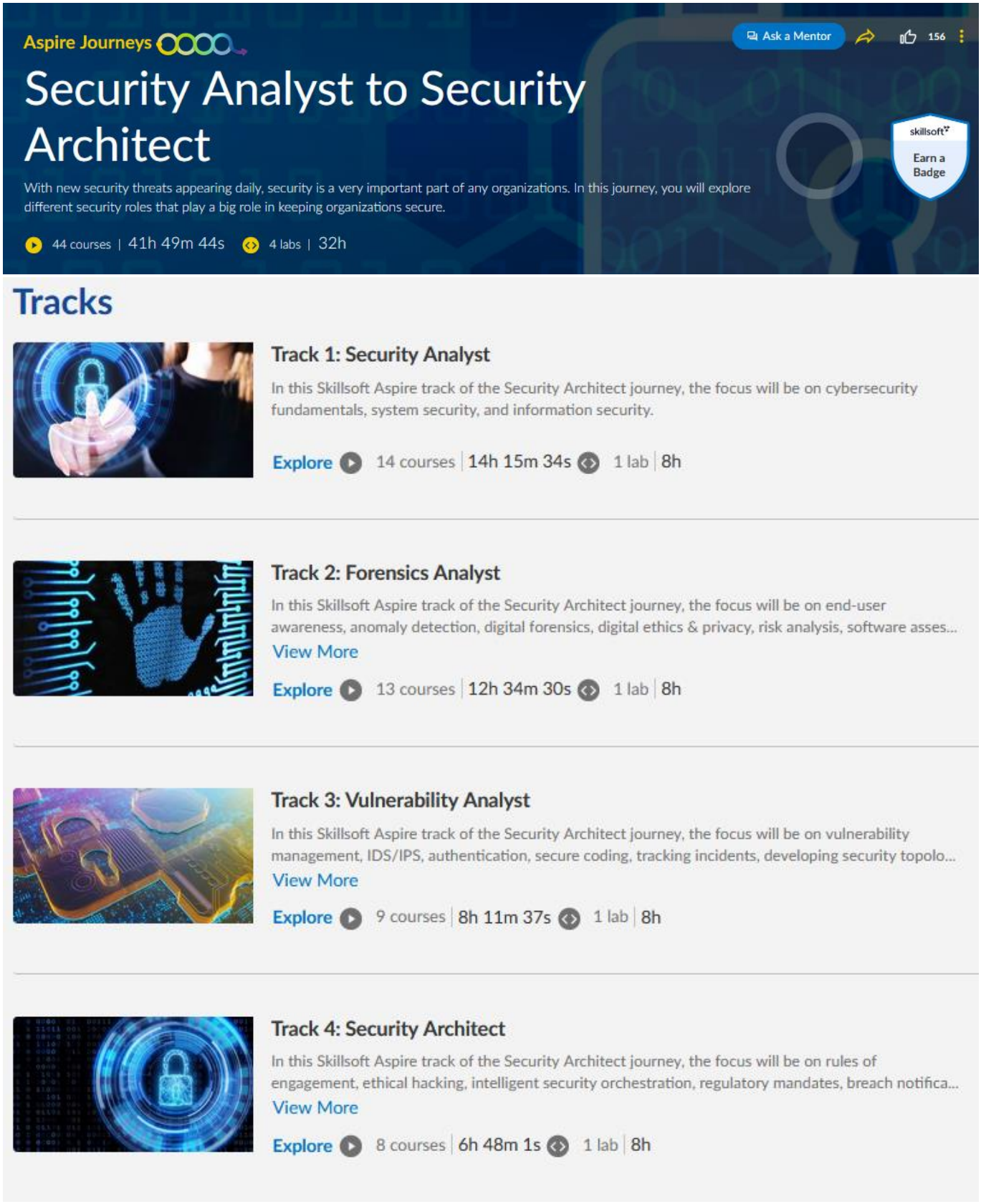
Security Analyst to Security Architect

SKILLSOFT ASPIRE JOURNEY

skillsoft | percipio



Prerequisites

We recommend the following prerequisite skills:

- Knowledge in traditional on-premise security practices
- Knowledge on the planning and implementation of security measures that combat risks associated with Cloud, AI and machine learning solutions.

Session & Risk Management

Objectives

- recognize digital assets that have value to the organization along with related threats
- identify and prioritize risks
- implement security controls to mitigate risk
- describe account management actions that secure the environment
- use Group Policy to implement user account hardening
- recognize how HTTP session management can affect security
- harden web browsers and servers to use TLS
- explain how centralized mobile device control can secure the environment
- recognize encryption techniques use to protect data
- configure a VPN to protect data in motion
- configure file encryption to protect data at rest
- configure encryption and session management settings

Auditing & Incident Response

Objectives

- list best practices related to IT security auditing
- use Group Policy to enable file system auditing
- scan hosts for security weaknesses from Windows
- scan hosts for security weaknesses from Linux
- describe the importance of securing mobile devices
- centrally apply security settings to mobile devices
- configure Amazon Web Services to use multifactor authentication
- recognize how security is applied to applications from design to use
- use file hashing to detect modifications
- specify actions used when dealing with security incidents
- view a packet capture to identify suspicious activity
- centrally apply security settings

An Executive's Guide to Security: Understanding Security Threats

Objectives

- describe what an attack surface is and how it must be understood in order to protect corporate information
- specify what network hardening is and how it relates to the protection of corporate information
- discuss network demilitarized zones and how they help protect corporate information
- describe the differences between threats, vulnerabilities, and risks in a corporate environment
- specify the top kinds of security threats facing organizations today
- discuss the common types of security attacks and how they each pose a risk to organizational data
- describe the role physical security plays in the protection of corporate data
- specify how social engineering is conducted and how it can be mitigated through corporate policy
- discuss the importance of corporate security policies and why they should be strictly adhered to
- describe the importance of password policies and why they should be adhered to
- specify the reasons why IT administrators need to protect an organization by refusing to bend the rules
- describe security threats, network hacks and attacks, and the human element in protecting organizational information

An Executive's Guide to Security: Protecting Your Information

Objectives

- describe best practices for working with and handling corporate information while traveling
- discuss the problems presented by organizational and personal e-mail, and best practices for working with e-mail, including how to protect yourself from spam
- specify the proper ways to handle sensitive company information, including the differences between working with online data and physical media
- describe best practices for sharing data with colleagues, customers, and the public
- discuss BYOD and IoT, how they pose a unique security threat for organizations, and how they should be treated on an organizational scale
- specify the challenges surrounding wireless networking and how wireless networks should be handled on an organizational scale
- discuss the dangers of posting on social media, as well as organizational policies and procedures
- specify the importance of implementing organizational security programs and why companies that don't have them put themselves at risk
- describe how employee training, awareness, and advocacy should be implemented and how it plays a crucial role in the protection of an organization's information
- discuss the importance of security programs and how to balance up-front costs vs. downtime in the long-run
- specify how new technology impacts security, and how to balance it in relation to convenience vs. security
- explain data protection practices, devices and social media, and corporate security principles and programs

Information Security: APT Defenses

Objectives

- define an Advanced Persistent Threat and its purpose
- list the steps of the APT lifecycle
- describe the motives behind an APT and the probable targets
- identify APT defense best practices
- identify the methods that can be used to make the APT defenses stronger
- recall the method(s) to deal with Advanced Persistent Threats
- describe the Equation AKA APT group and its involvement in various cyber crimes
- list the tools that are used when conducting an APT
- define risks and recall methods used to response, reduce, avoid, accept, and transfer risks
- define the risk assessment processes that can help you protect your assets
- identify the key points for creating an effective checklist to address APT attacks

Information Security: NACs & Gateways

Objectives

- identify the security risks introduced by BYOD and IoT along with their preventive measures
- list the major challenges with BYOD in an organization
- define NAC and the importance it has in a network
- illustrate the NAC architecture
- list the different features of NAC
- describe the impact of an improperly configured NAC
- list various NAC elements
- recall the best practices of implementing NAC
- identify the key point for creating an effective checklist for NAC Security
- list the NAC authentication methods

Information Security: Subnetting & DNS for Security Architects

Objectives

- describe subnetting and its advantages
- define the CIDR notation
- recognize subnetting tips and tricks
- compare VMs and containers
- describe the deployment considerations for virtual machines and containers
- recognize best practices for deploying virtual machines
- recognize best practices for VM and container security
- describe the various types of DNS attacks and their mitigations
- recognize the various types of subnetting attacks and mitigations

Information Security: Securing Networking Protocols

Objectives

- list the common protocols used in a network
- identify some of the security issues of the TCP/IP model at the layer level
- list the threats, vulnerabilities, and mitigation techniques in a network security
- identify the types of weak protocols and their replacements
- classify the various types of security protocols
- identify the ways to use security protocols in different situations
- describe the importance of implementing security protocols
- describe the security-first mindset and its necessity

Information Security: Hardened Security Topologies

Objectives

- define security topologies
- describe the elements used in designing goals of a security topology
- list the advantages and disadvantages of different security topologies
- describe the impact of integrating cloud topologies
- list the various layers of security in cloud computing
- name the different methods used to harden security topologies

Information Security: Continual Infrastructure Testing

Objectives

- define continuous security practices
- identify the need for continuous security in a DevOps environment
- describe the importance of continuous security
- list the benefits of using DevOps
- define continuous security monitoring and list its benefits
- identify the best practices of DevOps security
- define the secure DevOps lifecycle
- identify the security risks of DevOps
- list the various tools used for DevOps testing

Information Security: Security Governance

Objectives

- distinguish between governance and management
- describe the different types of IT governance frameworks
- identify the various roles and responsibilities of senior management in governance
- list the measures used to ensure good IT security governance
- identify the risks and opportunities in security governance
- describe the process of rolling out a security governance program
- describe the structure of a governance framework

Information Security: Honeypots

Objectives

- describe a honeypot
- classify the various types of honeypots that can be used
- describe the role played by honeypots in overall network security
- list honeypot disadvantages
- describe honeypot uses
- recognize the deployment strategies of a honeypot
- list the various open-source and commercial honeypot products available in the market
- specify how honeypots are placed in a network
- install and configure a honeypot using KFSensor honeypot softwaredescribe how honeypot data analysis is conducted

Information Security: Pen Testing

Objectives

- list the steps performed during the pen testing process
- specify the reasons an organization needs to perform pen testing
- distinguish between pen testing and vulnerability assessments
- compare different types of pen testing
- list the weaknesses of pen testing
- identify the various types of tools used in pen testing
- describe the target selection for pen testing
- identify the threat actors
- describe the types of assets in an organization
- compare the types of risk responses that an organization may adapt
- use the Metasploit framework in Kali Linux
- create an exploit using MSFvenom

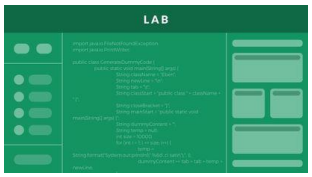
Final Exam: Security Analyst

Objectives

- classify the various types of honeypots that can be used
- classify the various types of security protocols
- compare governance and management
- compare pen testing and vulnerability assessments
- compare the types of risk responses that an organization may adapt
- compare the various types of honeypots that can be used
- compare VMs and containers
- compare VMs and containers characteristics
- configure a VPN to protect data
- configure a VPN to protect data in motion
- configure file encryption to protect data at rest
- define an Advanced Persistent Threat and its purpose
- define continuous security monitoring and list its benefits
- define the risk assessment processes that can help you protect your assets
- define the secure DevOps lifecycle
- describe best practices for working with and handling corporate information while traveling
- describe honeypot uses
- describe how employee training, awareness, and advocacy should be implemented and how it plays a crucial role in the protection of an organization's information
- describes the benefits of Continuous Security
- describe subnetting and its advantages
- describe the characteristics of APTs as well as their goals and objectives
- describe the elements used in designing goals of a security topology
- describe the importance of securing mobile devices
- describe the motives behind an APT and the probable targets
- describe the process of rolling out a security governance program
- describe the role physical security plays in the protection of corporate data
- describe the target selection for pen testing
- describe the various types of DNS attacks and their mitigations
- describe types of security topologies
- discover the key concepts covered in this course
- discuss network demilitarized zones and how they help protect corporate information
- discuss the problems presented by organizational and personal e-mail, and best practices for working with e-mail, including how to protect yourself from spam
- distinguish between governance and management
- distinguish between pen testing and vulnerability assessments
- identify the key point for creating an effective checklist for NAC Security
- identify the phases of the secure DevOps lifecycle
- identify the risks introduced by BYOD and IoT along with their preventive measures
- identify the security risks introduced by BYOD and IoT
- identify the security risks introduced by BYOD and IoT along with their preventive measures
- identify the threat actors
- identify the types of weak protocols and their replacements
- identify the various roles and responsibilities of senior management in governance
- identify the various types of security protocols
- identify the various types of tools used in pen testing
- list best practices related to IT security auditing
- list the NAC authentication methods
- list the steps of the APT lifecycle

- list the threats, vulnerabilities, and mitigation techniques in a network security
- recognize how HTTP session management can affect security
- recognize the deployment strategies of a honeypot
- scan hosts for security weaknesses from Linux
- specify how honeypots are placed in a network
- specify how social engineering is conducted and how it can be mitigated through corporate policy
- specify the importance of implementing organizational security programs and why companies that don't have them put themselves at risk
- specify the proper ways to handle sensitive company information, including the differences between working with online data and physical media
- specify the top kinds of security threats facing organizations today
- specify what network hardening is and how it relates to the protection of corporate information
- use Group Policy to enable file system auditing
- use Group Policy to implement user account hardening

view a packet capture to identify suspicious activity



Security Analyst

Objectives:

- Practice Security Analysts tasks such as using file hashing, file encryption, Wireshark and performing code reviews. Then, test your skills by answering assessment questions after installing and configuring LXD, using group policy, configuring a honeypot and exploring the Metasploit framework.

End-User Security: The End-User Perspective

Objectives

- describe shared responsibility
- define acceptable use policies
- distinguish physical security controls
- classify authentication technologies
- recognize the importance of hardware and software updates
- describe security suites and endpoint protection
- recognize browser best practices
- define e-mail security basics
- describe cloud security issues
- protect data in storage
- describe concepts and technologies of end-user security

End-User Security: The Security Administrator Perspective

Objectives

- recognize the present threatscape
- describe security policies
- define training and awareness
- compare access switch and WAP security
- describe 802.1x and MACsec
- describe Endpoint Detection and Response
- describe next-generation EDR
- list characteristics of next-generation EDR solutions, actions you can take with 802.1X PNAC, and attributes of an effective security policy

End-User Security: Securing End Users against Attackers

Objectives

- describe attack motivation
- define malware-as-a-service
- compare phishing techniques
- describe ransomware
- describe data breaches and theft
- define cryptojacking
- describe DoS and DDoS attacks
- compare common exploit kits
- list common motives for attacking endpoints, common ransomware payloads, and exploit kits

Anomaly Detection: Aspects of Anomaly Detection

Objectives

- recognize different anomalies or outliers, such as configuration faults or a malicious presence
- describe the benefits of anomaly detection, such as early response and planning for the unexpected
- recognize limitations of traditional approaches to anomaly detection, such as chasing false positives
- differentiate between manual and automated detection techniques
- describe the importance to building a profile of what is normal, such as user activity
- describe multimodal attributes and how they relate to anomaly detection
- differentiate between least frequency of occurrence and baselining
- describe the benefits of machine learning
- recognize the benefits of using auto-periodicity to aid in identifying anomalies

Anomaly Detection: Network Anomaly Detection

Objectives

- recognize concepts and applications of network behavior anomaly detection
- recognize how to implement frequency analysis
- identify beaconing activity
- recognize the signs of a brute force attack
- describe protocol analysis approaches and techniques
- deduce activity of encrypted web traffic
- analyze SSH authentication behavior
- provide an overview of population analysis
- describe techniques used to reveal hidden connections using behavioral analytics
- differentiate between different NBAD triage methods
- describe methods and techniques for performing network anomaly analysis and the benefits of anomaly detection
- describe how network forensics can be used to protect mission critical areas of business

Digital Forensic Techniques & Investigative Approaches

Objectives

- provide an overview of digital forensics
- recognize the different types of forensics including computer, mobile, network, vehicle, and IoT
- differentiate between criminal, civil, and intellectual property investigations
- describe a typical methodology or investigative approach, including preservation, collection, examination, analysis, and presentation in court
- describe the procedure to properly establish and maintain chain of custody
- recognize best practices and considerations when working with digital evidence
- describe the role of forensic laboratories and hardware and software tools
- recognize legal considerations including search warrants and privacy considerations
- describe challenges of working with cloud computing environments
- recognize how viruses and other malware work
- recognize the importance of ethical decision making related to digital forensic work
- describe approaches and techniques used when working with live or volatile data, such as confirming if encryption is in use and acquiring system memory

Ethics & Privacy: Digital Forensics

Objectives

- define what is considered a reasonable expectation of privacy
- differentiate between legal authorization forms such as consent forms and warrants
- describe the primary function of attorney-client privilege and confidentiality
- recognize legalities surrounding digital forensics investigative techniques
- describe the need for ethics in digital forensics
- describe best practices for ethics and forensics
- recognize the steps for regulating ethical behavior
- recognize possible conflicts of interest and how to avoid them
- describe the importance of ongoing training for both investigators and management on the importance of ethics
- recognize the different standards for analyzing digital evidence

Risk Analysis: Security Risk Management

Objectives

- describe risk as it relates to information systems
- differentiate between threats, vulnerabilities, impacts, and risks
- describe the first step of the NIST risk management framework, categorizing risk
- describe the second step in the RMF, selecting security controls
- describe the third step in the RMF, implementing security controls
- describe forth step in the RMF, assessing security control effectiveness
- describe the fifth step in the RMF, examining output of security controls assessment to determine whether or not the risk is acceptable
- describe the last step in the RMF, monitoring controls
- recognize the benefits of a control focused risk management approach
- list keys to presenting risk to shareholders, such as soliciting stakeholder input
- differentiate between different risk responses such as accepting, avoiding, mitigating, sharing, or transferring risk

Security Software Assessments

Objectives

- describe the major components of a security assessment and test strategies approaches
- recognize security control review methods including log and code reviews
- recognize security control testing mechanisms such as code testing
- describe the importance of a security management process and its common functions
- recognize steps to properly test software to ensure it is secure
- recognize methods to detect potential software vulnerabilities
- list common software vulnerabilities such as buffer overflow and injection flaws
- recognize how to avoid vulnerabilities by using secure coding techniques
- recognize steps and techniques to analyze risk
- describe penetration testing and its purpose
- describe microservices and APIs and highlight security concerns associated with each

Cyber Security Audits

Objectives

- describe cyber security auditing concepts and the NIST Cybersecurity Framework and how they are used to improve infrastructure security
- describe how to perform a cyber security assessment
- describe audit review, analysis, and reporting
- use the Wireshark network security auditing tool
- use the nmap perimeter security tool
- describe how to perform web application auditing and secure web application and web sites
- describe how to monitor and audit Windows using audit policies and the Event Viewer
- describe how to monitor the Linux system by reviewing system logs
- use the Tiger security audit and intrusion detection tool
- describe guidelines and standards for defining cyber security audit strategies
- compare available security audit tools and outline their features and benefits
- use the Nessus audit tool to run a Nessus security system scan

Cryptography: Introduction to Cryptography Services

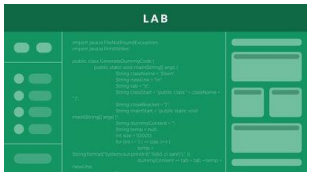
Objectives

- define the goals of information security
- describe cryptography services and associate those services with the goals of information security
- describe encryption and encryption history
- use CrypTool and the Caesar cipher
- describe symmetric encryption
- define common symmetric encryption algorithms
- demonstrate CryptTool and symmetric encryption
- describe asymmetric encryption
- define common asymmetric encryption algorithms
- describe the purpose of hashing
- define common hashing algorithms
- use CryptTool and hashing

Cryptography: Introduction to PKI

Objectives

- describe PKI and its components
- describe a certificate and the different types of certificates
- configure certificate properties
- identify certificate authority types and hierarchies
- install a certificate authority
- describe how digital signatures work
- describe how SSL is used to secure web traffic
- SSL enable a web site
- define the purpose of a CRL and how it works
- revoke a certificate and describe the effect of revocation
- install a certificate authority and secure web traffic to an IIS webserver by installing a certificate



Forensics Analyst Lab

Objectives:

- Practice Security Analysts tasks such as using file hashing, file encryption, Wireshark and performing code reviews. Then, test your skills by answering assessment questions after installing and configuring LXD, using group policy, configuring a honeypot and exploring the Metasploit framework.

Final Exam: Forensics Analyst

Objectives

- classify authentication technologies
- compare audit review, analysis, and reporting
- compare available security audit tools and outline their features and benefits
- configure certificate properties
- deduce activity of encrypted web traffic
- define common hashing algorithms
- define common symmetric encryption algorithms
- define cryptojacking
- define e-mail security basics
- define the goals of information security
- define the purpose of a CRL and how it works
- define training and awareness
- define what is considered a reasonable expectation of privacy
- describe 802.1x and MACsec
- describe a certificate and the different types of certificates
- describe approaches and techniques used when working with live or volatile data, such as confirming if encryption is in use and acquiring system memory
- describe asymmetric encryption
- describe audit review, analysis, and reporting
- describe cryptography services and associate those services with the goals of information security
- describe data breaches and theft
- describe DoS and DDoS attacks
- describe forth step in the RMF, assessing security control effectiveness
- describe guidelines and standards for defining cyber security audit strategies
- describe how network forensics can be used to protect mission critical areas of business
- describe how SSL is used
- describe how SSL is used to secure web traffic
- describe how to monitor the Linux system by reviewing system logs
- describe how to perform web application auditing and secure web application and web sites
- describe next-generation EDR
- describe ransomware
- describe shared responsibility
- describe symmetric encryption
- describe the first step of the NIST risk management framework, categorizing risk
- describe the importance of a security management process and its common functions
- differentiate between criminal, civil, and intellectual property investigations
- differentiate between different risk responses such as accepting, avoiding, mitigating, sharing, or transferring risk
- differentiate between least frequency of occurrence and baselining
- differentiate between legal authorization forms such as consent forms and warrants
- differentiate between threats, vulnerabilities, impacts, and risks
- distinguish physical security controls
- identify beaconing activity

- list common software vulnerabilities such as buffer overflow and injection flaws
- list keys to presenting risk to shareholders, such as soliciting stakeholder input
- protect data in storage
- provide an overview of digital forensics
- provide an overview of microservices and APIs and highlight security concerns associated to each
- provide an overview of population analysis
- recognize best practices and considerations when working with digital evidence
- recognize concepts and applications of network behavior anomaly detection
- recognize different anomalies or outliers, such as configuration faults or a malicious presence
- recognize how viruses and other malware work
- recognize legalities surrounding digital forensics investigative techniques
- recognize limitations of traditional approaches to anomaly detection, such as chasing false positives
- recognize possible conflicts of interest and how to avoid them
- recognize steps and techniques to analyze risk
- recognize steps to properly test software to ensure it is secure
- recognize the benefits of an event focused risk management approach
- recognize the benefits of using auto-periodicity to aid in identifying anomalies
- recognize the different standards for analyzing digital evidence
- recognize the different types of forensics including computer, mobile, network, vehicle, and IoT

Security Vulnerabilities: Managing Threats & Vulnerabilities

Objectives

- describe the categories of vulnerabilities using the STRIDE model
- describe authenticity and identity spoofing threats
- describe how to validate integrity and tampering threats
- describe authentication threats and non-repudiation
- describe information threats such as privacy breaches or data leaks
- describe the threat of denial of service attacks
- describe the privilege escalation threat model
- recognize examples of security misconfiguration threats
- describe methods of brute force attacks and key sizes
- perform a local network scan using Nmap
- perform a targeted remote scan using Nmap
- perform a DOS vulnerability diagnostic test on a host

Intrusion Detection: Best Practices

Objectives

- describe the approaches to network security through traffic analysis
- describe the tools and techniques used by intrusion detection systems
- describe the network forensic approach to computer networks
- describe the types of application controls that can be used for traffic analysis
- describe the placement and use of sniffing and IDS sensors
- describe the concepts of signal and noise when it comes to network traffic analysis
- perform IDS with Snort using a sample ruleset
- configure Bro to detect a common attack pattern
- use Wireshark to inspect network packets
- perform nmap scans using methods to evade IDS detection
- perform a brute force analysis with nmap
- perform a mock DOS attack with nmap

Intrusion Prevention: Best Practices

Objectives

- describe approaches to IPS and how it differs from IDS
- describe options and deployment strategies for IPS
- describe advantages and disadvantages of various approaches to IPS
- describe the role of IPS in preventing kernel attacks
- describe methods used to discover vulnerabilities
- describe remediation strategies related to intrusions
- block an attacker after too many failed login attempts
- describe methods used in IPS to evade intrusions
- use tools to scan for potential intrusions on a local system
- scan a system for potential malware infections using nmap
- use Suricata to implement a packet diversion for intrusion prevention

Authentication & Encryption: Best Practices

Objectives

- describe authentication, authorization, and encryption factors and how they fit together
- describe methods of authentication and their best practices
- describe methods of authorization and access control
- describe the use of encryption methods and best practices in implementing encryption
- differentiate between public and private keys and their ciphers
- describe methods of keeping login and authentication credentials secure
- describe system authentication and authorization through user account administration in Linux
- handle security policy trade-offs in situations where solutions might not align with policy
- implement and secure remote access to a system using SSH
- create secure certificates and keys using OpenSSL
- verify software package integrity using OpenSSL
- encrypt and decrypt files with OpenSSL

Security Topologies: Developing Secure Networks

Objectives

- describe the challenges of a secure-first network design
- describe a network design approach from a security mindset
- describe the challenges to DevOps and Agile mindsets in terms of security decisions
- describe the network security concerns for hybrid cloud models
- configure an NGINX HTTP service to prevent insecure file access
- configure web application security settings in NGINX
- describe the dangers of file upload remote execution
- use SSH as a secure proxy for web browsing from an insecure location
- configure an SSH client to use preset server connection settings
- use the local /etc/hosts to block unwanted connections
- describe the threat of user account discovery and how it is carried out
- use password security tools to enforce a strong password policy

Security Architect: Secure Coding Concepts

Objectives

- describe the principles that define a security architecture
- describe the issues and steps involved in security design
- describe the process and potential security flaws in security architecture implementation
- describe considerations for deploying and operating an application in secure environments
- describe methods and tools that can be used to help secure software through automation and testing
- describe approaches to assessing the risk of an application
- describe the life cycle of vulnerabilities in software
- describe common coding pitfalls that lead to security vulnerabilities
- describe industry standards and the application domains they apply to
- describe security concerns when adopting new technologies, coding languages, and platforms
- describe secure coding architecture when deploying cloud applications
- describe practical approaches to secure coding practices

Incident Tracking & Response

Objectives

- describe the key terms and definitions for communicating incident tracking concepts
- describe the categories of incidents and how they need to be tracked
- describe who needs to have access to incident tracking information
- describe how incident tracking can be integrated into an organization
- describe effective incident tracking practices
- describe tools used for incident tracking
- describe approaches to setting incident response policies
- describe metrics used to measure the effectiveness of incident tracking
- describe the continuous monitoring approach to active incident tracking
- describe the life cycle of an attack and how it is tracked
- describe how to take a proactive approach to tracking incidents
- describe some of the cyber-security regulations when it comes to tracking and responding to incidents

Defensible Security

Objectives

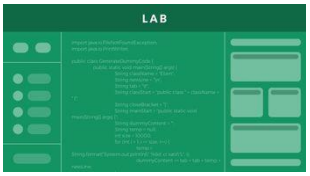
- describe the challenges and deficiencies of traditional security architectures
- describe some of the standards that address the challenges of security architectures
- describe the concepts and approaches to defensible architecture
- describe the zero-trust model for security
- describe the security architecture needs for layer 1, 2, and 3
- describe the principle of least privilege and how it pertains to security architecture
- describe the security benefit of reproducible builds
- configure a deny-first firewall using ufw
- configure a firewall to block all but a trust subnet
- configure a VPN service using WireGuard
- configure a secure VPN client to connect to a VPN server
- configure a firewall to block untrusted egress

Final Exam: Vulnerability Analyst

Objectives

- block an attacker after failed login attempts
- block an attacker after too many failed login attempts
- compare between public and private keys and their ciphers
- configure a deny-first firewall using ufw
- configure a firewall to block all but a trust subnet
- configure a firewall to block untrusted egress
- configure an NGINX HTTP service to prevent insecure file access
- configure a secure vpn client to connect to a vpn server
- describe advantages and disadvantages of various approaches to IPS
- describe a network design approach from a security mindset
- describe approaches to IPS and how it differs from IDS
- describe approaches to secure coding practices
- describe authentication threats and non-repudiation
- describe authenticity and identity spoofing threats
- describe common coding pitfalls that lead to security vulnerabilities
- describe effective incident tracking practices
- describe how incident tracking can be integrated into an organization
- describe how to validate integrity and tampering threats
- describe industry standards and the application domains they apply to
- describe information threats such as privacy breaches or data leaks
- describe methods and tools that can be used to help secure software through automation and testing

- describe methods of authentication and their best practices
- describe methods of authorization and access control
- describe methods of brute force attacks and key sizes
- describe methods of keeping login and authentication credentials secure
- describe methods used to discover vulnerabilities
- describe metrics used to measure the effectiveness of incident tracking
- describe options and deployment strategies for IPS
- describe practical approaches to secure coding practices
- describe security concerns when adopting new technologies, coding languages, and platforms
- describe some of the cyber-security regulations when it comes to tracking and responding to incidents
- describe the categories of vulnerabilities using the STRIDE model
- describe the challenges and deficiencies of traditional security architectures
- describe the challenges of a secure-first network design
- describe the continuous monitoring approach to active incident tracking
- describe the dangers of file upload remote execution
- describe the life cycle of an attack and how it is tracked
- describe the network forensic approach to computer networks
- describe the network security concerns for hybrid cloud models
- describe the placement and use of sniffing and IDS sensors
- describe the principles that define a security architecture
- describe the process and potential security flaws in security architecture implementation
- describe the security benefit of reproducible builds
- describe the threat of user account discovery and how it is carried out
- describe the tools and techniques used by intrusion detection systems
- describe the use of encryption methods and best practices in implementing encryption
- describe the zero-trust model
- describe the zero-trust model for security
- differentiate between public and private keys and their ciphers
- handle security policy trade-offs in situations where solutions might not align with policy
- identify how incident tracking can be integrated into an organization
- perform a targeted remote scan using Nmap
- perform IDS with Snort
- perform IDS with Snort using a sample ruleset
- perform nmap scans using methods to evade IDS detection
- recognize examples of security misconfiguration threats
- use password security tools to enforce a strong password policy
- use the local /etc/hosts to block unwanted connections
- use tools to scan for potential intrusions on a local system
- use Wireshark to inspect network packets



Vulnerability Analyst

Practice Vulnerability Analyst tasks such as performing local network scans, configuring Snort IDS, configuring and implementing intrusion detection, as well as configuring remote access with Secure Shell. Then, test your skills by answering assessment questions after cleaning input data, managing incidents, and configuring secure HTTPS and VPN services.

Security Rules: Rules of Engagement

Objectives

- provide a general overview of the Rules of Engagement, how the ROE relates to business, and the potential consequences of not having the ROE in place
- provide an overview of the benefits of having a easy reference checklist or templates prepared when defining RoE
- recognize how to determine the appropriate scope of engagement
- describe client (IT staff) considerations such as client contact details and potential impacts on their working environment
- describe common risks and limitations you should outline such as impact on systems, and ensuring backups are available and the disaster recovery plan is intact
- list key logistical considerations such as testing tools, personnel, and test schedules
- describe incident handling best practices such as law enforcement contact, sensitive data/privacy, and encryption
- describe best practices you should outline in the event that testing is successful or unsuccessful
- outline best practices to follow or consider when in possession of a company's data, such as encryption and data destruction
- describe elements that should be included in a final report such as actions taken, problems, and findings
- describe warranty, limitation of liability, and indemnification considerations to include when outlining the intent of testing activities, as well as and any liability concerns
- describe how to ensure proper authority has been granted to commence any testing, such as obtaining signatures from key stakeholders

Security Architect: Ethical Hacking Best Practices

Objectives

- provide an overview of the importance of ethical hacking in today's world
- list different types of ethical hacking such as web application, system hacking, web server, wireless, and social engineering
- list different types of real-world hackers such as white hat, black hat, and grey hat
- list benefits of ethical hacking such as discovering vulnerabilities and exploits, saving money, and better uptime
- describe how to outline the rules of engagement prior to performing an ethical hacking exercise
- describe how proactive ethical hacking can build better overall security through vulnerability assessments
- list common ethical hacking tools such as Nmap, Wireshark, Metasploit, and Kali Linux
- conduct a network scan using Nmap
- recognize how to respond to and manage incidents
- recognize the importance of using templates or checklists prior to and during a penetration test
- recognize best practices when testing uncovers exploits or vulnerabilities
- recognize legal considerations when performing an ethical hacking exercise

Intelligent Orchestration: Automating Security Incident Processing

Objectives

- identify security solutions that align with business objectives
- plan how security can be implemented with DevOps
- identify the relevance of security baselines, compliance reports, and regulatory compliance
- recall common security tools and techniques
- recognize the need for proactive security incident planning
- identify security incident response processes that could be automated
- differentiate between automation and orchestration solutions in IT
- describe how SIEM allows for centralized security event monitoring
- recognize the need for automated security incident triage and response
- plan the automation of security triage
- recall how playbooks create a workflow that enables automated security incident responses
- describe how machine learning can be used to identify potential security incidents

Security Program Regulatory Integration

Objectives

- establish the importance of building regulatory compliance into your company's IT security program
- describe PII and PHI
- recall PCI security requirements
- recognize how HIPAA protects medical information
- recall how GDPR protects European Union citizen data
- recall how GLBA applies to financial institutions
- identify how FISMA strives to protect sensitive U.S. government information
- recognize NIST security standards
- recognize ISO security standards
- recall how SOX requires organizational financial transparency

Data Security Breach Notification Process

Objectives

- identify the sections of the data breach response plan and why it is important to have one
- identify the best practice for creating a data privacy breach plan and notifying stakeholders
- identify stakeholders that need to be notified during a security breach incident and best practices for notifying them
- identify common types of security data breaches and how the notification process is different for each type
- discuss the Digital Privacy Act and breach response obligations and focus areas for the compliance plan
- discuss the General Data Protection Regulation breach guidelines and stakeholder response obligations
- discuss the HIPAA breach guidelines and stakeholder response obligations
- discuss the Gramm Leach Bliley Act breach guidelines and stakeholder response obligations
- identify the individuals who need to be notified during a HIPAA data breach violation
- recognize the consequences of failing to comply with data breach notification regulations when a data breach occurs
- identify acceptable methods for notifying affected parties of a data security breach
- recognize the legal and communication risks when notifying stakeholders of a data security breach

Security Incident Triage

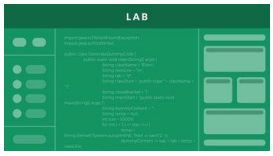
Objectives

- describe the concepts of security triage and strategies to implement triage
- describe the tools used in security triage
- describe automation techniques in security triage
- describe common tips and rules of thumb for security triage
- describe the importance of communication and stakeholder management in security triage
- describe approaches to detecting anomalies and handling them with security triage
- describe common protocol anomalies that require triage
- describe monitoring for incidents in security triage
- analyze SSH activity and describe security events to look for
- analyze DNS activity and describe security events to look for
- analyze HTTPS activity and describe security events to look for
- analyze system log activity and describe security events to look for

Unified Security: Playbook Approach to Security

Objectives

- describe the use of automation to improve consistency for security practices
- describe various approaches to security through playbooks
- describe the important elements needed in a security playbook
- describe the transition to playbooks and services in the cloud
- describe the goals and measures for success in using security playbooks
- describe some of the challenges in implementing security playbooks
- describe the concepts and features implemented in typical playbook tools
- install Ansible and remotely execute commands on a managed host
- execute a simple Ansible playbook
- configure the iptables firewall using an Ansible playbook
- configure an IPS to protect a system with an Ansible playbook
- configure unattended upgrades with an Ansible playbook to keep a system up to date



Security Architect

Objectives

- Practice Security Architect tasks such as implementing testing best practices, executing Ansible playbooks, automating upgrades with playbooks, and analyzing SSH activity. Then, test your skills by answering assessment questions after examining security data breach categories, applying NIST standards on encryption, working with ethical hacking tools and applying mitigation tools and techniques.

Final Exam: Security Architect

Objectives

- analyze DNS activity and describe security events to look for
- analyze system log activity and describe security events to look for
- compare ethical hacking tools such as Nmap, Wireshark, Metasploit, and Kali Linux
- compare the relevance of security baselines, compliance reports, and regulatory compliance
- configure an IPS to protect a system with an Ansible playbook
- configure unattended upgrades with an Ansible playbook to keep a system up to date
- describe approaches to detecting anomalies and handling them with security triage
- describe automation techniques in security triage
- describe best practices you should outline in the event that testing is successful or unsuccessful
- describe common protocol anomalies that require triage
- describe common risks and limitations you should outline such as impact on systems, and ensuring backups are available and the disaster recovery plan is intact
- describe common tips and rules of thumb for security triage
- describe elements that should be included in a final report such as actions taken, problems, and findings
- describe how proactive ethical hacking can build better overall security through vulnerability assessments
- describe how SIEM allows for centralized security event monitoring
- describe how to ensure proper authority has been granted to commence any testing, such as obtaining signatures from key stakeholders
- describe of the benefits of having a easy reference checklist or templates prepared when defining RoE
- describe PII and PHI
- describe some of the challenges in implementing security playbooks
- describe the concepts of security triage and strategies to implement triage
- describe the importance of communication and stakeholder management in security triage
- describe the important elements needed in a security playbook
- describe the tools used in security triage
- describe the transition to playbooks and services in the cloud
- describe the use of automation to improve consistency for security practices
- describe various approaches to security through playbooks
- describe warranty, limitation of liability, and indemnification considerations to include when outlining the intent of testing activities, as well as and any liability concerns
- discuss the Digital Privacy Act and breach response obligations and focus areas for the compliance plan
- discuss the General Data Protection Regulation breach guidelines and stakeholder response obligations
- discuss the Gramm Leach Bliley Act breach guidelines and stakeholder response obligations
- discuss the HIPAA breach guidelines and stakeholder response obligations
- execute a simple Ansible playbook
- identify common types of security data breaches and how the notification process is different for each type

- identify security solutions
- identify security solutions that align with business objectives
- identify stakeholders that need to be notified during a security breach incident and best practices for notifying them
- identify the best practice for creating a data privacy breach plan and notifying stakeholders
- identify the relevance of security baselines, compliance reports, and regulatory compliance
- identify the sections of the data breach response plan and why it is important to have one
- install Ansible and remotely execute commands on a managed host
- list common ethical hacking tools such as Nmap, Wireshark, Metasploit, and Kali Linux
- list different types of ethical hacking such as web application, system hacking, web server, wireless, and social engineering
- list different types of real-world hackers such as white hat, black hat, and grey hat
- list key logistical considerations such as testing tools, personnel, and test schedules
- plan how security can be implemented with DevOps
- plan security can be implemented with DevOps
- plan security with DevOps in mind
- provide an overview of the benefits of having a easy reference checklist or templates prepared when defining RoE
- provide an overview of the importance of ethical hacking in today's world
- recall how GDPR protects European Union citizen data
- recall how GLBA applies to financial institutions
- recall PCI security requirements
- recognize best practices when testing uncovers exploits or vulnerabilities
- recognize how HIPAA protects medical information
- recognize how to determine the appropriate scope of engagement
- recognize how to respond to and manage incidents
- recognize ISO security standards
- recognize NIST security standards
- recognize the importance of using templates or checklists prior to and during a penetration test
- recognize the need for proactive security incident planning

Business & Leadership for Security Architects

Optional

COURSE

Confronting Your Assumptions

711

COURSE

Identifying Risks in Your Organization

367

COURSE

Managing a Project to Minimize Risk and Maximiz...

466

COURSE

Taking Your Team to the Next Level with Delegation

232

COURSE

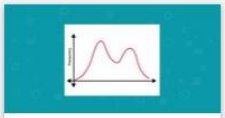
Developing and Supporting an Agile Mind-set

802

COURSE

Listening Even When it's Difficult to Listen

754



COURSE

Data Analysis and Root Cause Analysis in Six Sigma

265

COURSE

Managing for Operational Excellence

348

COURSE

Enabling Business Process Improvement

779

Productivity Tools for Security Architects

Optional

COURSE

Signing in & Setting up a Team

20

COURSE

Using the Conversation Tools

20

COURSE

Creating & Managing Projects

16

COURSE

Finding & Sharing Items

9

COURSE

Running Reports & Configuring Projects

10

COURSE

Signing In & Setting Up

25

COURSE

Using the Team Communication Tools

72

COURSE

Setting Up & Tracking Projects

22

COURSE

Managing your Project Tasks & Assets

19

COURSE

Using the Calendar Tools

19

COURSE

Using Basecamp for iOS

17

COURSE

Sign-in & Setup

14

COURSE

Communication Tools

17

COURSE

Working with Groups

12

COURSE

Creating, Finding, & Sharing Information

10

COURSE

Configuring Convo

6

COURSE

The Convo iOS App

11

COURSE

Sign-in & Setup

51

COURSE

Creating Teams & Boards

35

COURSE

Managing Cards

18

Productivity Tools for Security Architects cd.

COURSE

Finding & Sharing Information

18

COURSE

Setting Up

52

COURSE

Posting & Reacting to Status Updates

39

COURSE

Using Groups

13

COURSE

Collaborating & Communicating

74

COURSE

Configuring Networks

24

COURSE

Creating & Setting Up Projects

126

COURSE

Configuring & Managing Boards

88

COURSE

Planning & Working on a Software Project

64

COURSE

Reporting in Jira Software

63

COURSE

Getting to know the application

955

COURSE

Using Teams & Channels

708

COURSE

Communicating via the App

681

COURSE

Formatting, Illustrating & Reacting to Messages

520

COURSE

Creating, Finding & Organizing Files

500

COURSE

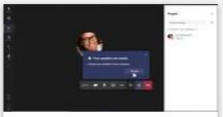
Working with Apps, Tabs & Wiki

449

COURSE

Making calls, Organizing Contacts & Using Voicemail

438



COURSE

Creating, Joining & Managing Meetings

441

Bookshelf Optional

BOOK
Computer and Cyber Security: Principles,...
8

BOOK
Cyber Security: A Practitioner's Guide
19

BOOK
Practical Information Security Management: A...
7

BOOK
Cybersecurity Essentials
15

BOOK
Cybersecurity for Dummies
18

BOOK
Information Security Policies, Procedures, and Standards:...
33

BOOK
Modern Cryptography: Applied Mathematics for...
2

BOOK
Digital Forensics
5

BOOK
Network Security and Cryptography: A Self-...
9

BOOK
Cybersecurity for Executives: A Practical Guide
4

BOOK
Beginning Ethical Hacking with Kali Linux:...
10

BOOK
Cybersecurity and Cyberwar: What Everyone Needs To...
4

BOOK
Network and System Security, Second Edition
14

BOOK
Information Security: A Practical Guide
10

BOOK
Assessing Information Security: Strategies, Tactics...
1

BOOK
Implementing Digital Forensic Readiness: From...
3

BOOK
Digital Forensics: Threatscape and Best...
5

BOOK
The Basics of Digital Forensics: The Primer for...
10

BOOK
Cryptography Made Simple
3

BOOK
The State of the Art in Intrusion Prevention and...
3

BOOK
Cybersecurity Incident Response
7

BOOK
Securing Systems: Applied Security Architecture and...
6

BOOK
Ethical Hacking and Penetration Testing Guide
60

BOOK
Introduction to Security, 10th Edition
3

FOLLOW US ON:

www.skilltech.pl

email: biuro@skilltech.pl

tel. +48 22 44 88 827

SkillTech
Technology hired for excellence