Syllabus

Cybersecurity Analytics

# Table of Contents

* [Curriculum Overview](#mhwft84g8d47)
* [Competencies](#is2u9ea0cry)
* [Learning Objectives](#9ql2kasp7u1d)

# Curriculum Overview

The Cybersecurity Analytics Bootcamp is an immersive, hands-on course designed to equip you with the skills and training you need to land a job in one of the world’s fastest growing fields. Learning will be scaffolded through seven engaging units. Additionally, you will complete four Career Simulations, or projects, throughout the bootcamp. Career Simulations are authentic, fictionalized tasks. They are realistic and messy, like those that a cyber analyst encounters on the job.

| **Unit** | **Title** | **Description** |
| --- | --- | --- |
| 1 | Cybersecurity Fundamentals | Welcome to the Cybersecurity Analytics Bootcamp! This is your first step toward a thriving career in tech, and we are happy to have you. You will learn from industry-leading experts, a powerful network of alumni, and your classmates. Building a security mindset and learning about virtualization technologies; the confidentiality, integrity, and availability (CIA) triad; and emerging security issues will prove pivotal to your success in both the bootcamp and your career. |
| 2 | Asset and Inventory Management | The Linux operating system (OS) is one of the most important items in the career of a cybersecurity professional. Such professionals use Linux distributions to do penetration testing and vulnerability assessments. And they use them to provide a forensic analysis after a security breach. Most network devices and security tools also use Linux. These tools include routers, wireless access points (WAPs), virtual private networks (VPNs), and more. Gaining a working knowledge of the Linux OS is the foundation of this bootcamp and of the rest of your career in cybersecurity. |
| Career Simulation 1 | | You have been hired as a SOC Analyst 1 at StackFull Software, a fictitious company. While on the job, you notice a configuration issue preventing you from examining logs. You will need to modify the configuration file so you can properly view logs. Then, your manager would like you to write a report that will be shared with executive leadership to describe how StackFull Software can improve the confidentiality of the configuration file so only authorized users can modify it. |
| 3 | Network Systems | Because of the ubiquity of network-connected devices, it is very important for a cybersecurity professional to understand the mechanics of how these devices are transmitting and receiving data. Today you can buy PCs, phones, televisions, and even refrigerators that are connected to the Internet. Underneath it all, these devices are still communicating using the basic principles and some of the same protocols that were first refined on ARPANET, the first network that resembled the Internet we use today. |
| 4 | Programming with Python | Python is an extremely useful programming language for cybersecurity professionals because it can perform a multitude of cybersecurity functions, including malware analysis, scanning, and penetration testing tasks. Python is often recommended as the first language people new to cybersecurity should learn. One of the main reasons to learn Python is the ease with which Python can be used to analyze and parse logs to extract important information. The other reason to learn Python is the ability to read, understand, and adapt existing scripts to meet your own needs. |
| 5 | System Administration | Windows is a widely utilized operating system for both desktop and server purposes. Many businesses rely solely on Windows to host and access their enterprise systems, while systems administrators work to keep the underlying resources functioning in the background. Additionally, for cybersecurity professionals who can confidently determine what data sets they are looking for, PowerShell provides a more efficient means of querying the system. |
| Career Simulation 2 | | You are working with the IT Security Manager to implement a new onboarding process at StackFull Software. Your first assignment is configuring a new user and their computer for a team member who just joined the company. Use your technical knowledge to complete this process. |
| 6 | Red Team | Offensive security is a proactive and adversarial approach to protecting computer systems, networks, individuals, and their data from attacks. It is a method of testing where testers target systems or applications to determine whether vulnerabilities can be exploited to compromise the application, its data, or its environment resources. Testers are given information about the targets to test in the form of a rules of engagement document. There are two ways to perform offensive security assessments: penetration testing and red teaming. |
| Career Simulation 3 | | You are shadowing the in-house offensive security team at StackFull Software. One of your clients is Fullstack Academy (FSA). FSA would like a penetration test of an isolated portion of the network.  Use your technical knowledge to complete the engagement and write a penetration test to describe your findings. |
| 7 | Blue Team | Defense security is the backbone of becoming a SOC Analyst. Through tasks such as log collection, parsing, and analysis, cybersecurity professionals can use data to respond to incidents. Additionally, Security Information and Event Management (SIEM) solutions make investigating large amounts of data easier and faster for administrators and give opportunities to create alerts on unusual behaviors. When there is a cyber incident, digital forensics is vital in figuring out the who, what, where, when, why, and how of an incident. Cybersecurity professionals need to be well-versed in incident response and the NIST Cybersecurity Framework to improve an organization’s security posture and prevent attacks. |
| Career Simulation 4 | | You choose a real-world scenario and solution related to blue or purple team concepts. |

# Competencies

The competencies in our Cybersecurity Analytics bootcamp allow you to assess your abilities, identify areas you may need to improve, learn about a defined area of expertise, and understand your future employer’s workforce needs. They were adapted from those identified from the Workforce Framework for Cybersecurity (NICE Framework) by the National Initiative for Cybersecurity Careers and Studies (NICCS).

| **Category** | **Competency** |
| --- | --- |
| Organizational | **Asset and Inventory Management**  The process of identifying, developing, operating, maintaining, upgrading, and disposing of assets. |
| **Risk Management**  The principles, methods, and tools used for risk assessment and mitigation, including assessment of failures and their consequences. Includes the oversight, evaluation, and support of the documentation, validation, assessment, and authorization processes necessary to ensure that existing and new technology systems meet organizational cybersecurity and risk requirements. |
| Technical | **Computer Languages**  Computer languages and their applications to enable a system to perform specific functions. |
| **Data Analysis and Security**  Systematically applying statistical and logical techniques to describe, illustrate, condense, summarize, and evaluate data. The synthesis and analysis of various types of data to reach a decision, make a recommendation, or to compile reports, briefings, executive summaries, and other correspondence to support organizational work, goals, and plans. It includes the methods and procedures that protect data and information systems by ensuring their confidentiality, integrity, and availability. |
| **Digital Forensics**  The application of tools and techniques used in data recovery and preservation of electronic evidence. This includes the collection, processing, preservation, analysis, and presentation of computer-related evidence in support of network vulnerability mitigation and criminal, fraud, counterintelligence, or law enforcement investigations. |
| **Incident Management**  The tactics, technologies, principles, and processes to analyze, prioritize, and handle cybersecurity incidents. |
| **Infrastructure Design**  The architecture and topology of software, hardware, and networks, including LANS, WANS, and telecommunications systems, their components and associated protocols and standards, and how they operate and integrate with one another and with associated controlling software. |
| **Mathematical Reasoning**  Solving practical problems and determining if an assertion is correct by choosing appropriately from various mathematical and statistical techniques. |
| **Network Management**  The operation, management, and maintenance of computer network and telecommunication systems and linked systems and peripherals. |
| **Vulnerabilities Assessment**  The principles, methods, and tools for assessing vulnerabilities and developing or recommending appropriate mitigation countermeasures. |
| **Encryption**  This is the cryptographic process of transforming data to ensure that it can only be read by the person who is authorized to access it. |
| **System Administration**  The installation, configuration, troubleshooting, and maintenance of computer systems to ensure their confidentiality, integrity, and availability. This includes the management of accounts, firewalls, and patches, as well as access control, passwords, and account creation and administration. |
| Professional | **Interpersonal Skills**  Developing and maintaining relationships with others to work effectively. This includes being sensitive to and inclusive of cultural diversity, race, gender, disabilities, and other individual differences, as well as considering and responding appropriately to the needs, feelings, and capabilities of customers and colleagues. Includes understanding when and how to adapt messages for different audiences, listening to others’ instructions, ideas, and intentions, attending to nonverbal cues, and responding appropriately. |
| **Problem-Solving**  Determining the accuracy and relevance of information; using sound judgment to generate and evaluate alternatives; and making well-informed, objective recommendations and decisions that consider facts, goals, constraints, and risks while perceiving the impact and implications of the decisions. This includes comprehending the meaning and identifying main ideas, noting details and facts, detecting inconsistencies, critically evaluating and analyzing the information, and applying what is learned to new situations. |
| **Writing**  This is using written language to compile information and prepare written documents. It includes citing sources and articulating thoughts and ideas clearly and effectively to persons inside and outside of the organization. |
| **Career Preparation**  This is networking, career pathways, interviews and negotiation, and job search. It includes creating personal marketing tools such as a pitch, employee profiles, and a resume. |

# Learning Objectives

Each competency is aligned with the learning objectives you will develop throughout the bootcamp. These skills will be used to assess your learning and mastery of the competencies.

| **Competency** | **Learning Objective** |
| --- | --- |
| Asset and Inventory Management | Explain how a file system is organized in an operating system. |
|
| Navigate the command line of an operating system. |
| Find, view, create, move, and delete files and directories. |
| Use tools that sort and format output and minimize root access. |
| Review and change permissions on files and directories. |
| Create, inspect, and modify user accounts and groups. |
| Investigate running services using a service and initialization manager. |
| Map MAC addresses to manufacturers. |
| Perform software asset inventory functions on Windows systems. |
| Risk Management | Identify how information security revolves around confidentiality, integrity, and availability (CIA). |
|
| Explain emerging security issues, risks, and vulnerabilities. |
| Implement and explain the implementation tiers and profiles of the NIST cybersecurity framework. |
| Explain the basic components of governance, risk and compliance. |
| Create a threat model to document security threats and make business decisions. |
| Apply patches to software to increase an organization's security posture. |
| Hash plaintext values and decrypt a message to identify a ransomware attack. |
| Deploy an intrusion detection system to analyze traffic on a network. |
| Computer Languages | Write, test, and modify scripts with conditional statements, loops, and functions to automate tasks. |
| Assign, reassign, and generate variables and concatenate data. |
| Identify and debug errors in a program. |
| Use string and list methods, including indexing and slicing, to manipulate and edit code. |
| Parse log files using a scripting language to break them down into component parts. |
| Generate system reports with PowerShell. |
| Use Splunk Processing Language (SPL) to perform search queries. |
| Data Analysis and Security | Examine SSL certificates to find data. |
| Extract and explain different types of data that can be collected for security purposes. |
| Use different capabilities and functions of Splunk to model and analyze data and statistics. |
| Create and baseline Splunk techniques and alerting functions. |
| Compress, decompress, and archive files and directories. |
| Test, improve, and verify that a monitoring script is logging the proper events. |
| Identify, analyze, and categorize sources of log data and identify log collection techniques. |
| Preserve forensic evidence and explain why it is important. |
| Digital Forensics | Mount and access data from various devices and systems. |
| Analyze packet captures with Wireshark. |
| Identify and use the tools, phases, and processes of digital forensics to investigate malicious processes. |
| Explain the components of ISO 27041-3 standards. |
| Explain anti-forensics techniques and what they do. |
| Conduct an investigation and forensics on a device. |
| Incident Management | Identify how organizations can prevent and overcome serious incidents or disasters and quickly resume normal operations within a reasonable timeframe. |
| Explore the structures in place at organizations to comply with rules and regulations. |
| Explain CVSS and research the metrics to determine the severity of an incident. |
| Explain the importance of responding quickly and creating an incident response plan. |
| Finalize an incident response plan by deploying SIEM/SOAR tools and utilizing endpoint detection and response. |
| Explain what a cyber disaster is and how organizations can recover from an incident. |
| Infrastructure Design | Use virtualization technologies to solve problems. |
| Identify and explain network components, such as peer-to-peer and client-server interactions, network devices and topologies, and the differences between WANs and LANs. |
| Explore the components and layers of the OSI model, including types of firewalls. |
| Dissect an ipv4 packet header. |
| Create filters in Wireshark to eliminate unwanted network traffic. |
| Extract credentials from FTP sessions. |
| Mathematical Reasoning | Use symbolic and octal notation to change file permissions. |
| Manipulate variables and data types using addition, subtraction, multiplication, division, and modulus. |
| Convert numbers between binary and decimal. |
| Interpret and convert netmasks to and from CIDR notation. |
| Break an IP address into octets, network IDs, and host IDs. |
| Convert between various types of encoding, such as ASCII, HTML, and Base64. |
| Network Management | Use ping and nslookup to check the connectivity of hosts and query and benchmark public DNS servers. |
| Identify the parameters needed for a modern network connection. |
| Identify and find network ports and the common services associated with them. |
| Enumerate network hosts and assess their visibility on a network. |
| Probe unknown ports to determine the services running behind them. |
| Analyze and capture network traffic to recognize any possible malicious activity. |
| Assess and explain the use of VLANs and VPNs. |
| Vulnerabilities Assessment | Read and interpret firewall logs to find suspicious traffic. |
| Use and explain how the MITRE ATT&CK framework allows security teams to test their defenses against known adversarial techniques. |
| Perform passive reconnaissance to get a better understanding of an external footprint. |
| Exhibit ethical hacking protocols to evaluate the security of and identify vulnerabilities in target systems, networks, or system infrastructure. |
| Perform vulnerability scanning using a variety of tools. |
| Explain the purpose of OWASP and the resources they provide. |
| Use and configure tools to perform offensive security techniques. |
| Exploit a web application to expose client-side vulnerabilities. |
| Exploit an SQL injection and command injection vulnerability. |
| Explain how file inclusion vulnerabilities can be remediated. |
| Identify web server vulnerabilities that can lead to compromise. |
| Explain the purpose of social engineering and how to avoid it. |
| Establish a reverse shell on a Linux server. |
| Use modules within Metasploit and explain their purpose. |
| Establish Meterpreter sessions and explain how to use them. |
| Create malicious payloads with MSFVenom. |
| Extract SAM NTLM hashes and explain their value. |
| Look for privilege escalation opportunities through lateral movement. |
| Apply the pass-the-hash technique to take advantage of flaws in NTLM authentication. |
| Explain how exploitation is performed within modern computing environments. |
| Encryption | Use the command line to create, edit, and transfer files from one machine to another. |
| Use a secure shell to connect to a remote machine. |
| Differentiate between encoding and encryption. |
| Use historical ciphers and modern symmetric key encryption to encrypt and decrypt messages and files. |
| Generate self-signed certificates and Certificate Signing Requests. |
| Decrypt an SSL-encrypted packet. |
| System Administration | Install and uninstall packages on an operating system. |
| Use automation tools to perform maintenance tasks. |
| Explain the differences, pros, and cons between host-based and network-based firewalls. |
| Create firewall rules to block and accept traffic using UFW and IPtables. |
| Explain how defense in depth is used to protect networks. |
| Identify the major Windows release versions. |
| Explain security concerns for Windows operating systems. |
| Relate knowledge of Linux systems to Windows environments. |
| Install and remove Windows applications. |
| Analyze system resource usage by application. |
| Manage startup and default applications on Windows systems. |
| Centrally manage Windows security settings through Group policies. |
| Manage access to Windows system resources through Active Directory security groups. |
| Control account settings and passwords for domain user accounts in Active Directory. |
| Identify Windows administrative tools. |
| Manage firewall rules on Windows systems. |
| Analyze system health through event log data. |
| Interpersonal Skills | Develop constructive and cooperative working relationships. |
| Identify problems using a group approach and develop solutions based on a group consensus. |
| Apply active listening skills using reflection, restatement, questioning, and clarification. |
| Convey information clearly, correctly, and succinctly. |
| Respond appropriately to positive and constructive feedback. |
| Reach agreements that promote mutual goals and interests. |
| Problem-Solving | Observe and evaluate the outcomes of implementing solutions to assess the need for alternative approaches and to identify lessons learned. |
| Recall previously learned information that is relevant to the problem. |
| Use a security mindset to identify assets and security goals, potential adversaries and threats, and potential weaknesses. |
| Have sufficient inductive and deductive reasoning abilities to successfully do the job. |
| Use man pages to learn about unfamiliar commands and/or switches. |
| Search for online information and interact with websites and web applications. |
| Critically review, analyze, synthesize, compare, and interpret information. |
| Research measures that have been taken to prevent the use of Mimikatz on Windows systems. |
| Writing | Communicate thoughts, ideas, and information, which might include technical material, in a logical, organized, and coherent manner. |
| Tailor the content to the appropriate audience and purpose. |
| Explain the importance of reporting and documentation in forensics. |
| Analyze penetration reports and explain their purpose. |
| Create a recovery playbook to respond to an incident. |
| Explain the significance of using a postmortem at the end of an incident. |
| Career Preparation | Identify the day-to-day tasks and responsibilities of a SOC analyst. |
| Explain the SOC Analyst's role in business continuity planning and continuity of operations. |
| Build a technical resume. |
| Optimize a LinkedIn profile. |
| Network within the industry. |
| Practice technical and behavioral interview techniques. |
| Utilize tips and tricks to maximize the job search process. |
| Craft cover letters to stand out from applicants. |