Arizona State University

ARIZONA STATE UNIVERSITY

CYBERSECURITY BOOT CAMP

CURRICULUM OVERVIEW

“Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace.” - U.S. Department of Homeland Security

The frequency of data and security breaches in the news grows almost daily, and as a result, there is tremendous job demand for cybersecurity professionals. It’s important now, more than ever, to have trained, skilled professionals securing our data and personal information.

The **24-week Cybersecurity Boot Camp** is a challenging, part-time program that takes a multidisciplinary approach to attain proficiency in information technology, networking and modern information security.

Throughout the course, you’ll gain experience with a host of popular tools such as Wireshark, Kali Linux, Metasploit, Nessus and more. In addition, you will learn skills applicable to certifications such as the CompTIA Security+ and Certified Ethical Hacker (CEH), which can greatly enhance desirability and employability in today’s job market. You’ll also learn methods, techniques and best practices for convincingly conveying the severity of the risks facing an organization’s security posture.

IS THIS PROGRAM RIGHT FOR YOU?

The Cybersecurity Boot Camp is for anyone who needs to know how to keep data safe from prying eyes. Enrolling can help you achieve your goals if you say “yes” to any of the following:

> You’re currently a technical professional, such as a web developer, network administrator or help desk technician, who is looking to move into cybersecurity.

> You’re a manager in a company whose revenue depends on the confidentiality, availability and integrity of client data.

> You’re a manager dedicated to managing growing cyber risks to your organization.

> You’re a tech enthusiast looking to get your foot in the door in the world of networking and security.

THE SKILLS YOU'LL GAIN

You'll complete the program with a foundation in cybersecurity and networking, including:*

Networking

- Packet analysis
- Wireshark

Systems

- Windows and Linux administration techniques
- Windows and Linux hardening

Cybersecurity

- Cloud security
- Cryptography
- Identity and access management
- Risk management
- Secure network design and architecture
- Vulnerability assessment

Ethical hacking and penetration

- Burp Suite
- Hashcat
- Kali Linux
- Metasploit
- Web vulnerabilities and security

Cybersecurity careers

- Digital forensics methods
- Penetration testing
- Security operations and analytics
- Vulnerability assessment

Programming and scripting

- Bash scripting

*The material covered in this course is subject to change due to market demand.

BUILDING ON THE BASICS

Achieving your goals in cybersecurity requires not only deep security knowledge, but also experience with the application of that knowledge.

Our curriculum is designed to give you both the knowledge you need to move toward the cybersecurity industry and ample experience applying that knowledge to real-world problems. Throughout the program, you'll learn tools and technologies vetted by current practitioners and learn skills applicable to certifications expected of all serious security professionals.

As part of our program, we'll provide you with two weeks of certification test prep for the Security+ and CEH exams, one year access to CompTIA's CertMaster online test prep platform for the Security+ exam and at the end of the course, a free voucher valid for one year to take the Security+ exam.

REAL WORLD APPLICATION, REAL JOBS

Those who complete the Cybersecurity Boot Camp will learn critical skills relevant to the following careers:

- Cyber network defender
- Cybersecurity analyst
- Cybersecurity operations specialist
- Digital forensics examiner
- Incident response analyst
- Information assurance specialist
- IT auditor
- Network or system security administrator
- SOC analyst
- Systems security analyst
- Vulnerability assessment analyst

WHAT YOU WILL LEARN

By the time you complete the program, you can expect to be able to:

- Advise on cybersecurity best practices and risk management strategies.
- Analyze packet traffic flowing over a network in order to better troubleshoot issues such as poor network performance.
- Conduct vulnerability assessments using tools like Metasploit to profile an application for vulnerabilities and then exploit those vulnerabilities.
- Configure machines on a virtual network, deploy them to the cloud and investigate cloud security risks.
- Develop best practices in implementing security strategy policies across an organization.
- Gain insight into the important best practices around password selection and storage to crack into (mock!) user accounts.
- Identify suspicious patterns of user behavior to identify bots, intruders and other malicious actors.
- Implement access control policies as an additional layer of security over an organization's private data.
- Perform administrative and security tasks to Windows and Linux operating systems.
- Perform network, system and web penetration testing activities.
- Understand and implement network theory.
- Understand cybersecurity threats, actors and methods.
- Write Bash scripts to automate security and operating systems tasks.

COURSE STRUCTURE

The program will consist of both insightful lectures and individual and group exercises, meant to reinforce the tools and ideas introduced in class. The skills covered in the course are also applicable to in-demand certifications, such as Security+ and CEH. Better yet, you'll learn how to apply these technologies in the real world.

DISCUSSION

Industry professionals lead lectures and class discussions on the background, history and applications of a new technology or concept.

CERTIFICATION KNOWLEDGE BUILDING

Gain valuable experience and learn skills applicable to top certifications in the cybersecurity industry, including CEH and Security+ certifications. During and after the course, use the CompTIA CertMaster companion tool to study for the Security+ exam and take the Security+ exam with your free voucher.

HANDS-ON EXERCISES

Throughout the course, you'll apply the skills you've learned in labs and in other practical scenarios. By the completion of the program, these assignments will give you a vast array of first-hand cybersecurity and networking experience.

WE'RE HERE TO HELP

As you move up the learning curve, you're likely to have questions around some of the concepts covered in class. We're here to help — through in-person and virtual office hours, as well as a dedicated #slack channel where you can get assistance from instructors, support staff and your fellow learners. In addition to learning cybersecurity and network security, you'll have access to career services that will help you prepare for technical roles after after completing the boot camp, such as:

Career Content and Practice Sessions

Database of Customizable Tools and Templates

- Creating an elevator pitch
- Developing a bio
- GitHub best practices
- Guidelines to building a portfolio
- Multiple technical resume templates

Online Career Events with Industry Professional

Soft Skills Training

One-on-One Career Coaching

MEETING EMPLOYER EXPECTATIONS

It's a fact: companies care about what you can do, not what you say you can do. For that reason, our curriculum teaches you how to apply what you've learned to simulated and lab based environments.

The curriculum emphasizes in-depth exploratory labs, ranging from conducting intrusion detection to attacking and securing a vulnerable web application. Individuals will use personal laptops to practice the skills and abilities included in this course.

SAMPLE PROJECTS

Network analysis and troubleshooting

A substantial part of modern cybersecurity requires monitoring and analyzing the data flowing over networks. Familiarity with patterns at the packet level is essential for both basic troubleshooting and more intensive tasks. In this activity, you'll monitor the packets being transmitted over a network to gain insight into problems such as dropped packets and explore other patterns apparent only at the packet-level.

Skills Needed

- Familiarity with TCP/IP, HTTP and other protocols
- Packet and protocol analysis
- Tapping into networks
- Wireshark

Objectives

- Articulate the relationships between different network protocols such as TCP/IP and HTTP.
- Identify suspicious patterns of network activity to hone in on malicious users.
- Use Wireshark to analyze packets and identify transmission patterns associated with poor network performance.

Network security monitoring and logging

The modern IT landscape is defined by the sheer amount of data it's responsible for. There is far more data than can be examined directly, but it all must be protected. Monitoring and logging can help security specialists identify suspicious trends in data, thereby identifying potential incidents and informing future intrusion detection efforts. You'll analyze log data, identify and characterize intrusion evident from the data, and perform incident response.

Skills Needed

- Network monitoring
- Packet analysis
- SIEMs configuration

Objectives

- Configure logging and monitoring systems and periodically collect and analyze data they capture

Attacking a web application

The modern web is one of the most popular places for people to spend their time and store their data. Because of this popularity, websites are common avenues of attack. In this activity, you'll explore, attack and profile a vulnerable website with tools like Burp Suite. Then, you'll summarize the site's vulnerabilities with policy recommendations for managers and leadership.

Skills Needed

- HTTP
- JavaScript
- SQL
- XSS
- XSRF
- Familiarity with cookie-based authentication

Objectives

- Distill the technical results of a penetration test into policy recommendations bound for management.
- Explore common web application exploits — such as SQL injection XSS and XSS — from an offensive perspective, to better understand how hostile parties analyze and assault their targets.
- Explore the various available attack vectors and insertion points relevant to web applications.
- Use Burp Suite to automate web-app vulnerability scanning.

Cracking and securing password-Protected Data

Most of the web's user-provided data is secured by little more than a password. Since users often reuse passwords between accounts and/or use easily guessed passwords, the onus is on the cybersecurity professional to enforce best practices around password creation, storage and database management. In this activity, you'll gain experience with password cracking strategies and write a report suggesting technical, governance and UX policies effective for minimizing vulnerability to such attacks.

Skills Needed

- Hashing algorithms
- Password storage best practices
- Dictionary attacks
- Brute-force attacks
- Rainbow Tables
- Hashcat

Objectives

- Articulate policy recommendations for managers to reduce the surface area of password-based attacks.
- Articulate the relative strengths and weaknesses of different password cracking techniques.
- Guess a user's password via both dictionary and brute-force attacks.

PROJECTS continued...

Penetration testing

Ultimately, the best indication of a system's security is how well it holds up against an actual attack. Penetration testing is the cybersecurity professional's opportunity to don the proverbial Black Hat and probe pre-made systems for vulnerabilities using tools like Metasploit. You'll conclude your exploration of these systems with recommendations for mitigating any vulnerabilities that may have been uncovered during the pen test.

Skills Needed

- Ability to perform active and passive reconnaissance
- Ability to perform Open Source intelligence gathering
- Kali Linux
- Metasploit
- Network intrusion
- Vulnerability scanners

Objectives

- Develop familiarity with the main phases of a penetration test, including reconnaissance, scanning, access acquisition, access maintenance, and clearing tracks/erasing evidence.
- Translate the technical results of the penetration test into a document with actionable policy resources for management.
- Use Metasploit to probe an application for vulnerabilities and then attack the application via a series of pertinent, Metasploit-provided exploits.

Digital forensics

Users often delete data from devices that they would prefer others not to see — but, sometimes, organizations find themselves in need of the very information that was deleted. You'll receive an introduction to digital forensics investigation and response. Topics include legal compliance, chain of custody procedures, procedures for investigating computer and cybercrime, and concepts for collecting, analyzing, recovering and preserving forensic evidence.

Skills Needed

- Digital forensics
- Electronic discovery
- Data recovery

Objectives

- Describe the steps in performing digital forensics from the initial recognition of an incident through the steps of evidence gathering, preservation and analysis, through the completion of legal proceedings.
- Discuss the rules, laws, policies and procedures that affect digital forensics.
- Use one or more common tools such as FTK, Sleuthkit, Kali Linux, Volatility or SNORT.

COURSE CURRICULUM BY MODULE

Module	Description	What You'll Learn
Learning Module: Security Fundamentals	In this module, you'll learn to think like a cybersecurity professional by assessing threats and mitigating risks. You'll also look at security from an organizational perspective as you dive into governance, risk and compliance. You'll learn how security controls impact an organization and its employees. This will enable you to communicate with non-security professionals, work with stakeholders outside of the security space and understand how teams interact in an organization.	» Business continuity planning » CIA triad » Compliance » Disaster recovery » Governance » Risk analysis and risk mitigation
Learning Module: Systems Administration	You'll cover both Linux and Windows systems administration. You'll gain hands-on experience working with the command line and bash commands that are prominent in IT roles. You'll configure and audit servers, as well as harden and secure them from malicious attacks.	» Active directory » Bash scripting and programming » Kerberos » Linux server configuration » Logging » Tar, Cron and Cronjobs » Windows server configuration
Learning Module: Networks and Network Security	You'll dive into network configuration, design, protocols and data communication. You'll study cryptography, network security, cloud security and virtualization.	» Cloud security and virtualization » Cryptography and encryption » Email security » Network architecture, operations and security » Port scanning » Wireless security » Wireshark and traffic analysis
Learning Module: Defensive Security	You'll dive into SIEMs and network security monitoring. You'll cover the incident response framework and practice responding to different breaches and attacks. You'll also cover digital forensics and how to recover deleted data as part of preparing evidence for a legal case.	» Data extraction and recovery » Forensics » Incident response » Monitoring and logging » Splunk
Learning Module: Offensive Security	You'll gain a thorough understanding of web applications, databases, and the vulnerabilities and hardening associated with them. You'll dive into penetration testing using tools like Metasploit to attack and compromise networks and servers.	» Burp Suite » Execution standard » File inclusion and command injection vulnerabilities » Metasploit » Penetration testing » Pivoting networks » Searchsploit and Metasploit Zenmap » SQL injection » Webshells » XSS vulnerabilities and payloads
Learning Module: Test Prep and Final Projects	You'll focus on certification prep for Security+ and CEH exams and conclude the program with a final group project.	» Security+ » CEH