NORTHWESTERN CYBERSECURITY BOOT CAMP

CYBERSECURITY

CURRICULUM OVERVIEW

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

Big data needs big protection. That's because 90 percent of the world's data has been created in just the last two years[1]. As computer networks grow, so too does the quantity of vulnerable information.

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

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

1. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WRL12345USEN

Is This Program Right For You?

The Northwestern 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 are currently a technical professional, such as a web developer, network administrator, or help desk technician, who wants to better understand how to keep data secure.

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

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

> You are looking to move into cybersecurity from an already technical field, such as systems administration.

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

The Skills You'll Gain

You will complete the program with a foundation in Cybersecurity and Networking, including*:

Networking

- Packet Analysis
- Wireshark
- Router and switch configuration
- LAN, WAN networking
- Subnetting

Systems

- Windows and Linux Administration Techniques
- Windows and Linux Hardening
- Web Technology Architecture and Security

Cybersecurity

- Secure network design and architecture
- Risk Management
- Cryptography
- Vulnerability Assessment
- Identity and Access Management

Ethical Hacking and Penetration

- Kali Linux
- Metasploit
- Hashcat
- Burp Suite

Cybersecurity Careers

- Digital Forensics Methods
- Cyber Threat Intelligence
- Penetration Testing
- Vulnerability Assessment
- Security Operations and Analytics

Programming and Scripting

- Python Programming
- Bash Scripting

*The material covered in this program 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 will learn tools and technologies vetted by current practitioners, and learn skills applicable to three certifications expected of all serious security professionals.

Real World Application, Real Jobs

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

- Cyber Network Defender
- Cybersecurity Analyst
- Vulnerability Assessment Analyst
- Cybersecurity Operations Specialist
- Network or System Security Administrator
- Systems Security Analyst
- Information Assurance Specialist
- Penetration Tester
- Digital Forensics Examiner
- Incident Response Analyst
- IT Auditor
- Secure Coding Specialist

What You Will Learn

When you complete the program, you can expect to be able to:

- Successfully design and configure networks using Cisco IOS
- Analyze packet traffic flowing over a network in order to better troubleshoot issues such as poor network performance
- Understand and implement network theory
- Analyze malware to identify its origin and purpose, and determine methods for uninstalling it
- Perform administrative and security tasks to Windows and Linux Operating Systems
- Understand cybersecurity threats, actors, and methods
- Conduct vulnerability assessments using tools like Metasploit to profile an application for vulnerabilities, and then exploit those vulnerabilities
- Perform network, system, and web penetration testing activities
- Identify suspicious patterns of user behavior to identify bots, intruders, and other malicious actors
- Perform Python programming along with Bash and scripting
- Gain insight into the important best practices around password selection and storage to crack into (mock!) user accounts
- Advise on cybersecurity best practices and risk management strategies
- Implement access control policies as an additional layer of security over an organization's private data
- Develop best practices in implementing security strategy policies across an organization

Course Structure

Over the course of 24 weeks, you'll attend insightful lectures and take part in a variety of individual and group exercises, meant to reinforce the tools and ideas introduced in class. While this boot camp program is not a certification preparation program, every few weeks, a part of your studies will focus on a a set of skills applicable to in-demand certifications. 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: The Network+, Security+, and CISSP Certifications.

HANDS-ON EXERCISES

Throughout the course, you will 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 students. All work is done via Github, so you can create issues directly on your own projects for instructors to assist you in a truly asynchronous fashion. In addition to learning cybersecurity and network security, you will have access to career services that will help you prepare for technical roles after program completion such as:

Career Content and Practice Sessions

Database of Customizable Tools and Templates

- Multiple Technical Resume Templates
- Github Best Practices
- Guidelines To Building a Portfolio
- Creating an Elevator Pitch
- Developing a Bio

Online Career Events With Industry Professionals

High Impact Career Events

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. Students will use personal laptops to practice the skills and abilities included in this program.

Sample Projects

Network Analysis & 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 will 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

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

Objectives

- Use Wireshark to analyze packets and identify transmission patterns associated with poor network performance
- 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

Data Driven Security Analysis: Identifying Suspicious Login/ Request Patterns

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. Data analysis can help security specialists identify suspicious trends in data, thereby identifying potential incidents and informing future intrusion detection efforts. In this activity, you'll search for patterns in large quantities of log data, ultimately identifying and characterizing intrusions evident from the data, and developing protocols for detection of such intrusions in the future.

Skills Needed

- Network monitoring
- Packet analysis
- Threat intelligence
- Database management
- Machine learning

Objectives

- Use common data analysis tools to analyze large amounts of log data for telltale patterns of cyberattacks
- Deploy powerful machine learning techniques to profile previously unknown, suspicious patterns of activity, so they can be prevented and identified later
- Configure logging and monitoring systems and periodically collect and analyze data they capture

Sample Projects Continued...

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 will explore, attack, and profile a vulnerable website with tools like Burp Suite. Then, you will 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

- 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
- Use Burp Suite to automate web-app vulnerability scanning
- Explore the various available attack vectors and insertion points relevant to web applications
- Distill the technical results of a penetration test into policy recommendations bound for management

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 use 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

Objectives

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

Sample 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 will conclude your exploration of these systems with recommendations for mitigating any vulnerabilities that may have been uncovered during the pen test.

Skills Needed

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

Objectives

- Use Metasploit to probe an application for vulnerabilities and then attack the application via a series of pertinent, Metasploit-provided exploits
- Develop familiarity with the main phases of a penetration test, including Reconnaissance, Scanning, Access Acquisition, Access Maintenance, and Clearing Tracks/ErasinEvidence
- Translate the technical results of the penetration test into a document with actionable policy resources for management

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. Deleted data is often recoverable using the techniques of modern digital forensics, which you will practice in this activity to recover hidden, encrypted, and deleted files from a provided disk drive image.

Skills Needed

- Python
- Digital forensics
- Electronic discovery
- Data recovery
- Encryption and decryption

Objectives

- Use Python and digital forensics tools to recover deleted files from a hard drive
- Discover hidden and otherwise private information on a hard drive using various modern data-discovery techniques
- Gain access to encrypted files and folders using popular decryption modules and techniques

Course Curriculum By Module

Module	Description	What You'll Learn
Learning Module: Intro to Computing, Networking, and Programming	Students begin with an introduction to fundamental concepts such as Network Topologies, Python Scripting, Cryptography, Encryption, and more.	» Command Line » Shell Scripting » Python Programming » Cryptography and Encryption
Learning Module: Networks and Network+ Skill Building	Dive into network configuration, design, and hardware as well as protocols and data communication. At the end of this section, students will learn skills applicable to the Network+ certification exam.	» Network Architecture » Network Operations » Network Security » Troubleshooting » Industrial Standards, Practices, and Network Theory » Wireshark and Traffic Analysis » Packet Tracer and Packet Analysis
Learning Module: Offensive Security	Students gain a thorough understanding of web applications, databases, operating systems, and the vulnerabilities and hardening associated with them. They utilize their newfound knowledge to become familiar with tools like Metasploit and Exploit DB.	» Web Application Architecture » HTML/CSS/JavaScript » Databases and APIs » Windows OS » Linux OS » Kali Linux » Metasploit » Exploit DB » Burpsuite » Pentesting Frameworks
Learning Module: Defensive Security	Students will cover topics including risk analysis, policy, governance, and auditing. They will build out a sample enterprise security strategy for an organization. At the end of this section, students will learn skills applicable to the Security+ certification exam.	» SIEMS » Incident Response » Business Continuity Planning (BCP) » Threat Modeling/ Vulnerability Assessments » Compliance/ Policy/ Auditing » Enterprise Security Strategy
Learning Module: New and Future Technologies	Students will explore technologies such as Blockchain and Cloud Security. They will participate in classroom wide offensive/defensive security exercises.	» Amazon Web Services » Connecting to APIs » Data setup and monitoring