The Cyber Academy

The Cyber Academy is a progression of three courses designed to impart a strong foundation of offensive and defensive information security skills in 34 weeks of full-time study. Development of the 100% project-based, learn-by-doing program was funded, in part, by the Department of Defense (under agreement C5-16-0023), and the curriculum was designed in conjunction with DoD-selected experts.

Students work through 20 tasks (spending 1-2 weeks per task) online in a private cloud environment with help, advice, and feedback from a knowledgeable mentor and extensive online learning resources. The tasks are embedded in the realistic, but fictional, context of work as an entry-level employee of a government cyber operations agency.

In addition to the task-based curriculum, an implicit curriculum runs throughout the program via which students learn and practice the cognitive skills essential for success in all areas of information security. These include:

- Understanding complex, novel problems
- Effectively researching solutions
- Designing and testing solutions
- Making evidence-based decisions
- Communicating effectively with stakeholders
- Self-directed learning

Given the constantly changing nature of threats and challenges, these skills are arguably of equal or greater importance than the task-specific skills students learn. Students must pass each successive course to be eligible to continue.

Immediate Immersion 2021

Course Overview

The field of Information Security deals with the ever-growing volume of threats to businesses and government entities. While hardening computer and network infrastructure with patching, firewalls, and intrusion protection systems is important, those tools will probably never stop the threats completely. Adept individuals are needed to monitor the security tools, watching for threats that bypass the automated protections. The analysts in the Security Operations Center (SOC) are the last line of defense. The SOC tries to detect and remediate threats that make it past the protections. The SOC analyst role has traditionally been an entry-level position, but a great deal of knowledge and skills are necessary for success.

The success of a SOC is difficult to measure since attackers and attacks never stand still: Everything is a moving target. Success is typically measured by reducing organizational risk by detecting, remediating, and automatically preventing future instances of known attacks. In reality, this is far beyond the capability of most SOCs today. And to make matters even worse, SOC analysts rarely have the tools, tactics, procedures, or training to deal with all the threats that can affect organizations today. Nobody wants to admit how difficult the struggle is, which means it's difficult to even get the conversation going.

Qualifications for entry-level SOC analysts are problematic because most applicants have little if any training in information security. Realistically, an entry-level SOC analyst can only be expected to be passionate about security and have some networking background – which happen to be the prerequisites for this course.

In this six-week "on-ramp" course, you will be working at a managed security service provider that provides outsourced information security services to a range of clients. You will investigate alerts by analyzing network traffic. We have designed this course to provide you with initial experience analyzing and understanding what alerts mean through three realistic hands-on tasks. (Future courses will deal with log analysis, malware analysis, digital forensics, and incident response.)

Immediate Immersion 2021 includes the following tasks:

1. Exploit a website and fix its vulnerabilities

    Students learn to think like attackers. They investigate a defense contractor's website surreptitiously, fix a vulnerability, and remove malware. To accomplish this, they must use an LFI exploit uncovered by human intelligence to access to the webserver themselves and then crack the

webmaster's encrypted password, so they can remove the malware and patch the vulnerability that left the system open to attack.

OBJECTIVE: Think like an attacker
OBJECTIVE: Exploit a website using a local file inclusion vulnerability
OBECTIVE: Crack a password
OBJECTIVE: Determine if a website has embedded malware
OBJECTIVE: Conduct online technical research
OBJECTIVE: Patch the code of a website to eliminate a local file inclusion vulnerability

2. Investigate an insider threat

You receive a report that an employee had unusual text on his screen which didn't seem to be work related. The company's security team captured a recording of that employee's network traffic from the time of the report. Your task is to use two traffic analysis tools to determine what the employee was doing. Was his activity benign—or was this evidence of an insider attack?

OBJECTIVE: Conduct an investigation of a cybersecurity incident
OBJECTIVE: Analyze network traffic using NetworkMiner
OBJECTIVE: Analyze network traffic using Wireshark

3. Analyze suspicious network traffic

You will analyze suspicious network traffic moving in and out of a US military aide's personal laptop. Using packet capture (PCAP) files, you will determine if it was infected by malware and if so what malware and how the infection occurred.

OBJECTIVE: Analyze suspicious network traffic in a PCAP using Snort and Wireshark.
OBJECTIVE: Recognize a cushion redirect in network traffic.
OBJECTIVE: Recognize the identifying features of a specific exploit kit.
OBJECTIVE: Recognize a malware payload being transferred to a targeted host.

Who Should Enroll

Students who wish to explore a career in cybersecurity to determine if it is right for them. The ideal student is intensely curious, unwilling to give up on a problem no matter how difficult it is, and predisposed towards self-directed learning.

Learning Outcomes

Students will learn will learn and practice key SOC analyst skills including:

- Conducting online technical and open source intelligence research
- Analyzing and verifying Snort alerts
- Distinguishing between true and false positive alerts
- Analyzing packet capture (PCAP) files
- Analyzing suspicious user behavior
- Identifying vulnerabilities based on vulnerability scans
- Distinguishing between attacks and vulnerability scans
- Identifying open ports using scanners such as NMAP, Nikto, and WPScan
- Identifying OS/Application fingerprints
- Analyzing attacks that employ exploit kits.

Prerequisites

1. Only basic computer skills are required, but basic knowledge of computer networks, protocols, and the fundamentals of operating systems is strongly recommended.

2. Taking and passing a free pre-assessment is REQUIRED before students are allowed to register for this program. If students have an IT background, they can ask to be exempted from this requirement. For more information about the pre-assessment, please click here.

Additional Info

Textbook: Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems, 3rd Edition by Chris Sanders is highly recommended for this course (ISBN-13: 978-1593278021). It can be ordered from nostarch.com (purchases made from nostarch.com include a full-text searchable ebook version of the text, available for download immediately after purchase) (Links to many additional online learning resources are provided within the course, specific to each task.)

Students must successfully complete *Immediate Immersion 2021* to be permitted to enroll in the next course in this program, The Cyber Academy: Defense. Success will be assessed by a student's mentors whose decision is final.

The Cyber Academy: Defense

Course Overview

The *Cyber Academy: Defense* builds on the defensive skills and experience students gained in *Cyber Attack and Defense: Immediate Immersion 2020*. The course is designed to impart a strong foundation of defensive information security skills in 13 weeks of study at 25 hours per week, preparing students for entry-level careers as security operations center analysts and digital forensics analysts.

Students work through 6 online real-life tasks (spending 1-2 weeks per task) in a private cloud environment with help, advice, and feedback from a knowledgeable mentor and extensive online learning resources. The tasks are embedded in the realistic, but fictional, context of work as an entry-level employee of a government cyber operations agency.

The Cyber Academy: Defense includes the following tasks:

1. Analyze a remote intrusion attempt

   A security operations center analyst has seen evidence of a password cracking attempt within a key network. Students analyze a packet capture file (PCAP) and event logs within a security information and event management system (the Splunk SIEM) to determine if any passwords were compromised and if the network was breached as a result. The student must also identify which tools were used by the attacker and which steps should be taken to safeguard specific hosts in the network from similar cracking attempts in the future.

   OBJECTIVE: Analyze suspicious network traffic in a PCAP using Wireshark.
   OBJECTIVE: Analyze network and system logs using Splunk
   OBJECTIVE: Cross-correlate events seen in a PCAP with events seen in logs
   OBJECTIVE: Recognize a Hydra brute-forcing attack
   OBJECTIVE: Determine if a brute-forcing attack has been successful

   Tasks 2 through 6 are set in the context of a single complex cyber attack.

2. Investigate an incident using a SIEM

   Students analyze a possible “watering hole” attack in which clicking on a malicious link embedded in an otherwise legitimate website launches an exploit kit that infects a user’s machine with a “banking trojan.” To accomplish this, they must analyze multiple logs within the Splunk SIEM.

   OBECTIVE: Analyze network and system logs using Splunk

OBJECTIVE: Pivot among multiple logs using Splunk's search facilities
OBJECTIVE: Identify possible indicators of compromise
OBJECTIVE: Determine if devices are likely to have been infected using indicators of compromise
OBJECTIVE: Tentatively identify the malware used and the intent of the attack

3. Begin to understand malware

Students use a "hash" of a possible malware-containing file to conduct research using VirusTotal, online sandboxes, and open source intelligence sources to determine specific indicators of compromise to guide forensic analysis of memory and file system images of infected devices.

OBJECTIVE: Use VirusTotal to identify a malware sample
OBJECTIVE: Use advanced features of VirusTotal to learn detailed information about a malware sample
OBJECTIVE: Use the HybridAnalysis sandbox to perform static and dynamic analysis of a malware sample
OBJECTIVE: Use open source threat intelligence to learn more about specific malware

4. Examine a compromised host's memory

Students perform a forensic examination of a memory image taken from a computer to identify sophisticated malware that infected the system.

OBJECTIVE: Acquire a working knowledge of process structures in memory using Volatility
OBJECTIVE: "Know normal to find evil"
OBJECTIVE: Formulate plan for a memory forensics investigation
OBJECTIVE: Recognize malware "footprints" in a forensic memory image
OBJECTIVE: Locate a malicious binary in a forensic memory image
OBJECTIVE: Corroborate findings with other sources such as [Splunk] SIEM logs
OBJECTIVE: Identify malware actions such as privilege escalation and browser hooking

5. Conduct a forensic disk examination

Students perform disk forensics on an infected system. By analyzing an image of the computer's file system, the students are able to identify malware infections and to create a timeline for the attack.

OBJECTIVE: Analyze a forensic disk image and identify indicators of compromise using Autopsy.
OBJECTIVE: Generate a timeline of suspicious events in a forensic disk image.
OBJECTIVE: Determine how a device was infected and what malware variant was

used

6. Close your investigation

   Students are asked to conclude their investigation by compiling a timeline for the attack and writing a comprehensive report for technical and non-technical stakeholders.

   OBJECTIVE: Cross-correlate information from a range of sources
   OBJECTIVE: Combine information from a range of sources into a comprehensive report
   OBJECTIVE: Communicate a complex story effectively to technical and non-technical audiences.

Who Should Enroll

Students who have successfully completed *cyber academy: Immediate Immersion* and who aspire to professional careers in defensive cyber security.

Learning Outcomes

Students will learn to:

- Analyze network traffic
- Analyze network and system logs using a security information and event monitoring system
- Cross-correlate log information and network packet traffic
- Use online sandboxes for static and dynamic analysis of malicious executable files to identify indicators of compromise
- Use threat intelligence
- Identify malware
- Perform memory forensics
- Perform disk forensics
- Compile a comprehensive timeline of a cyber attack
- Report appropriately to technical and non-technical stakeholders

In addition to the task-based curriculum, an implicit curriculum runs throughout the course via which students will learn and practice the cognitive skills essential for success in all areas of information security. These include:

- Understanding complex, novel problems
- Effectively researching solutions
- Designing and testing solutions
- Self-directed learning

Prerequisites

Successful completion of *cyber academy: Immediate Immersion*. Only basic computer skills are required, but basic knowledge of computer networks and protocols and the fundamentals of operating systems is *strongly recommended*.

The Cyber Academy: Attack (Reverse Engineering and Exploitation)

Course Overview

The Cyber Academy: Attack focuses on key offensive skills. This 15 week program, requiring 25 hours of work per week, will start students on the path to becoming penetration testers or offensive cyber operations professionals. Development of the program was funded, in part, by the United States Department of Defense, and the curriculum was designed in conjunction with DoD and industry experts.

In the project-based, learn-by-doing curriculum of *The Cyber Academy: Attack*, students work through eleven tasks online in a private cloud environment with constant help, advice, and feedback from knowledgeable mentors and extensive online learning resources. The tasks are embedded in the realistic, but fictional, context of work as an entry-level employee of a government cyber operations agency.

1. Analyze a suspicious file

   Students analyze a suspicious binary file from a laptop confiscated from a cyber-crime scene. They learn how to use basic reverse engineering to crack a password-protected binary so they can run the program and gain access to a cybercrime group's Internet Relay Chat (IRC) channel. They then eavesdrop on online conversations, and start compiling intelligence on the crime group's actors and connections.

   OBJECTIVE: Perform static analysis of unknown executable files using IDA Pro
   OBJECTIVE: Create a "hacker persona"
   OBJECTIVE: Conduct open source intelligence gathering by accessing and eavesdropping on IRC conversations

2. Analyze a related suspicious file

   Students now reverse engineer a more complex binary confiscated from a ransomware attacker's computer. This time, they must crack an encrypted password to gain access to another protected IRC channel, which yields login credentials for the crime group's FTP server.

   OBJECTIVE: Perform static analysis of unknown executable files using IDA

Pro and Relyze
OBJECTIVE: Create a "hacker persona"
OBJECTIVE: Conduct open source intelligence gathering by accessing and eavesdropping on IRC conversations

3. Analyze the FTP credentials app

   Students must now reverse engineer a binary and crack a doubly-encrypted password in order to access a file that identifies the website of a small defense contractor that is vulnerable to a local file inclusion exploit and was also infected with malware by the crime group or another actor.

   OBJECTIVE: Perform static analysis of unknown executable files using IDA Pro and Relyze
   OBJECTIVE: Perform dynamic analysis of unknown executable files using IDA Pro

4. Conduct OSINT analysis

   Students infiltrate a Russian cyber crime network by logging into an eastern European social media site using stolen credentials. They mask themselves as a member of the Russian crime group and gather intelligence about the group members and their connections from the posts on the social media site (which is a facsimile of the Russian "Facebook" site VK.ru filled with authentic posts in Russian). Students also develop a realistic persona which they will use while undercover within the group.

   OBJECTIVE: Conduct open source intelligence gathering via social media
   OBJECTIVE: Analyze foreign language material using Google Translate
   OBJECTIVE: Map the power and status relationships within an organization

5. Develop buffer overflow exploits

   The student goes undercover to infiltrate the cyber crime group. The crime group's leader asks students to execute a remote buffer overflow exploit on a vulnerable server to prove their worth to the crime group they are infiltrating. The student's government boss permits them to perform this exploit in order to strengthen the relationship with the crime group so they can continue gathering important intel about them. The student's attack provides the crime group a persistent foothold on the targeted computer.

OBJECTIVE: Conduct simple and complex buffer overflow exploits
OBJECTIVE: Use OllyDbg and Immunity Debugger for exploit development
OBJECTIVE: Control data execution prevention and structured exception handler overwrite protection on a Windows host
OBJECTIVE: "Fuzz" a server
OBJECTIVE: Generate and deploy a reverse_TCP shell using a buffer overflow exploit (Metasploit/MSFVenom/Meterpreter)
OBJECTIVE: Use MSFConsole to interact with an active exploit

6. Strengthen a buffer overflow exploit

The crime group now asks the students to strengthen their last exploit because a recompilation of the server's code has apparently turned on data execution prevention (DEP). They need to re-implement the exploit using return-oriented programming (ROP) so it works well in the altered environment.

OBJECTIVE: Troubleshoot a deployed exploit that stops working
OBJECTIVE: Use return-oriented programming to exploit an application compiled with data execution prevention
OBJECTIVE: Generate and deploy a reverse_TCP shell using return-oriented programming
OBJECTIVE: Use MSFConsole to interact with an active exploit

7. Evade antivirus

The student's boss explains that "off-the-shelf "Metasploit payloads (which students have been using until now) are typically recognized by most antivirus software. He asks the students to experiment with a variety of ways to obscure such payloads to evade detection.

OBJECTIVE: Generate malicious payloads that will evade antivirus detection using Metasploit-based and other techniques
OBJECTIVE: Test malicious payloads using online services without exposing the payloads to scrutiny by the information security community

8. Develop a custom malware payload

The Russian hacker group asks the students to design a custom payload for them. Students must deliver working shellcode that deletes Windows security logs.

OBJECTIVE: Write a custom exploit
OBJECTIVE: Generate a shellcode payload
OBJECTIVE: Deploy a custom shellcode payload via a buffer overflow exploit

9. Spearphish a company

   The crime group asks the students, working undercover, to gain access into a defense contractor's network through a spearphishing attack on an HR person's machine. Posing as a job applicant, students create a fake persona and resume, which is infected with a custom payload, reply to the job posting, infect the HR person's machine, and gain a persistent foothold in the company's network.

   OBJECTIVE: Craft a realistic fake persona
   OBJECTIVE: Generate an infected document
   OBJECTIVE: Configure an email client
   OBJECTIVE: Execute a spearphishing attack
   OBJECTIVE: Establish persistence on a target machine

10. Exploit a company's database

    Working undercover in the crime group and using the persistent foothold gained on an HR person's machine, students access the company's personnel database using SQL injection and exfiltrate data (which is scrubbed before passing it on to the crime group).

    OBJECTIVE: Test a database for common (OWASP) vulnerabilities
    OBJECTIVE: Exploit a database using SQL Injection
    OBJECTIVE: Exfiltrate data

11. Attack a nation-state

    Human intelligence determines that the cyber crime group is connected to a Russian security agency. On behalf of the US government, students spearphish the leader of the crime group, use a keylogger to obtain his login credentials, and then surreptitiously log into his computer. Using access provided by the crime boss's computer, they then gain a foothold on a Russian intelligence officer's machine. Students exploit a vulnerability in a Python framework to gain access to a C2 database of classified information from which they exfiltrate a key document.

OBJECTIVE: Plan a complex attack
OBJECTIVE: Execute a spearphishing attack
OBJECTIVE: Establish persistence on a target machine
OBJECTIVE: Conduct reconnaissance on an exploited target machine
OBJECTIVE: Fingerprint a server to determine vulnerabilities
OBJECTIVE: Exfiltrate data

Who Should Enroll

Students who have successfully completed the *Cyber Academy: Defense* and who want to learn more about the "attack side" of cyber security and cyber operations.

Learning Outcomes

Students will learn to:

- Reverse engineer unknown binary (executable) files using static and dynamic analysis
- Conduct open source intelligence
- Exploit server and application software using buffer overflow exploits and return-oriented programming
- Exploit database systems using SQL injection
- Develop custom shellcode exploits
- Evade antivirus software
- Spearphish a trusting victim
- Plan and conduct a complex cyber attack
- Pivot through a network
- Exfiltrate data

In addition to the task-based curriculum, an implicit curriculum runs throughout the program via which students will learn and practice the cognitive skills essential for success in all areas of information security. These include:

- Understanding complex, novel problems
- Effectively researching solutions
- Designing and testing solutions
- Self-directed learning

Prerequisites

Successful completion of the *Cyber Academy: Defense*.

Additional Info

Registration in this course is currently only available to US citizens and green card holders.