EBOOK

Getting Started in Cybersecurity

GUIDEPOINT
SECURITY
UNIVERSITY

Introduction

Kevin Woods

Director of GuidePoint Security University

Hello! My name is **Kevin Woods** and I am the Director of GuidePoint Security University. Prior to joining GuidePoint Security, I served in the United States Army, which gave me a start in Cyber Threat Intelligence, before I moved into an Incident Response Team Lead position. Now, in my current role at GuidePoint Security, I have had the opportunity to mentor, evaluate, hire, and speak to thousands of students, service members, and career-changers looking to get into cybersecurity. Every day I see firsthand how difficult it can be to get started in this industry. I strongly believe that anyone can have a successful career in security if they are determined and given an opportunity. I wrote this document to share my thoughts on getting started and to help you secure that opportunity.

There are many training resources available to you in the cybersecurity industry. If you show up to an interview and say you want to get into cybersecurity but have done nothing to make it happen, this is a bad sign. If you have a sincere interest in cybersecurity, go out and learn it! You don't need any special infrastructure, money, or connections to gain critical security skills. You just need a computer and an internet connection.

Why This Was Created

This resource was created to help people land their first job in cybersecurity. Oftentimes, we see **two areas** where people struggle:

ONE It can be difficult to wade through the myriad of resources available and come up with an effective plan.

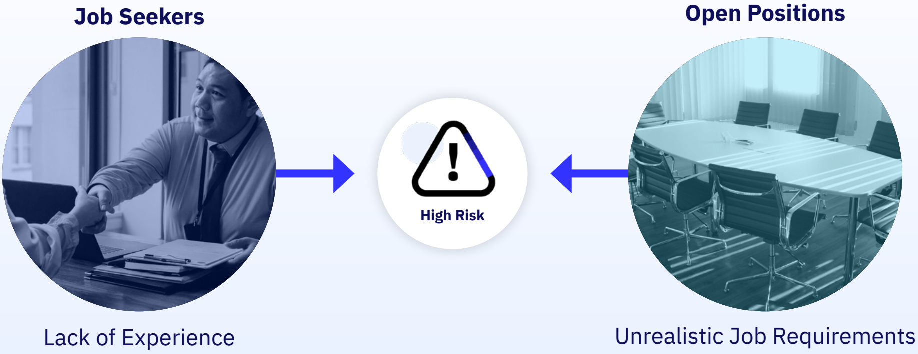
TWO It can also be frustrating applying to hundreds of jobs and hearing nothing back.

After reading this booklet, you will better understand what hiring managers are looking for, and will be equipped to create a training plan that establishes the foundational industry knowledge you need to

BEGIN YOUR CAREER.

The Cybersecurity **Skills Gap**

Let’s start by discussing the current cyber landscape. If you’ve recently entered the job market, you are probably used to seeing “entry-level” jobs that require 4+ years of experience, along with a plethora of certifications. Unfortunately, the industry overall is fairly risk averse, which forces hiring managers to set unrealistic requirements. This has made it quite prohibitive for new job seekers looking to enter the workforce. From the company perspective, this is an industry that deals primarily in risk management.



Job Seekers

Lack of Experience

High Risk

Open Positions

Unrealistic Job Requirements

Hiring inexperienced practitioners introduces high levels of risk: both in terms of personnel turnover and in operational risk. New employees cost more to train and are more likely to leave (especially if they don’t know what they want to do) than existing personnel. On the operational side, junior employees are more likely to make mistakes, which can have devastating impacts to the employer or a client. Thus, we get this growing skills gap, where job seekers lack the experience to land a job, but the industry doesn’t have enough experienced practitioners to effectively manage cyber risk.

As a job seeker, you can’t control what hiring teams do; but you can make yourself more marketable by standing out from the crowd and lessening the perceived risk to a potential employer.

How to Use This Resource

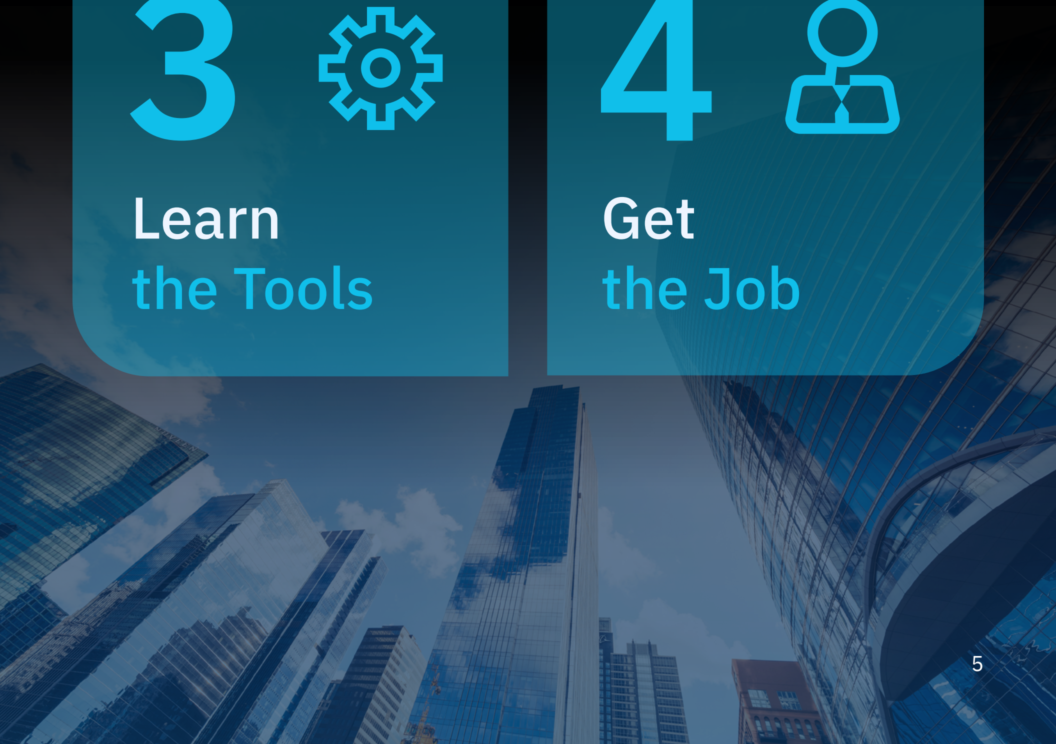
In the following pages, we will take you through our **four steps to landing a job in cybersecurity:**

1 Understand the Industry

2 Establish a Foundation

3 Learn the Tools

4 Get the Job



What this Resource Is Not

This resource will not teach you everything you need to know to get a job in cybersecurity. It will help you understand what organizations look for and make you aware of available training resources. This is not a guide meant to hold your hand. It is purely a basis to get you down the right track.

This document does not serve as a one-size-fits-all, nor a complete listing of all resources available. Do your own research to find the resources that help you learn best. At the end of this document, you will find additional resources and example training plans. This should give you an idea for how to put your own plan together.

General Advice

Work Through Problems

Technology is changing so quickly that it is very difficult to keep training resources and videos up to date. Things hardly ever run perfectly the first time you try. If you run into an error while consulting a resource – work through it! Start by Googling the error message. It is likely that someone else has already encountered this same problem and found a solution. Sites like **StackOverflow** are good places to ask questions and search for solutions to your problems.

Be Curious

Hiring managers seek curious cybersecurity professionals because it shows passion. Curious individuals tend to approach problems with a desire to understand the root causes and explore different solutions.

Curiosity also drives individuals to seek out new information, technologies, and techniques. In a rapidly changing industry, being curious ensures that professionals stay updated with the latest trends, tools, and vulnerabilities. This is crucial for long-term success in cybersecurity.

So the next time you follow a tutorial, don't just copy/paste commands. Understand why you are issuing each command. Research what the command is actually doing. Try to understand the entire process, not just memorize steps. Troubleshooting is a large part of any cybersecurity job. If you are unwilling to work through errors as they occur, this may not be the right career choice for you.

1 Understand the Industry

The cybersecurity industry plays a crucial role in safeguarding digital assets and infrastructure against a wide range of threats. It encompasses the practices, technologies, and strategies aimed at protecting networks, systems, data, and users from malicious attacks, unauthorized access, and other cyber risks. Professionals in this field employ a variety of tools and techniques to detect, prevent, and respond to threats effectively. With the ever-growing number of sophisticated attacks, the demand for skilled professionals is at an all-time high.

Roles and Specialities

Conduct research on the different specialty focus areas within the industry. **Ensure that you understand the following:**

- ✓ IT vs. Software Engineering vs. Cybersecurity
- ✓ Red Team vs. Blue Team vs. Purple Team
- ✓ Security Engineering vs. Security Operations
- ✓ Security Engineer vs. Security Analyst
- ✓ Network Security vs. Application Security

Cybersecurity is NOT the same as software development or IT. Do not interview for a SOC Analyst position and tell the hiring manager that you want to be in IT or write code all day.

You should be aware that cybersecurity vendor companies are actually developing a product to sell, so there are programmers involved. Do not confuse these positions with security professionals.

You will find there are many different names for the same roles within cybersecurity. Entry-Level roles include:

- ✓ Information Security Analyst/ Specialist
- ✓ Associate Security Engineer
- ✓ Junior Security Analyst
- ✓ SOC Analyst – Tier 1

The Security Operation Center (SOC) is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

Certifications

Cybersecurity is an industry that places a heavy emphasis on certifications. In fact, some organizations find more value in certifications than they do in a college degree. Additionally, if you wish to work in the government or defense sector, you may be required to hold some of these certifications prior to getting account privileges on a computer, but many offer at least some form of free training, along with free trials of their platform. Technical certifications can be offered through a certification provider or directly through a vendor.

If you are looking for a Federal position, check out DoD 8570, which lists certifications required for different roles in the government.

Vendor-Neutral Certification Providers

These certifications are administered and recorded by a central party. Vendor-neutral certifications are a good way to demonstrate that you have the necessary foundational knowledge to learn a specific job role. If you are brand new to information technology, Network+ is a good place to start. If you want a baseline certification to show a desire in security, check out CompTIA's Security+ or ISC2's Certified in Cybersecurity (CC). Some of the most popular vendor-agnostic certs include:

- ✓ CompTIA
- ✓ ISC2
- ✓ ISACA
- ✓ Cloud Security Alliance
- ✓ EC-Council
- ✓ OffSec
- ✓ TCM Security

Vendor Certifications

Many of the popular vendors in the industry offer some form of training and certification. If you know which area of cybersecurity you'd like to get into, you can research key vendors in that space. For instance, if you want to become a SOC Analyst, get certified on a SIEM tool. Adding a well-known industry tool to your resume will make you stand out to hiring managers. Every vendor is different, but many offer at least some free training.

2 Establish a Foundation

Learning the technical foundations of cybersecurity before entering the field is crucial. Technical knowledge forms the bedrock upon which effective security strategies are built, enabling professionals to anticipate and respond to emerging threats confidently and precisely.

Going into an interview with a solid technical foundation instills credibility and competence, which is essential for gaining the trust of employers. Mastering technical skills also fosters problem-solving abilities and critical thinking in real-world scenarios. By showing that you can grasp the technical intricacies early on, you are demonstrating your ability to adeptly navigate complex challenges, while making meaningful contributions to combat cyber threats.

GPSU breaks down the technical foundations into three areas: **Systems, Networking, and Security**. In learning this way, one will develop a deeper understanding of the underlying principles and mechanisms that govern secure architecture.

Get Familiar with the Language

It is vital that you know the lingo to be successful in this field. This may come from time and experience, but you'll need to be able to speak the terms during an interview. You can find some decent lists just by Google searching for “Common Cyber Terms”.

Pillar 1:
Networking Basics

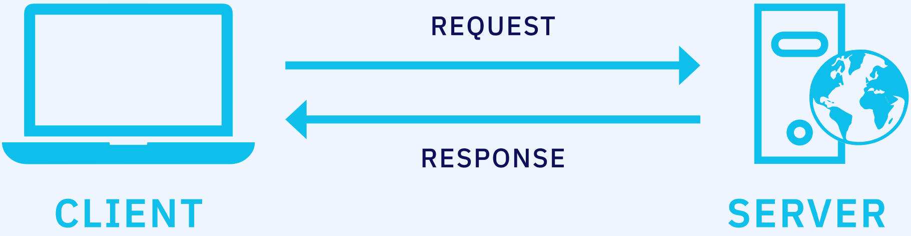
It is highly encouraged that you begin your journey by learning the basics of computer networking. There are many ways to do this, including free courses online. One great way to learn is to study for the Certified Cisco Networking Associate (CCNA). This certification training teaches learners from the absolute beginning, covering many important topics that are necessary to know for security professionals. It may be worthwhile to spend ~$20 on a Udemy or LinkedIn course. CCNA training may be time-consuming, but it is a worthwhile investment if you are serious about getting into IT or cybersecurity. CompTIA's Network+ is another option for an introductory networking certfication if CCNA is too costly. For practice, try using the free Cisco tool Packet Tracer to explore networking devices and communication protocols.

Clients, Servers, and the OSI Model

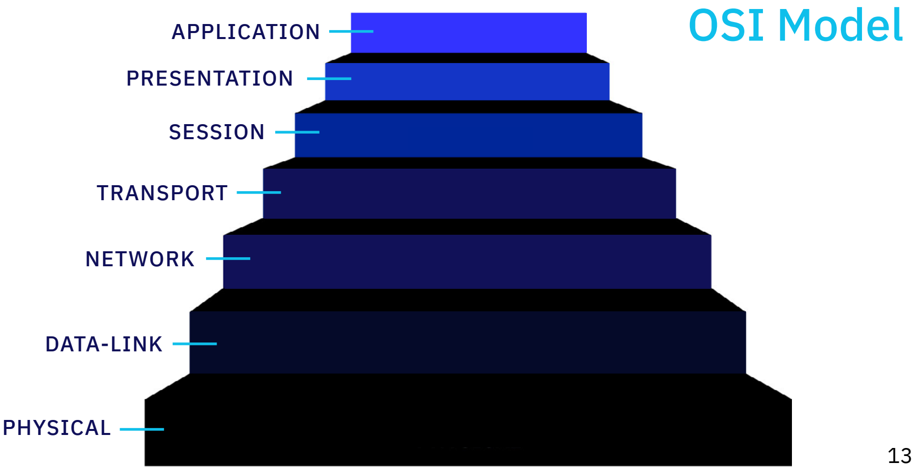
Begin by researching the Client-Server architecture. This represents nearly every form of communication between computing systems. As you progress through your studies, you should be able to look at a transmission and easily pick out the client and the server.

Client = Device initiating communication and requesting data

Server = Device responding to clients, often providing a function or service



Once you understand the relationship between a client and server, move on to the OSI Model. This is a conceptual framework used primarily for teaching purposes. You should know the layers by heart, along with the types of transmission that occur at each layer.



Understand Network Addressing

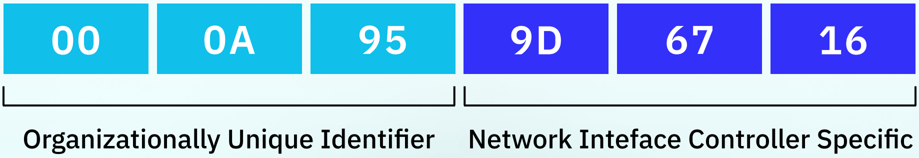
MAC Address

A **layer 2** address, also called a physical address. A MAC address is a unique, unchanging identifier for every network device. It can be used to transmit data across the Local Area Network (LAN), but not outside the LAN. With regard to access control, an organization may use MAC addresses to whitelist approved computers for remote workers.

Whitelist = A security strategy that only allows access to an approved list of objects.

An example MAC address is: **00:0A:95:9D:67:16**. The first characters of the MAC address identify the organization which developed the device (Dell, Apple, Cisco, etc.). The second half is unique for that device.

Media Access Control Address



00 0A 95 9D 67 16

Organizationally Unique Identifier

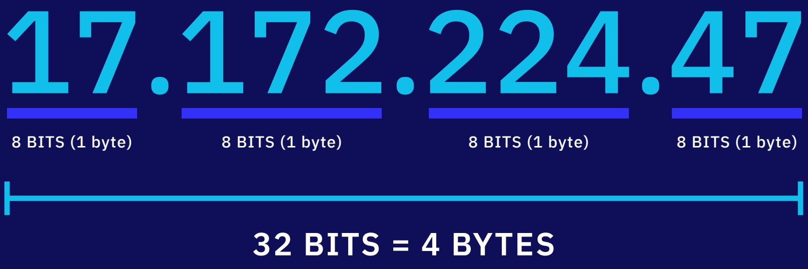
Network Inteface Controller Specific

IP Address

A **layer 3** address, also called a logical address. IP addresses are not immutably tied to a device, like a MAC address. In fact, IP addresses change quite frequently if a network uses the default dynamic host configuration protocol (DHCP), which randomly assigns IP addresses. Instead of dynamic assignment, organizations can manually set Static IP addresses so that a device does not receive a new IP every time it connects to the network, but this is also reversible.

What is an IP Address?

An IP address is made up for 4 bytes, with each containing a number between 0 - 255 (2^8). To understand IP addressing further, you should learn the difference between Public and Private IP addresses.

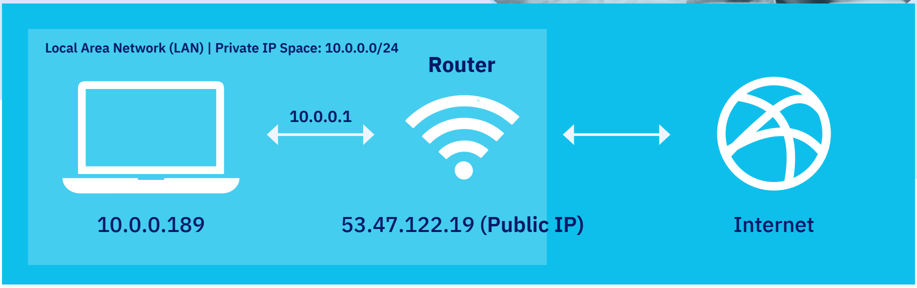


Private IP

Private IP addresses are how systems on your local network communicate with local devices. Private IPs are generally not exposed to the public internet. LAN devices communicating to the internet will connect via a router, which hosts the network's Public IP. Privates IPs fall into three ranges: 10.x.x.x, 172.16.x.x, and 192.168.x.x

Public IP

Public IP addresses are how systems OUTSIDE of your local network can reach you. Public IP addresses are also how we reach resources across the internet, like web pages. Each Public IP address can only be used by one device at a time.



Subnetting

You probably won't need to know subnetting for most analyst jobs in security. However, you should be able to recognize some CIDR notation. For instance, know that /24 (pronounced "slash 24") is 256 IPs and represents the entire last byte of an IP address.

192.168.1.0/24 has 256 addresses
192.168.1.0 is the **Network Address**
192.168.1.1-254 are **Available Addresses** (can be assigned to devices)
192.168.1.255 is the **Broadcast Address** (send to all devices in subnet)

There are plenty of ways to learn subnetting online, including free resources like subnetting.net and Sunny Subnet on Youtube.

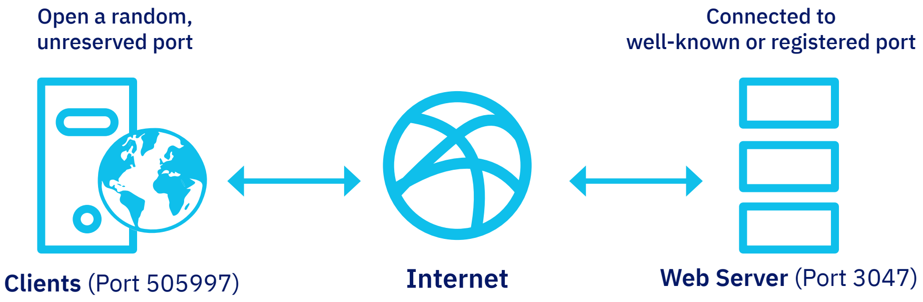
Recognize the Common Ports and Protocols

Ports and Protocols are introduced at **layer 4** of the OSI model. A port and IP address together form a Socket, which may be written as such: **10.200.1.13:8000**.

A **Port** is a number assigned to identify a connection endpoint. Ports are often associated with a particular service, or “protocol”. A **Protocol** is a set of rules for communicating across a service. For instance, we use specific language when sending emails, which is how a server knows how to read what a computer sends to it. This is part of the Simple Mail Transfer Protocol on Port 25.

Well-Known Ports	Registered Ports	Unreserved Ports
0-1023	1024-49151	49152-65535

Ports are placed into three groups: **Well-Known, Registered,** and **Unreserved** (aka Ephemeral). Well-known ports are associated with vendor-agnostic industry protocols, such as SSH and HTTP. Registered ports are assigned to an organization for a particular function. For instance, Microsoft has registered the Remote Desktop Protocol to port 3389 and XBOX Live to port 3074. Unregistered ports are opened by clients when initiating a connection, as a place to receive information from servers.


Open a random, unreserved port
Connected to well-known or registered port
Clients (Port 505997)
Internet
Web Server (Port 3047)

Some of the common ports and protocols you should know are listed below. As you go through your studies, start to think about how an attack may take advantage of each protocol.

Port #	Protocol Name	Protocol Description
20 21	File Transfer Protocol (FTP)	Establishes file transfers between two systems.
22	Secure Shell (SSH)	Encrypted login to a terminal on a remote system.
23	Telnet	Unencrypted login to a terminal on a remote system.
25	Simple Mail Transfer Protocol (SMTP)	Used for email routing between mail servers.
53	Domain Name System (DNS)	Resolves domain names (i.e. google.com) to IP addresses (i.e. 142.250.72.206)
67	Dynamic Host Configuration Protocol (DHCP)	Automatically assigns IP addresses, so an IT admin doesn't have to do it manually.
80	HTTP	How computers talk to web servers. This is how we communicate with web servers and request web pages. HTTP is NOT secure.
123	Network Time Protocol (NTP)	How computers keep time.
443	HTTPS	A secure version of HTTP. This incorporates SSL to add a layer of encryption, and also verifies the server's identity.
514	Syslog	System logging allows for the transfer of logs to a central location.
3389	Remote Desktop (RDP)	Used for remote access to a desktop environment.

Start Virtualizing

Once you become familiar with the basics, you can start exploring virtual machines (VMs) and networks. This provides a more hands-on approach to learning, while also creating a safe place for you to practice with security tools. You can easily create local VMs using one of the below popular virtualization softwares:

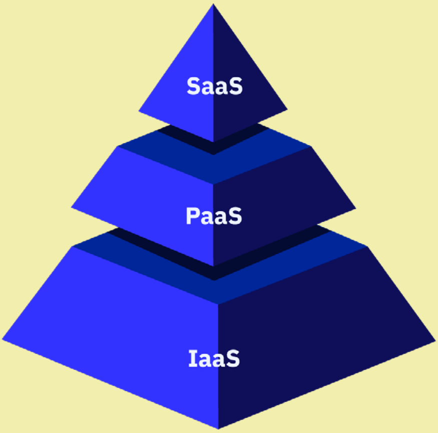
- ✓ Oracle VirtualBox
- ✓ VMWare
- ✓ Microsoft Hyper-V
- ✓ Parallels

After installing your first VM, create another one and get them talking! Experiment with OpenVPN if you want to take it a step further. Once you have multiple VMs communicating, you can start attacking from one machine into the other, or practice using popular security tools.

For all your home network and virtualization needs, Youtube is your friend!

Cloud Service Models

You should also understand the different types of cloud service models (IaaS vs. PaaS vs. SaaS).



The Cloud

At the very least, you should understand what the cloud is, and how it has different security implications than the traditional on-premises architecture. There are three major players in the cloud industry, all of which offer training to learn their platforms.

- ✓ **Amazon Web Services (AWS).** AWS has many different ways to learn, including free live trainings via Twitch, and several free digital courses to get you started. You can also sign up for a free AWS account and work through Well-Architected Labs.
- ✓ **Microsoft Azure.** Microsoft offers free fundamental training for Azure. If you want to test yourself further, you can take a certification exam for a relatively low price (compared to other certifications).
- ✓ **Google Cloud Platform (GCP).** Google offers free cloud training to learn its cloud platform along with free, interactive training events through its Cloud OnBoard initiative.

Pillar 2: Operating Systems

A security professional should be comfortable in both Windows and Linux. Many people are unfamiliar with Linux, so I recommend starting there, before moving into Windows administration. Having this foundational systems knowledge will allow you to better understand threat tactics, host forensics, and tool detection methods.

Linux Operating Systems

Linux is widely used for enterprise-level databases and security tools. There are many different flavors of the Linux operating system, almost all of which are free and open-source. Many distributions are derived from Debian, including Ubuntu, Mint, Kali and Parrot OS.

Aside from Debian-based systems, there are Red Hat Package Manager (RPM) Linux distros, including Red Hat Enterprise Linux (RHEL). While RHEL is a commercial product, Fedora is the upstream, free community version of RHEL, with additional derivatives, such as Amazon Linux and CentOS. Take a class on Linux Server Management, such as the free Coursera course offered by the University of Colorado.

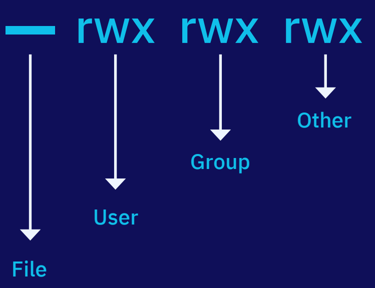
NOTE: Mac OS and Linux are considered *unix systems. They share a similar file structure and many of the same terminal commands.

Linux Terminal

Learn how to use the Linux terminal, which will translate well to Mac OS and cloud shell commands. One fun way to learn the Linux terminal is to go through OverTheWire's Bandit Games. You should use a Linux VM to go through these levels.

At a minimum, you should be able to use the following commands:

- **Navigate/Read:** cd, ls, pwd, cat, echo
- **Create/Move:** mv, cp, rm, mkdir, touch
- **Permissions:** chmod, chown, sudo, su
- **Networking:** ping, traceroute, ifconfig, ip, netstat, ssh
- **Help:** man

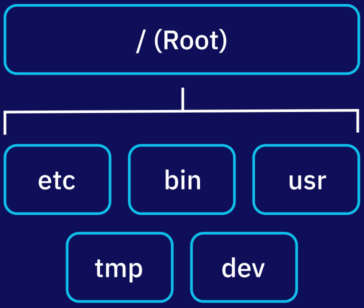


Linux File System

While learning Linux security, you should cover the following files, which are commonly exploited during attacks:

- **Account Files:** /etc/passwd, /etc/shadow, /etc/group
- **DNS Files:** /etc/hosts, /etc/resolv.conf
- **Boot Files:** /etc/system.d, /etc/init.*, cron-jobs

Additionally, Linux largely runs on the permissions: ***Read (r), Write (w), Execute (x),*** for ***User***, ***Group***, and ***Other***. File permissions are used as the standard means of access control in Linux, so you should be comfortable speaking on them. The Linux file system follows a tree hierarchy, spanning from the root directory.



Windows Operating System

When we talk about understanding the Windows OS, it does not mean being able to open a game of Solitaire or create a PowerPoint presentation. You must become familiar with the directory structure, command prompt, user accounts, running processes, common vulnerabilities, etc.

Windows Servers and Security

Take a class on Windows Server Management, such as the free Coursera course offered by the University of Colorado.

One of the major differences between Windows and Linux is the filesystem. Whereas Linux uses a tree structure stemming from a root directory, Windows uses drives.

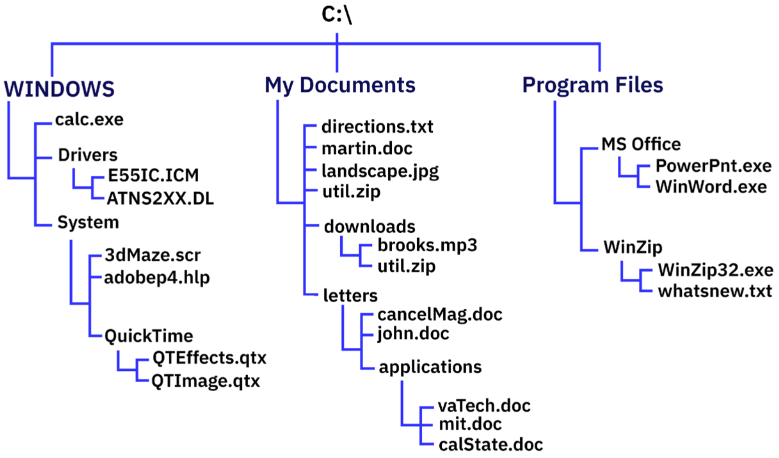
Commond Prompt and Powershell

Just like in Linux, you should learn how to issue commands via a command line interface (CLI). At a minimum, you should be able to execute the following in a command prompt:

- **Navigate/Read:** cd, dir, pwd, systeminfo
- **Create/Move:** copy, del, mkdir, rmdir
- **Permissions:** whoami, net user, runas
- **Networking:** ping, tracert, ipconfig, netstat
- **Help:** help

Windows also has PowerShell, which is a very powerful command-line tool that helps automate and streamline CLI operations. Microsoft Learn has a free Introduction to PowerShell course if you wish to learn more.

Windows



When studying the Windows Operating System, be sure to research the following:

- ✓ C:\Windows\system32\
- ✓ C:\Program Files\
- ✓ C:\Windows\SAM
- ✓ C:\pagefile.sys
- ✓ C:\Documents and Settings\
- ✓ C:\Windows\Prefetch
- ✓ C:\Windows\Users*\NTUSER.dat
- ✓ C:\swapfile.sys

Active Directory and Systinternals

Active Directory (AD) stores information about objects on the network and makes this information easy for administrators and users to find and use. It creates a centralized location for resources, identity management, and security administration. For most roles, you do not need to know AD in depth, but should become familiar with Group Policy Objects, Domain Controllers, LDAP, and Kerberos.

Sysinternals may be slightly more advanced, but something people getting into forensics should definitely know. There are several overview videos on Youtube, but you can also learn sysinternals on Microsoft Learn, or go to the source by googling Sysinternals by Mark Russinovich.

Pillar 3:
Security Fundamentals

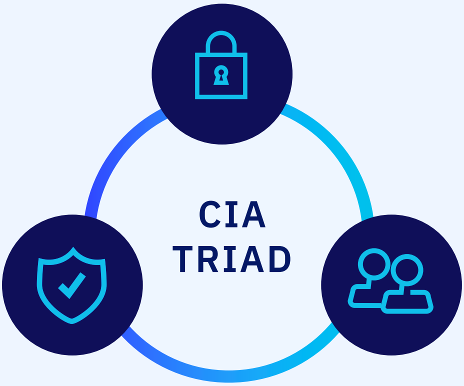
There are a few different ways to learn the common themes and best practices that show up all the time in our industry. Do a Google search and find the course that's right for you! I suggest checking out *University of Maryland's Cybersecurity for Everyone* or the *University of London's Cyber Security Fundamentals* courses on Coursera (you can audit these classes, no need to purchase the certificate).

As a reminder, this booklet will only cover a few basic topics of security. You will need to do additional research to develop your security foundation.

Nearly every introductory security course starts with the CIA triad. The idea of the triad is that everything in security comes down to Confidentiality, Integrity and Availability. It is designed in a way to show that increasing one area pulls away from another. For instance, if we limit the people who can access a network resource, this will improve confidentiality. However, it removes availability, as less people can access it. Thus, like many things in cybersecurity, it becomes a balancing act.

🔒 = Confidentiality   🛡 = Integrity

👥 = Availability



Network Security

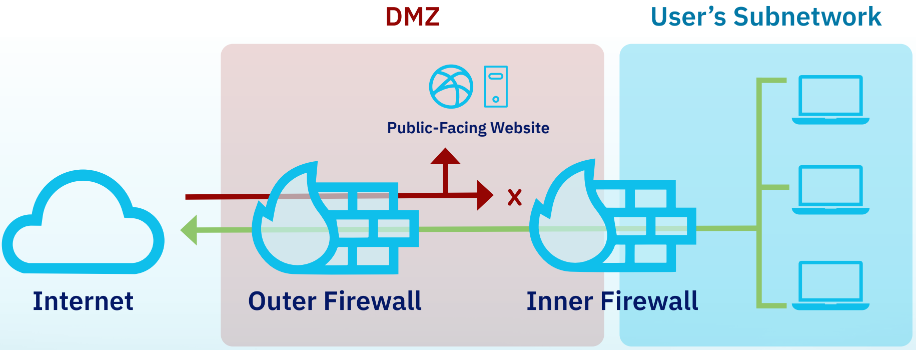
In modern businesses and organizations, network design must factor best security practices into all areas of their architecture. Creating a secure network architecture begins with a thorough understanding of the network's requirements and risk potential. The first step is defining the network's perimeter and critical resources.

From there, one can segment the network into different zones based on permissions and functionality. For instance, you can separate public-facing web servers from internal user databases through the use of Demilitarized Zones (DMZs). Each segment should be protected with firewalls, intrusion detection/prevention systems (IDS/IPS), and access control lists (ACLs) to regulate traffic and prevent unauthorized access. Implementing strong authentication and encryption methods is crucial for protecting data in transit and at rest.

Using Virtual Private Networks (VPNs) for secure remote access, deploying Multi-Factor Authentication (MFA), and ensuring end-to-end encryption can significantly enhance security.

Regularly updating and patching all network devices and software helps mitigate vulnerabilities. Additionally, employing network access controls ensures that only authorized and compliant devices can connect to the network. Regular security audits and monitoring through Security Information and Event Management (SIEM) systems help in the early detection and response to potential threats, maintaining the network's integrity and security over time.

Typically, we are looking to create a Defense-in-Depth strategy, so even if one defense fails, there are other defenses in place to protect the network.



Zero Trust

Zero Trust is both a model and set of security standards focused on providing security controls around digital assets that are separate from and do not solely depend on traditional network controls or perimeters. A zero trust architecture applies zero trust concepts and incorporates the relationship between network components, workflow planning, and access policies. This type of architecture advocates granting access to a user or device based on the level of confidence that exists with the device identity and device health, in combination with user authentication.

Cloud Security

Cloud security refers to the protection of information, applications, data, platforms, and infrastructure that operate or exist within the cloud. It consists of a variety of tools, policies, architectures, strategies, controls, and technologies designed to reduce the likelihood of theft, inappropriate access, deletion, exposure, or leakage. With so many business activities now being conducted in the cloud and with cyberthreats on the rise, cloud security becomes critically important.

System Hardening

Hardening a computer system involves implementing measures to reduce its vulnerability to cyber attacks. One crucial step is to ensure that all software, including the operating system and applications, are up to date with the latest patches and security updates. Applying patches in a timely manner removes the risks associated with known vulnerabilities. Additionally, shutting down unused ports, disabling unnecessary services and applications reduces the attack surface, making it harder for attackers to find and exploit potential weaknesses.

Access Management

Access management is all about controlling who has access to the data. It is a combination of policy, technical processes, and physical protections. **Two major concepts for access management are Authentication and Authorization:**

1 **Authentication** is the process of confirming an entity (such as an individual, service, site, or object) is in fact who it claims to be. Common forms include: Passwords, Tokens, and Biometrics.

2 **Authorization** confirms whether an entity has sufficient permissions or privileges to execute some action on a system. This process ensures that only trusted entities are able to perform the action.

Single Sign-On (SSO) is an authentication process that allows users to log into various systems, networks, or applications using a single identifier. Typically, SSO only requires the user to log in once, granting them access to multiple systems without needing to re-enter their credentials. As an extra layer of security, organizations should implement Multi-Factor Authentication (MFA) which requires users to log in with a combination of two or more components. These components often include something the user knows (a username and password), something the user has (a security token), and something the user is (such as facial recognition, voice recognition, or a fingerprint).

Role-based access controls (RBAC) help manage user access by assigning users to one or more roles, each designated with specific privileges. RBAC simplifies managing complex roles or role hierarchies and allows administrators to limit user privileges, enforcing a ‘least-privilege’ approach. Modern identity solutions support RBAC and role mining, utilizing AI and machine learning to analyze and recommend role compositions proactively.

Threat Actors

Cybersecurity threats can be categorized based on their motivations and the techniques, tactics, and procedures (TTPs) they use. Cybersecurity threats can be categorized based on their motivations and the techniques, tactics, and procedures (TTPs) they use.

Hacktivists are politically motivated individuals or groups who engage in activities like defacing websites and launching denial-of-service (DOS) attacks to promote their causes.

Script Kiddies, on the other hand, aim for small financial gains or seek to showcase their hacking abilities by exploiting known vulnerabilities with simple exploits.

State-Sponsored attackers are driven by political influence, financial gains, or intelligence gathering, with their methods varying based on their specific goals and the country they represent.

Criminals, primarily motivated by financial gain, are often associated with ransomware attacks.

Insider Threats come from individuals within an organization who might sabotage operations or seek personal financial gain by using removable devices to transfer data externally or through installing malware.

Lastly, **Environmental threats**, though not human-induced, are crucial to consider in cybersecurity. These include natural disasters such as hurricanes and tornadoes, which can significantly impact data and network protection strategies.

Common Cyber Attacks

There are many different types of cyber attacks. Most of which won't fall directly into one of these categories, but it is important to understand this terminology so we can speak a common language throughout the industry. Additionally, many of these attacks are done in combination. For instance, a threat actor may use a social engineering tactic like phishing to place a virus on a system that exfils user credentials to an external system, which then uses a rainbow table to harvest credentials.

Social Engineering

Social engineering attacks exploit human psychology to deceive individuals into divulging confidential information or performing actions that compromise security. Some techniques you should be familiar with are:

- Phishing, Whaling, Smishing, Vishing
- Dumpster Diving, Tailgating, Shoulder Surfing
- Pretexting, Business Email Compromise, Baiting

Common Mitigations: User Training, Administrative Policies

Malware

Malware is short for "malicious software", and is a general term used to describe software that is harmful or intrusive. Some of the topics discussed below (viruses, ransomware, worms, and trojans) are all examples of malware.

A **VIRUS** is a program that requires human intervention to trigger a response and replicate.

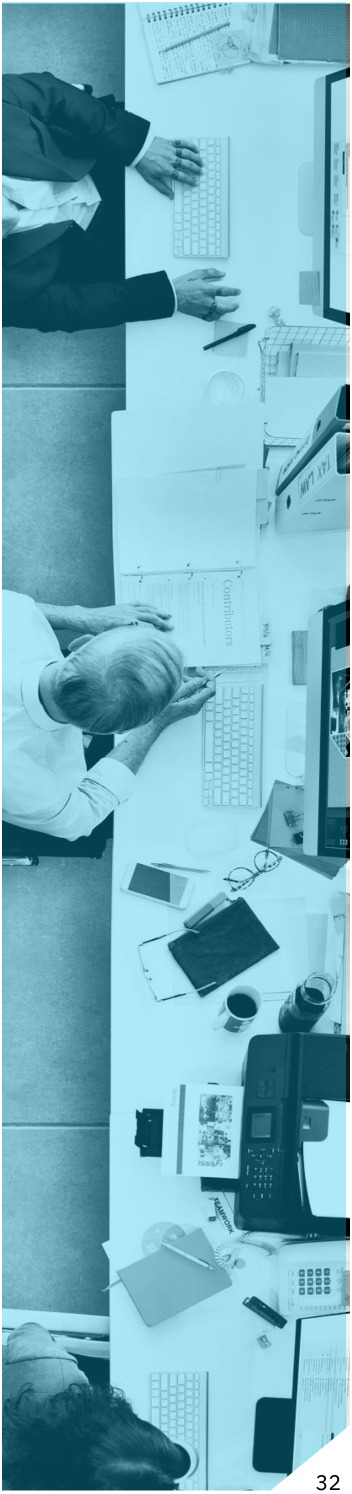
Viruses typically contain code that causes an unwanted, unexpected, and usually malicious event to occur after some time. This ‘payload’ might corrupt data or cause other types of problems on your computer.

A **WORM** is a piece of malware that replicates itself in order to spread to other computers/devices. It often uses a computer network to spread, relying on security failures on the target computer to access it. It will use this machine as a host to scan and infect other computers.

A **TROJAN** is a malicious program that poses as a legitimate one.

Ransomware is malware that encrypts a system’s data, making it unusable for the user. The threat actor then holds the data “ransom” until the victim pays to get the decryption key. Note that traditional ransomware does not require the exfil of data out of a network, which makes the attack very fast and difficult to detect during execution.

Common Mitigations: Patching, Antivirus, Endpoint Detection & Response, Backups



Password Attacks

- **Brute Force** – try a bunch of credentials until one works. It is an attack in which cybercriminals utilize trial-and-error tactics to decode passwords or other forms of login data by leveraging automated software to test large quantities of possible combinations.
- **Dictionary Attack** – a common type of brute force that uses a list of dictionary words.
- **Rainbow Table** – more of a tool than an attack; rainbow tables allow attackers to reverse look-up passwords from stolen hashes.

Common Mitigations: Strong Password Policies, MFA

Denial of Service

Denial-of-Service (DoS) attacks are a category of cyber attack that aim to make a computer, network, or service unavailable to its intended users. Most often this is achieved by overwhelming the system with a flood of illegitimate traffic. This type of attack disrupts the normal functioning of the target, making it impossible for legitimate users to access the resources they need.

A more advanced and potent version of DoS is the Distributed Denial-of-Service (DDoS) attack. In a DDoS attack, the attacker uses multiple compromised systems, often part of a botnet (a network of infected computers), to launch an attack on the target. The distributed nature of these attacks makes them harder to defend against, as the attack traffic comes from many different sources.

Common Mitigations: Attack Surface Reduction, WAF, Rate Limiting

Web Attacks

When it comes to web application attacks, you should know about the OWASP Top Ten. You can also explore some of these vulnerabilities through free lab exercises on Kontra.

Though there are many types of web attacks, you should at least know the following:

- **SQLi:** This happens when a hacker submits destructive code into an input form. If your systems fail to validate this information, it can be submitted into the database, changing, deleting, or revealing data to the attacker.
- **Directory Traversal:** Also resulting from the improper validation of inserted data, these web server attacks involve injecting patterns into the server's file hierarchy that allow bad actors to obtain user credentials, databases, configuration files, and other information stored on hard drives.
- **Cross-Site Scripting (XSS):** This involves an attacker uploading a piece of malicious script code onto a website that can then be used to steal data or perform other kinds of mischief. Although this strategy is relatively unsophisticated, it remains quite common and can do significant damage.
- **Cross-Site Request Forgery (XSRF):** An attack that forces an end user to execute unwanted actions on a web application in which they are currently authenticated.
- **Remote/Local File Inclusion:** An attack technique that involves forcing the web application to execute a file either located on the system (local) or from another system (remote).

2 Learn the Tools

Defensive Tools

For candidates applying without experience, one of the greatest deficiencies is the lack of vendor tools on a resume. Now I do not mean “Wireshark” - nearly every candidate out there has that on their resume. Set yourself apart by adding some big-name vendor tools (not just open-source). Many of the industry vendors have Community Editions or Free Trials that you can use to get hands-on experience, and some even offer free training to get started.

Antivirus

An antivirus product is a program designed to detect and remove viruses and other kinds of malicious software from a system. Antivirus is used on personal computers, as well as enterprise machines.

Application Security Tools

Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) tools are used in different phases of the software development life cycle (SDLC) to find risks in an application. SAST tools are used to analyze source code to identify flaws and potential vulnerabilities that could lead to a data breach or disruptive attack. DAST tools do not have access to the underlying code, but instead simulate more of an attacker’s perspective, looking to identify vulnerabilities that allow threat actors to conduct attacks, such as code injection and cross-site scripting.

EDR

Endpoint Detection and Response (EDR) tools record behaviors on individual systems, called ‘end points’ - *think of your laptop* - and send that data to a centralized source for analysis. Oftentimes, these tools are programmed to automatically detect anomalies/malicious behavior and theninitiate an appropriate response, as programmed by security engineers.

SIEM

A Security Information and Event Management (SIEM) tool is a data aggregation system used to identify potential threats or malicious activity on a network. SIEMs are capable of collecting large amounts of data and presenting that data in a way that allows analysts to quickly spot anomalies. SIEMs are one of the most popular tools used in industry, and are found in nearly every Security Operations Center (SOC).

SOAR

Another common SOC tool is a Security Orchestration, Automation, and Response (SOAR) platform, which is used to automate security actions in sequence through playbooks. SOAR technologies free up time for security analysts by having automated responses to common attacks (phishing, brute force, malware downloads, etc.).

Vulnerability Scanners

Vulnerability scanners are automated tools that allow organizations to quickly identify known vulnerabilities on their network devices and systems. These tools are typically easy to use and allow for automation, so they can run on a schedule, and immediately report critical findings.

Secure Architecture Tools

Firewalls

A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. In reality, "firewalls" are everywhere - they can be free software that comes on common networking devices, but can also be standalone devices with advanced features, like a Next Generation Firewall (NGFW). These are typically what vendors are selling.

Email Gateways

An email gateway is a server or device that acts as a barrier between the internet and a corporate email system. Many email security providers offer advanced detection, utilizing AI capabilities, that inspect email messages for specific phrases that indicate malicious activity, along with address information, such as IPs to identify threat actors or foreign traffic. In general, information security teams use email gateways to help protect end users from spam, phishing, redirects, malicious file downloads, and more.

Identity and Access Management

Identity and access management solutions and technologies are designed to secure enterprise assets (systems, data, devices, networks, and applications) and protect them from internal and external threats. IAM solutions and technologies are applicable to devices, as well as cloud-based and on-premise systems, networks, data, and applications. Privileged Access Management (PAM) deals with managing and monitoring privileged accounts that have access levels above and beyond a regular user. PAM solutions provide features such as password vaulting, privilege session monitoring and recording.

Risk Management & Intelligence

Cyber Threat Intelligence

Cyber Threat Intelligence (CTI) is the process of collecting, analyzing, and interpreting information about potential and existing cyber threats to inform and enhance an organization's security measures. Intel helps organizations proactively identify and mitigate potential cyber threats, reducing the risk of data breaches and financial losses. We often use threat intelligence feeds and solutions to quickly identify known threat tactics, techniques, and procedures (TTPs).

External Risk Management Tools

Everything in cybersecurity relates back to risk management. Typically, an organization can identify risks and take calculated measures to protect their internal assets. But sometimes an organization is faced with external factors that seem outside of their control. For instance, a company's social media page may be flooded with brand-damaging posts, a corporate executive may be impersonated, or a fraudulent site might pose a legitimate company, selling with no intention of providing the purchased good or service. External cybersecurity tools help protect against external attacks through real-time monitoring of social media platforms and the dark web.

Third Party Risk Management

Third Party Risk Management (TPRM) tools help businesses assess, monitor and mitigate risks associated with their vendors, suppliers, and other external partners. These tools provide upfront assessments of third-party solutions, in addition to providing continuous monitoring of those third parties, to provide historical insights, along with real-time knowledge of known and perceived risks to the organization. In this way, TPRM tools helps businesses make decisions on who to partner with, and to take immediate action if an external partner is compromised.

Offensive Tools and Techniques

Penetration testing (Offensive Security) is a very difficult specialty to get into. However, there are many, many resources for learning offensive security. Even if you do not plan on going into penetration testing as a specialty, you can learn a lot by practicing ethical hacking using some of the below resources.

Kali Linux

Not a traditional "tool", Kali Linux is an operating system (like Mac OS or Windows) that is used for penetration testing. Simply put, you MUST know Kali Linux to get into offensive security. Install it as a VM on your home computer and start practicing. There is also Parrot Security, which is an alternate OS to Kali Linux. However, if you are unfamiliar with Kali, you should start there instead of Parrot.

Techniques

Some of the common offensive techniques you should learn include:

- Host and Service Discovery
- Reverse Shells
- Privilege Escalations (Windows, *unix)
- Establishing Persistence
- Harvesting Credentials
- Using Publicly Released Exploits (CVEs, Exploit-DB)

Offensive Tools

In addition to learning these techniques, you should experiment with each of the below tools, if possible.

- Burp Suite
- Metasploit
- Mimikatz
- nmap
- Hydra
- John the Ripper
- Ghidra
- SQLmap

There are plenty of open source (free) vulnerability scanners: Nikto, OpenVAS, BurpSuite, Nmap that offensive individuals tend to use. Organizations typically pay for enterprise scanners, such as Nessus, for their ability to generate readable reports; along with the ability to inject specific feeds into the scanner (more up-to-date than open source).

Programming Languages

Learn a language! Python is a fairly easy language to learn and one of the most popular programming languages in the industry. Additional popular languages include BASH Scripting, C++, and JavaScript.

Check out these free resources to get started:

- freeCodeCamp.org
- Codecademy.com
- LearnPython.org
- Codewars.com

2 Get The JOB

Take a Targeted Approach

Figure out what you want to do, then research companies who hire those positions. Look up a dozen positions and see what requirements are listed. You'll see many commonalities - those are what you want to develop and showcase on your resume.

Be Realistic

Just because you took an online hacking course doesn't mean you are a Penetration Tester or that you should ask for $200k. Yes, cybersecurity professionals are in demand, but that doesn't mean you can ask for whatever you want. There are still hundreds of applicants for each position posted. There is a steep learning curve to enter the industry, and companies spend tens of thousands to train entry-level new hires.

Be Flexible

Be willing to accept shift work or a lower salary to get started. There is plenty of opportunity for growth and development; people move up quickly in this industry. Likewise, if you are coming from another industry, realize that not all of your experience will translate. You may be a "Senior" level in your current role, but if you have no cybersecurity experience, you should probably be looking for junior positions.

The Resume

Hiring teams might only spend a few seconds looking at each application, so it is crucial that your resume is formatted appropriately to quickly demonstrate the skills relevant to the role. A well-crafted resume not only highlights one's ability to mitigate risks and manage security incidents but also demonstrates a commitment to ongoing learning and adaptation in a rapidly evolving field.

Do...

- Add your LinkedIn Profile (if you don't have one, create one).
- Ensure that your LinkedIn profile matches your resume and that you have a professional photo.
- Include Github, Medium, or other sites you have contributed to - be sure to include your handle or direct links.
- Add projects if you do not have formal experience. Include specific tools you used and be prepared to discuss these projects during an interview.
- Be consistent with your formatting.

Do Not...

- Put something on your resume that you cannot speak to. For instance, if I see SIEM under your Skills section, I'm going to ask you about the specific tool you used and what exactly you were doing.
- Add that you are working on 3+ certs. If you are honestly working toward a cert, list an expected date of completion. However, it is unrealistic that you are working toward SEC+, CEH, and CISSP all at the same time. This comes across as either deceitful or as poor judgment.
- Have errors on your resume. This sounds obvious, but nearly half of the applications I review have a spelling mistake, grammatical error, or fail to follow instructions.

Never be dishonest on an application. You are wasting your time and ours. If I see this, not only do I pass on the candidate immediately for my job role, I flag the candidate as Do Not Hire for the entire company.

Acing the Interview

Getting the interview is half the battle. As a hiring manager, I will not spend my time interviewing you if I do not see you as a legitimate candidate. You should be excited to get the opportunity and prepare as much as possible before the interview.

Research the Company

Set yourself apart by doing research on the company and job roles. Companies want to see that you have a good understanding of the industry prior to committing to training you. Look up the company values, business objectives, and mission. Try to understand how the company makes money, or identify challenges the organization is currently facing.

Interacting with the Hiring Team

An important part of interviewing is avoiding pitfalls and red flags to the hiring team. There is an art to interacting with the hiring team. You do not want to harass them. For instance, sending 3 follow-up emails within 24 hours of applying is only hurting your chances. It is okay to send a thank you note, or to even send an email after you submit an application to state your interest and appreciation for consideration. Do NOT send emails every day asking for updates.

You should also know the people. Most likely, your point of contact will be a recruiter, so communicate through them. Be sure to read emails carefully and pay attention to phone calls you receive. It is a VERY bad look if you cannot follow instructions from the start. This sounds simple, but many people we interview fail in this regard.

Discuss Current Events

Understand the industry enough that you can speak confidently. Stay updated on current cyber events. For instance, you should know recent large-scale attacks, new industry trends, and if a particular threat group is becoming more popular, along with security efforts.

Let the Hiring Team Lead the Interview

The interviewing team has specific topics and questions they use to evaluate you. You may be eager to ask questions or discuss your qualifications, but taking over the interview may come off as aggressive or prevent the interviewer from fully evaluating you, which could limit your chances of moving forward.

Come with Questions

Prepare a few questions that are specific to the company and position. This is a good way to show a level of preparation, along with an interest in the role.

Technical Questions

Guiding Principles

- Elaborate. Never just spell out acronyms or give a Yes/No answer.
- Offer multiple methods of security.
- It is okay not to know. In fact, it’s often worse to give an incorrect answer.
- Study for the particular job you’re interviewing for. Review the job description and responsibility - identify particular tools the company uses. If it’s in the offensive space, you’ll want to brush up on port scanning, pentesting methodology, etc. Or if it’s a Vulnerability Management role in the healthcare field, practice with some VM tools and review HITECH/HIPAA.

Additional Practice Questions

1. Explain the OSI model. How does it compare to the TCP/IP model?
2. Explain the CIA triad.
3. Explain APTs and TTPs.
4. Explain the three-way handshake process.
5. Explain the client-server model.
6. What is the difference between a threat, a vulnerability, and an exploit?
7. What is the difference between XSS and CSRF?
8. What is the difference between HTTP and HTTPS?
9. What is the difference between a public and private IP?
10. What is DNS? Explain the security implications of using DNS.
11. What is the most vulnerable asset in an organization?
12. Craft a Linux command that will search through all logs to identify failed login attempts on an Apache web server.
13. What is a common way to prevent web application attacks, such as SQLi, cross-site scripting, and remote file upload?
14. What is a brute force attack and how can you prevent it?
15. What is a ransomware attack and how can you mitigate it?
16. Which is worse – a false positive or false negative? (Careful! This is a trick question; neither is good. It is a balancing act.)

Example Practice Questions

Below are a couple of web security questions and how I would go about answering them.

How would you secure a web server?

There are many things you can do, and many right answers, but try to give a layered approach that addresses the defense-in-depth strategy. For instance, I would discuss:

- Network Security: create a DMZ, filter traffic with a firewall, implement IDS/IPS
- Web Application Security: input validation, limited user account runs web service, consider a third-party ASA
- System Hardening: remove default accounts, implement password policy & MFA, close unused ports, restrict services to only those required, restrict access to only those required, encrypt drives
- Standard Upkeep: frequent backups, patching and updates; set up logging and create alerts for abnormal traffic, known malicious activity, and unusual processes

How does SSL make HTTP secure?

Secure Socket Layer (SSL) has technically been replaced by TLS, but largely used interchangeably. SSL is introduced during layer 6 of the OSI model, following a full TCP connection, to establish an encrypted link between the client and server. During the SSL handshake, the server's identity will be verified by checking the SSL certificate with a third-party Certificate Authority (CA). The handshake will also use asymmetric encryption to discuss and set parameters that will establish a shared session key to use for symmetric encryption (faster). Once the encrypted link is established, the client will send HTTP requests like normal to the server, but in a secure fashion (confidentiality), giving us HTTPS.

Additional Resources

Try a Practice Scenario

Follow the steps below to create a virtual environment containing an attack, a victim, and a monitoring machine. The goal is to attack a vulnerable web application and be able to identify/alert on that attack.

STEP 1

Create Three Test Machines

This may be done through local virtualization (VirtualBox, VMware), Docker containers, or a cloud provider (AWS, Azure, GCP). Install the following operating systems on these three machines:

✓ Kali Linux ✓ CentOS Server ✓ Ubuntu Desktop

STEP 2

Connect All Three Test Machines

You can do this by creating a private subnet or through public IPs (if using cloud provider). All three need to be able to communicate between one another.

STEP 3

Download and Install Tools

- Install a vulnerable application, such as DVWA, Broken Crystals, or Juice Shop, on the CentOS Server.
- Set up a SIEM on the Ubuntu Desktop.

STEP 4

Open Ports & Check Web Apps

- You should be able to reach the vulnerable web application via a browser on the Kali box.
- You should be able to sign into the SIEM via a browser (on the Ubuntu Desktop).

STEP 5

Set Up Forwarding To SIEM

- Open a SIEM listener port on the Ubuntu Desktop.
- Forward appropriate httpd logs from the CentOS server.
- Confirm traffic from the CentOS web application logs is populating in the SIEM.

STEP 6

Use Kali Linux To Attack/Detect in SIEM

- Conduct a brute force attack on the vulnerable web application from the Kali box.
- Identify the populated events in the SIEM.

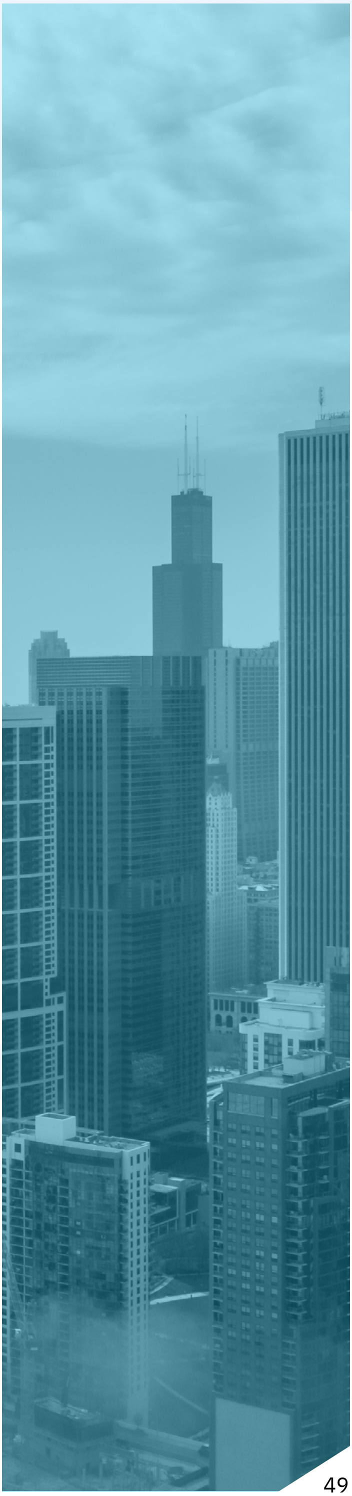
STEP 7

Create Alerts in SIEM

- Create a real-time alert in the SIEM to notify on potential brute-force attacks.
- Consider alerting for multiple failed logins of a single user, as well as many failed logins coming from a single source.

BONUS: Conduct a command injection or SQLi attack on the vulnerable web app. See if you identify the attack in your SIEM. Take it one step further and create an alert for similar activity.

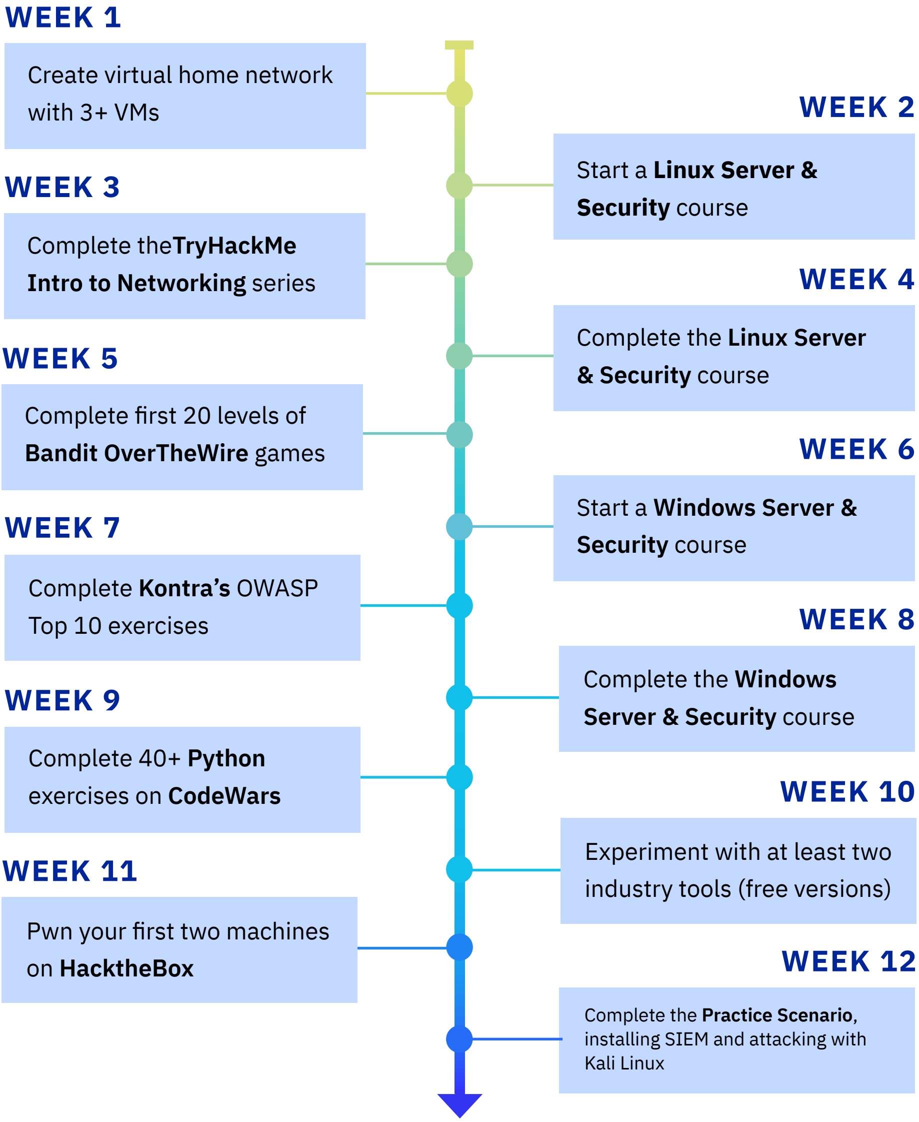
Creating a Training Plan



Starting the path into the cybersecurity field can be overwhelming, so create a training plan to help you stay on track! Be sure to make a plan that is realistic (don't expect to get CISSP during week 1) and evaluate yourself as you progress. It is okay if your goals change but ensure that you have set study times weekly, and that you are actually learning during those times.

Below is an example training plan for someone who can spend 1-2 hours daily developing their cybersecurity skills. You can use this as a framework to get started, but your plan should be personalized based on your current knowledge and situation.

Example Training Plan



WEEK 1

Create virtual home network with 3+ VMs

WEEK 2

Start a **Linux Server & Security** course

WEEK 3

Complete the**TryHackMe Intro to Networking** series

WEEK 4

Complete the **Linux Server & Security** course

WEEK 5

Complete first 20 levels of **Bandit OverTheWire** games

WEEK 6

Start a **Windows Server & Security** course

WEEK 7

Complete **Kontra's** OWASP Top 10 exercises

WEEK 8

Complete the **Windows Server & Security** course

WEEK 9

Complete 40+ **Python** exercises on **CodeWars**

WEEK 10

Experiment with at least two industry tools (free versions)

WEEK 11

Pwn your first two machines on **HacktheBox**

WEEK 12

Complete the **Practice Scenario**, installing SIEM and attacking with Kali Linux

PASS CERTIFICATION EXAM!

GuidePoint Security

GuidePoint Security provides cybersecurity expertise, solutions, and services that help organizations make better decisions and minimize risk. We act as your trusted advisor to understand your business and challenges, helping you through an evaluation of your cybersecurity posture and ecosystem to expose risks, optimize resources and implement best-fit solutions.

GuidePoint Security University

GuidePoint Security University (GPSU) is a training and development pipeline to help those interested in a cybersecurity career develop critical industry skills and apply cyber knowledge to develop real-world solutions. GPSU has an internship component, which is tailored to create an individualized experience based on your background and aptitude that teaches both technical and soft skills.

Pre-requisites for the GuidePoint Security University Training Program

The below skills are required prior to entering a GPSU technical training program.

- ✓ Understanding of the OSI model, including common ports and protocols
- ✓ General understanding of network architecture and devices
- ✓ Ability to create a virtual machine and network
- ✓ Able to navigate the Linux terminal
- ✓ Knowledge of common attack types
- ✓ Familiarity with cyber acronyms and language
- ✓ Ability to write simple functions with a common programming language

Additional skills are required based on the specialty chosen.

CONTACT INFORMATION:

GPSU@guidepointsecurity.com
Find out more at **www.guidepointsecurity.com/gpsu**

GUIDEPOINT
SECURITY
UNIVERSITY

2201 Cooperative Way, Suite 225, Herndon, VA 20171
guidepointsecurity.com • info@guidepointsecurity.com • (877) 889-0132
09.2024