

Starting Cybersecurity Training with No IT Background:

Navigating the Learning Curve part I:

- I have been in IT well over 20 years, I have taken multiple courses in relating to the IT industry and now I have been in cybersecurity for 5 years.
- In today's digital landscape, cybersecurity plays a vital role in protecting our data and systems from malicious actors.
- Today, I want to address the challenges faced by individuals who are new to cybersecurity but have no previous experience in IT. I will also provide guidance on how to overcome these challenges and embark on a successful cybersecurity training journey.

I. Understanding the Challenge:

- It is true that starting cybersecurity training without an IT background can be challenging.
- Without foundational knowledge of IT concepts, individuals may struggle to grasp the intricacies of securing and protecting network infrastructure.
- However, with the right approach and resources, it is possible to bridge this gap and thrive in the cybersecurity field. Let me be clear; I am not saying it will be easy and by no means "it will be"; there are many, many terminologies involving cybersecurity, that if you hear all these training companies promising you a 6 figure job, it is all "crap", at least I advise you to get CompTia A+ certify! Learn the fundamentals.

II. Building the Foundation: A. Exploring Fundamental IT Knowledge:

- Gaining a basic understanding of IT concepts is crucial. This includes learning about computer networks, operating systems, and protocols.
- Online courses, tutorials, and books offer excellent resources for beginners to learn the basics of IT.

B. Focus on Networking Concepts:

- Networking knowledge is a fundamental pillar of cybersecurity. Concepts such as IP addressing, subnetting, routing, and network protocols are essential to secure network infrastructure effectively.
- Online courses, practice labs, and networking textbooks provide valuable resources for building this foundational knowledge.

III. Bridging the Gap: A. Entry-Level IT Roles:

- Consider starting with entry-level IT roles, such as help desk support or network administration. These roles provide practical experience and exposure to IT infrastructure.
- For example, someone without an IT background can gain hands-on experience by working in a help desk role, troubleshooting network issues, and learning about different technologies.

B. Cybersecurity Certifications:

- Pursuing entry-level cybersecurity certifications can provide a structured learning path and validate your knowledge.
- Certifications like CompTIA Security+, Certified Information Systems Security Professional (CISSP), or Certified Ethical Hacker (CEH) are excellent starting points.
- These certifications demonstrate your commitment to learning and provide credibility in the field.

C. Hands-On Practice:

- Engage in practical exercises and hands-on projects to apply theoretical knowledge.
- Setting up a home lab or using virtual environments allows you to practice configuring routers, implementing security controls, and performing vulnerability assessments.
- Document your findings and progress to showcase your practical skills.

IV. Leveraging Resources: A. Networking and Mentoring:

- Engage with professionals in the cybersecurity field by attending conferences, joining online forums, and participating in local meetups.
- Networking provides opportunities to learn from experienced individuals, gain insights, and potentially find mentors who can guide you on your cybersecurity journey.

V. Conclusion:

- Starting cybersecurity training with no IT background may present challenges, but it is certainly achievable.
- By building a solid foundation in IT concepts, exploring networking knowledge, gaining practical experience, pursuing certifications, and leveraging networking opportunities, you can overcome these challenges and succeed in the cybersecurity field.

Embrace the learning journey, stay dedicated, and continuously update your skills to keep pace with the evolving cybersecurity landscape. **Navigating the Learning Curve**

Part II: what you would need to know to be able to succeed as a cybersecurity analyst.

This is by no mean an exhaustive list but some good point to take into account if you really want to pursue a career in this field.

Below are some technical skills you should have if you want to get into cybersecurity:

Securing a Router

Securing a router is essential to protect your home network from unauthorized access and potential cyber threats. Here are some steps you can take to enhance the security of your router:

1. **Change the default admin password:** One of the first things you should do is change the default admin password of your router. This prevents unauthorized access to the router's settings and ensures that only authorized individuals can make changes.
2. **Change the Wi-Fi network password:** It is crucial to change the default Wi-Fi network password to a strong and unique password. This prevents unauthorized users from connecting to your network and helps protect your devices and information..
3. **Enable encryption:** Enable encryption on your Wi-Fi network to secure the data transmitted between your devices and the router. The recommended encryption protocol is WPA3, which provides stronger security than older protocols like WPA2..
4. **Disable remote management:** Disable remote management of your router to prevent unauthorized access from outside your home network. This ensures that only devices connected to your network can manage the router's settings.
5. **Keep the router firmware up to date:** Regularly check for firmware updates from the router manufacturer and install them promptly. Firmware updates often include security patches that address vulnerabilities and improve the overall security of the router..
6. **Disable UPnP (Universal Plug and Play):** UPnP can be a potential security risk as it allows devices on your network to automatically open ports and communicate with the internet. It is recommended to disable UPnP unless it is necessary for specific applications.
7. **Use a strong network password:** Ensure that your network password is strong and unique. Avoid using common passwords or personal information that can be easily guessed. A strong password should be a combination of uppercase and lowercase letters, numbers, and special characters..

8. **Enable network encryption:** Use encryption protocols like WPA2 or WPA3 to encrypt the data transmitted over your network. Encryption adds an extra layer of security and prevents unauthorized access to your network..
9. **Disable SSID broadcasting:** By disabling SSID broadcasting, you make your network less visible to potential attackers. This means that users will need to manually enter the network name (SSID) to connect to your Wi-Fi network..
10. **Enable MAC address filtering:** MAC address filtering allows you to specify which devices are allowed to connect to your network based on their unique MAC addresses. By enabling this feature, you can restrict access to your network to only trusted devices.

To effectively protect a router, a cybersecurity analyst should have knowledge in the following areas:

1. **Router Configuration:** Understanding how routers work and being familiar with their configuration settings is crucial. This includes knowledge of router interfaces, protocols, and services.
2. **Network Security:** A cybersecurity analyst should have a strong understanding of network security principles and best practices. This includes knowledge of encryption protocols, firewall configurations, access control lists (ACLs), and network segmentation.
3. **Router Vulnerabilities:** Being aware of common router vulnerabilities is essential for protecting against potential attacks. This includes knowledge of common exploits, such as default credentials, firmware vulnerabilities, and misconfigurations.
4. **Firmware Updates:** Keeping router firmware up to date is critical for addressing known vulnerabilities and ensuring the latest security patches are applied. Understanding how to check for firmware updates and how to apply them is important.
5. **Authentication and Access Control:** Knowledge of authentication mechanisms, such as passwords and access control lists, is necessary for securing router access. This includes understanding the importance of strong passwords, multi-factor authentication, and limiting access to authorized individuals.
6. **Wireless Security:** Understanding wireless security protocols, such as WPA2 or WPA3, and their configurations is important for securing Wi-Fi networks. This includes knowledge of encryption, SSID hiding, and disabling unnecessary features like Wi-Fi Protected Setup (WPS).
7. **Logging and Monitoring:** Knowing how to enable and configure router logging and monitoring features is crucial for detecting and responding to potential security incidents. This includes understanding log analysis, intrusion detection systems (IDS), and security event management.
8. **Router Hardening:** Implementing router hardening techniques is essential for reducing the attack surface and enhancing security. This includes disabling unnecessary services, closing unused ports, and implementing access control measures.

9. **Security Auditing and Compliance:** Understanding security auditing processes and compliance requirements is important for ensuring routers meet industry standards and regulatory guidelines. This includes knowledge of security frameworks, such as NIST or ISO 27001, and conducting security assessments.
10. **Emerging Threats and Trends:** Staying updated on the latest cybersecurity threats, trends, and emerging technologies is crucial for a cybersecurity analyst. This includes knowledge of new attack vectors, vulnerabilities, and security solutions.

Remember, securing a router is an ongoing process, and it requires continuous monitoring, updates, and adaptation to evolving threats.

As a cybersecurity analyst, you should already know what is being discussed above, if you have no idea what the above points are, then you need to go to the basics, again at least be A+ certified, or you will have a hard time understanding any branch of cybersecurity.

.....

To effectively protect a switch, a cybersecurity analyst should know the following:

1. **Switch Security Features:** Understand the security features provided by the switch, such as VLANs (Virtual Local Area Networks), access control lists (ACLs), port security, and MAC address filtering. These features help control access and secure network traffic.
2. **Switch Management:** Be familiar with the switch's management interface and protocols, such as SNMP (Simple Network Management Protocol) and SSH (Secure Shell). Understanding how to securely configure and manage the switch is essential for maintaining its security.
3. **Default Configurations:** Default configurations can pose security risks. It is important to change default passwords, disable unnecessary services, and review default VLAN configurations to ensure they align with security best practices.
4. **Firmware Updates:** Keeping the switch's firmware up to date is crucial for addressing known vulnerabilities and ensuring the latest security patches are applied. Regularly check for firmware updates from the manufacturer and apply them promptly.
5. **Port Security:** Implement port security measures to prevent unauthorized devices from connecting to switch ports. This includes techniques like MAC address filtering, limiting the number of MAC addresses per port, and enabling sticky MAC addresses.
6. **Monitoring and Logging:** Enable logging and monitoring features on the switch to detect and respond to potential security incidents. This includes monitoring network traffic, analyzing logs, and setting up alerts for suspicious activities.
7. **Physical Security:** Physical security is often overlooked but critical. Ensure that the switch is physically secured in a locked cabinet or room to prevent unauthorized access or tampering.

8. **Network Segmentation:** Understand the concept of network segmentation and how to implement it using VLANs. Network segmentation helps isolate different parts of the network, limiting the impact of a security breach.
9. **Switch Hardening:** Implement switch hardening techniques to reduce the attack surface and enhance security. This includes disabling unused ports, enabling port security features, and configuring secure management access.
10. **Security Auditing and Compliance:** Understand security auditing processes and compliance requirements to ensure that the switch meets industry standards and regulatory guidelines. This includes conducting security assessments and implementing necessary controls.

Remember, securing a switch requires a combination of technical knowledge, best practices, and ongoing monitoring. Regularly review and update the switch's configurations and security measures to adapt to evolving threats. Get yourself a used switch and a router, build a lab, get hands on!

Here is how to protect a switch, a cybersecurity analyst can follow these steps and use the following tools:

1. **Configure Port Security:** Enable port security features to protect against unauthorized devices being connected to the network. This can include techniques like MAC address filtering and limiting the number of MAC addresses per port.
2. **Implement VLANs:** Use Virtual Local Area Networks (VLANs) to segment the network and control access between different network segments. This helps isolate traffic and restrict unauthorized access.
3. **Enable Access Control Lists (ACLs):** ACLs can be used to filter and control network traffic based on specific criteria, such as IP addresses, port numbers, or protocols. They help prevent unauthorized access and protect against network threats.
4. **Secure Management Access:** Enable secure management protocols like SSH (Secure Shell) and disable insecure protocols like Telnet. This ensures that management communications with the switch are encrypted and protected.
5. **Firmware Updates:** Regularly update the switch's firmware to address known vulnerabilities and apply security patches. This helps protect against potential exploits and ensures the switch is running the latest security enhancements.
6. **Monitoring and Logging:** Enable logging and monitoring features on the switch to detect and respond to potential security incidents. This includes monitoring network traffic, analyzing logs, and setting up alerts for suspicious activities. Network monitoring tools like Argus, Nagios, or Splunk can be used for this purpose.
7. **Physical Security:** Ensure that the switch is physically secured in a locked cabinet or room to prevent unauthorized access or tampering. Physical security measures are essential to protect the switch from physical attacks.
8. **Network Access Control (NAC):** Implement NAC solutions like Cisco ISE or ForeScout NAC to enforce network access policies and ensure that only

authorized devices and users can connect to the network. These tools provide advanced security features for controlling network access.

Remember, the specific tools used may vary depending on the organization's requirements and the complexity of the network. It's important to select tools that align with the organization's security goals and ensure they are used in accordance with legal and ethical guidelines.

.....

Servers:

To protect a server, a cybersecurity analyst should know the following:

1. **Server Hardening:** Implement server hardening techniques to reduce vulnerabilities and enhance security. This includes disabling unnecessary services, applying security patches, and configuring access controls.
2. **Access Control:** Implement strong access control measures to ensure that only authorized individuals have access to the server. This includes using strong passwords, implementing multi-factor authentication, and regularly reviewing user privileges.
3. **Patch Management:** Regularly apply security patches and updates to the server's operating system, software, and applications. This helps address known vulnerabilities and protect against potential exploits.
4. **Secure Configuration:** Configure the server securely by following industry best practices and security guidelines. This includes disabling unnecessary protocols, configuring secure communication channels, and enabling appropriate logging and monitoring.
5. **Backup and Recovery:** Implement regular backup procedures to ensure that critical data is protected and can be restored in the event of a security incident or system failure. Test the backup and recovery processes to ensure their effectiveness.
6. **Intrusion Detection and Prevention:** Deploy intrusion detection and prevention systems (IDS/IPS) to monitor network traffic and detect potential security breaches. These systems can help identify and respond to malicious activities in real-time.
7. **Security Auditing and Logging:** Enable logging and auditing features on the server to track and monitor security events. Regularly review logs for suspicious activities and security incidents.
8. **Vulnerability Scanning:** Conduct regular vulnerability scans on the server to identify potential weaknesses and security gaps. Use tools like Nessus, OpenVAS, or Qualys to perform comprehensive vulnerability assessments.
9. **Antivirus and Malware Protection:** Install and regularly update antivirus and anti-malware software on the server to detect and remove malicious software. Use reputable security solutions that provide real-time protection and regular signature updates.
10. **Security Information and Event Management (SIEM):** Implement a SIEM solution to centralize and analyze security event logs from various sources. SIEM

tools like Microsoft Sentinel, Splunk, ArcSight, or ELK Stack can help identify patterns, detect anomalies, and facilitate incident response.

Remember, the specific tools used may vary depending on the organization's requirements and the server's operating system. It's important to select tools that align with the organization's security goals and ensure they are used in accordance with legal and ethical guidelines.

When it comes to choosing an Intrusion Detection and Prevention System (IDPS) for server protection, there are several options available. Here are a few examples:

1. **Snort:** Snort is a widely used open-source IDPS that can detect and prevent network-based attacks. It offers real-time traffic analysis, signature-based detection, and can be customized with additional rules to suit specific security needs.
2. **Suricata:** this is another open-source IDPS that provides network intrusion detection and prevention capabilities. It supports multi-threading, high-speed packet processing, and can detect a wide range of network-based threats.
3. **Cisco Firepower:** Cisco Firepower is a comprehensive network security solution that includes IDPS functionality. It offers advanced threat detection, real-time threat intelligence, and automated response capabilities.
4. **Palo Alto Networks Next-Generation Firewall:** Palo Alto Networks offers a range of next-generation firewalls that include integrated IDPS features. These firewalls provide advanced threat prevention, application visibility, and granular control over network traffic.
5. **Trend Micro Deep Security:** Trend Micro Deep Security is a security platform that includes IDPS capabilities. It offers host-based intrusion detection and prevention, virtual patching, and integrates with other security tools for comprehensive server protection.
6. **McAfee Network Security Platform:** McAfee Network Security Platform provides network-based IDPS functionality. It offers real-time threat detection, advanced analytics, and can be deployed as a physical or virtual appliance.

Remember, the choice of IDPS depends on various factors such as the organization's specific requirements, budget, and the level of expertise available for managing and maintaining the system. It's important to evaluate different solutions and select the one that best fits the organization's security needs.

.....

To protect an endpoint, such as a computer or mobile device, a cybersecurity analyst should know the following:

1. **Endpoint Protection Software:** Install and regularly update endpoint protection software, such as antivirus and anti-malware solutions. These tools help detect and remove malicious software that could compromise the security of the endpoint. Examples include:

- **Symantec Endpoint Protection:** Provides advanced threat protection, including antivirus, firewall, and intrusion prevention capabilities.
 - **McAfee Endpoint Security:** Offers comprehensive protection against malware, ransomware, and other threats.
 - **Kaspersky Endpoint Security:** Provides multi-layered protection against various types of cyber threats.
2. **Patch Management:** Regularly apply security patches and updates to the operating system and software installed on the endpoint. This helps address known vulnerabilities and protect against potential exploits. Examples of patch management tools include:
- **Microsoft WSUS (Windows Server Update Services):** Allows centralized management and distribution of updates for Microsoft products.
 - **Ivanti Patch:** Provides automated patch management for various operating systems and third-party applications.
3. **Endpoint Encryption:** Implement endpoint encryption to protect sensitive data in case of loss or theft. This ensures that even if the device falls into the wrong hands, the data remains secure. Examples of endpoint encryption tools include:
- **BitLocker:** A built-in encryption feature in Windows operating systems.
 - **FileVault:** A built-in encryption feature in macOS.
4. **Endpoint Detection and Response (EDR):** Deploy EDR solutions to monitor and respond to advanced threats on endpoints. These tools provide real-time visibility into endpoint activities and help detect and respond to security incidents. Examples include:
- **CrowdStrike Falcon:** Offers advanced threat detection, incident response, and endpoint protection capabilities.
 - **Carbon Black:** Provides endpoint security and EDR solutions to detect and respond to advanced threats.
5. **Mobile Device Management (MDM):** For mobile endpoints, implement MDM solutions to enforce security policies, manage device configurations, and remotely wipe data if necessary. Examples of MDM tools include:
- **Microsoft Intune:** Offers cloud-based mobile device and application management for iOS, Android, and Windows devices.
 - **VMware Workspace ONE:** Provides unified endpoint management for mobile devices, desktops, and applications.

Remember, the specific tools used may vary depending on the organization's requirements and the type of endpoints being protected. It's important to select tools that align with the organization's security goals and ensure they are used in accordance with legal and ethical guidelines.

.....

In my opinion, a technical analyst, Level 1 up to Administrator, including Cybersecurity analyst, should know the OSI model; this really helps in your troubleshooting analysis.

The OSI (Open Systems Interconnection) model is like a set of rules that helps computers talk to each other and share information. It's divided into seven layers, and each layer has a special job to do. Let's imagine it like building a cake!

1. **Physical Layer:** This is the bottom layer, like the cake base. It's all about the physical stuff, like the wires and cables that connect computers. It makes sure the information can travel through the wires properly. (bits)
2. **Data Link Layer:** This layer is like the yummy filling between the cake layers. It takes the information and organizes it into small pieces called "frames." It also checks if the information has any mistakes.
3. **Network Layer:** This layer is like the frosting on the cake. It adds special addresses to the information, called IP addresses, so it knows where to go. It helps the information find its way across different networks. (packets)
4. **Transport Layer:** This layer is like the cake slices. It takes the information and breaks it into smaller pieces called "segments." It also puts numbers on each piece, so they can be put back together correctly.
5. **Session Layer:** This layer is like the party planner. It helps different applications on different computers start, have a conversation, and say goodbye when they're done.
6. **Presentation Layer:** This layer is like the language translator. It makes sure the information looks the same on different computers, even if they speak different languages. It can also make the information secret and safe.
7. **Application Layer:** This is the top layer, like the decorations on the cake. It includes all the fun stuff we do on computers, like playing games, browsing the internet, and sending emails.

So, the OSI model is like building a cake with different layers. Each layer has a special job to make sure the information gets from one computer to another. Just like a cake needs all its layers to be delicious, computers need all the layers of the OSI model to communicate properly. There are many examples explaining the OSI model, I invite you to do a more in depth study on it.

.....

Having a solid IT background, including knowledge of networking concepts like IP addresses, subnetting, and router functionality, can be beneficial for a cybersecurity analyst. Understanding these foundational concepts allows analysts to better secure and protect network infrastructure. Having a basic understanding of how routers function, what IP addresses are, and how subnetting works enables analysts to identify potential vulnerabilities and implement appropriate security measures. It helps them configure routers, set up secure network architectures, and detect and respond to network threats effectively. While it is ideal for a cybersecurity analyst to have a strong IT background, it is not an absolute requirement. Some individuals may enter the field with limited IT knowledge and acquire the necessary skills through dedicated learning

and practical experience. They can start by gaining a solid understanding of networking fundamentals and gradually expand their knowledge in cybersecurity-specific areas. Certifications like CompTIA Network+ or Cisco Certified Network Associate (CCNA) can provide a comprehensive understanding of networking concepts and serve as a valuable foundation for a cybersecurity career. These certifications cover topics such as IP addressing, subnetting, and router configuration. In summary, while a solid IT background is advantageous for a cybersecurity analyst, individuals without prior IT experience can still enter the field by actively learning and acquiring the necessary knowledge and skills. It is important to continuously learn, stay updated with industry trends, and gain practical experience to excel in the cybersecurity domain.

The learning curve:

Individuals without prior IT background may face a steeper learning curve when entering the cybersecurity field. The absence of foundational knowledge can pose some challenges initially. However, with dedication and a structured learning approach, it is still possible to bridge the gap and succeed in cybersecurity.

Foundational IT Knowledge: Start by gaining a solid understanding of fundamental IT concepts. This includes learning about computer networks, operating systems, protocols, and basic hardware concepts. Online courses, tutorials, and books can provide structured learning resources.

1. **Focus on Networking Concepts:** Networking is an essential aspect of cybersecurity. Invest time in thoroughly understanding networking concepts such as IP addressing, subnetting, routing, and network protocols. Resources like online courses, practice labs, and networking textbooks can help in building this foundation.
2. **Seek Entry-Level IT Roles:** Consider starting with entry-level IT roles, such as help desk support or network administration, to gain hands-on experience and practical exposure to IT infrastructure. These roles can provide valuable insights into network configurations, troubleshooting, and security considerations.
3. **Cybersecurity Certifications:** Pursue entry-level cybersecurity certifications that focus on foundational knowledge. Certifications like CompTIA Security+, Certified Information Systems Security Professional (CISSP), or Certified Ethical Hacker (CEH) can provide a structured learning path and validate your knowledge.
4. **Hands-On Practice:** Engage in practical exercises and hands-on projects to apply theoretical knowledge. Build a home lab or use virtual environments to practice configuring routers, implementing network security controls, and performing vulnerability assessments.
5. **Networking and Mentoring:** Engage with professionals in the field, join cybersecurity communities, and seek mentoring opportunities. Networking can provide guidance, mentorship, and opportunities to learn from experienced individuals who can share their insights and experiences.

Remember, while the learning curve may be challenging, it is not insurmountable. With persistence, continuous learning, and practical experience, individuals without prior IT background can acquire the necessary knowledge and skills to succeed in the cybersecurity field. Take it one step at a time and embrace the learning journey.