🛠️ Hacker Roadmap

Hack, Dominate & Own the Web 💀⚡

-By Codelivly

CODELIVLY

LEARN CYBERSECURITY

Growing up in the 90s inundated me with images of hackers portrayed as mysterious, hoodie-clad figures breaking into systems with a few keystrokes. Little did I know then that this portrayal wasn't far from reality, albeit with a twist. Today, as someone deeply immersed in the tech industry, I've come to appreciate ethical hacking as one of the most captivating fields out there.

Ethical hacking isn't just about breaking into systems; it's a dynamic blend of strategy, problem-solving, and constant learning. Picture it as an ongoing chess match between security measures and potential vulnerabilities. You're either honing your skills to penetrate systems and uncover flaws or fortifying defenses to keep would-be intruders at bay.

In this guide, I'll take you on a journey through the essential skills and requirements needed to become an Ethical Hacker. We'll delve into how to acquire these skills, addressing common questions along the way.

So, whether you're a coding novice or a seasoned tech enthusiast, by the end of this guide, you'll be well-equipped to kickstart your journey into the captivating realm of Ethical Hacking. So, grab a coffee, settle in, and let's embark on this exciting adventure together! This is not your normal article. We got most of the topic covered here...

Why to Choose Ethical Hacking for Career?

So why should you consider diving into the world of ethical hacking for your career? Well, let me break it down for you.

First off, ethical hacking is like being a digital detective. You get to uncover all the sneaky tricks hackers use to break into systems, but here's the kicker - you're the good guy. You're using your skills to protect companies and organizations from getting hacked.

Imagine this: You're getting paid to play the ultimate game of cat and mouse. Hackers are constantly coming up with new ways to break into systems, and it's your job to

outsmart them. It's like being in a never-ending puzzle-solving adventure, and who wouldn't want to get paid for that?

Plus, the money's pretty good in this field. Companies are willing to shell out big bucks to keep their systems secure, which means you can make a decent living doing what you love.

But here's the best part - there's always something new to learn. Technology is always evolving, which means there are endless opportunities to expand your skills and stay ahead of the game.

So, if you're someone who loves a challenge, enjoys problem-solving, and wants to make a difference in the digital world, ethical hacking might just be the perfect career for you.

What Is the Attraction of an Ethical Hacking Career?

The allure of an ethical hacking career is like being drawn to a mystery waiting to be solved.

For starters, there's the thrill of the chase. Ethical hackers get to play the role of cyber detectives, hunting down vulnerabilities before the bad guys do. It's a constant battle of wits, where every exploit uncovered feels like a victory for the good guys.

Then there's the intellectual challenge. Ethical hacking is a field that constantly pushes you to think outside the box. You're not just following a set script; you're using your creativity and problem-solving skills to outsmart the hackers. It's like being in a never-ending game of chess, where every move counts.

But perhaps the most rewarding aspect is the sense of purpose. In a world where cyber threats are ever-present, ethical hackers are the unsung heroes, quietly working behind the scenes to keep our digital world safe. Knowing that your work is making a difference, protecting businesses and individuals from harm, is incredibly gratifying.

And let's not forget the perks. Ethical hacking offers competitive salaries, ample job opportunities, and the flexibility to work in various industries. Plus, there's the satisfaction of being part of a community of like-minded individuals, sharing knowledge and collaborating to tackle new challenges.

How long does it take to become an Ethical Hacker?

Becoming an ethical hacker can be a bit like leveling up in a video game—it depends on how far you want to go and how quickly you can pick up new skills. If you're aiming for a junior position, you could get the basics down pat in as little as 3 to 6 months, or even faster if you're a quick learner.

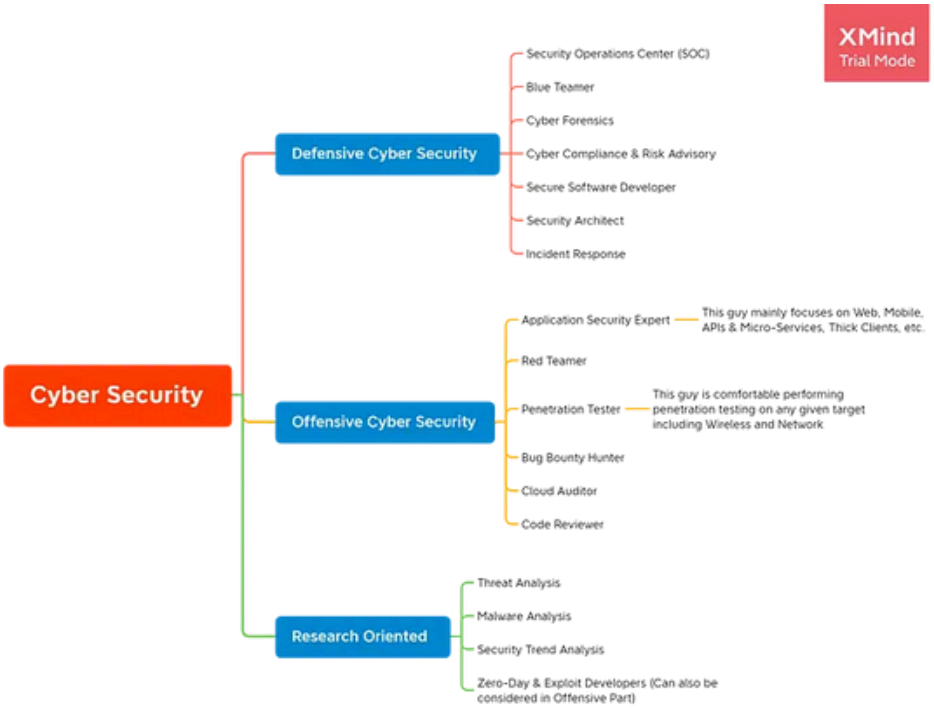
But here's the thing: The journey doesn't stop there. If you're eyeing more senior or specialized roles, you'll need to keep leveling up your skills and gaining real-world experience. That might mean diving deeper into specific areas of cybersecurity or racking up a few years of hands-on practice.

My advice? Start by mastering the essentials to get your foot in the door, then hit the ground running. The sooner you start gaining experience, the sooner you can start climbing the ladder to higher-paying positions.

Types of Job Roles For Ethical Hackers

Ethical hackers have a diverse range of job roles to choose from, each with its own set of responsibilities and requirements. Here's a rundown of some common job roles you might encounter in the world of ethical hacking:

Let's Understand these Job Roles …



1. Ethical Hacker / Penetration Tester:

- Hacking for good with written permission.
- Simulation Attacks on Network.
- Tries Not to Harm the infrastucture during Live attacks.
- Takes care of informative to High impact bugs.
- Provides a full test report and finding (Report writting).
- Need Good Communication skills.
- Part of Red team’

2. Chief information Security Officer (CISO)

- Head of Security Team
- Directs the Strategy, operations & Budget for security.
- Responsible for major Security Decisions

3. Malware Analyst

- Identifies malware in a Computer or Network.
- Reverse Engineer malware to understand its functionality.
- Identifies ways to detect and prevent the malware from spreading.

4. Exploit Developer

- Researches vulnerabilities in software and systems.
- Develops specialized code to exploit identified vulnerabilities.
- Tests and refines exploit code for effectiveness and safety.
- Collaborates with security teams to validate findings and enhance defenses.
- Contributes to improving overall security posture of organizations.

5. Incident Responder / Forensic Analyst

- Helps to analyze/recover erased/encrypted data.
- Analyzes and Monitors all network activities and logs.
- Helps to identify intrusions or suspicious activities inside network.
- Part of Blue Team.
- Works with Red team to fix the Bugs and Vulnerabilities

6. Cryptographer

- Designs and analyzes cryptographic algorithms and protocols.
- Develops encryption and decryption techniques to secure data.
- Conducts research to stay ahead of emerging cryptographic threats.
- Collaborates with security teams to implement cryptographic solutions.

7. Security Researchers

- Conducts in-depth analysis of security vulnerabilities and threats.
- Identifies weaknesses in software, systems, and networks.

- Explores new attack vectors and trends in cyber threats.
- Collaborates with security teams to develop mitigation strategies.
- Contributes to the advancement of cybersecurity knowledge through research and publications.

8. Security Architect

- Designs and implements security solutions for organizations.
- Develops architecture to protect against cyber threats.
- Collaborates with stakeholders to understand security requirements.
- Evaluates and selects security technologies and products.

9. Security Engineer

- Implements and maintains security technologies within organizations.
- Configures and manages firewalls, intrusion detection systems, and encryption tools.
- Troubleshoots security issues and responds to incidents.
- Collaborates with other IT teams to integrate security controls.
- Implements security policies and procedures to mitigate risks.

10. Security Analyst

- Monitors and analyzes security events and incidents.
- Detects and responds to security breaches and threats.
- Conducts forensic investigations to determine the root cause of incidents.
- Generates reports and recommendations for improving security posture.
- Works closely with other IT teams to implement security controls and measures.

11. Security Operation Center (SOC)

- Security Operations Center (SOC) monitors and manages organization's security.
- Analysts detect, investigate, and respond to security incidents.
- They use specialized tools to monitor networks for threats.
- SOC plays a critical role in maintaining overall security.

Before We Begin…

The world of cybersecurity, with its various branches like ethical hacking, application security, penetration testing, and bug bounties, is gaining popularity among people of all ages and backgrounds worldwide.

Yet, for beginners, entering this domain can seem like stepping into an ocean. Where should one start? What should be learned first? The sheer amount of information can be overwhelming, leading to doubts and questions like, "Will it take years for me to catch up?" or "Is there a shortcut, or should I just give up?"

As someone who often receives such inquiries, I understand the confusion and uncertainty. Hence, this blog aims to address these questions and provide a concise learning path based on my perspective on how to start a journey in cybersecurity.

Cybersecurity is vast and encompasses various career options. When someone mentions cybersecurity, it may not always be clear which specific domain they are referring to. It could be bug bounty hunting, blue teaming, cyber forensics, or something else entirely. Therefore, let's first break down some general career options in cybersecurity to help you clarify your goals.

But before we delve into resources, there are a few crucial points I must emphasize. Firstly, building a strong foundation in IT is paramount before delving into advanced hacking techniques. Think of your hacking career as a house—without a solid foundation, it's prone to collapse. Similarly, skipping foundational skills can leave you feeling lost and overwhelmed, potentially discouraging you from pursuing the hacker path.

Secondly, ethical hacking is undoubtedly an enticing field. It offers the allure of getting paid to break into networks, applications, and even physical buildings. The high salaries in this field reflect the demand for skilled professionals. However, it's essential to recognize that choosing a career solely for financial gain is misguided. Hacking requires dedication, constant learning, and a genuine passion for the craft. Simply put, if hacking excites you, the money is just a bonus. But remember, complacency has no place in this field. You must be prepared to be a lifelong learner, staying abreast of new exploits and defenses to remain competitive.

Start the Journey

If you're just starting to explore the realms of hacking, it's essential to build a solid foundation of basic knowledge. Here's a roadmap to get you started:

1. ***Computer Fundamentals:***

Computer fundamentals encompass a wide range of skills, including the ability to build, troubleshoot, and maintain computer systems. This skillset is essential for roles in help desk support and lays a solid foundation for further IT and cybersecurity studies. Here's what you should focus on:

- **Building a Computer:** Learn how to assemble a computer from individual components such as the motherboard, CPU, RAM, storage drives, power supply, and peripherals. Understand how these components interact to create a functional system.
- **Identifying Parts:** Familiarize yourself with the various components of a computer and their functions. This includes understanding the role of the CPU (Central Processing Unit), RAM (Random Access Memory), GPU (Graphics Processing Unit), motherboard, hard drives (HDDs and SSDs), optical drives, and expansion cards.
- **Troubleshooting and Fixing Issues:** Develop the ability to diagnose and resolve common hardware and software issues that computer users encounter. This includes troubleshooting problems with hardware components, operating system errors, driver issues, and software conflicts.

To gain proficiency in computer fundamentals, consider pursuing certifications such as the CompTIA A+ certification (current version 220-1101 & 220-1102). This certification is widely recognized in the IT industry and covers essential topics related to hardware, software, networking, and security.

If you're new to IT and starting from scratch, here are some recommended resources to help you get started:

- **CompTIA A+ Certification Study Guide:** Utilize study guides specifically designed for the CompTIA A+ certification exam. These guides cover all the topics you need to know to pass the exam and build a strong foundation in computer fundamentals.
- **Online Courses:** Enroll in online courses that offer comprehensive training in computer hardware, software, and troubleshooting skills. Look for courses that include hands-on labs and practical exercises to reinforce your learning.
- **Practice Labs:** Set up a home lab environment where you can practice building and troubleshooting computers. Use virtualization software to simulate different hardware configurations and operating systems, allowing you to gain hands-on experience in a safe and controlled environment.

2. ***Operating System:***

An operating system (OS) is the foundation of any computer system, facilitating communication between hardware and software. Understanding both Windows and Linux operating systems is crucial for aspiring cybersecurity professionals. Here's what you should focus on:

- **Windows OS:** Familiarize yourself with the various versions of the Windows operating system, including their features, improvements, and differences. Don't be afraid to encounter errors; every possible issue has likely been discussed online, providing ample resources for troubleshooting. Practice performing day-to-day tasks in the Windows OS environment and gain proficiency in basic troubleshooting techniques. Gain proficiency in performing common administrative tasks in Windows, such as managing auto-start locations, using registry editors, manipulating services, and utilizing the task manager. These skills are essential for both defending and attacking Windows systems.
- **Linux OS and Uses, Different Distributions:** Linux is an open-source operating

system that offers versatility and customization options. Learn about the Linux kernel, which serves as the core of the operating system, and understand its functions. Explore different Linux distributions (distros) and their unique characteristics. Gain insights into the basic differences between Linux distributions, such as package management systems, desktop environments, and target user bases. Just like Windows, having basic Linux administrative knowledge is essential in the world of cybersecurity and hacking. Linux is ubiquitous, powering everything from web servers to mobile devices, TVs, and more. Therefore, understanding Linux to some extent is crucial.

It's essential to recognize that the debate over the best OS for hackers is futile. The effectiveness of a hacker is not determined by the operating system they use but by their skills, knowledge, and ability to adapt to different environments. Both Windows and Linux platforms are equally capable of most tasks in cybersecurity. Whether you choose a Linux distro or Windows, focus on installing the necessary applications and tools required for your work.

Avoid falling into the trap of so-called "***hacking***" OS distributions, which often comprise a collection of tools that may not be practical for everyday use. Instead, focus on mastering your chosen operating system and customizing it to suit your specific needs and preferences. Remember, it's not about the OS you use; it's about your proficiency in utilizing it to accomplish your tasks effectively.

You can check Our Linux Playbook For Hackers for the fundamentals to advanced topics covered

3. ***Learning How to do Google Search like Hackers***

Mastering the art of effective Google searching is perhaps the most critical skill for any aspiring hacker. It's not just about typing keywords into the search bar; it's about understanding how to refine your queries to yield the most relevant results. Here's why it's crucial:

- **Searching/Researching:** The ability to search and research effectively is what sets hackers apart. It's the cornerstone of problem-solving and finding solutions. Whenever you encounter a challenge or need information, turn to Google and

search for it. You'll find that you can resolve 99% of problems or at least find something closely related to the issue and its solution.

- **Start by Searching:** Begin by searching for topics relevant to your interests and goals. Whether it's learning how to become a hacker, following a penetration tester roadmap, or understanding how websites work, Google is your go-to resource.
- **Never Stop Reading:** Don't limit yourself to just one page of search results. Take the time to explore multiple pages and read different sources. Each page you visit adds to your knowledge base and helps you gain a deeper understanding of the topic at hand.
- **Deep Web/Dark Web:** Contrary to popular belief, the real "deep web" or "dark web" is not some mysterious part of the internet accessible only through specialized browsers. In reality, it's often found on the second page of Google search results. Always remember to venture beyond the first page of search results, as you may uncover valuable information that wasn't readily apparent initially.

4. ***Learning about Cyber Security, Hacking, Penetration Testing, and More***

To embark on your journey into the world of cybersecurity, it's crucial to understand the foundational concepts and various domains within the field. Here's how you can start:

- **What is Cyber Security?**

Search for definitions and explanations of cybersecurity. Understand its importance in protecting digital assets, data, and systems from cyber threats.

- **What is Hacking?**

Explore different perspectives on hacking and its various forms. Learn about ethical hacking (white hat), malicious hacking (black hat), and the gray areas in between.

- **Why Do We Need Cyber Security?**

Research the importance of cybersecurity in today's digital age. Understand the risks posed by cyber threats and the consequences of inadequate security measures.

- **What Hackers Do?**

Delve into the activities and motives of hackers. Learn about common hacking techniques, such as phishing, malware attacks, and social engineering.

- **What Are Jobs in Cyber Security?**

Search for different roles and positions within the cybersecurity field. Explore job titles such as cybersecurity analyst, penetration tester, security engineer, and more.

- **What Skills Are Needed to Get a Job in Cyber Security?**

Identify the key skills and competencies required for various cybersecurity roles. These may include technical skills like network security, programming, and cryptography, as well as soft skills like communication and problem-solving.

- **Roles and Responsibilities of Cyber Security Jobs**

Visit job websites like LinkedIn to explore the roles and responsibilities of cybersecurity positions. Gain insights into the day-to-day tasks and requirements of roles you're interested in pursuing.

- **Recent News Related to Cyber Security**

Stay updated on the latest developments and news in the cybersecurity field. Explore reputable websites and publications to learn about emerging threats, industry trends, and best practices.

Remember to approach your learning with curiosity, research diligently, and be patient with your progress. Don't rely on Hollywood portrayals of hacking, as they often exaggerate or misrepresent the realities of cybersecurity. Instead, seek knowledge from reliable sources and question what you learn to deepen your understanding.

Towards Basic Knowledge of Security & Hacking

1. ***Computer Programming (Start basics)***

Embarking on your journey into security and hacking, it's crucial to dip your toes into computer programming. Here's where to start:

- **Start with Basics:** Choose one or two programming languages and dedicate at least 20 hours to learning them. Popular choices include Python, JavaScript, or any other language you're interested in.
- **Is Programming Really Necessary for Hacking?**

No, it's not an absolute requirement, but here's the catch: Can you truly be a proficient hacker without understanding basic programming? The chances are quite rare.

- **Choosing a Programming Language:**

Which language should you learn? It depends on your future goals. However, grasping the basics of programming is always beneficial. Here's why:

1. **Python:** Known for its simplicity and versatility, Python is widely used in hacking

for its ease of learning and powerful libraries. It's great for automating tasks and making your life easier.

2. **JavaScript:** With the ubiquitous use of JavaScript in web development, understanding its basics is essential. It's rare to find a website these days that doesn't utilize JavaScript in some form.
3. **Other Languages:** While Python and JavaScript are highly recommended, learning additional languages like C++, Java, or even newer ones like Go (Golang) can broaden your skill set and enhance your understanding of different programming paradigms.

● **Why Learn Multiple Languages?**

Imagine encountering a website built on a framework you're unfamiliar with or needing to decipher VBScript or C++ code to complete a task. Knowing multiple languages gives you the flexibility to adapt and overcome such challenges.

● **Automating Tasks with Python:**

Python shines in automating day-to-day tasks, making it an invaluable tool for hackers. Whether it's writing scripts to streamline processes or developing custom tools, Python's simplicity and readability are unmatched.

● **Adapting to the Changing Landscape:**

The tech world is constantly evolving, and new languages and frameworks emerge regularly. By staying adaptable and continuously learning, you'll be better equipped to tackle the challenges of hacking in an ever-changing environment.

Investing time in learning programming basics lays a strong foundation for your journey into security and hacking. Embrace the opportunity to explore different languages and expand your skill set, knowing that each new language learned opens doors to new possibilities and insights.

2. ***Cyber Security & Hacking Terms***

In the vast landscape of cybersecurity and hacking, certain terms and jargon recur frequently. It's essential to familiarize yourself with these terms to avoid confusion and

navigate discussions effectively. Here are some key terms to search and learn:

- **Vulnerability:** Weaknesses or flaws in a system that can be exploited to compromise security.
- **Exploit:** A piece of software or code that takes advantage of a vulnerability to carry out an attack.
- **Threat:** Any potential danger to a system or network, including malware, hackers, or other malicious actors.
- **Malware:** Malicious software designed to infiltrate or damage a computer system.
- **Virus:** A type of malware that spreads by attaching itself to other programs or files.
- **Botnet:** A network of compromised computers controlled by a central server or hacker for malicious purposes.
- **Cloud:** A network of remote servers hosted on the internet to store, manage, and process data.
- **Firewall:** A security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- **Ransomware:** Malware that encrypts a victim's files or system and demands a ransom for their release.
- **Trojan:** A type of malware disguised as legitimate software to deceive users and gain unauthorized access to their systems.
- **Worm:** A self-replicating malware that spreads across networks without user intervention.
- **Spyware:** Software that secretly gathers information about a user's activities without their knowledge.
- **Adware:** Software that displays advertisements on a user's device, often without their consent.
- **Rootkit:** A type of malware that provides unauthorized access to a computer system while hiding its presence from users and security software.
- **Phishing:** A social engineering technique used to trick individuals into revealing sensitive information, such as passwords or financial details, by posing as a trustworthy entity.
- **Spear Phishing:** A targeted phishing attack that tailors messages to specific

individuals or organizations to increase the likelihood of success.

- **DoS (Denial of Service):** An attack that disrupts or disables a network or service by flooding it with excessive traffic or requests.
- **DDoS (Distributed Denial of Service):** A DoS attack carried out from multiple sources to overwhelm a target's resources.
- **Encryption:** The process of converting data into a secure form to prevent unauthorized access.
- **Encoding:** The process of converting data into a specific format for transmission or storage purposes.
- **Penetration Testing:** The practice of testing a system, network, or application for vulnerabilities and weaknesses by simulating real-world attacks.
- **Vulnerability Scanning:** The process of identifying and assessing vulnerabilities in a system or network.
- **Social Engineering:** The use of psychological manipulation to deceive individuals into divulging confidential information or performing actions that compromise security.
- **Clickjacking:** A technique used to trick users into clicking on malicious links or buttons disguised as legitimate elements on a webpage.
- **White-Hat:** Ethical hackers who use their skills for defensive purposes to identify and mitigate security vulnerabilities.
- **Black-Hat:** Malicious hackers who exploit vulnerabilities for personal gain or malicious intent.
- **SAST (Static Application Security Testing):** A security testing technique that analyzes source code for vulnerabilities without executing the program.
- **DAST (Dynamic Application Security Testing):** A security testing technique that analyzes running applications for vulnerabilities by sending requests and observing responses.
- **APT (Advanced Persistent Threat):** A sophisticated, long-term cyberattack carried out by a well-funded and highly skilled adversary.
- **Authentication:** The process of verifying the identity of a user or system attempting to access resources.
- **Authorization:** The process of granting or denying access to resources based on the user's identity and permissions.
- **Bug:** An error, flaw, or fault in a system or software program that may cause

unexpected behavior or vulnerabilities.

And the list goes on. Continuously expand your knowledge by researching and understanding these terms, as they form the building blocks of cybersecurity and hacking concepts.

3. ***Computer Networks***

Importance of Networks:

- Networks serve as the vital infrastructure that enables communication, data exchange, and resource sharing among devices.
- They provide access to the internet and external resources, facilitating research, communication, and online activities.
- Networks underpin the connectivity within organizations and across the globe, forming the cornerstone of contemporary computing.

Key Network Concepts:

1. **Understanding Network Devices:** Delve into the roles and functionalities of essential network components such as routers, switches, modems, firewalls, and load balancers.
2. **Mastering IP Addressing:** Grasp the intricacies of IP addressing, encompassing public/private IP addresses, subnetting, IP ranges, and the distinctions between classful and classless addressing schemes.
3. **Navigating OSI Layers & TCP/IP Model:** Explore the layers of the OSI model and the TCP/IP protocol suite, offering a comprehensive framework for comprehending network communication protocols.
4. **Unraveling the Server-Client Model:** Examine the server-client architecture and its pivotal role in facilitating communication and data exchange across networked devices.
5. **Demystifying DNS Resolution:** Understand the intricacies of Domain Name System (DNS) resolution, elucidating the process of translating domain names into corresponding IP addresses.
6. **Harnessing Proxies and VPNs:** Discover the functionalities of proxies (both forward and reverse) and virtual private networks (VPNs) in bolstering security

and anonymizing network traffic.

7. **Exploring Firewalls and Load Balancers:** Delve into the functionalities of firewalls for network security enhancement and load balancers for optimizing traffic distribution across multiple servers.
8. **Navigating Ports and Protocols:** Familiarize yourself with network ports and their applications, including common ports utilized for specific services and protocols such as SSH, FTP, HTTP/HTTPS, and SSL/TLS.
9. **Grasping DHCP and SSL:** Gain insights into the significance of Dynamic Host Configuration Protocol (DHCP) in dynamically assigning IP addresses and Secure Sockets Layer (SSL) for ensuring secure data transmission over the internet.

Operating Systems and Network Fundamentals:

- **Subnetting Basics:** Acquire fundamental knowledge of subnetting concepts, distinguishing between public and private IP addresses, and understanding essential terms like localhost, CIDR, subnet mask, and default gateway.
- **Network Terminology Mastery:** Familiarize yourself with essential network terminologies, including VLAN, DMZ, ARP, VM, NAT, IP, DNS, and DHCP.
- **Operating System Integration:** Learn the installation, configuration, and troubleshooting of networking components across various operating systems, ensuring seamless integration and functionality.
- **Protocol Proficiency:** Explore common network protocols, network topologies, and the OSI model, comprehending the function of each OSI layer and their implications in network communication.
- **Topology Insights:** Examine diverse network topologies such as star, ring, mesh, and bus, while also gaining insights into common protocols and their applications.
- **Protocol Deep Dive:** Dive into protocols such as SSH, RDP, FTP, SFTP, HTTP/HTTPS, and SSL/TLS, unraveling their basics, functionalities, and practical applications.
- **Port Understanding:** Acquire a comprehensive understanding of common ports and their applications in network communication, enhancing your ability to navigate networked environments effectively.
- **Storage Fundamentals:** Gain insights into Network-Attached Storage (NAS) and Storage Area Network (SAN), understanding their significance in data storage

and accessibility within networked environments.

We Got this Covered in Our Computer Networking : All-in-One For Dummies . Designed for beginners and enthusiasts alike, this book offers a thorough exploration of fundamental concepts, and advanced topics in networking.

4. ***Lab Setup : Building Your Virtual Environment***

Setting up a lab environment is crucial for hands-on learning and experimentation. Here's how to get started:

1. Choose Virtualization Software:

- Research and select virtualization software suitable for your operating system (OS), such as VirtualBox, VMWare Player/Workstation, VMWare Fusion, HyperV, or Parallels.
- Compare the features and functionalities of different virtualization software to determine the best fit for your needs.

2. Understand Network Modes:

- Familiarize yourself with network modes in virtualization software, including common types like Bridged, NAT (Network Address Translation), and Host-Only Network.
- Explore the purposes and usage scenarios for each network mode to make informed decisions during lab setup.

3. Install Operating Systems:

- Experiment with installing various operating systems (OS) on virtual machines (VMs), such as Windows and Linux distributions.
- Practice setting up dual-boot configurations, installing both Windows and Linux on the same VM to understand compatibility and interoperability.

4. Explore Windows Subsystem for Linux (WSL):

- Learn about Windows Subsystem for Linux (WSL), a compatibility layer enabling native Linux command-line tools and utilities to run on Windows.

- Experiment with WSL to understand its functionalities and explore the seamless integration of Linux within the Windows environment.

5. Experiment with Snapshots and Backups:

- Gain hands-on experience with snapshots and backups in virtual environments to safeguard your lab setups and configurations.
- Practice taking snapshots of VMs at different stages of configuration and experimentation, allowing you to revert to specific states if needed.

6. Leverage Online Resources:

- Utilize online resources, tutorials, and documentation provided by virtualization software vendors and communities to troubleshoot issues and optimize your lab environment.
- Engage with online forums, discussion boards, and user communities to seek guidance, share experiences, and collaborate with fellow enthusiasts.

Practical Hacking & Security

Now that we've covered the basics of Windows, Linux, networks, programming, virtual machines, and essential hacking/security concepts, it's time to put our knowledge into practice through practical hacking and security exercises. Setting up your own lab environment for experimentation and learning is not only legal but also highly encouraged. So, let's dive in and start hacking!

1. ***Network Hacking***

Information Gathering & Reconnaissance:

Before launching into any hacking endeavor, it's essential to gather as much information as possible about the target network. This phase involves various techniques:

1. **Host Discovery:** Identify active hosts within the network using tools like Nmap, which allows you to probe for live hosts and discover their IP addresses.
2. **Network Scanning:** Perform comprehensive network scans using Nmap to map out the network topology, identify open ports, and determine available services.

3. **Nmap Scan Types:** Familiarize yourself with different Nmap scan types, including TCP SYN scan, TCP Connect scan, UDP scan, and more, each serving specific purposes in reconnaissance.
4. **Port Scan and Discovery:** Conduct port scanning to enumerate open ports on target hosts, providing insights into potential entry points for exploitation.
5. **Scanning with Vulnerability Assessment Tools:** Utilize advanced vulnerability assessment tools like Nessus or Qualys to identify security vulnerabilities across network devices and systems.
6. **Nmap Scripts:** Leverage Nmap scripts (NSE scripts) to automate reconnaissance tasks and gather detailed information about target hosts, such as version detection, service enumeration, and vulnerability scanning.
7. **Active and Passive Search:** Combine active scanning techniques, such as port scanning and network probing, with passive information gathering methods, such as analyzing publicly available data and passive DNS reconnaissance.
8. **Whois and Similar Searches:** Use Whois lookup tools to retrieve domain registration information, IP address allocation details, and contact information of network administrators, aiding in reconnaissance efforts.
9. **Email Harvesting:** Employ email harvesting techniques to collect email addresses associated with the target network, facilitating social engineering attacks or further reconnaissance.

There are more info to gather so have a research and mainly seek what are you willing to hack so based on that gather the required info also not required may be it will be useful.

We got the Nmap Covered in Our Network Scanning Mastery: Unveiling the Secrets of Nmap. 🔍 Discover the basics of Nmap in a fun and engaging way. From understanding what Nmap does to why it's so important, we've got you covered. Plus, we'll show you some seriously cool features that'll make you feel like a cybersecurity superhero!

Weaponization, Delivery, Exploitation:

After thorough reconnaissance, the next phase involves weaponizing identified vulnerabilities and exploiting them to gain unauthorized access to target systems. This process includes:

1. **Choosing Exploits:** Select appropriate exploits based on reconnaissance findings, targeting vulnerabilities discovered during the scanning phase. This involves matching known vulnerabilities with available exploits.
2. **Metasploit Exploits and Meterpreter:** Utilize Metasploit Framework, a powerful penetration testing tool, to leverage pre-built exploits and payloads for launching attacks against vulnerable systems. Meterpreter, a Metasploit payload, provides advanced post-exploitation capabilities for remote control and data exfiltration.
3. **Exploit-DB and Searchsploit:** Explore Exploit-DB, a comprehensive database of exploits and vulnerabilities, to search for relevant exploits matching identified vulnerabilities. Additionally, leverage Searchsploit, a command-line utility, to quickly search Exploit-DB's repository for relevant exploit code.
4. **0day Exploits:** In rare cases, if a previously unknown vulnerability (0day) is identified during reconnaissance, attempt to exploit it to gain unauthorized access. However, exercise caution and adhere to ethical hacking principles when handling 0day exploits.
5. **Mapping Open Ports/Services to Exploits:** Map knowledge of open ports and services obtained during reconnaissance to specific exploits or attack techniques. Determine which exploits are applicable to target systems based on their exposed services and configurations.

Exploitation & Command-Control:

Once vulnerabilities have been successfully exploited, the focus shifts to establishing command and control over compromised systems, escalating privileges, and executing further attacks. This phase involves:

1. **Windows Privilege Escalation:** Exploit weaknesses in Windows systems to elevate user privileges, granting unauthorized access to sensitive resources and functionalities. Techniques may include abusing misconfigurations, exploiting known vulnerabilities, or manipulating system components to gain higher privileges.
2. **Linux Privilege Escalation:** Similarly, exploit vulnerabilities or misconfigurations in Linux-based systems to escalate privileges and gain root access. Techniques may involve exploiting SUID binaries, misconfigured sudo permissions, or kernel vulnerabilities to achieve elevated privileges.

3. **Reverse Shells:** Deploy reverse shell payloads to establish command and control over compromised systems, allowing attackers to remotely execute commands and interact with compromised hosts. Reverse shells facilitate remote access and enable further exploitation and data exfiltration.
4. **Netcat (nc):** Learn how to use Netcat, a versatile networking utility, to establish network connections, transfer files, and create reverse shells. Mastering Netcat is essential for conducting various post-exploitation activities and maintaining persistence on compromised systems.
5. **One-Liners for Shells:** Familiarize yourself with one-liner commands that trigger and provide reverse shells, enabling quick and efficient establishment of command and control over compromised systems. These concise commands streamline the process of setting up remote access and executing further attacks.

Resources:

- **GTFOBins:** GTFOBins is a curated collection of Unix binaries that can be used to bypass local security restrictions, providing valuable insights into privilege escalation and post-exploitation techniques.
- **PentestMonkey:** PentestMonkey offers a range of practical resources and cheat sheets for penetration testers and security professionals, covering various aspects of ethical hacking, including privilege escalation and data exfiltration.

1. **Data Exfiltration Techniques:** Explore various methods and tools for exfiltrating sensitive data from compromised systems while maintaining covert communication channels. Techniques may include file transfer over network protocols, steganography, or encryption to conceal data during transmission.

Well Mastering exploitation techniques, privilege escalation methods, and command-and-control mechanisms, security professionals can effectively establish control over compromised systems and execute further attacks or gather critical intelligence for security assessments.

Network Sniffing and Analysis:

Network sniffing plays a crucial role in cybersecurity by allowing security professionals to intercept and analyze network traffic for identifying vulnerabilities, suspicious

activities, or potential security threats. Key aspects of network sniffing include:

Wireshark & Packet Capture:

- Wireshark is a powerful network protocol analyzer that enables the capture and inspection of network traffic in real-time.
- Security professionals use Wireshark to analyze packets, identify communication patterns, and detect anomalies or malicious activities within network traffic.
- Packet capture involves capturing and storing network packets for subsequent analysis, providing valuable insights into network behavior and potential security incidents.

Man-in-the-Middle (MitM) Attacks:

- MitM attacks involve intercepting and manipulating communication between two parties without their knowledge.
- Attackers positioned as intermediaries can eavesdrop on communication, modify data packets, or inject malicious content into the traffic stream.
- Security professionals utilize MitM techniques for security assessments, evaluating network vulnerabilities and implementing appropriate countermeasures to mitigate risks.

TCPDump:

- TCPDump is a command-line packet analyzer that allows security professionals to capture and analyze network traffic directly from the command line.
- Similar to Wireshark, TCPDump enables packet capture and filtering based on various criteria, facilitating network troubleshooting, security monitoring, and forensic analysis.

2. ***Cloud & Cloud Security:***

Cloud computing has revolutionized the way organizations manage and deliver IT services, offering scalability, flexibility, and cost-efficiency. Understanding cloud technologies and their security implications is essential for modern cybersecurity professionals. Key aspects of cloud and cloud security include:

Cloud Skills and Knowledge:

- Gain proficiency in cloud computing concepts, architectures, and services offered by major cloud providers.
- Understand the shared responsibility model, which delineates security responsibilities between cloud service providers and customers.

Cloud Services:

- Familiarize yourself with common cloud service models:
  - Software as a Service (SaaS)
  - Platform as a Service (PaaS)
  - Infrastructure as a Service (IaaS)
- Explore leading cloud platforms such as AWS, Google Cloud Platform (GCP), and Microsoft Azure.

Basic Idea of AWS, Azure, and GCP:

AWS (Amazon Web Services):

- AWS is a comprehensive cloud computing platform offering a wide range of services, including computing power, storage, networking, databases, and more.
- Security Concerns:
  - AWS Identity and Access Management (IAM): Manage user access and permissions to AWS resources.
  - Amazon Virtual Private Cloud (VPC): Create isolated virtual networks for enhanced security.
  - AWS Security Groups: Define firewall rules to control inbound and outbound traffic to AWS resources.
  - AWS Key Management Service (KMS): Securely manage encryption keys used to encrypt data stored in AWS.
  - AWS CloudTrail: Monitor and log AWS account activity to enhance security and compliance.

Azure (Microsoft Azure):

- Azure is a cloud computing platform by Microsoft, offering services for computing, analytics, storage, and networking.
- Security Concerns:
  - Azure Active Directory (AAD): Manage user identities and access to Azure resources.
  - Azure Virtual Network (VNet): Create private networks in Azure with control over IP addresses, DNS settings, and security policies.
  - Azure Security Center: Provides unified security management and advanced threat protection across hybrid cloud workloads.
  - Azure Key Vault: Safeguard cryptographic keys and secrets used by cloud applications and services.
  - Azure Sentinel: Cloud-native security information and event management (SIEM) service for threat detection and response.

GCP (Google Cloud Platform):

- GCP is Google's cloud computing platform offering a variety of services for computing, storage, machine learning, and data analytics.
- Security Concerns:
  - Google Cloud Identity and Access Management (IAM): Manage access control for Google Cloud resources.
  - Virtual Private Cloud (VPC) Network: Isolate resources and control network traffic with customizable firewalls and routing tables.
  - Cloud Security Command Center: Provides security and data risk insights across GCP services.
  - Google Cloud Key Management Service (KMS): Manage cryptographic keys for cloud services and applications.
  - Google Cloud Armor: Protect web applications against distributed denial of service (DDoS) attacks and web threats.

Docker Basics & Container Security:

Docker Basics:

- Docker is a popular platform for developing, shipping, and running applications using containerization technology.
- Key Concepts:
  - Docker Engine: The runtime environment for containers.
  - Docker Images: Lightweight, standalone, executable packages that contain everything needed to run an application.
  - Docker Containers: Runnable instances of Docker images.
  - Dockerfile: Text file containing instructions for building Docker images.
- Benefits:
  - Portability: Docker containers can run on any platform that supports Docker.
  - Consistency: Applications behave consistently across different environments.
  - Isolation: Containers isolate applications and their dependencies from the underlying infrastructure.

Container Security:

- Container security involves protecting the entire container lifecycle, from image creation to runtime execution.
- Best Practices:
  - Secure Base Images: Start with minimal and trusted base images to reduce vulnerabilities.
  - Image Scanning: Use image scanning tools to identify and remediate vulnerabilities in container images.
  - Runtime Security: Implement runtime security measures such as container isolation, least privilege access, and network segmentation.
  - Continuous Monitoring: Monitor containerized applications for security threats and anomalous behavior.
  - Container Orchestration Security: Secure container orchestration platforms like Kubernetes by configuring authentication, authorization, and

network policies.

Understanding the basics of AWS, Azure, and GCP, along with Docker fundamentals and container security principles, equips cybersecurity professionals with the knowledge needed to secure cloud environments and containerized applications effectively.

3. ***Web Application Security***

Basic Understanding of Web Languages:

- While not directly related to security, having a basic understanding of web languages can be beneficial for understanding how web applications work and identifying potential vulnerabilities.
- Spend around 7 hours each on:
  - HTML and CSS: Basic structure and styling of web pages.
  - JavaScript: Client-side scripting language used for dynamic interactions on web pages.
  - PHP: Server-side scripting language commonly used for web development.
  - Node.js or other backend frameworks: Understanding backend logic and server-side processing.

Database Technologies:

- Familiarize yourself with various database technologies commonly used in web applications, including:
  - MySQL: Relational database management system (RDBMS) often used with PHP-based applications.
  - NoSQL: Non-relational databases like MongoDB, used for flexible data storage and retrieval.
- Understanding database technologies helps in identifying vulnerabilities such as SQL injection and NoSQL injection.

Common Web Application Vulnerabilities:

- SQL Injection: Exploiting vulnerabilities in database queries to manipulate or access unauthorized data.

- Cross-Site Scripting (XSS): Injecting malicious scripts into web pages viewed by other users.
- Cross-Site Request Forgery (CSRF): Executing unauthorized actions on behalf of authenticated users.
- Insecure Direct Object References (IDOR): Accessing or modifying unauthorized resources by manipulating object references.
- Authentication and Session Management: Identifying weaknesses in user authentication and session handling mechanisms.
- Security Misconfigurations: Exploiting misconfigured web servers, databases, or application frameworks.
- File Upload Vulnerabilities: Uploading malicious files to compromise the server or execute arbitrary code.

Never ending list....

Web Application Testing Techniques:

- Black Box Testing: Testing web applications without access to internal code or architecture details.
- White Box Testing: Analyzing source code and internal workings of web applications for vulnerabilities.
- Penetration Testing: Simulating real-world attacks to identify and exploit vulnerabilities in web applications.
- Vulnerability Scanning: Using automated tools to scan web applications for known vulnerabilities and misconfigurations.
- Code Review: Manual inspection of source code to identify security flaws and weaknesses.
- Web Application Firewalls (WAFs): Implementing WAFs to protect web applications from common attacks and threats.

Web Application Security Tools:

Man-in-the-Middle (MiTM) Proxy:

- Utilize tools like Burp Suite and OWASP ZAP for web application penetration testing (PT).

- Burp Suite: Widely used for web security testing, includes various tools like Proxy, Scanner, Intruder, etc.
- OWASP ZAP: Open-source alternative to Burp Suite, offering similar features for web security testing.

Burp Suite:

- Essential tool for web application security testing.
- Community version provides basic functionality, suitable for learning and small-scale testing.
- Components include:
  - Proxy: Intercepts and modifies HTTP/S requests between the browser and the web server for analysis and manipulation.
  - Scanner: Automatically identifies security vulnerabilities in web applications.
  - Intruder: Performs automated attacks like brute force, fuzzing, etc., to identify vulnerabilities.
  - Repeater: Allows manual manipulation and re-sending of individual requests for testing.
  - Sequencer: Analyzes the randomness and quality of tokens or session identifiers.
  - Decoder: Decodes various types of data encoding used in web applications.
  - Extender: Supports the integration of additional functionalities through extensions or plugins.

OWASP ZAP:

- Free and open-source web application security scanner.
- Offers functionalities similar to Burp Suite, including proxy, scanner, and various attack tools.
- Suitable for beginners and professionals alike, with active community support and regular updates.

OWASP Top 10 Web Application Vulnerabilities:

The OWASP (Open Web Application Security Project) Top 10 is a regularly updated list of the most critical security risks facing web applications. Here are the vulnerabilities listed in the 2013, 2017, and 2021 editions:

OWASP Top 10 - 2013:

1. **Injection:** SQL, NoSQL, OS Command, etc.
2. **Broken Authentication and Session Management:** Improperly implemented authentication mechanisms.
3. **Cross-Site Scripting (XSS):** Injection of malicious scripts into web pages viewed by other users.
4. **Insecure Direct Object References:** Accessing unauthorized data by manipulating object references.
5. **Security Misconfiguration:** Poorly configured security settings, default passwords, etc.
6. **Sensitive Data Exposure:** Exposure of sensitive data through insufficient protection mechanisms.
7. **Missing Function Level Access Control:** Unauthorized access to functionalities or resources.
8. **Cross-Site Request Forgery (CSRF):** Execution of unwanted actions on behalf of an authenticated user.
9. **Using Components with Known Vulnerabilities:** Use of outdated or vulnerable third-party components.
10. **Unvalidated Redirects and Forwards:** Redirecting users to malicious websites or resources.

OWASP Top 10 - 2017:
The OWASP Top 10 list was not updated in 2017.

OWASP Top 10 - 2021:

1. **Injection:** Injection flaws such as SQL injection, NoSQL injection, OS command injection, etc.
2. **Broken Authentication:** Issues related to authentication mechanisms like weak

passwords, improper session management, etc.
3. **Sensitive Data Exposure:** Exposure of sensitive data through insufficient protection mechanisms.
4. **XML External Entities (XXE):** Vulnerabilities related to XML parsing and external entity references.
5. **Broken Access Control:** Inadequate enforcement of access controls leading to unauthorized access.
6. **Security Misconfiguration:** Poorly configured security settings, default passwords, unnecessary features enabled, etc.
7. **Cross-Site Scripting (XSS):** Injection of malicious scripts into web pages viewed by other users.
8. **Insecure Deserialization:** Vulnerabilities related to the deserialization of untrusted data.
9. **Using Components with Known Vulnerabilities:** Use of outdated or vulnerable third-party components.
10. **Insufficient Logging & Monitoring:** Lack of proper logging and monitoring of security events.

Staying updated with the OWASP Top 10 vulnerabilities is crucial for web developers, security professionals, and organizations to prioritize their security efforts and mitigate potential risks effectively.

API Security:

APIs (Application Programming Interfaces) have become a fundamental part of modern software development, enabling interaction between different software systems and services. However, they also introduce unique security challenges. The OWASP (Open Web Application Security Project) provides a list of the top security risks associated with APIs, similar to its Top 10 Web Application Vulnerabilities. Here's an overview of the OWASP API Security Top 10:

OWASP API Security Top 10:

1. **Broken Object Level Authorization:** Inadequate access controls leading to unauthorized access to resources or actions.
2. **Broken Authentication:** Weak authentication mechanisms, improper session

management, etc., leading to unauthorized access to APIs.

3. **Excessive Data Exposure:** Exposure of sensitive information through APIs due to lack of proper data protection mechanisms.
4. **Lack of Resources & Rate Limiting:** Absence of rate limiting and resource limitations leading to API abuse, DoS attacks, or excessive usage.
5. **Broken Function Level Authorization:** Inadequate enforcement of access controls on individual API endpoints or functions.
6. **Mass Assignment:** Acceptance of unexpected parameters or data during API calls, leading to potential security vulnerabilities.
7. **Security Misconfiguration:** Poorly configured security settings, default configurations, unnecessary features enabled, etc.
8. **Injection:** Injection vulnerabilities in API parameters, such as SQL injection, NoSQL injection, etc.
9. **Improper Assets Management:** Inadequate tracking and management of API-related assets, such as keys, tokens, credentials, etc.
10. **Insufficient Logging & Monitoring:** Lack of proper logging and monitoring of API activities and security events, hindering incident response and forensic analysis.

Addressing these API security risks is essential for ensuring the integrity, confidentiality, and availability of both the API itself and the data it handles. Organizations must prioritize API security measures, including authentication, authorization, encryption, input validation, rate limiting, and logging, to mitigate potential threats and vulnerabilities effectively.

Vulnerabilities

Vulnerabilities in software systems can pose significant security risks, potentially leading to data breaches, unauthorized access, and other malicious activities. Here are some common examples of vulnerabilities that attackers may exploit:

1. **Cross-Site Scripting (XSS):** Allows attackers to inject malicious scripts into web pages viewed by other users.
2. **HTML Injection:** Similar to XSS, but specifically targets HTML code to manipulate the appearance or behavior of web pages.
3. **Cross-Site Request Forgery (CSRF):** Tricks users into executing unwanted

actions on a web application where they are authenticated.

4. **XXE (XML External Entity) Injection:** Exploits vulnerable XML parsers to disclose confidential data, execute remote code, or perform server-side request forgery (SSRF).
5. **SQL Injection:** Allows attackers to execute malicious SQL queries to manipulate or access unauthorized data in a database.
6. **File Upload Vulnerabilities:** Allows attackers to upload and execute malicious files on a web server, potentially compromising its security.
7. **Directory Traversal:** Exploits insufficient input validation to access files and directories outside the intended directory structure.
8. **Authentication & Authorization Issues:** Weak authentication mechanisms or improper authorization controls can lead to unauthorized access to sensitive resources.
9. **Business Logic Vulnerabilities:** Exploits flaws in the logic of an application's workflows or processes to achieve unauthorized actions or access.
10. **Rate Limiting Bypass:** Exploits weaknesses in rate limiting mechanisms to perform brute force attacks or overload server resources.

Vulnerabilities: Just Examples, the list is never-ending

To stay updated on the latest vulnerabilities and security trends, consider exploring the following resources:

- HackerOne Reports: Browse vulnerability reports submitted by security researchers on the HackerOne platform to learn about real-world vulnerabilities and their impacts.
- Personal Blogs and Twitter Hashtags: Follow security researchers, bug bounty hunters, and cybersecurity professionals on personal blogs and social media platforms like Twitter. Explore hashtags such as #infosec, #bugbounty, and #bugbountytips for valuable insights and tips on vulnerability discovery and mitigation strategies.

4. ***Network Defense:***

Defending a network is a formidable challenge in the face of constantly evolving technology and expanding attack surfaces. Here are some key areas and strategies for

network defense:

Endpoint Security:

- Implement antivirus and endpoint detection and response (EDR) solutions to defend against malware.
- Understand common malware injection methods and how antivirus software works.
- Maintain asset and inventory management to ensure security software and policies are applied uniformly across all machines.
- Employ Data Leak/Loss Prevention (DLP) systems to prevent the unauthorized transmission of sensitive data.

Email Security:

- Protect against spam and phishing emails by implementing email gateway security software.
- Develop strategies to identify and mitigate spam and phishing attempts.
- Utilize email security measures to safeguard communication channels.

Firewall, Proxy, VPN:

- Configure firewall policies to control network traffic and enforce security measures.
- Maintain access control lists (ACLs) and monitor DNS resolvers.
- Utilize block lists and allow lists to manage network access effectively.
- Deploy enterprise VPN and proxy configurations for secure remote access.

Web Application Firewall (WAF):

- Configure NG firewalls to protect web applications from common attacks.
- Implement threat hunting techniques to proactively identify and mitigate security threats.
- Conduct malware analysis and reverse engineering to understand and mitigate malicious software.

Insider Threat Analysis:

- Analyze and monitor internal network activity to detect and prevent insider threats.
- Identify and mitigate potential vulnerabilities in the network infrastructure.

SIEM, SOC, IHR:

- Implement Security Information and Event Management (SIEM) systems to centralize security log data.
- Establish a Security Operations Center (SOC) to monitor and respond to security incidents in real-time.
- Form an Incident Handling and Response (IHR) team to coordinate incident response efforts and collaborate with relevant stakeholders.

By implementing robust network defense strategies across these areas, organizations can effectively mitigate security risks and protect their networks from various cyber threats.

5. ***Basics of Cryptography:***

Cryptography forms the foundation of modern cybersecurity, providing methods for secure communication and data protection. Here are some fundamental concepts:

- **Hashing:** Hash functions transform input data into a fixed-size string of characters, known as a hash value. They are used to verify data integrity, password storage, and digital signatures.
- **Key Exchange:** Key exchange protocols facilitate the secure exchange of cryptographic keys between parties to enable encrypted communication.
- **Salting:** Salting involves adding a random value (salt) to input data before hashing to prevent the same input from producing the same hash value, enhancing password security.
- **PKI (Public Key Infrastructure):** PKI is a framework that manages the creation, distribution, and revocation of digital certificates, which contain public keys used for encryption and authentication.
- **Private Key vs. Public Key:** In asymmetric encryption, a pair of keys is used: a

private key for decryption and a public key for encryption. The private key is kept secret, while the public key is shared.

- **Obfuscation:** Obfuscation techniques obscure code or data to make it difficult to understand, reverse engineer, or tamper with, often used to protect intellectual property.
- **Secure vs. Insecure Protocols:** Secure protocols, such as SSL/TLS, provide encryption and data integrity mechanisms, while insecure protocols transmit data in plaintext, making them vulnerable to interception.
- **FTP vs. SFTP:** FTP (File Transfer Protocol) transfers data in plaintext, while SFTP (SSH File Transfer Protocol) encrypts data during transmission using SSH.
- **SSL vs. TLS:** SSL (Secure Sockets Layer) and its successor TLS (Transport Layer Security) are cryptographic protocols that secure communication over a network, such as the internet.
- **DNSSEC:** DNSSEC (Domain Name System Security Extensions) adds cryptographic authentication to DNS to prevent DNS spoofing and cache poisoning attacks.
- **LDAPS:** LDAPS (LDAP over SSL) encrypts LDAP (Lightweight Directory Access Protocol) traffic using SSL/TLS for secure directory services communication.
- **SRTP:** SRTP (Secure Real-time Transport Protocol) provides encryption, message authentication, and integrity protection for real-time communication protocols, such as VoIP.
- **IPSEC:** IPsec (Internet Protocol Security) provides network layer security by encrypting and authenticating IP packets, ensuring confidentiality, integrity, and authenticity of data.

6. ***LETS HACK / DEFEND Like a PRO***

Learning in the field of cybersecurity and hacking is an ongoing journey, and testing your skills on various platforms is an excellent way to reinforce what you've learned and discover new areas for improvement. It's true that there's always more to explore, and the vastness of the field means there's something for everyone, whether you're passionate about offensive or defensive security, or even specialized areas like IoT and blockchain security.

Security is indeed a multifaceted domain, and both attackers and defenders play crucial roles in safeguarding systems and data. While attacking may seem more glamorous,

defending is equally challenging and essential for maintaining the integrity and security of networks and applications.

Remember, cybersecurity and hacking are all about continuous learning and research. Each concept or keyword mentioned in this guide can lead to deeper exploration and understanding. With your curiosity and dedication, you can delve further into any topic and expand your knowledge exponentially.

TryHackMe

- TryHackMe offers a variety of virtual environments and challenges covering different cybersecurity topics, from beginner to advanced levels.

HackTheBox

- HackTheBox provides a platform for users to engage in penetration testing challenges, offering realistic scenarios to practice hacking skills.

PortSwigger Labs

- PortSwigger Labs offers web security labs where you can practice finding and exploiting web vulnerabilities using Burp Suite and other tools.

Try2Hack

- Try2Hack offers a collection of hacking challenges and puzzles to solve, ranging from basic to advanced levels.

echoCTF

- echoCTF hosts Capture The Flag (CTF) competitions and challenges, allowing participants to test their hacking skills in a competitive environment.

CertifiedSecure

- CertifiedSecure provides a platform for hands-on cybersecurity training and certifications, covering various topics such as ethical hacking, penetration testing, and more.

Root Me

- Root Me offers a wide range of challenges and virtual environments to practice hacking and security skills, including web exploitation, network analysis, and cryptography.

VulnHub

- VulnHub hosts vulnerable virtual machines for users to download and exploit, providing real-world scenarios to practice penetration testing and vulnerability assessment.

OverTheWire

- OverTheWire offers interactive war games and challenges focused on cybersecurity and hacking, designed to improve problem-solving and technical skills.

PentesterLab

- PentesterLab provides hands-on exercises and labs to learn web penetration testing techniques, covering topics such as XSS, SQL injection, and more.

LetsDefend

- LetsDefend offers a platform for blue teamers to practice defending against cyber threats and conducting incident response exercises.

SecurityBlueTeam

- SecurityBlueTeam provides resources and challenges for blue teamers and defenders to enhance their skills in detecting and mitigating security threats.

So keep exploring, keep learning, and never hesitate to dive into new challenges and opportunities for growth. Happy hacking and defending!

Courses / Certifications / Resources

1. ***Starting into Security***

For those starting their journey into cybersecurity, here are some recommended courses and certifications to build a strong foundation:

1. **CEH (Certified Ethical Hacker)**: This certification provides a comprehensive overview of ethical hacking concepts, tools, and techniques, covering topics such as penetration testing, vulnerability assessment, and network security fundamentals.
2. **CompTIA Security+**: This entry-level certification covers essential cybersecurity concepts, including network security, cryptography, risk management, and threat detection, making it an excellent starting point for beginners.
3. **Practical Ethical Hacking - TCM**: Offered by The Cyber Mentor, this practical course provides hands-on experience in ethical hacking techniques, focusing on real-world scenarios and practical skills development.
4. **eJPT (eLearnSecurity Junior Penetration Tester)**: This certification program is designed for aspiring penetration testers, covering topics such as reconnaissance, scanning, exploitation, and post-exploitation techniques.
5. **SANS SEC460: Enterprise Threat and Vulnerability Assessment**: This SANS course focuses on performing comprehensive threat and vulnerability assessments within enterprise environments, equipping professionals with the skills to identify and mitigate security risks effectively.
6. **SANS SEC301: Intro to Cyber Security**: This introductory course by SANS covers foundational cybersecurity concepts, terminology, and principles, providing a solid understanding of cybersecurity fundamentals for beginners.

2. ***Network Hacking***

Here are some highly recommended courses, certifications, and resources for network hacking:

1. **SANS SEC660**: SANS Institute offers this course titled "Advanced Penetration Testing, Exploit Writing, and Ethical Hacking." It covers advanced techniques for penetration testing and exploit development.

2. **SANS SEC760**: Another course by SANS Institute, "Advanced Exploit Development for Penetration Testers," focuses specifically on exploit development techniques for penetration testers.
3. **eCPTX - Advanced Penetration Testing**: The eLearnSecurity Certified Penetration Tester eXtreme (eCPTX) certification is designed for experienced penetration testers who want to validate their advanced skills and knowledge.
4. **OSCP (Offensive Security Certified Professional)**: Offered by Offensive Security, OSCP is one of the most respected certifications in the industry. It emphasizes practical hands-on skills in penetration testing and network exploitation.
5. **IppSec YouTube Channel**: IppSec is known for his detailed walkthroughs of Hack The Box machines and other Capture The Flag (CTF) challenges. His channel is an excellent resource for learning network hacking techniques in a practical context.

To kickstart your journey into network hacking , here are some essential resources and platforms:

1. **HackTheBox**: An online platform offering hands-on labs to test and improve your penetration testing and cybersecurity skills. It provides a wide range of realistic scenarios to practice hacking techniques in a controlled environment.
2. **VulnHub**: Offers a variety of downloadable virtual machines (VMs) that simulate vulnerable systems for practicing penetration testing and network security concepts. These VMs provide real-world scenarios to test your skills in a safe environment.
3. **OffensiveSecurity ProvingGrounds**: This platform allows you to practice pentesting skills in a standalone, private lab environment. With additions like PG Play and PG Practice, Offensive Security's Proving Grounds offers comprehensive training labs to enhance your skills.
4. **TryHackMe**: An online platform designed to teach cybersecurity through gamified, real-world labs. It caters to both beginners and experienced hackers, offering guides and challenges to accommodate different learning styles. TryHackMe provides interactive labs covering various cybersecurity topics, including network security.
5. **HackTricks GitBook**: A comprehensive collection of resources covering various attack vectors in network, mobile, and web security. This GitBook serves as a

valuable reference for learning and mastering different cybersecurity concepts and techniques. 3. ***Web Application***

For diving deep into web application security, here are some excellent courses, certifications, and resources:

1. **SANS SEC642**: This course, titled "Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques," offered by SANS Institute, provides advanced training in web application penetration testing and exploitation techniques.
2. **eWPTXv2 - Advanced Web Application Penetration Testing**: The eLearnSecurity Web Application Penetration Tester eXtreme (eWPTXv2) certification is designed for experienced professionals looking to validate their advanced skills in web application security testing.
3. **OSWE (Offensive Security Web Expert)**: Offered by Offensive Security, the OSWE certification focuses on advanced web application security testing skills, including hands-on exercises in identifying and exploiting security vulnerabilities in web applications.

Getting Started with Web Application Security:

- **OWASP Testing Guide**: A comprehensive resource explaining various security issues and how to test for them in web applications.
- **PortSwigger Web Security Academy**: Practical learning resources followed by labs to master web application security testing techniques.
- **Bugcrowd Vulnerability Rating Taxonomy**: A helpful resource for understanding multiple security issues and their associated severity ratings.
- **OWASP Juice Shop**: A real-life application for practicing testing various security vulnerabilities.
- **Cobalt.io Vulnerability Wiki**: Provides explanations, proof of concepts, and risk ratings for various security issues based on OWASP ASVS.
- **PayloadAllTheThings**: An open-resource GitHub repository containing a vast list of payloads for different security issues.
- **Learn365 GitHub Repository**: Contains various learning resources for web

application security and other attack vectors.

- **HackTricks GitBook**: A collection of resources covering various network, mobile, and web attack vectors.
- **InfoSec Writeups, PentesterLand & HackerOne Disclosures**: Great resources for reading bug bounty writeups and learning from real-world hacking experiences.

If you're open to paid subscriptions, consider these two labs:

- **PentesterLab**: Offers a platform for hands-on practice with web application security testing techniques.
- **PentesterAcademy — AttackDefense Labs**: Provides a wide range of content covering attack and defense scenarios in web application security.

4. ***Mobile Application Security***

To dive into the realm of mobile application security, consider these valuable resources and tools:

1. **OWASP Mobile Security Top 10**: OWASP provides a comprehensive list of the top security risks faced by mobile applications. Understanding these risks is crucial for securing mobile apps effectively.
2. **The Mobile Application Hacker's Handbook**: This handbook offers in-depth insights into mobile application security, covering topics such as reverse engineering, static and dynamic analysis, and common vulnerabilities.
3. **HackTricks GitBook**: Explore this extensive collection of resources covering various attack vectors in network, mobile, and web security. It serves as a valuable reference for learning and mastering different aspects of mobile application security.
4. **OWASP iGoat**: iGoat is a deliberately insecure iOS application designed to teach iOS developers and security professionals about common vulnerabilities in mobile apps. It provides hands-on exercises for practicing mobile app security testing.
5. **Insecure Bank**: This is an insecure Android banking application designed for educational purposes. It allows security professionals to practice identifying and exploiting vulnerabilities commonly found in Android apps.

5. ***Cloud Pentest***

For those interested in cloud pentesting, SANS offers several valuable courses:

1. **SANS SEC588: Cloud Penetration Testing and Ethical Hacking**: This course provides hands-on training in performing security assessments of cloud environments, including AWS, Azure, and GCP. Participants learn techniques for identifying and exploiting vulnerabilities in cloud-based infrastructure and applications.
2. **SANS SEC488: Cloud Security Essentials**: While not specifically focused on pentesting, this course covers essential concepts in cloud security, including architecture, governance, risk management, and compliance. Understanding these fundamentals is crucial for conducting effective cloud penetration tests.
3. **SANS SEC534: Secure DevOps and Cloud Application Security**: This course explores security considerations for cloud-native applications and DevOps practices. Participants learn how to assess the security posture of cloud-based applications and integrate security into the software development lifecycle.

6. ***Defence***

For those interested in defense-oriented cybersecurity roles, here are some recommended courses and certifications:

1. **eNDP (Network Defense Professional)**: This certification focuses on building expertise in network defense strategies, including threat detection, incident response, and network security architecture.
2. **Firewall - PaloAlto Firewall**: This training program provides in-depth knowledge of Palo Alto Networks' firewall technologies, equipping professionals with the skills to configure, manage, and optimize firewall deployments for effective network defense.
3. **eCTHPv2 - Threat Hunting Professional**: This certification program focuses on threat hunting techniques and methodologies, empowering security

professionals to proactively detect and mitigate advanced threats within enterprise networks.

4. **SANS SEC699: Purple Team Tactics - Adversary Emulation for Breach Prevention & Detection**: This course covers purple teaming strategies, which involve collaboration between red and blue teams to improve an organization's overall security posture through realistic adversary emulation.
5. **SANS FOR500: Windows Forensic Analysis**: While primarily focused on digital forensics, this course provides valuable insights into incident response and malware analysis techniques for defending Windows-based systems.
6. **SANS FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics**: This course delves into advanced incident response techniques, threat hunting methodologies, and digital forensics practices, equipping professionals with the skills to effectively respond to and mitigate security incidents.
7. **SANS FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response**: This course focuses on network forensics and threat hunting, enabling professionals to analyze network traffic, detect malicious activity, and respond to security incidents effectively.
8. **SANS SEC555: SIEM with Tactical Analytics**: This course covers security information and event management (SIEM) technologies and tactical analytics, providing hands-on experience in configuring and using SIEM platforms for effective threat detection and response.
7. ***Penetration Testing***

For individuals interested in specializing in penetration testing, here are some recommended courses and resources:

1. **eCPPTv2 (eLearnSecurity Certified Professional Penetration Tester)**: This certification program focuses on practical penetration testing skills, covering topics such as reconnaissance, scanning, exploitation, and post-exploitation techniques, leading to the mastery of penetration testing methodologies.
2. **LiveOverflow Youtube Channel**: LiveOverflow offers a wide range of educational content on cybersecurity, including penetration testing, reverse engineering, and exploit development, providing valuable insights and tutorials for aspiring penetration testers.
3. **SANS SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling**: This

SANS course dives deep into the tools, techniques, and methodologies used by hackers, focusing on practical skills development in penetration testing and incident handling.

4. **SANS SEC560: Network Penetration Testing and Ethical Hacking**: This SANS course is designed to equip professionals with the knowledge and skills needed to conduct effective network penetration tests, covering topics such as network reconnaissance, vulnerability assessment, and exploitation techniques.

Breakdown!!!

Here's a breakdown of foundational skills, hacking basics, and advanced topics for individuals looking to work in cybersecurity:

Foundational Skills:

- Understanding of computer networking principles and protocols.
- Knowledge of operating systems (Windows, Linux, etc.) and their architecture.
- Familiarity with programming languages such as Python, Bash scripting, and PowerShell.
- Basic understanding of cybersecurity concepts, including threats, vulnerabilities, and risk management.

Hacking Basics:

1. **Active Directory Hacking**: Learn how to exploit weaknesses in Active Directory environments, which are widely used in corporate networks.
2. **Web Application Hacking**: Gain skills in identifying and exploiting vulnerabilities in web applications using tools like Burp Suite and OWASP resources.
3. **Wireless Hacking**: Understand how to crack WPA2 Personal and Enterprise networks and gain access to wireless networks.
4. **Certifications**: Consider practical and affordable certifications like PNPT, CRTO, and CRTP, which provide hands-on training in penetration testing skills.
5. **Privilege Escalation**: Develop skills in escalating privileges on Windows and Linux systems, a crucial aspect of post-exploitation in penetration testing.

Beyond the Basics:

1. **Advanced Active Directory Hacking**: Dive deeper into Active Directory security with resources from experts in the field like @PyroTek3, @_dirkjan, and @Haus3c.
2. **Advanced Web Application Hacking**: Explore more advanced web hacking techniques and bug bounty platforms like HackerOne and Bugcrowd for real-world practice.
3. **Certifications**: Consider more advanced certifications like OSCP, which provide practical experience and are highly valued in the industry.
4. **Exploit Development:** Further refine your exploit development skills with advanced topics like heap exploitation and format string vulnerabilities.
5. **Privilege Escalation**: Master privilege escalation techniques on both Windows and Linux systems, including kernel exploits and DLL hijacking.

By focusing on these areas and continually expanding your knowledge and skills through hands-on practice and learning from industry experts, you can build a strong foundation and advance your career in cybersecurity.

Personalized Paths and Practical Advice

The roadmap I provided may not suit everyone's goals and preferences. It's tailored towards those interested in network hacking and web application/API hacking, but there are many other paths to explore within the realm of cybersecurity.

For individuals interested in areas like game hacking, mobile hacking, malware analysis, and more, additional research and exploration are necessary. These fields require specialized knowledge and skills, and there are plenty of resources available to help you dive into these areas.

It's essential to recognize that the journey to becoming a proficient ethical hacker can indeed be overwhelming at times, and it may take anywhere from 1 to 2 years or even longer. Taking your time and enjoying the learning process is crucial, rather than rushing towards the end goal.

Here are some key recommendations and personal advice to keep in mind as you embark on your journey:

1. Network with other hackers and cybersecurity researchers through platforms like Twitter and LinkedIn. Learning from others' experiences and perspectives can be invaluable.
2. Watch hackers' podcasts and engage with online communities to gain insights and knowledge that may not be available in traditional courses.
3. Stay curious about new technologies and updates in the cybersecurity field. The landscape is constantly evolving, so staying informed is essential.
4. Utilize platforms like TryHackMe, Hack The Box, and PortSwigger's Web Security Academy to practice and hone your skills in a hands-on environment.
5. Embrace programming languages as they can help automate tasks and create tools tailored to your work. Programming skills can significantly enhance your capabilities in cybersecurity. python is my personal suggestion along with **C++** or other more
6. Take advantage of free resources available online. There are numerous free courses, tutorials, and learning materials accessible to anyone willing to explore them.
7. Stay active on LinkedIn to connect with professionals, share insights, and discover valuable resources and opportunities within the cybersecurity community.
8. Remember that consistency is key, but it's essential to maintain a healthy balance. Take breaks when needed, and don't hesitate to step away from learning if you're feeling burnt out. Engage in fun activities to recharge and come back with renewed energy and focus.

In the vast world of ethical hacking, there's no one-size-fits-all roadmap that will take you from start to finish. With technology constantly evolving, this field requires a mindset of lifelong learning. Each day presents new challenges and updates, demanding a commitment to continuous education until the day you retire.

When you find yourself stuck along the way, here are some steps to help you navigate through:

1. **Search on Google:** The internet is your best friend. A quick Google search can often lead you to the solution you're looking for.
2. **Use ChatGPT or Similar AI:** AI tools like ChatGPT can provide quick answers and guidance when you need assistance.
3. **Explore YouTube:** YouTube is a treasure trove of tutorials and walkthroughs for almost any topic. A well-crafted search can yield valuable insights and solutions.

Remember, searching for answers is an integral part of the game.

Don't Skip the Fundamentals:

- Introductory Researching: Learn effective research techniques to find information efficiently.
- Networking Basics: Understand the foundations of computer networking, including protocols and architectures.
- Linux Basics: Familiarize yourself with the Linux operating system, a staple in the world of cybersecurity.
- How the Web Works: Gain insights into web technologies, protocols, and communication mechanisms.
- Web Application Basics: Learn the basics of web development and common vulnerabilities.
- DBMS Basics (Database Management System) - Optional: Explore database fundamentals, such as MySQL, which can be invaluable when tackling issues like SQL injection.

By prioritizing these fundamental skills and embracing the ethos of self-directed learning, you'll be well-equipped to navigate the ever-changing landscape of ethical hacking."

While delving into the fundamentals, it's beneficial to simultaneously explore additional areas that complement your foundational knowledge. Here are some topics you can start learning alongside the basics or afterward, depending on your preferences:

1. Basics of Cybersecurity: Understand the fundamentals of cybersecurity, including concepts like the CIA triad (Confidentiality, Integrity, Availability) and various types of malware.
2. Types of Penetration Testing: Familiarize yourself with different types of penetration testing, including Black Box, Gray Box, and White Box testing, along with the steps involved in penetration testing methodologies.
3. Network Hacking: Dive into the world of network hacking by learning about network protocols such as TCP/IP, UDP/IP, HTTP, and FTP. Explore networking tools like Ping, Traceroute, and Netstat, and understand network services enumeration. Also suggest our own book on Networking For Dummies - where it is focused for beginners hackers or who want to delve into the vast field of Computer Networking.
4. Introduction to Web Hacking: Begin your journey into web hacking with introductory courses covering topics like hacking web applications, understanding web protocols, and learning essential web hacking techniques.
5. Hacking Courses: Take advantage of free resources available online, such as YouTube tutorials and Capture The Flag (CTF) platforms, to enhance your skills. Explore courses like TCM Security's "*Ethical Hacking in 15 Hours*" series and practice your skills through CTF challenges.
6. Intermediate Hacking Content: Once you've gained proficiency in the basics, challenge yourself with intermediate-level content covering topics like Linux privilege escalation and Active Directory hacking.

Join Our Communities

Join our vibrant communities at Codelivly and connect with like-minded individuals passionate about cybersecurity and hacking. Here's where you can find us:

Facebook: facebook.com/codelivly
Instagram: instagram.com/codelivly
Twitter: twitter.com/codelivly
Telegram: t.me/codelivly
Telegram Group Chat: t.me/codelivly_chat
LinkedIn: linkedin.com/company/codelivly

Stay updated on the latest trends, discussions, and events in cybersecurity, share your knowledge, and network with professionals from around the world. Join us today and be a part of the Codelivly community!

Conclusion

In conclusion, I trust that you've found this comprehensive guide beneficial on your journey into the realm of cybersecurity and hacking. While this article covers a vast array of topics, it's important to remember that learning in this field is a continuous process, and there's always more to explore and discover.

The links and resources provided here have been instrumental in shaping my own path, and I encourage you to delve deeper into each topic and seek out additional resources beyond what's listed here. Every individual's journey is unique, and your exploration will undoubtedly lead you to new insights and experiences.

With the wealth of information provided, you now have more than enough material to keep you engaged and learning throughout the year. Embrace the challenges, stay curious, and most importantly, enjoy the journey. Happy hacking!

FAQs (Frequently Asked Questions)

What is the difference between white hat and black hat hacking?

- *Answer:* White hat hackers, also known as ethical hackers, use their skills for good, often employed to find vulnerabilities in systems and help organizations improve their security. Conversely, black hat hackers engage in illegal activities, exploiting vulnerabilities for personal gain or malicious purposes.

How can I protect myself from cyber attacks?

- *Answer:* You can protect yourself from cyber attacks by practicing good cybersecurity hygiene, such as using strong, unique passwords, enabling two-factor authentication, keeping your software and devices updated, avoiding suspicious links and attachments, and using reputable antivirus software.

What are common signs of a cyber attack?

- *Answer:* Common signs of a cyber attack include unusual computer behavior, such as slow performance, unexpected pop-ups, changes in system settings, unexplained account activity or unauthorized access, missing or altered files, and unusual network activity.

What is social engineering?

- *Answer:* Social engineering is a manipulation technique used by attackers to deceive individuals into divulging confidential information, providing access to systems, or performing actions that compromise security. It often involves psychological manipulation and exploits human behavior rather than technical vulnerabilities.

What is ransomware and how does it work?

- *Answer:* Ransomware is a type of malware that encrypts files or locks users out of their systems, demanding a ransom payment in exchange for restoring access. It typically spreads through phishing emails, malicious attachments, or compromised websites, and once activated, it encrypts files or systems, making them inaccessible until the ransom is paid.

What is the dark web and should I access it?

- *Answer:* The dark web is a part of the internet that is not indexed by search engines and is often used for illegal activities, such as buying and selling drugs, weapons, and stolen data. Accessing the dark web can be risky and illegal in some cases, as it may expose you to malicious actors and illegal content.

How do I report a cyber crime?

- *Answer:* If you are a victim of cyber crime or encounter suspicious activity online, you can report it to the appropriate authorities, such as your local law enforcement agency, the Internet Crime Complaint Center (IC3), or the Cybersecurity and Infrastructure Security Agency (CISA).

What steps should I take if my accounts are hacked?

- *Answer:* If your accounts are hacked, you should immediately change your passwords, enable two-factor authentication if available, review your account activity for any unauthorized changes or transactions, and report the incident to the affected service provider. Additionally, consider running antivirus scans on your devices to check for malware.

Is DSA important or required to become a cyber security expert?

- *Answer:* While expertise in Data Structures and Algorithms (DSA) is not a strict requirement for becoming a cybersecurity expert, it can certainly be beneficial. DSA knowledge helps in understanding how data is organized, stored, and manipulated, which can be valuable when analyzing and securing systems and networks.