

🛠️ 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.

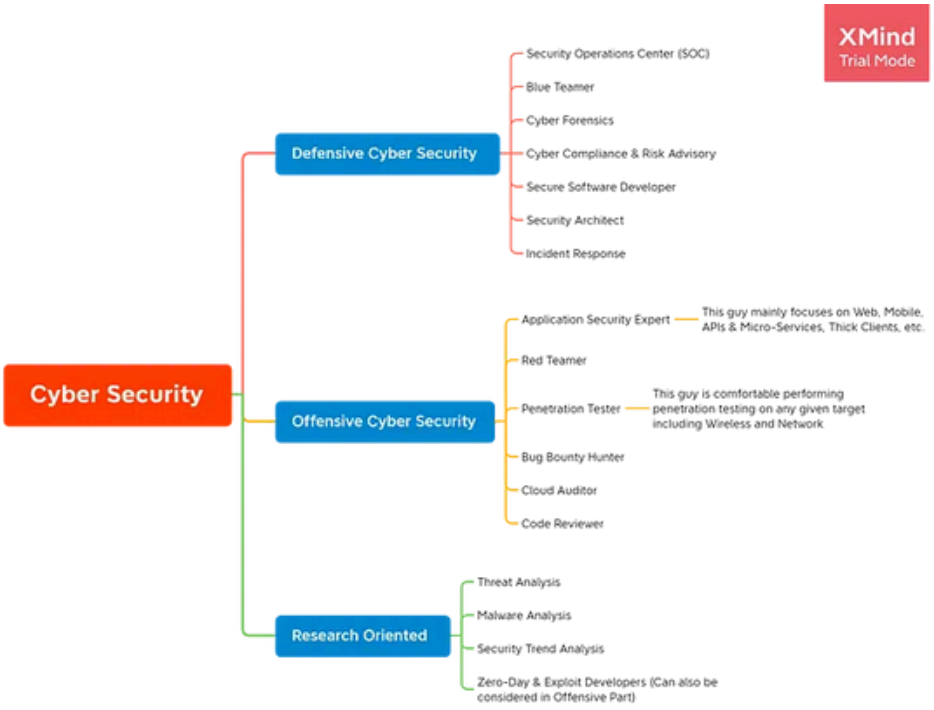
But here's the thing: The journey doesn't stop there. If you're eyeing more senior or specialized roles, you'll need to keep leveling up your skills and gaining real-world experience. That might mean diving deeper into specific areas of cybersecurity or racking up a few years of hands-on practice.

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