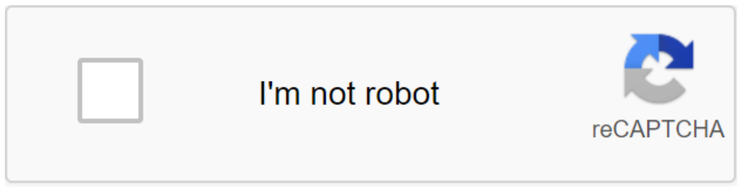
Certified ethical hacking version 9 pdf



Continue

Being labeled as a hacker usually comes with a lot of negative connotations. If you call yourself a hacker, people often perceive you as someone who causes evil just for giggles. But as I described in this article explaining the difference between good and bad hackers, there are also ethical hackers who end up doing similar tasks for good rather than evil. But while ethical hackers exist, is it possible to make a living of ethical hacking? I have studied various steps to getting into an ethical hacking career - training, experience and jobs. It turns out that it is quite possible, but to get into it is difficult and requires a lot of preparation. However, if you stick to it and succeed as an ethical hacker, you can create a very good career path. What is an ethical hacker? A hacker is a person with a computer and/or programming knowledge and skills who use said assets to hack into a computer system and use it. While stereotypical criminal hackers scramble computer systems to cause chaos, ethical hackers try to hack into systems without causing too much damage and then report their findings to the owner. In other words, ethical hackers are finding holes that criminal hackers can exploit and allowing the owner to know about them so they can fix them before any real damage from a criminal hacker is done. Ethical hacking is also known as penetration testing, intrusion testing and red command. Becoming an ethical hacker is not an easy task to accomplish - it requires a lot of knowledge, especially when it comes to the security of computer systems, and a lot of experience to have a chance at the ethical work of hacking. In case I haven't done enough attention on it - experience is vital, even if you have a computer science degree, a certificate, or anything else you may have. Educational training Before you even get to the experience part, however, it's still a good idea to understand how computers work and communicate with each other. All of this can be achieved through a degree in computer science or other similar courses - even taking a few courses through openly available OpenCourseWare from places like the Massachusetts Institute of Technology are a great thing to do if you can't afford to take actual college courses. A degree is preferable, but the knowledge and experience to support it can be effective as well. Gaining experience can get two different ways - freelance jobs and good ol'Messin' around. Using the Internet is crucial because it contains a huge amount of free information to help you learn how you try new things. There are also plenty of resources to watch, such as James' tutorial on how to hack a WEP protected wireless network, Linux distribution, which specializes in penetration testing, and tools such as Droidsheep that filter through unprotected wireless traffic. These are just some very basic ways to get started with the whole concept of hacking, but there are much more advanced topics that you will need to learn in to get a serious idea of what it takes to be an effective ethical hacker. Please remember that in all your adventures, you must stay within the law with your activities. This means that you should practice techniques on your own equipment, or ask the owner's permission before trying anything. If you end up doing something that is illegal, it can permanently damage your reputation in addition to legal issues, fines, etc. Appropriate jobs as you work your way up helps a lot too. Don't expect to go from anything straight to ethical hacking. Getting a job since once you have a good education along with a few years of experience, you are ready to hit it big as an ethical hacker. Freelance jobs are not only a good way to gain experience, but they can also give you a decent amount of income that can increase as your reputation among freelance communities increases. The downside of freelance jobs is that you don't have a stable position, so income is never as certain as you would like. Once you are ready to move away from freelance jobs, you can start applying to various technology companies for permanent positions. Remember that you don't need to contact the biggest tech companies - there are so many small ones that can pay you just as well. In addition, you can also set up a computer security consulting service in order to be able to work for multiple companies at the same time. This can be done in addition to a permanent position, or as a step between freelance work and permanent work. Certified Ethical Hacker In order to legitimize yourself as good in ethical hacking, you can become a Certified Ethical Hacker (CEH) by completing a supplier-neutral certification course. This gives you a well-rounded experience on security issues that you may or may not have covered while you were gaining experience on your own. However, in order to get certified, you must complete the course or have at least two years of experience as approved by the employer. Getting such certification can give you bragging rights as well as more leverage at scoring better jobs or raising wages. The conclusion is as you can see, it's definitely possible to make a living of ethical hacking. While the process of getting to this point is definitely not easy (neither for every computer guy), it can be well worth it if you're good and enjoy doing it. In addition, you can tell others that you are doing them a service while keeping them safe online. Will a career in ethical hacking interest you? What other cool, but unusual job you know? Let us know in the comments! Image Credits: Apple's catatronic, slworking2 shows the powerful and budget-friendly HomePod Mini New HomePod is packed with lots of great features, but don't worry about it breaking the bank. Related topics Programming Job Search Hacking by author Danny Stieben (488 Articles Published) More from Danny Stieben's Best Open Source Online Ethical Hacking Tools used by hackers: If hacking is performed to identify potential threats to a computer or network, then it will be ethical hacking. Ethical hacking is also called penetration testing, intrusion testing, and red commands. Hacking is the process of gaining access to a computer system for the purpose of fraud, data theft, invasion of privacy, etc., by identifying its weaknesses. Ethical Hackers: A person who performs hacking activities is called a hacker. There are six types of hackers: Ethical Hacker (White Hat)CrackerGrey hatScript kiddiesHacktivistPhreakerA security professional who uses his hacking skills for defensive purposes called ethical hackers. To enhance security, ethical hackers use their skills to find vulnerabilities, document them, and suggest ways to fix them.Companies that provide online services or those that are connected to the Internet must perform penetration testing by ethical hackers. Infiltration testing is another name for ethical hacking. It can be done manually or using an automation tool. Ethical hackers work as an information security expert. They are trying to compromise the security of a computer system, network or application. They identify weaknesses and, on the basis of this, provide advice or suggestions for strengthening security. The programming languages used for hacking include PHP, S'L, Python, Ruby, Bash, Perl, C, C, Java, VBScript, Visual Basic, C Sharp, JavaScript and HTML. Few Hacking Certifications include: qgt'; contact us to offer a list here. Below is a list of the most popular Hacker software that is available on the market. Let's explore! #1) Kiuwan Security Code (SAST)Price: Free trial. A one-time scan costs $599. For continuous scanning, visit the Kiuwan website. Kiuwan Code Security is a vulnerability scanning tool. It identifies vulnerabilities in source code using the most stringent security standards, including OWASP, CWE, SANS 25, HIPPA, and more. Integrate Kiuwan into your IDE for instant feedback while you're developing. Kiuwan supports all major programming languages and integrates with leading DevOps tools. Features: Automatic creation of action plans to address vulnerabilities. Integrates with leading IDEs including Eclipse, Visual Studio, IntelliJ IDEA, Phpstorm, Pycharm and Webstorm.Supports 20 programming languages for desktop, web and mobile applications. Best for: Finding and fixing vulnerabilities in the source code during development. Kiuwan also has a tool called Research, which reports vulnerabilities in open source #2 and helps manage license compliance. This is open source software and available for free. Supports cross-platform. It can be used for network networks manage service update schedules, as well as monitor host and service downtime. It can work for one host as well as for large networks. It provides binary packages for Linux, Windows and Mac OS X.Features: Nmap Suite has: Data transfer, redirection and debugging tool (Ncat), utility comparison scan results (Ndiff), Package Generation and Response Analysis Tool (Nping), GUI and Review Results (Nping)Using raw IP packages it can identify: Available hosts on the network. Their services are offered by these available hosts. Their OS. The package filters they use. And many other characteristics. Best for: Nmap is best suited for scanning the network. It's easy to use and fast as well. Website: Nmap-3) NetsparkerNetsparker is a dead-end accurate ethical hacking tool that simulates a hacker's actions to identify vulnerabilities such as S'L injections and cross-site scenarios in web applications and web API.Netsparker unequivocally checks identified vulnerabilities that prove they are real, not false positives, so you don't need to spend hours manually verifying vulnerabilities. It is available as a Windows software and online service.' Visit the Netsparker HereIntruder website is a fully automated scanner that finds weaknesses in cybersecurity in your digital real estate, and explains the risks and helps with their recovery. This is a great addition to your arsenal of ethical hacking tools. With over 9,000 security checks available, The Attacker makes enterprise-grade vulnerability scanning available to companies of all sizes. Its security checks include identifying incorrect calculations, missing patches, and common web application problems such as S'L injection and cross-site scripts. Built by experienced security professionals, Intruder takes care of most of the hassle of managing vulnerabilities, so you can focus on what really matters. This saves you time by prioritizing results based on their context, as well as proactive scanning of systems for the latest vulnerabilities, so you don't need to emphasize this. The attacker also integrates with major cloud service providers as well as Slack s Jira. Acunetix Acunetix is a fully automated ethical hacking tool that detects and reports more than 4,500 web application vulnerabilities, including all s'L and XSS injection options. The Acunetix scanner fully supports HTML5 and JavaScript and one-page applications, allowing for auditing of complex, proven applications. It bakes in advanced vulnerability management functions right into its core, prioritizing data-based risks through a single, consolidated look, and zgt; integrating scanner results into others and platforms. Metasploit Pro is a commercial product. The free trial is available for 14 days. Contact the company to learn more about its price details. This is software for penetration testing. Use of Metasploit Metasploit You can design and execute exploit codes against a remote machine. Supports cross-platform. Features: It's helpful to know about security vulnerabilities. Helps in penetration testing. Helps develop IDS signatures. You can create security testing tools. It is best suited to create tools to combat forensics and tax evasion. Website: Metasploit-7) Aircrack-NgPrice: FreeAircrack-ng provides a variety of tools to assess the security of the Wi-Fi network. They are all command-line tools. To ensure Wi-Fi security, the focus is on monitoring, attack, testing and hacking. It supports Linux, Windows, OS X, Free BSD, NetBSD, OpenBSD, Solaris and eComStation 2.Features:Aircrack-ng can focus on playback attacks, de-authentication, fake hotspots and others. It supports the export of data to text files. It can check the wi-fi card and the driver's capabilities. It can crack WEP keys and for that, it uses FMS attacks, PTW attacks, and dictionary attacks. He can hack WPA2-PSK and for that, he uses dictionary attacks. Best for: Supports any wireless network controller. Website: Aircrack-Ng-8) WiresharkPrice: FreeWireshark is a package analyzer and can perform a deep review of many protocols. Supports cross-platform. This allows you to export access to various file formats such as XML, PostScript, CSV and Plaintext. It provides an opportunity to apply coloring rules to the package list, so that the analysis will be easier and faster. The image above will show the capture of the packages. Features: It can unpack gzip files on the fly. It can decipher many protocols such as IPsec, ISAKMP, sSL/TLS, etc. This allows you to view captured network data using the TShark GUI or TShark utility in TTY mode. Best for: Analysis of data packets. Website: Wireshark-9) EttercapPrice: Free.Ettercap supports cross-platform. Using the Ettercap API, you can create custom plugins. Even with a proxy connection, it can do sniff http SSL protected data. Features: Sniffing live connections. Content filtering. Active and passive autopsy of many protocols.Network and host analysis. Best for: It allows you to create custom plugins. Website: Ettercap-10) MaltegoPrice: Community Version, Maltego CE is available for free. The price for the Maltego Classic is $999. The price for Maltego XL is $199. These are two desktop products. The price for server products such as CTAS, ITDS and Comms starts at $40,000, which also includes training. Maltego is a tool for linking analysis and data analysis. Supports Windows, Linux and Mac OS. To discover data from open sources and visualize in graphic format, it provides a library of transformations. It collects data and collects information in real time. Features:Represents data on site-based graph patterns. Maltego XL can work with large charts. It will provide you with a graphic image, thereby telling you about weaknesses and network anomalies. Best for: It can work with very large graphics. Website: Website: NiktoPrice: FreeNikto is an open source tool for scanning a web server. It scans the web server for dangerous files, outdated versions, and specific problems with versions. This keeps the report in text files, XML, HTML, NBE, and CSV formats. Nikto can be used in a system that supports the basic Perl installation. It can be used in Windows, Mac, Linux and UNIX systems. Features: It can check web servers for more than 6,700 potentially dangerous files. It has the full support of http proxies. Using headers, favicons and files, it can identify installed software. It can scan the server for outdated server components. Best for: As a penetration testing tool. Website: Nikto-12) Burp SuitePrice: It has three pricing plans. The community edition can be downloaded for free. The price of the enterprise edition starts at $3,999 per year. The price of a professional edition starts at $399 per user per year. Burp Suite has an online vulnerability scanner and has advanced and necessary hand tools. It provides many features to keep your web applications safe. It has three publications, community, enterprise and professional. With community publishing, it provides basic hand tools. With paid versions, it provides more features, such as an online vulnerability scanner. Features: This allows you to plan and repeat the scan. It scans 100 common vulnerabilities. It uses out-of-range techniques (OAST). It provides detailed user recommendations for reported vulnerabilities. It integrates CI. Best for: Security testing. Website: Burp Suite No.13) John the RipperPrice: FreeJohn Ripper is a tool for cracking passwords. It can be used on Windows, DOS and Open VMS. It's an open source tool. It's designed to detect weak UNIX passwords. Features:John the Ripper can be used to test various encrypted passwords. He performs dictionary attacks. It provides different password crackers in one package. It provides a customizable cracker. Best for: It's quick in hacking passwords. Website: John the Ripper No. 14) Angry IP ScannerPrice: FreeAngry IP Scanner is a tool for scanning IP addresses and ports. It can scan both locally and online. Supports Windows, Mac and Linux operating systems. Features: It can export the result in many formats. It's a team-line interface tool. It is extensible with many data fetchers. Website: Angry IP ScannerConclusion As explained here, Nmap is used for computer security and network management. This is good for scanning the network. Metasploit is also for safety and good for creating anti-forensics and evasion tools. is a free package sniffer and injector and supports cross-platform. Wireshark is a package analyzer and analyzes data packets well. According to reviews available online, people recommend using Nmap instead of the Angry IP scanner because Angry IP Scanner comes with unwanted applications. John the Ripper is quick in cracking passwords. Nikto is a good open source tool for penetration testing. Maltego presents the data in graphic form and information about weaknesses and anomalies. We recommend reading ethical hacking courses and contact us to offer a list here. It was all about ethical hacking and top ethical hacking tools. I hope you find this article useful! Useful!!