AARON NELSON PH.D

ETHICAL HACKING

FOR BEGINNERS AND DUMMIES

Contents

Introduction

The term hacking has been around for a long time now. The first recorded instance of hacking dates back to the early 1960s in MIT where both the terms, ‘Hacking’ and ‘Hacker’ were coined. Since then, hacking has evolved into a broadly followed discipline for the computing community. Understanding the reason why an individual may want to infiltrate or hack into a system is usually the most difficult task, the intention behind cyber-attacks usually allows room for prevention as the user may be able to defend against any possible system vulnerability. EH is used as a penetration testing tool in order to prevent breach of basic rights, privacy and free will. Ethical hackers are usually professionals or network penetration testers who use their hacking skills and toolsets for defensive and protective purposes. Then again there are three sorts of programmers: Black Hat, Grey Hat and White Hat as indicated by (Hoffman 2013). White Hats are usually software engineers that hack for good, and hack with respect to corporate/business networking structures. A Grey Hat hacker may do things imperfect in nature, however not to intentionally hurt people or damage systems, unless there is a genuine positive result. A Black Hat Hacker will maliciously misuse computers and networks with pernicious aim, with no legitimate reason. Hacking also means accessing a system that one is either not authorized to access, or who accesses a system at a level beyond their authorization, clearly abandoning the possibility of ethics being applied to it. The rise in cybercrime is a major breaching issue for organizations and it has been reported that over 30,000 SME websites are hacked daily. The need for advanced cyber security is a necessity to fight of Black Hat Hackers, and organizations all over the world need to start implementing such procedures to protect their businesses, but the costs related to EH make it impossible for smaller companies to cope. EH is gone beyond just professionals as universities all around the world have been offering courses to graduate and undergraduate students to increase their understanding on how to protect data and apply security procedures in an ethical way. Making it easier for organizations to employ talent rather than pay for services from external organizations, however teaching young students the profession of hacking without knowledge of their intent could be suicidal. EH can be applied to many circumstances however this paper will discuss the advantages and disadvantages of EH within three

separate sectors, education, business and governmental to allow the reader to truly understand and grasp the importance of the subject at hand.

“Ethical hackers employ the same tools and techniques as the intruders, but they neither damage the target systems nor steal information. Instead, they evaluate the target systems’ security and report back to owners with the vulnerabilities they found and instructions for how to remedy them. In addition, EH is applying penetration testing, or deliberately accessing networks through ‘unlawful means’ specifically to decide the depth of a system's security, these tests are usually carried out by larger corporations. Organizations and large corporations today are under huge pressure to shield their data from external and inner security dangers towards their computer frameworks. Accordingly the majority of them have taken precautionary arrangements of employing Ethical Hackers. "To catch a thief, you must think like a thief. That’s the basis for ethical hacking. Knowing your enemy is absolutely critical. In other words Ethical Hackers are experienced security and system specialists that play out an assault on an objective framework with authorization from the company, in order to discover escape routes and vulnerabilities that malicious hackers could exploit, this procedure is additionally known as Penetration Testing. The true objective of ethical hackers is to learn framework vulnerabilities with the intention to repair the damage and help organizations fight of cyber criminals. Every Ethical Hacker has to follow three critical guidelines: Firstly ‘working ethically’. All activities performed by the hacker has to benefit the association’s objectives and so Reliability is an absolute fundamental. Secondly ‘respecting privacy’ as all data that is collected must be treated with the most extreme regard, and finally making sure ‘systems remain intact’ this usually takes place due to the hacker taking the system lightly. The procedure of EH contains a wide range of steps. The primary thing that is done is to detail out a step by step plan. At this stage getting approval and an agreement from the association to carry out the infiltration test is critical. Next the ethical hacker utilizes filtering systems to check for open ports on the framework. Once a malicious hacker scans all computers and realises which operating system they use than almost all kinds of attacks are possible. This strategy is utilized by Black Hats with malicious intent or purpose. After careful examination the ethical hacker will choose the instruments that he will use for specific tests on the network. These tools can be used for password cracking and planting entry points for future attacks.

The tests should be precisely performed, on the off chance that they are done inaccurately they could harm the framework. Finally the arrangement should be executed and the after effects of the considerable number of tests should then be assessed. Based on the outcomes the ethical hacker informs the company concerning their security vulnerabilities and also how they can be fixed to make it more secure.

What is Hacking

Hacking is the activity of identifying weaknesses in a computer system or a network to exploit the security to gain access to personal data or business data. An example of computer hacking can be: using a password cracking algorithm to gain access to a computer system. Computers have become mandatory to run a successful businesses. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. System hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cybercrimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.

What is Ethical Hacking?

Hacking is the process of finding vulnerabilities in a system and using these found vulnerabilities to gain unauthorized access into the system to perform malicious activities ranging from deleting system files to stealing sensitive information. Hacking is illegal and can lead to extreme consequences if you are caught in the act. People have been sentenced to years of imprisonment because of hacking. Nonetheless, hacking can be legal if done with permission. Computer experts are often hired by companies to hack into their system to find vulnerabilities and weak endpoints so that they can be fixed. This is done as a precautionary measure against legitimate hackers who have malicious intent. Such people, who hack into a system with permission, without any malicious intent, are known as ethical hackers and the process is known as ethical hacking. So now that we know what exactly ethical hacking is, and who ethical hackers are, let’s go over the different types of hackers.

What are the types of Hackers?

Hackers can be segregated according to their intent.

White Hat Hacker

White Hat Hacker - It is another name for an Ethical Hacker. They hack into a system with prior permission to find out vulnerabilities so that they can be fixed before a person with malicious intent finds them.

Black Hat Hacker

They are also known as crackers, who hack in order to gain unauthorized access to a system & harm its operations or steal sensitive information. It's always illegal because of its malicious intent which includes stealing corporate data, violating privacy, damaging the system etc.

Grey Hat Hacker

Grey Hat Hacker - They are a blend of both black hat and white hat hackers. They mostly hack for fun and exploit a security weakness in a computer system or network without the owner's permission or knowledge. Their intent is to bring the weakness to the attention of the owners & earning some bug bounty.

Suicide Hacker

Suicide Hacker - A suicide hacker is a person who works with the intent to bring down major corporations and infrastructure. These kinds of hackers are not scared of the consequences of their actions as they mostly work with a vengeance in their mind. These people are also known as hacktivists.

What are the different types of hacking

Now that we have discussed the various types of Hackers, let’s go over the different types of hacking. We can segregate hacking into different types depending on what the hacker is trying to achieve.

Website Hacking

Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.

Network Hacking

Hacking a network means gathering information about a network by using tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. with the intent to harm the network system and hamper its operation.

Email Hacking

This includes gaining unauthorized access to an Email account and using it without taking the consent of its owner for sending out spam links, third-party threats, and other such harmful activities.

Password Hacking

Password Hacking - This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.

Computer Hacking

Computer Hacking - This is the process of stealing computer ID and password by applying hacking methods and getting unauthorized access to a computer system.

Phases of Ethical Hacking

Like every discipline out there in the world, ethical hacking is divided into distinct phases. Ethical hacking has 6 distinct phases. These phases are not strict rules, but more like a guideline to be followed.

Reconnaissance

Reconnaissance is the process of information gathering. In this phase, the hacker gathers relevant information regarding the target system. These include detecting services, operating systems, packet-hops to reach the system, IP configuration etc. Various tools like Nmap, Hping, Google Dorks etc are used for reconnaissance purposes

Scanning

In the scanning phase, the hacker begins to actively probe the target machine or network for vulnerabilities that can be exploited. Tools like Nessus, Nexpose, and NMAP are widely used by hackers in this process.

Gaining Access

In this phase, the vulnerability located during scanning is exploited using various methods and the hacker tries to enter the target system without raising any alarms. The primary tool that is used in this process is Metasploit.

Maintaining Access

Cyber Security Training

This is one of the most integral phases. In this phase, the hacker installs various backdoors and payloads onto the target system. Just in case you don’t know, Payload is a term used for activities performed on a system after gaining unauthorized access. Backdoors help the hacker gaining quicker access onto the target system in the future.

Clearing Tracks

This process is an unethical activity. It has to do with the deletion of logs of all the activities that take place during the hacking process. Nonetheless, Ethical Hackers still have to perform this phase to demonstrate how a Black

Hat Hacker would go about his activities.

Reporting

Reporting is the last step of finishing the ethical hacking process. Here the Ethical Hacker compiles a report with his findings and the job that was done such as the tools used, the success rate, vulnerabilities found, and the exploit processes.

Reasons to Learn Ethical Hacking

Ethical Hacking is compromising computer systems for assessing their security and acting in good faith by informing the vulnerable party. Ethical hacking is a key skill for many job roles related to securing the online assets of an organization. The professionals working on these job roles maintain the organization's computers, servers and other components of its infrastructure in working conditions preventing unauthorized access through non-physical channels. If you are a student or a budding IT professional, you might be thinking about learning ethical hacking as a career option. In this book, we will tell you how you might be thinking just right. The reasons are evaluated on the parameters of earning, future scope, social status, self-satisfaction, and intellectual growth.

Pays Well (More Than Well)

Cyber Security professionals get a much higher median salary than their counterparts in the field of computer science. This is for the simple reason that protecting what's built online against cyber-attacks is essential to the company's growth and sustainability. A cyber-attack can not only cost in terms of immediate damage to the systems and finances but also terms of user trust. For these reasons, companies pay decent salaries to their cyber warriors. For this reason, companies pay a decent starting salary with an average hike of 50% per year according to Simplilearn, an ed-tech firm.

Highly In-Demand Skill

Cyber security as a profession has not received much enthusiasm until in very recent years (2016+). The main reason for this is considered the fact that companies tend to underestimate the criticality of their internet-facing systems. Things changed after a series of massive cyber-attacks on large companies that were responsible for running many websites by providing hosting, cloud storage, and other services. Due to this trend, there is a wide gap between the sudden need for highly skilled professionals and a few number of such professionals. In India, there are 30, 000 cyber security posts currently unfilled, according to Economic Times. The gap is almost the same

at the global level too. The global market of cybersecurity is expected to grow to $35 billion by 2025.

Help in Creating a Secure Internet for All

Not all the cyber attacks require complex exploits. Some require finding a gullible person and luring them into giving up their credentials. Phishing is a highly used technique for this purpose. It is very likely that one or more such attempts of phishing were made on you too(You might have seen some shady emails about winning a grand sum of money or some refugee having trouble in managing millions of dollars), but since you were smart, you didn't fall for those. (You didn't right?). A basic understanding of how cyber attacks work and how one can be safe online can be the key to preventing such frauds. This is why everyone should learn about basic ethical hacking principles and tools.

One Can Become a National Asset

Cybersecurity professionals will be the soldiers of future warfare which will be primarily about securing own online systems and destroying enemies'. Since almost every device, even the ones with the highest criticality will be connected to some network. Cyberwarfare goes on even during times of no apparent tension among countries. Country A may try to use its skilled hackers to:

• Take over and disable large power grids of country B.

• Disrupt share markets of country B.

• Intervene in national or state elections of country B.

• As a cybersecurity professional, you will be useful in the prevention of your national assets and reputation from jeopardy.

Good to Learn Something New

One needs to learn a variety of things before they can think of learning ethical hacking. Programming, scripting, computer networking, web technologies, cryptography, etc. are some of the subjects to be mastered before expecting a decent and smooth introduction to ethical hacking. Being an active cybersecurity professional also requires staying updated on newly discovered vulnerabilities, their exploitation, and mitigation, new frameworks, new attack techniques, new bypasses to previous mitigations, etc. This is as pleasantly challenging as it sounds.

Places to Practice Ethical Hacking

The practice is essential for mastery of an art. Hacking is mostly an art since it's more about how you use the tools you know and less about how many tools you know. While it might be easy to get a basic idea of what a certain technique is about during introductory phases, getting comfortable with that technique is highly improbable without hands-on practice. The majority of ethical hacking skills can be practiced with a decent computer and an internet connection only. Some of the skills may require additional hardware like adapters and controllers. For example, WiFi hacking on Virtual Machine will require an external WiFi adapter. Similarly, RFID hacking will require an appropriate RFID kit with the scanner and key cards. Setting up a system for practicing will require download and installation of tools. To setting up your virtual lab for practicing ethical hacking, go through this book.

PortSwigger's Web Security Academy Labs

You must have heard of BurpSuite, the tool used for penetration testing of web applications. The developers of BurpSuite now provide free of cost online training in web application security. The training contains tutorials and labs on almost every vulnerability commonly found in modern web applications. Once you are good enough, you can compete with others in solving a newly added challenge before others. They have a HOF for expert hackers and provide swag for top performers.

HackTheBox

HackTheBox is a collection of vulnerable applications called "machines". Each of the machines is unique and contains a set of vulnerabilities, the hacker has to compromise it and gain the required privileges. The good thing about HTB is that a large number of machines are already there for practice and walkthrough tutorials are available in case you are stuck. New ones are added regularly containing most recently found vulnerabilities. The free version offers access to "live" machines only, old machines and walkthroughs are available on a paid subscription.

Hack This Site:

This one is very famous among hackers, probably because its founder got arrested for illegal cyber activities. The negative fame has helped well in marketing HackThisSite without significant efforts. HackThisSite is versatile. The hacking challenges on this site are called “missions” and are classified like:

- Basic missions
- Realistic missions
- Application missions
- Programming missions
- Phone phreaking missions
- Javascript missions
- Forensic missions
- Extbasic missions
- Stego missions
- Irc missions

As quoted on hackthissite.org, “You should Tune in to the hacker underground and get involved with the project”.

PentesterLab

One of the biggest platforms for web application security, PnetesterLabs hosts tutorials and labs on a very wide range of vulnerabilities of the web. But its quality content costs more than a decent sum. We advise you to keep checking the website for promos, as the courses can be grabbed at as little as 25% of the original price during certain promo events. PentesterLab has exercised on XSS, SQLi, XXE, CSRF, SAML related vulnerabilities, cross-

site leakage, and many more.

HellBound Hackers

The name sounds badass, and the site lives to its name. It has books, tutorials, hacking challenges, and a forum. You can practice web hacking, email tracking, software cracking, encryption challenges (which are decryption challenges), steganography, and even social engineering. Hell Bound Hackers have been under controversy for allegedly distributing “hacking tools”. However, this page on their site clarifies that they are providing security-related material in a legal manner.

How Should I Start Learning Ethical Hacking on My Own?

Ethical hacking refers to offensive testing of computer systems in order to find out security-related loopholes. These loopholes are called security vulnerabilities. It has been a very popular career choice for students of all backgrounds (non-CS students can also learn it easily and be equally good as CS students, or even better than them). Since ethical hacking is about compromising the systems, it assumes familiarity with how those systems actually work. During your process of hacking (ethically), you will come across networks, networking devices, networking protocols, websites, web technologies, content delivery mechanisms, and many more components of online infrastructures. Being comfortable with what these components do and how they work together is essential. Knowledge of the markup language of the web (HTML) a scripting language(JavaScript) a data transfer language(XML or JSON), components of a web-based system, knowledge of computer networks and TCP/IP suite, knowledge of basic programming in C/C++/Java/Python is good enough to get you started. You can learn ethical hacking effectively by following this two-step process. The first step would be to learn about concepts and to understand them well. On the internet

Hacking for Dummies: The “for dummies” series of Wiley focuses on publishing beginner-friendly books on various topics. This book introduces the user to ethical hacking through concepts and tools. It is very useful for people who want to start learning ethical hacking but are not very comfortable with programming. This should however be understood that being an elite hacker is almost impossible without learning to program.

CEHv10 Study Guide by SYBEX: This book is aimed to aid the preparation of CEH(Certified Ethical Hacker), a popular certification course in ethical hacking. It explains the ethical hacking methodology and the phases of it. Each phase of ethical hacking is well explained with details of the concepts and practice on the tools.

Hacking, the Art of Exploitation: This book has been very popular in the

community of white hat hackers for a long time. Probably because of the content it covers and the depth it goes into. The good thing about this book is that even if you are a novice with absolutely no knowledge about programming and networks, you can still benefit immensely. The book covers Basic Programming in C, Scripting with Bash, basics of memory management in computers, filesystems, overflow based vulnerabilities and their exploitation, basic networking, attacks on networks, writing shell-code, and cryptology.

How to Make a Career in Ethical Hacking

Indeed, Cyber Security is one of the fastest evolving industries across the world. Moreover, due to the rapidly increasing number of cyber-attacks, almost every organization is demanding for the professionals who can deal with such situations and can take preventive measures to avoid the security breach or loss of data. And here comes the role of Ethical Hackers – a cybersecurity professional who legitimately assess or penetrates the organization's network structure to find security vulnerabilities and fix them accordingly. There are various IT giants like Microsoft, Intel, Amazon, etc. that offer ravishing career opportunities in the Ethical Hacking domain. Before moving further, let's take a brief introduction to Ethical Hacking. Ethical Hacking is a lawful practice of getting into the system or network which is done by professionals to identify potential security threats and data breaches in the organization's network. The main aim of practicing Ethical Hacking is to strengthen the network security system of an organization. Moreover, Ethical Hackers are also known as 'White Hat Hackers' and follow the same techniques & methodologies as Black Hat Hackers but in a lawful and authorized manner. An Ethical Hacker can be responsible for various roles & responsibilities in an organization such as:

• Determine the security breaches and vulnerabilities in the organization's system or network.

• Regularly monitor the data flow, network activity, etc. to analyze the security level.

• Comes up with various suggestions & plans for network security improvements.

• Conduct penetration tests on the latest embedded security measurements, etc.

Now the question arises – How to make a successful & worthwhile career in Ethical Hacking? And with the same concern, let's go through the

complete career path that needs to be followed to get into Ethical Hacking:

Start with the Academics

This is the first & foremost thing you need to do to make a career in Ethical Hacking – ensure your study field is concerned or related to the Ethical Hacking (in general, CyberSecurity or IT world!!). Although, it is not mandatory to have a specific educational background for getting into the Ethical Hacking field still having a degree or academic background in the related domain such as Computer Science, Information Technology, etc. will lay your foundation and help you to make it big in the Ethical Hacking. You can opt for Bachelor's or Master's degree in CS/IT or can also go with specific programs or courses related to Ethical Hacking. Moreover, various organizations also demand these educational qualifications as prerequisites while recruiting for Ethical Hackers.

Learn Programming Languages & Operating Systems

For being a worthwhile Ethical Hacker, you're required to get proficient with Programming Languages and the frameworks. It helps Ethical Hackers to identify programming errors or vulnerabilities, implementation of security solutions, automation of the tasks, and many more aspects. You can opt for programming languages like C/C++, Java, Python, Ruby, etc. to get into Ethical hacking. Meanwhile, you're also required to learn about several Operating Systems such as LINUX, UNIX, Windows, iOS, etc. You must have a thorough understanding of the functionalities of these operating systems along with the respective commands to emerge as an affluent Ethical Hacker.

Sound Knowledge of Network & Security

Needless to say, understanding of Computer Networks & CyberSecurity concepts is the core aspect of Ethical Hacking. You're required to have a knowledge of computer networking & security from basic to the advanced level such as Virtual Private Networks (VPN), firewalls, cryptography, Denial of Service attacks (DoS attacks), etc. Although several hacking concepts such as Penetration Testing, Cloud Computing malware, SQL Injection, Vulnerability Assessment, and various others are also required to be taken into consideration. You can opt for books, tutorials, journals, and

various other resources command over the computer networks and cybersecurity concepts.

Join Training Programs to Enhance Ethical Hacking Skills

Ethical Hacking is a vast and in-depth domain and you're required to acquire the knowledge of ethical hacking from beginner to advanced level to get expertise in the field. Meanwhile, you can start to learn Ethical Hacking skills through reading books. But after reaching a certain level you'll be required to interact with the professionals, gain some practice knowledge, etc. to gain more exposure and understanding of the domain. And with the same concern, you're recommended to go for relevant and worthwhile training programs or boot camps to learn and practice the ethical hacking skills in a real-world environment.

Get Relevant Certifications

Once you'll get done with the above-mentioned learning processes, now you're required to get certified and validate your ethical hacking skills. These certifications will not help you to prove your knowledge & skills but can directly land up you various career opportunities in IT giants even without having enough experience in the industry. There are various prestigious certifications in the Ethical Hacking domain such as Certified Ethical Hacker, Global Information Assurance Certification, Offensive Security Certified Professional, Certified Vulnerability Assessor, and various others. Among all these certifications, Certified Ethical Hacker (CEH) is one of the most demanding and renowned ethical hacking certifications. The CEH exam consists of 125 multiple-choice questions related to the ethical hacking field such as SQL Injection, Backdoors, Session Hijacking, etc. that need to be solved within 240 minutes.

Dive into Ethical Hacking Profession

Now, it's time to start your professional career in the field of Ethical Hacking. In the initial stages, you can start with several entry-level jobs in the domain such as Security Analyst, Penetration Tester, etc. and then switch

over to senior-level Ethical Hacker jobs. There are various job profiles associated with ethical hacking such as Network Security Administrator, System Manager, Web Security Manager, Information Security Manager, and many more. Meanwhile, Apart from the private IT giants, you can join several government organizations such as the investigation department, law & military enforcement, etc. as Ethical Hackers.

Some Important terms in Ethical Hacking

Authorization:

The organization gives official permission to access something or do something with the network or application. For example, suppose an organization XYZ gives you permission to access the admin panel and to make changes for the organization. It ensures and confirms the user identity to enter the system. For example, to enter the examination hall you need to show your identity card. In the same way, you need to confirm your identity by logging in with your credentials to enter the system.

Vulnerability Assessment:

To identify the risks or threats in the network or web application. If any vulnerability is found, it will enable the hacker to access the data and manipulate it. So, Vulnerability Assessment can help organizations to make their web applications and networks more secure when tested by white hat hackers.

Penetration Testing:

Vulnerability Assessment includes Penetration testing or pen testing, i.e., identifying vulnerabilities in a network or applications by testing it. The main goal of pen testing is to find vulnerable loopholes in applications and patch them to avoid black hat hackers to exploit them. So, by pen testing, you can secure a web application and network and therefore it is one of the most important terms in ethical hacking.

How to Set Up a Personal Lab for Ethical Hacking

Ethical hacking is a skill that is learned over time. It requires practice and patience to get to a decent skill level in this field. Having a lab setup handy can help you a lot in your learning. A lab lets you practice your skills in a controlled environment, reducing the risks that arise from practicing on real systems. Having your virtual lab will help you in many ways:

• You can practice anytime as per your convenience.

• You don’t have to put your data under the dangers of getting wiped because of malware infection.

• You are also saved from legal troubles that may result from testing on a real website that you do not own.

• You get the freedom to experiment and tweak around (mostly impossible with online labs).

• The requirements for setting up the lab are hardware and software tools. Let’s go through the hardware requirements first.

Hardware Requirements:

• A laptop or a desktop with as much RAM and processor power you can arrange.

• A large HDD or SSD to store your tools and other important files.

• A host OS for your computer system. It can be Windows, Linux(any family, any flavor) or Mac OS depending on your choice.

• Latest security patches must be installed on your guest OS before you start.

• A WiFi adapter that supports monitor mode. (Optional)

Software Requirements:

Virtual Machine Player or Hypervisor: This will be used to host all the guest operating systems, vulnerable virtual machines, and test servers. There are many free and paid options for hypervisors provided by many vendors. For example, VMware has VMWare workstation, Oracle has Oracle VirtualBox and Microsoft has HyperV. You can choose any of these depending on your choice and budget.

Guest Operating Systems: Guest operating systems will include unpatched versions of Windows and Linux. These will be installed to test for zero-days and other vulnerabilities for which patches, as well as exploits, have been released.

Vulnerable VMs: Vulnerable Virtual Machines are developed intentionally for being highly vulnerable. Most of the VMs are parts of hacking events and are released later online. These VMs are usually CTFs with hidden strings that are to be found after compromising (pwning) the VM. Some popular vulnerable VMs are Metasploitable, OWASP broken web application, DVWA (Damn Vulnerable Web Application), BadStore, De-Ice, and Multidae, etc.

Essential Tools:

Once you have found and installed your favorite vulnerable assets, it is now time to get the tools required for pwning them. Install these tools on your computer to get started.

Metasploit Framework (MSF): An open-source version of the Metasploit tool is used extensively for exploiting known vulnerabilities in systems and software. The exploit list is updates regularly with exploits of most recent findings that went public.

WireShark: It is a tool used by network administrators but you can use it to supplement your hacking tools arsenal. For you as a hacker (ethical, of course) this tool will help in network pentesting by the same basic feature of network monitoring: it can help you harvest sensitive data like plaintext

passwords over unencrypted connections (http, telnet), analyze malware behavior by figuring out the endpoints it tries to connect, and many more.

Nmap: One tool to rule ’em all, it is used by almost every penetration tester. It is a port scanner with a set of additional utilities like OS detection and network mapping (nmap stands for “network mapper”). It can be automated by writing scripts in NSE (nmap scripting environment). Port scans are used to enumerate services and applications on the target. These enumeration data can be really useful in some cases for pwning the target.

John The Ripper: It is a free and open-source password cracking tool which is highly popular among penetration testers. Popularity is the reason why it is available on fifteen platforms. The tools were initially designed for cracking UNIX password hashes. However, the latest stable release from May 2019 supports Windows NTLM, Kerberos and hundreds of other hashes.

Burpsuite or OWASP ZAP: Both are great all in one tool for penetration testing web applications. Learning about hacking web applications is crucial for an aspiring (ethical) hacker since most of the services are provided online. These two tool-sets contain all the tools you will need for hacking (ethically) into a web application.

Kali Linux: It is an operating system developed primarily for white hat hackers and penetration testers. This OS has a wide array of tools for almost every task before, during and after a penetration testing session.

Phishing in Ethical Hacking

Go through the “Spam” section of your Email. What do you see?? You might have won a brand new Audi or a mind-boggling amount in a lottery that you didn’t even purchase, asking for credit card details. Or your bank might be asking to verify your account details via email in urgency. Do you see things similar to the above cases in your spam section? Phishing is a type of Social Engineering attack that aims to obtain sensitive information including the bank account number, usernames, passwords, and credit card details. It is mostly done by sending fake emails that appear to have come from a legitimate source, or it can be in the form of Vishing. The recipient is mostly manipulated to click a malicious link that can install malware or access sensitive information. Or it can simply be a case of Typosquatting that redirects the recipient to a malicious website in order to obtain login credentials.

Common Features of Phishing Emails:

• It will have an eye-catching subject such as “Congratulations! You’ve won an iphone”.

• It will reflect a sense of urgency so that the recipient doesn’t get enough time to re-think and make a mistake in the hurry that can later benefit the attackers.

• It will have attachments that make no sense with respect to that email.

Threats of Phishing:

Almost all kinds of Internet theft is possible through Phishing. It can be very dangerous if the received malicious link is being clicked. It can:

• Redirect to a website used for malicious purposes.

• Install malware or Ransom ware to the PC.

• Steal confidential data of the Internet users such as credit card information.

• Steal the identity of the users for the purpose of Identity theft.

Preventive Measures:

The first and foremost thing that I recommend is to go through the email thoroughly. The attackers make tiny mistakes which often gets skipped while reading. Re-check the spellings, the source, the subject before taking any further step.

Computer security tools should be in updated form.

Never open suspicious email attachments.

Never click on suspicious email links.

Don’t provide confidential information via email, over phone or text messages.

Don’t post your personal data, like your vacation plans, or your address or phone number, publicly on social media.

Ethical Hacking Benefits

From coast to coast and in countries around the world, businesses are spending millions of dollars and countless IT hours to keep hackers out of their computers. So, it may seem counterintuitive that some businesses are welcoming the hackers with open arms. It may seem strange, but businesses are using ethical hackers to identify weak points in their cyber defenses, provide valuable insights into the actions of their less ethical counterparts and create better, stronger and more resilient networks. If you do not think that a hacker could help your business instead of hurting it, you may want to rethink those assumptions

They Know How the Bad Guys Think

Even if you have an IT background, getting inside the mind of a hacker can be a real challenge. Failing to understand how hackers think and what they want could be devastating to your business, and the bad guys are ready to exploit your blind spots. They may be ethical in their actions, but white hat hackers know what makes their less scrupulous counterparts tick. They understand how hackers operate, and they can use that knowledge to protect your network for intrusion.

They Know Where to Look

Each business network is amazingly complex, with interconnected computers, mobile devices, home-based workers and traveling employees logging on from the road. Knowing what to look for when assessing cyber security can be a real challenge, but ethical hackers know where to start and where potential weak spots are likely to be hiding.

They Can Expose Weak Spots You Have Overlooked

You may think your network is as secure as possible, but it could have hidden weak spots you do not know about. Those weaknesses may be invisible to you, but an experienced ethical hacker will see them from a mile away. Finding hidden weaknesses in their cyber defenses is one of the biggest reasons to hire an ethical hacker. These good guy hackers are experts

at finding open ports, back doors and other possible entry points into your computer network.

Their Testing Skills are Second to None

Testing and retesting your network is a key part of successful cyber defense, but the success of the strategy rests on the skillfulness of the testers. If the people testing your network do not know what to look for, you could end up with a false sense of security – and a devastating data breach. When it comes to network testing and intrusion detection, ethical hackers are second to none. With years of experience probing networks for weaknesses, they know how testing should be conducted, so you can rely on the accuracy of the results.

They Can Help You Build a Robust Network from the Start

If you are new to the business world, making an ethical hacker part of your start-up team can help you build a better and more robust network. Building a computer network with built-in security features will vastly reduce your susceptibility to breaches and data theft and employing white hat hackers gives you a major advantage. Members of the ethical hacker community have seen all kinds of networks, and they understand how those systems should be constructed. If you want to build a network that is fast, scalable and resistant to hacking, these experts can help you do it. It may seem strange to invite hackers into your company, but the right hackers can actually enhance the security of your organization and your network. Employing ethical hackers is a great way to test your cyber defenses, so you can build a better and safer corporate network.

Disadvantages of Ethical Hacking

Following are the disadvantages of Ethical Hacking:

• It sometimes corrupts the files of the organization.

• Ethical hackers often use vital information and get out of it useful insights for malicious use.

• Ethical hackers are very costly. They incur high charges if any company hires them.

• The company’s privacy is compromised.

• This system is not legal.

• Denial of service attacks are quite common

• It can hamper system operation.

SME’s and applying Ethical Hacking.

Having the adequate preventative measures in place to prevent security breaches within an organization is very important in society today. As technology has grown vastly over time and computer networks becoming a necessity to speed up business processes, it has become paramount for SME’s to take security procedures to prevent breaches. Most businesses today secure confidential client data and information which in compliance with data protection can only be seen, touched or changed by the client himself and the business they are in contract with. However businesses are vulnerable to malicious cyber-attacks and security breaches due to the lack of security measures in place by the organization itself, leading to a leak of confidential information.

Regardless of the level of security breach there is a dispute on whether EH is suitable or will benefit all organizations. Knowing hacking can be a very powerful tool in order to protect organizations and society and it could protect companies from malicious attacks due to weaknesses within their security. However due to a lack of resources or no particular concern it is very unlikely for a company to take protective measures against such attacks. A recent survey from Unisys and Ponemon institution found that nearly 70% of firms responsible for power, water and other crucial infrastructure have suffered at least one security breach which had led to a loss of confidential information. 64% expected another serious attack to take place at the end of the reported year however only 24% of the companies ranked information security as a serious threat and strategic priority.

The protection of company infrastructure could come down to the pressure put on organizations by Grey Hat hackers who look for security breaches within a business infrastructure for the better good of society as they believe the importance of society is far more greater than the importance of consumers. It is evident from vast amount of cases that huge corporations such as Microsoft, Paypal and Apple have delayed strict security breaches with each vulnerability only taking a matter of minutes to repair. If a company is to separate finances for the purpose of protecting client information they would indeed benefit the public however the costs of doing

so would inevitably wound the pocket of the company.

The costs for employing programmers has increased over time with the development of technology and major companies which would affect the economy of a country are being targeted, therefore it is vital for such infrastructures to have security precautions in place. However SME's are organizations which are a lot smaller and applying strict security precautions would costs a great deal of money, making it financially difficult to exist. The fact that EH costs a lot of money and hackers who have studied the profession charge preposterous amounts contradicts the "ethics" behind ethical hacking. How can organizations hire ethical hackers to protect and apply security measures for their infrastructure if they cannot afford to do so? The profession almost seems like a scheme to hold organizations ransom as there is a need for a hacker's expertise. Therefore it is vital for smaller organizations to look for alternative roots to protect their data from potential hacks in the near future, there are several free open source web tools which could be used for penetration testing. It is important for all information to be stored on external infrastructures which are not connected directly to a network making it near impossible for hackers to steal information unless the hacker is working within.

This is an easy and cheaper alternative for SME's to protect confidential information and safeguard their data. If however an SME does decide to seek help from an external organization to protect their data, then as an organization they would need to understand they are allowing an 'ethical hacker' to look through unauthorized information and putting trust in someone who has no emotional attachment to the organization, therefore the possibility the hackers intent could change exists.

It is clearly evident that as technology continues to grow the number of SME's with a network connection in order to trade online also grows, which mean the threat of hackers breaching a system increases. Small firms are attacked with viruses, denial of service and worm attempts at an average rate of 500 attempts every month.

SME's accounted for 99.1% of the UK's population. The average cost of a company's most serious breach is in the region of £1000 and for larger organizations 120,000 it was also reported in a survey from IBM in 2005 that

over 237 million security attacks were carried out against companies over the course of 6 months. Since the majority of the UK’s economy is SME populated it is vital to apply a strong IT security infrastructure in order to reduce financial losses and security breaches.

Ethical Hacking at a Government Level.

In order for the government to protect valuable information to protect the country from possible terrorist attacks or breach of national security EH is considered with the utmost importance. Fighting against terrorism is the highlight of every nation and is considered as of the highest priority, therefore the use of EH in order to counteract major attacks on their security systems is an obvious fundamental. However this is not the only requirement, EH could be used as a tool in order to reduce crime rate, and to protect individual data and confidentiality. Numerous cases have been addressed with Metropolitan Police successfully tracking down hackers stealing confidential information. EH on a Government level will require the programmer to handle information with strict secrecy and delicacy, information on the countries weaponry and defense systems could aid enemy nations, which is clearly a matter of national security and could lead to potential terrorist attacks. However such information cannot be handed over to penetration testers solely on trust alone, information of such requires a nations trust to be placed in the hands of programmers, the possibility of an ethical hacker using their knowledge to carry out malicious activities or to blackmail government officials always remains a possibility. If ethical hackers learn about the vulnerabilities within a government infrastructure they could easily destroy the entire system with illicit coding or malware. However the likelihood of such a scenario taking place remains slim as correct precautions would take place before penetration testing begins. Acts carried out by Government officials may not be deemed ethical even though they justify it as a method to counter terrorism. EH has been used to spy on American citizens, breaching privacy and confidentiality. Glenn Greenwald a US American journalist known for his patriotism covered an amazing story which leaked confidential government data, including documents on how America spied on its millions of citizens in the name of countering terrorism. The use of EH was inappropriate even though the outcome was for the better good, millions of citizens were spied on and information on their private affairs were in the hands of government officials. Edward Snowdon, now seeking asylum in Russia, was the Grey Hat hacker, thinking about the greater good of the nation and its people, he is now a target and a wanted man, for committing perjury and hacking the NSA. The government's use of

technology to hack and record millions of conversations cannot be deemed ethical in any way. It is clearly evident that government officials are in need of policing and the defects of EH are but apparent. Regardless of the negativity surrounding how the government use Ethical Hacking, it is clearly evident that the benefits outweigh the drawbacks, Militaries are trying to protect and secure assets they have worked years to build and spent a fortune on, weaponry and arsenal now runs on software making it useless if hacked into. Surveillance used to manage and run air control from flights coming in and out the country are in jeopardy if breached. EH is a must in order to prevent a whole nation from falling, regardless of the drawbacks and the misuse, protection of lives holds the highest priority.