Daniel Rao

Jan 24th, 2021

Vince

Ethical Hacking

We humans are highly tech advanced in today's times with the extensive use of the Internet and modern technologies. Protecting digital data in today’s world is a massive challenge and one example could be like protection of banking data or maybe medical records. In 2017 of May there was a ransomware attack also known as ‘one to cry’ ransomware that happened in Asia and then it spread across the world within a day. More than 230000 computers were infected across 150 countries. The one to cry crypto worm encrypted the data and locked the users out of their systems for decryption of the data and hence the users were asked for a ransom of 300 to 600 dollars in Bitcoin which is a form of crypto currency. The users who used the unsupported version of Microsoft Windows and those who hadn't installed the security update of April 2017 were targeted in this attack. The one to cry attack took a toll on every sector of top organizations. Companies like Nissan and FedEx had to put their businesses on hold as their systems were affected too. According to one source, “Cybercrimes are estimated to cost $6 trillion in 2021 and to tackle these cybercrimes organizations are continuously on the lookout for cybersecurity professionals” (Lessie).

In order to prevent such attacks cybersecurity is implemented. Cybersecurity can be defined as a practice of protecting networks programs computer systems and their components from unauthorized digital attacks. These attacks maybe legal or illegal depending on the type of hacker. Hacking refers to exploiting weaknesses in a computer network to obtain unauthorized access to information, whereas a hacker is a person who tries to hack into computer systems.

There are hackers who work with different motives and based on that they have been categorized into the following categories:

1. Black Hat Hackers: Black hat hackers are individuals who illegally hack into a system for gain.
2. White Hat Hackers: White hat hackers are type of hackers who exploit the vulnerabilities in the system of an organization by hacking into it with permission. Hence, they are also called ethical hackers.
3. Grey Hat Hackers: grey hat hackers as the mix of both white and black. These types of hackers discover vulnerabilities in the system and report it to the organization, which is a good act, but they do this without the owner's permission.

Professional Ethical hackers use various methods or form of testing to break into the system or network to find vulnerabilities into the system. One such practice is known as penetration testing or in other words could also be called as pentesting. Based on the practice there can be different kinds of pentesting which are mainly: network services, web applications, client side wireless, social engineering and physical. A penetration test is performed to find and exploit the vulnerabilities in the system to gain access to the system, steal data, or may even spy or cause different kind of attacks on the host system. Some companies or organizations may have two sets of ethical hackers’ team mainly known as red team which is more on the offensive side and blue team which is more on the defensive. The whole motive of the penetration test is to find and exploit the vulnerability and finally create a report on how the exploit was achieved and the steps that may possibly be taken to neutralize the threat or vulnerability. The test may be performed externally or internally to simulate different attacking methods and depending on the goals of each test, a penetration tester may or may not have prior knowledge of the environment and systems are attempting to breach. Each penetration test can be categorized into box models based the level of knowledge and access granted to the pentester at the beginning of the assignment. These include:

Black Box Model: In a black box testing assignment, the penetration tester is placed in the role of the average hacker, with no internal knowledge of the target system. These testers are not provided with any network architecture diagrams or source code that is not publicly available.

White Box Model: penetration testers are given full access to source code, architecture documentation and so forth. The pentester works his way into the system based on this knowledge.

Gray Box Model: If a black box model tester is examining a system from an outsider’s perspective, a gray-box tester has the access and knowledge levels of a user, potentially with elevated privileges on a system.

Penetration testing is just like science, and like any other science a consistent methodology needs to be used to achieve the best results. To conduct an effective penetration test it requires 6 phases which are: pre-engagement, reconnaissance, vulnerability Assessment, Exploitation, Post Exploitation and reporting.

1. Pre- engagement: In pre-engagement we determine the type of device that we are interested in exploitation. A personal computer, a web server or internet-of-things device would have a drastic impact on all of the following steps. It’s also important to consider legal actions on performing exploitations on such device.
2. Reconnaissance: In this phase we use tools such as Nmap to scan entire networks or tools like Shodan to scan the entire internet to find the devices are potentially vulnerable to exploitation.
3. Vulnerability Assessment: This is the phase where we narrow down the number of devices that we gathered in phase 2 which is ‘Reconnaissance’ which we know are vulnerable to known exploitation. For this we can use pre-built tools, or we could use the knowledge of outdated versions of software’s to find devices which are known to be vulnerable.
4. Exploitation: This is where the attack happens and the center of penetration test. This is the phase where we gather the information, we gathered in previous 3 steps and apply to exploit our targeted device. This can we widely based on the type of exploitation.
5. Post-Exploitation: Post-Exploitation is only possible only after a successful exploitation is completed. This is where after access to the device we either raise our privileges or gain permanent access to the device.
6. Reporting: In this phase we gather all the knowledge we gained throughout the penetration test organize it and publish it so that the owner or managing team can be aware of this vulnerability.

Citation:

Lessie, J. (2021, January 06). Ethical Hacking. Retrieved January 25, 2021, from https://medium.com/technology-hits/ethical-hacking-bcf212c9648c