IJECRT- International Journal of Engineering Computational Research and Technology, Volume 2, Issue 1, December 2017
ISSN (Online): 2456-9852
www.ijecrt.org

A STUDY ON ETHICAL HACKING AND PENETRATION TESTING

Alfred Seipeleng Moselekatsi
Post Graduate Student, Faculty of Computing
Botho University, Botswana
alfred.moselekatsi@bothouniversity.ac.bw

Dr. Srinath Doss
Head of Department, Faculty of Computing
Botho University, Botswana
srinath.doss@bothouniversity.ac.bw

Abstract: - Because of escalating vulnerabilities to today's changing security environment, Organizations are now prioritizing the Information security protection. Because now Internet allow public to be connected anywhere and anytime, that global accessibility on its own has triggered Organizations weaknesses because its security controls can be either be internally and externally compromised. Hence the mandate of this article is to parallel discus and bring awareness of ethical hacking in conjunction with penetrations testing. At the end of this article one will agree that Ethical Hacking and Penetration testing are preventative measure which involves a pool of legitimate tools that identify and exploit Organization security loopholes. Technically their techniques are like those malicious hackers' uses to attack vulnerabilities in company's security systems, which then at the end can be guard against and closed. The ideal gain of conducting the two is to reveal how easy a company security controls can be penetrated by hackers as well as obtaining access to private and confidential information.

Key-Words: - penetration testing, ethical hacking, system security, Information security

1 Introduction

Corporate entities find themselves in a tight corner faced with unenviable duty of wanting to defend their organizations against different types of intrusive attacks. Even though they have put in place their traditional methods of security defense such as firewalls and intrusion detection systems there is a need to engage and take advantage of security specialists who can in depth exploit known and unknown weaknesses in organizations to determine the security posture [11]. It triggered Ethical hackers and Penetration testers whom as of now have managed to create a niche for themselves in the defense in-depth spectrum. But before going into evaluating and analyzing context of the two, it is very important to highlight and clear the confusion which readers have about the two concepts being penetration testing and ethical hacking.

People tend to interchangeably treat them as one concept just because both of their processes operate on legal basis or ethically. For instance, one will say they both have same mandate of identifying flaws in the target environment. Ideally Penetration testing is a narrowly focused practice; it simply identifies flaws on the target environment with the mandate to penetrate the system thus owning control over that system [12]. Basically, Penetration testing gain access on the target company security, compromise the infrastructure system and gain access to the information. Sources from various researchers like [1] state that "Penetration testing is a subset of Ethical hacking in the sense that, Ethical Hacking is regarded as expansive term encompassing all hacking techniques, and computer attack to find security flaws with the permission of the target owner and with the goal of improving the target's security while penetration testing is more focused on the process of finding vulnerabilities in a target environment."

Throughout the article we will get more analytical description of Ethical hacking types that can be placed in categories of various Hat hackers. That means we have three hats distinguished as black, grey and white. Black hat hackers conduct unauthorized attacks against target environments which may or not are illegal in the country they are conducting attack. In contrast, white hat hackers are the ones regarded as ethical hackers as they do their legit security

tests bounded by a contractual agreement. Whereas lastly, we have Grey hat hackers which find themselves falling in between black and white hackers simply because, even though they perform their activity legally but at times they slightly go out of the boundaries [7]. On this article when defining the scope of Penetration testing, types will be covered, namely their Boxes being Black, White and Gray box. In White box test all information is revealed about the target environment to the testing team before the start of the test. In Black box testing no information is revealed at all about the target environment. Whereas in Gray box testing it is fifty-fifty in the sense that some information is revealed and some is hidden. The analysis should be concluded by bringing comparison and outlining different phases that the later concepts go through during their practice. And in a nutshell Tools used for vulnerability exploitations are going to be discussed as well.

Threads and Risks Found in Organizations

By virtue for companies to arrive to a decision of engaging ethical Hackers or Penetration testers, first there should be threats and risk identified. The following common risks being internal and external threats will be discussed.

Internal Risk/Threat

The worst challenge a company can face is no matter how robust computer security is designed, if employee's lacks knowledge pertaining security issues there is always going to be security challenge. Because of this lack of security awareness, employees can haphazardly open phishing emails, which may be containing viruses; just by doing that company can be placed at risk with thousands of lost revenues [9]. In addition, employees, nowadays have adapted to cloud computing services such as Dropbox and Google drive; by so doing Information Technology department procedures and policies are bypassed in the sense that cloud systems are independently and remotely managed in terms of security wise. Therefore, there is likelihood that cloud can compromise confidential and critical information, thus increasing rogue IT risk.

External Risk/Threat

This involves broad range of activities which are practiced by real criminal hackers simply because there are security gaps in organization's system. External hackers will have a room to exploit and gain unauthorized access to temper and delete sensitive information such as Bank card credentials. Technical issues, human mistakes and incorrect policy or security configurations are one of the root courses of compromization of security. These concerns must be guard against because they can degrade business effectiveness thus losing revenues, damaged reputation and loss of credibility in the eyes of clientele.

Ethical Hacking Overview

People only associate hacking as a negative and illegal way of gaining unauthorized access into the systems or networks, but the truth is everything has its positive and negative side; with that we can say there are hackers who are disclosing vulnerabilities as a way of protecting organizations security in contrast to those who practice malicious activities. First let's bring an understanding and the difference between the terms itself Hacking in contrast with Ethical Hacking. One will say hacking driven by factors such curiosity, or simply being ambitious to learn the details of the computer system in intention to enhance capabilities [3]. These are the people whom we regard as criminals of the Cyber World who intent to harm someone network or data. Additionally, they are gifted with a skill in various programming languages, computer system and networks. They practice malicious hacking with the aid of programs such as malware consisting of Trojan horses to gain unauthorized access. This paint a picture that hackers enjoy illegally penetrating computer security to learn more details about the computer system thus stretching their capabilities which is different from most users who are just interested in learning necessary details. On the flip side of the context we have Ethical Hackers who get authorization before breaking into computer system. They are also referred to as Red teaming, intrusion testers or experts who specialize in identifying loopholes (if any) into

organization security. Their process needs time and persistence to gain access to the system security and it has been realized that techniques skills to locate vulnerabilities of the target environment are like both malicious hacker and ethical hacker, the only difference is the intention of the hacker. Table 1 bellow can be referenced to gain insight of comparison between types of hackers and penetration testers.

Penetration Testing Overview

A penetration test is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source [1]. It can be divided into the following categories:

Logical: It is associated with organization's computers, infrastructure devices, software and applications.

Physical: Actual physical security for instance door that does not lock properly, Sensitive information that is accidentally ended up in dumpster, vulnerability of employees to social engineering and lack of company policies/procedures or an employee failure to follow up policy/ procedure

Classification of Penetration Test:

Internal testing: When a test is done inside the organization's internal network.

External testing: When test is conducted against Internet-facing hosts.

1. The difference between the two is the amount of information available to the test team before starting the test.
2. A complete penetration test will encompass testing both external and internal.

Fig. 1: Steps in penetration Testing

2 Literature Survey

Hacking has two flip sides being good and bad. It is a prominent aspect in Cyber Space and it is very important to practice ethical hacking without damaging the tested system to avoid worsening the situation by creating new vulnerabilities but rather identify vulnerabilities and fix them subsequently [7]. There are some real-life examples of Penetration testing whereby we came to know that Mr. Chris Goggans who have been certified as a Penetration tester since 1991 took only six hours to exploit FBI Crime Database systems without permissions. He achieved that by using FBI Webserver as a loophole after finding out that it is unpatched. He simply pulled out user name and passwords that were re-used in FBI enterprise and escalated his privileges to gain administrative rights and get full control of the system.

Information should be kept safe and it is one of the most vital sources of any company while running daily business operations. Organizations including government agencies are forced to adapt to either ethical hacking or penetration testing tools to implement security for critical documents [3]. The mandate of Penetration testing and ethical hacking are somehow associated [11]. With the aid of tools attack can be identified before it can affect the entire Organization.

Gupta, A. K (May, 2014) on 2008 students presented a platform called Solar Sword that will allow penetration testers to easily deploy their process in developed on Open Solaris [4]. This platform addressed previous limitations such as situations whereby Penetration testing team being restricted to work under limited time. It is a kind like client server architecture that operate from a central location at the same time coordinating many connected clients to the server.

Fruitfully the following author's assumptions were addressed: It is mandatory for test to be performed in an automatic way, the fact that test must start from different angles, quick deployment is required and platform must not be prone attacks as well as having slim chances of being controlled by attackers.

3 Proposed Study

In this proposed study Table 1. Depicting the difference between Types of Hackers/Ethical (EH) hacking in contrast to Types of Penetration

Testing (PT). It is important to point out that PT is a subset of EH and EH must have depth knowledge of software programming while PT does not require comprehensive knowledge but rather only understanding of specific areas for which testing is going to done.

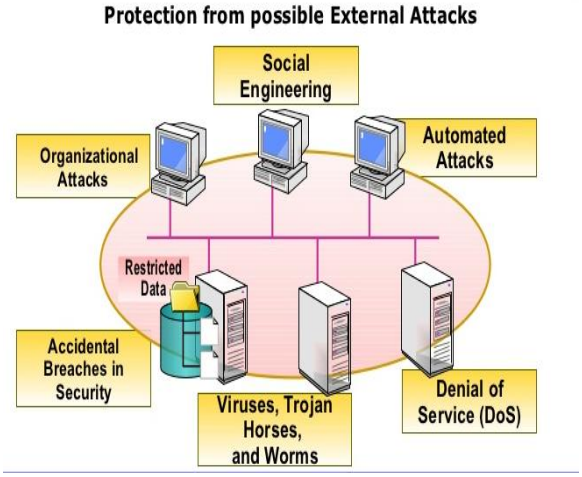

Fig.2: Need for Ethical Hacking

From the figure 2, we can understand the various sources of attack such as social engineering, organizational attack, automated attack, accidental breaches, Viruses, worm, Trojan Horses and DoS /DoSS attacks.

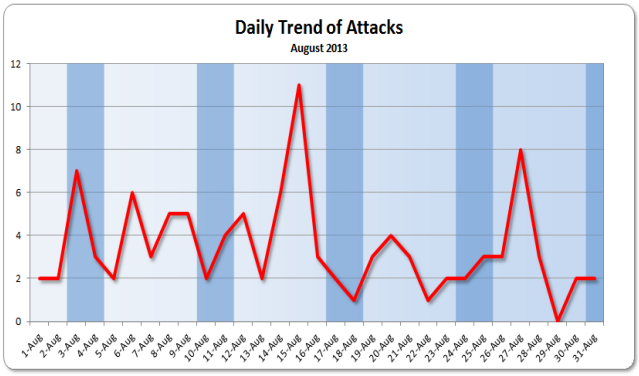

Fig. 3: Sample Daily trend of attack (Internet source)

Figure 3, shows the attack has been done on restricted data frequently on daily basis.

TABLE 1
TYPES OF ETHICAL HACKER AND PENETRATION TESTERS

Types of Hackers/Ethical Hackers	Types of Penetration Testers
I. White Hat Hackers: These are hackers who breach security as a security research or employed as security professionals. In most cases they are employed by companies to expose security vulnerabilities before an intruder or attacker can have a chance to exploit the vulnerability. II. Black hat Hackers: These are those who are commonly known as Hackers because they are on the negative side because of cracking company securities practices. III. Gray Hat Hackers: These are Hackers which are regarded as intermediaries between a white hat and black hat hacker. They also violate ethical standards by exploiting security vulnerability but in contrast to Black Hat hacking, Gray Hat Hackers look for vulnerabilities without	I. White box testing: Information will be provided so that the team is able to assess the security of a specific target. The test team will be given as much information equivalent to the amount of information a network administrator knows.E.g. Network ranges and topologies. But the team will not be given usernames and passwords. II. Gray box testing: The test team is given information such as: • Hostnames • Few IP addresses • Whether senior management can connect to the network remotely. NB: The test team is given enough common information a

malicious intent. In addition, what differentiates Gray Hat from White Hacking is that, White Hat Hacking alerts system owners and vendors after discovery of vulnerability. This is different from Gray Hat Hacking which publicizes vulnerability findings to the public. Types of Hackers can be expanded to the following: • Script Kiddie: Hackers who are not expert in exploiting work but rather depend on pre-packaged automated tools/using exploits which are already being made by someone else. Even though Kidding may be able to exploit the target with the little knowledge they have. In case of exploitation not functioning, Kiddies may experience difficulties because by nature Kiddies are not able to modify or debug an already created exploit. • Elite Hackers: These are skilled Hackers with deep knowledge on how exploit works. They can create exploit nor able to modify those exploits which were created by someone else. • Hacktivists: This involves group of Hackers who exploits vulnerabilities for purposes such as freedom of speech, political gain and human rights. They commonly associated with bringing denial of service or website defacement.	normal/unprivileged user can know. III. Black box testing: In this context, the test team is provided with little or no information except just the company name. In addition, it is up to the test team to acquire information from other sources such as internet. Types of PT can be expanded: • Web penetration testing • Shrink-wrap PT • Wireless PT • Bluetooth PT Some regard this type of test as the best as compared to white and gray testing because it mimics the way an attacker would have launched an attack. NB: All these above test types can be conducted either internally or externally. In addition to types of attacks we should also touch on the following variations: • Announced test: The penetration team works in full cooperation with the IT staff and the IT staff has full knowledge about the test e.g. what to be tested and when. • Unannounced test: Only specific members of tested company e.g. higher-level management are aware that the testing will take place but they may know the testing window not the exact date.

Table 2. Depicting phases of Ethical Hacking and Penetration testing. The bellow table shows phases which are like those which can be done by the malicious attacker, the difference will simply lie on the intention of penetrating the security system. For instance, hackers who intend to do harm to Organization infrastructure and will focus more on covering their tracks on the Post attack phase whereas those who penetrate the network under the limit of legal legislation will only have to roll back the systems to their pre-state before the testing was done.

TABLE 2
DEPICTING PHASES OF ETHICAL HACKING AND PENETRATION TESTING

Phases of Ethical Hacking	***Phases of Penetration testing***
• Reconnaissance: In this phase, much information gathered from the target in prior to conduct an attack. • Scanning: Contacting the target by doing a scan to find about mostly open ports and weaknesses on the target architecture or network. • Gaining Control: Conducting an actual	• Pre-Attack phase consist of passive and active reconnaissance. The team investigates the potential target through the process called reconnaissance. Passive does not draw any attention as it does not touch the target while active reconnaissance is contacting target network to gather as much as possible information about the target

attack to the target. For instance, access and control can be done at Operating system level. When there is a need an attacker can escalate their privileges. This is a phase where we experience Denial of Service attack, password cracking, overflow of buffers etc.

- Maintaining access: This is where an attacker remains persistent with the aid of Trojan horses and backdoors. Already attacked victims can be anonymously used as zombies to expand the attack to reach more machines.
- Covering Tracks: Erase of tracks is done by malicious Hackers, but is not vital to ethical hackers, as they are only concerned with reverting systems back to their initial state (before the test was done).

company.

- Attack Phase: It is complimented by Pre-attack phase in the sense that the actual compromise of the target will be done based on vulnerabilities found from Pre-attack phase.
- Post Attack Phase: In most cases is all about resetting the systems to their preset state. The following are examples of activities:
  - Deleting of any tools, files and folders which were uploaded or installed during testing.
  - Revert registry to its original state.
  - Changes made on access control list are reversed.
  - Restoration of network devices and infrastructure.

4 Tools

It is important to note that both Penetration testing and Ethical Hacking use similar tools and as an advantage these are similar tools that malicious hackers uses too. For simplicity and for the sake of this article, only a few numbers of tools will be discussed based on their categories.

Tools used for Port scanning:

Network Mapper (Nmap) - It is an open source that is mainly used for auditing security and network discovery in general. It is also useful for network inventory as well identification of open ports. Basically, through Nmap one may know which hosts are present on the network, application versions and running services. Nmap is available in both command line and graphical user interface and fruitfully after Nmap scanning one will be able to determine the nodes need patching or not. Port scanning tools can be extended to the following:

- Nikto
- Autoscan
- Angry IP Scanner

Tools used for Packet Sniffers:

Wireshark- User friendly tool used to capture network packets in real time and concert them to human readable format. Its user friendliness is boosted by its features such as filters, and color coding's which gives human a platform to dig deep into network traffic thus analyzing network packets. Packet sniffers can be extended to the following:

- TCP dump
- Ethercap
- EtherApe

Tools used for vulnerability exploitation:

Metasploit- It is a framework that is by Ethical hackers and Penetration testers to gain access into different places hence providing a user with a vital information regarding security loopholes as a way of assisting in terms of formulating ethical hacking/ Penetration testing, strategies and methodologies for exploitation. Vulnerability exploitation tools can be extended to the following:

- Sql map
- Social Engineer Toolkit
- BeEf

Operating system:

There is endless list operating used by Penetration testers and ethical hackers precisely designed for hacking. Majority of above listed tools come bundled in Linux distro's namely BackBox and Kali Linux. With that it is recommended to install correct Linux for the sake of test easiness. Operation systems can be extended to the following:

- Backtrack5r3
- BlackBuntu
- Caine

5 Conclusion

After this analysis, we acknowledge that Hacking brings both benefits and risks. Hackers are diverse and they have the capability of bankrupting the Organization and on the contrary, may protect data hence increasing the revenues for the company. Ethical hackers as well as Penetration tester's helps to understand the company's security needs by giving security stakeholders to take remedial measures to rectify the loopholes that exist in the security system. Both Ethical and Penetration tools have been notorious for malicious hacking that it why each company must make it a mandate to stay one step ahead of the crackers. But it is still stand that these testing techniques are not panacea to all computer security problems.

References

[1] Bacudo, A. G, Xiaolhong Yuan, bei Tseng Chu, and Monique Jones., "An Overview of Penetration testing", Vol.3,.No.6,2011

[2] Byeon., "Effective Testing Methodology", Ethical Hacking IBM Systems Journal,Vol.40, No.3,2003.

[3] F.Tipton, h., & Micki Krause., " Why Ethical Hacking" .CRC Press LLC, 2004.

[4] Gupta, A. K., Asia Srivastava, Tinesh Kumar Goyal, and Piyush Saxena, "Ethical hacking: An approach towards Penetration Testing", International Journal of Modern Communication Technologies and Research ,Vol.2,No.5,2014

[5] Hartley, R. D., "Ethical hacking: Teaching Students to Hack". East Carolia University,2013.

[6] Juneja, G. K. "A Technique to Enhence Information security", International Journal of Innovative research in science, engineering and Technology, Vol.2, No.12, 2013.

[7] Pangaria, M., and Vivek Shrivastava. " Need of Ethical Hacking OnlineWorld", International Journal of Science and Research,Vol.2.,No.4,2014

[8] Subbulaksmi, and Pavan Kumar, "Ethical Hacking techniques with Penetration Testing,International Journal of Computer sciencd and Information Technology,Vol.5,No.3,2014.

[9] Tekade, A. P., Pravin Gurjar, Pankaj R. Ingle, and Dr.B.B.Meshram., "Ethical hacking in Linux environment", International Journal of Engineering research and Applications ,Vol.3,No.1,2013.

[10] Chiem Trieu and Wei Qi Yan. "An overview of Penetration testing", International Journal of Digital Crime and Forensics,Vol.6,No.4,Pp.50-74,2014.

[11] Anestis Bechtsoudis and Nicolas Sklavos, "Aiming at Higher Network Security through Extensive Penetration Tests", IEEE Latin America Transaction, Vol.10,No.3,Pp.1752-1756,2012.