COMPROMISING SYSTEMS: IMPLEMENTING HACKING PHASES

Marlon intal tayag[1] and Maria emmalyn asuncion de vigal capuno[2]

[1]College of Information and Communications Technology,Holy Angel University, Angeles, Philippines
[2]Faculty of Information Technology, Future University, Khartoum, Sudan

ABSTRACT

In the cyber world more and more cyber-attacks are being perpetrated. Hackers have now become the warriors of the internet. They attack and do harmful things to compromised system. This paper will show the methodology use by hackers to gained access to system and the different tools used by them and how they are group based on their skills. It will identify exploits that can be used to attack a system and find mitigation to those exploits.

In addition, the paper discusses the actual implementation of the hacking phases with the virtual machines use in the process. The virtual machines specification is also listed. it will also provide means and insights on how to protect one system from being compromised.

KEYWORDS

compromised systems, hacking, penetration testing, exploit, vulnerability

1. INTRODUCTION

With the outset of the computer and internet age, cyber security is now in the headlines of every topic being discussed in terms of securing system and personal data that resides in enterprise system or cloud infrastructure.

As more and more systems are being compromised and data being stolen, there is now a need to understand how these things are being perpetrated in the mindset of an individual called a hacker.

The work hacking is actually a misnomer. Hacking is the action done by a person who is knowledgeable on his field of expertise such as technology [1] . Technically a hacker is someone who likes to explore and tinker things, by learning how computer systems runs and love discovering new things [2]. The person involved in this action is called a hacker. In its true form, the media is defining it the wrong way, a person who sets out to destroy or compromise a system and gain access to it with the intention of wreaking havoc is actually called a cracker.

Hackers are divided into different categories based on their skills as shown on Figure 1. White Hat hacker, is person or individual who uses his hacking skills to find vulnerabilities either in hardware or software and reports those vulnerabilities to the person or organization affected and help them find solution to their security weakness [3]. EC-Council, is a training company that offers certification and training to individual who wants to become ethical hackers, according to them a cyber security specialist needs to put himself in the shoe of the hacker to understand how they think, that is “to beat an hacker, you have to think like an hacker” [4]. Next we have the

DOI: 10.5121/ijcsit.2019.11203

Black hat hacker, are individual who attempts to gain unauthorized access to system by means exploiting its weakness. They implicit damage once they gained access and steal data [5]. Black hats can be cyber criminals or cyber terrorist.

And the last one is the Grey Hat hacker, is a mixture of a white hat and a black hat, they hack into system without permission and look for the vulnerability, once it is found they report it to the owner and for fee they will patch-up the vulnerability. They are malicious in nature; however, this type of hacking is still illegal because no permission is given by the owner to test the system for vulnerability [6].

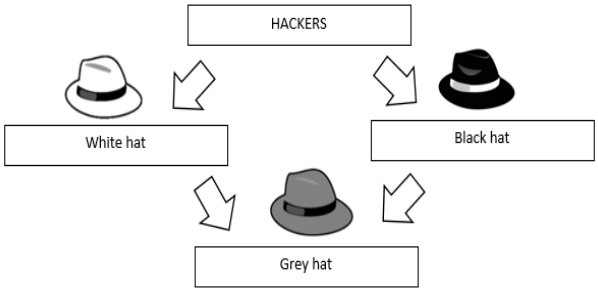


Figure 1: Hacker Categories

Hacking does not only pertain to targeting system and hardware but covers individual who uses those systems. Targeting people or person to divulge information useable to the hacker is called Social Engineering, one such example is calling an employee in which the hacker can pretend as a member of the technical team in charge on maintaining the servers. The hacker will ask the employee's password or credential with the excuse that they are currently implementing preventive maintenance on the server and they need the employee account to do backup.

As the need for securing system arises, some hackers are using their skill in a positive way. They work with companies in protecting their system by actually hacking their way in and providing the information to the companies on how they compromised and find ways to protect their system. Hackers for hire who protect and help companies do what is term as Ethical Hacking or Penetration Testing [7] [8].

Following pre-determined rules and guideline Penetration Testing is an attempt to compromised a system by finding its weakness and attacking those weakness using an exploit. The finding or result from the process is used to help company to mitigate or find solution and protect the company from cyber attacks

Pen Testing can be categorized in two types, White Box, where the Pen Tester is provided with information on the target system (e.g. infrastructures, server, ip addresses etc.) and the other one Black Box, also called as 'blind' testing, were no information whatsoever is provided to the Pen Tester.

1.1 CONTRIBUTIONS OF THIS PAPER

The main contributions of this paper are as follows:

1. Demonstrate the hacking phases and used different hacking tools to do so.
2. Identify vulnerabilities and exploits in compromising system, at the same time recommend solution to mitigate the problem

The remainder of the paper discusses the actual implementation of the hacking phases with the virtual machines use in the process. The virtual machines specification is also listed.

2. RELATED WORK AND TERMINOLOGY

On a paper presented by Teresa Guarda, Walter Orozco, Maria Fernanda Augusto and Filipe Mota Pinto, they discussed the three areas which penetration testing acts on, these includes application, network and system workflow. Each of these areas is inter-related. Vulnerability on one area affects the security of the other two. Point in case is the network, identifying treats that can create risk and weakness[9].

In “Ethical Hacking”, Ashar Ushmani points out the common process in compromising private data or confidential information. He discusses the different types of hackers from White hat, Black hat and Grey hat. He explained the difference between an ethical hacker and a hacker who target system for financial gain. He discussed the impact of hacking on the business side, were businesses suffered thru theft of valuable information [8] .

Pen Tester focuses on key area to investigate. He said that they have the network perimeter where network defense is setup. The pen tester tests network device configuration such as routers and firewall rules. Next is the application perimeter, where an application such as a web app is tested to see any vulnerability which can be exploited. Last but the least the workflow, testing by means of social engineering to identify individual in the workflow process of an organization (Fig.2).

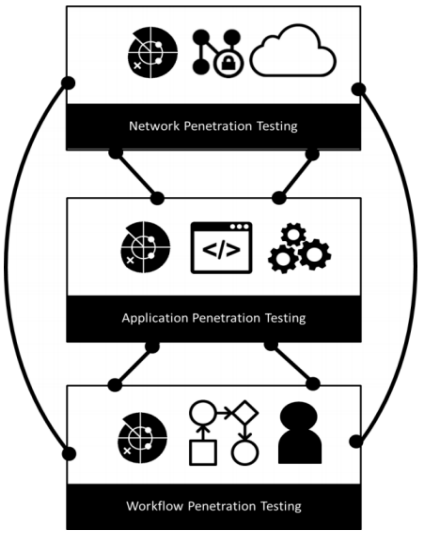


Figure 2: Acting Areas For Pen Testing

On the positive side ethical hacking as stated by Bhawana Sahare,Ankit Naik and Shashikala Khandey they pointed out testing a system for vulnerability will help the network or system administrator in patching up problems. They also cited the need to implement a mature security program with a combination of procedures and policies the work together.

Their paper also discusses the limitation of ethical hacking that is the test is based on one simple principle finding the securities vulnerabilities a hacker can used to attack a system. This can be compared to a diagnostic test [10] .

David Hafele, stated on his paper the benefits of implementing penetration testing, finding vulnerabilities before hackers can exploit them. Understanding false positive and false negative alerts, to which remediation can be implemented [11].

3. HACKING PROCESS

A. Ethical Hacking Phase

Ethical hacking follows a pre-defined process to find vulnerabilities on a given system. Each steps help the Pen Tester or hacker to achieved his goal in compromising a system (Fig. 3).

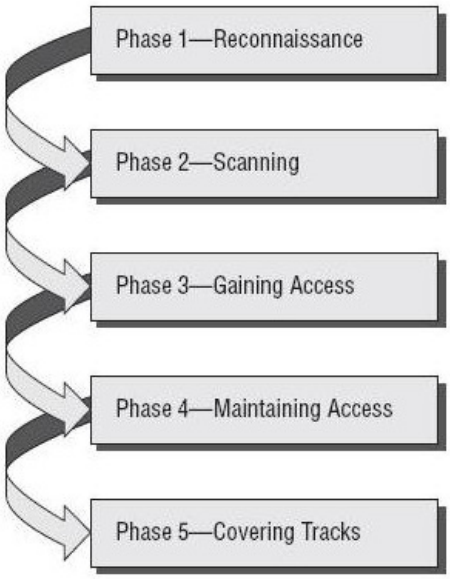


Figure 3: Hacking Process

1. Reconnaissance – gathering information on the target (e.g. network, domains) this will help the attacker to better understand the target and any potential weakness.
2. Scanning and Enumeration – in this phase the attacker will implement passive scanning, these includes using various scanning tools to determine open ports and services.
3. Identify Vulnerabilities' – the attacker will use tools that can identify weaknesses on the system. Such tool includes Nessus and OpenVAS.
4. Exploitation – Using the knowledge gain from phase three, the attacker will now implement active attack by exploiting the weakness and gained access to the target.
5. Covering Tracks– Once the attacker gain access to the system. The attacker will try to remove all evidence of his attack. One such activity is deleting the system log files.

B. Testing Requirements

To test the given process, a cyber-laboratory was implemented to isolate attacks from the live network. In this paper virtual machines that run two operating systems was used. Virtual Machines is basically a software computer that runs actual operating system, it uses physical resources such memory and CPU cycles[9]. It made use of security or hacking tool to locate the target, find open ports thru scanning, find and exploit the target by means of its weakness. These are as follows:

A. Operating System: Kali Linux (2019 Rolling) and Windows XP unpatched (32 bit)
B. Virtualization Software: Virtual Box, a free virtualization software for virtualizing PC
C. Software Tools:

    a. Nmap – is an open source application use to scan a specific target and show running or active ports and services.
    b. Metasploit Framework – is a penetration testing framework that allows pen tester to write, test, and run exploits. It contains a range of tools specifically designed for finding security vulnerabilities, enumerations of target network or devices, by compromising systems and avoid detection.
    c. Nessus – is a vulnerability scanner design to find weakness on a target. It creates a report by cross linking its results to the Common Vulnerabilities and Exposure database (CVE).
    d. Meterpreter – is an advanced payload DLL injection system and currently part of the Metasploit Framework. It allows the attacker to run either bind or reverse bind shell in compromising the target.

C. System and Hardware Requirements

To properly simulate the Cyber Security Laboratory, the following VM configuration are needed. The host PC should have 8 to 16 gig of memory running Window 7 or Windows 10. Each of the VM are configured as follows:

Table 1: Virtual Machine Specifications

Virtual Machine	Memory	Storage
Kali Linux	4 GIG	40 GIG
Windows XP	256 MB	20 GIG

3.1 IMPLEMENTING ATTACK THROUGH CYBER LAB

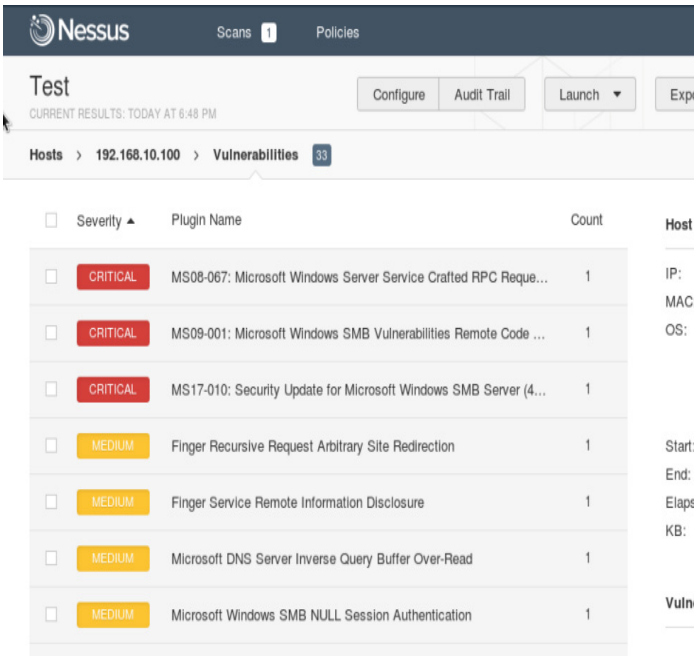
Implementation of hacking and compromising the system will use the ethical hacking process:

Step 1: Reconnaissance

For this phase, the attacker can use tools such Ping Sweeps, Packet Sniffing and Network Discovery to identify live target.

Step 2: Scanning and Enumeration

Nmap can be used to search for open ports and services. The hacker can scan the target and list all active ports and services. As shown on Fig.4, the nmap scan **nmap –sT –p- -PN 192.168.10.100** is use to implement a TCP connect scan and show all open ports with the running services. The information provided by the nmap scan can be used by hacker to further investigate any vulnerable services which can be exploited



root@kali:# nmap –sT –p- -PN 192.168.10.100

Figure 4: Nmap scanning of target

Step 3: Identify Vulnerabilities

Vulnerability scanning of the target can be done by using Nessus, based on the port scan found by nmap, the attacker can have rough idea of what the target is and what are the running services. With Nessus the attacker can find the weakness of those services. Nessus categories the level of vulnerability found on the target. Critical vulnerabilities are colored red. They are the priority weakness that needs to mitigated or resolved. Orange is high, Yellow is medium and blue is information (Fig.5).

Figure 5 : Nessus vulnerability scanning

Step 4: Exploitation

With the weakness identified the hacker can now proceed to exploit and gain access to the target. One of the critical areas found is a security issue on Microsoft NetAPI service (MS08-067).

The Nessus scan output (Fig. 6) MS08-067 vulnerability can allow a hacker to run remote code execution, basically running a remote shell which the hacker can use to control and do anything he wants on the target system.

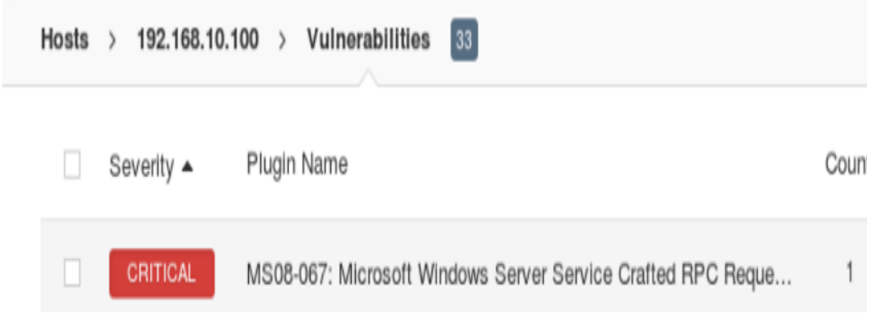


Figure 6:MS08-067 Security Issue

The said issue can be exploited by using metasploit **exploit/windows/smb/ms08_067_netapi**, allowing the hacker to gained SYSTEM access – highest user privilege in Windows (Fig. 7).

Figure 7: Using Metasploit on MS08-067 Vulnerability

Considered as one of the most popular exploit use to attack Microsoft Windows.

The exploit attacks the NetAPI32.dll library thru the Server Service[12]. The attacker gain access to the system an implemented remote view to the target with the metasploit payload VNCInject reverse bind connection (Fig.7).

Figure 8: Gaining Access To The Target

C. Implementing Mitigation

MS08-067 vulnerability is just one of the vulnerabilities that may affect an operating system, that is, it is a windows operating system. With that in mind the best way to patch-up the operating system is to do a security update.

Microsoft on their Security Bulletin provides a security update of the said security vulnerability. Keep in mind that if not patch the attacked can implement a Remote Code Execution[13].

4. CONCLUSION

Cyber Security is an area that will have a huge impact on how we protect our personal data and enterprise information. With the proliferation of ready to used tools on the internet anyone can become a hacker. Hacker can be either a white hat, grey hat or a black hat hacker who uses his skill to do harm to people by stealing their information.

Implementing Penetration Testing internally or hiring Pen Testing Team from outside can help an organization to find critical security issues. The concept of a contain network is long gone. Currently, networks are also connected to the Internet which provides a huge opportunity for hackers to infiltrate internal organization network. With the advent of the Internet of Things devices such as network printer improperly configured are a ticking bomb. Ethical Hacking or Penetration testing is a useful tool along with basic computer security knowledge are essential part of the securing the organization.

As demonstrated, improper updates on system such Windows OS can lead to a hacker compromising the organization system. Learning to protect ourselves, knowing the proper cyber etiquette is a must.

REFERENCES

[1] S. Begum and S. Kumar, “IJESRT INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY A COMPREHENSIVE STUDY ON ETHICAL HACKING,” vol. 5, no. 8, pp. 214–219, 2016.

[2] “Role of Ethical Hacking in System,” no. May, 2018.

[3] "What is white hat? - Definition from WhatIs.com." [Online]. Available: https://searchsecurity.techtarget.com/definition/white-hat. [Accessed: 14-Mar-2019].

[4] "What is ethical hacker? - Definition from WhatIs.com." [Online]. Available: https://searchsecurity.techtarget.com/definition/ethical-hacker. [Accessed: 14-Apr-2019].

[5] "Types of Hackers and What They Do: White, Black, and Grey | EC-Council Official Blog." [Online]. Available: https://blog.eccouncil.org/types-of-hackers-and-what-they-do-white-black-and-grey/. [Accessed: 14-Mar-2019].

[6] "What is the Difference Between Black, White and Grey Hat Hackers?" [Online]. Available: https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html. [Accessed: 14-Mar-2019].

[7] S. Satapathy and D. Ranjan Patra, "Ethical Hacking," Int. J. Sci. Res. Publ., vol. 5, no. 6, pp. 2250–3153, 2015.

[8] C. C. Palmer, "Ethical hacking," vol. 40, no. 3, pp. 769–780, 2001.

[9] I.-C. MIHAI, "Penetration Tests on Virtual Environment," Int. J. Inf. Secur. Cybercrime, vol. 1, no. 1, pp. 37–45, 2016.

[10] B. Sahare, A. Naik, and S. Khandey, "Study Of Ethical Hacking," vol. 2, no. 4, pp. 6–10, 2014.

[11] D. Hafele, "Information Security Reading Room Three Different Shades of Ethical Hacking : Black , White and Gray In tu ll r igh," 2019.

[12] "Exploitable vulnerabilities #1 (MS08-067)." [Online]. Available: https://blog.rapid7.com/2014/02/03/new-ms08-067/. [Accessed: 14-Mar-2019].

[13] " Microsoft Security Bulletin MS08-067 - Critical | Microsoft Docs." [Online]. Available: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067. [Accessed: 21-Mar-2019].