PHYSICAL SCIENCES

OPERATING SYSTEM SECURITY AND PENETRATION TESTING

Adoga, H. U., Ezugwu, E. A. and Umar, M. B.
Department of Computer Science, Faculty of Science, Federal University Lafia, Nasarawa State, Nigeria
Corresponding Email: haruna.adoga@fulafia.edu.ng

Date Manuscript Received: 30/11/2016 Accepted: 30/12/2016 Published: December, 2016

ABSTRACT
Penetration testing is an integral part of any organization or individual that employs the use of Information Technology services. This ensures that their computing infrastructures are checked for vulnerabilities in a routine manner. This paper explains the processes and phases involved in ethical hacking. In addition, major penetration testing types available are also discussed. A Local Area Network (LAN) was designed in a virtual environment running Linux and Windows Operating Systems. We carried out a white box penetration test on the systems. Kali Linux; an open source Debian-based Linux distribution designed for penetration testing and digital forensics was used for the experiment. Several built-in tools in Kali Linux were used, while going through the main phases of penetration testing. Starting from the reconnaissance phase of the process, information about computers was gathered, the network was scanned for vulnerabilities in the scanning phase, and identified vulnerabilities were exploited in the third phase of the penetration test, which is gaining access. Backdoors to exploited system(s) were created to maintain access and event logs were deleted to prevent detection in the final phase of the process.

Keywords: *Malware, operating system security, work station virtualization, penetration testing, network security.*

INTRODUCTION

With the rapid growth of Information Technology (IT) and increased accessibility in recent years, we produce more data now than ever before. Therefore, this calls for an urgent need to protect information and information systems from all sorts of manipulation and unauthorized access. Ensuring the protection of network infrastructure and computer systems, and the services they provide is paramount to the success of any business. Sensitive data, such as financial records, medical records and e-commerce services amongst other sensitive information, need to be protected by ensuring the Confidentiality, Integrity and availability (CIA) of such information.Host and server based operating systems faces an increasingly high level of security threats by the day.Penetration testing provides a way for organizations to check their computer infrastructure for vulnerabilities that could be exploited by an adversary.

There are some very important objectives that we set aim to achieve by carrying out this research; these objectives are listed below. They include, using Kali Linux, which is an open source Linux distribution designed for digital forensics and penetration testing, in determining the possible vulnerabilities that exist in a typical Local Area Network environment, design of a typical Local Area Network, in a virtual environment, consisting of both open source and proprietary Operating Systems as obtainable in most network environments, the implementation of each phase of ethical hacking and penetration testing using the digital forensics tool (Kali Linux) and exploiting any vulnerability found with the aim of providing useful recommendations, which can help organizations harden their network infrastructure even better.

Kali Linux is the most advanced Debian-based Linux distribution for penetration testing available at the time of this research. This distribution provides applications and tools that can be used in each of the five main phases of penetration testing. An empirical approach was adopted in reviewing ethical hacking and penetration-testing procedures with focus on commonly used operating systems in today's network infrastructures.

Ethical hacking can be described as a process of testing the computer infrastructure of an organization or individual by professional certified hacker(s) with the aim of assessing the infrastructure for possible vulnerabilities and making them known to the management of the organization for appropriate security measures. Unlike black hat hackers who gain unauthorized access to computer systems (networks) without the authorization of the owner, ethical hacking is usually done with the consent of the organization or owner of the computer system or network. A certified ethical hacker will normally use the same tools that a black hat hacker will use to achieve their aim. According to Whitaker and Newman (2006), a penetration tester is an ethical hacker who is hired to attempt to compromise the network of a company for the purpose of assessing its data security.

There are basically five phases of ethical hacking, as reported by Engebretson (2013).
Reconnaissance is basically the process of gathering information about the target infrastructure and systems. This is the first phase of the ethical hacking process as it allows the ethical hacker to have a good understanding of the organization's infrastructure and the underlying technology in use. At the end of this phase, the pen tester should have a good idea of information such as the facility information, phone numbers, employee information, Internet Protocol (IP) address ranges, and namespaces.Nidhra and Dondeti (2012).

Vulnerability Scanning is a phase that makes use of data gathered to find out the valuable resources the target has, presence of known vulnerabilities in infrastructure the target uses.According to Nidhra and Dondeti (2012), the pen tester gets information on hosts, ports on the hosts and services that may be running on the hosts. Scanning is predicated on the assumption that reconnaissance has been successfully completed.

Gaining access (Exploitation) is a phase of the penetration testing lifecycle where the hacker attempts to gain access to the target system(s) using the information gathered from previous phases of the process. Broad and Bindner (2014) reported that information such as usernames, permissions and passwords gotten from early phases are utilized to exploit any known vulnerabilities on the target systems.

Maintaining access to the target system after securing it is an important phase of a penetration test, as this will ensure that the pen tester stays connected long enough to carry out all the tests (attacks). The use of backdoors and key loggers are employed in this phase, backdoors will allow pen testers to connect to the same target at a later time even when a patch (update) has been implemented to fix the vulnerability. It is great to exploit a computer, networking device, or a firewall device, however the goal of penetration testers is to maintain access to the exploited system(s) Broad and Bindner (2014).

This is the final phase in the ethical hacking process, as known existing vulnerabilities have been exploited. Activities in this phaseinvolves deleting event logs that might reveal that the hacker was there in the first place. Engebretson (2013) reported that anattacker who wishes to remain untraceable after successfully carrying out an attack, needs to erase all the tracks that may lead back to him/her.

MATERIALS AND METHODS

A Local Area Network (LAN) was designed with both Linux and Windows Operating Systems in a virtualized environment. According Cisco Systems (2016), the benefits of a centralized design include IP address management, simplified configuration and troubleshooting, and roaming at scale. Using Kali Linux, we went through the phases of penetration testing on the LAN. Information about the Operating Systems was gathered and the computers were scanned for vulnerabilities. Finally, some of the vulnerabilities were exploited and recommendations made. Figure 1 below depicts the phases involved in performing penetration testing.

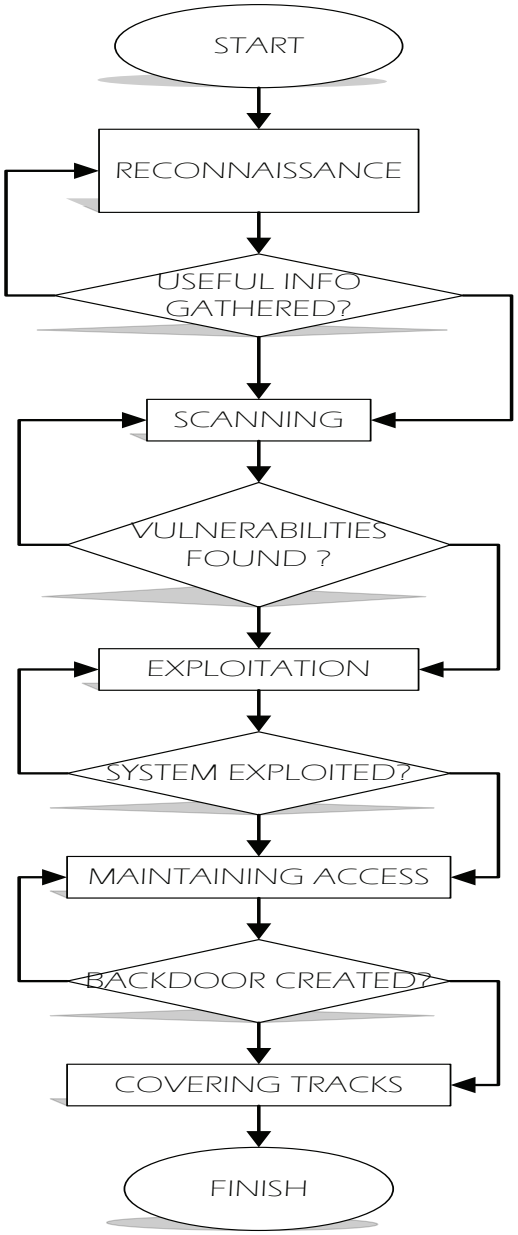

Figure 1. Penetration testing flowchart

Based on the information depicted in Figure 1 above, the flowchart starts with the reconnaissance phase of penetration testing, where information about live hosts were collected, upon completion, the network was scanned in order to reveal available ports and services. Vulnerabilities found in the scanning phase were exploited in the exploitation phase of the penetration test. Backdoors were also created in order to maintain access to the exploited systems. The process completes by covering the tracks, to avoid detection by system administrators.

The experiment from the reconnaissance phase of ethical hacking and walked through subsequent phases of the process in the following sections. The different phases of penetration testing were performed using Kali Linux. The network infrastructure was simulated in a virtual environment using VMware workstation 11. A comprehensive network topology structure was designed based on the information collected from the reconnaissance phase of the penetration testing carried out (See Table 1 and Figure 2).

Reconnaissance

Identification of live hosts

Running the ***ifconfig*** command on the Kali Linux terminal reveals the local IP address on Kali (a static IP address was assigned), having this information can help you get an idea of the subnet mask of the network you are connected to. A ping sweep was done on the network as part of the information gathering reconnaissance phase. This reveals some important information about host IP addresses on the network and the output shows that 5 hosts are up with their respective IP and mac addresses displayed.

IP addressing scheme from ping sweep

Using ping sweep with nmap tool on Kali Linux, i.e running the nmap -sP 192.168.1.0/24 command with sP option to specify ping sweep. The IP addresses on the network are as shown in Table 2 below.

Table 1. Ip addressing and MAC address discovered using nmap tool

Host MAC address	IP address	Subnet mask
00:0c:29:84:e3:39	192.168.1.1	255.255.255.0
00:0C:29:56:DA:E2	192.168.1.2	255.255.255.0
00:0C:29:A0:FF:18	192.168.1.3	255.255.255.0
00:0C:29:08:35:C1	192.168.1.4	255.255.255.0
00:0C:29:D0:EC:2F	192.168.1.5	255.255.255.0

After performing a ping sweep on the network, the IP addresses of hosts on the network were revealed.

Based on the information gathered from the reconnaissance activity above, it is now known to the pen tester that 4 more devices are connected on the same network and a network topology can be drawn in order to make the subsequent phases of the ethical hacking process more efficient and precise. The network topology used to model

the experimental setup is illustrated in Figure 2.

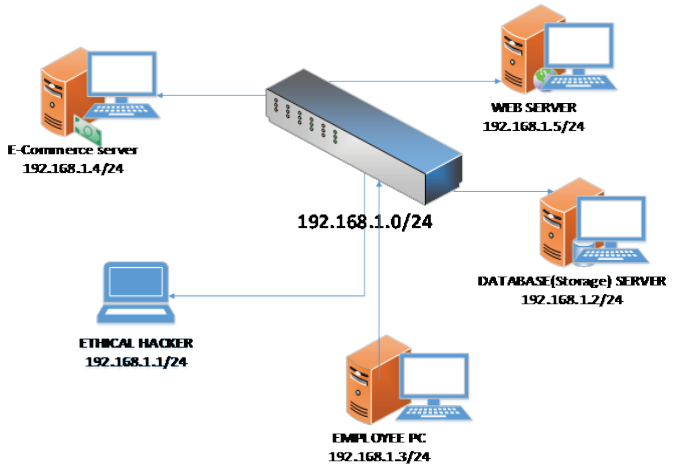

Figure 2. Network topology designed from reconnaissance.

Vulnerability scanning was performed on the e-commerce server, using the Nmap tool on Kali Linux. A list of open ports and services available on the server are shown in the table below.

Table 2: Msf console scan on the e-commerce server (192.168.1.4/24)

s/n	Port type	Port number	Status	Service
1	Tcp	135	open	Msrpc
2	Tcp	139	open	Netbios-ssn
3	Tcp	445	open	Microsoft-ds

Nmap scan on the web server (192.168.1.2) shows a

potential vulnerability, telnet port 23 is open. We will try to exploit this vulnerability in the exploitation phase. Nmap scan on the web server (192.168.1.5/24) shows potential vulnerabilities i.e. open ports and services that can be exploited using penetration testing. Figure 3 below depicts the data collected on the web server.

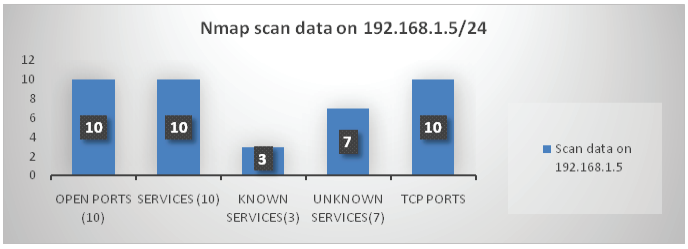

Figure 3. Open ports and services on web server 192.168.1.5/24

Gaining access (Exploitation)

On 192.168.1.4/24, we exploited the ms08_067_ netapi vulnerability identified during the scan. Figure 4 shows the screenshot of the ms08_067 attack carried out on the e-commerce server on the network infrastructure, which gives access to the command prompt of the server, data can be modified and system settings can be tampered with.

Figure 4: Ms08_067 vulnerability exploit on e-commerce server 192.168.1.4/24.

The figure below depicts the vulnerability levels, their indications, which followed by a brief summary of each vulnerability level.

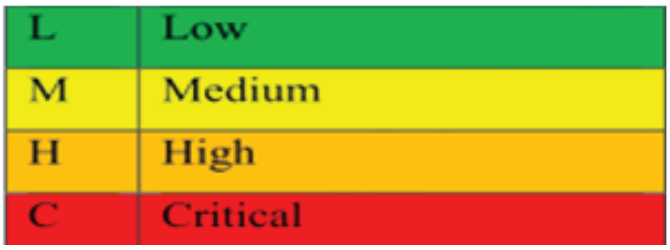

Figure 5:Vulnerability level color codes.

From the image shown above, L depicts low and this means a particular vulnerability would not course serious harm to the system even though it exists, it can be fixed by updating the Operating to get latest patches and fixes.

M depicts medium level of vulnerability, which implies that, the threat level has a mild effect on the Operating System. A more specific patch, which is peculiar to the vulnerability need to be used.

H depicts high level of vulnerability, it basically means that, it can cause damage to the Operating System when exploited.

C depicts critical level of vulnerability, if exploited, this can bring the system to a complete halt, and an attacker can take over the system remotely.

Multi/handler can be used with a payload of 'windows/ metsvc_bind_tcp' to connect to the remote system, as shown in Figure 6 below.

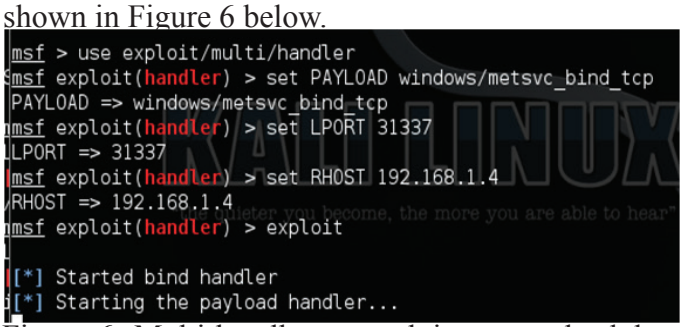

Figure 6. Multi-handler to exploit metsvc backdoor on e-commerce server.

RESULTS AND DISCUSSION

Thhe outcome of the penetration test carried out on the network created in the experiment phase shows that using the nmap tool on Kali Linux, we were able to discover the number of computers on the network, which comprises of both client and server operating systems. We were able to discover both the Media Access Control addresses of the devices and their respective ip addresses. Using this information, a network topology was drawn, which assigns valid IP addresses to both client and server operating systems found on the network. The network topology presented depicts all the devices that are on the network, including the Kali Linux PC used for carrying out the pen test on the network.Although the structure of the penetration testing process requires that results are presented after each phase, we have also presented the important results in table 3 below, followed by a detailed analysis of some results in subsequent subsections.

Table 3. Results and description

Device name	Device Internet Protocol address	Vulnerabilities and open ports found	Vulnerabilities exploited	Description	Proposed solution
E-commerce server.	192.168.1.4/24	TCP port 135, TCP port 139, TCP port 445 (Msrpc, Netbios-ssn, Microsoft-ds)	Ms08_067_netapi vulnerability.	This attack carried out on the E-commerce server gives full access to the command prompt, where changes can be made to the exploited Operating System.	The Ms08_067_netapi vulnerability patch should be implemented on the server, including other supported patches. Open ports on the server should be closed, allowing only ports that are in use by the server.
Web server.	192.168.1.5/24	Telnet port 23, 3 known services, 10 open ports, 7 unknown services.	Using the telnet protocol on port 23 sends data in clear text form.	This gives access to remote data using a packet sniffing tool.	The telnet protocol which uses port 23 for remote access should be replaced with SSH, which is more secured and operating on port 22. Telnet port 23 should always be closed and the protocol deactivated.
E-commerce server.	192.168.1.4/24	metsvc_bind_tcp	The multi-handler tool was used for exploiting the metsvc_bind_tcp vulnerability found on the server.	This vulnerability was exploited by maintaining access to the server.	The local port number 31337 on the server should be closed at all times.
E-commerce server.	192.168.1.4/24	metsvc payload	Backdoor exploit using meterpreter	Using the metsvc payload gave us the ability to create a backdoor on the e-commerce server.	A patch should be selected and installed from updates that are made available by the Operating System vendor.
E-commerce server.	192.168.1.4/24	Covering tracks	425 system data were wiped, and 236 app data were also wiped on the server to cover the tracks upon completion, as shown in figure 7.	This phase of the ethical hacking process is important since it helps in clearing all the activities of the ethical hacker.	Suggested solutions from subsequent phases of the pen test process should be implemented to prevent the hacker from getting to this final stage of covering tracks.

The Ms08_067 Vulnerability Analysis

The vulnerability could allow remote code execution if an affected system received a specially crafted RPC request. On Microsoft Windows Server systems, an attacker could exploit this vulnerability without authentication to run arbitrary code. The MS08_067 vulnerability can also be used to shut down the server remotely, which can have a catastrophic effect on the company's business.

Threat level: Critical

Vulnerability level: Critical

Denial of Service attack on webserver 192.168.1.5/24

The Table belowdepicts the screenshot of the Denial of Service (DoS) attack carried out on the web server.

Table 4. Denial of service attack on webserver 192.168.1.5/24 using port 80 (SYN flood)

S/N	Parameter	Value
1	LHOST (local host)	192.168.1.1
2	RHOST (remote host)	192.168.1.5
3	RPORT (remote port)	80
4	SNAPLEN (LENGTH)	65535
5	TIMEOUT	500

Denial of Service analysis

A Denial of service (DoS) attack on port 80 of the webserver results when the web server is continuously flooded with packets until it makes it unavailable or unable to reply legitimate requests from clients. Denial of service overloads the target's resources and other system resources affected are: CPU usage, network bandwidth, Hard disk space, database pool, and server memory.

Threat level: Critical
Vulnerability level: Critical

Backdoor exploit analysis

metsvc payload will give access back to the exploited server at later time using meterpreter shell. Having such backdoor access has a catastrophic effect on the server. Using the clearev command on the meterpreter prompt will clear the event log on the victim's computer and thus make it difficult for the victim to notice any changes or even know their system has been hacked. Figure 7 below shows the data that was wiped from the e-commerce server to prevent detection by the organization after completing the exploit.

Threat level: Critical
Vulnerability level: Critical

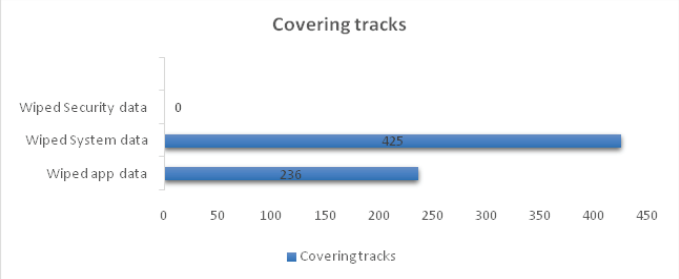

Figure 7: covering tracks using clearev on e-commerce server.

CONCLUSION

Ethical hacking unlike black hat hacking or hacking with malicious intent is an integral part of any organization or business that employs the use of Information Technology (IT). This ensures that computer systems and infrastructure are tested in a routine manner to prevent against hackers; this paper has shed light on the procedures by going through the five phases of penetration testing. Organizations need to employ pen testers to routinely test their server and host operating systems for vulnerabilities and make recommendations that will strengthen security of such systems. Kali Linux, an open source toolkit can be used to perform these tests as it provides all the tools needed to go through all the phases of penetration testing. The future direction of our work is to have this same technique of penetration testing, using Kali Linux, implemented in a datacenter environment, where more servers with different kinds of Operating Systems are available, and with connections to Wide Area Networks.

We conclude the experiment section by presenting the following recommendations:

1. The MS08_067 vulnerability found on the e-commerce server is a huge security risk as it allows a hacker access to sensitive information. Latest patches should be applied to the server to remedy this vulnerability.
2. The use of telnet service for remote access should be discouraged and replaced with SSH on port 22, as it is more secure sending encrypted traffic.
3. Hosts and network devices should be configured to block ICMP echo requests from unknown source addresses (broadcasts) by default. This is a suspicious behavior which hackers use for information gathering about the IP and mac addresses on the network using ping sweeps.
4. Organizations making use of various types of Operating Systems as emulated in the virtual network designed in this work should always have the Operating Systems updated to versions that include latest patches with built-inIntrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).
5. Patches to Operating Systems should be managed using patch management systems, as this is a more effective and efficient way of applying patches. This will ensure a centralized control of updates to all systems, which reduces the burden of manual updates by system administrators thus enhancing overall system security.
6. Penetration testing should be conducted at least twice a year and vulnerability assessment be conducted at least three times a year, this will help fix security challenges when major changes are carried out in the organization's computer infrastructure.

REFERENCES

Broad, J.and Bindner, A. (2014). Hacking with Kali. Massachusetts: *Elsevier.* Pp167-172.

Cisco Systems Inc. (2016). *Campus Wireless LAN Design Fundamentals,* San Francisco, Cisco Publishing, Pp7-24.Engebretson, P., 2013. *The basics of hacking and penetration testing*: ethical hacking and penetration testingmade easy. Elsevier.

Global Knowledge. (2011). *The 5 Phases of Hacking: Covering Your Tracks*. Available: http://blog.globalknowledge.com/technology/security/hacking-cybercrime/the-5-phases-of-hacking-covering-your-tracks/. Last accessed 16th April 2015.

Naik, A, Kurundkar, D, Khamitkar, D. and Kalyankar, V. (2009). Penetration Testing: A Roadmap to NetworkSecurity. *Journal of Computing*. 1 (1):187-190.

Nelson, W.B.V., Laizerovich, D., Bunker, E.E. and Van Schuyver, J.D., Achilles Guard Inc.,2008. *Network security testing*. U.S. Patent 7,325,252.

Nidhra, S and Dondeti, J. (2012). Black Box and White Box Testing Techniques- A literature Review. *International Journal of Embedded Systems and Applications* (IJESA). 2 (2):29-50.

Oriyano, S (2014). Certified Ethical Hacker Study Guide. 8th ed. Indiana: John Wiley & Sons, Inc. Pp444-473.

Simpson, T., Backman, K. and Corley J. (2011). Ethical Hacking Overview. In: Helba, S. and Bellegarde,Marah HANDS-ON ETHICAL HACKING AND NETWORK DEFENSE. Boston:Cengage Learning. Pp4-5.

Stallings, W (2012). *Operating Systems: Internals and Design Principles*. 7th ed. NewJersey, Prentice Hall. Pp620-700.

Sulagna. (2009). Introduction to API Testing. Available:http://www.scribd.com/doc/9808382/Introduction-to-API-Testing#scribd. Last accessed 20th April 2015.

Tang, A. (2014) A guide to penetration testing. Network Security, Pp8-11.

Whitaker, A & Newman, D. (2006). Understanding Penetration Testing. In: John Kane and BrettBartow *Penetration Testing and Network Defense*. Indianapolis: Cisco Press. Pp5-6

Yeo, J. (2013) *Using penetration testing to enhance your company's security. Computer Fraud & Security* 2013.4 (2013), Pp17-20.