# Importance Of Penetration Testing For Legacy Operating System

Poorvi Bhatt

**Abstract:** Penetration testing is very important technique to find vulnerabilities in commercial networks. There are various techniques for ethical hacking via penetration testing. This report explains a white hat hacker approach of penetration testing. I have performed this test on private network where three PCs are connected through LAN via switch and without firewall. This network is not connected with Internet. All the PCs have windows operating system. The attacker host has windows server 2003 with Service Pack1, second host has windows XP with Service Pack 2 and third host has windows 2000 with service pack 4.

**Index Terms:** Penetration Testing, Ethical Hacking, Cyber Security, White Hat, NMAP, NETCAT, Metaspoilt,

## 1. Introduction

A penetration test is the process of actively evaluating your information security measures. There are number of ways that this can be undertaken, but the most common procedure is that the security measures are actively analyses for design weaknesses, technical flaws and vulnerabilities; the results are then delivered comprehensively in a report, to Executive, Management and Technical audiences. This report explains a white hat hacker approach of penetration testing. I have performed this test on private network where three PCs are connected through LAN via switch and without firewall. This network is not connected with Internet. All the PCs have windows operating system. The attacker host has windows server 2003 with Service Pack1, second host has windows XP with Service Pack 2 and third host has windows 2000 with service pack 4.

## 2. Steps to Perform Penetration Testing

In general penetration testing can be performed in five steps,

- Reconnaissance (Knowing about target.)
- Scanning target to find vulnerabilities
- Gaining access using that vulnerabilities
- Maintaining Access
- Covering Tracks.

### 2.1 Reconnaissance

It is all about knowing the target. This can be done in two ways

Active: This involves finding vulnerable ports in the target system. Once the access is gained the system can be exploited. [1]

Passive: This involves gathering information about the target through social engineering, finding about network setup, systems and staff. Using WHOIS maximum information can be gained. [2]

- *Poorvi Bhatt is currently working as Sr. Software Engineer*
- *at Leidos (Legacy Lockheed Martin IS&GS), Atanta, GA, USA. Ph-No: 4047353416,*
  *Email: poorvy@gmail.com*

In this situation, network is very simple and without firewall so it is easy to ping all the machines in the network. That is why I have used Active Enumeration Technique to gain access. By ipconfig command, I managed to find out ip of my machine and using the following command ping other PCs.

FOR /L %i IN (1,1,255) DO ping -n 1 192.168.250.%i

This command will ping all the PCs in the network and will show which host is up and running. In my network both the host are up and running with the IP 192.168.250.154 and 192.168.250.201. As firewall not installed ping helped me other wise traceroute (tracert) technique can be used to find the location of firewall and then target machine. Other active enumeration techniques like SNMP (Simple Network Map Protocol), Firewalking or Banner Grabbing can also be used.

### 2.2 Scanning

Now the next step is to scan the target machine so that we can know which ports are open and which services are running on that port. There are various tools available to scan the network such as NMAP and LANguard Network Security Scanner. I have used NMAP 4.11 for windows: “Nmap ("Network Mapper") is a free open source utility for network exploration or security auditing.” [3] Nmap is free software, available with full source code under the terms of the GNU GPL. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Nmap runs on most types of computers and both console and graphical versions are available. The advantage of using Nmap over LANguard is, it is available for linux operating systems also. In addition, nmap could not be detected by many firewalls. Following are the very well know commands of nmap

namp –sT –p 1-x.x.x.x
nmap –sS x.x.x.x
nmap –sF x.x.x.x
nmap -sS -sR -O -P0 192.168.250.154

-sT Stealth mode TCP Connect() is a three way handshake (SYN,SYN/ACK/ACK)

-sS TCP SYN stealth port scan (default if privileged (root))
-sR/-I RPC/Identd scan (use with other scan types)
-O Identifying Remote Operating System.
-P0 Don't ping hosts.

First, I scanned this host to see whether it is vulnerable or not. As the nmap could not detect many ports and it also could not detect the Operating System. Therefore, it seems that this host is not easily vulnerable. I tried next one.

nmap –sS –sR –O –P0 192.168.250.201

As shown in the Figure-1 the nmap result shows various ports are open on the target machine and various services are running on those ports. It also shows that windows2000 is operating system.

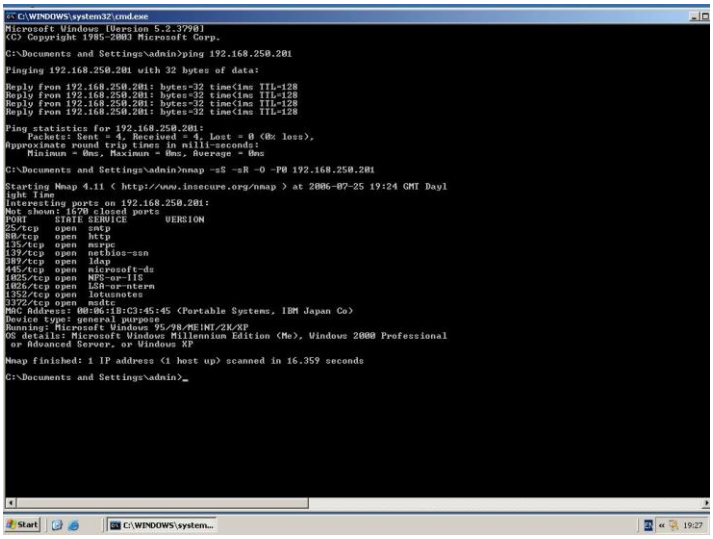


***Figure: 1*** *nmap scan results.*

Port 135 is open and msrpc (Microsoft Remote Procedure Call) service is running on this port. "Msrpc service provides plenty of attack surfaces for buffer- overflow exploits and the like." [4] This service is highly vulnerable and it can not be disabled easily without affecting the core functionality of Operating System. As the open port has been founded, it is easy to exploit target host using Metasploit Framework or any other tools.

### 2.3 Exploiting Target Machine And Gaining Access

To exploit the target host I have used Metasploit Framework-2.6.

"The Metasploit Framework is an advanced open-source platform for developing, testing, and using exploit code. This project initially started off as a portable network game and has evolved into a powerful tool for penetration testing, exploit development, and vulnerability research." [5] This Metasploit Framework is also provided by whoppix, but I have used windows based Metasploit Framework 2.6. This framework provides console based, command line base and web based interface. I have used web-based interface. After installing Metasploit Framework 2.6 run MSFWEB as shown in the Figure-2.

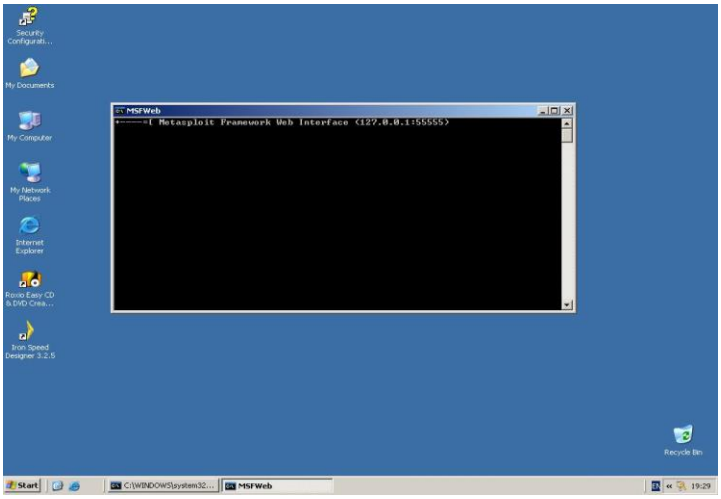


***Figure: 2*** *Running Metasploit Framework*

Then open explorer and type in 127.0.0.1:55555 and you will see the screen shown in Figure-3.

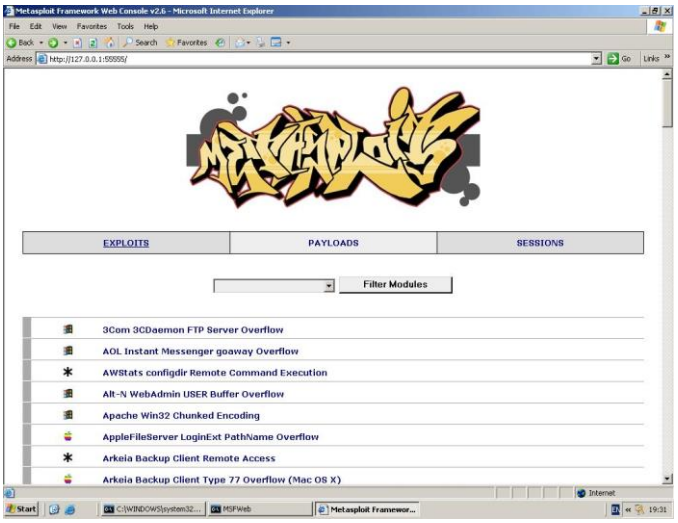


***Figure: 3*** *Web-Based Metasploit Framework*

As shown in Figure-3 Metasploit Framework provides list of exploit modules. These modules are categorized under different applications. I have used DCOM application to select Microsoft RPC DCOM MSO3-026 exploit.

- About Microsoft RPC DCOM Exploit

Microsoft found out about this exploit in July, 2003. [6] This exploits has three vulnerabilities, which highly affect Microsoft Windows family of operating systems. Among these vulnerabilities, two are buffer overflow vulnerabilities, which can be exploited to execute arbitrary code on local system/ target machine. These vulnerabilities are called MS03-026 and MS03-039. These flaws occurred because of the error in the RPC Service. RPC Service deals with the message exchange over TCP/IP. If the message handling is incorrect then this vulnerability affects a Distributed Component Object Model (DCOM) interface with RPC. And if the message sent to server is specially modified then they may be able to crash the service and can run any code with

administrative privileges. These vulnerabilities affect Windows NT, Windows XP, Windows 2000 and Windows Server 2003. But it does not affect Windows Millennium Edition. To resolve this issue Microsoft has provided various security patches according to operating systems. But if that patch is not installed on the host machine, then the host machine can be hacked easily. [6] The third vulnerability is called Denial of Service (DoS) attack against the vulnerable host. [7] This vulnerability occurred because of the error in RPCSS Service. "Depending on variables such as network latency and CPU load, one RPCSS thread may free a memory buffer before another thread has finished processing the same buffer. This causes memory corruption that can lead to termination of the RPCSS process." [8]
I have used vulnerability MS03-026, as it is critical compare to Denial of Service as shown from the assessment [9] As my target machine has Service Pack 4 and windows 2000 though I was able to hack it using vulnerability because the required patch was not installed. After filtering the exploit based on the application, you will see screen as shown in below Figure-4.

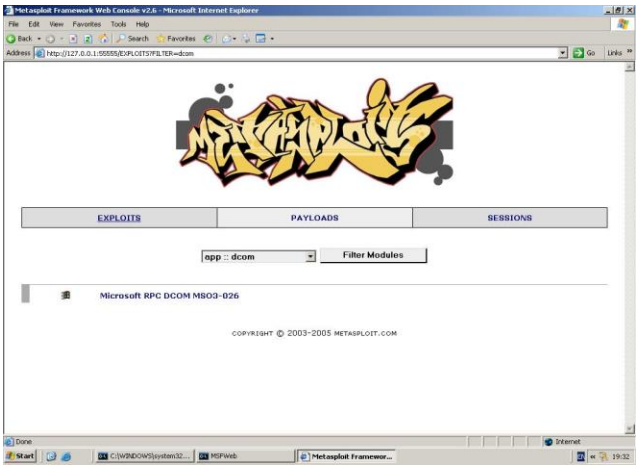


***Figure: 4*** *Filtered Module*

When you click on the Microsoft RPC DCOM MSO3-026 the following screen will appear.


***Figure: 5*** *Description of Microsoft RPC DCOM MS03-026 Exploit*

This Figure-5 shows more information about the exploit. It will also show that which operating system can be exploited using this vulnerability and up to which service pack it is vulnerable. By clicking on Select Target link following list of payloads will appear.

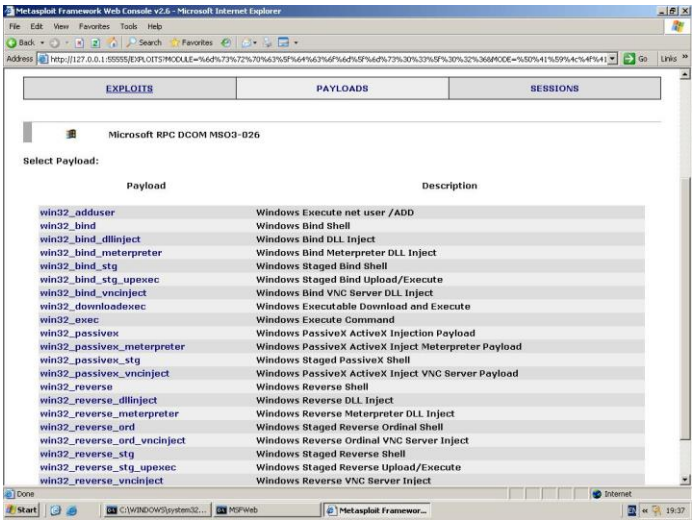


***Figure: 6*** *List of Payloads of Microsoft RPC DCOM MS03-026 Exploit.*

From the above list of payload select win32_reverse shell payload. Win32_reverse will give us a shell, which can be used to pass data back and forth. This will give us a session and connection on both the sides, which is quite useful. Click on that payload and the following screen will appear.

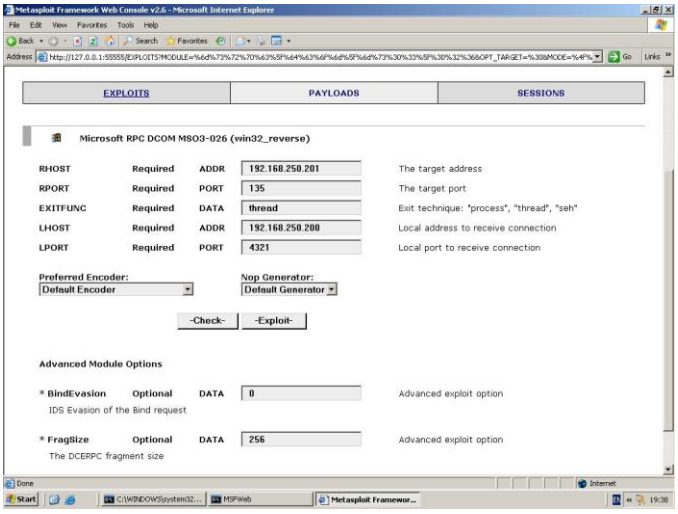


***Figure: 7*** *Enter ip of target machine and exploit.*

Here type in the IP of target machine and click on Exploit Button.

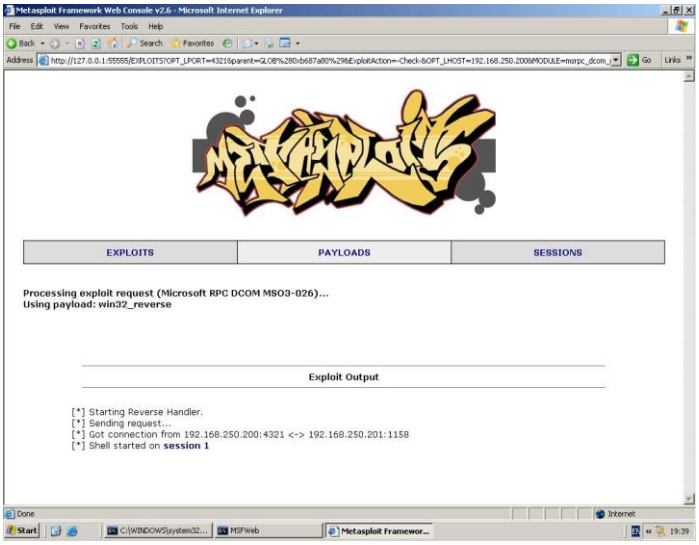


***Figure: 8*** *Session 1 has started*

As shown in Figure-8 session 1 has started. Click on session 1 and type in ipconfig to make sure you have gain access to the target machine.

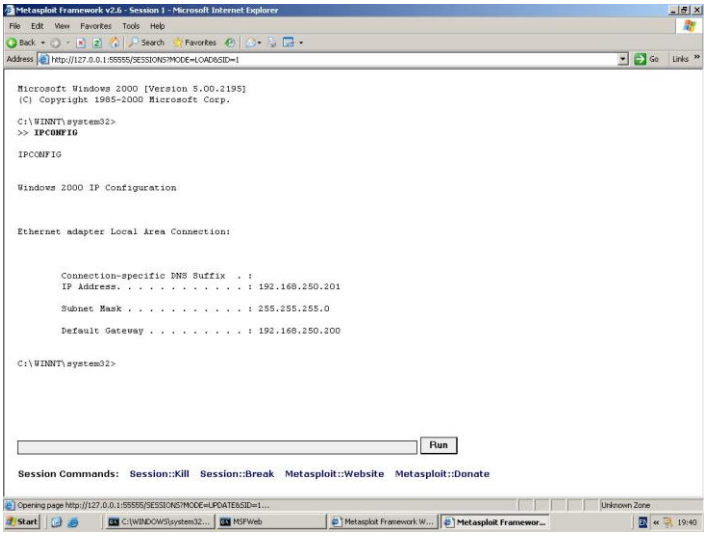


***Figure: 9*** *Session 1, showing connection with the target machine.*

Now the next step is to create a user on the target machine and giving administrative privileges to that user.

### 2.4 Privilege Escalation & Account creation

By using the following command user is created and added in to administrative group as shown in the following figure.
net user netadmin testpen /add
net localgroup administrators /add
netadmin

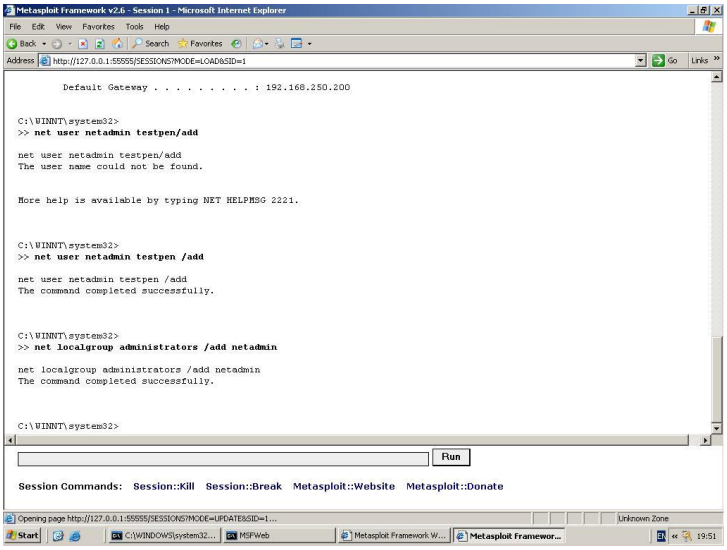


***Figure: 10*** *Demonstration of user created and added to administrative group.*

After gaining the access it is important to maintain the access.

### 2.5 Maintaining Access

Every hacker would try to create a backdoor, which can be used at later stage. This can be done using various tools such as using TFTP server install Netcat on target machine and create one port on target machine which will always remain open to listen.

### 2.6 Covering Tracks

If the hacker wants to come back s/he will cover the tracks. For example if the netcat service is running on the target machine that can easily be detected. In order to hide this service it can be renamed to other service name.

## 3. CONCLUSION

Using NMAP and Metasploit Framework I managed to get access of the target machine. But it is not that simple as first time I failed to scan the host 192.168.250.154 the reason was so many security patches were installed on that host. Whilst I managed to exploit 192.168.250.201 using Microsoft RPCDCOM-MS03-026 though it has operating system windows2000 and service pack 4 because the security patch against MS03-026 vulnerability was not installed. Metasploit Framework provides large range of exploits with the list of which operating system is vulnerable up to which service pack. But in real world scenario it is important to cover full range of threat. The testing should be performed on networks with antivirus and firewalls and the patches installed to get the actual result. And those tools should be used which have latest vulnerability exploits such as Metasploit Framework.

## 4. REFERENCE

[1] http://wi-fiplanet.webopedia.com/TERM/A/active_reconnaissance.html

[2] Lecture notes and Practical Guidance by Mr. Suranjith

[3] http://www.insecure.org/nmap/

[4] http://searchsecurity.techtarget.com/general/0,295582,sid14_gci1088904,00.html

[5] http://www.metasploit.com/projects/Framework/

[6] http://www.microsoft.com/technet/security/Bulletin/MS03-026.mspx

[7] http://www.kb.cert.org/vuls/id/547820

[8] http://www.kb.cert.org/vuls/id/568148

[9] http://www.microsoft.com/technet/security/bulletin/MS03-039.mspx See Technical Details.