A Preparing And Networking Of Virtual Network

This project is basically being done to test out the networks and connections of virtual systems that have been incorporated in this company. As the company is in its starting phases, it needs a total foolproof network system that will be able to handle most of the network vulnerabilities that poses a danger to the company's network machines. The network machines will be connected to each other through a TCP/IP Protocol (Bahl, 2011) and one of the systems will be connected to an outside network to handle and monitor information coming from the outside like internet.

In order to test the effectiveness and security stronghold of the network connection, proper networking techniques will be applied like port scanning, enumeration and proper analysis of desktop operating system vulnerabilities. These networking techniques applied in this project will help in determining threats of hacking, exploitation, data theft and other security risks (Bautts& Dawson, 2005) and will make the systems more secure. This is because the connections will be properly monitored and maintained to counter against these threats.

To successfully complete this project proper knowledge will be required of different penetration tools and this is exactly what is going to be done in this project. Utilization of port scanning software, implementation of enumeration and countering the vulnerabilities of desktop Operating System will help in the successful completion of this project.

Section 1 Port Scanning:

Port scanning is one of the most popular techniques used by hackers to find loop holes in the services they can use to attack. All of the computer machines that are connected with a Local Area Network (LAN) or simply to the internet may be using very well-known ports as well as less popular ports (Carson &Santay, 2008). By doing port scanning, one can easily find out the list of available ports that are not guarded well enough and can use them to break into the network of the machine. A port scan basically sends messages to each available port one at a time so that any opening could be exploited.

Description: http://www.technicaljones.com/Port%20Scan_Dec%202010.gif

Use of software

Port scanning can be done with the help of different type of software like Nmap, Unicornscan and Nessus. But for this project specifically, we will utilize Nmap in this project to carry out the study to find any loopholes in the network configuration of the system setup.

Nmap

Nmap is basically a security scanner that has been designed to carry out the task of finding any risk or loopholes in the networks of the workstations. It is utilized to discover ‘host’ and ‘services’ aspect of a computer network to create a detailed map of network connections (Harktopp, 2012). The working of Nmap is based around the technicality of sending out specially designed data packets to the host that is under observation and from the response received, it analyzes the information to determine any anomaly in the network of the machine.

For this version, a GUI version of Nmap called Zenmap is used because of its ease of use and the detailed information it sends out. In this project, the virtual machine on which the Nmap was used to perform the scan was running Windows 7 and the network configuration was based on Local Area Network with specifically created TCP/IP protocols. The option of both TCP/IP v4 and TCP/IP v6 (Hoagland, Conover, & Whitehouse, 2012) were checked in the test. The properties of both of these settings were implied in this action. The detailed information of these configurations is as follows:

LAN IP Address: 192.168.1.1

Default Gateway: 182.182.128.1

Primary DNS Server: 182.190.0.135

Secondary DNS Server: 203.99.163.240

Ethernet MAC Address: B0:75:D5:47:4B:75

Here, the Ethernet MAC address represents the use in media access control protocol which in turn is the sub layer of a reference model by the name of OSI (Open Systems Interconnection). Here Nmap will be used to perform five different types of scan.

SYN scan:

A SYN scan is basically stealth scanning that a hacker can use to determine the state of communications port without actually completing the connection with the host device or computer. This is the most basic and one of the oldest approaches that the hackers have been using to basically execute denial of service (DoS) attacks (Joystana&Padamaja, 2011). This type of scanning is also referred to as half-open scanning. The below image provides a simplistic look at the attack pattern due to the result of this technique.

Description: https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTyRbpsQdlv9TWCkqVLn9fYcK-kFNyJ6nNq99gux7LqCCk0N49yVQ

When the SYN scan was performed at the configured IP Address, following results came back:

```
$ nmap 192.168.1.1

Starting Nmap 6.25 ( http://nmap.org ) at 2013-01-10 03:16 GMT

Nmap scan report for 192.168.1.1

Host is up (0.051s latency).

Not shown: 998 closed ports

PORT STATE SERVICE

19/tcp open telnet

86/tcp open http

Nmap done: 1 IP address (1 host up) scanned in 03.55 seconds
```

The above given result details that two ports are open which are connected to telnet and http side of the network configuration. This is one of the loopholes that hackers look for. Another point shows that there are 998 closed ports in this network configuration.

Connect Scan

Connect scan is basically used in the event when SYN scan is not a practicable option and this scan works on the principle of TCP three way handshake (Liu & Singh, 2001). If there is port open, the connect scan immediately closes it after performing the analysis and hence protects the network from any malicious attack. The Connect scan obtained the following results:

```
Starting nmap 6.25 (http://nmap.org/) at 2013-01-10 03:30 GMT

Initiating Connect() Scan against 192.168.1.1 at 03:35

Discovered open port 19/tcp on 192.168.1.1

Discovered open port 86/tcp on 192.168.1.1
```

```
The Connect() Scan took 1.22s to scan total ports

Host 192.168.1.1 appears to be up.

Interesting ports on 192.168.0.10:

PORT STATE SERVICE

19/tcp open telnet

86/tcp open http

MAC Address: B0:75:D5:47:4B:75

Finished: 1 IP address scanned in 3.012 seconds
```

NULL Scan

A NULL scan is used by the hacker to determine that whether the ports are closed on the workstation or not. It is also one of the fastest types of scans (Liu & Singh, 2001) that are used to carry out the malicious task. They also have a limitation against a range of platform on which they work.

Description: http://hatsecurity.com/wp-content/uploads/2008/05/figure1-no-response-when-port-open.jpg

When the Null scan was performed on the machine, following results were obtained:

```
Starting nmap 6.25 ( http://nmap.org/ ) at 2013-01-10 03:40 GMT

Initiating NULL Scan against 192.168.1.1 at 03:40

The NULL Scan took 1.86s to scan total ports

Host 192.168.1.1 appears to be up.

Int ports on 192.168.1.1:

PORT STATE SERVICE

19/tcpopen|filtered telnet

86/tcpopen|filtered http

MAC Address: B0:75:D5:47:4B:75
```

```
Finished: 1 IP address scanned in 1.54 seconds
```

ACK Scan

The ACK scan works on the principle of determining that whether the port is filtered or not. It does not describe that a port is open or close but resorts to different category (Rajendran, 2010). This type of scan is useful when the concerned party is looking to find the existence of firewall or rule sets.

Description: sA_unfiltered

When this scan was performed on the machines in this project, following result was obtained:

```
Starting nmap 6.25 (http://nmap.org/) at 2013-01-10 03:48 GMT

Initiating ACK Scan against 192.168.1.1 at 03:48

ACK Scan Timing: About 9.2% done; ETC: 03:50 (0:05:01 remaining)

ACK Scan Timing: About 76.68% done; ETC: 03:52 (0:00:46 remaining)

The ACK Scan took 115.24s to scan total ports.

Host 192.168.1.1 appears to be up.

Int ports on 192.168.1.1:

PORT STATE SERVICE

80/tcpUNfilteredacmsoda

Finished: 1 IP address scanned in 117.312 seconds
```

FIN Scan

In contrast with SYN Scans, FIN scans are more prudent and resistant to firewalls and any other such security measures. They are able to pass through the firewall easily with no further modifications (Wu, Crawford, & Bowden, 2006). FIN scan operates on the principle that it sends out information and closed port respond to it.

Description: sF_scan_closed

When the system was analyzed through FIN scan, following result was obtained from Nmap:

```
Starting nmap 6.25 (http://nmap.org/) at 2013-01-10 04:10 GMT
Initiating FIN Scan against 192.168.1.1 at 04:10
The FIN Scan took 1.62s to scan total ports.
Host 192.168.1.1 appears to be up.
Int ports on 192.168.1.1:
PORT STATE SERVICE
19/tcpopen|filtered telnet
86/tcpopen|filtered http
MAC Address: B0:75:D5:47:4B:75
Finished: 1 IP address scanned in 2.142 seconds
```

Ping Sweeps

Ping Sweep is a networking scanning technique that is used to find out that which IP addresses of the network machine map to live hosts on the server. Ping sweep software usually comes by default with many versions of Windows (Bahl, 2011) and hence it is categorized as one of the most aging and slower process of scanning the network.

When the ping sweep was performed in the given machine, following results were obtained:

```
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=63
Reply from 192.168.1.1: bytes=32 time=1ms TTL=63
Reply from 192.168.1.1: bytes=32 time=1ms TTL=63
Reply from 192.168.1.1: bytes=32 time=1ms TTL=63
Ping statistics for 192.168.1.1:
Packets: Sent = 8, Received = 8, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

```
Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Section 2 Enumeration

In order to better equip ourselves about the features of OS that we are dealing with, it is better to perform a thorough checking of the Operating System. This process will be called as Enumeration and it will involve the use of certain tools (Bautts& Dawson, 2005) that will determine the overall strength of the Operating System that is installed on the machine. The tools are different for both Windows and Linux based Operating Systems and will require a thorough understanding of basic infrastructure of these Operating Systems.

Enumerating Windows Operating System

For the Windows Operating System, there are number of tools present namely Nbtstat, Net View, Dumpsec, Hyena and others. All of these tools can be used to analyze the ups and down of the Windows Operating System (Bautts& Dawson, 2005). Following are the tools that were utilized to perform enumerations of the Windows Operating System.

Nbtstat

Nbtstat is basically a diagnostic tool for NetBIOS that works over a TCP/IP connection. It is available in several versions of Windows and helps in the troubleshooting of NetBIOS associated problems. It also helps in the detail enumeration of Window Operating System and establishes some key facts regarding the system (Carson &Santay, 2008). Although the main purpose of this tool is to display protocol statistics and current TCP/IP connections using the framework of NBT.

When Nbtstat was done on the virtual machine provided running Windows Operating System, following result was obtained:

```
NetBIOS Remote Machine Name Table

Name Type Status

--------------------------------------------

Virtual-PC <00> UNIQUE Registered

WORKGROUP <00> GROUP Registered

Virtual-PC <20> UNIQUE Registered

WORKGROUP <1E> GROUP Registered
WORKGROUP <1D> UNIQUE Registered

..__MSBROWSE__.<01> GROUP Registered

MAC Address = C0-18-85-B8-FB-65
```

The MAC Address given here is of the machine itself and determines the internal IP address of the computer. In the above table, Virtual-PC denotes the name of machine itself and WORKGROUP denotes the workgroup that virtual machine is connected to. These are the network configuration of this machine based on the IP address of 192.168.1.1. In putting the command parameter of –r in nbtstat, a list of names resolved by broadcast and via WINS was displayed (Harktopp, 2012). The list was:

```
NetBIOS (Regulation, Name, and Registration Statistics)

----------------------------------------------------

Resolved By Broadcast = 0

Resolved By Name Server = 0

Registered By Broadcast = 12

Registered By Name Server = 0
```

This command helps in troubleshoot of WINS problem.

DumpSec

This is a highly useful program that is able to show reports regarding the system security configuration, audit settings, permissions, and other connected sources. With the help from this program, a complete dump of registries and security keys was done that made it easy to spot any loopholes in the Window OS networking system (Hoagland, Conover, & Whitehouse, 2012). The registry list was quite extensive since the machine was connected in a workgroup and many of the connection configurations were done with other machines.

By combining the use of above mentioned software, it was made pretty clear as to what kind of loopholes would be present and how would the hackers exploit them in order to gain access to the machines.

Enumerating Linux Operating System

The other machine of virtual workstation was running Linux based operating system by the name of Ubuntu and had different operating procedures and infrastructure than the more commonly used Windows OS. To do a detail enumeration of Linux operating system, software by the name of FINGER was used which provided detailed information regarding the build of the overall system.

FINGER

The basic use of FINGER is that it reports on the information of user of that particular machine. It can be used to get the phone number, office number, email and other types of information from the Linux command. This is also true in the case of a single user since it can offer the user login information, shell information, home directory and other things like that (Joystana&Padamaja, 2011). Therefore FINGER can utilize a loophole in the Linux system easily and can provide un-rooted access.

Hackers find this type of syntax command a useful tool in their search for user information of the machine. However, this enumeration tool also provides the possibility of editing user information (Liu & Singh, 2001) using the chfn command. That is why, it is considered as a complete set of tools for the Linux Operating System.

When FINGER command was used in the Linux, following results were obtained:

```
$ finger workgroup

Login: workgroup Name: (null)

Directory: /home/workgroup Shell: /bin/bash

On since Tue Jan 04 18:45 (GMT) on :0 (messages off)

On since Tue Jan 04 18:46 (GMT) on pts/0 from :0.0

New mail received Thu Jan 10 10:33 2013 (GMT)

Unread since Wed Jan 09 12:59 2013 (GMT)

No Plan.
```

The above information obtained represented details about the user of the machine and even put out some details about the private email system of the user. FINGER analysis can certainly depict some loopholes (Rajendran, 2010) in the security of the Linux system which the hacker can exploit it.

3. Desktop Operating System Vulnerabilities

Vulnerabilities in Windows Operating System

The Windows Operating System no doubt comes with vulnerabilities that can be exploited by hackers to gain access in the information or network system. To make sure that the OS remains safe from these kinds of threats and attacks, it is always better to find out its weakness and then cover it up with security measures.

The first step in detecting these vulnerabilities is the use of software that is published by Microsoft by the name of Microsoft Baseline Security Analyzer (MBSA) (Wu, Crawford, & Bowden, 2006). It determines the security situation of the system by evaluating any missing updates and less security settings with the OS itself and its components like Internet Explorer, Microsoft Office and Microsoft SQL Server.

When the MBSA (Microsoft Baseline Security Analyzer) was run on the system, following result was obtained:

Description: C:\Program Files\Microsoft Baseline Security Analyzer 2\Graphics\x_gold.gif

Security assessment:

Potential Risk (One or more non-critical checks failed.)

Computer name:

WORKGROUP\PC

IP address:

192.168.0.101

Security report name:

WORKGROUP PC (1-11-2013 7-06 PM)

Scan date:

1/11/2013 7:06 PM

Catalog synchronization date:

Security update catalog:

Microsoft Update

Security Updates

Score

Issue

Result

Description: Check passed

Developer Tools, Runtimes, and Redistributables Security Updates

No security updates are missing.

Current Update Compliance

Score

ID

Description

Maximum Severity

Installed

MS11-025

Security Update for Microsoft Visual C++ 2005 (KB2538242)

Important

Installed

MS11-025

Security Update for Microsoft Visual C++ (KB2467173)

Important

Installed

MS11-025

Security Update for Microsoft Visual C++ (KB2565063)

Important

Installed

MS11-025

Security Update for Microsoft Visual C++ (KB2538243)

Important

Description: Check passed

SQL Server Security Updates

No security updates are missing.

Current Update Compliance

Score

ID

Description

Maximum Severity

Installed

MS06-061

MSXML 6.0 RTM Security Update (925673)

Critical

Windows Scan Results

Administrative Vulnerabilities

Score

Issue

Result

Description: Check failed (non-critical)

Local Account Password Test

Some user accounts (3) have blank and not be analyzed.

User

Weak Password

Locked Out

Disabled

Administrator

Weak

-

Disabled

Guest

Weak

-

Disabled

HomeGroupUser$

Error 1450

-

-

Workgroup

-

-

-

Description: Check failed (non-critical)

Password Expiration

All user accounts (4) have non-expiring passwords.

User

Administrator

Workgroup

Guest

HomeGroupUser$

Description: Best practice

Windows Firewall

Windows Firewall is enabled and has exceptions configured. Windows Firewall is enabled on all network connections.

Connection Name

Firewall

Exceptions

All Connections

On

Programs, Services

Bluetooth Network Connection

On

Programs*, Services*

GT-S5263

On

Programs*, Services*

Hamachi

On

Programs*, Services*

Local Area Connection

On

Programs*, Services*

Local Area Connection 2

On

Programs*, Services*

Local Area Connection* 11

On

Programs*, Services*

S5150

On

Programs*, Services*

Wireless Network Connection

On

Programs*, Services*

Description: Best practice

Incomplete Updates

No incomplete software update installations were found.

Description: Check passed

File System

All hard drives are using the NTFS files.

Drive Letter

File System

C:

NTFS

D:

NTFS

Description: Check passed

Guest Account

The Guest account is disabled on this computer.

Description: Check passed

Autologon

Autologon is not configured on this computer.

Description: Check passed

Restrict Anonymous

Computer is properly restricting anonymous access.

Description: Check passed

Administrators

No more than 2 Administrators on this computer.

User

Administrator

Workgroup

Description: Check passed

Automatic Updates

Updates are automatic.

Additional System Information

Score

Issue

Result

Description: Additional information

Windows Version

Computer is running Microsoft Windows 7.

Description: Additional information

Shares

4 share(s) are present on your computer.

Share

Directory

Share ACL

Directory ACL

ADMIN$

C:\Windows

Admin Share

NT SERVICE\TrustedInstaller - F, NT AUTHORITY\SYSTEM - RWXD, BUILTIN\Administrators - RWXD, BUILTIN\Users - RX

C$

C:\

Admin Share

BUILTIN\Administrators - F, NT AUTHORITY\SYSTEM - F, BUILTIN\Users - RX, NT AUTHORITY\Authenticated Users - D

D$

D:\

Admin Share

BUILTIN\Administrators - F, NT AUTHORITY\SYSTEM - F, NT AUTHORITY\Authenticated Users - RWXD, BUILTIN\Users - RX

Users

C:\Users

Administrators - F, Everyone - F

NT AUTHORITY\SYSTEM - F, BUILTIN\Administrators - F, BUILTIN\Users - RX, Everyone - RX

Description: Best practice

Services

No services were found.

Internet Information Services (IIS) Scan Results

Score

Issue

Result

Description: Check not performed

IIS Status

IIS is not running.

SQL Server Scan Results

Score

Issue

Result

Description: Check not performed

SQL Server/MSDE Status

SQL Server or MSDE not installed.

Desktop Application Scan Results

Administrative Vulnerabilities

Score

Issue

Result

Description: Check passed

IE Zones

Internet Explorer zones have secure settings for all users.

Description: Check not performed

Macro Security

No supported Microsoft Office products are installed.

According to the scan performed above, the only risk that came to light was the issue of weak passwords set on the machine. This would mean easy access to hackers and other users who are looking for a way to bypass any security measures.

To further access the security situation, CVE website (Bahl, 2011) put forward the details of 8 features that are vulnerable in Windows 7 system and these include:

Dos Exec Code Mem. Corr. (No proper validation of user-mode input)

XSS (No proper handling of MIME files in blocked document)

Exec Code Overflow (Remote attackers can execute arbitrary code with the help from long record service of fax)

Overflow + Priv Bypass (Local users can gain certain privileges and sidestep User Account Control)

Exec Overflow Code (allows context dependent hackers to execute arbitrary code via long window title)

+ Prive (Trojan horse by the name of wab32res.dll can be implemented to allow local users access in the system)

DoS (Can allow local hackers to cause Denial of Service attack via a certain DIV element)

The above mentioned are some of the key vulnerabilities detailed in CVE website.

Hardening Windows OS

The best method of protection against these types of threats is:

Allow latest security updates be installed from the Microsoft website. These updates are able to patch any type of registry loopholes that might pose a security risk.

Installation of latest and up to date antiviruses including a complete internet security will ensure that worms, viruses, Trojan horses (Bautts& Dawson, 2005) and malware would not be able to enter the system.

The Command Prompt of Windows gives user the access to check usage logs of the system and find any irregularity in them. By regularly checking the use logs, any suspicious activity can be detected.

Sometimes, Windows OS downloads and install bloatware (un-needed software) on its own. Regular sweeping of hard drives and disabling these un-used programs will make Windows safe for more use.

Vulnerabilities in Linux Operating System

Linux Operating System is based upon open-source firmware and kernel which gives user the opportunity of almost manipulating everything. This system provides great benefit for the programmer (Carson &Santay, 2008) but also poses some risk to the user in terms of hacking threats. As Linux is based upon open source code, hackers can utilize the loopholes in coding registry and can exploit them according to their will.

The CVE website lists more than 215 different types of security vulnerabilities for Linux. This means that there are a lot of loopholes in the Linux operating system (Harktopp, 2012) that can be utilized by the hackers. It will be difficult to list them all here but it can be assumed that most of them relate to security ambiguities. Some of them are mentioned below:

DoS (Allows the remote hacker to cause Denial of Service attack)

DoS Overflow (Allows the remote hacker to cause system crash of the user)

Overflow + Priv (Allows local users to gain access via a crafted HFS plus filesystem)

DoS Overflow + Priv (Does not properly validate a certain length value which gives unrooted access)

ByPass (Does not handle the use of file system capabilities well enough)

Dos Overflow + Priv Mem Corr (Allows local users to gain unlimited privelages)

Dos Overflow Mem.Corr (This allows the hackers to perform Denial of Service attack)

These are just some of the 215 vulnerabilities present in the Linux Operating System.

Hardening of Linux OS

Although the Linux OS has much vulnerability present, they can be remedied through different procedures which include:

Encrypt the data communication occurring between the server and host machine with the use of scp or ssh software.

Reduce the number of software installed to reduce the vulnerability of Linux.

The Network Service per system should only be limited to one machine at a time to reduce any chances of attack.

The Linux kernel and software should be kept up to date.

Unwanted services should also be disabled in the Linux OS to prevent any unauthorized access.

An Intrusion Detection System should be installed to prevent any unwanted access into the Linux Servers.

Section 4

Lessons learnt from this project

This project was very helpful in clearing certain concepts related to the security testing of virtual machines and the steps associated with it. There are tons of different ways through which one can make the virtual machines and network safe from intruders and hackers. The main purpose of this study was to equip ourselves about the knowledge of both Operating Systems and the security risks associated with it (Hoagland, Conover, & Whitehouse, 2012).

We performed different scanning techniques in this project on both Windows and Linux operating system that gave us some details regarding the conditions of network on both of these operating systems. As both of these operating systems possess different kinds of coding, the threat type was different for them and hence it gave us knowledge about the conditions surrounding them.

By analyzing different security risks associated with both Operating Systems, we were also able to suggest some recommendations based upon the solution to these problems (Wu, Crawford, & Bowden, 2006). By exposing the vulnerabilities of both operating systems we were able to cover them up with the proposed solutions. Hence this made us understand the whole procedure more clearly.