"Detecting known host security flaws over a network connection"

A Thesis

submitted to the Department of Computer Science and Engineering

of

BRAC University

by

Syeda Tasnuva Ahsan (Student ID: 06110001)

&

Samina Rabiul Alam (Student ID: 06110028)

In Partial Fulfillment of the

Requirements for the Degree

of

Bachelor of Science in Electronics & Communication Engineering

August 11, 2009

DECLARATION

We hereby declare that this thesis is based on the results found by ourselves. Materials of work found by other researcher are mentioned by reference. This thesis, neither in whole nor in part, has been previously submitted for any degree.

Signature of Supervisor:

…………………….

(Sadia Hamid Kazi)

Signature of Author:

…………………………….

(Syeda Tasnuva Ahsan)

&

…………………………..

(Samina Rabiul Alam)

ACKNOWLEDGEMENTS

Special thanks to our thesis supervisor Ms. Sadia Hamid Kazi for giving us the opportunity to work on such an interesting topic and for supporting us throughout the whole thesis work. We would also like to thank BRAC University for providing us all necessary supports to complete our thesis.

ABSTRACT

To test if a host contains any known security flaws over a network connection a Vulnerability Assessment (VA) could be used. This thesis describes different techniques used by VA tools over a network connection to detect known security flaws. To decrease the risk of flaws not being detected, several VA tools could be used. In this paper firstly types of vulnerabilities are discussed and also the impacts of different vulnerabilities are pointed out. This paper mainly focuses on two different categories of VA tool, Port Scanner and Vulnerability Scanner. As an example of port scanner this paper discusses about Nmap port scanner and as vulnerability scanner it discusses about Nessus. Both these tools are open source VA tools. This paper contains the scan reports using these tools over a range of IP addresses. The analysis part of this paper gives an idea about how these tools scan for security flaws and suggest solutions to make a host or network out of risk.

TABLE OF CONTENTS

ATTACHMENTS

1. **Nmap Scan Report (Important Data Copied from Excel Report)**
2. **Nessus Scan Report (Important Data Copied from Excel Report)**

LIST OF CHARTS

LIST OF GRAPHS

THESIS OVERVIEW

The purpose of this thesis is to identify known security flaws over a network using some vulnerability assessment tools. These VA tools are used for vulnerability assessment to detect the known security flaws within the host and the network. This information got by examining a particular host tells what security flaws the host might contain. There is also a need to manage those collected information. Here more than one tools are to be studied and used to work within a network for detecting its security flaws. There might be a problem handling large quantities of information. So the purpose is to derive a better method for handling the information collected.

THESIS OBJECTIVE

Since we are to find a method of detecting security flaws within a network, knowledge about security flaws that may occur in it is very necessary. So the prime objective during building this method will be like as written as below:

1. Study of various types of network security flaws
2. Testing and analyzing of different vulnerability assessment tools

NETWORK SECURITY FLAWS & THEIR IMPACTS

A flaw in a system security that can lead to an attacker utilizing the system in a manner other than that which the designer intended. This can include impacting the availability of the system, elevating access privileges to an unintended level, complete control of the system by an unauthorized party an many other possibilities.

This definition stated above is taken from the context of computer software vulnerabilities, which is the vulnerability area of this thesis.

Types of Vulnerabilities:

- **Access control error** – It is an error due to lack of enforcement pertaining to users or functions that are permitted or denied access to an object or resource.

- **Authentication error** - It is an error due to inadequate identification mechanisms, such that an user or a process are not correctly identified.

- **Boundary error** - It is an error due to inadequate checking/validating mechanisms, such that the length of the data is not checked/validated against the size of the data storage or resource.

- **Configuration error** - It is an error due to improper configuration of system parameters or leaving the default configuration settings as it is.

- **Exception handling error** -It is an error due to improper setup or coding such that the system fails to handle or properly respond to exceptional or unexpected data or conditions.

- **Input validation error** - It is an error due to lack of verification mechanisms to validate the input data or contents.

- **Randomization error** - It is an error due to mismatch in random data results in insufficient random data for the process.

- **Resource error** - It is an error due to lack of resources available for correct operations or processes.

Impacts of Vulnerabilities:

- **Denial of service**-Denial-of-service is a situation wherein legitimate users of a service are prevented from using that service.

- **Remote code execution**- Remote code execution is an impact due to exploitation of vulnerability, thereby results in execution of arbitrary code remotely using a system process or software.

- **Privilege escalation**- Privilege elevation is an impact due to vulnerability in a system such that an unauthorized or less privileged process or person obtains higher privileges.

- **Unauthorized User access**- actions that have been attempted by users who have been assigned access roles that do not grant them permission to view or modify enterprise resources or configurations.

- **Disclosure of user information**- The security issue caused due to certain user information data being stored in the registry and the local file system with insecure permissions. This can be exploited to disclose local user information (e.g. administrative passwords).

VULNERABILITY ASSESSMENT TOOL

Vulnerability assessment tool examines a particular aspect of systems such as the operating system but ignores the other system components such as the routers. The primary advantage of it is that it provides a flexible, modular, extensible approach to vulnerability assessment. VA tools have developed foundation technologies that can be applied to three distinct applicable domains: security risk assessment, security modeling and security applications.

There are certain categories of Vulnerability Assessment Tool:

0. Port Scanner
0. Vulnerability Scanner

NMAP

The importance of firewalls is well known and well documented. While this is a good first step to improving system security, it is not the only step. Another necessity in keeping network system secure is regular maintenance of the system. One very good tool which would be helpful to perform auditing on the system is Nmap

Nmap -Network Mapper is a port scanner which is a open source tool for network exploration and security auditing. It can be used to evaluate any particular host or networks security and help to tighten security.

A problem many people have—especially those new to Linux—is that they don't understand that many daemons run on a typical Linux system or they may understand that there are a number of daemons running but may not know what each does or how to turn it off—or hide it from the outside world—if necessary. This is where Nmap comes in handy.

Use of Nmap:

Running *nmap* on a target helps to determine changes in the status of listening services on the system.

It helps to find out whether an unauthorized program is running on the computer, which may be something the administrator forgot to turn off or protect or which could be the result of someone having broken into the system and setting up their own daemon to allow himself access.

It was designed to rapidly scan large networks, although it works fine against single hosts.

It determines 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.

Working with Nmap :

Before coming into how nmap works an idea of port scanner is very much needed.

PORT SCANNER

A port scanner is a tool used by both system administrators and attacker(s) to identify vulnerabilities in operating systems. Port scanners identify vulnerabilities by sending normal and abnormal packets to computer ports and waiting for a response to determine what port(s) are 'open'. From this data, a system administrator, or an attacker, can determine what holes need to be patched or what holes can be exploited.

By setting different TCP flags or sending different types of TCP packets the port scan can generate different results or locate open ports in different ways.

A SYN scan will tell the port scanner which ports are listening and which are not depending on the type of response generated.

A FIN scan will generate a response from closed ports- but ports that are open and listening will not send a response, so the port scanner will be able to determine which ports are open and which are not.

How Nmap Works:

Nmap being the portscanner uses raw IP packets in novel ways to find the open ports on target system, and with that information, appropriate firewall rules can be written to make those ports unavailable to the outside world.

Commands for Nmap:

There are certain commands that nmap uses to perform its scan against the target. Depending on that command or switches nmap performs a particular scan and detects the state and condition of the target. will be used (each of the selected switches will be described in detail later):

-sS This switch performs a SYN scan

-sX This switch performs a XMAS scan

-sF This switch performs a FIN scan

-O This switch performs operating system detection

there are many other commands to audit the network specifically. All these switches or commands are processed by sending different TCP packets and flags. Before going into the analysis of report we needed to know how these packets work.

How TCP responds to specific packets:

These responses are based on two TCP states. These states are CLOSED and LISTEN. When a port is in the closed state, the following rules apply:

-Any incoming segment containing a RST is discarded.

-Any incoming segment NOT containing a RST (i.e. SYN, FIN, and ACK) will cause a RST to be sent in response.

For a port in the LISTEN state, the following rules apply:

-Any incoming segment containing a RST will be ignored (dropped), and

-Any incoming segment containing an ACK will cause a RST to be sent in response.

If the SYN bit is set:

-If the incoming segment is not allowed then a RST is sent in response.

-If the incoming segment is allowed then a SYN|ACK is sent in response (part 2 of the three-way handshake).

Additional study:

Nmap sometimes sends FIN, PSH and URG all set at the same time to perform a particular scan. What each flag does:

- FIN : "The sending machine is finished sending data."[1] *I'm through!*
- PSH : "Set when the receiver should pass this data to the applications as soon as possible."[2] *Hurry up and with this data!*
- URG: "The urgent pointer is valid."[3] "Allows one end to tell the other end that "urgent data" of some form has been place in the normal stream of data."[4] *Speaks for itself.*

In short what the FIN, PSH, URG combination tells the computer is to begin tearing down the connection, pass the data ASAP and then there is "urgent" data to be passed on the normal stream of data.

NESSUS

Nessus is the world's most popular vulnerability scanner estimated to be used by over 75,000 organizations worldwide. It is a freely available, open-source vulnerability scanner. The power and performance of Nessus, combined with the price- FREE- make it a compelling choice for a vulnerability scanner. In computer security Nessus is proprietary comprehensive vulnerability scanning software. It is free of charge for personal use in a non-enterprise environment.

Before coming into how Nessus works an idea of vulnerability scanner is very much needed.

Vulnerability Scanner:

A vulnerability scanner is a computer program designed to search for and map systems for weaknesses in an application, computer or network. Typically the scanner will first look for active IP addresses, open ports, OSes and any applications running. Secondly, It may at this point create a report or move to the next step. Thirdly, it tries to determine the patch level of the OS or applications. In this process the scanner can cause an exploit of the vulnerability such as crash the OS or application. At the final phase the scanner may attempt to exploit the vulnerability. Scanners may either be malicious or friendly. Friendly scanners usually stop at step 2 and occasionally step 3 but never go to step 4. Vulnerability Scanners can be used to conduct network reconnaissance, which is typically carried out by a remote attacker attempting to gain information or access to a network on which he is not authorized or allowed. Network reconnaissance is increasingly being used to exploit various network standards and automated communication methods in order to determine what types of computers are present, along with additional information about those computers, such as the type and version of its operating system.

How Nessus works:

Nessus makes no assumptions regarding what services are running on what ports and it actively attempts to exploit vulnerabilities rather than just comparing version numbers of the active services.

Goal of using Nessus:

Its goal is to detect potential vulnerabilities on the tested systems. For example:

0. Vulnerabilities that allow a remote cracker to control or access sensitive data on a system.
0. Misconfiguration (e.g. missing patches, etc).
0. Default password, a few common passwords and blank/absent passwords on some system accounts.
0. Denial of service against the TCP/IP stack by using mangled packets.

Some of Nessus's vulnerability tests may try to cause vulnerable services or operating systems to crash. This lets a user test the resistance of a device before putting it in production.

Requirements for running Nessus:

- The Nessus Server component requires a POSIX system such as FreeBSD, GNU/Linux, NetBSD or Solaris.

- The Nessus Client component is available for all Linux / Unix systems. There is also a Win32 GUI client that works with any version of Microsoft Windows.

Features of Nessus

The Nessus vulnerability database is updated daily.

Because of the modularity of Nessus it is also possible to create unique plugins to test against. This can be done by a special feature of Nessus named as NASL- scripting language for nessus.

Nessus is also smart enough to test services running on non-standard ports, or to test multiple instances of a service (for instance if you are running an HTTP server on both port 80 and port 8080).

Basic Components of Nessus:

The unique architecture, on which Nessus is built, makes it such an wonderful tool. The flexibility and resourcefulness of the Nessus architecture has taken every element of the security life cycle into consideration. From the large scale batch execution of vulnerability scans that capture the data, to the graphical and hyperlinked reports that represent the data, to fix description that are invaluable in patch remediation, all of these aspects create the foundation of a healthy security posture. The architecture of Nessus includes:

- The Nessus Server & Client
- The Nessus Plug-ins
- The Nessus Knowledge Base

The Nessus Security Scanner is structured as client-server architecture. The Nessus client configures the various target, scanning, and plug-in options, and it reports the findings from the scan to the user. The Nessus server performs all of the scanning and security checks, which are implemented as plug-ins written in *Nessus Attack Scripting Language* (NASL). All communication between the client and the server pass over a *Transport Layer Security* (TLS) encrypted connection. The Nessus knowledge base is quite simply the list of information gathered about a host being tested. It allows plug-ins or tests, to share information about the target system allowing for both, more intelligent testing and more conservative use of bandwidth and processing power.

Operation of Nessus:

In typical operation, Nessus divides its work into two steps:

1- Does a port scan with one of its four internal portscanners to determine which ports are open on the target and then tries various exploits on the open ports.

2- Does the vulnerability tests, available as subscriptions, are written in **NASL** (Nessus Attack Scripting Language), a scripting language optimized for custom network interaction.

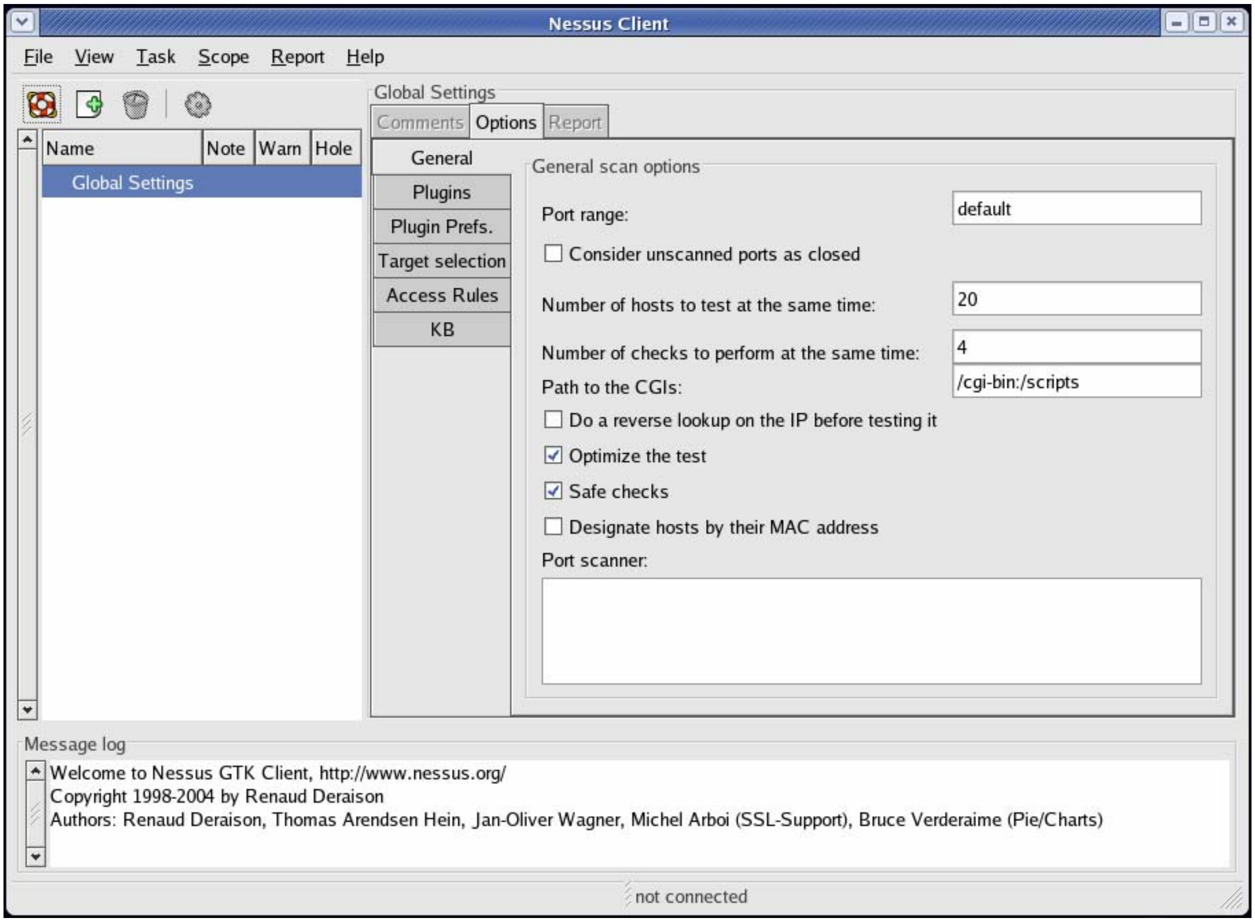
Different Modes of Operation:

At a high level, Nessus can be run in two different modes: with or without authentication credentials. When run without credentials, Nessus will perform remote network-based security checks, testing how the target host responds to specific network probes. When run with credentials, Nessus will additionally log into the remote host and perform a number of local security checks, such as ensuring that the latest security patches have been installed.

Employment of Nessus:

Nessus gives a lot of options when it comes to running the actual vulnerability scan. One can scan individual computers, ranges of IP addresses or complete subnets. It can be used for testing against the entire collection of over 1200 vulnerability plugins, or specifying an individual or set of specific vulnerabilities to test for. Unlike some other open source and commercially available vulnerability scanners, Nessus does not assume that common services will be running on common ports. If you run an HTTP service on port 8000 it will still find vulnerabilities rather than assuming that it should find HTTP on port 80. It also does not simply check the version number of the services running and assume the system is vulnerable. Nessus actively attempts to exploit the vulnerabilities.

Some screen shots are presented to give an overview of how Nessus scan is performed.



Port range: default

□ Consider unscanned ports as closed

Number of hosts to test at the same time: 20

Number of checks to perform at the same time: 4

Path to the CGIs: /cgi-bin:/scripts

□ Do a reverse lookup on the IP before testing it

☑ Optimize the test

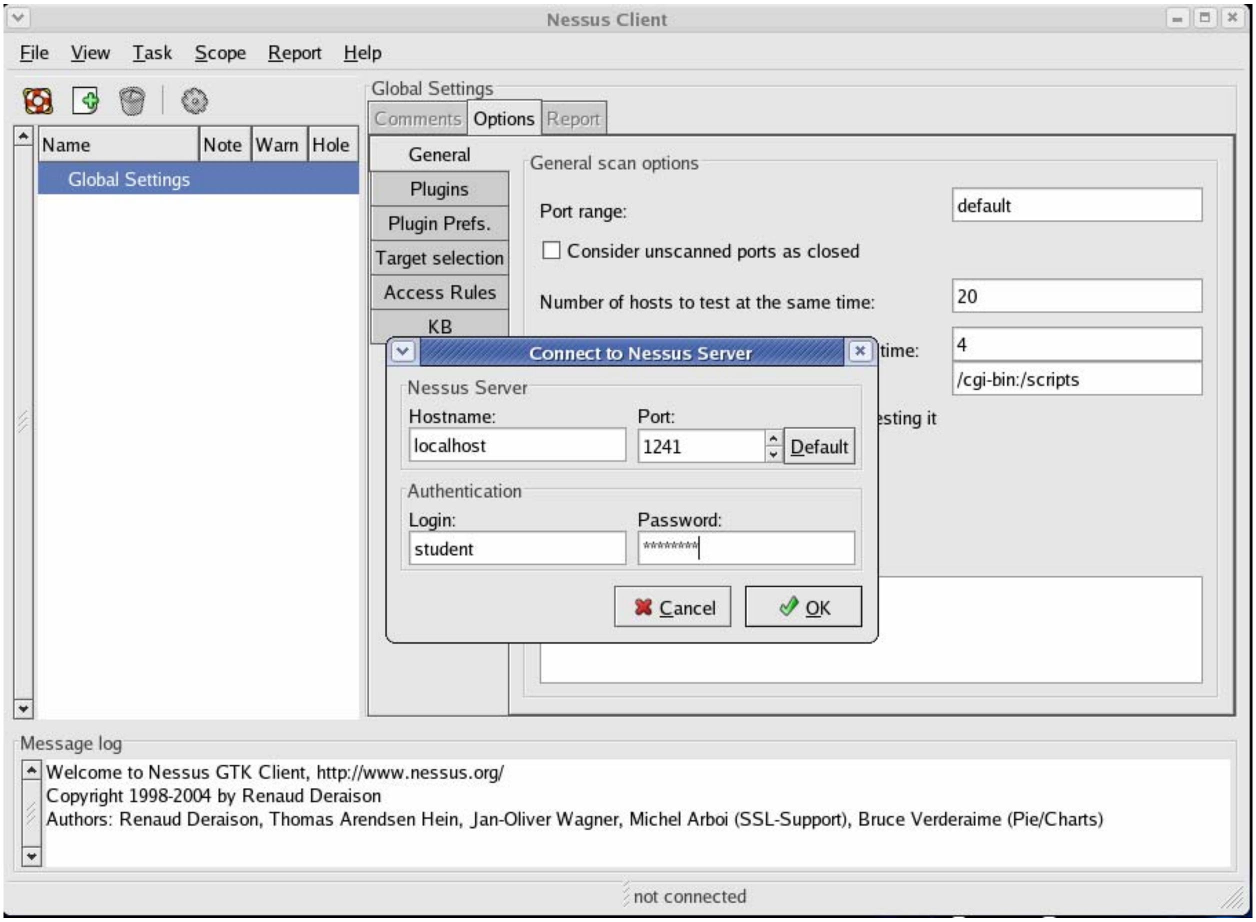
☑ Safe checks

□ Designate hosts by their MAC address

Port scanner:

```
Welcome to Nessus GTK Client, http://www.nessus.org/
Copyright 1998-2004 by Renaud Deraison
Authors: Renaud Deraison, Thomas Arendsen Hein, Jan-Oliver Wagner, Michel Arboi (SSL-Support), Bruce Verderaime (Pie/Charts)
```

Figure 1: Nessus Client



Global Settings

General scan options

Port range: default

□ Consider unscanned ports as closed

Number of hosts to test at the same time: 20

time: 4

/cgi-bin:/scripts

sting it

Nessus Server

Hostname: localhost

Port: 1241

Authentication

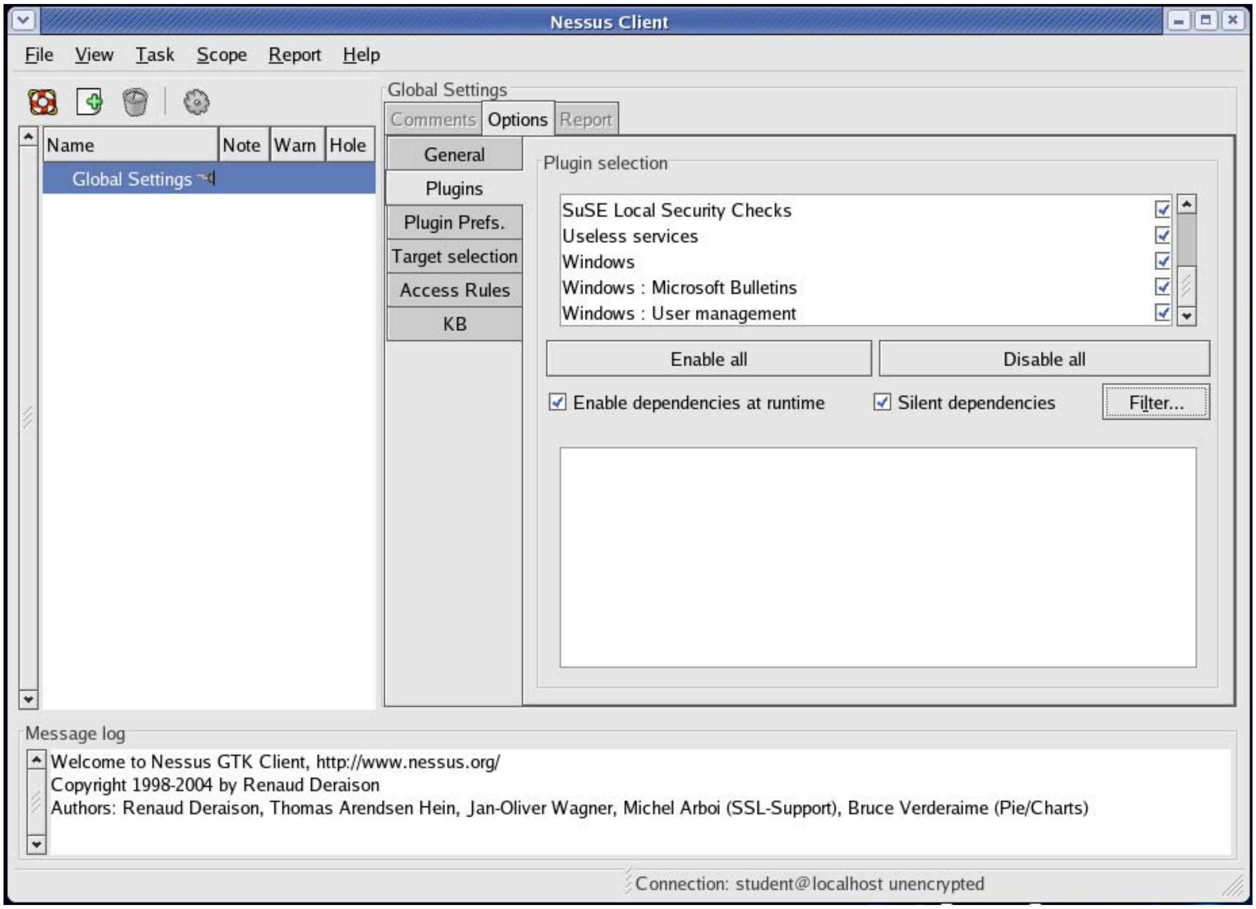
Login: student

Password: ********

```
Welcome to Nessus GTK Client, http://www.nessus.org/
Copyright 1998-2004 by Renaud Deraison
Authors: Renaud Deraison, Thomas Arendsen Hein, Jan-Oliver Wagner, Michel Arboi (SSL-Support), Bruce Verderaime (Pie/Charts)
```

not connected

Figure 2: Logging into the server



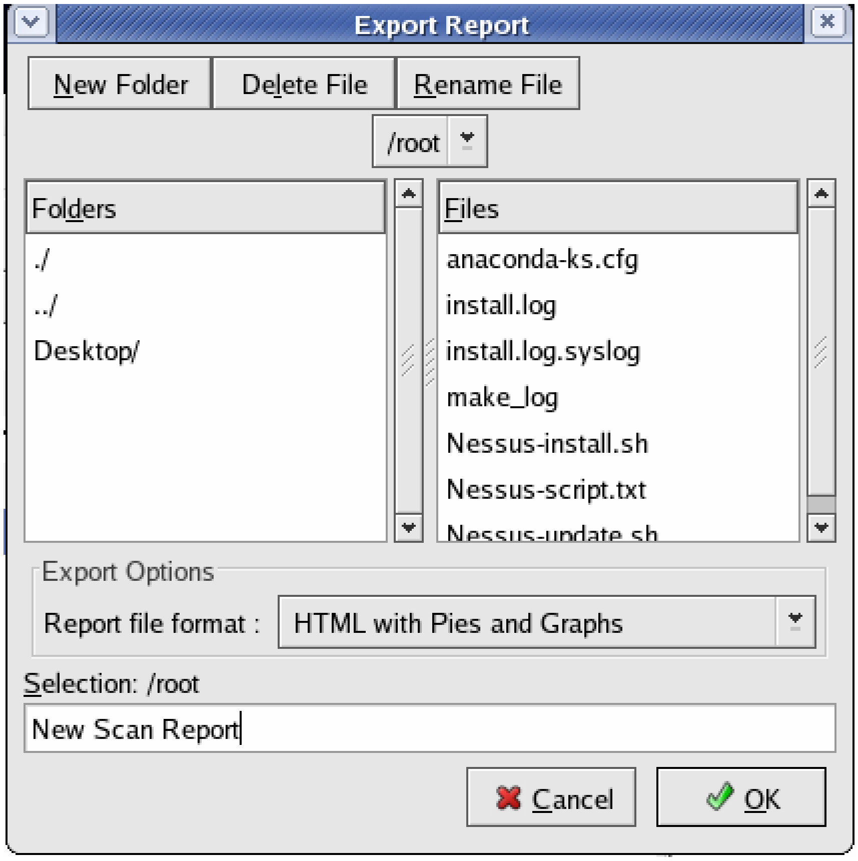
SuSE Local Security Checks	☑
Useless services	☑
Windows	☑
Windows : Microsoft Bulletins	☑
Windows : User management	☑

☑ Enable dependencies at runtime ☑ Silent dependencies

```
Welcome to Nessus GTK Client, http://www.nessus.org/
Copyright 1998-2004 by Renaud Deraison
Authors: Renaud Deraison, Thomas Arendsen Hein, Jan-Oliver Wagner, Michel Arboi (SSL-Support), Bruce Verderaime (Pie/Charts)
```

Connection: student@localhost unencrypted

Figure 3: Client Plug-ins Tab



/root

Folders:
./
../
Desktop/

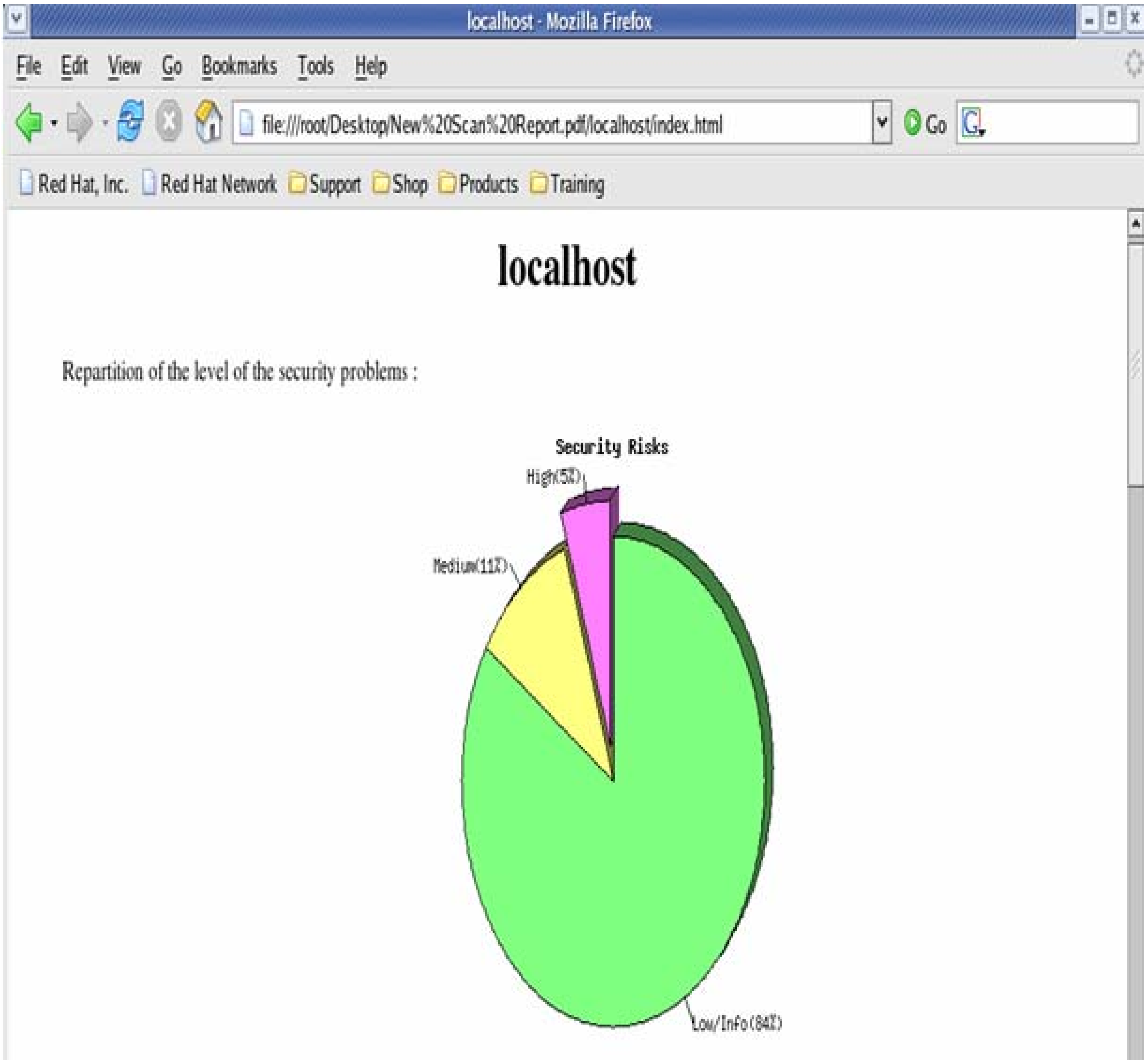
Files:
anaconda-ks.cfg
install.log
install.log.syslog
make_log
Nessus-install.sh
Nessus-script.txt
Nessus-update.sh

Report file format : HTML with Pies and Graphs

Selection: /root

New Scan Report

Figure 4: Saving Scan Report



localhost

Repartition of the level of the security problems :

Figure 5: Interpreting Nessus Report

ANALYSIS

In this thesis work, a range of IP addresses was scanned. Both the tools, Nmap and Nessus have shown scan reports for the range of 192.168.1.1-32 IP addresses. These range of IP addresses belong to BRAC University network. The whole scanning process we run on Linux (Ubuntu).

ANALYSIS OF NMAP REPORT

In this report we have analyzed how the packets communicate with the server, for different command executed on batch.

BATCH REPORT

nmap does not show a standard output automatically. Firstly we got it from the batch and then using commands stated later got a standard output tha is XML output.

SCAN OPTION:

SCAN-1:

#batch command:

```
root@ThreeOS:~# nmap -sS 192.168.1.7
```

```
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-09 11:19 BDST

Interesting ports on student.bracu.ac.bd (192.168.1.7):
Not shown: 982 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
106/tcp   open  pop3pw
110/tcp   open  pop3
111/tcp   open  rpcbind
143/tcp   open  imap
```

```
443/tcp   open  https
587/tcp   open  submission
631/tcp   open  ipp
993/tcp   open  imaps
995/tcp   open  pop3s
2049/tcp  open  nfs
3306/tcp  open  mysql
32768/tcp open  unknown
32770/tcp open  sometimes-rpc3
MAC Address: 00:11:3B:0E:C4:4D (Micronet Communications)
Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds


# used option: '-sS'

#Scan type:  SYN scan
```

#discussion:

The -sS switch sends a SYN(s) to a port(s) and waits for a response. The response should be either a SYN | ACK if the port is open or a RST | ACK if the port is closed. This scan is considered a "half-scan", the theory behind a "half -scan" is NMAP will send SYN's to a computer, if the port(s) are closed then a rest is sent back notifying NMAP that the port is closed. If NMAP sends a SYN to an open port, that port will respond with a SYN | ACK. Once NMAP detects the SYN | ACK it automatically replies back with a RST. This RST will break the connection and in some cases, a computer will not log this attempt. This also lets NMAP know what ports are open and what ports are closed.

#analysis:

NMAP sends out one- (1) echo requests (highlighted in red). This is done to ensure the victim is up and running.

The second signature in this scan is the lone ACK packet. From the previous discussion we can conclude that the two ACK packets are sent to verify that the computer to be scanned is up and running.

The ports respond with a SYN-ACK. Thus Nmap knows they are in open state.

After that nmap sends a RST to break the connection.

SCAN-2:

#batch command:

```
root@ThreeOS:~# nmap -sX localhost
```

```
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-06 16:55 BDST

Interesting ports on localhost (127.0.0.1):
```

```
Not shown: 997 closed ports

PORT     STATE         SERVICE

80/tcp   open|filtered http
631/tcp  open|filtered ipp
3306/tcp open|filtered mysql

Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds
```

#used option: '-sX'

#scan type: xmas scan

#port status: open filtered

#Discussion:

Because of the odd TCP flags (FIN, PSH and URG) set by this scan, some firewalls (poorly configured) will allow these packets to pass through.

#analysis:

NMAP sends out two echo request and ACK packets to ensure that the target is in fact up and running. The odd TCP flags that is FIN, PSH and URG is set by this scan.

SCAN-3:

#batch command:

```
root@ThreeOS:~# nmap -sF -O localhost


Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-06 17:28 BDST

Interesting ports on localhost (127.0.0.1):

Not shown: 997 closed ports


PORT     STATE         SERVICE


80/tcp   open|filtered http

631/tcp  open|filtered ipp

3306/tcp open|filtered mysql


Too many fingerprints match this host to give specific OS details

Network Distance: 0 hops

OS detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
```

#used option: '-sF'

#scan type: FIN scan

#port state: unable to determine whether the ports are open or filtered.

#discussion:

nmap sets a flag FIN while doing the scan.If the port(s) are in closed and a FIN is sent a reset is sent in response. In this case, if a FIN is sent and the port(s) are open then TCP drops the FIN and does not send back any replies.

#analysis:The -sF scans computers with the FIN bit set. It seems that open ports gave no response. The lack of response could mean that a packet filter dropped the probe or any response it elicited. So Nmap does not know for sure whether the port is open or being filtered.

SCAN-4

#batch command:

```
root@ThreeOS:~# nmap -O localhost


Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-06 17:29 BDST

Interesting ports on localhost (127.0.0.1):

Not shown: 997 closed ports


PORT     STATE SERVICE


80/tcp   open  http

631/tcp  open  ipp

3306/tcp open  mysql
```

```
Device type: general purpose

Running: Linux 2.6.X

OS details: Linux 2.6.17 - 2.6.28

Network Distance: 0 hops

OS detection performed. Please report any incorrect results at
http://nmap.org/submit/ .


Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds
```

#used option: '-O'

#scan type: the switch does Operating System fingerprinting.

#port state: open

#discussion:NMAP's -O function identifies a probbable Operating System to the user.

# analysis: here the OS being used is Linux 2.6.17

Nmap OUTPUT:

COMMAND:

1. nmap -oX myscan.xml target……………………………………………….….….(6)

 prints XML to myscan.xml and fills standard output from the batch.

After this the XML file was imported to EXCEL for better observation.

This excel report represents port ID and status for different IP addresses, the reasons for the ports being open and closed, which applications are running on which particular port and also the Smooth Round Trip Time (SRTT) and Round Trip Time Variation(RTTVar) for packets.

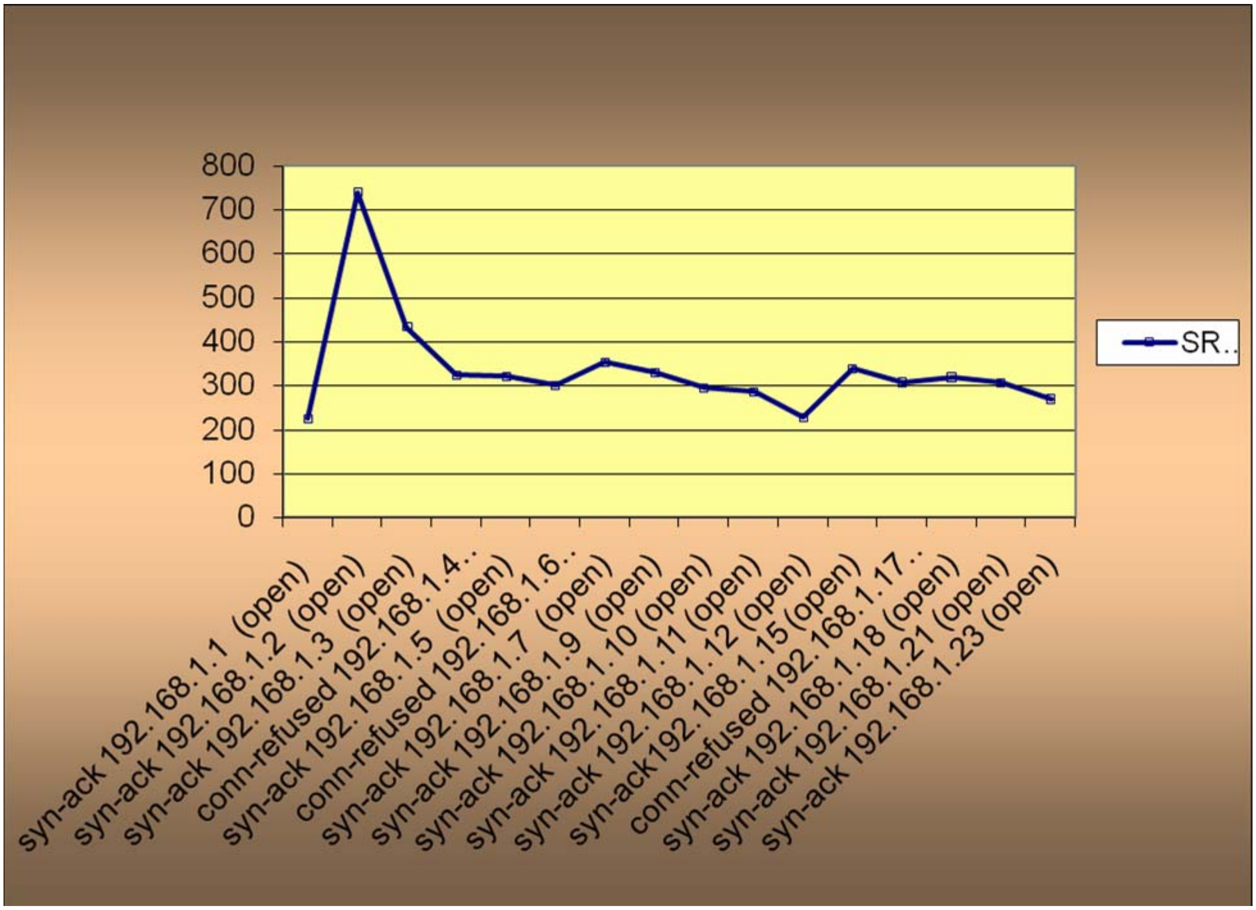
Observation:

Here observing the excel report we get the idea of port status of range of host. We can see the ports being open or closed and if open what protocols are running. Now assessing the situation we need to find out the flaws over the network. As for example here we can see the open ports with http running has a lower risk factor also having the FTP and SSH ports open is normal. The SMTP port should be accessible only by the localhost, so we should restrict access to port 25 from the outside world, as well as the netbios ports, mysql etc. All of those ports should be available only to the localhost, because no one outside of the system has any reason to be connecting to the local server or to your MySQL server.

Nmap GRAPH:

Vulnerability of a particular host can be determined observing the SRTT and RTTVar status using graphs. These graphs are described now.

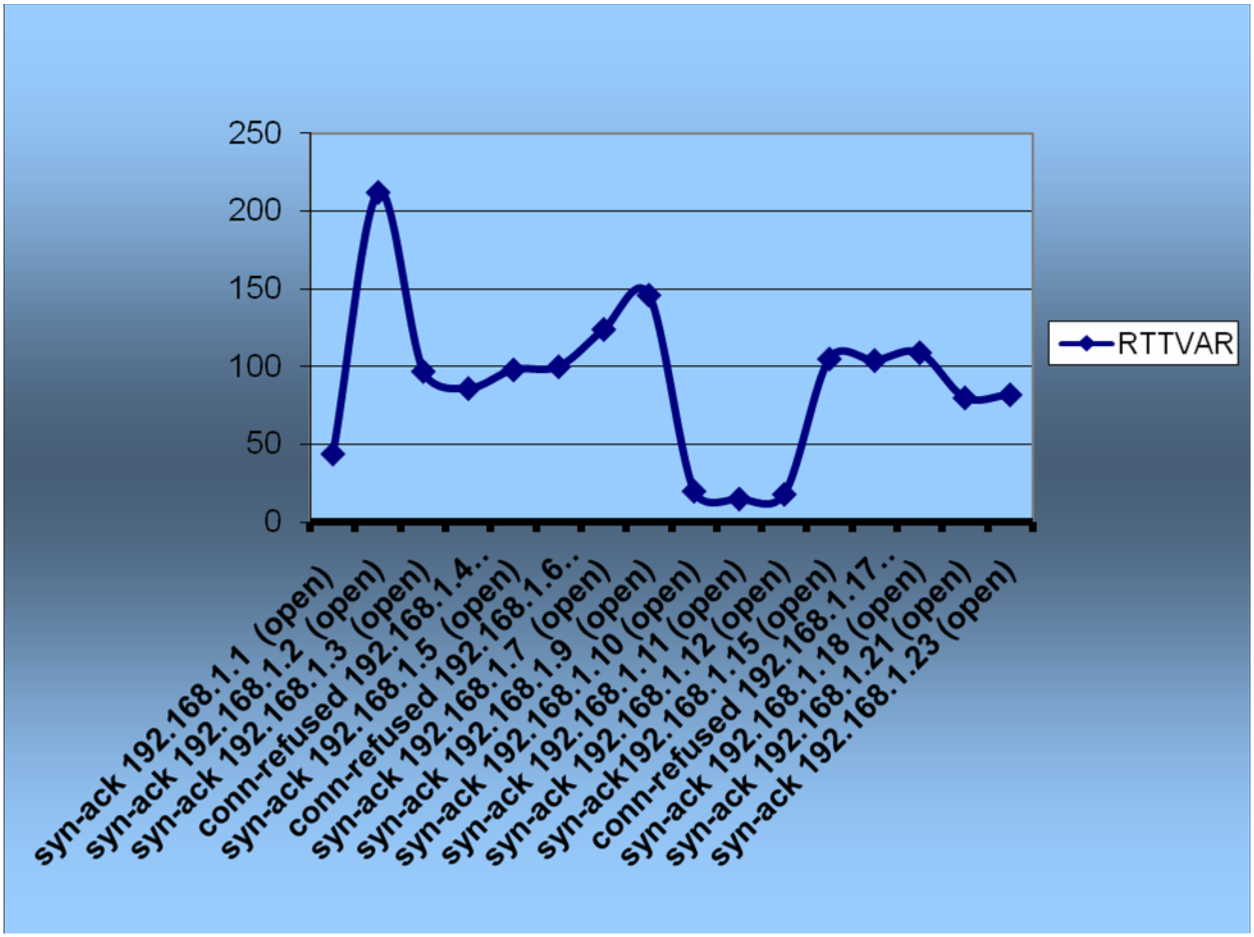
Graph 1: IP Address & Port Status vs SRTT



In this graph in the X axis we have the IP address along with the port status, the scan types are also seen. In the Y axis we have the SRTT (7) (smoothed round trip time) values. The generated graph gives us an idea of the network .

In this graph we see the SRTT for all the hosts have similar values except one.- 192.168.1.2. So we can assume that the host has a delayed response. The delay could be because of congestion within the network or because of an intruder who can cause a TCP sender to compute a large value of RTO (7) by adding delay to a timed packet's latency, or that of its acknowledgment. So this makes the process slower.

Graph 2: IP Address & Port Status vs RTTVar



This graph is based on host Vs RTTvar (round trip time variation). (7) Here we see too odd values for two hosts. For 192.168.1.2 we have a higher value which makes us understand that either there would be a congestion or an intruder trying to delay the process.

For 192.168.1.10-15 they responded very quickly. The reason might be an intruder could cause TCP endpoints to respond more aggressively in the face of congestion by forging acknowledgments for segments before the receiver has actually received the data, thus lowering RTO to an unsafe value. This indicates some packets may be lost while sending to this reciever.

NESSUS SCAN REPORT ANALYSIS

After performing Nessus scan, we got scan report in a .nbe file, which was converted to an .xml file.

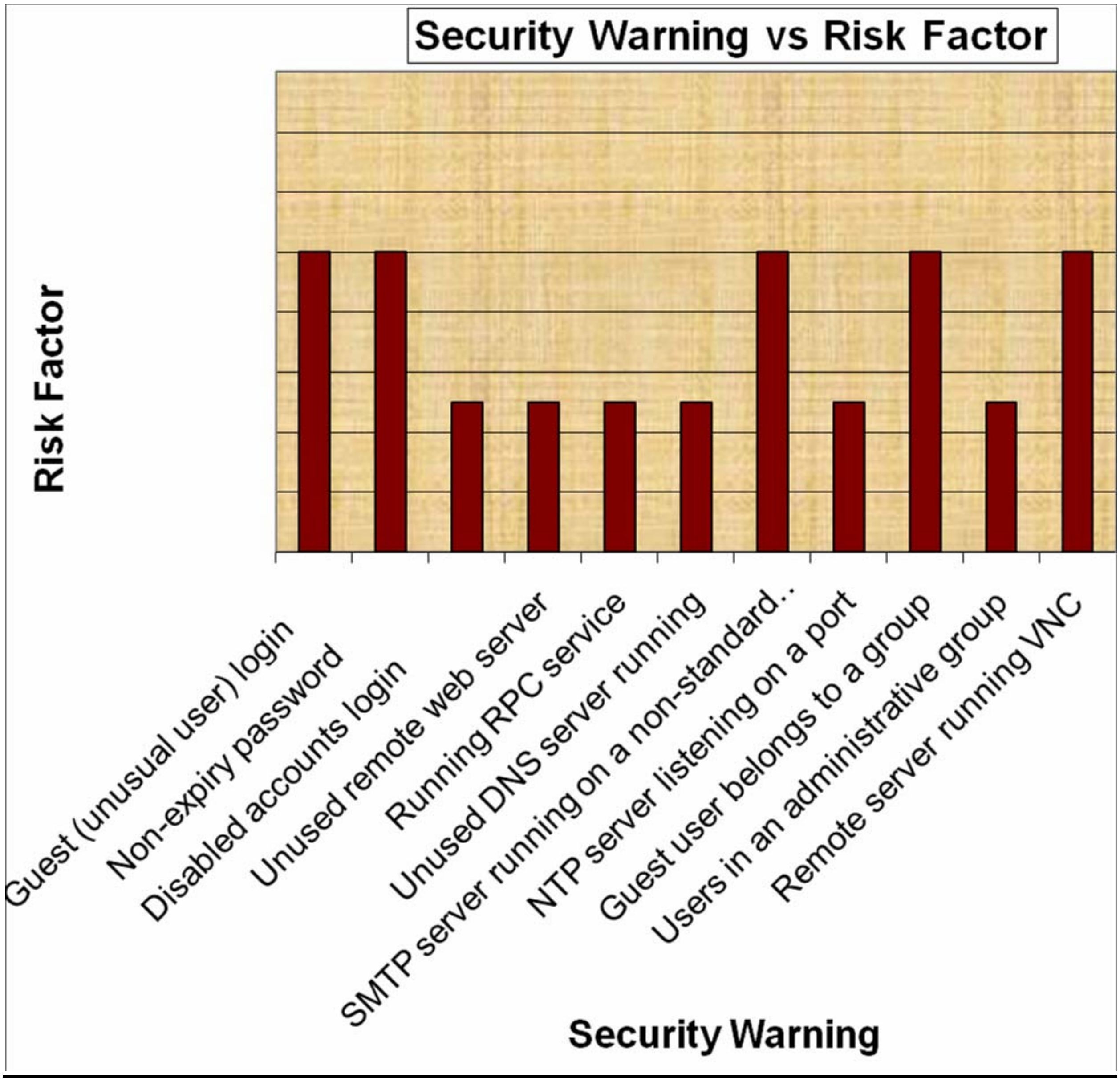
Command for converting nbe to XML file :

```
$ nessus -i in.nbe  -o out.xml
```

Then the xml format was imported to Excel.

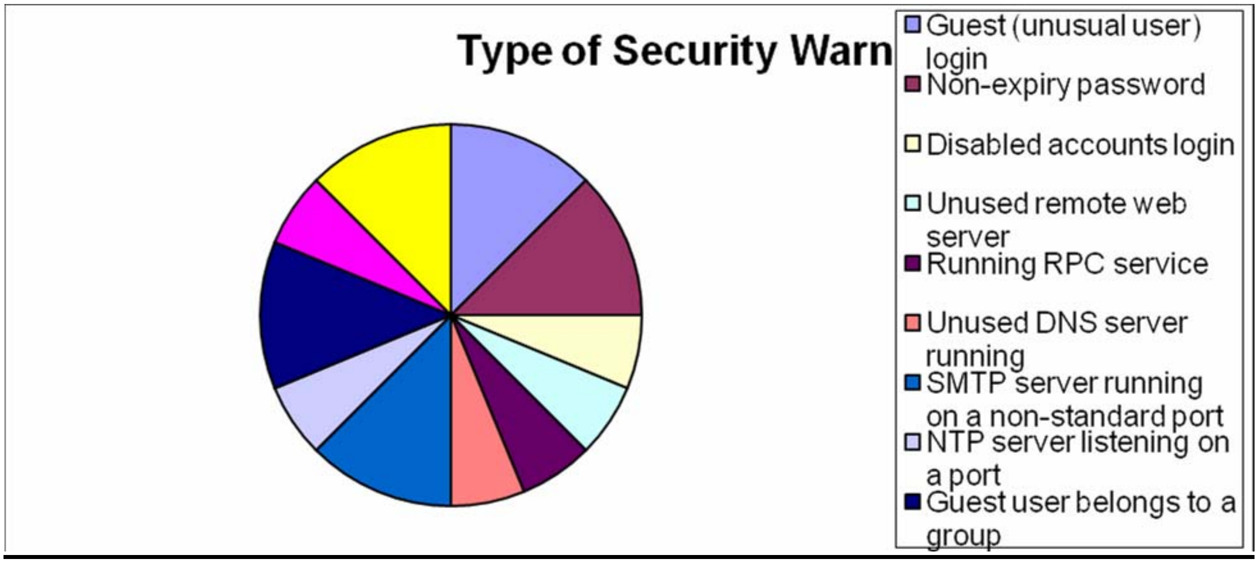
The excel report represents port ID for different IP addresses, which protocols and which applications are running on different ports, the security note, security warning and their solutions and also the risk factor for each security risk. Below a chart and two graphs are shown to analyze the Nessus scan report. The chart shows the security warnings and their solutions. One of the graphs shows the status of risk factor for each security warning. And the other graph is a pie chart which shows the percentage of risk factors.

Graph 3: Security Warning vs Risk Factor

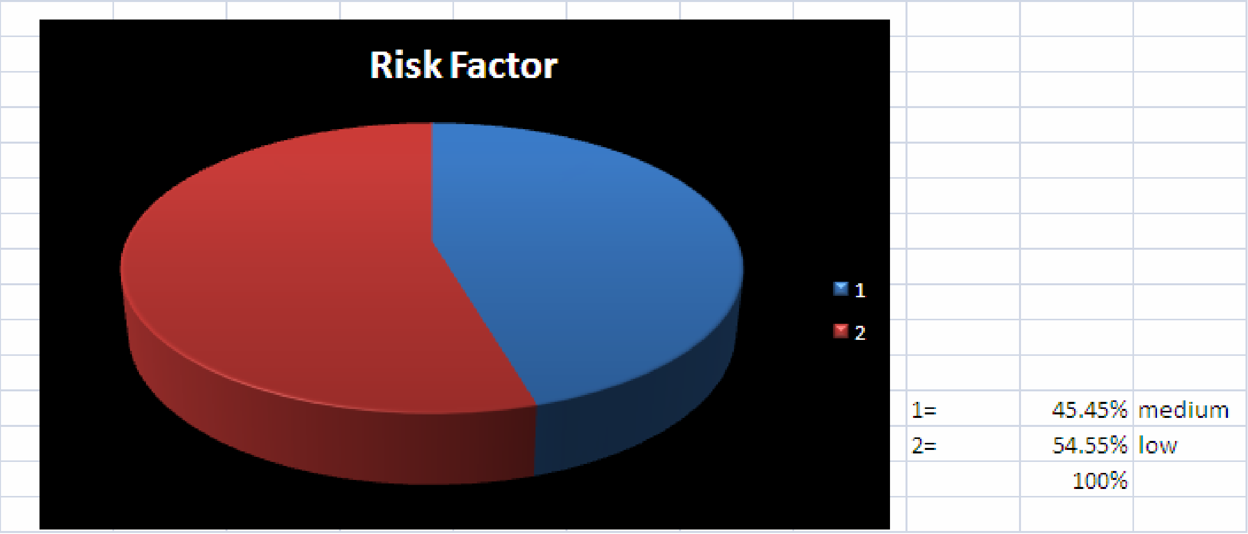


This graph shows what level of risk factor is there for a certain security warning. In the X-axis the security warnings are shown and in the Y-axis the level of risk factor is shown. From the range of IP Addresses scanned for this thesis work, we get medium and low level of risk factor for certain security warning. There is no such security warning found which has high risk factor.

Graph 4: Type of Security Warning



Graph 5: Percentage of Risk Factor over the Range of IP Address



1=	45.45%	medium
2=	54.55%	low
	100%	

This graph shows the percentage of risk factor over the range of IP addresses scanned. Here 45.45% of IP addresses has medium risk factor and 54.55% of IP Addresses has low risk factor.

Chart 1 : Nessus Scan report Analysis

Type of security warning	Risk factor	Solution
Guest (unusual user) login	Medium	Suppress unusual user accounts
Non-expiry password	Medium	Allow password with limited life time, disable password non-expiry
Disabled accounts login	Low	Permanently delete disabled accounts
Unused remote web server	Low	Disable the service
Running RPC service	Low	Disable the service
Unused DNS server running	Low	Disable the service
SMTP server running on a non-standard port	Medium	Check and clean the configuration
NTP server listening on a port	Low	Make sure security check
Guest user belongs to a group other than guest users or domain guests	Medium	Disable guest user’s membership from group
Users in an administrative group	Low	Make sure only proper users belong to this group
Remote server running VNC	Medium	Disable VNC access from the network using a firewall or top the service if not needed

CONCLUSION

This thesis work included analysis of two very popular network flaws detecting tools. Two of them come from a different criteria of vulnerability detecting tool. So its not possible to be judgemental about their effectiveness one upon another. Nmap which comes under the criteria of port scanner gives the state of ports of the target which not only helps to detect the flaws but also makes the work of an administrator easier by auditing the network. On the other hand, Nessus which is a vulnerability scanner also scans the port and in addition to it detects the flaws individually and gives a particular solution of it. A question may arise if nessus has a port scanner what is the function of nmap in assessing the vulnerabilities. The problem is nessus port scanner cannot be used seperately , it will run along with its vulnerability scans. So here nmap becomes very handy. But nessus can import scan reports done by another tool like nmap and do its vulnerability scan. Both the tools have one thing common that they makes the administrators work easier.

REFERENCE

0. 1. www.insecure.org

0. 2. www.sans.org

www.accessmylibrary.com

www.articles.techrepublic.com

0. 3. www.nessus.org

0. 4. http://books.google.com.bd/books

0. 5. www.tenablesecurity.com

www.openvas.org

0. 6. http://www.computersecuritylaw.us/2008/03/06/tutorial-on-how-to-generate-an-excel-compatible-nessus-report.aspx

0. 7. http://www.ietf.org/rfc/rfc2988.txt

ATTACHMENT 1: Nmap Scan Report

IP Address	Port ID	State	Reason	Application Running	SRTT	RTTVAR
192.168.1.1				http	255	44
192.168.1.1	80	open	syn-ack	msrpc	255	44
192.168.1.1	135	open	syn-ack	netbios-ssn	255	44
192.168.1.1	139	open	syn-ack	microsoft-ds	255	44
192.168.1.1	445	open	syn-ack	ms-term-serv	255	44
192.168.1.1	3389	open	syn-ack	vnc-http	255	44
192.168.1.1	5800	open	syn-ack	vnc	255	44
192.168.1.2	5900	open	syn-ack		740	212
192.168.1.2				echo	740	212
192.168.1.2	7	open	syn-ack	discard	740	212
192.168.1.2	9	open	syn-ack	daytime	740	212
192.168.1.2	13	open	syn-ack	qotd	740	212
192.168.1.2	17	open	syn-ack	chargen	740	212
192.168.1.2	19	open	syn-ack	smtp	740	212
192.168.1.2	25	open	syn-ack	nameserver	740	212
192.168.1.2	42	open	syn-ack	domain	740	212
192.168.1.2	53	open	syn-ack	http	740	212
192.168.1.2	80	open	syn-ack	kerberos-sec	740	212
192.168.1.2	88	open	syn-ack	msrpc	740	212
192.168.1.2	135	open	syn-ack	netbios-ssn	740	212
192.168.1.2	139	open	syn-ack	ldap	740	212
192.168.1.2	389	open	syn-ack	https	740	212
192.168.1.2	443	open	syn-ack	microsoft-ds	740	212

192.168.1.2	445	open	syn-ack	kpasswd5	740	212
192.168.1.2	464	open	syn-ack	printer	740	212
192.168.1.2	515	open	syn-ack	afp	740	212
192.168.1.2	548	open	syn-ack	http-rpc-epmap	740	212
192.168.1.2	593	open	syn-ack	ldapssl	740	212
192.168.1.2	636	open	syn-ack	LSA-or-nterm	740	212
192.168.1.2	1026	open	syn-ack	ms-lsa	740	212
192.168.1.2	1029	open	syn-ack	optima-vnet	740	212
192.168.1.2	1051	open	syn-ack	unknown	740	212
192.168.1.2	1064	open	syn-ack	unknown	740	212
192.168.1.2	1065	open	syn-ack	instl_boots	740	212
192.168.1.2	1067	open	syn-ack	instl_bootc	740	212
192.168.1.2	1068	open	syn-ack	unknown	740	212
192.168.1.2	1075	open	syn-ack	globalcatLDAP	740	212
192.168.1.2	3268	open	syn-ack	globalcatLDAPssl	740	212
192.168.1.2	3269	open	syn-ack	unknown	740	212
192.168.1.2	34571	open	syn-ack	unknown	740	212
192.168.1.3	34572	open	syn-ack		434	97
192.168.1.3				echo	434	97
192.168.1.3	7	open	syn-ack	discard	434	97
192.168.1.3	9	open	syn-ack	daytime	434	97
192.168.1.3	13	open	syn-ack	qotd	434	97
192.168.1.3	17	open	syn-ack	chargen	434	97
192.168.1.3	19	open	syn-ack	smtp	434	97

192.168.1.3	25	open	syn-ack	nameserver	434	97
192.168.1.3	42	open	syn-ack	domain	434	97
192.168.1.3	53	open	syn-ack	http	434	97
192.168.1.3	80	open	syn-ack	kerberos-sec	434	97
192.168.1.3	88	open	syn-ack	msrpc	434	97
192.168.1.3	135	open	syn-ack	netbios-ssn	434	97
192.168.1.3	139	open	syn-ack	ldap	434	97
192.168.1.3	389	open	syn-ack	https	434	97
192.168.1.3	443	open	syn-ack	microsoft-ds	434	97
192.168.1.3	445	open	syn-ack	kpasswd5	434	97
192.168.1.3	464	open	syn-ack	printer	434	97
192.168.1.3	515	open	syn-ack	afp	434	97
192.168.1.3	548	open	syn-ack	http-rpc-epmap	434	97
192.168.1.3	593	open	syn-ack	ldapssl	434	97
192.168.1.3	636	open	syn-ack	LSA-or-nterm	434	97
192.168.1.3	1026	open	syn-ack	ms-lsa	434	97
192.168.1.3	1029	open	syn-ack	unknown	434	97
192.168.1.3	1039	open	syn-ack	unknown	434	97
192.168.1.3	1042	open	syn-ack	unknown	434	97
192.168.1.3	1045	open	syn-ack	unknown	434	97
192.168.1.3	1054	open	syn-ack	unknown	434	97
192.168.1.3	1056	open	syn-ack	unknown	434	97
192.168.1.3	1057	open	syn-ack	nimreg	434	97
192.168.1.3	1059	open	syn-ack	unknown	434	97

192.168.1.3	1082	open	syn-ack	unknown	434	97
192.168.1.3	34571	open	syn-ack	unknown	434	97
192.168.1.4	34572	open	syn-ack		324	86
192.168.1.4				echo	324	86
192.168.1.4	7	open	syn-ack	discard	324	86
192.168.1.4	9	open	syn-ack	daytime	324	86
192.168.1.4	13	open	syn-ack	qotd	324	86
192.168.1.4	17	open	syn-ack	chargen	324	86
192.168.1.4	19	open	syn-ack	msrpc	324	86
192.168.1.4	135	open	syn-ack	netbios-ssn	324	86
192.168.1.4	139	open	syn-ack	microsoft-ds	324	86
192.168.1.4	445	open	syn-ack	printer	324	86
192.168.1.4	515	open	syn-ack	afp	324	86
192.168.1.4	548	open	syn-ack	unknown	324	86
192.168.1.4	1057	open	syn-ack	polestar	324	86
192.168.1.4	1060	open	syn-ack	unknown	324	86
192.168.1.5	1061	open	syn-ack		321	98
192.168.1.5				ssh	321	98
192.168.1.5	22	open	syn-ack	http	321	98
192.168.1.5	80	open	syn-ack	rpcbind	321	98
192.168.1.5	111	open	syn-ack	https	321	98
192.168.1.5	443	open	syn-ack	http-proxy	321	98
192.168.1.5	8080	open	syn-ack	https-alt	321	98
192.168.1.6	8443	open	syn-ack		301	100

192.168.1.6				ssh	301	100
192.168.1.6	22	open	syn-ack	rpcbind	301	100
192.168.1.7	111	open	syn-ack		353	124
192.168.1.7				ftp	353	124
192.168.1.7	21	open	syn-ack	ssh	353	124
192.168.1.7	22	open	syn-ack	smtp	353	124
192.168.1.7	25	open	syn-ack	domain	353	124
192.168.1.7	53	open	syn-ack	http	353	124
192.168.1.7	80	open	syn-ack	pop3pw	353	124
192.168.1.7	106	open	syn-ack	pop3	353	124
192.168.1.7	110	open	syn-ack	rpcbind	353	124
192.168.1.7	111	open	syn-ack	imap	353	124
192.168.1.7	143	open	syn-ack	https	353	124
192.168.1.7	443	open	syn-ack	submission	353	124
192.168.1.7	587	open	syn-ack	ipp	353	124
192.168.1.7	631	open	syn-ack	imaps	353	124
192.168.1.7	993	open	syn-ack	pop3s	353	124
192.168.1.7	995	open	syn-ack	nfs	353	124
192.168.1.7	2049	open	syn-ack	mysql	353	124
192.168.1.7	3306	open	syn-ack	unknown	353	124
192.168.1.7	32768	open	syn-ack	sometimes-rpc3	353	124
192.168.1.9	32770	open	syn-ack		330	146
192.168.1.9				smtp	330	146
192.168.1.9	25	open	syn-ack	http	330	146

192.168.1.9	80	open	syn-ack	msrpc	330	146
192.168.1.9	135	open	syn-ack	netbios-ssn	330	146
192.168.1.9	139	open	syn-ack	https	330	146
192.168.1.9	443	open	syn-ack	microsoft-ds	330	146
192.168.1.9	445	open	syn-ack	netsaint	330	146
192.168.1.9	1040	open	syn-ack	unknown	330	146
192.168.1.9	1054	open	syn-ack	unknown	330	146
192.168.1.9	1063	open	syn-ack	fpo-fns	330	146
192.168.1.9	1066	open	syn-ack	ms-sql-s	330	146
192.168.1.10	1433	open	syn-ack		294	20
192.168.1.10					294	20
192.168.1.10				ssh	294	20
192.168.1.10	22	open	syn-ack	smtp	294	20
192.168.1.10	25	open	syn-ack	domain	294	20
192.168.1.10	53	closed	conn-refused	http	294	20
192.168.1.10	80	open	syn-ack	pop3	294	20
192.168.1.10	110	open	syn-ack	imap	294	20
192.168.1.10	143	open	syn-ack	https	294	20
192.168.1.10	443	open	syn-ack	smtps	294	20
192.168.1.10	465	open	syn-ack	submission	294	20
192.168.1.10	587	open	syn-ack	imaps	294	20
192.168.1.10	993	open	syn-ack	pop3s	294	20
192.168.1.11	995	open	syn-ack		285	15
192.168.1.11				ftp	285	15

192.168.1.11	21	open	syn-ack	telnet	285	15
192.168.1.11	23	closed	conn-refused	smtp	285	15
192.168.1.11	25	closed	conn-refused	http	285	15
192.168.1.11	80	open	syn-ack	pop3	285	15
192.168.1.11	110	closed	conn-refused	netbios-ssn	285	15
192.168.1.11	139	open	syn-ack	imap	285	15
192.168.1.11	143	closed	conn-refused	https	285	15
192.168.1.11	443	open	syn-ack	microsoft-ds	285	15
192.168.1.11	445	open	syn-ack	ms-term-serv	285	15
192.168.1.12	3389	closed	conn-refused		228	18
192.168.1.12					228	18
192.168.1.12				ssh	228	18
192.168.1.12	22	open	syn-ack	smtp	228	18
192.168.1.12	25	closed	conn-refused	domain	228	18
192.168.1.12	53	closed	conn-refused	http	228	18
192.168.1.12	80	open	syn-ack	pop3	228	18
192.168.1.12	110	closed	conn-refused	imap	228	18
192.168.1.12	143	closed	conn-refused	https	228	18
192.168.1.12	443	open	syn-ack	smtps	228	18
192.168.1.12	465	closed	conn-refused	submission	228	18
192.168.1.12	587	closed	conn-refused	imaps	228	18
192.168.1.12	993	closed	conn-refused	pop3s	228	18
192.168.1.15	995	closed	conn-refused		338	105
192.168.1.15				ssh	338	105

192.168.1.15	22	open	syn-ack	http	338	105
192.168.1.15	80	open	syn-ack	rpcbind	338	105
192.168.1.15	111	open	syn-ack	http-proxy	338	105
192.168.1.17	8080	open	syn-ack		308	104
192.168.1.17				msrpc	308	104
192.168.1.17	135	open	syn-ack	netbios-ssn	308	104
192.168.1.17	139	open	syn-ack	microsoft-ds	308	104
192.168.1.17	445	open	syn-ack	IIS	308	104
192.168.1.17	1027	open	syn-ack	netinfo	308	104
192.168.1.17	1033	open	syn-ack	ms-sql-s	308	104
192.168.1.17	1433	open	syn-ack	msdtc	308	104
192.168.1.17	3372	open	syn-ack	vnc-http	308	104
192.168.1.17	5800	open	syn-ack	vnc	308	104
192.168.1.17	5900	open	syn-ack	unknown	308	104
192.168.1.18	14000	open	syn-ack		319	109
192.168.1.18				smtp	319	109
192.168.1.18	25	open	syn-ack	http	319	109
192.168.1.18	80	open	syn-ack	msrpc	319	109
192.168.1.18	135	open	syn-ack	netbios-ssn	319	109
192.168.1.18	139	open	syn-ack	https	319	109
192.168.1.18	443	open	syn-ack	microsoft-ds	319	109
192.168.1.18	445	open	syn-ack	unknown	319	109
192.168.1.18	1047	open	syn-ack	unknown	319	109
192.168.1.18	1064	open	syn-ack	unknown	319	109

192.168.1.18	1074	open	syn-ack	ms-sql-s	319	109
192.168.1.18	1433	open	syn-ack	msdtc	319	109
192.168.1.18	3372	open	syn-ack	vnc-http	319	109
192.168.1.18	5800	open	syn-ack	vnc	319	109
192.168.1.21	5900	open	syn-ack		307	80
192.168.1.21				smtp	307	80
192.168.1.21	25	open	syn-ack	http	307	80
192.168.1.21	80	open	syn-ack	msrpc	307	80
192.168.1.21	135	open	syn-ack	netbios-ssn	307	80
192.168.1.21	139	open	syn-ack	https	307	80
192.168.1.21	443	open	syn-ack	microsoft-ds	307	80
192.168.1.21	445	open	syn-ack	unknown	307	80
192.168.1.21	1028	open	syn-ack	iad2	307	80
192.168.1.21	1031	open	syn-ack	netinfo	307	80
192.168.1.21	1033	open	syn-ack	ms-sql-s	307	80
192.168.1.23	1433	open	syn-ack		270	82
192.168.1.23				http	270	82
192.168.1.23	80	open	syn-ack	msrpc	270	82
192.168.1.23	135	open	syn-ack	netbios-ssn	270	82
192.168.1.23	139	open	syn-ack	microsoft-ds	270	82
192.168.1.23	445	open	syn-ack	NFS-or-IIS	270	82
192.168.1.23	1025	open	syn-ack	IIS	270	82
192.168.1.23	1027	open	syn-ack	unknown	270	82
192.168.1.23	1801	open	syn-ack	zephyr-clt	270	82

192.168.1.23	2103	open	syn-ack	eklogin	270	82
192.168.1.23	2105	open	syn-ack	unknown	270	82
192.168.1.23	2107	open	syn-ack	ms-term-serv	270	82
	3389	open	syn-ack			

ATTACHMENT 2: Nessus Scan Report

IP Address	Protocol	Port ID	Application Running	Information Running
192.168.1.9	tcp	9385	unknown	The remote web server type is : Microsoft-IIS/5.0
192.168.1.9	tcp	9385	unknown	A web server is running on this port
192.168.1.9	tcp	25	smtp	A SMTP server is running on this port
192.168.1.9	tcp	25	smtp	An SMTP server is running on this port Here is its banner : 220 OldSrv.bracu.ac.bd Microsoft ESMTP MAIL Serv Aug 2009 14:05:25 +0600
192.168.1.9	tcp	139	netbios-ssn	An SMB server is running on this port
192.168.1.9	tcp	445	microsoft-ds	The following local accounts have never logged in : Guest Unused accounts are very helpful to hacker Solution : suppress these accounts Risk factor : Medium
192.168.1.9	tcp	445	microsoft-ds	The following accounts have never logged in : Guest Unused accounts are very helpful to hacker Solution : suppress these accounts Risk factor : Medium

192.168.1.9	tcp	445	microsoft-ds	The following accounts have passwords which neve Administrator Guest Password should have a limited lifetime Solution : disable password non-expiry Risk factor : Medium
192.168.1.9	tcp	445	microsoft-ds	The following accounts are disabled : Guest To minimize the risk of break-in, permanently disab should be deleted Risk factor : Low
192.168.1.9	tcp	445	microsoft-ds	The following accounts have never changed their pa Administrator To minimize the risk of break-in, users should change their password regularly
192.168.1.9	tcp	445	microsoft-ds	The following local accounts are disabled : Guest To minimize the risk of break-in, permanently disab should be deleted Risk factor : Low
192.168.1.9	Tcp	445	microsoft-ds	A CIFS server is running on this port
192.168.1.9	tcp	80	http	The remote web server seems to have its default we It probably means that this server is not used at all. Solution : Disable this service, as you do not use it

				Risk factor : Low
192.168.1.9	tcp	80	http	The remote web server type is : Microsoft-IIS/5.0
192.168.1.9	tcp	80	http	A web server is running on this port
192.168.1.9	udp		general/udp	For your information, here is the traceroute to 192. 192.168.0.96 192.168.1.9
192.168.1.7	udp	954	unknown	The yppasswd RPC service is running. If you do not disable it as it may become a security threat in the f is discovered. Risk factor : Low
192.168.1.7	udp	954	unknown	RPC program #100009 version 1 'yppasswdd' (yppas
192.168.1.7	tcp	947	unknown	RPC program #100007 version 2 'ypbind' is running RPC program #100007 version 1 'ypbind' is running
192.168.1.7	udp	944	unknown	RPC program #100007 version 2 'ypbind' is running RPC program #100007 version 1 'ypbind' is running
192.168.1.7	tcp	934	unknown	RPC program #600100069 version 1 'fypxfrd' (freebs
192.168.1.7	udp	932	unknown	RPC program #600100069 version 1 'fypxfrd' (freebs
192.168.1.7	tcp	926	unknown	RPC program #100004 version 2 'ypserv' (ypprog) is RPC program #100004 version 1 'ypserv' (ypprog) is
192.168.1.7	udp	923	unknown	RPC program #100004 version 2 'ypserv' (ypprog) is RPC program #100004 version 1 'ypserv' (ypprog) is
192.168.1.7	udp	845	unknown	The rquotad RPC service is running. If you do not us disable it as it may become a security threat in the f is discovered. Risk factor : Low

				CVE : CAN-1999-0625
192.168.1.7	udp	845	unknown	RPC program #100011 version 1 'rquotad' (rquotapr RPC program #100011 version 2 'rquotad' (rquotapr
192.168.1.7	udp	111	sunrpc	RPC program #100000 version 2 'portmapper' (port
192.168.1.7	tcp	111	sunrpc	RPC program #100000 version 2 'portmapper' (port
192.168.1.7	tcp	587	submission	A SMTP server is running on this port
192.168.1.7	tcp	587	submission	An SMTP server is running on this port Here is its banner : 220 student.bu.ac.bd ESMTP Sendmail 8.12.11/8.12 Tue, 4 Aug 2009 13:02:16 +0600
192.168.1.7	tcp	22	ssh	Remote SSH version : SSH-1.99-OpenSSH_3.6.1p2
192.168.1.7	tcp	22	ssh	An ssh server is running on this port
192.168.1.7	tcp	25	smtp	Remote SMTP server banner : 220 student.bu.ac.bd ESMTP Sendmail 8.12.11/8.12 Tue, 4 Aug 2009 13:03:25 +0600 This is probably: Sendmail version 8.12.11
192.168.1.7	tcp	25	smtp	A SMTP server is running on this port
192.168.1.7	tcp	25	smtp	An SMTP server is running on this port Here is its banner : 220 student.bu.ac.bd ESMTP Sendmail 8.12.11/8.12 Tue, 4 Aug 2009 13:02:15 +0600
192.168.1.7	tcp	995	pop3s	A pop3 server is running on this port
192.168.1.7	tcp	995	pop3s	A SSLv2 server answered on this port
192.168.1.7	tcp	110	pop3	A pop3 server is running on this port

192.168.1.7	udp	2049	nfs	RPC program #100003 version 2 'nfs' (nfsprog) is ru RPC program #100003 version 3 'nfs' (nfsprog) is ru RPC program #100003 version 4 'nfs' (nfsprog) is ru
192.168.1.7	tcp	2049	nfs	You are running a superfluous NFS daemon. You should consider removing it CVE : CAN-1999-0554, CAN-1999-0548
192.168.1.7	tcp	2049	nfs	RPC program #100003 version 2 'nfs' (nfsprog) is ru RPC program #100003 version 3 'nfs' (nfsprog) is ru RPC program #100003 version 4 'nfs' (nfsprog) is ru
192.168.1.7	tcp	3306	mysql	Remote MySQL version : 3.23.58
192.168.1.7	tcp	631	ipp	The remote web server type is : CUPS/1.1
192.168.1.7	tcp	631	ipp	A web server is running on this port
192.168.1.7	tcp	993	imaps	An IMAP server is running on this port through SSL
192.168.1.7	tcp	993	imaps	A SSLv2 server answered on this port
192.168.1.7	tcp	143	imap	An IMAP server is running on this port
192.168.1.7	tcp	443	https	The remote web server type is : Apache/2.0.51 (Fedora) Solution : You can set the directive 'ServerTokens Pr the information emanating from the server in its res
192.168.1.7	tcp	443	https	A web server is running on this port through SSL
192.168.1.7	tcp	443	https	A SSLv2 server answered on this port

192.168.1.7	tcp	80	http	The remote web server type is : Apache/2.0.51 (Fedora) Solution : You can set the directive 'ServerTokens Pr the information emanating from the server in its res
192.168.1.7	tcp	80	http	A web server is running on this port
192.168.1.7	udp		general/udp	For your information, here is the traceroute to 192. 192.168.0.96 192.168.1.7
192.168.1.7	tcp	848	gdoi	RPC program #100011 version 1 'rquotad' (rquotapr RPC program #100011 version 2 'rquotad' (rquotapr
192.168.1.7	tcp	21	ftp	Remote FTP server banner : 220 (vsFTPd 1.2.1)
192.168.1.7	tcp	21	ftp	A SMTP server is running on this port
192.168.1.7	tcp	21	ftp	An FTP server is running on this port. Here is its banner : 220 (vsFTPd 1.2.1)
192.168.1.7	udp	32768	filenet-tms	RPC program #100024 version 1 'status' is running o
192.168.1.7	tcp	32768	filenet-tms	RPC program #100024 version 1 'status' is running o
192.168.1.7	tcp	32769	filenet-rpc	RPC program #391002 version 2 'sgi_fam' (fam) is ru
192.168.1.7	udp	32772	filenet-pa	RPC program #100021 version 1 'nlockmgr' is runnin RPC program #100021 version 3 'nlockmgr' is runnin RPC program #100021 version 4 'nlockmgr' is runnin
192.168.1.7	tcp	32770	filenet-nch	RPC program #100021 version 1 'nlockmgr' is runnin RPC program #100021 version 3 'nlockmgr' is runnin RPC program #100021 version 4 'nlockmgr' is runnin
192.168.1.7	udp	53	domain	A DNS server is running on this port. If you do not u Risk factor : Low

192.168.1.7	tcp	53	domain	A DNS server is running on this port. If you do not u Risk factor : Low
192.168.1.7	tcp	106	3com-tsmux	This SMTP server is running on a non standard port. This might be a backdoor set up by crackers to send or even control your machine. Solution: Check and clean your configuration Risk factor : Medium
192.168.1.7	tcp	106	3com-tsmux	A SMTP server is running on this port
192.168.1.6	tcp	713	unknown	RPC program #100024 version 1 'status' is running c
192.168.1.6	udp	111	sunrpc	RPC program #100000 version 2 'portmapper' (port
192.168.1.6	tcp	111	sunrpc	RPC program #100000 version 2 'portmapper' (port
192.168.1.6	tcp	22	ssh	The remote SSH daemon supports the following ver SSH protocol : . 1.99 . 2.0 SSHv2 host key fingerprint : 9f:a7:98:a5:33:e2:07:39
192.168.1.6	tcp	22	ssh	Remote SSH version : SSH-2.0-OpenSSH_4.3
192.168.1.6	tcp	22	ssh	An ssh server is running on this port
192.168.1.6	udp		general/udp	For your information, here is the traceroute to 192. 192.168.0.96 192.168.1.6
192.168.1.6	udp	710	entrust-ash	RPC program #100024 version 1 'status' is running c
192.168.1.5	tcp	925	unknown	RPC program #100024 version 1 'status' is running c
192.168.1.5	udp	922	unknown	RPC program #100024 version 1 'status' is running c
192.168.1.5	udp	111	sunrpc	RPC program #100000 version 2 'portmapper' (port
192.168.1.5	tcp	111	sunrpc	RPC program #100000 version 2 'portmapper' (port

192.168.1.5	tcp	22	ssh	The remote SSH daemon supports the following ver SSH protocol : . 1.99 . 2.0 SSHv2 host key fingerprint : 18:2a:aa:8e:0b:28:05:9
192.168.1.5	tcp	22	ssh	Remote SSH version : SSH-2.0-OpenSSH_4.3
192.168.1.5	tcp	22	ssh	An ssh server is running on this port
192.168.1.5	tcp	8443	pcsync-https	A web server is running on this port through SSL
192.168.1.5	tcp	8443	pcsync-https	A TLSv1 server answered on this port
192.168.1.5	udp	123	ntp	An NTP (Network Time Protocol) server is listening c Risk factor : Low
192.168.1.5	tcp	443	https	The remote web server type is : Apache/2.2.3 (CentOS) Solution : You can set the directive 'ServerTokens Pr the information emanating from the server in its res
192.168.1.5	tcp	443	https	A web server is running on this port through SSL
192.168.1.5	tcp	443	https	A TLSv1 server answered on this port
192.168.1.5	tcp	8080	http-alt	The GET method revealed those proxies on the way HTTP/1.0 std-proxy.bracu.ac.bd:8080 (squid/2.6.S
192.168.1.5	tcp	8080	http-alt	The remote web server type is : squid/2.6.STABLE6
192.168.1.5	tcp	8080	http-alt	A (non-RFC compliant) web server seems to be runn
192.168.1.5	tcp	80	http	A (non-RFC compliant) web server seems to be runn

192.168.1.5	udp		general/udp	For your information, here is the traceroute to 192. 192.168.0.96 192.168.1.5
192.168.1.4	tcp	9790	unknown	
192.168.1.4	tcp	17	qotd	qotd (Quote of the Day) seems to be running on thi
192.168.1.4	tcp	515	printer	
192.168.1.4	tcp	139	netbios-ssn	An SMB server is running on this port
192.168.1.4	tcp	445	microsoft-ds	The following local accounts have never logged in : Guest TsInternetUser Unused accounts are very helpful to hacker Solution : suppress these accounts Risk factor : Medium
192.168.1.4	tcp	445	microsoft-ds	The following accounts have never logged in : Guest TsInternetUser Unused accounts are very helpful to hacker Solution : suppress these accounts Risk factor : Medium
192.168.1.4	tcp	445	microsoft-ds	The following accounts are disabled : Guest To minimize the risk of break-in, permanently disab should be deleted Risk factor : Low

192.168.1.4	tcp	445	microsoft-ds	The following accounts have never changed their pa Administrator TsInternetUser To minimize the risk of break-in, users should change their password regularly
192.168.1.4	tcp	445	microsoft-ds	The following local accounts are disabled : Guest To minimize the risk of break-in, permanently disab should be deleted Risk factor : Low
192.168.1.4	tcp	445	microsoft-ds	The following local accounts have never changed th Administrator TsInternetUser To minimize the risk of break-in, users should change their password regularly
192.168.1.4	tcp	445	microsoft-ds	A CIFS server is running on this port
192.168.1.4	udp		general/udp	For your information, here is the traceroute to 192. 192.168.0.96 192.168.1.4
192.168.1.4	tcp	7	echo	An echo server is running on this port
192.168.1.4	tcp	19	chargen	Chargen is running on this port
192.168.1.4	tcp	548	afpovertcp	This host is running an AppleShare File Services ove Machine type: Windows NT Server name: SERVER2 UAMs: ClearTxt Passwrd/Microsoft V1.0/MS2.0 AFP Versions: AFPVersion 2.0/AFPVersion 2.1/AFP2

192.168.1.3	tcp	7235	unknown	The remote web server type is : Microsoft-IIS/5.0
192.168.1.3	tcp	7235	unknown	A web server is running on this port
192.168.1.3	tcp	25	smtp	A SMTP server is running on this port
192.168.1.3	tcp	25	smtp	An SMTP server is running on this port Here is its banner : 220 server1.bracu.ac.bd Microsoft ESMTP MAIL Ser Aug 2009 14:05:27 +0600
192.168.1.3	tcp	17	qotd	qotd (Quote of the Day) seems to be running on thi
192.168.1.3	tcp	515	printer	
192.168.1.3	udp	123	ntp	An NTP (Network Time Protocol) server is listening o Risk factor : Low
192.168.1.3	tcp	139	netbios-ssn	An SMB server is running on this port
192.168.1.3	tcp	42	name	
192.168.1.3	tcp	1029	ms-lsa	A CIS (COM+ Internet Services) server is listening on Server banner : ncacn_http/1.0
192.168.1.3	tcp	445	microsoft-ds	The guest user belongs to groups other than guest users or domain guests. As guest should not have any privilege, you should fix this. Risk factor : Medium
192.168.1.3	tcp	445	microsoft-ds	The following users are in the domain administrato . Administrator . Fahima You should make sure that only the proper users ar

				Risk factor : Low
192.168.1.3	tcp	445	microsoft-ds	The following accounts are disabled : Guest To minimize the risk of break-in, permanently disab should be deleted Risk factor : Low
192.168.1.3	tcp	445	microsoft-ds	The following accounts have never changed their pa TsInternetUser IUSR_NETFINITY IWAM_NETFINITY ASPNET To minimize the risk of break-in, users should change their password regularly
192.168.1.3	tcp	445	microsoft-ds	A CIFS server is running on this port
192.168.1.3	tcp	636	ldaps	
192.168.1.3	tcp	464	kpasswd	
192.168.1.3	tcp	88	kerberos	
192.168.1.3	tcp	443	https	
192.168.1.3	tcp	593	http-rpc-epmap	

192.168.1.3	tcp	80	http	The remote web server seems to have its default we It probably means that this server is not used at all. Solution : Disable this service, as you do not use it Risk factor : Low
192.168.1.3	tcp	80	http	The remote web server type is : Microsoft-IIS/5.0
192.168.1.3	tcp	80	http	A web server is running on this port
192.168.1.3	udp		general/udp	For your information, here is the traceroute to 192. 192.168.0.96 192.168.1.3
192.168.1.3	tcp	19	chargen	Chargen is running on this port
192.168.1.3	tcp	548	afpovertcp	This host is running an AppleShare File Services ove Machine type: Windows NT Server name: SERVER1 UAMs: ClearTxt Passwrd/Microsoft V1.0/MS2.0 AFP Versions: AFPVersion 2.0/AFPVersion 2.1/AFP
192.168.1.23	tcp	3469	pluribus	The remote web server type is : Microsoft-IIS/6.0
192.168.1.23	tcp	3469	pluribus	A web server is running on this port
192.168.1.23	tcp	139	netbios-ssn	An SMB server is running on this port
192.168.1.23	tcp	445	microsoft-ds	A CIFS server is running on this port
192.168.1.23	tcp	80	http	The remote web server type is : Microsoft-IIS/6.0
192.168.1.23	tcp	80	http	The following CGI have been discovered : Syntax : cginame (arguments [default value]) /LibraryWeb/KeyWordSearch.asp (u_field [] u_searc
192.168.1.23	tcp	80	http	A web server is running on this port

192.168.1.23	udp		general/udp	For your information, here is the traceroute to 192. 192.168.0.96 192.168.1.23
192.168.1.21	tcp	3964	unknown	The remote web server type is : Microsoft-IIS/5.0
192.168.1.21	tcp	3964	unknown	A web server is running on this port
192.168.1.21	tcp	25	smtp	A SMTP server is running on this port
192.168.1.21	tcp	25	smtp	An SMTP server is running on this port Here is its banner : 220 aalbu.bracu.ac.bd Microsoft ESMTP MAIL Servic Aug 2009 14:05:32 +0600
192.168.1.21	tcp	139	netbios-ssn	An SMB server is running on this port
192.168.1.21	tcp	445	microsoft-ds	The following local accounts have never logged in : Guest TsInternetUser SQLDebugger Unused accounts are very helpful to hacker Solution : suppress these accounts Risk factor : Medium
192.168.1.21	tcp	445	microsoft-ds	The following accounts have never logged in : Guest TsInternetUser Unused accounts are very helpful to hacker Solution : suppress these accounts Risk factor : Medium

192.168.1.21	tcp	445	microsoft-ds	The following accounts have passwords which neve Guest TsInternetUser Password should have a limited lifetime Solution : disable password non-expiry Risk factor : Medium
192.168.1.21	tcp	445	microsoft-ds	The following accounts are disabled : Guest To minimize the risk of break-in, permanently disab should be deleted Risk factor : Low
192.168.1.21	tcp	445	microsoft-ds	The following accounts have never changed their pa Administrator TsInternetUser To minimize the risk of break-in, users should change their password regularly
192.168.1.21	tcp	445	microsoft-ds	The following local accounts are disabled : Guest To minimize the risk of break-in, permanently disab should be deleted Risk factor : Low
192.168.1.21	tcp	445	microsoft-ds	A CIFS server is running on this port

192.168.1.21	tcp	80	http	The remote web server seems to have its default we It probably means that this server is not used at all. Solution : Disable this service, as you do not use it Risk factor : Low
192.168.1.21	tcp	80	http	The remote web server type is : Microsoft-IIS/5.0
192.168.1.21	tcp	80	http	A web server is running on this port
192.168.1.21	udp		general/udp	For your information, here is the traceroute to 192. 192.168.0.96 192.168.1.21
192.168.1.2	tcp	25	smtp	A SMTP server is running on this port
192.168.1.2	tcp	25	smtp	An SMTP server is running on this port Here is its banner : 220 netfinity.bracu.ac.bd Microsoft ESMTP MAIL Se Aug 2009 14:05:26 +0600
192.168.1.2	tcp	17	qotd	qotd (Quote of the Day) seems to be running on thi
192.168.1.2	tcp	515	printer	
192.168.1.2	udp	123	ntp	An NTP (Network Time Protocol) server is listening o Risk factor : Low
192.168.1.2	tcp	139	netbios-ssn	An SMB server is running on this port
192.168.1.2	tcp	3753	nattyserver	The remote web server type is : Microsoft-IIS/5.0
192.168.1.2	tcp	3753	nattyserver	A web server is running on this port
192.168.1.2	tcp	42	name	
192.168.1.2	tcp	3269	msft-gc-ssl	The service closed the connection after 0 seconds w It might be protected by some TCP wrapper
192.168.1.2	tcp	3268	msft-gc	

192.168.1.2	tcp	1029	ms-lsa	A CIS (COM+ Internet Services) server is listening on Server banner : ncacn_http/1.0
192.168.1.2	tcp	445	microsoft-ds	The following accounts have never logged in : Guest TsInternetUser ASPNET Unused accounts are very helpful to hacker Solution : suppress these accounts Risk factor : Medium
192.168.1.2	tcp	445	microsoft-ds	The guest user belongs to groups other than guest users or domain guests. As guest should not have any privilege, you should fix this. Risk factor : Medium
192.168.1.2	tcp	445	microsoft-ds	The following users are in the domain administrator . Administrator . Fahima You should make sure that only the proper users ar Risk factor : Low
192.168.1.2	tcp	445	microsoft-ds	The following accounts are disabled : Guest To minimize the risk of break-in, permanently disab should be deleted Risk factor : Low

192.168.1.2	tcp	445	microsoft-ds	The following accounts have never changed their pa TsInternetUser IUSR_NETFINITY IWAM_NETFINITY ASPNET To minimize the risk of break-in, users should change their password regularly
192.168.1.2	tcp	445	microsoft-ds	A CIFS server is running on this port
192.168.1.2	tcp	636	ldaps	The service closed the connection after 0 seconds w It might be protected by some TCP wrapper
192.168.1.2	tcp	464	kpasswd	
192.168.1.2	tcp	88	kerberos	
192.168.1.2	tcp	80	http	The remote web server seems to have its default we It probably means that this server is not used at all. Solution : Disable this service, as you do not use it Risk factor : Low
192.168.1.2	tcp	80	http	The remote web server type is : Microsoft-IIS/5.0
192.168.1.2	tcp	80	http	A web server is running on this port
192.168.1.2	udp		general/udp	For your information, here is the traceroute to 192. 192.168.0.96 192.168.1.2
192.168.1.2	tcp	7	echo	An echo server is running on this port
192.168.1.2	udp	53	domain	A DNS server is running on this port. If you do not u Risk factor : Low
192.168.1.2	tcp	53	domain	A DNS server is running on this port. If you do not u

				Risk factor : Low
192.168.1.2	tcp	19	chargen	Chargen is running on this port
192.168.1.2	tcp	548	afpovertcp	This host is running an AppleShare File Services ove Machine type: Windows NT Server name: NETFINITY UAMs: ClearTxt Passwrd/Microsoft V1.0/MS2.0 AFP Versions: AFPVersion 2.0/AFPVersion 2.1/AFP
192.168.1.18	tcp	5800	vnc-http	The remote server is running VNC. VNC permits a console to be displayed remotely. Solution: Disable VNC access from the network by using a firewall, or stop VNC service if not needed. Risk factor : Medium
192.168.1.18	tcp	5800	vnc-http	A web server is running on this port
192.168.1.18	tcp	5900	vnc	The remote VNC server chose security type #2 (VNC
192.168.1.18	tcp	8749	unknown	A web server is running on this port
192.168.1.18	tcp	3372	tip2	A MSDTC server is running on this port
192.168.1.18	tcp	25	smtp	A SMTP server is running on this port
192.168.1.18	tcp	25	smtp	An SMTP server is running on this port Here is its banner : 220 printserver.bracu.ac.bd Microsoft ESMTP MAIL 4 Aug 2009 14:05:25 +0600
192.168.1.18	tcp	139	netbios-ssn	An SMB server is running on this port
192.168.1.18	tcp	445	microsoft-ds	The following local accounts have never logged in : Guest TsInternetUser Unused accounts are very helpful to hacker Solution : suppress these accounts

				Risk factor : Medium
192.168.1.18	tcp	445	microsoft-ds	The following accounts have never logged in : Guest TsInternetUser Unused accounts are very helpful to hacker Solution : suppress these accounts Risk factor : Medium
192.168.1.18	tcp	445	microsoft-ds	The following accounts are disabled : Guest To minimize the risk of break-in, permanently disab should be deleted Risk factor : Low
192.168.1.18	tcp	445	microsoft-ds	The following accounts have never changed their pa TsInternetUser To minimize the risk of break-in, users should change their password regularly

192.168.1.18	tcp	445	microsoft-ds	The following local accounts are disabled : Guest To minimize the risk of break-in, permanently disab should be deleted Risk factor : Low
192.168.1.18	tcp	445	microsoft-ds	The following local accounts have never changed th TsInternetUser IUSR_PRINTSERVER IWAM_PRINTSERVER To minimize the risk of break-in, users should change their password regularly
192.168.1.18	tcp	445	microsoft-ds	A CIFS server is running on this port
192.168.1.18	tcp	80	http	The remote web server type is : Microsoft-IIS/5.0
192.168.1.18	tcp	80	http	The remote web server seems to have its default w It probably means that this server is not used at all. Solution : Disable this service, as you do not use it Risk factor : Low
192.168.1.18	tcp	80	http	A web server is running on this port
192.168.1.18	udp		general/udp	For your information, here is the traceroute to 192. 192.168.0.96 192.168.1.18
192.168.1.17	tcp	5800	vnc-http	The remote server is running VNC. VNC permits a console to be displayed remotely. Solution: Disable VNC access from the network by using a firewall, or stop VNC service if not needed.

				Risk factor : Medium
192.168.1.17	tcp	5800	vnc-http	A web server is running on this port
192.168.1.17	tcp	5900	vnc	The remote VNC server chose security type #2 (VNC
192.168.1.17	tcp	3372	tip2	A MSDTC server is running on this port
192.168.1.17	tcp	139	netbios-ssn	An SMB server is running on this port
192.168.1.17	tcp	445	microsoft-ds	The following local accounts have never logged in : Guest TsInternetUser Unused accounts are very helpful to hacker Solution : suppress these accounts Risk factor : Medium
192.168.1.17	tcp	445	microsoft-ds	The following accounts have never logged in : Guest TsInternetUser Unused accounts are very helpful to hacker Solution : suppress these accounts Risk factor : Medium
192.168.1.17	tcp	445	microsoft-ds	The following accounts are disabled : Guest To minimize the risk of break-in, permanently disab should be deleted Risk factor : Low

192.168.1.17	tcp	445	microsoft-ds	The following accounts have never changed their pa TsInternetUser To minimize the risk of break-in, users should change their password regularly
192.168.1.17	tcp	445	microsoft-ds	The following local accounts are disabled : Guest To minimize the risk of break-in, permanently disab should be deleted Risk factor : Low
192.168.1.17	tcp	445	microsoft-ds	The following local accounts have never changed th TsInternetUser To minimize the risk of break-in, users should change their password regularly
192.168.1.17	tcp	445	microsoft-ds	A CIFS server is running on this port
192.168.1.17	udp		general/udp	For your information, here is the traceroute to 192. 192.168.0.96 192.168.1.17
192.168.1.15	udp	111	sunrpc	RPC program #100000 version 2 'portmapper' (port
192.168.1.15	tcp	111	sunrpc	RPC program #100000 version 2 'portmapper' (port
192.168.1.15	tcp	22	ssh	The remote SSH daemon supports the following ver SSH protocol : . 1.99 . 2.0 SSHv2 host key fingerprint : f2:7a:40:18:63:f3:68:b5

192.168.1.15	tcp	22	ssh	Remote SSH version : SSH-2.0-OpenSSH_4.3
192.168.1.15	tcp	22	ssh	An ssh server is running on this port
192.168.1.15	udp	123	ntp	An NTP (Network Time Protocol) server is listening o Risk factor : Low
192.168.1.15	udp	691	msexch-routing	RPC program #100024 version 1 'status' is running o
192.168.1.15	tcp	8080	http-alt	A (non-RFC compliant) web server seems to be runn
192.168.1.15	tcp	80	http	A (non-RFC compliant) web server seems to be runn
192.168.1.15	tcp	694	ha-cluster	RPC program #100024 version 1 'status' is running o
192.168.1.15	udp		general/udp	For your information, here is the traceroute to 192. 192.168.0.96 192.168.1.15
192.168.1.13	tcp	9980	unknown	The remote web server type is : Apache/2.0.54 (Win32) Solution : You can set the directive 'ServerTokens Pr the information emanating from the server in its res
192.168.1.13	tcp	9980	unknown	A web server is running on this port
192.168.1.13	tcp	139	netbios-ssn	An SMB server is running on this port
192.168.1.13	tcp	445	microsoft-ds	A CIFS server is running on this port
192.168.1.13	udp		general/udp	For your information, here is the traceroute to 192. 192.168.0.96 192.168.1.13
192.168.1.12	tcp	22	ssh	The remote SSH daemon supports the following ver SSH protocol : . 1.99 . 2.0

				SSHv2 host key fingerprint : 31:9a:82:7c:70:69:01:cc
192.168.1.12	tcp	22	ssh	Remote SSH version : SSH-2.0-OpenSSH_4.7
192.168.1.12	tcp	22	ssh	An ssh server is running on this port
192.168.1.12	tcp	443	https	The remote web server type is : Apache/2.2.6 (Fedora) Solution : You can set the directive 'ServerTokens Pr the information emanating from the server in its res
192.168.1.12	tcp	443	https	A web server is running on this port through SSL
192.168.1.12	tcp	443	https	A TLSv1 server answered on this port
192.168.1.12	tcp	80	http	The remote web server type is : Apache/2.2.6 (Fedora) Solution : You can set the directive 'ServerTokens Pr the information emanating from the server in its res
192.168.1.12	tcp	80	http	A web server is running on this port
192.168.1.12	udp		general/udp	For your information, here is the traceroute to 192. 192.168.0.96 192.168.1.12
192.168.1.11	tcp	139	netbios-ssn	An SMB server is running on this port
192.168.1.11	tcp	445	microsoft-ds	A CIFS server is running on this port
192.168.1.11	tcp	443	https	A web server is running on this port
192.168.1.11	tcp	80	http	A web server is running on this port

192.168.1.11	udp		general/udp	For your information, here is the traceroute to 192. 192.168.0.96 192.168.1.11
192.168.1.10	tcp	465	urd	Remote SMTP server banner : 220 mail.bracu.ac.bd ESMTP Sendmail 8.13.8/8.13.8 Tue, 4 Aug 2009 14:07:53 +0600 This is probably: Sendmail
192.168.1.10	tcp	465	urd	A SMTP server is running on this port
192.168.1.10	tcp	465	urd	An SMTP server is running on this port through SSL Here is its banner : 220 mail.bracu.ac.bd ESMTP Sendmail 8.13.8/8.13.8 Tue, 4 Aug 2009 14:07:37 +0600
192.168.1.10	tcp	465	urd	A TLSv1 server answered on this port
192.168.1.10	tcp	587	submission	Remote SMTP server banner : 220 mail.bracu.ac.bd ESMTP Sendmail 8.13.8/8.13.8 Tue, 4 Aug 2009 14:07:53 +0600 This is probably: Sendmail
192.168.1.10	tcp	587	submission	A SMTP server is running on this port
192.168.1.10	tcp	587	submission	An SMTP server is running on this port Here is its banner : 220 mail.bracu.ac.bd ESMTP Sendmail 8.13.8/8.13.8 Tue, 4 Aug 2009 14:05:46 +0600
192.168.1.10	tcp	22	ssh	The remote SSH daemon supports the following ver SSH protocol : . 1.99 . 2.0

				SSHv2 host key fingerprint : 58:3e:e4:7c:f3:af:0a:ed
192.168.1.10	tcp	22	ssh	Remote SSH version : SSH-2.0-OpenSSH_4.3
192.168.1.10	tcp	22	ssh	An ssh server is running on this port
192.168.1.10	tcp	25	smtp	Remote SMTP server banner : 220 mail.bracu.ac.bd ESMTP Sendmail 8.13.8/8.13.8 Tue, 4 Aug 2009 14:07:53 +0600 This is probably: Sendmail
192.168.1.10	tcp	25	smtp	A SMTP server is running on this port
192.168.1.10	tcp	25	smtp	An SMTP server is running on this port Here is its banner : 220 mail.bracu.ac.bd ESMTP Sendmail 8.13.8/8.13.8 Tue, 4 Aug 2009 14:05:12 +0600
192.168.1.10	tcp	995	pop3s	A pop3 server is running on this port
192.168.1.10	tcp	995	pop3s	A SSLv2 server answered on this port
192.168.1.10	tcp	110	pop3	A pop3 server is running on this port
192.168.1.10	tcp	993	imaps	A SSLv2 server answered on this port
192.168.1.10	tcp	443	https	The remote web server type is : Apache/2.2.3 (CentOS) Solution : You can set the directive 'ServerTokens Pr the information emanating from the server in its res
192.168.1.10	tcp	443	https	A web server is running on this port through SSL

192.168.1.10	tcp	443	https	A TLSv1 server answered on this port
192.168.1.10	tcp	80	http	The remote web server type is : Apache/2.2.3 (CentOS) Solution : You can set the directive 'ServerTokens Pr the information emanating from the server in its res
192.168.1.10	tcp	80	http	A web server is running on this port
192.168.1.10	udp		general/udp	For your information, here is the traceroute to 192. 192.168.0.96 192.168.1.10
192.168.1.1	tcp	5800	vnc-http	The remote server is running VNC. VNC permits a console to be displayed remotely. Solution: Disable VNC access from the network by using a firewall, or stop VNC service if not needed. Risk factor : Medium
192.168.1.1	tcp	5800	vnc-http	The remote web server type is : RealVNC/4.0
192.168.1.1	tcp	5800	vnc-http	A web server is running on this port
192.168.1.1	tcp	5900	vnc	The remote VNC server supports those security type + 5 (RA2)
192.168.1.1	tcp	5938	unknown	An unknown server is running on this port. If you know what it is, please send this banner to th 0x00: 17 24 0A 20 .$.
192.168.1.1	tcp	3519	nvmsgd	
192.168.1.1	udp	123	ntp	An NTP (Network Time Protocol) server is listening o Risk factor : Low
192.168.1.1	tcp	139	netbios-ssn	An SMB server is running on this port

192.168.1.1	tcp	445	microsoft-ds	A CIFS server is running on this port
192.168.1.1	tcp	80	http	A web server is running on this port
192.168.1.1	udp		general/udp	For your information, here is the traceroute to 192. 192.168.0.96 192.168.1.1