Volume 4, Issue 12, December 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Network Based Approach to Discover Security Vulnerability on Host System

Sandeep Kumar Yadav[*]
M.Tech Scholar, Dept. of CSE
RKDFIST Bhopal (M.P.), India

Daya Shankar Pandey
Asst. Professor, Dept. of CSE
RKDFIST Bhopal (M.P.), India

Shrikant Lade
Asst. Professor, Dept. of CSE
RKDFIST Bhopal (M.P.), India

Abstract— In the present scenario peoples are in computer era where very far person also connect to other by a single click. Networking plays an important role to achieve this. Every single organization whether small or big should have their own intranet-working. By their highly interdependent and each machine overall susceptibility to attack depends upon the vulnerabilities of other machines in the network. Hackers can take this advantage of several vulnerabilities in every possible manner to penetrate a network and compromise organizations critical system to find sensitive information. With increasing sophisticated attacks are rises day by day so in order to protect an organization's network, it requires not only understanding about single system vulnerabilities but also their interdependencies. The ability to quickly mitigate vulnerabilities is very essential. If vulnerabilities left undetected introduce a serious security threat to enterprise systems and can leave vital critical data exposed to attacks by hackers. For organization it means huge loss of revenue and productivity, organization may end up with that. The main objective of this paper is to discover the security vulnerabilities on the host systems over a network connection. For this A lot of port scanner and vulnerability scanner has been proposed to tackle this, but none of them single are capable to detect vulnerabilities completely. So here presenting a set of security tools and also analysis of their results which provides better understanding of top security flaws.

Keywords— Vulnerability Scanner, Vulnerability assessment, computer security, host security, network security, detecting security flaws, port scanning.

I. Introduction

Today's Computer network security is main concern of any organization because the network is the medium over which most attacks or intrusions on computer systems are launched. As more and more critical information is being stored on computer systems and transferred over computer networks, there are an increasing number of attacks on these systems in an attempt to steal, destroy or corrupt that information. Because of most computer systems have some kind of security flaws that may allow outsiders (or hackers) to gain unauthorized access to sensitive information. In most cases, it is infeasible to replace such a flawed system with a new, more secure system. Even a more secure system can still be vulnerable to insiders misusing their privileges. So there is a definite mechanism that can be detecting vulnerability on host systems [1].

Assessing and mitigating the vulnerabilities requires in depth understanding of these vulnerabilities. It becomes very necessary enough to know the basic idea that works behind these vulnerabilities such as what makes them to appear in the system, what flaws need to be corrected. There is an open platform recommended by the SANS Institute as a critical control and by US based National institute of Standards and Technology (NIST) for assessing all critical vulnerabilities[02]. Here we used the best practices for security; the Open Source Security Testing Methodology Manual (OSSTMM) introduced a model [03] of vulnerability detection system setup on distributed intranet network architecture [04].

Our work involves the study of various port scanners and vulnerability scanners. It is my belief that a network vulnerability scanner should be capable of identifying poorly configured services, default services that have poor security mechanism and software with known security vulnerabilities. We use Nmap [05] and Nessus [06] VA (Vulnerability Assessment) tools to scanning of various remote hosts. Because the results show significant variation in discovered security vulnerabilities by different tools. It may be very helpful to analyzed various vulnerabilities and make a comparison of various scanners [07] based on their capability of revealing these vulnerabilities. These comparison results are only a quick overview, we have not followed up each identified vulnerability to check false positives and false negatives.

Section II explains the various components of scanners before the use of vulnerability scanners. Section III describes various scanners in detail with their results, when applied on our institute's intranet network. Section IV has comparative view of the various VA tools result and analysis. Section V has the overall conclusion after observing different scanners.

II. COMPONENTS OF VULNERABILITY SCANNER

Generally vulnerability scanners have four basic modules, such as a User Interface, a Scan Engine, Database of Known vulnerability, and a Scan Report.

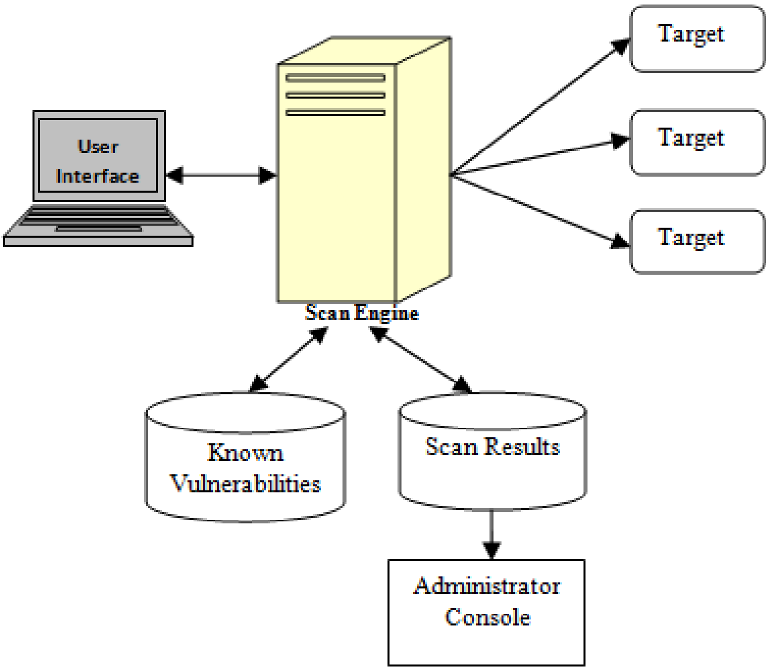


Figure 1 Components of general vulnerability scanner

1) The User Interface provides a platform for admin to operate on scanners. It may be either Command line Interface (CLI) or it may be Graphical User Interface (GUI).
2) The scan Engine executes security checks according to their installed plug-ins and payloads for identifying system information and vulnerabilities. It may also the capability to scan more than one host at a same time and compares the results against known vulnerabilities.
3) The known vulnerability database stores scan results and other information used by scanner. The number of plug-ins will vary depending on corresponding vendor. Each vendor regularly updating their plug-ins timely. Each plug-ins might be contains not only the test cases but also a specific vulnerability description, a Common vulnerabilities and Exposures (CVE) [08-14] detected and also their fixing instructions for a detected vulnerability.
4) The Scan Results gives different levels of reports, such as detailed technical reports with their recommendation to fix each of them.
   When the organization's network is very wide, then Distributed Network Scanners are helpful. In this a centralized management console is assessing vulnerabilities across geographically dispersed networks.

III. VULNERABILITY ASSESSMENT TOOLS

Vulnerability assessment is a process to identifying the vulnerabilities in the system before they could be used by anyone else with bad intentions of harming the network and connected systems. Some time enterprise management more focus on the firewall security but the internal security mechanism is also matters. VA tools is not only focused on single application or system but it takes into consideration all the factors that can provide system related information such as ports open or closed, what services running, which operating system used etc.

There are certain categories of Vulnerability Assessment Tool:

- Port Scanners
- Vulnerability Scanners
- Application Scanners

A. NMAP

A port scanner is a tool used by both system administrators and attacker(s) to identify vulnerabilities in operating systems. Nmap is a port scanner that takes an IP address of target machine[09] or the host name and then finds the basic information related to it. It also finds the number of ports that are running on that particular host, number of ports that are opened, number of closed ports, services running on those ports, for instance, whether services are TCP-oriented or FTP-oriented[10-11]. It also predicts the type of operating system being used on that particular host. The network topology of the scanned host is recorded in the graphical format which shows the various gateways through which the local machine accesses that particular remote host.

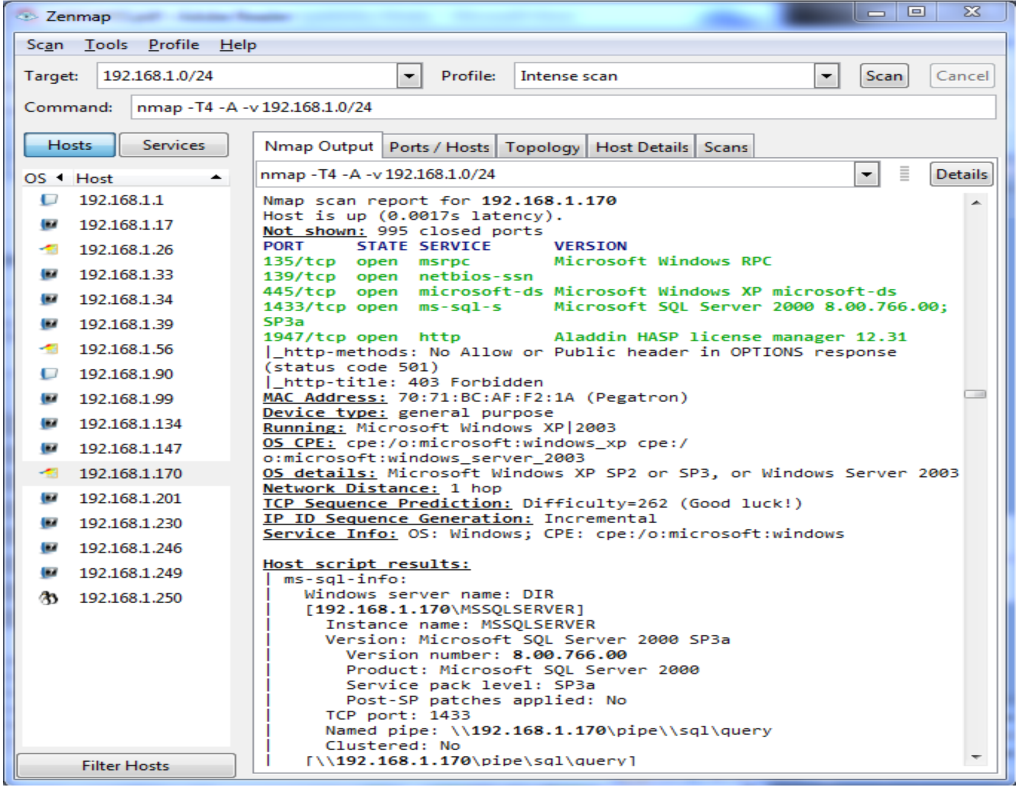
From this scan results, a system administrator, or an attacker, can determine what loop holes need to be patched or what can be easy to exploit.

Nmap Port Scanning Techniques Summary: A quick view of all the Nmap scanning switches and their comparison on the bases of their usability for privileged users and also which scans identify TCP ports, and which identify UDP ports are shown in Table 1 [12-14].

Table 1 nmap port scanning switches

Nmap Scan Type	Commmand Syntax	Requires Privileged Access	Identifies TCP Posts	Identifies UDP Ports
TCP SYN Scan	-sS	YES	YES	NO
TCP connect() Scan	-sT	NO	YES	NO
FIN Scan	-sF	YES	YES	NO
Xmas Tree Scan	-sX	YES	YES	NO
Null Scan	-sN	YES	YES	NO
Ping Scan	-sP	NO	NO	NO
Version Detection	-sV	NO	NO	NO
UDP Scan	-sU	YES	NO	YES
IP Protocol Scan	-sO	YES	NO	NO
ACK Scan	-sA	YES	YES	NO
Window Scan	-sW	YES	YES	NO
RPC Scan	-sR	NO	NO	NO
List Scan	-sL	NO	NO	NO
Idle Scan	-sI	YES	YES	NO
FTP Bounce Attack	-b	NO	YES	NO

A number of various host have been scanned using Nmap. The figure below depicts the results obtained after scanning an engineering institute’s Local Area Network (LAN).



Target: 192.168.1.0/24 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.1.0/24

```
192.168.1.1
192.168.1.17
192.168.1.26
192.168.1.33
192.168.1.34
192.168.1.39
192.168.1.56
192.168.1.90
192.168.1.99
192.168.1.134
192.168.1.147
192.168.1.170
192.168.1.201
192.168.1.230
192.168.1.246
192.168.1.249
192.168.1.250
```

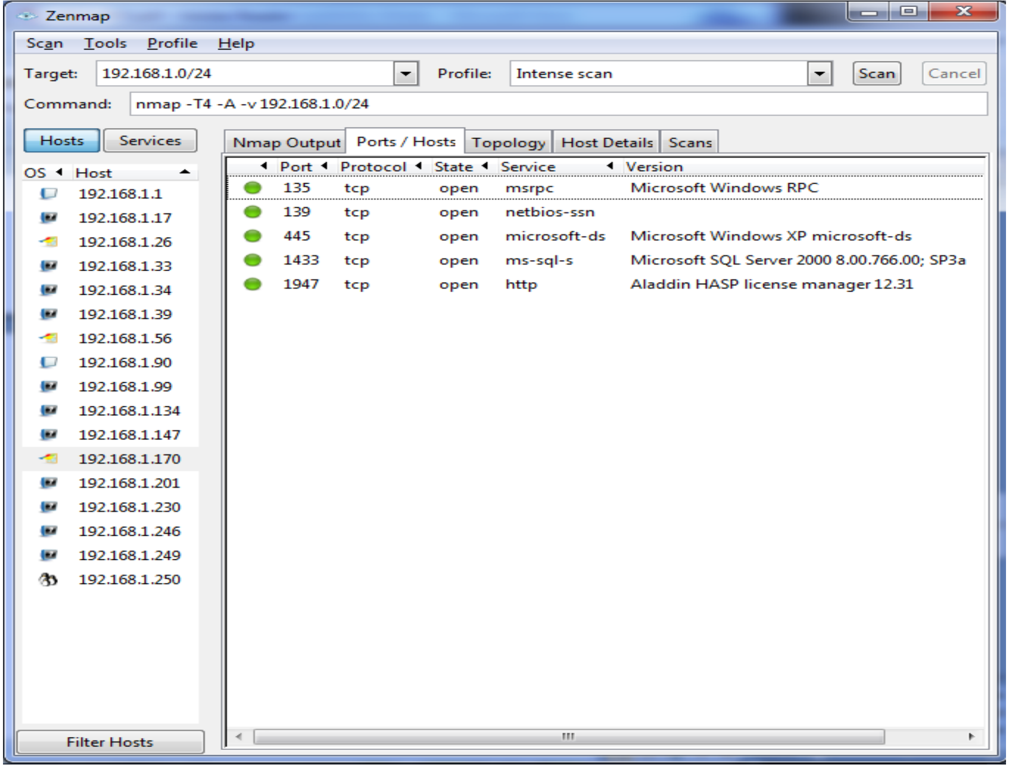
```
nmap -T4 -A -v 192.168.1.0/24

Nmap scan report for 192.168.1.170
Host is up (0.0017s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
1433/tcp open  ms-sql-s     Microsoft SQL Server 2000 8.00.766.00;
SP3a
1947/tcp open  http         Aladdin HASP license manager 12.31
|_http-methods: No Allow or Public header in OPTIONS response
(status code 501)
|_http-title: 403 Forbidden
MAC Address: 70:71:BC:AF:F2:1A (Pegatron)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/
o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| ms-sql-info:
|   Windows server name: DIR
|   [192.168.1.170\MSSQLSERVER]
|     Instance name: MSSQLSERVER
|     Version: Microsoft SQL Server 2000 SP3a
|       Version number: 8.00.766.00
|       Product: Microsoft SQL Server 2000
|       Service pack level: SP3a
|       Post-SP patches applied: No
|     TCP port: 1433
|     Named pipe: \\192.168.1.170\pipe\\sql\query
|     Clustered: No
|   [\\192.168.1.170\pipe\sql\query]
```

Figure 2 Nmap basic output for after scanning Institutes Local Area Network

Figure 2 shows the basic output after scanning our Institutes Local Area Network. It shows IP address, number of available ports, discovered open ports, running services with their versions.



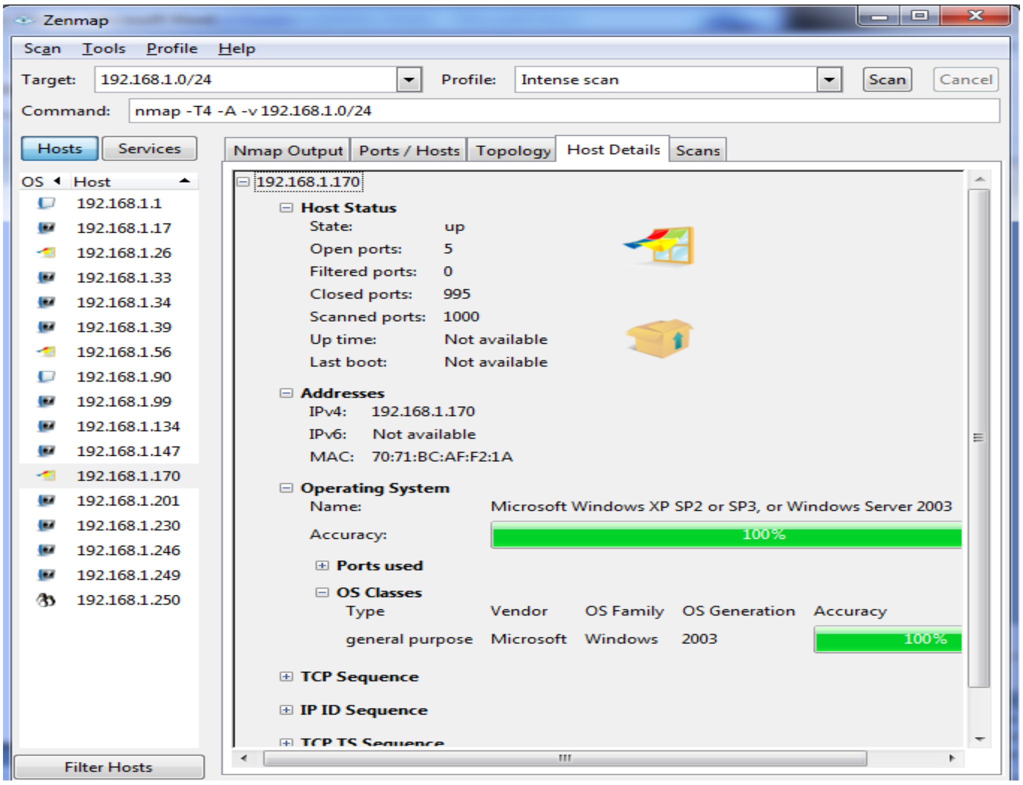
Target: 192.168.1.0/24
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.1.0/24

OS	Host
	192.168.1.1
	192.168.1.17
	192.168.1.26
	192.168.1.33
	192.168.1.34
	192.168.1.39
	192.168.1.56
	192.168.1.90
	192.168.1.99
	192.168.1.134
	192.168.1.147
	192.168.1.170
	192.168.1.201
	192.168.1.230
	192.168.1.246
	192.168.1.249
	192.168.1.250

	Port	Protocol	State	Service	Version
●	135	tcp	open	msrpc	Microsoft Windows RPC
●	139	tcp	open	netbios-ssn	
●	445	tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds
●	1433	tcp	open	ms-sql-s	Microsoft SQL Server 2000 8.00.766.00; SP3a
●	1947	tcp	open	http	Aladdin HASP license manager 12.31

Figure 3 Details of open and closed ports of host system with IP Address 192.168.1.170

Figure 3 shows the list of open ports on host system with IP Address 192.168.1.170. It shows the port number, protocol used on that port, its state of being open or closed or filtered, type of service provided on that port and the version details.



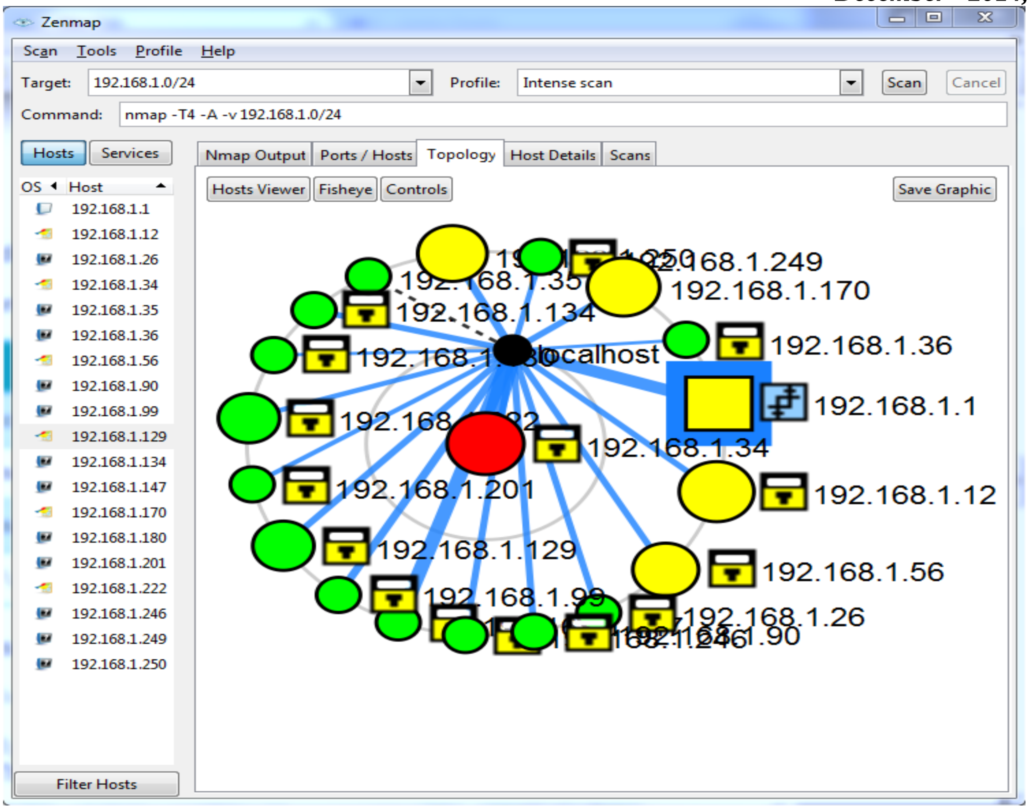
Target: 192.168.1.0/24
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.1.0/24

OS	Host
	192.168.1.1
	192.168.1.17
	192.168.1.26
	192.168.1.33
	192.168.1.34
	192.168.1.39
	192.168.1.56
	192.168.1.90
	192.168.1.99
	192.168.1.134
	192.168.1.147
	192.168.1.170
	192.168.1.201
	192.168.1.230
	192.168.1.246
	192.168.1.249
	192.168.1.250

```
⊟ 192.168.1.170
    ⊟ Host Status
        State:          up
        Open ports:     5
        Filtered ports: 0
        Closed ports:   995
        Scanned ports:  1000
        Up time:        Not available
        Last boot:      Not available
    ⊟ Addresses
        IPv4:   192.168.1.170
        IPv6:   Not available
        MAC:    70:71:BC:AF:F2:1A
    ⊟ Operating System
        Name:           Microsoft Windows XP SP2 or SP3, or Windows Server 2003
        Accuracy:       100%
        ⊞ Ports used
        ⊟ OS Classes
            Type             Vendor      OS Family   OS Generation   Accuracy
            general purpose  Microsoft   Windows     2003            100%
    ⊞ TCP Sequence
    ⊞ IP ID Sequence
    ⊞ TCP TS Sequence
```

Figure 4 Host details of IP Address 192.168.1.170.

Figure 4 outlays the host details of 192.168.1.170 which includes the host status that shows the total number of ports scanned, number of port available, number of filtered ports. It also shows IPv4 address of the host; IPv6 are not available, but MAC address reveals. Further, the type of operating system detected may be Microsoft Windows XP SP2 or Windows Server 2003. The accuracy with which this result has been obtained is 100% approximately.



Target: 192.168.1.0/24
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.1.0/24

192.168.1.1
192.168.1.12
192.168.1.26
192.168.1.34
192.168.1.35
192.168.1.36
192.168.1.56
192.168.1.90
192.168.1.99
192.168.1.129
192.168.1.134
192.168.1.147
192.168.1.170
192.168.1.180
192.168.1.201
192.168.1.222
192.168.1.246
192.168.1.249
192.168.1.250

Figure 5 Shows the topology structure of all discovered host

Figure 5 depicts topology formed for scanning all local hosts with their IP Address and connection links.

B. NESSUS

Nessus is a vulnerability scanner that search for and map systems for weakness in application, computer or their network. It identifies both internal and external network scan. Internal scan means scanning is performed within a particular router. External scan means scanning involves the hosts outside the particular router or a remote host. Nessus has the capability to multiple scanning of the hosts at a same time. The main advantage, nessus makes no assumptions for what services are running on what ports and it actively attempts to exploit identifies vulnerabilities.

Its main objective is to detect potential vulnerabilities on the target systems such vulnerabilities that allows a remote attacker to control or access sensitive information on a system, systems default settings, default password etc. Nessus Plug-ins uses its own scripting language NASL (Nessus Attack Scripting Language). The vulnerability identified by Nessus exists in four different types of severity levels - High, Medium, Low and Informational [13].

Nessus – Architecture: Nessus is based on client –server architecture. Each session is controlled by the client and the test is run on the server side. The Nessus server performs all of the scanning and security checks, which are implemented as plug-ins written in Nessus Attack Scripting Language (NASL).

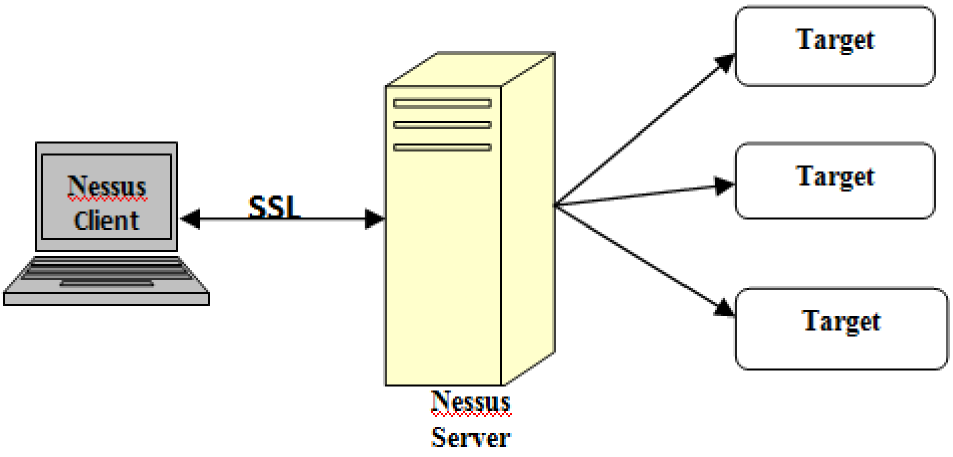
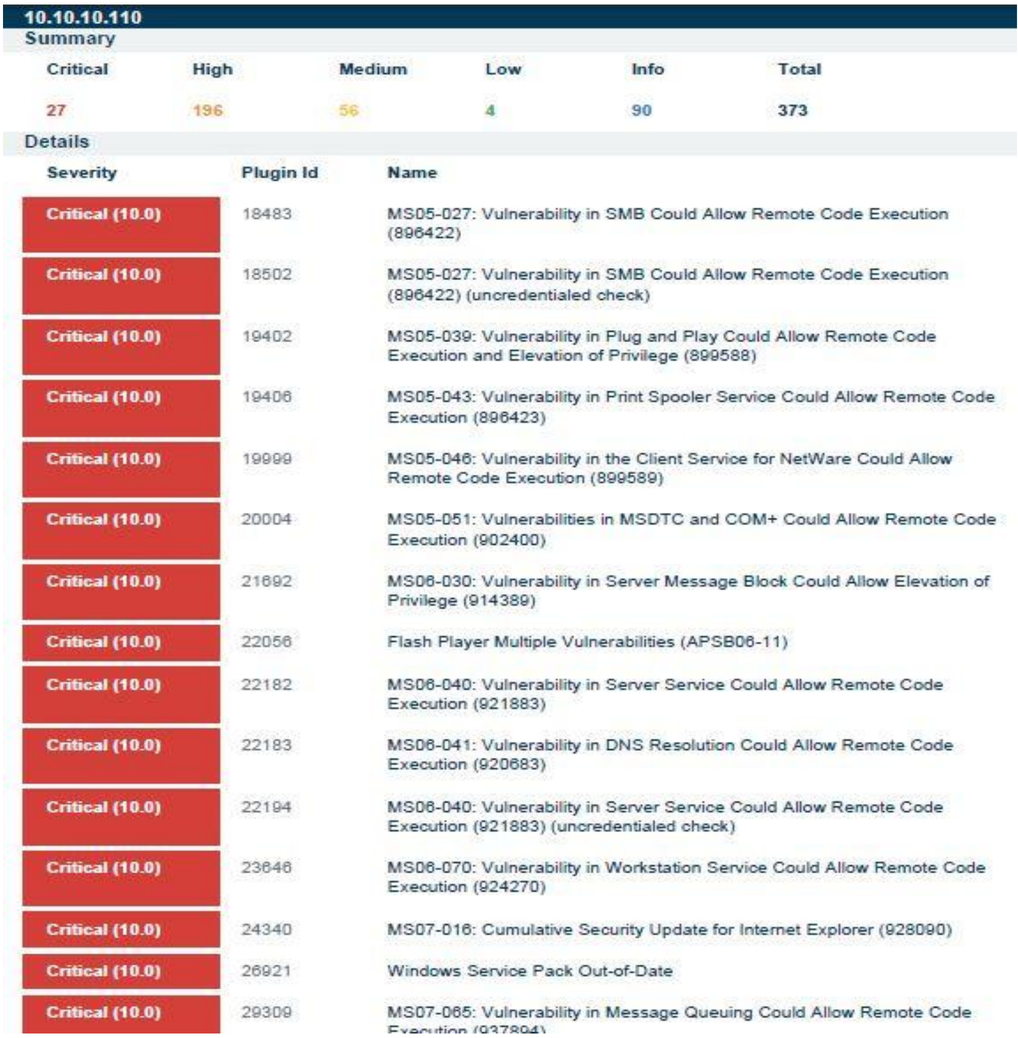


Figure 6 Client-server architecture of Nessus

We can scan vulnerability on multiple host system at simultaneously but here following figure depicts the results obtained for scanning a virtual machine with IP Address 10.10.10.110. It shows the number of vulnerability with severity as critical, high, medium, low and informational.



10.10.10.110

Summary

Critical	High	Medium	Low	Info	Total
27	196	56	4	90	373

Details

Severity	Plugin Id	Name
Critical (10.0)	18483	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422)
Critical (10.0)	18502	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)
Critical (10.0)	19402	MS05-039: Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege (899588)
Critical (10.0)	19406	MS05-043: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (896423)
Critical (10.0)	19999	MS05-046: Vulnerability in the Client Service for NetWare Could Allow Remote Code Execution (899589)
Critical (10.0)	20004	MS05-051: Vulnerabilities in MSDTC and COM+ Could Allow Remote Code Execution (902400)
Critical (10.0)	21692	MS06-030: Vulnerability in Server Message Block Could Allow Elevation of Privilege (914389)
Critical (10.0)	22056	Flash Player Multiple Vulnerabilities (APSB06-11)
Critical (10.0)	22182	MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883)
Critical (10.0)	22183	MS06-041: Vulnerability in DNS Resolution Could Allow Remote Code Execution (920683)
Critical (10.0)	22194	MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)
Critical (10.0)	23646	MS06-070: Vulnerability in Workstation Service Could Allow Remote Code Execution (924270)
Critical (10.0)	24340	MS07-016: Cumulative Security Update for Internet Explorer (928090)
Critical (10.0)	26921	Windows Service Pack Out-of-Date
Critical (10.0)	29309	MS07-065: Vulnerability in Message Queuing Could Allow Remote Code Execution (937894)

Figure 8. Vulnerability details for host with IP Address 10.10.10.110 using Nessus

Figure 8 shows the scan results for host system with IP Address 10.10.10.110 using Nessus scanner. It shows total 373 vulnerabilities where 27 critical, 196 High, 56 Medium, 4 Low, 90 Informal. The range of either being high, medium, low or informal type is also given. For instance, Windows Service pack out-of-date is belongs to critical category ranging to 10.0 with its plug-in ID given as 26921.

IV. COMPARION OF VA TOOLS

Table 2 shows comparative view of the VA tools described above on the basis of the vulnerabilities these tools detect.

Table2. Comparative view of the vulnerabilities detected by the VA tools

Vulnerability	Nmap	Nessus
FTP 21 Anonymous FTP Access	YES	YES
FTP 21 VsFTPd Smiley Face Backdoor	NO	YES
FTP 2121 ProFTPD Vulnerabilities	NO	NO
SSH 22 Weak Host Keys	NO	YES
PHP-CGI Query String Parameter Injection	YES	YES
CIFS Null Sessions	YES	YES
INGRESLOCK 1524 known backdoor drops to root shell	NO	NO
NFS 2049	NO	NO
MYSQL 3306 weak auth(root with no password)	YES	YES
RMI REGISTRY 1099 Insecure Default Config	NO	NO
DISTCCd 3632 dsitributed compiler	NO	NO
VNC 5900 weak auth(password)	NO	NO
IRC 6667 Unreal IRCd Backdoor	YES	NO
Tomcat 8180 weak auth	YES	YES

V. CONCLUSION

There are number of techniques available to list the vulnerabilities present in the remote host. Vulnerability assessment plays an important role in securing the organizations network system. Our observations shows that different tool detect different type of vulnerabilities. Hence a single tool is not capable of detecting all present vulnerabilities. This paper addressed two very popular VA tools. Both of them work on different criteria of detecting vulnerabilities. Nmap is very powerful tool for port scanning and gives the state of ports of target host. On the other hand, Nessus have the capability to discover the state of port and also it detects the flaws on particular system with a recommended solution to fix it. Nessus can import scan results done by another tools like Nmap etc. and perform vulnerability scan accordingly. Thus both the tools have one thing common that they makes the top managements work easier for network security.

REFERENCES

[1] Xia Yiming, 2006. "*Security Vulnerability Detection Study Based on Static Analysis*," Computer Science, 33(10), pp. 279-283, Symposium, 18-22 May 2008, pp. 143-157.

[2] Golnaz Elahi, Eric Yu, and Nicola Zannone,"*Security Risk Management by Qualitative Vulnerability Analysis*", IEEE, Third International Workshop on Security Measurements and Metrics, 2011.

[3] P. Zhang, J. Shang, and Z. Liang, "Application of Multi-Agent Model in Vulnerability Detection System", IEEE, First IEEE International Symposium, 2007.

[4] G. Corral, A. Zaballos, X. Cadenas, and A. Grane, "A Distributed Vulnerability Detection System for an Intranet", IEEE, the 39th annual 2005 international carnahan conference, 2005.

[5] http://www.insecure.org/nmap/index.html, 18-12-2014.

[6] http://www.tenable.com/products/nessus, 18-12-2014

[7] Peng Li and Baojiang Cui, December, 2010, "A Comparative Study on Software Vulnerability Static Analysis Techniques and Tools", in Proceedings of the IEEE International Conference on Information Theory and Information Security (ICITIS), IEEE International conference, 2010.

[8] http://cve.mitre.org/

[9] Ofir Arkin, Network Scanning Techniques, PubliCom, 1999.

[10] Fyodor, *Port scanning techniques*, http://nmap.org/book/man-port-scanning-techniques.html, 18-12-2014.

[11] K. Wei Lye and J. M. Wing., 2005."*Game Strategies in network security*", Int.J. In Sec. vol. 4, no. 1-2, pp 71-86.

[12] James Messer, "*Secrets of Network Cartography: A Comprehensive Guide to nmap*", published by A Network Uptime.com, e-book PDF edition 2005.

[13] http://en.wikipedia.org/wiki/Nessus_(software), 19th November 2014.

[14] nmap.org/docs/discovery.pdf, 19th November 2014.