ISSN:2229-6093

NETWORK SECURITY SCANNER

G. Murali[1] M.Pranavi[2] Y.Navateja[3] K.Bhargavi[4]

1. Assistant Professor, Department of Computer Science and Engineering, JNTUA- Pulivendula, AP, India.
2,3,4. Final year B.Tech students, Department of Computer Science and Engineering, JNTUA- Pulivendula, AP, India.

ABSTRACT:

Network Security Scanner (NSS) is a tool that allows auditing and monitoring remote network computers for possible vulnerabilities, checks your network for all potential methods that a hacker might use to attack it. Network Security Scanner is a complete networking utilities package that includes a wide range of tools for network security auditing, vulnerability Auditing, scanning, monitoring and more.

Network Security Scanner (NSS) is an easy to use, intuitive network security scanner that can quickly scan and audit your network computers for vulnerabilities, exploits, and information enumerations. Vulnerability management is an on-going process that protects your valuable data and it is a key component of an effective information security strategy, which provides comprehensive, preemptive protection against threats to your enterprise security. N.S.S is built on an architecture that allows for high reliability and scalability that caters for both medium and large sized networks.

NSS consists of six modules. They are Host Scanning, Port Scanning, Pinging, NSLookup, Vulnerability Auditing and Trace route. NSS also performs live host detection, operating system identification, SNMP Auditing. Finds rouge services and open TCP and UDP ports.

The ability varies to perform scanning over the network identifying the live hosts and guess the operating system of the remote hosts and installed programs into the remote hosts. Apart identifying the live hosts we could map the ports and list the services which are running in the host.

Keywords— **Network Security Scanner, Host Scanning, Port Scanning, Pinging, NSLookup, Vulnerability Auditing, Trace Route.**

1. INTRODUCTION

Network Scanner or Network Enumeration is a computer program used to retrieve user names, and info on groups, shares and services of networked computers. This aims to scan networks for vulnerabilities in the designed Network architecture. A vulnerability exits for every program or artificial design and this hole may be used by the intruder to exploit that network glitch to gain entry to the network and perform malicious activities which includes stealing of personnel data / installing a program which acts like a bot and reports all the activities to the intruder. We being White Hats, perform such audits over the network to identify the vulnerabilities and patch them or apply the countermeasures in according to the identified vulnerability.

The ability varies to perform scanning over the network identifying the live hosts and guess the operating system of the remote hosts and installed programs into the remote hosts. Apart identifying the live hosts we would map the ports and list the services which are running in the host. Overall, we can reveal and catalog a variety of information, including installed software, shares, users, drives, hot fixes, NetBios, RPC, SQL and SNMP information, open ports, which is called Host Discovery.

There is prevention used by the Security administrators so, that any one cannot scan their network connected to them remotely. But in this research project we would study the cases included in network probing and detecting the vulnerabilities internally and externally of the infrastructure. Technically there are default ports enabled in the network connected hosts, which includes 137, 138, 139, and 445 which are essential for network communication. But, this is proven to be a flaw as intruders can create a ESTABLISHED connection without our knowledge and as a security expert we should patch it applying countermeasures accordingly (an internal exploit). This study includes internal and external exploiting of network and understanding the countermeasures.

1.1MOTIVATION

In today's dynamic threat environment, there is a need of having proactive security solution to identify potential weaknesses and help prioritize which need to be addressed first. As vulnerabilities are commonly existing in every program to exploit that network glitch and to gain entry to the network the intruder may use that hole and perform malicious activities like stealing of personnel data / installing a program which acts like a bot and reports all the activities to the intruder.

Network Security Scanner is to find Security vulnerabilities in one or more systems connected to a network. The vulnerabilities should be Security Exploitable by someone who does not have prior authorization to use the target system the vulnerabilities should be Security Exploitable. The working of Network Security Scanner is done by testing for available services on a target machine, and known Security Exploit's against matching services are tried out.

1.2OBJECTIVES

The objectives of a Network Security Scanner are

- To find a way to gain unauthorized access to any of the target systems, or to cause a Denial of Service on any of those systems.
- Identifies security vulnerabilities and recommends action (or solutions).
- Easily creates different types (intense, normal) of scans and vulnerability tests.
- To list and detect blacklisted applications.
- To perform check for programs that run automatically (potential Trojans/Viruses).
- To find all shares on the network.
- To perform fast TCP/UDP port scanning.
- To find unused local users and groups.
- To find out if OS is advertising too much information.
- To perform simultaneous scans through the multithread scan engine.
- To provide NetBIOS hostname, currently logged username.
- To provide a detailed info of users, shares and registry information from remote computer (Windows).
- To identify Trojans/Viruses in remote PC's.
- Most scanners fail to bypass the firewall, which is done through intense scan and this tool includes the feature.
- The output can be diverted to a file so as to store the audit for further reference. It is also capable of identifying the Trojans/Viruses in Remote PC's.

2. PROJECT DESCRIPTION

Security scanner is designed to scan the network for flaws using scripts which would discover the vulnerabilities of a host in the network. It mainly includes

- Scanning of vulnerable servers

In scanning for vulnerable servers, for each known vulnerable script the scanner will attempt to connect to and exploit the targeted service. The main aim is to test a server for vulnerable scripts and exploits including Operating system, service, firewall, Remote Procedure Call and remote administration vulnerabilities.

To find security vulnerabilities on ports other than the standard HTTP and HTTP ports it is necessary for the scanner to try to connect on other ports and send carefully constructed network packets to try to exploit certain vulnerabilities. These packets may include buffer overrun code, commonly used/default username and passwords and other known methods to access a server on each port.

The project consists of total of 5 modules as listed below

- IP Scanner
- Vulnerability Audit
- Port Scanner
- NS Lookup
- Trace Route

2.1IPSCANNER

IPscanner tool used to test whether a particular host is reachable across an IP network; it is also used to self test the network interface card of the computer, or as a speed test.

The work of ping is done by sending ICMP “echo request” packets to the target host and listening for ICMP “echo response” replies. The round trip time is measured by ping also records any packet loss and prints when finished a statistical summary of the echo response packets received, the minimum, mean, max and in some versions the standard deviation of the round trip time.

ICMP packet

<table>
<tr><th></th><th>Bit 0 – 7</th><th>Bit8- 15</th><th>Bit16-23</th><th>Bit 24 - 31</th></tr>
<tr><td rowspan="5"><b>IP Header (160 bits OR 20 Bytes)</b></td><td>Version/IHL</td><td>Type of service</td><td colspan="2">Length</td></tr>
<tr><td colspan="2">Identification</td><td colspan="2"><i>flags</i> and <i>offset</i></td></tr>
<tr><td>Time To Live(TTL)</td><td>Protocol</td><td colspan="2">Checksum</td></tr>
<tr><td colspan="4">Source IP address</td></tr>
<tr><td colspan="4">Destination IP address</td></tr>
<tr><td rowspan="3"><b>ICMP Payload (64+ bits OR 8+ Bytes)</b></td><td>Type of message</td><td>Code</td><td colspan="2">Checksum</td></tr>
<tr><td colspan="4">Quench</td></tr>
<tr><td colspan="4">Data (<i>optional</i>)</td></tr>
</table>

Figure 3.1 Generic Composition Of An ICMP Packet

- Header (in blue):

Protocol set to 1 and *Type of Service* set to 0.

- Payload (in red):

Type of ICMP message (8 bits)

Code (8 bits)

Checksum (16 bits), calculated with the ICMP part of the packet (the header is not used)

The ICMP 'Quench' (32 bits) field, which in this case (ICMP echo request and replies), will be composed of identifier (16 bits) and sequence number (16 bits).

Data load for the different kind of answers (Can be an arbitrary length, left to implementation detail. It should be less than the maximum MTU of the network).

2.2VULNERABILITY AUDIT

Vulnerability scanner is a piece of software designed to search a network host for open ports. This is mostly used by administrators for checking the security of their networks and by hackers to compromise it. To port scan a host is for scanning listening ports on a single target host. For a specific listening port to port sweep is for scanning multiple hosts. The latter is typically used in searching for a specific service; for example, to port sweep looking for hosts listening on TCP/UDP port 1433 an SQL based computers might be used.

TCP/IP is the protocol stack most commonly used in the Internet today. Hosts and host services are referred in this system using two components: an address and a port number. The distinct and usable port numbers that are available are 65536. Only limited range of numbers are used by most services; when the service becomes important enough these numbers will be eventually become assigned by the IANA.

2.3PORTSCANNER

TCP scanning

The simplest port scanners use the operating system’s network functions and are generally the next option to go to when SYN is not a feasible option. The mode connect scan is called by the Nmap which is named after the UNIX connect () system call. The port scanner immediately closes the connection if a port which opens the operating system completes the TCP three-way handshake. Otherwise an error code is returned. The advantage of this mode scan is that the user doesn't require special privileges. However, the prevention of low-level control is done by using the OS network functions, so this scan type is less commonly used.

UDP Scanning

As there are technical challenges, UDP scanning is also possible. There is no equivalent to a TCP SYN packet as UDP is a connectionless protocol. If a UDP packet is sent to a port that is not open, with an ICMP port unreachable message the system will be responded. This scanning method is used by most UDP port scanners; to infer that a port is open the absence of a response is used. The false report that the port is open will be appeared by this method if the firewall blocks a port. All the ports will appear open if the message is blocked which is port unreachable. ICMP rate limiting also affects this method.

Hoping to bring about an application layer response an alternative approach is to send application-specific UDP packets. For example, when DNS query is sent to port 53 the response is received, if a DNS server is present. For identifying open ports it is more reliable. The alternative approach is limited to scanning ports for which an application specific probe packet is available. Generally some tools (e.g. nmap) have probes for less than 20 UDP services, while some commercial tools (e.g. nessus) have much more as 70. The service is organized not to respond to the particular probe packet in some cases though the service may be listening on the port.

Some scanners offer a hybrid method for coping different limitations of each approach. For example, using nmap with the -sUV option will start by using the ICMP port unreachable method, marking all ports as either "closed" or "open|filtered". The ports that are probed for application responses are open|filtered and marked as "open" if one is received.

2.4NSLOOKUP

Nslookup is a computer program used in Windows and UNIX to query Domain Name System (DNS) servers to find DNS details, including IP addresses of a particular computer, MX records for a domain and the NS servers of a domain. The "name server lookup" is the representation of *nslookup*. The most common version of the program is included as part of the BIND package.

The modern alternatives which also ship with BIND to nslookup are the "host" and "dig" programs.

2.5TRACEROUTE

To retrieve the route taken by packets across an IP network in computer network the tool used is Trace route. Traceroute6 which is an IPv6 variant is also available in great extent. On all Unix-like operating systems the trace route tool is practically available. Like trace path on modern Linux installations and tracert on Microsoft Windows operating systems similar functionality variants are also available. The path ping is also provided by Windows NT-based operating systems, which shows similar functionality.

The working of Trace route is done by increasing the "time-to-live" value of packets sent from each successive batch. The time-to-live (TTL) value of one (implying that they are not forwarded by the next router and make only a single hop) is given for the first three packets sent. The TTL value of 2 is given for next three packets, and so on. Normally the host decrements the TTL value by one when a packet is passed through a host and to the next host the packet is forwarded. A packet for which a TTL is one reaches a host, the packet is discarded by host and an ICMP time exceeded (type 11) packet is sent to the sender. The returning packets are used by the trace route utility to generate a list of hosts that the packets have traversed end route to the destination. The three timestamp values are the delay (aka latency) values typically in milliseconds (ms) for each host along the path are returned for each packet in the batch. A star (asterisk) is traditionally printed when the packet within the expected timeout window is not returned. The real hosts may not be listed by the trace route. It indicates that the first host is at one hop, the second host at two hops, etc. The guarantee is not given by the IP that all the packets follow the same route. The hop will be skipped in the output if there is no reply from the host at hop number N.

UDP data grams with destination ports number from 33434 to 33534 are used by the trace route utility by default on modern UNIX and Linux-based operating systems. As used by the Windows tracert utility to specify use of ICMP echo request (type 8) instead, usually has an option is used by trace route utility. You will need to allow both protocols in limit through your firewall (UDP with ports from 33434 to 33534 and ICMP type 8) if you have a firewall and if there is a need to trace route to work from both machines (Unix/Linux and Windows). The tcp trace route or lft are the trace route implementations that use TCP packets. The utility that is introduced with Windows NT combines ping and trace route functionality is Path ping. The enhanced version of ICMP trace route that is available for UNIX and Windows systems is mtr (My trace route). Being sent to the originator all implementations of trace route depend on ICMP (type 11) packets. To use ICMP packets (-I) the implementations of trace route shipped with FreeBSD, OpenBSD, and NetBSD includes an option. An option is included by the implementations shipped with FreeBSD and OpenBSD to use any arbitrary protocol (-P) such as TCP.

For network troubleshooting often used tool is trace route. To identify the path taken on the network to reach a particular destination it allows the user showing a list of routers traversed. This helps in detecting routing problems or firewalls that may blocks access to a site. Around a given host to gather information about network infrastructure and IP ranges penetration testers use trace route. During the data download also it can be used, if there are multiple mirrors available for the same piece of data, each mirror can be traced to get a good idea of which mirror would be the fastest to use. The detailed information that is supplied about the pathways was considered to be acceptable and convenient in the early days of the Internet. But it was considered to be questionable for privacy and security reasons in later. To acquire sensitive information about a company's network architecture hackers frequently use trace route information as a way. Intermediate routers can be quickly mapped out by the hackers for known destinations on a company's network architecture using the trace route command.

While trace route was unrestricted during the early days of the Internet in a great extent, trace route requests are blocked by many networks in these days, or de-prioritize the ICMP time exceeded message that is needed to calculate round trip time. However, except at network end-points filtering traffic is a controversial practice.

3. CONCLUSION

Finally we conclude that this system helps in improving the efficiency and performance of the system. The system provides an easy way of solving the problems like programs runs automatically (potential Trojans/Viruses), firewall bypassing, sending malformed packets, ICMP rate limiting, quick mapping of intermediate routers by hackers. The time taken to solve a particular problem will be decreased. The client need not move from his place to get his problem solved. This factor shows the importance of the project.

The functionalities done in Network Security Scanner were well implemented successfully, which ensures the basic functionalities for the users.

REFERENCES

[1]. Emmanuel Remy, 2001, “Generalities on java”.

http://pagespersoorange.fr/emmanuel.remy/Java/Generalities/Generalities.htm

[2]. E. Stewart Lee, 1999, “Essays about Computer Security” Cambridge.

[3]. Bank off, Greg, George Frerks and Dorothea Hilhorst., 2004, “Mapping Vulnerability”. Sterling: Earth scan.

[4]. Birkman, Joern (editor), 2006, “Measuring Vulnerability to Natural Hazards- towards Disaster Resilient Societies” UNU Press.

[5]. Complete reference for java Edition 4, By Herb Scheldt.

[6]. Thinking in java, By Bruce Eckel

[7]. JSP reference by visual builder team

[8].PortScanner: http://www.linuxreviews.org/dictionary/Port scanner.

[9]. Documents the Nmap Security Scanner and provides it for download. http://www.nmap.org

[10]. Main site, offering security news/updates, exploits world archive and other misc. http://www.insecure.org

[11]. Wikipedia, free Encyclopedia, online collaborative, universal and multilingual, 2008. http://www.eikipedia.org/

[12]. The official sites of JAVA.

http://www.java.sun.com
http://www.java2s.com
http://www.java4students.com