

Advanced Network Scanning

Ashiqur Rahman¹, Kantibhusan Roy Kawshik², Atik Ahmed Sourav³,
Al-Amin Gaji⁴

¹(M.Sc In Information Technology (IT), Jahangirnagar University, Bangladesh)

²(EEE, Royal University Of Dhaka, Bangladesh)

³(CSE, Royal University Of Dhaka, Bangladesh)

⁴(CSE, Royal University Of Dhaka, Bangladesh)

ABSTRACT: Network scanning is a procedure for identifying active hosts on a network, either for the purpose of attacking them or for network security assessment. Scanning procedures, such as ping sweeps and port scans, return information about which IP addresses map to live hosts that are active on the Internet and what services they offer. Another scanning method, inverse mapping, returns information about what IP addresses do not map to live hosts; this enables an attacker to make assumptions about viable addresses. Scanning is one of three components of intelligence gathering for an attacker. In the footprinting phase, the attacker creates a profile of the target organization, with information such as its domain name system (DNS) and e-mail servers, and its IP address range. Most of this information is available online. In the scanning phase, the attacker finds information about the specific IP addresses that can be accessed over the Internet, their operating systems, the system architecture, and the services running on each computer. In the enumeration phase, the attacker gathers information such as network user and group names, routing tables, and Simple Network Management Protocol (SNMP) data.

Keywords: HTTP, Telnet, DNS, TCP, UDP.

I. INTRODUCTION

Network scanning consists of network port scanning as well as vulnerability scanning. Network port scanning refers to the method of sending data packets via the network to a computing system's specified service port numbers (for example, port 23 for Telnet, port 80 for HTTP and so on). This is to identify the available network services on that particular system. This procedure is effective for troubleshooting system issues or for tightening the system's security [1]. Vulnerability scanning is a method used to discover known vulnerabilities of computing systems available on a network. It helps to detect specific weak spots in an application software or the operating system (OS), which could be used to crash the system or compromise it for undesired purposes. Network port scanning as well as vulnerability scanning is an information-gathering technique, but when carried out by anonymous individuals, these are viewed as a prelude to an attack. Network scanning processes, like port scans and ping sweeps, return details about which IP addresses map to active live hosts and the type of services they provide. Another network scanning method known as inverse mapping gathers details about IP addresses that do not map to live hosts, which helps an attacker to focus on feasible addresses. Network scanning is one of three important methods used by an attacker to gather information. During the footprint stage, the attacker makes a profile of the targeted organization. This includes data such as the organization's domain name system (DNS) and e-mail servers, in addition to its IP address range. During the scanning stage, the attacker discovers details about the specified IP addresses that could be accessed online, their system architecture, their OSs and the services running on every computer [2]. During the enumeration stage, the attacker collects data, including routing tables, network user and group names, Simple Network Management Protocol (SNMP) data and so on. Network scanning refers to the use of a computer network to gather information regarding computing systems. Network scanning is mainly used for security assessment, system maintenance, and also for performing attacks by hackers.

The purpose of network scanning is as follows:

- Recognize available UDP and TCP network services running on the targeted hosts
- Recognize filtering systems between the user and the targeted hosts

- Determine the operating systems (OSs) in use by assessing IP responses
- Evaluate the target host's TCP sequence number predictability to determine sequence prediction attack and TCP spoofing

II. FEATURES

Flexible: Supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles. This includes many port scanning mechanisms (both TCP & UDP), OS detection, version detection, ping sweeps, and more. See the documentation page.

Powerful: Nmap has been used to scan huge networks of literally hundreds of thousands of machines.

Portable: Most operating systems are supported, including Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, and more.

Easy: While Nmap offers a rich set of advanced features for power users, you can start out as simply as "nmap -v -A target host". Both traditional command line and graphical (GUI) versions are available to suit your preference. Binaries are available for those who do not wish to compile Nmap from source.

Free: The primary goals of the Nmap Project is to help make the Internet a little more secure and to provide administrators/auditors/hackers with an advanced tool for exploring their networks. Nmap is available for free download, and also comes with full source code that you may modify and redistribute under the terms of the license.

Well Documented: Significant effort has been put into comprehensive and up-to-date man pages, whitepapers, and tutorials.

Supported: While Nmap comes with no warranty, it is well supported by a vibrant community of developers and users. Most of this interaction occurs on the Nmap mailing lists. Most bug reports and questions should be sent to the nmap-dev list, but only after you read the guidelines. We recommend that all users subscribe to the low-traffic nmap-hackers announcement list. You can also find Nmap on Facebook and Twitter. For real-time chat, join the #nmap channel on Freenode or EFNet.

Acclaimed: Nmap has won numerous awards, including "Information Security Product of the Year" by Linux Journal, Info World and Codetalker Digest. It has been featured in hundreds of magazine articles, several movies, dozens of books, and one comic book series [3].

Popular: Thousands of people download Nmap every day, and it is included with many operating systems (Redhat Linux, Debian Linux, Gentoo, FreeBSD, OpenBSD, etc). It is among the top ten (out of 30,000) programs at the Freshmeat.Net repository. This is important because it lends Nmap its vibrant development and user support communities.

III. HOSTS & PINGS

LIVE Host Scanning

- Identify Live Hosts – Angry IP Scanner, nmap
- Identify Open Ports – nmap -sS/sT/sU/sX/ -v4 <ip-address>
- Identify Services – nmap -sS -sV -v4 <ip-address>
- Network Pings/Sweeps (ICMP, TCP, UDP)
- NMAP

ICMP Ping sweep

PE – ICMP Echo

PP – ICMP Timestamp

MAP, HPING (NPING), Super Scan

NMAP discovery option - sn (ICMP echo request, TCP SYN to port 443, TCP ACK to port 80, and an ICMP timestamp request) e.g. nmap -sn -PE --send-IP range

Service Sweep (TCP/UDP)

Target more common ports - web http/https (80/443), telnet (23), ftp (21), e.g. nmap -sS -p80 --open -Pn ip_range

- URG – indicates that the URGent pointer field is significant

- ACK – indicates that the ACKnowledgment field is significant (Sometimes abbreviated by tcpdump as ".")
- PSH – Push function
- RST – Reset the connection (Seen on rejected connections)
- SYN – Synchronize sequence numbers (Seen on new connections)
- FIN – No more data from sender (Seen after a connection is closed)

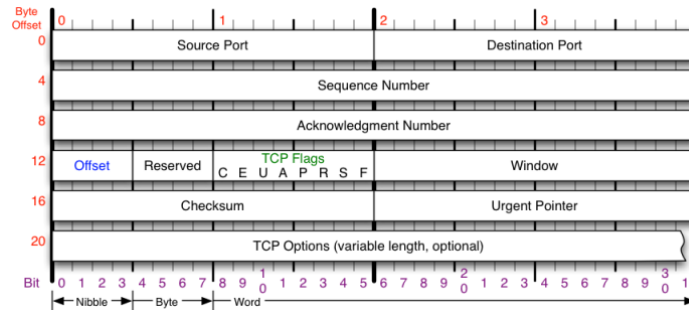


Fig 1: Port & TCP Number



Fig 2: Source & Destination

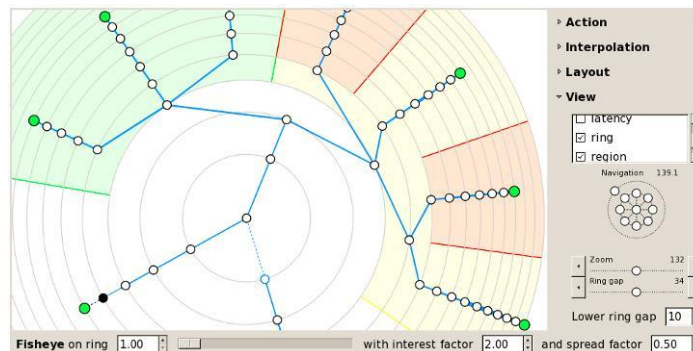


Fig 3: Networking Architecture

IV. ADVANCED IP SCANNER

Reliable and free network scanner to analyses LAN. The program shows all network devices, gives you access to shared folders and FTP servers, provides remote control of computers (via RDP and Radmin), and can even remotely switch computers off. It is easy to use and runs as a portable edition. It should be the first choice for every network admin.

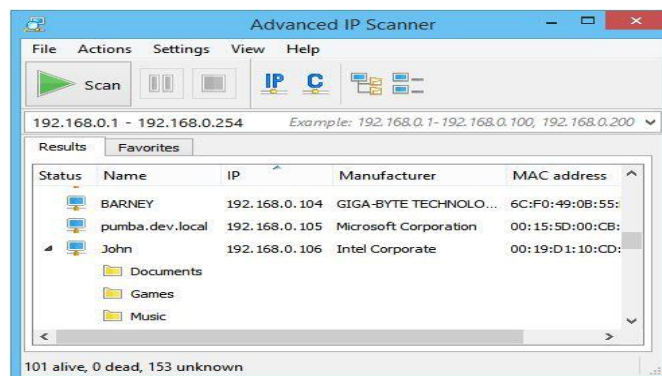


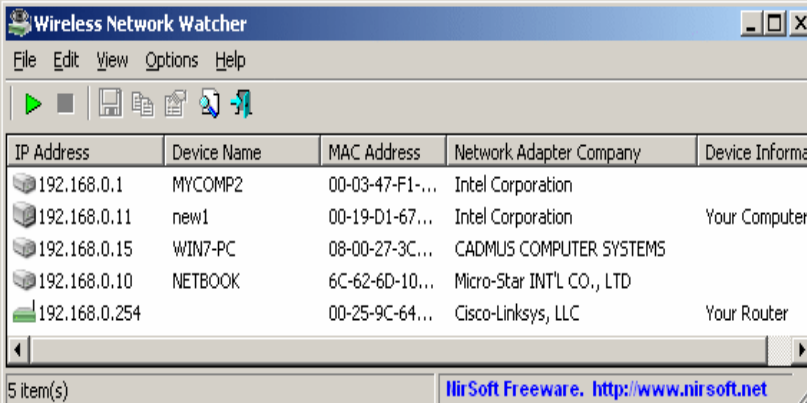
Fig 4: Advanced IP Scanner

V. PATCH MANAGEMENT

Patch management is vital to any business that takes security seriously. Network security breaches are most commonly caused by missing patches in your operating systems and other applications. Updating all of these manually every time an update is available takes a huge amount of time and commitment in the IT department. Automating this process is the best way to go. One of the greatest strengths of GFI LanGuard is its ability to manage patching for the most popular operating systems and other applications. Below you can find a list of all the products supported by GFI LanGuard [4]. More than 60,000 vulnerability assessments are carried out across your networks, including virtual environments, mobile and network devices. GFI LanGuard scans your operating systems, virtual environments and installed applications through vulnerability check databases such as OVAL and SANS Top 20. GFI LanGuard enables you to analyze the state of your network security, identify risks and address how to take action before it is compromised. GFI LanGuard provides a detailed analysis of the state of your network. This includes applications or default configurations posing a security risk. GFI LanGuard also gives you a complete picture of installed applications; hardware on your network; mobile devices that connect to the Exchange servers; the state of security applications (antivirus, anti-spam, firewalls, etc.); open ports; and any existing shares and services running on your machines

VI. WIRELESS NETWORKS

Wireless Network Watcher is a small utility that scans your wireless network and displays the list of all computers and devices that are currently connected to your network [5]. For every computer or device that is connected to your network, the following information is displayed: IP address, MAC address, the company that manufactured the network card, and optionally the computer name. We can also export the connected devices list into html/xml/csv/text file, or copy the list to the clipboard and then paste into Excel or other spreadsheet application.



IP Address	Device Name	MAC Address	Network Adapter Company	Device Information
192.168.0.1	MYCOMP2	00-03-47-F1-...	Intel Corporation	
192.168.0.11	new1	00-19-D1-67-...	Intel Corporation	Your Computer
192.168.0.15	WIN7-PC	08-00-27-3C-...	CADMIUS COMPUTER SYSTEMS	
192.168.0.10	NETBOOK	6C-62-6D-10-...	Micro-Star INT'L CO., LTD	
192.168.0.254		00-25-9C-64-...	Cisco-Linksys, LLC	Your Router

System Requirements and Limitations

- This utility works on Windows 2000, Windows XP, Windows Server 2003/2008, Windows Vista, Windows 7, Windows 8, and Windows 10.
- This utility can only scan a wireless network that you're currently connected to. It cannot scan other wireless networks.
- In rare cases, it's possible that Wireless Network Watcher won't detect the correct wireless network adapter, and then you should go to 'Advanced Options' window (F9), and manually choose the correct network adapter.
- Although this utility is officially designed for wireless networks, you can also use it to scan a small wired network.

VII. PATCH MANAGEMENT

IP Address: IP Address of the device or computer.

Device Name: The name of the device or computer. This field may remain empty if the computer or the device doesn't provide its name.

MAC Address: The MAC address of the network adapter.

Network Adapter Company: The Company that manufactured the network adapter, according to the MAC Address. This column can help you to detect the type of the device or computer. For example, if the company name is Apple, the device is probably a Mac computer, iPhone, or iPad. If the company name is Nokia, the device is probably a cellular phone of Nokia. By default, this utility uses an internal MAC addresses database stored inside the .exe file, but it's not always updated with the latest MAC address assignments. Folder where WNetWatcher.exe is located. When you run WNetWatcher.exe, it'll automatically load and use the external oui.txt instead of the internal MAC addresses database.

Device Information: This column displays 'Your Computer' if the device is the computer that you currently use. This column displays 'Your Router' if the device is the wireless router.

User Text: You can assign your own text to any device detected by WNetWatcher. By default, this field is filled with the device name. In order to change the User Text, simply double-click the item and type the desired text.

/cfg<Filename>	Start Wireless Network Watcher with the specified configuration file. For example: WNetWatcher.exe /cfg "c:\config\wnw.cfg" WNetWatcher.exe /cfg "%AppData%\WNetWatcher.cfg"
/stext<Filename>	Scan your network, and save the network devices list into a regular text file.
/stab <Filename>	Scan your network, and save the network devices list into a tab-delimited text file.
/scomma<Filename>	Scan your network, and save the network devices list into a comma-delimited text file (csv).
/stabular<Filename>	Scan your network, and save the network devices list into a tabular text file.
/shtml<Filename>	Scan your network, and save the network devices list into HTML file (Horizontal).
/sverhtml<Filename>	Scan your network, and save the network devices list into HTML file (Vertical).
/sxml<Filename>	Scan your network, and save the network devices list into XML file.

VIII. CONCLUSION

With increasingly sophisticated attacks on the rise, the ability to quickly mitigate network vulnerabilities is imperative. Vulnerabilities if left undetected pose a serious security threat to enterprise systems and can leave vital corporate data exposed to attacks by hackers. For organizations, it means extended system downtimes and huge loss of revenue and productivity. Vulnerability Assessment is a process of identifying the effectiveness of an enterprise network's security posture. The process qualifies the type of assets in the network, the probable areas for compromise and how to remediate vulnerabilities and protect assets. The core function of Security Manager Plus, network security scanner, is vulnerability scanning & detection of industry-known vulnerabilities on network assets and to offer remediation solutions. Security Manager Plus enables us to scan assets and asset groups, view vulnerable assets and their complete security information, e-mail scan reports and take appropriate action to safeguard our assets based on the remediation solutions provided.

REFERENCES

- [1]. M. S. Johns. Identification Protocol. RFC 1413, February 1993. <http://www.ietf.org/rfc/rfc1413.txt>; accessed Jan 07, 2008.
- [2]. J. Jung. Real-Time Detection of Malicious Network Activity Using Stochastic Models. PhD thesis, Massachusetts Institute of Technology, 2006.
- [3]. J. Jung, V. Paxson, A. Berger, and H. Balakrishnan. Fast portscan detection using sequential hypothesis testing. In IEEE Symposium on Security and Privacy, pages 211–225, 2004.
- [4]. C. Kruegel, T. Toth, and E. Kirda. Service specific anomaly detection for intrusion detection. Technical report, Technical University Vienna, Vienna, Austria. TU-1841-2002-28, 2002.
- [5]. C. Leckie and R. Kotagiri. A probabilistic approach to detecting network scans. In Eighth IEEE Network Operations and Management Symposium (NOMS 2002), pages 359–372, 2002.