Evaluation of Network Port Scanning Tools

Nazar El-Nazeer and Kevin Daimi
Department of Mathematics, Computer Science and Software Engineering
University of Detroit Mercy,
4001 McNichols Road, Detroit, MI 48221
{elnazen, daimikj}@udmercy.edu

ABSTRACT

Neglecting network port scans could result in unavoidable consequences. Network attackers continuously monitor and check communication ports looking for any open port. To protect computers and networks, computers need to be safeguarded against applications that aren't required by any function currently in use. To accomplish this, the available ports and the applications utilizing them should be determined. This paper attempts to evaluate eight port scanning tools based on fifteen criterions. The criteria were reached after fully testing each tool. The outcomes of the evaluation process are discussed.

Keywords

Network Security, Evaluation Criteria, Network Security Tools, Network Port Scanning

I. INTRODUCTION

A computer network is any group of independent computers and devices that communicate with one another over a shared network channel. With networking, people can share files, printers, and storage devices. Furthermore, they can exchange e-mail, disclose internet links of common interest, or conduct video conferences. Computer Networks are used for business, home, mobile, and social applications. There are different categories of networks including Local Area Networks, Wide Area Networks, Wireless Network, and Internetworks. Within a network, computers and devices communicate with each other via protocols [3], [11], and [27].

It is currently almost impossible to end or weaken the ties between humans and computer networks. People rely on computer networks to accomplish many essential and critical tasks. Therefore, it is very demanding to secure our networks. Network security implies protecting data and information from attacks during their transmission from the source to destination. Attackers can detect the vulnerabilities in networks and possibly pose enormous threats in these situations. To prevent problems, cryptology provides the most promising measures to deter, prevent, detect, and correct security violations.

To protect computer networks, a number of protection tasks need to be implemented. These tasks are needed to enforce the security for wireless network, electronic mail, IP, and at the transport level. Furthermore, these tasks should efficiently deal with intruders and malicious software [23].

Internet and web are tremendously vulnerable to various attacks. Therefore securing web services is a critical requirement. In particular, security at the transport layer must never be overlooked. The subdivision of the Internet by the transport layer presents ample outcomes both in the way in which business is performed on the network and with regard to the vulnerability caused by the openness of the network [6]. Patel et al [20] presented a system capable of granting a high level of security and performance. It permits each host to shield itself from untrusted transport code and to guarantee that this code will not impair other network users. For wireless networks, the Wireless Transport Layer Security (WTLS) should efficiently provide the highest level of protection. To achieve this, an efficient architecture for the hardware implementation of WTLS is demanding. Such architecture must support bulk encryption, authentication and data integrity, and operate alternatively for a set of ciphers, such as IDEA, DES, RSA, D.H., SHA-1 and MD5 [22].

Wireless Local Area Networks (WLANs) are subject to some vital security vulnerabilities and the preference of security protocol is a critical concern for IT administrators. Users need to be aware of the threats of the wireless security protocols; WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) [9]. Cryptology is

undoubtedly suitable for Wireless Sensor Networks (WSNs). The application of a simple non-interactive key exchange scheme at the system-level has been investigated with regards to its suitability. It was concluded that it is particularly suitable for many Wireless Sensor Network (WSN) scenarios. [25]. Attacks are possible on wireless LANs if suitable precautions are not exercised. Tews et al [26] introduced two possible attacks: an improved key recovery attack on WEP and an attack on WPA secured wireless networks. These attacks are effective if network traffic is encrypted using Temporal Key Integrity Protocol (TKIP).

Electronic mail (email) systems have demonstrated an increase in complexity to the point where their reliability and usability are becoming questionable [14]. A number of electronic mail security protocols exist, such as the Pretty Good Protocol (PGP), Secure/Multipurpose Internet Mail Extension (S/MIME), and DomainKeys Identified Mail (DKIM). Roth et al [21] indicated that support for robust electronic mail security is broadly available yet only few users appear to take advantage of these features. It seems that the operational cost of security outweighs its recognized advantages.

Internet Protocol (IP) security should be recognized by current and future users and applications [7]. IP security takes care of authentication, confidentiality, and key management. Any overlay network on top of IP, such as The IP Multimedia Subsystem (IMS), must be fully protected. IMS, which employs the Session Initiation Protocol (SIP) as the primary signaling mechanism, introduces a number of new security challenges for both network providers and users [15]. A survey of common security threats which mobile IP networks are exposed to as well as some proposed solutions to deal with such threats are presented in [18].

Unauthorized intrusion into computer networks poses a great threat, especially if it is not detected. Intrusion detection systems identify unusual activities or pattern of activities that are known to trigger attacks. Once such activities are detected, measures could be followed to prevent or minimize the consequences of such attacks. A number of approaches for intrusion detection have been suggested. A solution to the problem of capturing an intruder in a product network, based on the assumption of existing algorithms for basic member graphs of a graph product, was proposed in [16]. A process for the algebraic intruder model for verifying a brand of liveliness properties of security protocols was presented in [10]. With regards to this model, formal verification of fair exchange protocols was discussed.

Malicious software aims at harming computing systems when deliberately brought in or incorporated on a system. This is another critical threat that should be detected and deterred. The number of malware variants has increased dramatically. Automatic malware classification is becoming a central research area. A behavior-based automated classification method based on distance measure and machine learning was proposed in [17]. Confidential information protection is a key concern for organizations and individuals. One of the main threats to confidentiality is malicious software. Present security controls are insufficient for preventing malware infection [8]. To detect unknown malicious software, it is vital to analyze the software for its influence on the system when the software is executed. To implement that, the software code must be statically analyzed for any malicious activity [12].

Many network security tools exist. Some of these are open source tools. The goal of these tools is to scan various parts of the network looking for possible threats. This will enhance the security of what was mentioned above. Examples of these tools include Vulnerability Scanners, Packet Sniffers, Vulnerability Exploitation tools, and Port Scanners. A port is an application identifiable software construct acting as an endpoint in various communications. Ports are mainly used by the Transmission Control Protocol (TCP) and the User Diagram Protocol (UDP) of the Transport Layer. Ports are identified by numbers. For example, Port 25 is reserved for Simple Mail Transfer, and port 80 is used by HTTP. A port scan is an attack that tries to identify known vulnerabilities of a service on active ports. Both network administrators and attackers use port scanner tools to probe servers/hosts for open ports, but with different purposes. The administrator's goal is to verify and ensure that security policies are enforced. Attackers intend to compromise the running services.

The purpose of this paper is to evaluate network port scanning tools. For this purpose 17 tools have been initially selected for this study. For the time being, only eight tools are fully tested and selected for the evaluation purposes. The rest are by no means rejected, but will be included in the final evaluation process in the future. For the evaluation procedure, fifteen criterions have been selected. Evaluation tables will be presented and the findings will be discussed.

II. PORT SCANNING TOOLS OVERVIEW

The port scanning tools, which are included in the evaluation process, are briefly explained below.

A. Nmap

Nmap [19] is an open source program (GNU). It is an important tool for network administrators. Nmap can be used for discovering, monitoring, and troubleshooting TCP and UDP based systems.

Nmap is a general purpose network scanner. It supports most of the known operating systems including Windows, Linux, UNIX, and Mac OS X. However, for Windows the Windows Packet Capture Driver (WinPcap) is needed.

Command line arguments could be used but are case sensitive. Many scanning options require administrator privileges. On Linux and Unix, Nmap is run using the "sudo" command. If a user scans remote hops that are not in their LAN, incorrect information might be received due to the fact that firewalls, routers, proxy servers and other devices are capable of skewing the scanning results of Nmap. Aggressive scanning may crash some systems leading to system downtime and data loss.

B. SuperScan 4.0

The SuperScan [24] tool was created by Foundstone's security experts. They established the first network security consulting practices at two Big 6 accounting firms. Foundstone made their reputation as an enterprise network security company. They contributed to improving network security knowledge through numerous articles and white papers.

Foundstone was obtained by McAfee in September 2004. They will continue to provide their services as a division of McAfee.

SuperScan provides three main tools: TCP port scanner, Ping tool, and Resolver tool. To run the software, administrator privileges are needed.

C. Advanced Port Scanner

Advanced Port Scanner [2] is a GUI-based free and small tool. It is a fast and simple port scanner for Win32 and Win64 platforms. It contains descriptions for common ports database, and can perform scans on predefined port ranges.

Advanced Port Scanner is a multithreading tool. Therefore, it is capable of performing faster scans by increasing the maximum number of threads. It only allows the observation of alive/dead computers. Users can define the maximum time (in milliseconds) that the LAN scanner needs to take on each port scan.

D. Advanced Administrative Tools

Advanced Administrative Tools (AATools) [1] is mainly a security diagnostic and testing utility. It is used to verify the integrity of the security and firewall functions to protect the computer and the data it stores. AATools network monitor maps the operational ports to their proper applications. This implies that it provides a tracking facility to track applications with port maps.

This tool can perform the following tasks: Port Scanner, Proxy Analyzer, RBL Locator, Trace Route, Email Verifier, Links Analyzer, Network Monitor, Process Monitor, System Information, Resource Viewer, and Registry Cleaner.

The Port Scanner is used to conclude the active ports/services using TCP/UDP ports. It also allows multiple addresses and a list of ports scan, resolves or replaces host names into IP addresses, searches on the DNS for a host name before scanning, supports editing ports from a list, and scans active ports that Trojan or Backdoor programs may use.

E. Angry IP Scanner

Angry IP Scanner [4] is an open source GUI-based cross-platform software. It is free to use and can be redistributed, and modified. For this tool, Java presents a solid platform for cross-platform development, rendering more than 95% of the code to be platform independent.

It was selected to use the Standard Widget Toolkit (SWT), provided by the Eclipse project. Its advantages comprise the usage of native GUI controls and widgets on every supported platform. These will make Java programs indistinguishable from the native ones. This is important to users because they desire their system-wide settings, themes, and operating system standards to be admired.

F. Atelier Web Security Port Scanner

Atelier Web Security Port Scanner [5] can carry out TCP Port and UDP Port Scanning. It has the ability to map open ports to applications, provide complete details of local host network information as well as accurate and ample LAN details. It has a prevailing NetBIOS scanner, and ports database.

The tool also provides a complete statement of network errors during the TCP scanning. The statement includes standard service keyword, remote port number, error

description, and error number. Atelier Web Security Port Scanner has TCP Sync Scanning engine. The adjustable maximum number of all ports opened together is 60.

G. Unicornscan

Unicornscan [28] is a TCP and UDP port scanner. It was designed to produce an engine that would be accurate, scalable, effective, and adjustable. It runs under the rules of the GPL license. Unicornscan supports UNIX operating system and it has now an available version for Fedora Linux operating system.

Unicornscan is capable of providing asynchronous stateless TCP scanning with all alternatives of TCP Flags, asynchronous stateless TCP banner grabbing, asynchronous protocol specific UDP Scanning, packet capture (PCAP) file logging and filtering, and relational database output.

H. GFILANguard

GFILANguard [13] is employed for Patch Management, Vulnerability Checking and Network Auditing. This tool can scan networks and ports to detect, identify and correct security vulnerabilities. It manually or on scheduled basis scans and then analyzes the services running in the open ports. It deploys fingerprint technology to check whether the service is safe or there is a hijack operation. This helps to maintain the network. GFILANguard needs 102 MB to run.

GFILANguard supports Patch Management, Vulnerability Management, Network and Software Auditing, Assets Inventory, Change Management, and Risk Analysis and Compliance.

III. NETWORK SECURITY TOOLS EVALUATION

The eight tools were assessed using fifteen criterions. In section *A*, the criteria will be stated. Section *B* will provide the actual assessment using tables.

A. Evaluation Criteria

To evaluate the various tools, we have based our assessment on fifteen criterions. These criteria were concluded after examining the tools specifications and fully testing each tool. We only relied on the tool documentation for criterions 1 and 15. The rest are technical criterions, and thus, were extensively tested. We are not claiming, however, that the set of criterions is complete. The fifteen criterions are stated below:

- *Last Update*: Date when the current version was released.
- *IP Ranges*: Maximum number of IPs which the tool can scan in one entry.
- *Test Method*: Method used before initiating port scanning to check if the computer is live or not.
- *TCP SYN Scanning*: Capability of the tool to scan TCP.
- *UDP Scanning*: Capability of the tool to scan UDP.
- *Banner Grabbing*: Whether the tool can gather information about computer systems on a network and the services running on its open ports.
- *Port List DB*: Whether the tool contains a database of descriptions of services associated with the port number.
- *Useful Tools*: Other features or services besides the basic port scanning.
- *Interface*: Type of user interface.
- *Platform*: Supported operating systems.
- *Active Port Mapping*: Whether the tool allows a mapping of the open port with the application using that port.
- *MAC Address Detection*: Ability to detect MAC address.
- *Query Application Protocols:* Whether the tool is capable of looking for all types of application protocols, such as web servers, databases, DNS servers, FTP, and Gopher servers.
- *UN/PW Recovery*: Ability to recover user name (UN) and password (PW) using brute force.
- *Free*: Whether the tool is free or not.

B. Evaluation Procedure

The above criteria are used to compare the eight tools in question. The same approach will be used when new tools are added. The criteria were distributed among three tables, with five criterions per table. Depending

on the criteria used, some cells will contain yes/no, and others will contain various values. Tables I – III illustrate the outcomes of the evaluation.

Table I
TOOLS COMPARISON – PART I

	L/Update	IP Ranges	Test Methods	TCPSYN Scanning	UDP Scanning
Nmap	1,2011	Unlimited	ICMP	Yes	Yes
SuperScan 4.0	8,2003	Unlimited	ICMP	Yes	Yes
Advanced Port Scanner	7,2006	Unlimited	ICMP	Yes	Yes
AATools	1,2006	Unlimited	ICMP	Yes	Yes
AngryIP	3,2009	Unlimited	ICMP	Yes	Yes
AWSP	2,2002	Unlimited	ICMP	Yes	Yes
Unicornscan	2,2010	Unlimited	ICMP	Yes	Yes
GFILANguard	11,2010	3999	ICMP	Yes	Yes

Table II
TOOLS COMPARISON – PART II

	Banner grabbing	Port List DB	Useful Tools	Interface	Platform
Nmap	yes	Yes	179 Scripts, 60 Libraries	GUI and command line	Linux, Mac OS X, Windows, and many UNIX platforms (Solaris, FreeNet/OpenBSD, etc.), and some smart cell phone
SuperScan 4.0	yes	Yes	Ping, Traceroute, Whois	GUI	Windows 2000 and XP
Advanced Port Scanner	No	No		GUI	Windows95/98/ME/NT4.0/2000/ XP /2003/Vista/2008 and Windows 7 (32 bit, 64 bit)
AATools	No	Yes	Proxy Analyzer, Real Time Blacklist Locator, Trace Route, Email Verifier, Links Analyzer	GUI	9x/Me/NT4/2000/XP
AngryIP	No	No	Fetcher, Openers, Exporters,	GUI	Mac OS X, Linux systems, and Windows98/ME/2000/XP/Vista
AWSP	No	Yes	Ping, Traceroute, NSLookUP	GUI	Windows NT/2000/XP
Unicornscan	Yes	Yes	Relational database output, Custom module support	Only command line	Unix, fedora
GFILANguard	No	Yes	Patch Management, Vulnerability Checking, Network Auditing, DNS Lookup, Traceroute, Whois	GUI	(x86 or x64) - Windows Server 2008, 2003, 2000, Windows 7, Vista, XP, Windows SBS 2008, 2003

Table III
TOOLS COMPARISON – PART III

	Active Port Mapping	MAC Address Detection	Query Application Protocols,	UN/PW Recovery	Free
Nmap	Yes	Yes	Yes	Yes	Yes
SuperScan 4.0	No	No	No	No	Yes
Advanced Port Scanner	No	No	No	No	Yes
AATools	Yes	No	No	No	No
AngryIP	No	No	No	No	yes
AWSP	Yes	yes	No	No	No
Unicornscan	No	No	No	No	Yes
GFILANguard	Yes	Yes	No	No	No

IV. OUTCOMES DISCUSSION

A number of interesting observations can be spotted in the above tables. Table I reveals that all the tools are capable of TCP SYN and UDP Scanning. Also, all the tools in question use the ICMP method to check whether the computer is live or not. With regards to IP ranges, all of them allow unlimited range except *GFILANguard*, which is limited to 3999. *Nmap*, *Unicornscan* and *GFILANguard* received the most recent update.

Table II indicates that *Nmap*, *SuperScan 4.0*, and *Unicornscan* are capable of gathering information about computer systems on a network. All tools except *Advanced Port Scanner* and *AngryIP* support a database of service descriptions. In addition, all tools except

Advanced Port Scanner, grant other features or services with varying amounts of services in addition to the basic port scanning. The tools, with the exception of *Unicornscan*, accommodate GUI interface. *Nmap* adds a command line interface. The eight tools run on various operating systems. However, *Nmap, followed by AngryIP, GFILANguard, and Advanced Port Scanner* support more operating systems than the rest.

From Table III, we can detect that *Nmap*, *AATools*, *AWSP*, and *GFILANguard* allow for active port mapping. Only *Nmap*, *AWSP*, and *GFILANguard* can detect MAC addresses. Finally only NMAP grants querying application protocols, and recovering user name and password via brute force search.

The assessment exhibits that *Nmap* is the superior tool given these criteria. *AWSP* and *GFILANguard* follow. *The Advanced Port Scanner* and *AngryIP* satisfy fewer criterions than the rest.

V. CONCLUSIONS

Network administrators implement conditions and policies needed to inhibit and monitor unauthorized access, exploitation, modification, or denial of the network and its resources. To do this, there are many network security tools available for various security functions. This paper concentrated on network port scanning tools. To this extent, eight tools have been compared based on fifteen criterions. As this is a continuous process, more tools will be added in the future to complete the study. Based on the comparison tables above, it is concluded that *Nmap* provides more features than other tools involved in the study. The set of criterions is by no means a closed set. Further criterions will be added in the future.

REFERENCES

[1] Advanced Administrative Tools, G-Lock software, Available: http://www.glocksoft.com/aatools.htm.

[2] Advanced Port Scanner, Radmin, Available: http://www.radmin.com/products/previousversions/portscanner.php.

[3] M. Agrawal, *Business Data Communications*, Wiley, 2011.

[4] Angry IP Scanner, Available: http://www.angryip.org/w/Home.

[5] Atelier Web Security Port Scanner, AW Atelier Web, Available: http://www.atelierweb.com/pscan.

[6] J. A. Audestad, "Internet as a multiple graph structure: The role of the transport layer," *Information Security Technology Report*, Vol. 12, No. 1, pp. 16-23, March 2007.

[7] Z. Bojkovic , Some IP security issues, *in Proc. the 10th WSEAS International Conference on Mathematical Methods and Computational Techniques in Electrical Engineering*, Wisconsin, 2008, pp. 138-144.

[8] K. Borders, "Protecting confidential information from malicious software," Ph.D. Dissertation, Dept. University of Michigan, Ann Arbor, MI, USA, 2009.

[9] H. I. Bulbul, I. Batmaz, and M. Ozel, "Wireless network security: comparison of WEP (Wired Equivalent Privacy) mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) security protocols," *in Proc. 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia*, Adelaide, Australia, January, 2008.

[10] J. Cederquist, and M. Dashti, An Intruder Model for Verifying Liveness in Security Protocols, in Proc. the fourth ACM workshop on Formal methods in security (FMSE'06), Alexandria, VA, 2006, pp. 23-32.

[11] D. E. Comer, Computer Networks and Internets, Prentice Hall, 2009.

[12] J. Dai, "Detecting Malicious Software by Dynamic Execution," Ph.D. Dissertation, University of Central Florida, Orlando, FL, USA, 2009.

[13] GFILANguard, GFI, Available: http://www.gfi.com/lannetscan.

[14] R. Hall, "Fundamental Non-modularity in Electronic Mail," *Automated Software Engineering*, Vol. 12, No. 1, pp. 41-79, 2005.

[15] M. T. Hunter, R. J. Clark, and F. S. Park, Security issues with the IP multimedia subsystem (IMS), in Proc. the 2007 Workshop on Middleware for next-generation converged networks and applications (MNCNA'07), Newport Beach, 2007.

[16] N. Imani, H. Sarbazi-Azad, and A.Y. Zomaya, Capturing an Intruder in Product Networks, Journal of Parallel and Distributed Computing, Vol. 67, No. 9, pp. 1018-1028, 2007.

[17] J. Lin, On Malicious Software Classification, *in Proc. the 2008 International Symposium on Intelligent Information Technology Application Workshops (IITAW '08)*, Shanghai, China, 2008, pp. 368-371.

[18] M. C. Niculescu, E. Niculescu, and I. Resceanu, Mobile IP Security and Scalable Support for

Transparent Host Mobility on the Internet, *in Proc. 7th WSEAS International Conference on Applied Computer Science*, Wisconsin, 2007, pp. 214-221.
[19] Nmap, Nmap.org, Available: http://nmap.org/.
[20] P. Patel, A. Whitaker, D. Wetherall, J. Lepreau, and T. Stack, "Upgrading transport protocols using untrusted mobile code," *in Proc. the Nineteenth ACM Symposium on Operating Systems Principles (SOSP '03)*, New York, 2003, pp. 1-14.
[21] V. Roth, T. Straub, and K. Richter, "Security and usability engineering with particular attention to electronic mail," *Int. Journal of Human-Computer Studies*, Vol. 63, No. 1-2, pp. 51-73, 2005.
[22] N. Sklavos, P. Kitsos, K. Papadopoulos, and O. Koufopavlou, "Design, Architecture and Performance Evaluation of the Wireless Transport Layer Security," *The Journal of Supercomputing*, Vol. 36, No. 1, pp. 33-50, April 2006.
[23] W. Stallings, *Network Security Essentials – Applications and Standards*, Prentice Hall, 2011.
[24] SuperScan, McAfee Foundstone Practices, Available: http://www.foundstone.com/
[25] P. Szczechowiak, A. Kargl, M. Scott, and M. Collier, "On the application of pairing based cryptography to wireless sensor networks," *in Proc. the second ACM conference on Wireless network security (WiSec '09)*, New York, 2009, pp. 1-12.
[26] E. Tews, and M. Beck, "Practical attacks against WEP and WPA," *in Proc. The second ACM conference on Wireless network security (WiSec '09)*, New York, 2009, pp. 79.86.
[27] A.S. Tanenbaum, and D.J. Wetherall, Computer Networks, Prentice Hall, 2011.
[28] Unicornscan, Available: www.unicornscan.org.