Penetration Testing and Vulnerability Analysis in Computer Networks

AKHAND PRATAP SINGH
Research Scholar
SVCS&HE, Alwar, India
akhand.mca2009@gmail.com

SUNIL GUPTA
Associate professor
SVCS&HE, Alwar, India
sunilgupta8764@gmail.com

Abstract

Computer networks are use in communication between any two computer. It help to freedom to save our time and time and freedom to do any work with distributed environment. An Administrator always to check to either his system is secure or not. For this purpose we use vulnerability scanner, a vulnerability scanner find out any weakness on any computer. This may harm our computers or steal our important data. To ensure varieties of scanner tools are available in now a days. From the testing and information gathering it makes conclusions and reports the vulnerabilities it found in the network. If the scanner misses some vulnerabilities and the administrator of the network makes the conclusion that the network is secure enough the impact can be severe on the organisation or company. This paper is trying to find out to what extent a vulnerability scanner can be trust. The purpose of this is to provide an overview of the application of penetration testing to secure systems administration. As such, the presentation is not overly technical in scope, but covers instead what penetration testing is, what benefits stakeholders in a secure system receive from a test. In this paper we use for vulnerability scanner and try to find out what security issues are arises and how they can low our securities. The comparison between the findings of the vulnerability scanners and the vulnerabilities found and explored in the penetration test indicates to what extent the vulnerability scanners can be trusted. The result show that scanners miss some vulnerabilities or given low priorities but it has a measure issue for administrator.

Keywords:- Attack, Computer Network, Firewall.

Introduction

Network administrators try to secure the network form in-sider and outside threats. There are two types of attacker: Internal and External. An insider attacker is who in side organization and outsider is who from outside the organization. The insider is more dangerous than outsider because they know where is our crucial data, so administrator try to manage all these types of attacks.[4]**.** From the outside world there is always the possibility of someone using a flaw in the network togain access. On the inside there are the users that, although they have legitimate access to parts of the network.

Vulnerabilities Assessment: The term “vulnerability assessment” means find out weakness of any network. The scanner find vulnerabilities so they can be eliminated before exploited by malicious software or hackers. In most cases the vulnerabilities are known and can therefore be found. The vulnerabilities that constitute threats in a network include software defects, unnecessary services, mis configurations and unsecured accounts. **.**the vulnerability scanner does not find a “Zero day Exploit”. A Zero day exploit means a newly identified virus for which our antivirus not be updated. A vulnerability assessment starts to know how systems are running. This is a very important step of an assessment. If the administrator is not aware of what devices that are running on the network it is possible that these devices are not updated and secured in the way they should. A vulnerability assessment can be used as an inventory of the systems on the network and the Services they provide.

Proposed work

On this paper vulnerability scanners will be tested in a computer network. Penetration testing against the laboratory network will be conducted and the output from these tests will be compared with the findings of the vulnerability scanners and discussed.

What is secure network: the secure network can be classified in three categories:
CIA:

- **C**onfidentiality
- **I**ntegrity
- **A**vailability

Confidentiality: means the information is secure from unauthorized access. analysis[6]. Employing the following security measures can enhance the confidentiality of data in a network:

- **N**etwork security protocols
- **N**etwork authentication services
- **D**ata encryption services

Integrity:, integrity ensures that the information that was received is authorized.

Availability:, when ant attacker attack or hack any system and they may disrupt the services, the term availability ensure that the data is available when Required.**[6]** and security also required like Denial of Services(Dos). Some techniques are:

- Fault tolerance of disks, systems, and backups
- Acceptable log –in and process performance
- Firewall systems
- Reliable and functional security processes and mechanism.

Survivable System: Basically a survivable system is to provide continue services in case of failure, attacks, or damaged. A network system must have the capability of possible occurrence of attack. The quality levels of confidentiality, integrity and availability in a system must be withheld. But the level of survival and the demands of maintaining essential services.

Key property	Methods to protect
Resistance to attacks	Authentication, Access Control, Encryption, Message Filtering, Functional Isolation
Finding an Attacks	Intrusion Detection Integrity Checking
Recovery of Attacks	Data Replication, System backup and restoration

Table 1: Properties of Attacks.

Resistance to attacks: Making an effective strategy by which we can save our data and me With a strong authentication and access control, like strong passwords and access control that can grant or deny users, the system can resist attacks. E.g: use a Encryption to send data in network that will be protect from outside of network.

Finding an Attack: It is done by IDS(Intrusion Detection System) . They recognize typical attack patterns or use a baseline model for normal behavior. Integrity checkers are used checkers to find any attacks. **[8]**.

Some Vulnerabilities: Vulnerabilities are identified day by day but some common vulnerabilities are: Buffer Overflow, Router and firewall weaknesses, Web Server Exploits, Mail Server Exploits, Database Exploits, Denial of Service

Buffer Overflow: In computer security and programming, a **buffer overflow**, or **buffer** overrun, is an anomaly where a program, while writing data to a **buffer**, overruns the **buffer's** boundary and overwrites adjacent memory. This is a special case of violation of memory safety

Router and Firewall Weakness: A router is a device that forwards data packets between computer networks. This creates an overlay internetwork, as a router is connected to two or more data lines from different networks. Many routers still run telnet rather than SSH. This will be given a chance to attacker to grab our data. While a firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet.

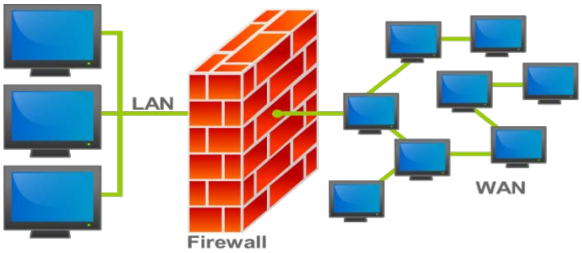

Figure 1: Network Architecture.

The possibility that any software have firewall exploits code but it is rare. But it will low our Firewalls security, Firewall often use web servers to interface with the users which make them vulnerable through that interface [7].

Web server Exploit: Most networks today involve a web server and these applications are well known for their bugs and security holes. A hacked web server can miss out data. The web servers are often Connected to other internal systems or perhaps a database that might contain information not Only for the web applications **[4].**

Mail server Exploit: For more than 20 years, e-mail has been one of the most important applications on the Internet. SMTP forms the backbone for most e-mail transfer. Because of its popularity, it is also the source of many security problems. There are many mail server exploits which are some of the given **Pipe** Attempts to forward e-mail to a program it can run

DEBUG Old admin backdoor

Hello long Intruder may be attempting a "buffer-overflow" exploit.

EXPN Attempts to find users by scanning the e-mail server.

VRFY Attempts to find users by scanning the e-mail server.

WIZ Very old admin backdoor

Too many recipients Spammer may be attempting to abuse your e-mail system by relaying spam through it.

Corrupted MAIL command Intruder may be attempting to compromise the system.

Database Exploit: Using database a website can have many functionality like filling any form, places any order. By using a loosely security a hacker may be stole your data. **[5]**

Denial of Services: it also knows as "Dos" that mean a legitimate user can not access his service due to any vulnerability.

Scanners: Different type of Scanners is used to scan network like Port Scanner, Application Scanner, and Vulnerability Scanner. Here we have focused on vulnerability scanner. Different scanner can use either TCP or UDP scan.

Penetration testing: A penetration test, occasionally pentest, is a method of evaluating computer and network security by simulating an attack on a computer system or network from external and internal threats. The process involves identifying the target systems and the goal, then reviewing the information available and undertaking available means to attain the goal. A penetration test target may be a white box (where all background and system information is provided) or black box (where only basic or no information is provided except the company name).

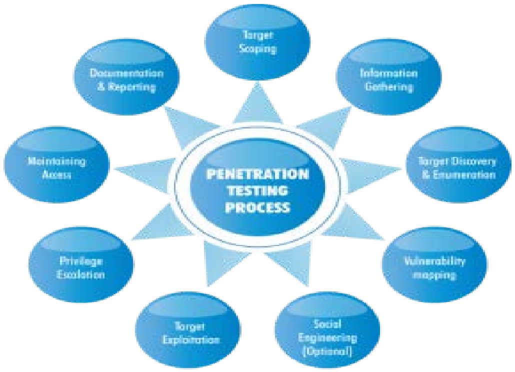

Figure 2: Penetration testing process.

Scanners: There are two types of scanner:

Port Scanner and Application Scanner. A port scanner scans all the available port in the target system while application scanner scan the all application at target system.

Port Scanner:A **port scanner** is a software application designed to scan a server or host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it.A**port scan** or **portscan** can be defined as an attack that sends client requests to a range of server port addresses on a host, with the goal of finding an active port and exploiting a known vulnerability of that service. A TCP port scanner like NMAP sends a command SYN to target devices and if reply comes with ACK means the port is active and finally to break the connection RST send that reset the connection.

Application Scanner: The application Scanner are the accessing the security configuration like Web, Database and NT Domains, the application scanner are Nikto. Nikto is included in the Nessus scanner. Other examples are SPIKE Proxy, Acunetix and Whisker or Libwhisker.

Vulnerability scanners: A vulnerability scanner is a computer program designed to access computers, computer systems, networks or applications for weaknesses. There are a number of types of vulnerability scanners available today, distinguished from one another by a focus on particular targets
Network-based scanners that run over the network, and host-based scanners that run on the target host itself.

Network Based Scanner: A network-
based scanner is usually installed on a single machine that scans a number of
other hosts on the network. It helps detect critical vulnerabilities such as miss-configured firewalls, vulnerable web servers,
Types of vulnerabilities: there are various types of vulnerabilities such as

OS Fingerprinting: Operating system fingerprinting is the process of learning what operating system is running on a particular device. By analyzing certain protocol flags, options, and data in the packets a device sends onto the network, we can make relatively accurate guesses about the **OS** that sent those packets, it is a powerful tools for target a system.

Active IP packet fingerprinting: Active IP packet Fingerprinting is to know what the current system or IP is active in network this will help to attacker to focus on that system
False positives: A false –positive is when the vulnerability scanner reports an error that is not present. There are a number of reasons of why a false positive occur. The causes can be defined into two different categories, technical false positives and contextual false positives **[10].**

False Negative: A false –negative is when the vulnerability scanner not reports any error or reports an error but has low priority but system has a major issue for security.
Tested scanners: there are variet of scanners are available some of the used on that paper which are:

Nessus: **Nessus** is a vulnerability scanner which is developed by Tenable Network Security. It is free of charge for personal use in a non-enterprise[12]environment. Nessus is the world's most popular vulnerability scanner, taking first place in the 2000, 2003, and 2006 security tools survey. Nessus 3.0 is also a freeware but to get the latest plug-ins, security checks, directly and not witha weeks delay the owner, Tenable security, will charge the user. **[2].** The old versions of Nessus as well as Nessus 3.0 use a script language called NASL (Nessus Attack Script Language), it is described as looking like the programming language C without the pointers and memory management, with some like Perl. Nessus uses a client –server architecture. Each session is configured and controlled by the client but the test is run on the server side. There are some advantages to this architecture, the scan can be conducted from outside of the network but started on the inside.

Retina: Retina Network security scanner, (www.eeye.com), is developed by “e Eye Digital Security” the company state at their website that they are the leading developer of endpoint security and vulnerability management software solutions. Retina works on 4 steps:

The first step to build a scan in LAN and discover option, retina try what type of application are running on target system, and second step is when it find active host then scan all the active port the third step is OS- Detection The last step is naturally the audit process. Each port and the associated service will be tested for vulnerabilities.

Netrecon: Netrecon, (www.symantec.com), is a vulnerability scanner from Symantec, the world leading in solutions for information security, information availability and information integrity. The latest release of the GUI of the Netrecon is the Netrecon 3.6 that was issued the year 2002. The scanner can simulate various scenarios and reports can be generated in HTML,XML,Ms-Word

ISS: ISS (Internet Security System) provided by IBM in 2006.The Internet Scanner vulnerability assessment application provides the foundation for effective network security for your small, medium or enterprise-sized business. Internet Scanner minimizes your risk by identifying the security holes, or vulnerabilities, in your network[15] so you can protect them before an attack occurs. The scanner uses scan sessions to define which devices on a network to scan. A scan session is the chosen policy that describes which checks to run, an encryption key for the session and the IP range defined by the user.

Testing the network:

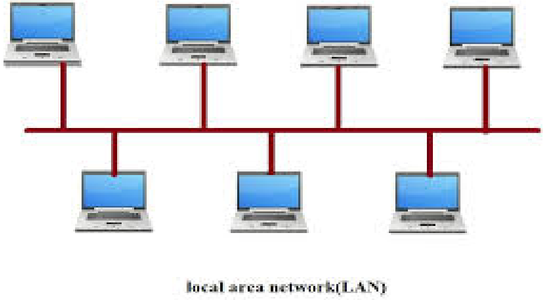

Figure 3: Local Area Network.

The objective of vulnerability scanner to find:

- How many host running on the network
- Status of the ports on that system
- What type of service running on that port
- Are the system are latest patched

After the penetration test on our network we have infected:

Varieties of vulnerabilities are found to scan the network:

Vulnerabilities	Retina	Nessus	Netrecon	ISS
RPCBIND			×	×
Finger SSH	×			
DCOM	×			
XSS				
LSASS.exe	×			×
IIS Printer	×	×	×	
ms08_067_netapi	×		×	

Table 2: Varieties of vulnerabilities.

Here (×) represent the vulnerability found in scanner

Conclusion

Hackers are increasingly targeting web applications. Gartner estimates that 70% of attacks against websites occur at the application layer. At the same time, many enterprises are relying more heavily on web applications to house critical business data, as well as confidential customer information such as credit card and social security numbers. With so much information and activity online[19], you need a comprehensive web application scanner that accurately assesses your exposure to attacks.

REFERENCES

[1] P. Santhosh Reddy, G.Sireesha, "Automated Security Test by using Formal Threat Models on Leakage Detection", International Journal of Advanced and Innovative Research (IJAIR), Vol. 2 Issue 2, 2013

[2] Prashant Belhekar, Alka Londhe, Bhavana Lucy, Santosh Kumar, "Finding Bugs In Web Applications Using Dynamic Test Generation", International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 5, May 2013.

[3] Michelle Elaine Ruse, "Model checking techniques for vulnerability analysis of Web applications", PhD Thesis, Iowa State University, Ames, Iowa, 2013

[4] Pallavali Radha, G. Sireesha, "Security Test by Using FTM and Data Allocation Strategies on Leakage Detection", International Journal Of Coputers& Technology, Vol. 4 No 2, March 2013

[5] A. Marback, H. Do, K. He, s. Kondamarri, D. Xu, "A threat model-based approach to security testing",

Software: Practice and Experience, Vol. 43 Issue 2, February 2013

[6] Sanon Chimmanee, Thanyada Veeraprasit, Kritsada Sriphaew, Aniwat Hemanidhi, "A Performance Comparison of Vulnerability Detection between Netclarity Auditor and Open Source Nessus", Recent Advances in Communications, Circuits and Technological Innovation, Paris, France, December 2-4, 2012

[7] Oleg Sheyner, Joshua Haines, SomeshJha, R. Lippman and J. M. Wing, May, 2002. “Automatedgeneration and analysis of attack graphs”, in Proceedings of IEEE Symposium on Security and Privacy.

[8] Anderson Robert H., Hearn Anthony C., & Hundley, Richard O. “RAND Studies of cyberspace security issues and the concept of a U.S minimum essential information infrastructure”, Proceedings of the 1997 IEEE Information Survivability Workshop.

[9] P. Jongsuebsuk,N. Wattanapongsakorn and C. Charnsripinyo “Network Intrusion Detection with Fuzzy Genetic Algorithm for Unknown Attacks” in IEEE 2013.

[10] Deepak Rathore and Anurag Jain “a novel method for intrusion detection based on ecc and radial bias feed forword network” in Int. J. of Engg. Sci. & Mgmt. (IJESM), Vol. 2, Issue 3: July-Sep.: 2012.

[11] Wing w. Y. Ng, rocky k. C. Chang and daniel s. Yeung “dimensionality reduction for denial of service detection problems using rbfnn output sensitivity” in Proceedings of the Second International Conference on Machine Learning and Cybernetics, Wan, 2-5 November 2009.

[12] Anshul Chaturvedi and Prof. Vineet Richharia “A Novel Method for Intrusion Detection Based on SARSA and Radial Bias Feed Forward Network (RBFFN)” in international journal of computers & technology vol 7, no 3. 2011.

[13] Mohammad Behdad, Luigi Barone, Mohammed Bennamoun and Tim French “Nature-Inspired Techniques in the Context of Fraud Detection” in ieee transactions on systems, man, and cybernetics part c: applications and reviews, vol. 42, no. 6, november 2012.

[14] Alberto Fernandez, Maria Jose del Jesus and Francisco Herrera “On the influence of an adaptive inference system in fuzzy rule based classification system for imbalanced data-sets” in Elsevier Ltd. All rights reserved 2009.

[15] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez and E.Vazquez “Anomaly-based network intrusion detection: Techniques, Systems and challenges” in Elsevier Ltd. All rights reserved 2008.