IOSR Journal of Engineering (IOSRJEN)
e-ISSN: 2250-3021, **p**-ISSN: 2278-8719
Vol. 3, Issue 5 (May. 2013), ||V2 || PP 34-39

Detection of Vulnerabilities in Network-Connected Servers

Mrs. S. Saritha, Mr. M.Raja Sekhar, Mr. Dharamvir
M.Tech 2nd Year, Dept. of CSE, Indira Priyadarshini College of Engineering. Engg.& Technology for women Nannur Village, Orvakal Mandal *Kurnool* Dist A.P. -518023
Asst. Professor ,Dept of CSE, Indira Priyadarshini College of Engg.& Technology for women Nannur Village, Orvakal Mandal, Kurnool Dist A. P .-518023
Asst. Professor. Dept. of MCA The Oxford College of Engineering 10th Milestone Bommanhalli , Hosur Main Road Bangalore, Karnataka - 560068

Abstract: Today, computer networks and distributed software systems are pervasive. Thus, the idea of secure computing is paramount. Secure Computing means avoiding improper disclosure of private or sensitive information. Data stored on a computer or processed by software should be modified only through legitimate, verifiable channels. We should guard against outsiders performing denial-of-service (DoS) attacks. For computing to be trustworthy, each bit of data the system uses and each user that interacts with the system must be authentic and legitimate. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

This paper considers some of the facts why business need information security policies, procedures, technical measures used to prevent unauthorized access, alteration, theft or physical damages. The major threats to business come from insiders who usually have some system knowledge and trust level. Secondly, most protection schemes target outsiders because attackers might control resource assets. For example controlling broadband Internet machines, target files containing trade secrets, credit-card numbers. Various issues for information protection system, application vulnerabilities, Security analysis, social engineering and phishing have been discussed for the benefit of IT business

Keywords: *DoS (Denial of Service), Vulnerability, Spoofing, Firewall, IDS, Hacking, Phishing*

I. INTRODUCTION

An easy starting point to improve computer network security is to look at whom or what could be a threat. If a system treats everyone equality and there are no access or service restrictions, there is little motivation for an attack. A variety of mechanisms available to protect the network are:

a) Filtering requests to the asset – firewalls, intrusion detection system
b) Access controls – permission, authentication
c) Tamper resistance – cryptography

Adversaries usually attack assets by installing their software on target machines. Attackers identify target entry points, analyze them for access vulnerabilities, and install their code. Unfortunately, regardless of any specific security measure you take, software often has embedded vulnerabilities that let attackers bypass security and gain access to assets. Many computer-security experts consider these vulnerabilities to be the biggest problem facing software developers and hackers' greatest ally.

According to NASSCOM, security can be segmented in the following broad categories:

i) Network security refers to securing the infrastructure, used for storage and transmission of information. Hardware Technology- Intrusion Detection Systems (IDS), Firewalls, Routers etc. Software Technology- Antivirus, Spyware, etc. Policies for access control, authentication etc.
ii) Physical Security refers to securing the building, work areas, devices and data in the form of documents. This is primarily done through the following measures:

- Access control mechanisms such as security guards, ID cards, swipe cards, etc.
- Restricted movement of media and papers
- Camera surveillance
- Fire safety etc

iii) Personnel Security refers to arrangements made to address the potential threat arising from the employees of offshore vendors. Some of the security measures used includes the following:

- Background checks such as reference checks, police checks etc
- Non-disclosure & confidentiality agreements
- Internet access policies
- Mobile computing policies

- Training and awareness etc

iv) Business Continuity and Disaster Recovery refers to practices followed to retrieve information and provide continuous services in case of any emergency. Some of these practices include the following:

- Data back-ups at remote locations
- Risk assessment and restoration processes
- Fire, link and power drills
- Alternate site management etc

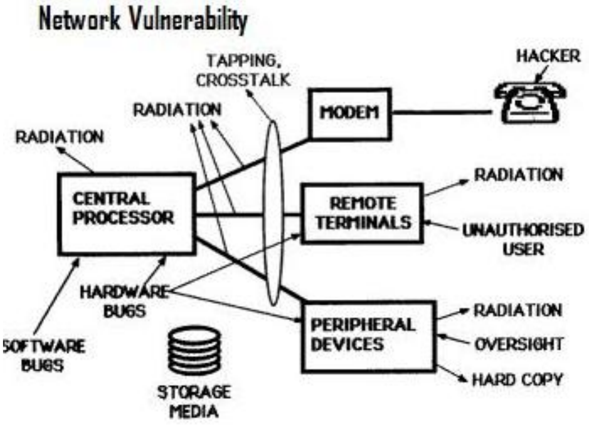
Source: Accessed from: http://www.nasscom.in Security standards such as BS 7799, CoBIT, etc have evolved over time. Companies providing offshore services are expected to comply with such standards since they are globally accepted and highlight best practices to ensure security

.

II. NETWORK VULNERABILITIES

Vulnerability is a system weakness that an attacker can exploit, usually to obtain access to some asset. Many circumstances inadvertently create system weakness, but they fall into three general areas: Service, Applications and User actions.

Networks are vulnerable for two reasons: Connectivity and Complexity



.

Services: Broadly speaking, services are when a computer opens an interface to communicate with other computers. Whether the interface is email, a Web page, a database, or other information-sharing services, it's much easier to exploit service weaknesses because they enable direct communication between attacking machines and their targets while requiring little or no user intervention. Example was Microsoft's Internet Information Server (IIS), which let the CodeRed worm spread in 2001.

Applications: Consider a virus-laden email or a Web page that contains malicious scripting. Users might have to navigate to the email or Web page- attackers have no control over the user's action – but if users unwittingly participate, the attacker can exploit an email client or Web browser vulnerability to gain control of their computers.

User actions: Users can create vulnerabilities when they misconfigure their machines or software. Attackers often trick users into giving out private information to assist in an attack. The tool most often used to do this is called *social engineering.* Social engineering is often – bribing someone to get a password or fooling them into divulging information that will lead to a breach, such as sending out a convincing but fake email from eBay or a bank. Such attacks are commonly known as phishing.

2.1 Different types of Vulnerabilities

2.1.1 Packet Sniffer

It is a program and/or device that monitor data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere. This makes them a favorite weapon in the hacker's arsenal. On TCP/IP networks, where they sniff packets, they're often called packet sniffers.

2.1.2 Port Scan

The port scan is an act of systematically scanning a computer's ports [in networks, an endpoint to a logical connection]. Since a port is a place where information goes into and out of a computer, port scanning identifies open doors to a computer.

Port scanning has legitimate uses in managing networks, but port scanning also can be malicious in nature if someone is looking for a weakened access point to break into your computer.

2.1.3 Script Kiddie

A person, normally someone who is not technologically sophisticated, who randomly seeks out a specific weakness over the Internet in order to gain root access to a system without really understanding what it is, he is exploiting because the weakness was discovered by someone else. A script kiddie is not looking to target specific information or a specific company but rather uses knowledge of a vulnerability to scan the entire Internet for a victim that possesses that vulnerability.

III. SOURCES OF INFORMATION TO PROTECT YOUR NETWORK

Newsletters at http://www.us-cert.gov/cas/ provide:

a) Technical Cyber Security Alerts provide timely information about current security issues, vulnerabilities, and exploits.

b) Cyber Security Bulletins provide bi-weekly summaries of security issues and new vulnerabilities. They also provide patches, workarounds, and other actions to help mitigate risk.

C yber Security Tips describe common security issues and offer advice for nontechnical home and corporate computer users.

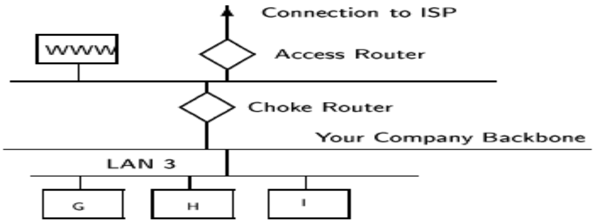
Resources from SANS (SysAdmin, Audit, Network, Security) Institute http://www.sans.org/newsletters *SANS NewsBites*: weekly, high-level executive summary of the most important news articles on computer security.

IV. SECURITY ISSUES

Open connection between the LAN and an Internet provider causes a security threats If your WAN uses the Internet, you can use secure options such as virtual private networking to connect the separate LANs together. A firewall is software running on the gateway server usually set up to block all incoming and outgoing traffic, with a list of known exceptions.

Many Web Servers either contain or have access to sensitive data. A server used for electronic commerce may contain customer records and credit card information, all of which must be kept from prying eyes. Some Web servers are attacked by crackers who want to change the content or crash the server altogether. The process of setting up a private network connection using VPN involves encrypting the data at one end of the connection and decrypting it at the other end. Doing so creates a virtual tunnel between the two sites through which they communicate and which is not visible or accessible at any point in between. For instance, the telecommuter might make a regular Internet connection and then use a VPN connection over the Internet to reach the office. VPN server and VPN client must use a robust method of encrypting data and follow certain standard security precautions.

Remote Access: The remote user runs a program using a modem, ISDN terminal adapter or other communication device to call directly to a similar device on a remote access server connected to the remote network. Remote Control: Once the user is authorized and a connection is established, the user can control every aspect of the remote computer as if his own terminal.



V. SECURITY THREATS

A security threat may be as simple as disturbing normal operation viz Denial of Service attacks or as complex as cracking security and taking control of network resources.

i) ***Denial of Service Attacks (DoS):*** A cracker might configure a utility to send packets in large sizes or containing unexpected data, causing the server to crash, hang or slow down. DoS is prevent others from using a system. E.g. If e-commerce site shut down by DoS attacks, the company may lose its heavy source of revenue.

ii) ***IP Spoofing:*** By forging the header so it contains a different address, an attacker can make it appear that the packet was sent by a different machine. The machine that receives spoofed packets will send response back to the forged source address, which means that this technique is mainly used when the attacker does not care about the response or the attacker has some way of guessing the response.

iii) ***Buffer Overflow:*** A buffer overflow on a network server can cause data loss or corruption, or it can cause the program or server to crash. It causes data to overwrite an adjoining section of memory, and the adjoining memory is part of the computer's instruction stack.

iv) ***Social engineering*** is the act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical hacking techniques. "Social engineering" as an act of psychological manipulation that was popularized by hacker-turned-consultant Kevin Mitnick. All social engineering techniques are based on specific attributes of human decision-making known as cognitive biases. These biases, sometimes called "bugs in the human hardware," are exploited in various combinations to create attack techniques.

VI. SECURITY POLICIES

When setting up a network, whether it is a local area network (LAN), virtual LAN (VLAN), or wide area network (WAN), it is important to initially set the fundamental security policies. Security policies are rules that are electronically programmed and stored within security equipment to control such areas as access privileges. Of course, security policies are also written or verbal regulations by which an organization operates. In addition, companies must decide who is responsible for enforcing and managing these policies and determine how employees are informed of the rules and watch guards. Security Policy, Device, and Multi-device Management functions as a central security control room where security personnel monitor building or campus security, initiate patrols, and activate alarms. The security policy management function should be assigned to people who are extremely trustworthy and have the technical competence required

VII. SECURITY TOOLS

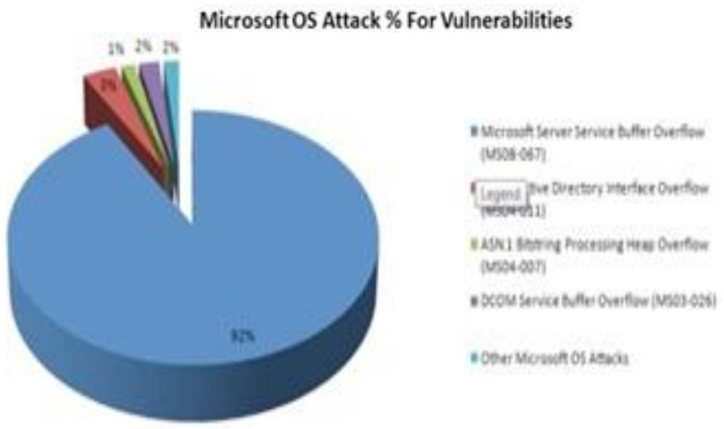
Organizations have an extensive choice of technologies, ranging from anti-virus software packages to dedicated network security hardware, such as firewalls and intrusion detection systems, to provide protection for all areas of the network. After such solutions are instated, tools can be deployed that periodically detect security vulnerabilities in the network providing ongoing, proactive security. In addition, professional network security consultants can be engaged to help design the proper security solution for the network or to ensure that the existing security solution is up to date and safe. With all of the options currently available, it is possible to implement a security infrastructure that allows sufficient protection without severely compromising the need for quick and easy access to information.

Intrusion Detection System (IDS)

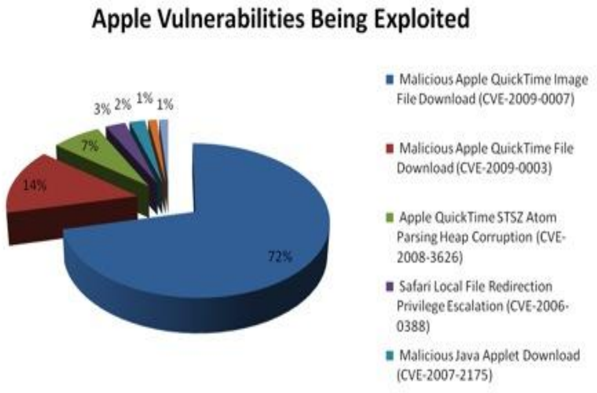
A network-based ID provides around-the-clock network surveillance. An IDS analyzes packet data streams within a network, searching for unauthorized activity, such as attacks by hackers, and enabling users to respond to security breaches before systems are compromised. When unauthorized activity is detected, the IDS can send alarms to a management console with details of the activity and can often order other systems, such as routers, to cut off the unauthorized sessions.

VIII. FINDINGS

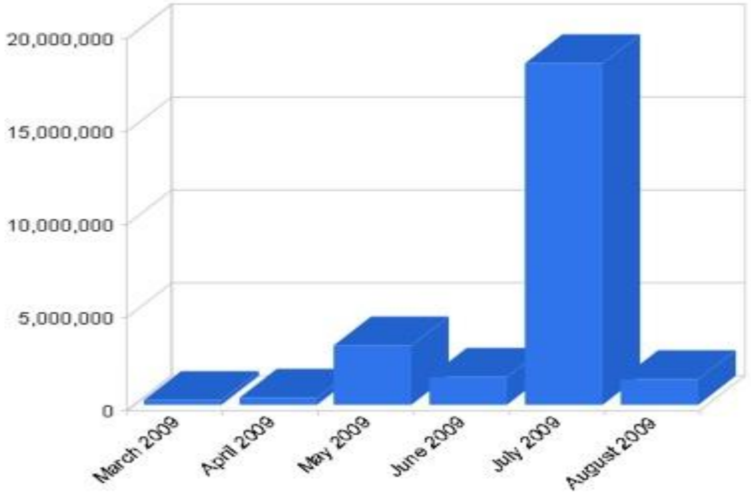
i) Attacks on Microsoft Windows operating systems were dominated by Conficker/ Downadup worm variants. For the past six months, over 90% of the attacks recorded for Microsoft targeted the buffer overflow vulnerability described in the Microsoft Security Bulletin MS08-067.



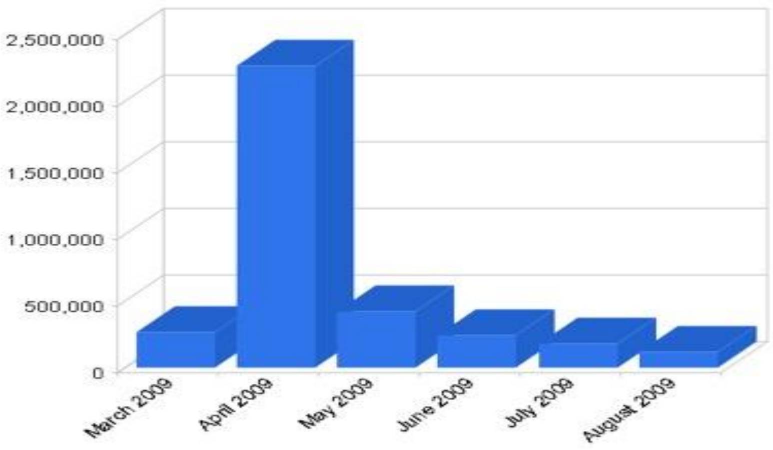
ii) Apple has released patches for much vulnerability in QuickTime over the past year. QuickTime vulnerabilities account for most of the attacks that are being launched against Apple software. Note that QuickTime runs on both Mac and Windows Operating Systems.



iii) A very large spike in SQL Injection attacks in July 2009 was caused mostly by an online advertiser who distributed code to many affiliates using SQL injection as functionality. The application was quickly pulled, resulting in a large drop in events for the month of August.



iv) “PHP File Include" attacks have seen a notable decline in the overall number of attacks that have taken place. With the exception of a major attacks originating from Thailand in April, the number of PHP File Include attacks in August is less than half the March/May average.



v) According to USCERT, 95% of downtime and IT related compliance issues are a direct result of an exploit against a CVE (Common Vulnerability Exposure). Your firewall, IDS, IPS, anti-virus software and other counter measures don't look for or show you how to remove your CVEs. So you are really only 5% secure.

IX. CONCLUSION

Despite the costly risks of potential security breaches, the Internet can be one of the safest means by which to conduct business. For example, giving credit card information to a telemarketer over the phone or a waiter in a restaurant can be more risky than submitting the information via a Web site, because electronic commerce transactions are usually protected by security technology. General fear and suspicion of computers still exists and with that comes a distrust of the Internet. This distrust can limit the business opportunities for companies, especially those that are completely Web based. Thus, companies must enact security policies and instate safeguards that not only are effective, but are also perceived as effective. Organizations must be able to adequately communicate how they plan to protect their customers.

It is found that inadequate network security is usually caused by a failure to implement security policies and make use of security tools that are readily available. It's vital that companies complete professional risk assessments and develop comprehensive security plans and infrastructures that are publicly supported by upper management.

As time goes on, more and more new technology will be developed to further improve the efficiency of business and communications. At the same time, breakthroughs in technology will provide even greater network security, therefore, greater piece of mind to operate in cutting edge business environments. Provided that enterprises stay on top of this emerging technology, as well as the latest security threats and dangers, the benefits of networks will most certainly outweigh the risks.

REFERENCES

[1]. CEH official Certified Ethical Hacker Review Guide – Kimberly Graves, Wiley India Pvt. Ltd.

[2]. Network Security Fundamentals – Peter Norton and Mike Stockman, Techmedia

[3]. Security in Computing, 3rd Edition, Charles P. Pfleeger, Shar's Lawrence pfleeger, Pearson Education

[4]. Cryptography & Network Security Principles & Practices, 3rd William Stallings, Prentice Hall of India Pvt. Ltd.

[5]. Technical Resource and Course Web Site for Cryptography and Network Security, Third Edition, by William Stallings

[6]. Firewalls and Internet Security, Second Edition, Repelling the Willy Hacker, by William R. Cheswick, Steven M. Bellowin, Aviel D. Rubin, Pearson Edition Inc

[7]. Network Security Fundamental: *www.sans.org/top-cyber-**security**-risks/*

[8]. Network Security Resources: www.government**security**.org/

[9]. Network Security Technologies and Solutions (CCIE Professional Development Series) By Yusuf Bhaiji. Published by Cisco Press, 2008

[10]. Network Security Hacks, Second Edition Tips & Tools for Protecting Your Privacy by Andrew Lockhart, O'Reilly Media, 2006

[11]. Hacking: The Next Generation by Nitesh Dhanjani, Billy Rios, Brett Hardin, O'Reilly Media, 2009

[12]. Hackers Beware: The Ultimate Guide to Network Security by Eric Cole, Sams 2001, 1st Edition