SURVEY OF NETWORK SECURITY WEAKNESSES IN ROUTER AND FIREWALL CONFIGURATION SYSTEM

SUCHITA R. RAUT¹, AMIT. M. BAJARE²

1. M.E. Student, Department of Computer Science and Engineering, RSCE, Buldana, Maharashtra, India.
2. Department of Computer Science and Engineering, RSCE, Buldana, Maharashtra, India.

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: Network security is main issue of this generation of computing because many types of attacks are increasing day by day. Enterprising a network is not a big issue for network administrators but protecting the entire network is a big issue. This paper was conducted the network security weaknesses in router and firewall network devices, type of threats and responses to those threats, and the method to prevent the attacks and hackers to access the network. Also this paper provides a checklist to evaluating a network is to best practices in network security and data confidentiality. The main aim of this research is to protect the network from vulnerabilities, threats, attacks configuration weaknesses and security policy weaknesses.

Keywords: Network Security, Configuration System

Corresponding Author: MS. SUCHITA R. RAUT

Access Online On:
www.ijpret.com

How to Cite This Article:
Suchita R. Raut, IJPRET, 2015; Volume 3 (9): 318-327

Available Online at www.ijpret.com
INTRODUCTION

Network security of Internet and Local Area Network is the center of computer network issues [1]. Each and every client is working on the internet, they want security of information but sometimes he or she doesn't know that someone else may be collecting the information. There are many of these threats have become cleverly exercised attacks by causing damage. The evolution of networking and Internet that threats are to be information and network has been increased dramatically. The Internet continues to increase by the exponentially. The personal, governmental, and business-critical applications are more common on the internet. These network-based applications can pose security risks to use personal as well as to the information resources of companies and government. The rush to get connected comes at the expense of network security. This information must be protected [2]. Without capably protecting or network security, many individuals, businesses, governments are at risk of decreasing that asset. This is imperative that all networks to be protected from threats and weaknesses in order for a business to achieve its fullest potential. The Network security is the process which is digital information is protected. These threats are persistent due to weaknesses, which can start from misconfigured hardware or software, poor network design inherent technology weaknesses. A router is similar to many computers it has many services enabled by default. There are many services are unnecessary and used by an attacker for collecting the information. The aims of network security are to protect the confidentiality, assurance of availability, and maintain integrity.

Many Routing protocols are management and maintaining of Wireless Sensor Network. From research and study of a large number of security threats are enumerated in WSN. All of the unnecessary services are disabled in the router configuration to prevent the attacker from using it damage the network or to the important information, or network devices configuration. Careful management and diligent audit of router and firewall operation improve security, prevent the attacks and hackers, network threats decrease. Routers and firewall are critical parts of network security and network operation.

2. NETWORK SECURITY AND PROTECTION

Security has main purpose of protect the assets. The approach of personal computers is LANs, and the wide-open world of the Internet. As e-business and Internet applications continue to increase, finding the balance between isolated and being open will be critical. With the increase number of LANs and personal computers, the Internet creates untold number of security risks. Firewall devices, which are software or hardware that enforce an access control policy between
two or more networks, that are introduce. This technology gave businesses a balance between security and simple outbound access to the Internet, which was mostly used to e-mail and Web surfing.

Real-world network security includes elimination, detection, and response. If the elimination mechanisms were perfect, you would not need detection responses. But there is no elimination mechanisms only have limited value. On the Internet, this translates to monitoring. The detection and response are not only more cost effective but also more effective than piling on more elimination. In network Protection, there are fortunately many preventative techniques to properly secure network against threats. The first method of protection is to address the actual physical layer of the network to assure that it is equipped. Additionally, firewalls and encryption should be incorporated into a network to heighten its security. Finally, several other passwords, variations of capital and small letters are further increase the strength of passwords.

Network security is the most important component in information security, because it is responsible for securing all information passed through networked computers [3, 4]. That security is required to provide an acceptable level of protection for hardware, software, and information in a network. In this network security refers to all hardware and software functions, characteristics, features, access controls, administrative and management policy. Network security is successful in preventing information loss that must follow three fundamental precepts. First, a secure network must have integrity such that all of the information stored therein is always correct and protected against fortuitous data corruption as well as willful alterations. Second, network security requires availability of information to its necessary recipients at the predetermined times without exceptions. Finally, to secure a network there must be confidentiality, or the ability to share information on the network with only these people for whom the viewing is intended. The three principles that network security must evolve from many years of practice and experimentation that make up network history.

Firewalls are another measure that used in increasing the level of security in a network. A firewall is in essence a portal through which information enters and exits. On one side of the portal is internal network that must remain secure, and on the other is the information needed from the outside of the world that is combined with the undesirable threats of external networks. There are three of the major types of firewalls that are listed in order of increasing quality and price; there are packet-filtering routers, application-level gateway, and circuit-level gateways.
3.1 Weaknesses, Threats and Attacks on Router

Discussing the network security, there are three common terms used are Weaknesses or vulnerability, threat, and attack. Vulnerability is weaknesses in network security systems that are inherent in every network and device. There should be includes routers, switches, servers, and security devices themselves. There are three primary weaknesses: [7, 8, and 9]

1. Technology weaknesses

2. Common security policy weaknesses

3. Common configuration weaknesses

Technological Weaknesses: Computer and network technologies have built-in security weaknesses. These include TCP/IP protocol weaknesses, operating system weaknesses, and network equipment weaknesses.

Security Policy Weaknesses: Security policy weaknesses can create security threats. The network may pose security risk to the network if users do not follow the security policy. There are some common Security Policy Weaknesses are listed in Table 2.

Configuration Weaknesses: Network security administrators need to learn what is the configuration weakness and correctly configuration their computing and network devices are compensated. There are some configurations weaknesses are given in Table1. [10, 11]

There are number of security threats that can be cause of network security attacks. Threats are the people willing, eager, and qualified to take advantage of each an every security weakness and they are continually search for new exploits and weaknesses. Then finally, the threats use a variety of tools, scripts, and programs to launch attacks against networks and network devices.

We discuss the two primary classes of threats to network security; there are internal threats and external threats. The Internal threats to a network are a major source security attained.

<table>
<thead>
<tr>
<th>Weakness</th>
<th>How the weakness is exploited</th>
</tr>
</thead>
<tbody>
<tr>
<td>Efficiency of written policy</td>
<td>An unwritten policy cannot be regularly.</td>
</tr>
<tr>
<td>Politics</td>
<td>Political battles and turf wars can make it hard to implement a constant security.</td>
</tr>
<tr>
<td>Lack of continuity</td>
<td>Frequent replacement of personnel can lead to an erratic approach</td>
</tr>
</tbody>
</table>
External threats to a network security referred to as hackers, that can be equally and sometimes more dangerous than internal threats. It can be obtain entry into a network or view sensitive information; hackers must be using some tools such as: 1- IP snooping, 2-password sniffers, 3- E-Mail attacks. IP spoofing or interface involves the capturing of the information in an Information packet (IP) to obtain the necessary address name that has a trusted relationship with another workstation. A hacker can act as one of the workstation and use the trusted relationship to gain entry into the other workstation where any number of actions can be performed. Password sniffers actually work with the execution of a packet sniffer that monitors traffic on a network passing through the machine. That sniffer acquires the password and log-on name used when the source machine attempts to connect to other machines and saves this information in a separate file.

**Table 2: Common configuration weaknesses**

<table>
<thead>
<tr>
<th>Weakness</th>
<th>How the weakness is exploited</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unsecured user accounts</td>
<td>User account information may be transmitted insecurely across the network, exposing usernames and password to snoopers.</td>
</tr>
<tr>
<td>System accounts with easily</td>
<td>This common problem is poorly selected and easily guessed user passwords.</td>
</tr>
<tr>
<td>guessed passwords</td>
<td></td>
</tr>
<tr>
<td>Misconfigured internet services</td>
<td>A common problem is to turn on JavaScript in web browsers, enabling attacks by way of hostile JavaScript when accessing untrusted sites, IIS, FTP, and Terminal services also pose problem. Sampling a key frame.</td>
</tr>
<tr>
<td>Unsecured default settings</td>
<td>Many products have default settings that allows security holes.</td>
</tr>
<tr>
<td>within products</td>
<td></td>
</tr>
<tr>
<td>Misconfigured network equipment</td>
<td>Misconfigurations of the equipment itself can cause significant security protocols, or SNMP community strings can open up large security holes.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Finally, E-Mail is extremely vulnerable and sensitive to a number of different attacks.

Table 3, shows identify the potential “threats” of these elements. The general threats on router or firewall network device include but are not limited: unauthorized access, session hijacking, rerouting, masquerading, denial of service (DOS), and information theft. We are presenting some attack techniques that can be cause for slow network performance, uncontrolled traffic, viruses etc. Then Attack techniques include: password guessing, routing protocol attacks, simple network management protocol (SNMP) attacks, IP fragmentation attacks – to bypass filtering, redirect (address) attacks, and circular redirect – for denial of service. We will explain the action of some attacks.

<table>
<thead>
<tr>
<th>Threat</th>
<th>Internal \ External</th>
<th>Threat consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>e-mail with virus</td>
<td>External origination, internal use</td>
<td>Could infect system reading email and subsequently spread throughout the entire organization.</td>
</tr>
<tr>
<td>Net-work virus</td>
<td>External</td>
<td>Could enter through unprotected ports, compromise whole network.</td>
</tr>
<tr>
<td>Web based virus</td>
<td>Internal browsing to external sites</td>
<td>Could cause compromise on system doing browsing and subsequently affect other internal systems.</td>
</tr>
</tbody>
</table>

1. The session attacks use a sequence of packets or application commands that can be recorded, possibly manipulated, and then replayed to cause an unauthorized access.

2. Rerouting attacks are including manipulating router updates to cause traffic to flow to unauthorized destinations. These kinds of attacks are sometimes called “route injection” attacks.

3. Masquerade attacks, these attacks occur when attackers manipulates IP packets to fake IP addresses.

4. Land attack, the land attacks are connect to sending a packet to the router with same IP address in the source and destination address fields, and with the same port and destination port fields.

5. Session hijacking attacks, this attack can insert falsified IP packets after session installation by IP spoofing, the sequent number prediction and alteration.
3.2 Router and Firewall Security Policy

Routers and firewalls perform many different jobs in modern networks, forwards traffic between two or more local networks within endeavor routers. The traffic between the different networks that make up the Internet is directed by backbone routers. Interior routers may introduce some restrictions on the traffic and they are forward between networks. Forwards traffic between different establishments.

The level of trust between the networks are associated by a backbone router is very low. Those routers are designed and configured to forward traffic as quickly as possible. The primary security objects for a backbone router are to ensure that the management and operation of the router are conducted. That security is only by constitutional parties, and to protect the integrity of the routing information it uses to forward traffic. That connected network without imposing any restrictions on it. The backbone routers employ Exterior Gateway Protocols to manage routes [5].

4. TEST BED PERFORMANCE TESTING

Test the security and performance of the recommended network model, a test bed was build and constitute as shown in Figure. The test bed is consisted from the two Cisco routers 2811, Cisco firewall (PIX) 516E, Cisco switch 2960, AAA (Authentication Authorization Attacks) server with TACACS+ protocol and two workstation work as the real attacker and hacker. The following procedures are taken to examine the network security straightforward against different types of attacks.

1. The program was used to simulate original investigation network that attacks on the target network. That testing program used to see what is on the network, the network program is an effective “sniffer”.

2. The Nmap program which is used to scan for open TCP and UDP ports are on a router and firewall interface ports.

3. The Super Scanner program use to simulate the original access attacks that are find the IP address is working in network and open in the network. The purpose of to obtaining the network IP address of a workstation or IP address of a network device, port scanner to discover which port is used and open.
4. Unconstitutional attempts are access to the network resources and devices, this operation was detected and prevented by AAA server and firewall network because both incoming and outgoing traffic in the networks.

5. This program is used to search the weaknesses in the network. This operation was prevented by incapacitated unused interfaces of all routers and firewall. The disable unneeded feature and services on route such as: CDP, http server, boot server, IP directed broadcast, TCP and UDP small services.

![Router with firewall configuration for a network test bed](image)

**Figure: Router with firewall configuration for a network test bed**

6. There are many uses of Mac tools program to manage the MAC spoofing and CAM table overflow attacks. This action was anticipated by apply port security on the switch in three ways: static secure MAC addresses, Dynamic secure MAC addresses and sticky secure MAC addresses.

5. **ACKNOWLEDGEMENT**

I would like to thank to Prof. Amit. M. Bajare for his advice and guidance from the start to the final level to build research paper, His quick invaluable observation has always been very helpful. They inspire and motivating me at each stage of the project and they also provides suggestions or hints whenever that require with respect to project.

5. **CONCLUSION**

This paper discusses the security weaknesses in routing and firewall configuration system and risk when connected to the Internet. Also this paper presented the tips and suggestion to achieve a best security and to protect the network from vulnerabilities, threats, and attacks by applying a security configuration on router and firewall. This work appears the firewall provides...
additional access control over connections and network traffic and perform user authentication. A poor router filtering configuration can reduce the overall security of a network that expose internal network components to scan and attacks.

REFERENCES


