International Journal of Engineering Research & Management Technology

ISSN: 2348-4039

September- 2014 Volume 1, Issue-5

Email: editor@ijermt.org www.ijermt.org

# Network Security Attacks – An Overview

**Gulshan Kumar**
Assistant Professor
SBS State Technical Campus
Ferozepur (Punjab)-India

**Sania Sethi, Amanjeet Kaur**
Reseach Scholar
SBS State Technical Campus
Ferozepur (Punjab)-India

## ABSTRACT

The Web has been perhaps the most outstanding innovation in the field of communication in the history of mankind. There are different kinds of applications like Social Networking Sites, Communication, Entertainment, Job Searches, Online or e-Shopping provided by the Internet. With the usage of these applications Network Security must be there to access the information safely.

Network security includes elements that prevent unwanted activities while supporting desirable activities. Efficient network security provides quick and easy access to resources for users. Hackers, viruses, vindictive employees and even human error all represent clear and present dangers to network. Threats, both internal and external, can cause a catastrophic system failure or compromise. And all computers users from the most casual Internet surfers to large enterprises could be affected by network security breaches. Network security must support workers in doing their jobs white protecting against compromise, maintaining high performance and keeping costs to a minimum. This paper provides you an overview of the most common network security threats. The paper will help the readers to understand of network attacks and current scenario of network attacks.

## I INTRODUCTION

Computer and network security is a new and fast moving Technology and as such, is still being defined and most probably will always be "still defined". Security incidents are rising at an alarming rate every year. As the complexity of the threats increases, so do the security measures required to protect networks. Data center operators, network administrators, and other data center professionals need to comprehend the basics of security in order to safely deploy and manage networks today.

With the ever- increasing number and complexity of attacks, vigilant approaches to security in both large and small enterprises are a must network security originally focused on algorithmic aspects such as encryption and hashing techniques [9]. While these concepts rarely change, these skills alone are insufficient to protect computer networks. As crackers hacked away at networks and systems, security courses arose that emphasized the latest attacks. There is always fault management, fault software, abuse of resources connecting to computer networks. These are the main reasons which cause security problems for a Network. Today, security problem has become one of the main problems for computer network and internet developing. However, there is no simple way to establish a secure computer network. In fact, we cannot find a network in the world, which does not have any security holes nowadays. The infrastructure of cyberspace is vulnerable due to three kinds of failure: Complexity, accident, and hostile intent **[1].**

Hundreds of millions of people now appreciate a cyber context for terms like "viruses", "denial of services", "privacy", "worms", "fraud", "crime" more generally. Attacks so far have been limited. While in some network attacks the value of losses is in the hundreds of millions, are damaged so far is seen as tolerable. The more specific defenses to be discussed may be usefully partitioned into two forms: **passive and active [2].**

Passive defense essentially consists in target hardening **[3].**

Active defense, in contrast, imposes some risk or penalty on the attacker. Risk or penalty may include identification and exposure, investigation and prosecution, or preemptive or counter attacks of various sorts **[4].**

## II Security principles and attacks

Three basic security concepts important to computer systems are confidentiality, integrity, and availability (CIA) [9].

### A. Confidentiality

When information is read or copied by someone not authorized to do so, the result is known as loss of confidentiality. For some types of information, confidentiality is a very important attribute. Examples include research data, medical and insurance records, new product specifications, and corporate investment strategies. In some locations, there may be a legal obligation to protect the privacy of individuals. This is particularly true for banks and loan companies; debt collectors; businesses that extend credit to their customers or issue credit cards; hospitals, doctors' offices, and medical testing laboratories; individuals or agencies that offer services such as psychological counseling or drug treatment; and agencies that collect taxes. Information can be corrupted when it is available on an insecure network.

Authentication and access control techniques are used to achieve Confidentiality and are mentioned in the section security practices.

**Confidentiality Attacks**

It is a passive form of attack where the attacker attempts to obtain confidential information about network users like login credentials, SSN, Credit Card information or e-mail password. This kind of attack may go undetected if the attacker masquerades as a legitimate user and then snoops private information, rather than trying to tamper with the data or crash the system. **[5]**

In most cases, application server, web server and database server interact with each other based on mutual trust relationships. So when an attacker becomes able to compromise the confidentiality of a web server, eventually he gets access to the sensitive data stored in database server as well. **An attacker can launch a confidentiality attack in the following ways:**

a. **Dumpster Diving:** The attacker obtains credential and other private information from un-shredded papers dumped in office bins.
b. **Social Engineering:** In most applications, users tend to generate passwords based on their dates of birth, some family-member's name, etc. An attacker can socialize with the target user to obtain his/her personal detail, and then use that information for guessing passwords
c. **Wire Tapping:** If the attacker is located in close physical vicinity of the target network. Then (s)he can tap into network lines and snoop over secret messages.
d. **Packet Capture:** The attacker can easily capture data packets travelling across a network. Therefore, by systematically intercepting a hub with which the victim is connected, or by tricking the packets to flow through his system by acting as a honeypot, the attacker can obtain a lot of sensitive information.
e. **Ping Sweep and Port Scanning:** An attacker can flood a network with a list of pings and capture positive responses from one or some of the pings. This allows him/her to glean a list of IP addresses of all network devices. After successfully locating device IP addresses, the attacker scans a range of servicing UDP and TCP ports to identify potential targets **[6].**

### B. Integrity

When information is modified in unexpected ways, the result is known as loss of integrity. This means that unauthorized changes are made to information, whether by human error. Integrity is particularly important for critical safety and financial data used for activities such as electronic funds transfers, air traffic control, and financial accounting. Information can be erased or become inaccessible, resulting in loss of availability. This means that people who are authorized to get information cannot get what they need **[7].**

**Integrity Attacks**

Integrity attack is based on confidentiality attack, except that the attacker does not stop after snooping, data; rather, (s) he tries to modify the content

**An integrity attack can be launched in the following ways:**

a. **Botnet attacks:**The attacker writes a piece of software called network robot ("botnet in short") and injects into the target system. This malicious piece or code makes the whole infected system act like a slave, thereby compromising the integrity and confidentiality of huge amounts of data.
b. Password attacks using Trojan horse, packet capture, key logger application or dictionary attacks to obtain user credentials from the system.
c. Hijacking legitimate TCP sessions.
d. Salami attack: Salami attack or penny shaving attack is a series of smaller attacks, which taken together engenders a devastating consequence [6].

**C. Availability**

Availability is often the most important attribute in service-oriented businesses that depend on information (e.g., airline schedules and online inventory systems). Availability of the network itself is important to anyone whose business or education relies on a network connection. When a user cannot get access to the network or specific services provided on the network, they experience a denial of service [5]. The major attack on the availability of networks is Denial of Service attack (DoS) [9]. The DoS attack consumes the network resources and make them unavailable to legitimate users.

**III Current Focus of Network Security**

The Network Security program emphasizes to secure a network. The following background information on security helps in making correct decisions. Some areas are conceptualized-oriented:

- **Attack Recognition:** Recognize common attacks, such as spoofing, man-in-the-middle, denial of service, buffer overflow, etc.
- **Encryption techniques:** Understand techniques to ensure confidentiality, authenticity, integrity, and no repudiation of data transfer. There must be understood at a protocol and at least partially at a mathematician or algorithmic level, in order to select and implement the algorithm matching the organization's needs.
- **Network Security Architecture:** Configure a network with security appliances and software, such as placement of firewalls, Intrusion Direction Systems, and log management.
- **Protocol analysis:** Recognize normal from abnormal protocol sequences, using sniffers. Protocols minimally include: IP, ARP, ICMP, TCP, UDP, HTTP, and encryption protocols: SSH, SSL, IPSec.
  - ✓ **Access Control Lists (ACLs):** Configure and audit routers and firewalls to filter packets accurately and efficiently, by dropping, passing, or protecting packets based upon their IP and/or port addresses, and state.
  - ✓ **Intrusion Detection/Prevention Systems:** Set and test rules to recognize and report attacks in a timely manner.
  - ✓ **Vulnerability Testing:** test all nodes to determine active applications, via scanning or other vulnerability test tools- and interpret results.
  - ✓ **Application Software Protection:** Program and test secure software to avoid backdoor entry via SQL injection, buffer overflow, etc.
  - ✓ **Incident response:** Respond to an attack by escalating attention, collecting evidence, and performing computer forensics. The last three skills incorporate computer systems security, since they are required

to counteract internet hacking. Network security applies business decision in a technical manner. Business requirement drives security implementations. Business-related skills include:

- ✓ **Security Evaluation:** Use risk analysis to determine what should be protected and at what cost.
- ✓ **Security Planning:** Prepare a security plan, including security policies and procedures.
- ✓ **Audit:** Prepare an Audit Plan and Report
- ✓ **Legal Response:** Understanding and interpreting the law regarding responding to computer/network attacks, corporate responsibility, and computer forensics [8].

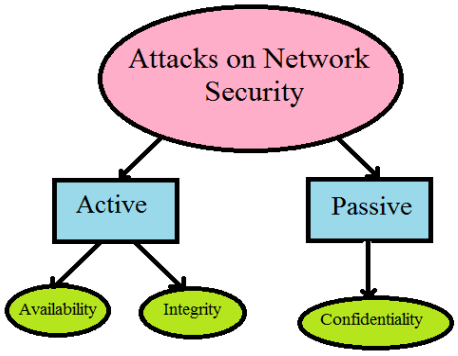


**Figure 1. Classification of network attacks**

## IV CONCLUSIONS

Network security includes elements that prevent unwanted activities while supporting desirable activities. Efficient network security provides quick and easy access to resources for users. Hackers, viruses, vindictive employees and even human error all represent clear and present dangers to network. Threats, both internal and external, can cause a catastrophic system failure or compromise. And all computers users from the most casual Internet surfers to large enterprises could be affected by network security breaches. Network security must support workers in doing their jobs white protecting against compromise, maintaining high performance and keeping costs to a minimum.

## REFERENCES

1. Suyog Dixit & Dr. R.K. Dixit, "Google Query-Serving Architecture", National Conference sponsored by NACC (National Assessment and Accreditation Council), 2010.
2. American Bar Association International Cyber Crime Project of the ABA Privacy and Computer Crime Committee: http://www.abanet.org/scitech/computercrime/cybercrimeprobject.html Accessed on 10-10-2014.
3. A. R. F. Hamedani, "Network Security Issues, Tools for Testing," School of Information Science, Halmstad University, 2010.
4. R. E. Mahan, "Introduction to Computer & Network Security," Washington State University, 2000.
5. McCabe M. Comment from the conflicts of interest, Privacy/Confidentiality, and Tissue Repositories: Protections, Policies, and Practical Strategies Conference co-sponsored by PRIM&R and the Columbia University Center for Bioethics. 2004 May 3-5; Boston, M.A.
6. Council of Europe. Convention on Cyber crime ETS no.: 185-Explanatory Report 23 November 2001
7. Raju Kumar, Sharanya Eswaran, and Thomas La Porta. End-to-End Rate Selection for Opportunistic Reception in Multi-Rate Wireless Networks. Technical Report NAS-TR-0128-2010, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, April 2010.
8. Li CHEN, Web Security: Theory And Applications, School of Software, Sun Yat-sen University, China.
9. Kumar, Gulshan, and Krishan Kumar. "Network security–an updated perspective." Systems Science & Control Engineering: An Open Access Journal 2.1 (2014): 325-334.