Internet Security - Bridge to Prevent Cyber Crimes

Simar Preet Singh
Research Scholar
University College of Engineering,
Punjabi University Patiala, Punjab, India - 147002

A Raman Maini
Associate Professor
University College of Engineering,
Punjabi University Patiala, Punjab, India - 147002

ABSTRACT

Since Internet Security is in the forefront of Cyber Crimes for protection from attackers, it is crucial to have a good understanding of threats of Internet Security. This paper evaluates the importance and need of the internet security with different kinds of threats related to internet security. Different kinds of internet security measures are studied in order to evaluate the threats of internet security. Further, the various types of internet security are studied to validate the threats. It has been observed that the Cyber Crimes are increasing these days due to lack of awareness of the user, and the lack of knowledge of preventing from those attacks.

Keywords

Network Security, E-mail Security, Threats, Keyloggers.

1. INTRODUCTION

The major function of Internet security is that it is a branch of computer security specifically related to the Internet. The objective of internet security is to establish rules and measure to use against attacks over the Internet. The Internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud[5].

There are 2 types of Internet Security. These are:
1. Network Security

2. Electronic-mail Security (E-mail Security)

In this paper, the first part contains introduction regarding the network security followed by the treats that can be there in network security.

After the network security, comes the E-mail security. We concluded the introduction regarding the E-mail security and then various threats regarding E-mail security.

2. NETWORK SECURITY

Network Security consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification or denial of the computer network and network-accessible resources. There is huge need for the Network Security. The need of network security is in-

a) Hacking
b) Security Related Crimes
c) E-mail Bombing
d) Denail of Service Attacks

3. NETWORK SECURITY THREATS

There are various threats in Network Security. The main threats are:

a) Denail of Service

b) TCP Attacks

c) Packet Sniffing

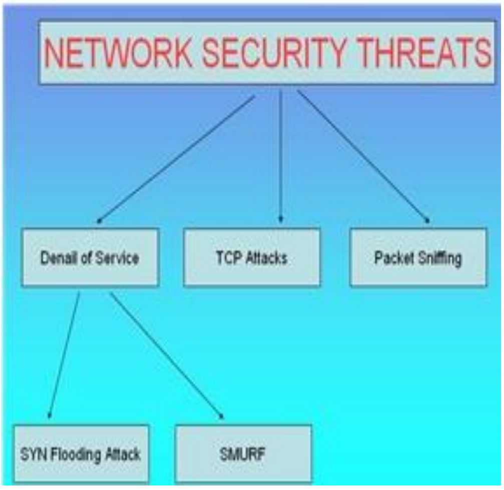

Figure 1: Network Security Threats

These threats are explained as follows:

a) Denail of Service & TCP Attacks: The purpose of the denial of service attack is to make the network service unusable, usually by overloading the server or network. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer[3].

The most common and obvious type of DoS attack occurs when an attacker "floods" a network with information. When you type a URL for a particular website into your browser, you are sending a request to that site's computer server to view the page. The server can only process a certain number of requests at once, so if an attacker overloads the server with requests, it can't process your request. This is a "denial of service" because you can't access that site.

An attacker can use spam email messages to launch a

similar attack on your email account. Whether you have an email account supplied by your employer or one available through a free service such as Yahoo or Hotmail, you are assigned a specific quota, which limits the amount of data you can have in your account at any given time. By sending many, or large, email messages to the account, an attacker can consume your quota, preventing you from receiving legitimate messages.

If we want to avoid this problem then unfortunately,

- there are no effective ways to prevent being the victim of a
- DoS attack, but there are steps you can take to reduce the
- likelihood that an attacker will use your computer to attack
- other computers. The various steps that one can take are
    - Install and maintain anti-virus software.
    - Install a firewall, and configure it to restrict traffic
- Coming into and leaving your computer.
    - Follow good security practices for distributing
- Your email address. Applying email filters may help you manage unwanted traffic.
- This attack has few symptoms from where we can jugde the presence of this allack in the computer. The following symptoms could indicate a DoS attack:
    - Unusually slow network performance (opening
- Files or accessing websites).
    - Unavailability of a particular website.
    - Inability to access any website.
    - Dramatic increase in the amount of spam you
- Receive in your account.

There are many different kinds of DoS attacks:

➢ SYN flooding

➢ SMURF

SYN FLOODING An SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system. When a client attempts to start a TCP connection to a server, the client and server exchange a series of messages which normally runs like this:

1. The client requests a connection by sending a SYN (synchronize) message to the server.

2. The server acknowledges this request by sending SYN-ACK back to the client.

3. The client responds with an ACK, and the connection is established.

This is called the TCP three-way handshake, and is the foundation for every connection established using the TCP protocol.

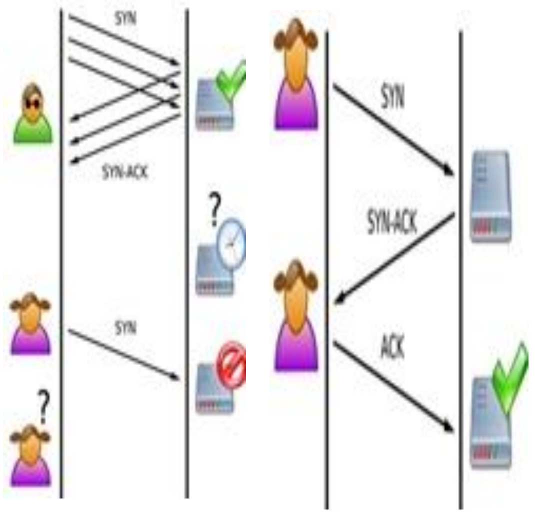

Figure 2: (a) A normal connection between a user (Alice) and a server. The three-way handshake is correctly performed. (b) SYN Flood.

The attacker (Mallory) sends several packets but does not send the "ACK" back to the server. The connections are hence half-opened and consuming server resources. Alice, a legitimate user, tries to connect but the server refuses to open a connection resulting in a denial of service.

The SYN flood is a well known type of attack and is generally not effective against modern networks. It works if a server allocates resources after receiving a SYN, but before it has received the ACK.

There are two methods, but both involve the server not receiving the ACK. A malicious client can skip sending this last ACK message. Or by spoofing the source IP address in the SYN, it makes the server send the SYN- ACK to the falsified IP address, and thus never receive the ACK. In both cases the server will wait for the acknowledgement for some time, as simple network congestion could also be the cause of the missing ACK.

- SMURF the Smurf attack is a way of generating significant computer network traffic on a victim network. This is a type of denial-of-service attack that floods a target system via spoofed broadcast ping messages.[3]. Key features of Smurf attack are-.
- Source IP address of a broadcast ping is forged.
- Large number of machines respond back to victim,

  Overloading it.

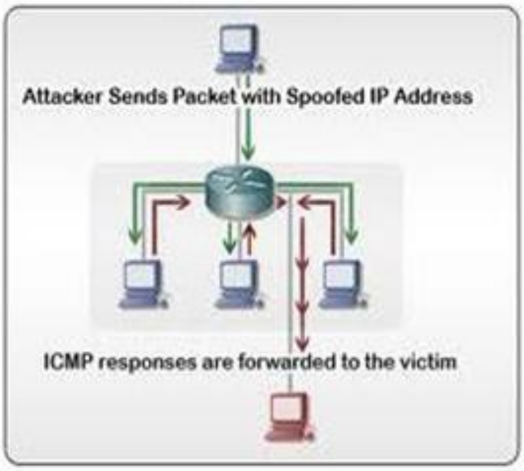
Attacker Sends Packet with Spoofed IP Address
ICMP responses are forwarded to the victim

Figure 3: Smurf Attack

b)Packet Sniffing: When someone wants to send a packet to some else, they put the bits on the wire with the destination MAC address and remember that other hosts are listening on the wire to detect for collisions. It couldn"t get any easier to figure out what data is being transmitted over the network. This works for wireless too. In fact, it works for any broadcast-based medium.

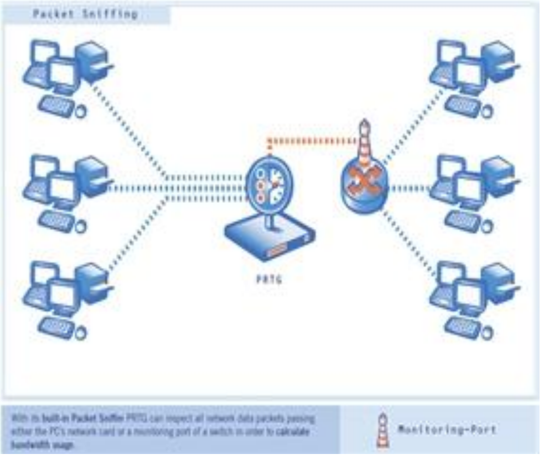
Packet Sniffing
PRTG
With its built-in Packet Sniffer PRTG can inspect all network data packets passing either the PC's network card or a monitoring port of a switch in order to calculate bandwidth usage.
Monitoring-Port

Figure 4: Smurf Attack

- The kind of data that we can get or in another way, kind of information that would be most useful to a malicious user is anything in plain text. Passwords are the most popular. We can protect ourselves by using various softwares-

- SSH, not Telnet

- Many people at CMU still use Telnet and send their password in the clear (use PuTTY instead!)

- Packet sniffing is, by the way, prohibited by Computing Services

- HTTP over SSL - Especially when making purchases with credit

unauthorized individual. Availability of email involves ensuring that mail servers remain online and able to service the user community. A weakness in any one of these three key areas will undermine the security posture of an email system and open the door to exploitation.

4. E-MAIL THREATS

Email Threats are as following:
Practically there are two types of Key loggers.
1) Software key logger
2) Hardware Key logger

Software key logger: A software that after being installed on victims pc, continuously maintain a log of pressed keys and screenshots that can be seen personally or remotely. This may also log your login details of your bank account.
Source: bootable cd, Zip or compress files, malicious E-mail.

Hardware Key Logger: A hardware that costs around 600 to 900rs is also capable of maintaining a log of the keys pressed by you.
Source: Cabinet easily accessible
Security Tip: Never let your Cabinet exposed.

1)Phishing Attack: A duplicate login screen is generated by viewing the source code option in internet explorer. That source code is copied and with a minute change in POST method, new web page is stored on a different server. The new link prank is sent to victim, and if victim fall in such prank, he/she fill his login details to Phishing page, that forward a copy of typed username and password to the desired address of hacker.
Security Tip: Check the URL, before surfing a website

Hyperlink - Shortcut To Become A Victim: Never click any un-trusted link, it may contain a transaction query, that directly execute a bank transaction, transaction may be of money transfer. Truth about E-Transaction: After filling a website form for any transaction, those filled details are triggered to bank server in a form of a address in the address bar, hacker copy this standard link, and paste it under and text, such that if linked is pressed, the transaction executes simultaneously and you may become a victim.
Security Tip: Do not click on unusual links.

2) Read Notify: Read notify is an internet service that unable a user to trace a mail sent by him. This feature is available on internet at www.readnotify.com . Demo version for 15 days or paid for full access. Initially a hacker makes an account on readnotify with a particular email address. Then he opens that email account to send a mail to victim such that in "TO" field email address is written in particular format i.e. victim@abc.com.readnotify.com. when mail is opened by the recipient, a automatic reply is sent to the hacker about the recipient identity including IP address, operating system geographical location and other details.
Security Tip: Don"t open unknown sender"s mail.

3) Email Bombing: This is the technique in which a hacker sends millions of mail to the victim which may irritate him for a long time.
Security Tip: Add attacker‟s mail address to spam or block list.
4) Malicious signature: A mail signature is a feature by which a sender may add a common text or any multimedia to his all out-going mails. Multimedia is added in mail using HTML language. This language is also capable of developing virus, Trojans and other malicious scripts.
Security Tip: Disable javascript from your web browser.
7) Email spoofing: A spoofed mail is an ordinary mail to any victim using other‟s identity. There are many website that provide a free feature of writing a mail to the victims using anybody‟s mail address without knowing his password.
Security Tip: confirm the sender‟s identity on receiving suspicious mails. Use auto response feature.

8) Malicious attachment: Generally all Mail servers provide an opportunity of sending, receiving and
scanning an attachment. If that attachment is in zip file, then sometime these scanners failed to find virus in them. Now hackers have found some new tricks to send a virus in these attachments. Virus can easily be attached to any MS office file with the help of macros. An inbuilt feature that provides a utility to the composer to add visual basic program to a word, excel and other files can make it possible[8].

Security Tip: Check the attachment with updated antiviruses.
9) Remember my password: Usually, many web login screens have an option of "remember me". one must avoid them by disabling them because these remember passwords can easily be retrieved using 3rd party option.

5. CONCLUSION

Internet security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. The environment in which machines must survive has changed radically since the popularization of the Internet. The root of most internet problems is the internet security that fails in unexpected ways.

Good Internet Security practices can help ensure that internet communication behaves properly. In this report, I have tried to explain various treats related to Network Security and E-Mail Security, as E-Mails are prevalent in every sphere of human life these days. Thus, one should have the sufficient knowledge about these threats, in order avoid semantic gap.

6. REFERENCES

[1] Simmonds, A; Sandilands, P; van Ekert, L (2004). "An Ontology for Network Security Attacks". Lecture Notes in Computer Science 3285: 317-323.

[2] A Role-Based Trusted Network Provides Pervasive Security and Compliance - interview with Jayshree Ullal, senior VP of Cisco

[3] William R. Cheswick, Steven M. Bellovin „Firewalls And Internet Security‟, Second Edition, pp.107-110, April
2003.

[4] John R. Vacca, „Practical Internet Security‟, published in 2007.

[5] Dave Dittrich, Network monitoring/Intrusion Detection Systems (IDS), University of Washington.

[6] Julian Fredin, Social software development program Wi-Tech

[7] Introduction to Network Security, Matt Curtin. [8] Hans -AntiHacking Anticipation Society

[9] Security Monitoring with Cisco Security MARS, Gary Halleen/Greg Kellogg, Cisco Press

[10] Network Security: PRIVATE Communication in a PUBLIC World, Charlie Kaufman | Radia Perlman | Mike Speciner, Prentice-Hall, 2002. ISBN .

[11] Network Infrastructure Security, Angus Wong and Alan Yeung, Springer, 2009.