Network Security : Attacks and Defence.

Sahil Mudgal, Pooja Nayak, Rajat Wason

ABSTRACT

Network Security has become very important in today's world, as a result of which various methods are adopted to prevent it. Network administrators need to keep up with the recent advancements in both the hardware and software fields to prevent their as well as the user's data. This paper describes the various attack methods which are used, as well as various defence mechanism against them.

Terms Used: DOS attacks, Firewalls, Encryption, Port Scanning, SSL, SHTTP, VPN

I. INTRODUCTION

Internet security is a fashionable and fast-moving field; the attacks that are catching the headlines can change significantly from one year to the next. Regardless of whether they're directly relevant to the work you do, network-based attacks are so high-profile that they are likely to have some impact, even if you only use hacker stories to get your client to allocate increased budgets to counter the more serious threats. The point is, some knowledge of the subject is essential for the working security engineer.

A network consists of routers from which information can be easily stolen by the use of malwares such as a "Trojan Horses". The synchronous network consist of switches and since they do not buffer any data and hence are not required to be protected. Network security is thus mainly focused on the data networks and on the devices which are used to link to the internet. Email is a widely used service today and it is also contain many serious flaws, there is no system of authenticating the sender as well as the recipient, it is stored in multiple places during transmission and can be easily intercepted and changed. SPAM are serious security threat they only require very less manpower but affect millions to billions of Email users around the world, they can malicious link or even false advertisements. A network contains many vulnerabilities but most of them can fixed by following very simple procedures, such as updating software and correctly configuring network and firewall rules, using a good anti-virus software etc.In this report most of the basic information regarding network security will be outlined such as finding and closing vulnerabilities and preventing network attacks and also security measures currently being used.

II. DIFFERENT TYPES OF SECURITY ATTACKS

A. Passive Attacks

This type of attacks includes attempts to break the system using observed data. One of its example is plain text attack, where both the plain text and cipher text are already known to the attacker.

Properties of passive attacks are as follows:

- **Interception:** The data passing through a network can be easily sniffed and thus attacking the confidentiality of the user, such as eavesdropping, "Man in the middle" attacks
- **Traffic analysis:** Also attacks confidentiality. It can include trace back on a network like a CRT radiation.

B. Active Attacks

In this attack the attacker sends data stream to one or both the parties involved or he can also completely cut off the data stream. Its attributes are as follows:

- **Interruption:** It prevents an authenticated user form accessing the site. It attacks availability. Such as DOS attacks.
- **Modification:** In this the data is modified mostly during transmission. It attacks integrity.
- **Fabrication:** Creating counterfeit items on a network without proper authorization. It attacks authentication.

C. DOS Attack

DOS attacks today have become a major threat to network security all over the world. They can be easily launched by anyone with the basic knowledge of network security. They don’t require as much time and planning as some other attacks, in short they are cheap and efficient method of attacking networks. They can shutdown the company network by overflowing it with requests and thus affects availability of the network. With the help of easy to use network tools such as Trinoo, which can be easily downloaded of the internet any normal user can initiate an attack. DOS attacks usually works by exhausting the targeted network of bandwidth, TCP connections buffer, application/service buffer, CPU cycles, etc. DOS attacks use many users connected to a network known as zombies most of the time users are unaware of that their computer is infected .

1. Different Types of DOS Attacks.

Many attacks are used to perform a DOS attack so as to disable service. Some of which are as follows: TCP SYN Flooding. When a client wants to connect to the server, the client first sends to an SYN message to the server. The server then responds to the client by sending a SYN-ACK message to the client. The client completes the connection by sending an ACK message. The connection is now established and data can be transferred easily. The problem arises when the connections remain half open and the server waits for the client side to send an ACK message. This takes system resources and the server will wait till the expiration date. The person exploiting the server will never send the ACK message and will keep on sending new connection demand, till the server is overloaded, thus cannot provide access [3].

ICMP Smurf Flooding: ICMP package is used to know whether the server is responding or not. The server replies with an ICMP echo command. In smurf attack the attacking host forges the ICMP echo requests having victims address as the source and the broadcast address of remote networks. These computers will then send back ICMP echo reply package to source, thus congesting victim's network.

UDP Flooding: Many networks now use TCP and ICMP protocols to prevent DOS attacks but a hacker can send large number of packages as UDP overloading the victim and preventing any new connection.

III. DEFENCE AGAINST NETWORK ATTACKS

An inherent weakness in the system may it be by design, configuration or implementation which renders it to a threat. But most of the vulnerabilities are not because of faulty design but some may be caused due to disasters both natural and made, or some maybe cause by the by same persons trying to protect the system [2].Most of the Vulnerabilities caused due to poor design, poor implementation, poor management, physical vulnerabilities, hardware and software, interception of information andhuman vulnerabilities. Many of the network attacks can be easily prevented by the network admin monitoring his network closely and applying the entire latest patch available from the vendor to his software. However this cannot prevent most of the attacks, to prevent them, the network requires configurations such as:

A. Configuration Management

It is as important as having a descent firewall to protect the system. As soon as a network setup is completed all its default logins, Ids, address must be changed as soon as possible as all these information is available on the internet for anyone to view. Anyone can use the default login to gain access to the network and it can put all the network at risk. The machines inside the network must be running the running up to date copies of O and all the patches especially the security patches must be installed as soon as they are available, configuration files must not have any known security holes, all the data is backed up in a secure manner, it allows us to deal with nine out of the ten topmost attacks. Several tools are also available which allows patches to deployed simultaneously and keep things tight.

B. Firewalls

The most widely sold solution to the problems of Internet security is the *firewall*. This is a machine that stands between a local network and the Internet, and filters out traffic that might be harmful. The idea of a "solution in a box" has great appeal to many organizations, and is now so widely accepted that it's seen as an essential part of corporate due diligence. (Many purchasers prefer expensive firewalls to good ones.)

Firewalls come in basically three flavors, depending on whether they filter at the IP packet level, at the TCP session level, or at the application level.

Packet Filtering

The simplest kind of firewall merely filters packet addresses and port numbers. This functionality is also available in routers and in Linux. It can block the kind of IP spoofing attack discussed earlier by ensuring that no packet that appears to come from a host on the local network is allowed to enter from outside. It can also stop denial-ofservice attacks in which malformed packets are sent to a host, or the host is persuaded to connect to itself (both of which can be a problem for people still running Windows 95).

Basic packet filtering is available as standard in Linux, but, as far as incoming attacks are concerned, it can be defeated by a number of tricks. For example, a packet can be fragmented in such a way that the initial fragment (which passes the firewall's inspection) is overwritten by a subsequent fragment, thereby replacing an address with one that violates the firewall's security policy.

Circuit Gateways

More complex firewalls, called *circuit gateways*, reassemble and examine all the packets in each TCP circuit. This is more expensive than simple packet filtering, and can also provide added functionality, such as providing a virtual private network over the Internet by doing encryption from firewall to firewall, and screening out black-listed Web sites or newsgroups (there have been reports of Asian governments building national firewalls for this purpose).

However, circuit-level protection can't prevent attacks at the application level, such as malicious code.

Application Relays

The third type of firewall is the *application relay*, which acts as a proxy for one or more services, such as mail, telnet, and Web. It's at this level that you can enforce rules such as stripping out macros from incoming Word documents, and removing active content from Web pages. These can provide very comprehensive protection against a wide range of threats.

The downside is that application relays can turn out to be serious bottlenecks. They can also get in the way of users who want to run the latest applications.

Combinations

At really paranoid sites, multiple firewalls may be used. There may be a *choke*, or packet filter, connecting the outside world to a screened subnet, also known as a *demilitarized zone* (DMZ), which contains a number of application servers or proxies to filter mail and other services. The DMZ may then be connected to the internal network via a further filter that does network address translation. Within the organization, there may be further boundary control devices, including pumps to separate departments, or networks operating at different clearance levels to ensure that classified information doesn't escape either outward or downward (Figure 1).

Such elaborate installations can impose significant operational costs, as many routine messages need to be inspected and passed by hand. This can get in the way so much that people install unauthorized back doors, such as dial-up standalone machines, to get their work done. And if your main controls are aimed at preventing information leaking outward, there may be little to stop a virus getting in. Once in a place it wasn't expected, it can cause serious havoc.

IV. Strengths and Limitations of Firewalls

Since firewalls do only a small number of things, it's possible to make them very simple, and to remove many of the complex components from the underlying operating system (such as the RPC and sendmail facilities in Unix). This eliminates a lot of vulnerabilities and sources of error. Organizations are also attracted by the idea of having only a small number of boxes to manage, rather than having to do proper system administration for a large, heterogeneous population of machines.

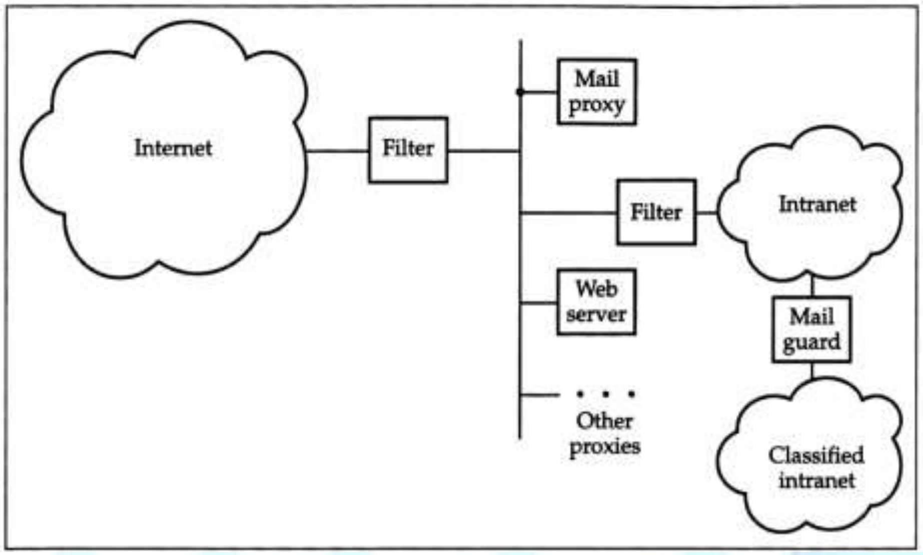

Figure 1 . Multiple firewalls.

C. Defence against DOS Attacks

To prevent DDoS attack many technologies have been developed such as intrusion detection systems (IDSs), firewalls, and enhanced routers. These things are used between the internet and servers. They monitor incoming connections as well as outgoing connections and automatically take steps to protect the network. They have traffic analysis, access control, redundancy built into them [15].IDSs are make a log of both the incoming and outgoing connections. These logs can then be compared to baseline traffic to detect potential Dos attacks. If there is unusually high traffic on the server it can also alert of a possible ongoing DOS attack such as TCP SYN flooding [14].Firewalls can also be used as defence against DOS attacks with the required configuration. Firewalls can be used to allow or deny certain packets, ports and IP addresses etc. Firewalls can also perform real time evaluation of the traffic and take the necessary steps to prevent the attack. Security measures can also be employed in routers which can create another defence line away from the target, so even if a DOS attack takes place it won't affect the internal network.

Service providers can also increase the service quality of infrastructure. Whenever a server fails a backup server can take its place, this will make effect of DOS attack negligible. If the service providers are able to distribute the heavy traffic of a DOS attack over a wide network quickly it can also prevent DOS attacks, however this method require computer and network resources and they can be very costly to provide on daily basis as a result only very big companies opt for this method.

D. Vulnerability Testing

To prevent any attacks on the network, one must find any open vulnerabilities in the network and close them, these may include open ports and also faulty and outdated software with known vulnerabilities, outdated firewall rules etc. There are different tools available which allows a user to test his own network security and also find vulnerabilities in a network [4]. One such method is using a port scanner which can be used to probe a server and find any open ports. This is used by many admins to verify policies of their servers and also can be used by attackers on a network to find exploits. Some of the tools which are available for free on the internet are Nmap, SuperScan. These tools can be downloaded by everyone and each comes with a detailed tutorial for using them.

V. ENCRYPTING THE WORLD WIDE WEB (WWW)

For the sake of privacy, confidentiality and availability our communications on the web should always be encrypted this reduces the number of attacks and prevents anyone to view the ongoing transmissions. These can be achieved by putting together a system of encryption and employing a system of digital certificates. The most important way of encryption is the SSL protocol [7].Network security can also be compared to human system. The human system can be taken as analogy, providing a protection at each point just like a body we can greatly improve the security. Using this mechanism we can spread our resources and prevent dependent on one system.

A. Secure Sockets Layer

It uses both asymmetric and symmetric keys encryption transfer data in a secure mode over a network. When SSL is used in a browser it establish a secure connection between the browser and the server. It’s like an encrypted tunnel in which the data can flow securely. Anyone listening on the network cannot decipher the data flowing in the tunnel. It provides integrity using hashing algorithms and confidentiality using encryption.The session begins with an asymmetric encryption. The server then sends the client its public key. After the asymmetric connection both the sides switches to a symmetric connection. Asymmetric algorithms are slow and uses much more CPU power than symmetric ones. Even while symmetric encryption, CPU load is high, servers can only handle a fraction of connections as compared to servers with no encryption .

B. Secure HTTP (SHTTP)

It’s an alternative to HTTPS, it has the same working as HTTPS and is designed to secure web pages and their messages. There are differences between SHTTP and SSL protocol such as SSl is a connection oriented protocol and it works it transport level by providing a secure tunnel for transmission whereas SHTTP works on application level and each message is encrypted separately, but secure tunnel is created. SSL can be used for secure TCP/IP protocols like FTP but SHTTP works only on HTTP. Its use is fairly limited as compared to HTTPS.

C. VPN

Virtual Private Network (VPN), is a way to transport traffic on an unsecured network. It uses a combination of encrypting, authentication and tunnelling. There are many different types of methods of VPN but of these 5 are easily recognized.The most known and used protocols are as follows:

- Point-to-Point Tunnelling Protocol (PPTP)
- Layer 2 Tunnelling Protocol (L2TP)
- Internet Protocol Security (IPsec)
- SOCKS

VPN allows a user to secure it privacy as it's very hard to correctly detect the location of the user as the network data may be routed through multiple locations spread across the world before finally reaching its destination. It also can be used to bypass firewall and blocks of websites.

VI. RECENT ADVANCES IN NETWORK SECURITY

Before the internet became popular and fairly common, intrusion detection meant detection of an unauthorized human user/person on a machine, but this definition radically changed with the advent of CodeRed worm and its variants in the year 2001. These were 1st generation worm they had high spread rats and made human countermeasures impossible. A real-time and an automated system was to be developed to detect and prevent further spread of these worms. These worms generated high traffic especially on Port 80, therefore a volumetric approach was proposed to detect them. It worked for the generation where network infrastructure was not widely deployed. However they became useless in the recent years because of the behaviour of worm is now specific in many cases and also users begin to generate high volume on their own using file sharing sites and network gaming [5]. Network security is being improved in two fields namely hardware and security in the following ways:

A. Hardware Development

This field is not developing very rapidly as its software counterpart but nonetheless some amazing developments are being made such as using Biometric systems and smartcards which can drastically reduce the number of unauthorised access. Biometric has very important use in the field of the network security, some obvious uses such a built in biometric scanner attached to a workstation can be used as an authentication mechanism which can be used as a login to the system, since two persons cannot have the same biometrics as the both persons, it is a full proof mechanism of login [1].People tend to forget their passwords and so they keep it near their workstation written on a slip or something else or even lock themselves out of their system by incorrectly entering it too many times. All this can be easily avoided by biometric systems as they provide users undeniable proof of identity. Smartcards are provided by companies to its workers, they only work when they are inserted in the computer and a pin issued the network administrator is entered, since the pin issued is only four characters and numeric, users don't forget it and don't write it down.

B. Software Developments

The software field is very wide when it comes to network security. It includes firewall, antivirus, VPN, intrusion detection, and many much more. The improvement of network security is basically still the same. When new virus are found virus definitions are updated, it's the same for firewalls instead their rules are updated. As more and more security transits to hardware such as biometric. The software must be able to use the information correctly and appropriately. Currently research is being focused on neural networks for facial recognition software. Most current algorithms require substantial processing power. This power cannot be available in small devices like sensors. Therefore, one must develop light weight algorithms to counter this problem [1].

Antivirus works on a very basic principle, they scan a file and then matches its digital signature against the known malwares. If the signature is match in the database it reports it, delete it or even disinfect it depending on the user's setting. This system however easy has a huge drawback, whenever a new malware is found, it takes time before the antivirus database can be updated and during this period the malware can already take complete control of the computer, disable the antivirus or even hides itself from the antivirus. To prevent this antivirus companies introduced a new system called cloud scanning this way not only will the digital signature be scanned across the database but also across millions of computers and servers across the world. This all happens and real time and results are very fast. This greatly reduces the chance of infection from a new malware.

VII. CONCLUSION

As internet has become a huge part of our daily life, the need of network security has also increased exponentially from the last decade. As more and more users connect to the internet it attracts a lot of criminals. Today, everything is connected to internet from simple shopping to defence secrets as a result there is huge need of network security. Billions of dollars of transactions happens every hour over the internet, this need to be protected at all costs.Even a small unnoticed vulnerability in a network can have disastrous affect, if companies records are leaked, it can put the users data such as their banking details and credit card information at risk, numerous software's such as intrusion detection have been which prevents these attacks, but most of the time it's because of a human error that these attacks occur.Most of the attacks can be easily prevented, by following many simply methods as outlined in this paper. As new and more sophisticated attacks occur, researchers across the world find new methods to prevent them. Numerous advancements are being made in the field of network security both in the field of hardware and software, it's a continuous cat and mouse game between network security analyst and crackers and as the demand of internet shows no signs of decreasing it's only going to get a lot harder.

VIII. REFERENCES

[1] B. Daya ,“Network Security: History, Importance, and Future ,”University of Florida Department of Electrical and Computer Engineering , 2013. http://web.mit.edu/~bdaya/www/Network%20Security.pdf

[2] Li CHEN,Web Security : Theory And Applications,School of Software,Sun Yat-sen University, China.

[3] J. E. Canavan, Fundamentals of Network Security, Artech House Telecommunications Library, 2000.

[4] A. R. F. Hamedani, “Network Security Issues, Tools for Testing,” School of Information Science, Halmstad University, 2010.

[5] S. A. Khayam, Recent Advances in Intrusion Detection, Proceedings of the 26th Annual Computer Security Applications Conference, Saint-Malo, France, pp. 224-243, 42, 2009

[6] M. M. B. W. Pikoulas J, “Software Agents and Computer Network Security,” Napier University, Scotland, UK.

[7] R. E. Mahan, “Introduction to Computer & Network Security,” Washington State University, 2000.

[8] Q. Gu, Peng Liu, “Denial of Service Attacks,” Texas State University, San Marcos.