CCNA Security: Common Network Attacks

www.certificationkits.com/cisco-certification/ccna-security-certification-topics/ccna-security-describe-security-threats/ccna-security-common-network-attacks/

The threats to the network can broadly be classified into two categories:

- **Internal Threats**

Internal Threats as the name suggests originate from within the network. These security threats originate from within the internal users. The attacks by internal users are severe in nature as the vulnerabilities of the network are known to these users. According to the results of a recent study carried out, 80% of all network misuse originates from internal users.

- **External Threats**

Once again, as the name suggests, these are the threats to the security of the network originating from the outside users. The probability of attacks falling under this category is much less than the probability of an internal attack. This is so for the simple reason that outside users do not have easy access to the network.

An attack on a network can take place in several stages. During the initial stage the attacker may be armed with only limited information about the target. The main types of network attacks are categorized based on their nature and behavior. The attacks and their nature are briefly discussed below:

- **Reconnaissance:** Knowledge is power goes the old and equally wise saying. This axiom is applicable to the arena of network attacks as well. The reconnaissance attack is one where the main purpose of the attacker is to find out information about the vulnerable points of the network which is being targeted.
- **Access Attacks:** There are several known loopholes and vulnerabilities in various types of services such as say FTP, authentication and web services. When an attacker tries to exploit these commonly known weak points for malicious purposes such as gaining unauthorized access to restricted and confidential information, it is called as an access attack. It could target important databases and web accounts of users for finding out information which is secret and valuable.
- **DoS and Distributed DoS:** Attacks that do not need to collect in depth information of the target network to be successful are typically denial of service (DoS) and distributed DoS attacks. DoS attacks, the most well known of the attacks are tough to handle as they cannot be completely eliminated. These attacks employ varied techniques like flooding network resources, reducing the functionality of the systems, rendering systems unavailable. The technique followed in denial of service attacks is to flood the target with innumerable requests via the web or through the network. When a server receives requests in such a large number, it slows down. Once it slows down it becomes unavailable to legitimate users and access.
- Distributed DoS attacks can be said to be the advanced form of DoS attacks. The networks attacked by this sort of attack are overwhelmed with packets from multiple sources. Most of these sources are spoofed IP addresses. These packets overwhelm the connectivity of the network. This is in contrast to the traditional denial of service attacks wherein only a single system was used for the attack, whereas in the distributed DoS, there could be innumerable systems which are attacking the given target simultaneously.

Reconnaissance Attacks and Mitigation

The word Mitigation as such means alleviation or lessening. The term Reconnaissance Attack as discussed above refers to the act of accumulating information about a target network. This is done by using readily available information and applications. It is possible to keep a check on such attacks, but first it sis important to understand the types of the attacks. These attacks can be in the form of :

- Packet Sniffers
- Port Scans
- Ping Sweeps
- Internet Information Queries

Packet Sniffers

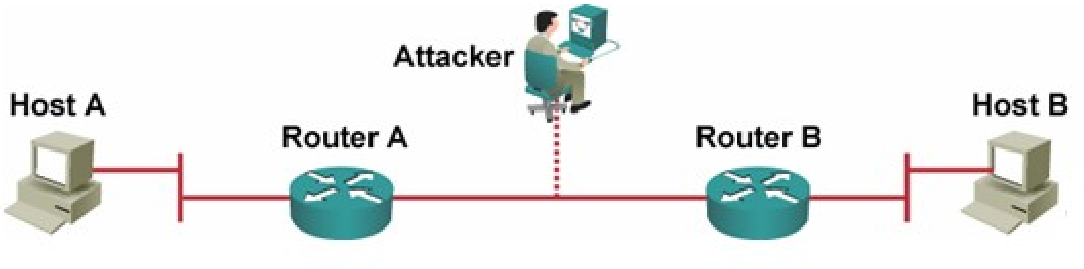

Figure 1: Packet Sniffer Application

A packet sniffer refers to a software that captures all network packets. It uses a network adapter card to capture all network packets. These exploit information which is passed in the plain text format. Unencrypted plain information is available in protocols such as Telnet, HTTP and so on. Packet Sniffers must be located at the same collision domain otherwise they will not work. These can be used legitimately, or can be specially designed for attack.

Packet Sniffer Mitigation

The mitigation techniques and tools include:

- **Authentication:** It is advised to use strong authentication as a defense against packet sniffers. It is a method of verifying users that cannot be allowed to gain access easily. OTP (One Time Password) is considered to be a strong tool as it works as a two factor authentication. Two factor authentication is combining something that you have with something that you know. The best example in this category are the ATM's. The card is something that a user has and the PIN is something that the user knows.

- **Cryptography:** In this method the packet sniffers are rendered irrelevant. It works as one of the best ways for countering packet sniffers. It is considered a better tool than detecting or preventing packet sniffers. A cryptographically secure channel will detect only packet sniffers in cipher text format and not the original format. The base for Cisco deployment of network level cryptography is based on IPsec. It is considered to be the standard network devices to communicate privately using IP. SSH (Secure Shell) and SSL (Secure Sockets Layer) are other cryptographic protocols.

- **Antisniffer Tools:** Hardware as well as software can be used to detect sniffers on a network. With the use of such softwares and hardware the complete threat is not done away with, but serve their purpose well when combined with the overall mitigation system. These tools detect changes in the response time of hosts, which forms the basis of determining whether more traffic is being processed by the hosts than their traffic loads indicate.

- **Switched Infrastructure:** This is one of the most common of technologies used for countering the use of packet sniffers in the network environment. This limits the ports to which attackers can gain access. If an entire organization deploys switched Ethernet, hackers will be able to gain access only to the traffic that flows on the specific port to which they have been able to connect. This tool does not eliminate the threat of packet sniffers entirely, but it reduces their effectiveness.

Port Scans and Ping Sweeps

The target of Port scans and ping sweeps are all services on the network; all hosts and devices connected to the network; the operating systems and all other vulnerable areas of the network.

Port Scan and Ping Sweep Mitigation

For objective of mitigating port scans and ping sweeps cannot be achieved without compromising on the abilities of the network. By using the Intrusion Prevention Systems (IPS) at network and hosts level such attacks can be mitigated.

Turning off ICMP echo and echo reply on edge routers can be used to stop Ping sweeps. This also results in loss on network diagnostic data. Port scans be run easily without full ping sweeps. The only deterrent factor is that it takes longer as even those IP addresses are scanned which may not be live.

Network based IPS and host based IPS are enabled to inform about a reconnaissance attack taking place or about to take place. This helps to be better prepared to deal with the attack. The Internet Service Provider can be informed so that the incoming traffic can be compared to the intrusion detection system (IDS) or the IPS signatures in their database. These signatures identify particular traffic patterns.

DNS

A DNS Query can be used to decipher a substantial amount of information about an organization. DNS's are designed in such a manner that they resolve IP addresses to DNS names. DNS information is easily available and simple to find out. 'DNS lookup' and 'whois query' are two such queries which can derive a lot of information. The DNS lookup query is able to provide information about the specific IP address, specific domain name and a whois query provides information about the name, identification, address, assigned public IP address space, public name, server address, technical contact name, telephone number etc.

Access Attacks

The nature of access attacks has already been discussed ahead. To put it simply, access attacks are attempts to gain unwarranted entry into the network.

Access attacks are used by intruders for

- For retrieving confidential data
- For gaining access
- For enhancing their access privileges

The following are included in access attacks:

- Password Attacks: In this the attacker attempts to gain access by guessing the passwords of the system. A dictionary attack is a common example of the same.
- Trust Exploitation: In this kind of attack, an attacker uses privileges which have been granted to a system in an unauthorized manner. This is done by compromising the target.
- Port Redirection: In these kinds of attacks, a system that has already been compromised is used to attack other targets. A tool which works as an intrusion tool is installed on the compromised system for session

redirection.

- Man-in-the-Middle Attacks: in these attacks the attackers place themselves in the middle of the communication taking place between two legitimate entities. The attacker reads and even modifies the data that is exchanged between two parties.
- Buffer Overflow: in this kind of attack a program writes the data beyond the allocated end of a buffer. The overflow is the result of a bug accompanied by an improper use of C or C++ languages. These languages are not considered to be memory safe. One of the consequence is that even valid data gets overwritten.

Mitigation of Password Attacks

The following techniques can be used to keep Passwords attacks to the minimum:

- Disallowing use of a single password over multiple systems;
- Disabling accounts after a certain number of unsuccessful login attempts have been availaed;.
- Discouraging the use of plaintext passwords.
- Encouraging the use “strong” passwords. (Use “mY8!Rthd8y” rather than “mybirthday”)

Mitigation of Trust Exploitation Attacks

To mitigate trust exploitation attacks, systems placed in the inside of a firewall should not show an absolute faith on the systems outside the firewall. Trust of the absolute level should be limited to specific protocols only. As much as possible validation should be done by more than just the IP address.

Mitigation of Port Redirection Attacks

Port Redirection attacks are kind of trust exploitation attacks. It uses a compromised host to pass the traffic that should not be passed rather dropped through a firewall.

Mitigation of Man-in-the-Middle Attacks

These attacks require that the hacker have access to network packets that come across a network. Such attacks are carried out by using:

- Network Packet Sniffers
- Routing and Transport protocols

The best method to mitigate these attacks is by the use of cryptographic encryption.

MitigationDoS and Distributed DoS Attack

As discussed above attacks that do not need to collect in depth information of the target network to be successful are typically denial of service (DoS) and distributed DoS attacks. These attacks can be mitigated by the use of :

- Anti-Spoof Features: Configuring anti spoof features on the routers and firewalls can mitigate the risk of attacks. Proper filtering is done by using techniques like access lists, unicast reverse path forwarding.
- Anti-DoS Features: Once again the anti dos features also require proper configuration. These can help in a long way to reduce the effects of attacks. These features involve fixing a limit to the number of half open TCP connections that a system will allow at a given point of time. It is also known as the SYN-flooding prevention. The same can be configured in different ways such as:
  - by limiting the overall number of half-open TCP sessions that can go through the router

    - by limiting the number of half-open sessions per minute
    - by limiting the number of half-open sessions destined to a specific server.

- Traffic Rate Limiting: Traffic rate can be limited by an organization with its ISP. This works by filtering the limits the amount of nonessential traffic that crosses network segments at a certain rate.