Types of Network Threats

Our internet has given us more ways to connect than we ever thought possible. Despite the best efforts of network security specialists, both hackers and criminals have found methods to compromise these networks. There are various ways that networks can be exposed to security threats, sometimes these threats include access to personal and account information. It is vital that we protect our computers from these threats, but first we need to understand about the different types of threats that are out there.

Reconnaissance

Reconnaissance Phase (Electronic) is the first phase in attacking a network. This phase consist of gathering information on a network to include what types of hardware are running and the services which said hardware are using. With this technique an attacker can discover and use known vulnerabilities in both the network hardware and software. This phase is similar to a thief surveying houses looking for one that is unlocked, which presents the easiest target.

Electrical reconnaissance typical involves the scanning of the target network using a ping sweeper. This tool pings a range of IP addresses and waits for a response. These responses or lack of responses let the attacker know what hosts are currently live on the network. Once the attacker determines the host IP address he/she would then begin probing to gather more information about was OS is being run, is it patched/updated, and what application services are running on the host.

The three main activities accomplished during the scan are host detection, port enumeration, and vulnerability assessment. Host detection looks for active host on the network. Either network address (IP) or hardware addresses (BSSID/MAC). Port enumeration checks what ports are using what services. Finally vulnerability assessment identifies potential vulnerabilities that could be exploited based off of the services being run.

A classification of probes.

Probes						
Activity	Host detection		Port enumeration		Vulnerability assessment	
Layer	Data link	IP	TCP	UDP	OS	Application
Desired Information	Hardware address	Network address	Service enumeration Port address		Identification Version identification Patch level information	
	Host liveness					

There are two types of probing/scanning:

Active probing: Involves some type of interaction with the target host or network, from the attacking machine. This type of probing will give an accurate description of all the open ports and the available services at the time of the probe. Active probing will not detect those services that are hidden behind a firewall. How active probing works is the attacking computer sends packets to the host computer and monitors the response. Based off of the response the attacking computer is able to figure out what

services are running on what ports. This type of probing is considered very intrusive and can be detected.

A classification of active probes.

Active probes						
Activity	Host detection		Port enumeration		Vulnerability assessment	
Layer	Data link	IP	TCP	UDP	OS	Application
Techniques	Echo	ICMP echo ICMP non-echo RESET scan Invalid Protocol Response	SYN scan (Full open) SYN scan (Half open) FIN scan XMAS scan NULL scan SYN/ACK scan ACK scan	UDP scan	TCP/IP stack fingerprinting Obtaining DNS host information (HINFO) Patch level Assessment	Exploitation Banner Grabbing Password Auditing

Passive probing: Involves the attacker restraining themselves to only sniffing and logging traffic which has originated from and is headed toward the target network. With this type of probing an individual can obtain relevant information such as the services being actively used, including those behind the firewall, as well as track the targets behavior. Passive probing works with specialized software and hardware that has the capabilities to sniff packets out of the air. From there the software does a deep packet inspection which will inspect the content of the packet past the IP and secondary transport layer header. This will reveal information about the services being run including version information. Passive probing does not detect idle processes but is able to detect processes that are hiding behind the firewall. Also passive probing is very difficult to detect as it does not directly interact with the target network.

Access Attack

An **access attack** happens while hackers are trying to gain unauthorized access to a component, or increasing their privileges on a network component. Access attacks exploit known weakness in authentication services, FTP services, and web services to gain entry to web accounts, confidential databases, and other sensitive information. A Network attacker can use packet sniffer tool to obtain user accounts and passwords information. There are two types of access attacks: Password Attack, Man-in-the middle attack.

Password attack: Normally, user login and logout from the system using password to shared network resources in a router or server. An attacker can repeatedly attempt to login to the resource or to gain unauthorized access to an organization's network.

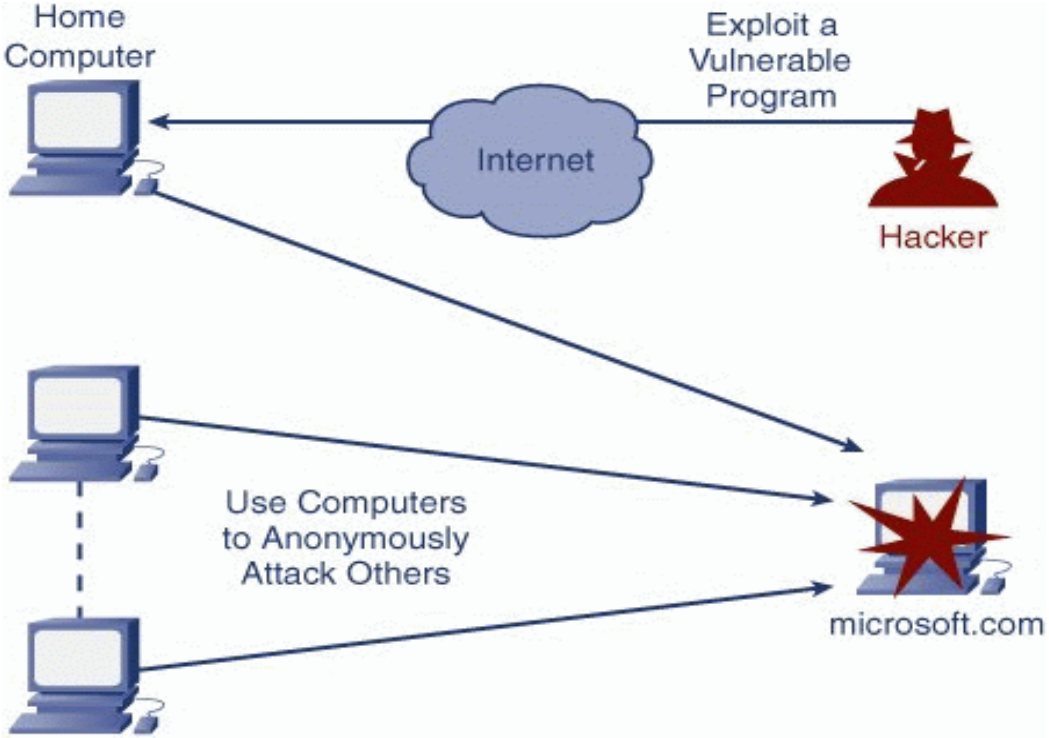
Man-in-the-Middle Attack: it occurs when someone between user and the person who is communicating with the user is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data.

Hacker who has gained access to a computer can install any devices to adjust the security protocol, including operating system alterations, software worms, covert listening devices and keys. The hacker then can also easily download large amount of data onto backup media, for instance CD-R/DVD-R, portable devices such as key-drives, digital equipment. Another common method is to boot an operating system contained on a bootable media and read the data from the hard-drive(s) this way. The only way to defeat this is to encrypt the storage media and store the key separate from the system.

Denial of Service

DOS (Denial of Service) attack is an effort to make a machine or network resource unreachable to its intended users. A denial of service attack starts when an attacker targets a computer and its network connection or multiple computers and network of the sites you are trying to use. This results in preventing one from accessing email, websites, online accounts and other servers that rely on the computer. The most widely known of DoS attack is when an attacker "floods" a network with information. When one tries to access a URL to a certain website, they send a request to the sites server to view the page. The server only processes a limited number of requests at one time; therefore the attacker overloads the server with requests, allowing the attacker to process the request. This is where the "denial of service" name comes from because the user cannot access the site.

Another method used by the attacker uses spam email messages to launch an attack on your email account. An attacker can take control of your computer by taking advantage of security vulnerabilities. The attacker then forces the computer to send data to a website or send spam to email addresses. The attack is known as "distributed" because the attacker uses multiple computers to launch the attack.



If a user correctly identifies a DoS or DDoS attack, it is almost impossible and very unlikely that they will be able to determine the target or source of the attacker. If you notice that you cannot access files or

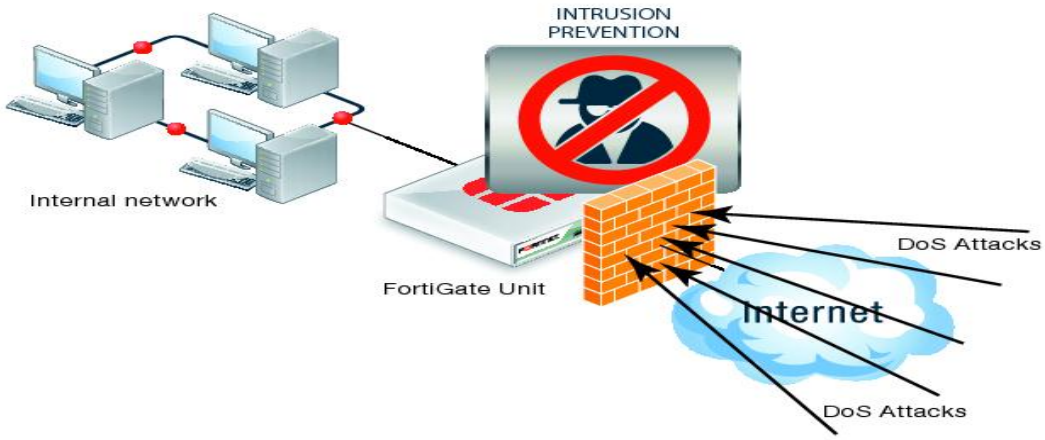
external website via your work computer, you should contact a network administrator. Likewise, if you are having similar issues on your home computer, you should contact your internet service provider. They should be able to determine the suitable course of action. Do not automatically assume that a disruption is a result of a denial of service attack, there may be technical network problems or maintenance in progress. If you suspect a denial of service attack look out for the following signs:

- Slow network performance
- Unavailability of a particular website
- Inability to access any website
- Increase in amount of spam emails

Protection

Although there are no effective ways to avoid being a victim of an attack, there are a few steps to reduce your chances:

- Install and use anti-virus software
- Install and configure a firewall
- Distribute your email address wisely
- Apply email filters to avoid unwanted traffic



Data Modification Attack

Another type of network attack is the **data modification attack**. The purpose of this attack is to remove, insert or modify files in a system. This type of attack normally operates in stealth-mode; victims do not notice any abnormalities in the operation of their software. The motive behind this type of attack can be to cause damage by modifying essential system files, to modify financial data for the benefit of the criminal, to modify an existing website, to interrupt network services, or any other similar motive. There are three types of data modification attacks: worms, viruses, and Trojan horses. These types of programs are commonly known as malicious software or malware.

A **worm** is standalone software, does not require an existing program to attach to, that replicates itself on the host computers memory and then locates new targets through the network. A worm attack follows a simple structure. One, create a loophole through a known exploit which can then be accessed by the attacker. Two using its parasitic ability, replicate itself then spread to other host machines.

Finally once the host computer is infected the attacker gains access through the loophole and escalates their privileges to administrator level to obtain complete access to the machine.

A **virus** is a piece of malware that attaches itself to another program. For a virus to be installed it needs to be run on the host computer. Viruses are the most destructive form of malware because they are used most for hard drive corruption and file deletion. The biggest difference between a worm and a virus is that a virus requires human interaction to be installed where a worm is its own entity that has the capabilities to act on its own.

Trojan horse is malicious software that disguises itself as a legitimate program but has a hidden agenda. Consider a game that one has downloaded on the internet. While he or she is playing the game, looking legitimate, the Trojan horse is busy at work in the background creating loopholes in the host computer and finding ways to spread, either through contact list or email. A Trojan horse creates a backdoor into a computer that allows an attacker to access the data.
Protection

Protection

The easiest way to protect oneself from these types of network threats is by utilizing an antivirus software. It is important to have a good piece of antivirus software installed and running on your computer. It is also important to keep that software updated because new viruses, worms, and Trojans are being created every day. Antivirus software alone will not keep your computer malware free. It is up to the end user to be aware of potential threats and avoid downloading “free” software from unknown websites.

References

1. Barlett, G. E. (2010, August). Network Reconnaissance Using Blind Techniques.
2. Shaikh, S. A., Chivers, H., & Nobles, P. (2008, November). Network Reconnaissance. Networking Security, 2008(11), 12-16.
3. OoiBC, ChuYL. Managing trust in peer to peer systems using reputation-based techniques[C] //The 4th International Conference on Web Age Information Management, Chengdu: WAIM, 2003: 159
4. “Security Tip (ST04-015)." US-CERT Tip ST04-015. N.p., n.d. Web. 01 Dec. 2012. <http://www.us-cert.gov/cas/tips/ST04-015.html>.
5. "Guard Against DoS and DDoS Attacks." Denial of Service (DoS) Protection & Network Intrusion Prevention. N.p., n.d. Web. 01 Dec. 2012. <http://www.radware.com/Solutions/Enterprise/Security/DoSProtection.aspx>.
6. http://en.wikipedia.org/wiki/Malware
7. http://en.wikipedia.org/wiki/Computer_worm
8. http://en.wikipedia.org/wiki/Computer_trojan
9. http://en.wikipedia.org/w/index.php?title=Website_defacement&oldid=524854194