SNS COLLEGE OF TECHNOLOGY

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A++' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

19ECT301-COMMUNICATION NETWORKS III YEAR/ V SEMESTER

UNIT 4- NETWORK & DATA SECURITY

TOPIC –Threats in Network

Introduction

- With an increasing amount of people getting connected to networks, the security threats that cause massive harm are increasing also.
- Network security is a major part of a network that needs to be maintained because information is being passed between computers etc and is very vulnerable to attack.
- Over the past five years people that manage network security have seen a massive increase of hackers and criminals creating malicious threats that have been pumped into networks across the world.(Source [1]: ITSecurity, 2007)

Security Threats

- According to ITSecurity.com the following are ten of the biggest network threats:
- "1.Viruses and Worms",
- "2.Trojan Horses",
- "3.SPAM",
- "4.Phishing",
- "5.Packet Sniffers",
- "6. Maliciously Coded Websites",
- "7. Password Attacks",
- "8.Hardware Loss and Residual Data Fragments",
- "9. Shared Computers",
- "10.Zombie Computers and Botnets" (ITSecurity [2], 2007)

Viruses and Worms

- A Virus is a “program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes (Webopedia [3], 2007)”.
- Viruses can cause a huge amount of damage to computers.
- An example of a virus would be if you opened an email and a malicious piece of code was downloaded onto your computer causing your computer to freeze.

Viruses and Worms (Cont.)

- In relation to a network, if a virus is downloaded then all the computers in the network would be affected because the virus would make copies of itself and spread itself across networks (Source [4]: Trendmicro.com, 2008).
- A worm is similar to a virus but a worm can run itself whereas a virus needs a host program to run. (Source [5]: TechFAQ, 2008)
- Solution: Install a security suite, such as Kaspersky Total Protection, that protects the computer against threats such as viruses and worms.

Trojan Horses

- A Trojan Horse is “a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. (SearchSecurity.com [6], 2004)”
- In a network if a Trojan Horse is installed on a computer and tampers with the file allocation table it could cause a massive amount of damage to all computers of that network.
- Solution: Security suites, such as Norton Internet Security, will prevent you from downloading Trojan Horses (Source: Symantec [7], 2007).

SPAM

- SPAM is "flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. (Spam.abuse.net [7], 2009)".
- I believe that SPAM wouldn't be the biggest risk to a network because even though it may get annoying and plentiful it still doesn't destroy any physical elements of the network.
- Solution: SPAM filters are an effective way to stop SPAM, these filters come with most of the e-mail providers online. Also you can buy a variety of SPAM filters that work effectively.

Phishing

- Phishing is "an e-mail fraud method in which the perpetrator sends out legitimate-looking emails in an attempt to gather personal and financial information from recipients. (SearchSecurity.com [9], 2003)"
- In my opinion phishing is one of the worst security threats over a network because a lot of people that use computers linked up to a network are amateurs and would be very vulnerable to giving out information that could cause situations such as theft of money or identity theft.
- Solution: Similar to SPAM use Phishing filters to filter out this unwanted mail and to prevent threat.

Packet Sniffers

- "A packet sniffer is a device or program that allows eavesdropping on traffic travelling between networked computers. The packet sniffer will capture data that is addressed to other machines, saving it for later analysis. (Wisegeek.com [10], 2009)"
- In a network a packet sniffer can filter out personal information and this can lead to areas such as identity theft so this is a major security threat to a network.
- Solution: "When strong encryption is used, all packets are unreadable to any but the destination address, making packet sniffers useless. (Wisegeek.com [11], 2009)" So one solution is to obtain strong encryption.

Maliciously Coded Websites

- Some websites across the net contain code that is malicious.
- Malicious code is "Programming code that is capable of causing harm to availability, integrity of code or data, or confidentiality in a computer system... (Answers.com [12], 2009)"
- AVG report that "300,000 infected sites appear per day (PC Advisor [13], 2009)"
- Solution: Using a security suite, such as AVG, can detect infected sites and try to prevent the user from entering the site.

Password Attacks

- Password attacks are attacks by hackers that are able to determine passwords or find passwords to different protected electronic areas.
- Many systems on a network are password protected and hence it would be easy for a hacker to hack into the systems and steal data.
- This may be the easiest way to obtain private information because you are able to get software online that obtains the password for you.
- Solution: At present there is no software that prevents password attacks.

Hardware Loss and Residual Data Fragments

- Hardware loss and residual data fragments are a growing worry for companies, governments etc.
- An example this is if a number of laptops get stolen from a bank that have client details on them, this would enable the thief's to get personal information from clients and maybe steal the clients identities.
- This is a growing concern and as of present the only solution is to keep data and hardware under strict surveillance.

Shared Computers

- Shared computers are always a threat.
- Shared computers involve sharing a computer with one or more people.
- The following are a series of tips to follow when sharing computers: “Do not check the “Remember my ID on this computer” box … Never leave a computer unattended while signed-in … Always sign out completely … Clear the browsers cache … Keep an eye out for “shoulder surfers” … Avoid confidential transactions … Be wary of spyware … Never save passwords … Change your password often (security.yahoo.com [14], 2009)”

Zombie Computers and Botnets

- "A zombie computer, or "drone" is a computer that has been secretly compromised by hacking tools which allow a third party to control the computer and its resources remotely. (WiseGeek.com [15], 2009)"
- A hacker could hack into a computer and control the computer and obtain data.
- Solution: Antivirus software can help prevent zombie computers.

Zombie Computers and Botnets (Cont.)

- A botnet "is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the internet. (SearchSecurity.com [16], 2004)".
- This is a major security threat on a network because the network, unknown to anyone, could be acting as a hub that forwards malicious files etc to other computers.
- Solution: Network Intrusion Prevention (NIP) systems can help prevent botnets (Source: SearchSecurity.com [17], 2009).

Conclusion

- Network Security is a very broad field and being a Network Security manager is not an easy job.
- There are still threats such as password attacks that have no prevention.
- Many of the threats set out to get personal information.


Thank You!