**Computer and Network Security**

Computer and Network security

Problem statement

Unauthorized Access

“As the threat of unauthorized access grows companies and people continue to look for security to upgrade.” (Howard, 2009)``Unauthorized access'' is a very high-level term that can refer to a number of different sorts of attacks. The goal of these attacks is to access some resource that your machine should not provide the attacker. For example, a host might be a web server, and should provide anyone with requested web pages. However, that host should not provide command shell access without being sure that the person making such a request is someone who should get it, such as a local administrator.

What network security is

The history of network security

“Sense the 1980’s networks have become more complex, so the need for security has become more complex.” (Mowers, 2006) The need for network security is a relatively new requirement. Prior to the 1980s most computers were not networked. It was not due to lack of desire to network them; it was more a result of the lack of technology. People or organizations could be interconnected over the shared network. It was no longer necessary to connect systems in a point-to-point configuration. Vulnerabilities were introduced with the deployment of this distributed environment utilizing shared, packet switched networks employing protocols such as TCP/IP and the concept of trusted systems. Systems on the network "trusted" each other. This situation was frequently made worse by connecting relatively secure LANs to an unsecured WAN. This early use of networking opened up some major security risks. The holes that allowed unauthorized access made it so, computers and networks needed new protocols to protect the systems.

Why Network security has become so important

Network security is a high priority form of security because many hackers try to infect as many computers as possible so they can get an arm of zombie machines for attacks. With these zombie machines hackers can gain entry to many networks at one time and start stealing dat. Also for corporations, it’s to stop industry sabotage and/or espionage. Network Security is very important; the Internet has grown and developed to reach the figure of several million units of computers that are connected in various parts of the world. Day to day information that is contained in the Internet network is more complete, accurate and important. Companies are now putting more stock on network security, because keeping data safe from unauthorized access is becoming harder to control. Hackers search for holes in network security, and making sure there are no holes is why network security has become so important, not leaking classified data to the wrong people.

Understanding unauthorized access

What unauthorized access looks like

Unauthorized Access is an act of illegally gaining access into any computer, network etc, or promoting such activity, which is banned under the “Unauthorized Access P0rohibition Law”. Unauthorized access consists Viewing private accounts, messages, files or resources when one has not been given permission from the owner to do so. Viewing confidential information without permission or qualifications is an action that people can see if their looking for it. Seeing the files opening without your permission, a password being used that you haven’t used, also seeing the history of the computer shows what has been accessed. “Depending on how good the hacker is, the signs of unauthorized access can be easy or hard. “Although a hacker always leaves a trail, so if you know what you’re looking for.” (Upstien, 2008)

Different techniques involved

Network cracking doesn't always involve sophisticated tools. It can be as simple as finding a sticky note with the password to the network written on it stuck right to the monitor or hidden under a keyboard. Another crude technique is known as "dumpster diving," which basically involves an attacker going through your garbage to find discarded documentation that may contain passwords.

Of course attacks can involve far greater levels of sophistication. Here are some of the more common techniques used in network cracking:

A simple dictionary attack is by far the fastest way to break into a network or machine. A dictionary file (a text file full of dictionary words) is loaded into a cracking application, which is run against user accounts located by the application. Because the majority of passwords are often simplistic, running a dictionary attack is often sufficient to the job.

Another well-known form of attack is the hybrid attack. A hybrid attack will add numbers or symbols to the filename to successfully crack a password. A brute force attack is the most comprehensive form of attack, though it may often take a long time to work depending on the complexity of the password. Some brute force attacks can take a week depending on the complexity of the password. Also there is fishing, data mining, and lifting, all of these techniques involve hiding viruses on unsecure web-sites or e-mails.

What to do problems it can cause

“Once a hacker gains entry they can anything they want, with the use of viruses, worms, and Trojans.” (Spivey, 2010) Computer viruses are small pieces of software that spread from computer to computer and network to network, like a human "virus" or infection. They can corrupt data, delete files; start e-mail programs to spread themselves to other contacts on the network or even wipe out an entire hard disk. Unauthorized access can bring these things into the light on your network. Symptoms of computer viruses:

- You get strange sounds or music from your speakers unexpectedly, with volume controls often disabled.

- Programs disappear although you did not intentionally remove any. Conversely, programs appear although you did not install them.

- The computer crashes every few minutes.

These symptoms often can crash a network unexpectedly and can cause data dumps, which unload mass amounts of data to the person with the unauthorized access.

The different ways of unauthorized access

Executing Commands Illicitly

It’s perceptibly adverse for a not known and untrusted person to be capable to execute commands on your server machines. The sternness of the problem is of two types of problem: first one is user access, and the next one is administrator access. A general user can perform so many things on the system such as read files edit them, and these things that a user cannot perform. Subsequently that an attacker can might perform configuration alterations to the host like changing the port number of the host system an d make the system shutdown so that the system can shut down every time as it is started. To perform this type of actions first the intruder has to get access of the administrator privileges.

Confidentiality Breaches

There suppose we assume that there is data that which is very confidential if that data is fell in the hands of intruder there may be a chance of modifying the data or he can change the entire data or he can replace the old data with new data In such type of situations the general user accounts on the system is enough to make damage against the company. As several intruders of these types of break-ins are merely thrill-seekers and they do not have interest in nothing to see a shell prompt for your computer on their screen, these are highly malicious.

Destructive Behavior

“Hackers use what we call Destructive Behavior, which involves two types of data hunting.” (Grace, 2011) Among the destructive sorts of break-ins and attacks, one of the two major categories is.

-Data Destruction

Some of the intruders are those who want to delete the things which there aim is to data destruction. In this situation, the bang on the computing competence and accordingly the businesses plus or minuses cannot be less than if a fire or any other natural calamity takes place so that other disaster caused your computing equipment to be completely destroyed.

How to prevent this

The primary thing that we think about the file is its security and we make the file to rid out of the problems that are discussed as above for that we have to perform file security. Problems given above like execution of commands illicitly, unauthorized access, confidentiality breaches and destructive behavior. There are many different techniques that people can employ to avoid these problems firewalls, antiviruses, and pop up blockers. Although the best prevention can be employees having the knowledge and understanding of network security, so they don’t break protocol. “Teaching employees security techniques has been a way to prevent attacks on networks for some time.” (House, 2009)

References

Howard, J. (2009) Unauthorized Access. “Network Security”

Mowers, K. (2006) History of Networks. “Computers”

Upstien, M. (2008) Unwelcomed changes in the Network “Information security”

Spivey, L. (2010) Techniques used in computer hacking “Computer Hacking”

Grace, H. (2011) Destructive Behavior “Tech Guide”