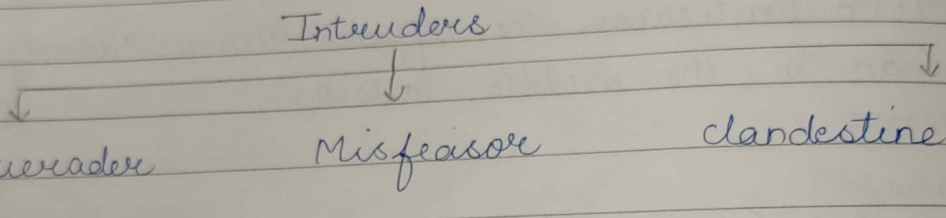
Page

SYSTEM SECURITY

Intruders

An intruders is a person who attempts to gain unauthorized access to a system, to damage that system, or to disturb data on that system

There are three classes of intruders



Masquerader: An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account

Misfeasor: A ~~legit~~ legitimate user who accesses data, programs, or resources for which such access is not authorized or who is authorized for such access but misuses his or her privileges.

clandestine User: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or suppress audit collection.

The masquerader is likely to be an outsider; the misfeasor generally is an insider; and the

Scanned with CamScanner

Date __/__/____
Page _____

clandestine user can be either an outsider or an insider.

Intruder attacks range from the benign to the serious. At the benign end of the scale, there are many people who simply wish to explore internets and see what is out there. At the serious end are individuals who are attempting to read privileged data, perform unauthorized modifications to data, or disrupt the system

Intrusion Techniques

The objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system. Generally, this requires the intruder to acquire information that should have been protected. In some cases, this information is in the form of a user password. With knowledge of some other user's password, an intruder can log into a system and exercise all the privileges accorded to the legitimate user.

Typically, a system must maintain a file that associates a password with each authorized user. If such a file is stored with no protection then it is an easy matter to gain access to it and learn passwords. The password file can be protected in one of two ways:

Scanned with CamScanner

- One-way function: The system stores only the value of a function based on the user's password. When the user presents a password, the system transforms that password and compares it with the stored value. In practice, the system usually performs a one-way transformation (not reversible) in which the password is used to generate a key for the one-way function and in which a fixed length output is produced.

- Access control: Access to the password file is limited to one or a very few accounts.

If one or both of these countermeasures are in place, some effort is needed for a potential intruders to learn passwords.

Techniques for guessing passwords

1. Try default passwords (used with standard accounts that is shipped with systems).
2. Try all short words, 1 to 3 characters long.
3. Try all the words in an electronic dictionary.
4. Collect information about the user's hobbies, family names, birthday, etc.

Scanned with CamScanner

Date / /
Page

5. Try user's phone number, social security number, street address, etc.

6. Try all license plate numbers (AP 12 AA 4453).

7. Use a Trojan horse.

8. Tap the line between a remote user and the host system.

Intrusion Detection System

Intrusion detection is the act of detecting unwanted traffic on a network or a device. Intrusion detection systems (IDSs) attempt to identify attacks by comparing collected data to predefined signatures known to be malicious or to a model of legal behavior.

Intrusion detection systems are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems.

Intrusion Prevention System

Although IDS have been one of the cornerstones of network security, they have covered only one component of the total network security picture

Scanned with CamScanner

Date __/__/__
Page _____

since they have been and they a passive component which only detects and reports without preventing

A promising model of intrusion is developing and picking up momentum. It is the intrusion prevention system (IPS) which, is to prevent attacks. Like their counterparts the IDS, IPS falls into Categories: Network-based & host based.

Malicious Software / Virus and related threats:

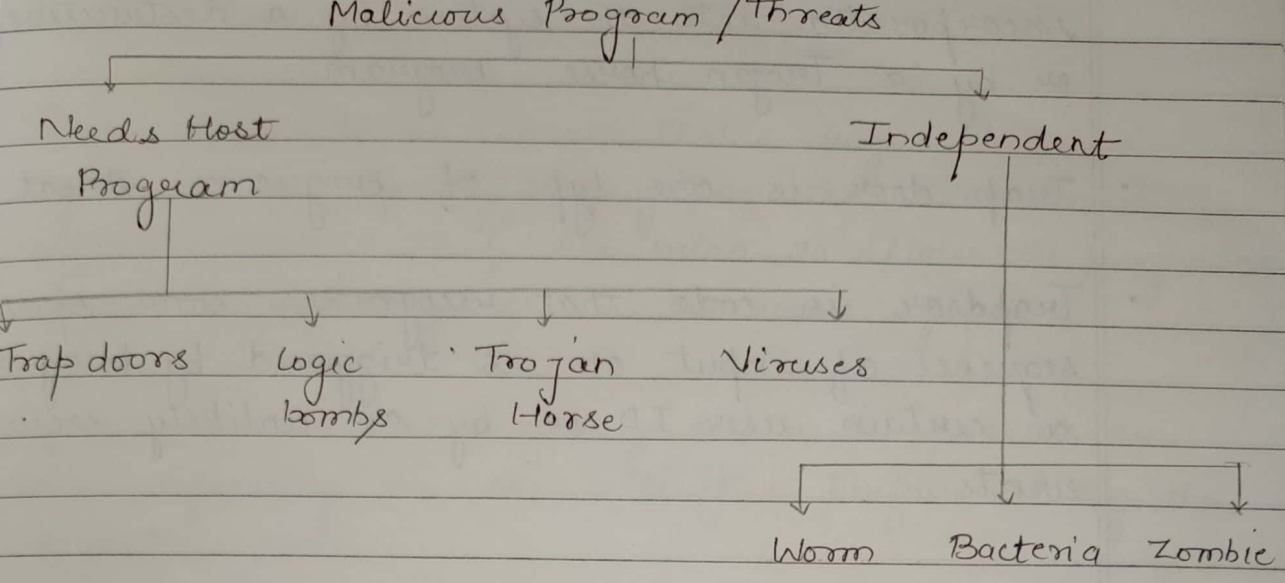
The generic term for threats is malicious software or malware. Malware is software designed to cause damage to or use up the resources of a target computer.

Malicious Programs:

These threat can be divided into two categories those that need a host program, and those that are independent. Which requires host program -s are essentially fragments of programs that cannot exist independently of some actual application program, utility or system program. Second categories, i.e, independent programs are self contained programs that can be scheduled and run by the operating system.

Scanned with CamScanner

Date __/__/____
Page _____



Trap Door

- Secret undocumented entry point into a program used to grant access without normal methods of access authentication
- Trap doors have been used legitimately for many years by programmers to debug and test programs.
- Trap door can be caused by a flow in the system design or they can be installed there by a system programmer for future use. Trap door including backdoor passwords are unspecified and non documented entry points to the system. A clever trap door could be included in a compiler.
- The compiler could generate standard object code as well as a trap door regardless of the source code being compiled. Trap door may also be a

Scanned with CamScanner

Date __/__/__
Page

incorporated into the system by a destructive virus or by a Trojan horse program.

- Trap door is one type of program threat
- Trapdoor is code that recognizes some special sequence of input or is triggered by being run from a certain user ID or by an unlikely sequence of events.
- It is difficult to implement operating system controls for trap doors. Security measures must focus on the program development and software update activities.

Logic Bomb

- Logic embedded in a computer program that checks for a certain set of conditions to be present on the system. When these conditions are met, it executes some functioning that result in unauthorized actions.
- Examples of conditions that can be used as triggers for a logic bomb are the presence or absence of certain files, a particular day of the week or date, or a particular user running the application.
- Once triggered, a bomb may alter or delete data or entire files, cause a machine halt or do some other damage.

Scanned with CamScanner

Page

Trojan Horse

- Trojan horse is a threat that's disguised as a legitimate or harmless program that sometimes carries within itself the mean to allow the programs creator to secretly access the users system.

- Trojan horse attack may either be passive or active depending on the activities performed by the clandestine code.

- For example; if the clandstine code simply steals information then it is of the passive type. But if it does something more harmful like destroying or corrupting files, then it is of the active type. A variation of the Trojan horse is a program that emulates a login program.

- Many systems have mechanisms for allowing programs written by users to be used by other users. These programs can improperly use the access rights of an ~~exchang~~ executing user and leak information.

- For example an intruder may write an editor program that works perfectly as an editor but also creates a copy of the edited file to a special area accessible to the intruder. The user is ignorant of the theft being made because the editor program performs all jobs in a perfectly normal fashion.

Scanned with CamScanner

Virus

- A Virus is a block of code that inserts copies of itself into other programs. A virus generally carries a pay-load, which may have nuisance value, or serious consequences. To avoid early detection, viruses may delay the performance of functions other than replication.

- Virus is one type of system threats.

- A virus is any unauthorized program that is designed to gain access to a computer system. Viruses need other programs to spread. Due to its spreading nature, a virus can cause severe damage to a system.

- Virus attacks are active type Trojan horse attacks. A macro virus is embedded in a word processing. When the recepient of an email or data file with embedded virus opens the document, the macro defined as an auto exec file, execute and immediately infects the systems. Viruses have even been found in legitimate applications software

- Most viruses include a string of characters that acts as a marker showing that the program has been infected. When an uninfected program is found, the virus infects it by attaching a copy of itself to the end of the program and replacing the first instruction of the program with a jump to the viral code.

Scanned with CamScanner

- Virus does not infect an already infected file in order to prevent an object file growing ever longer. This allows the virus to infect many programs without noticeably increasing disk space usage.

Precautions to prevent Virus problems

1. Buying software only from respectable store.
2. Avoid uploading of free software from public domain.
3. Avoid borrowing programs for someone whose security standards are less.

Nature of Virus

- A computer virus is a program that inserts itself into one or more files and then perform some action.

- Once a virus is executing, it can perform any function, such as erasing files and programs that is allowed by the privileges of the current user.

- During its lifecycle, a typical virus goes through the following four stages:

1. Dormant phase
2. Propagation phase
3. Triggering phase

Scanned with CamScanner

4. Execution phase

- Dormant Phase: The virus will eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit.

- Propagation Phase: The virus places an identical copy of itself into other programs or into certain system areas on the disk. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.

- Triggering Phase: The virus is activated to perform the function for which it was intended.

- Execution Phase: The function is performed. The function may be harmless, such as a message on the screen or damaging, such as the destruction of programs and data files.

Types of Viruses

1. Parasitic Viruses: A parastic virus attaches itself to executable files and replicates, when the infected program is executed, by finding other executable files to infect.

2. Memory-resident Virus: Lodges in main memory as part of a resident system program. From that

Scanned with CamScanner

point on, the virus infects every program that executes.

3. Boot Sector Virus: infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus.

4. Stealth Virus: A form of virus explicitly designed to hide itself from detection by antivirus software.

5. Polymorphic Virus: A virus that mutates with every infection, making detection by the signature of the virus impossible.

6. Metamorphic Virus: A metamorphic virus rewrites itself completely at every iteration, increasing the difficulty of detection. Metamorphic viruses may change their behavior as well as their appearance.

Macro Viruses

- Macro viruses are particularly threatening for a number of reasons.

1. A macro virus is platform independent virtually all of the macro viruses infect MS word documents.

Scanned with CamScanner

Date __/__/__
Page _____

2. Macro viruses infect documents, not executable portions of code.

3. Macro viruses are easily spread. A very common method is by electronic mail.

- Macro viruses take advantage of a feature found in word and other office applications such as Microsoft Excel, namely the Macro.

E-mail Viruses

- If the recipient opens the email attachment, the Word Macro is activated. The e-mail virus sends itself to everyone on the mailing list in the user's e-mail package. The virus does local damage.

- The first rapidly spreading e-mail viruses such as Melissa, made use of a Microsoft Word Macro embedded in an attachment.

WORMS

- Worm is a program that replicates itself by installing copies of itself on other machine across a network.

- An e-mail virus has some of the characteristics of worm because it propagates itself from system to system.

Scanned with CamScanner

- Network worm programs use network connections to spread from system to system. To replicate itself, a network worm uses some sort of network vehicle. Examples include the following:

1. Electronic mail facility
2. Remote execution capability
3. Remote login capability

- A network worm exhibits the same characteristics as a computer virus a dormant phase a propagation phase, a triggering phase and an execution phase.

- The propagation phase generally performs the following functions:

1. Search for other systems to infect by examining host tables or similar repositories of remote system addresses.

2. Establish a connection with a remote system.

3. Copy itself to the remote system and cause the copy to be run.

Zombie

A Zombie is a program that secretly takes over another internet-attached computer and then uses that computer to launch attacks that are difficult

Scanned with CamScanner

Date __/__/__
Page _____

to trace to the zoombie's creator. Zombies are used in denial-of service attacks, typically against targeted websites. The zoomble is planted on hundreds of computers belonging to unsuspecting third parties, and then used to overwhelm the target website by launching an overwhelming onslaught of Internet traffic.

Scanned with CamScanner