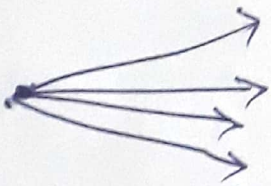
Basic concepts of Unix Access Control: users, Groups, files, processes

- Each user account has a unique UID
- The UID 0 means the super user (system admin)
- A user account belongs to multiple groups
- Subjects are processes
  - associated with uid/gid pairs, eg. (euid, egid)
- objects are files.

users and principals

(may be same set of UID & password so, single UID to each user each application)



users

Redwood users

Principals

unit of access control and authorization

- The system authenticates the human user to a particular principal
- There should be a one-to-many mapping from users to principals
  - a user may have many principals, but
  - each principal is associated with a unique user
  - Each object (files, directories) has
    - owner
    - group
    - 12 permission bits

change mode
chmod 735 <filename>
SUID if 111 Read write excel
SGID 101 Read Non "

⇒ process User ID Model in Modern Unix Systems

- Each process has three user IDs
  - real user ID (ruid) → owner of the process
  - effective user ID (euid) → used in most access control decisions
  - Saved user ID (suid)

and three group IDs

- real group ID
- effective group ID
- Saved group ID

① Real user ID → used to determine which user started the process.

⇒ Each Unix process has a user ID and a group ID associated with it, and when trying to open a file for writing, for instance, these IDs are used to determine whether the process should be granted access or not. These IDs constitute the effective privilege of the process, because they determine what a process can do and what it cannot. Most of the time, these IDs will be referred to as the effective uid and gid.

Confinement:- ensure misbehaving app cannot harm rest of system.
(custody)

An old ex:- chroot
- chroot /tmp/guest - root dir "/" is now "/tmp/guest"
suguest & UID set to "guest"

application cannot access files outside of jail.

problem:- all utility programs (header file) must live inside jail.

(i) Confinement techniques.

chroot:- The term chroot refers to a process of creating a virtualized environment in a Unix O.S, separating it from the main O.S and directory structure. This process essentially generates a confined space, with its own root directory, to run s/w programs. This virtual environment runs separately from the main operating system's root directory. Any s/w program run in this environment can only access files within its own directory tree. It cannot access files outside of that directory tree. This confined virtual environment is often called as "chroot jail".

(ii) jailkits:- jailkit is a specialized tool that is developed with a focus on security.
- jailkit is a set of utilities to limit user accounts to specific files using chroot() and or specific commands.

- It will abort in a secure way if the configuration is not secure, and it will send useful log messages that explain what is wrong to system log.

(iii) Free BSD jail:-

- It is a popular free and open source operating system that is based on the BSD version of the unix O.S.

- The jail mechanism is an implementation of Free BSD's OS-level virtualization that allows system administrators to partition a free-BSD-derived computer system into several independent mini-systems called jails, all sharing the same kernel, with very little overhead. It is implemented through a system call jail.

- The need for the free BSD jails came from a small shared-environment hosting provider's desire to establish a clean, clear-cut separation between their own services and those of their customers, mainly for security and ease of administration.

SUID, SGID and Sticky bits

These all 3 are the special permission that are available for executable files and directories

a) SUID. SUID is set user identification. SUID is a special permission assigned to a file.

- These permissions allow the file being executed to be executed with the privileges of the owner.

b) SGID - SGID is set group identification.

- when the set Group ID bit is set, the executable is run with the authority of the group.

c) Sticky bit - when the sticky bit is set on a directory, only the root user, the owner of the directory, and the owner of a file can remove files within said directory.

Unit 2 notes of Computer System Security

What is object

An object is anything on which a subject can perform operations usually objects are passive, for example file, folder, memory segment.

What is subject

A subject is a program executing on behalf of some principals. A principal may at any time be idle, or have one or more subjects executing on its behalf.

Describe the **Detour** used in UNIX user Ids and process Ids.

1. Every user in UNIX like operating system is identified by different integer number, this unique number is called as user ID
2. There are three types of UID defined for a process, which can be dynamically changed as for the privilege of task
3. The three different types of user IDs defined are:
    - Real user ID: it is account of owner of this process. It defines which files that this process has access to.
    - Effective user ID: it is normally same as real user ID, but sometime it is changed to enable a non privileged user to access file that can only be accessed by root
    - Saved user ID: it is used when a process is running with elevated privileges needs to do some under privilege work, this can be achieved by temporary switching on non privilege account
4. Each user account has a unique UID . The UID 0 means the Superuser (system admin) . A user account belongs to multiple groups. Subject are processes, associated with uid/ gid pairs.

Explain error 404 digital hacking in India part 2 chase

Some attacks discuss in error 404 digital hacking India part 2 chase are:

a. Israel Power Grid hit by a big hack attack it is being called one of the worst cyber attack ever
b. In 2014 hydro power plant in upstate New York got hacked
c. France in infrastructure including its main nuclear power plant is being targeted by a new and dangerous powerful cyber worm
d. Bangladesh best group hacked into nearly 20000 Indian website including the Indian border security force
e. First virus that could crash Power Grid or destroy pipeline is available online for anyone to download and Tinker with
f. India’s biggest data breach when the SBI debit card branch happens when this happened Bank where initially in a state of denial but subsequently they had to own up cyber security breach that took place in Indian history

Computer system security unit-2

VM based isolation

1. Virtualization technology allows the sharing of the same physical resources among several users
2. This enables the Consolidation of servers and a multitude of user machines into very small set of physical servers by replacing the physical machines with virtual machine , running on the same physical servers.
3. Temporal isolation or performance isolation among virtual machine refers to the capacity of isolating the temporal behavior of multiple VMs among each other despite them running on the same physical host and sharing a set of physical resources such as processes memory and disk.
4. Which machine search software instructions of real machines provide a virtual platform for running tasks.
5. Virtual machines have been employed to provide various features like Optimisation , translation, replication etc.
6. A virtual machine can support individual processor or a complete system depending on the obstruction level where virtualization occurs.

types of VM based isolation

a. Process virtualization machine:
    1. Process virtual machine support individual processes or a group of processes and enforce isolation between the processes and operating system environment.
    2. Process visualisation machine can run processes compiled for the same instructions set architecture based ISA 44 different ideas as long as the virtual machine runtime supports the translation.
    3. Isolation policies are provided by a runtime component which runs the processes under its control
    4. Isolation is guaranteed because the virtual machine runtime does not allow access to the resources
b. System virtual machines

    1 . System which all machines provide a full replica of the underlined platform and thus enable complete operating system to be Run within it.

    2. The virtual machine monitor runs at the highest privilege level and divides the platform hardware resources among multiple replicated guest system

    3. All Axis by the guest system to the underlying hardware resources are then mediated by the virtual machine monitor

    4. This mediation provides the necessary isolation between the virtual machines

    5. System virtual machines can be implemented in a pure isolation mode in which divisional systems do not share any resources between themselves or in a sharing mode in which the VM monitor multiplexers resources between the Machines

c. Hosted virtual machines

    1. Hostel virtual machines are built on top of an existing operating system called the host

2. The virtualization layers it's above the regular operating system and makes the virtual machine look like and application process

3. We then install complete operating system called guest operating system within the host virtual machines

4. The VM can provide the same instructions set in architecture as the host platform or it may also support a completely different instruction set architecture live running Windows IA 32 OS on a Mac running on the power PC platform.

5. VM were GSX server is an example where the host ISA and guest ISA are same.

6. The processes running inside the virtual machine cannot affect the operation of processes outside the virtual machine

7. System emulators are also loosely classified under hostel virtual machines

d. Hardware virtual machine:

1. Hardware virtual machines are visual machines build using virtualization primitives provided by the hardware like processor or input output devices

2. The advantage of hardware level virtualization is tremendous performance improvements over the software based approaches and guarantees better isolation between machines

3. The isolation provided by the hardware assisted virtualisation is more secure than that provided by the software counterpart for obvious reason.

Intrusion Detection System (IDS)

An **Intrusion Detection System (IDS)** is a system that monitors **network traffic** for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.

Intrusion prevention systems also monitor network packets inbound the system to check the malicious activities involved in it and at once sends the warning notifications.

Classification of Intrusion Detection System:
IDS are classified into 5 types:

1. **Network Intrusion Detection System (NIDS):**
   Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of an NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying crack the firewall.
2. **Host Intrusion Detection System (HIDS):**
   Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their layout.

3. **Protocol-based Intrusion Detection System (PIDS):**
   Protocol-based intrusion detection system (PIDS) comprises of a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol. As HTTPS is un-encrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.
4. **Application Protocol-based Intrusion Detection System (APIDS):**
   Application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application specific protocols. For example, this would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.
5. **Hybrid Intrusion Detection System :**
   Hybrid intrusion detection system is made by the combination of two or more approaches of the intrusion detection system. In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system. Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

Detection Method of IDS:

1. **Signature-based Method:**
   Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures.

   Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

2. **Anomaly-based Method:**
   Anomaly-based IDS was introduced to detect the unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model. Machine learning based method has a better generalized property in comparison to

signature-based IDS as these models can be trained according to the applications and hardware configurations.

Comparison of IDS with Firewalls:

IDS and firewall both are related to the network security but an IDS differs from a firewall as a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls restrict access between networks to prevent intrusion and if an attack is from inside the network it don't signal. An IDS describes a suspected intrusion once it has happened and then signals an alarm.