Confinement Principle

The confinement principle deals with preventing a server from disclosing the information that the user of the service considers confidential. The confinement ensures that the webserver should allow accessing certain services to authorized users only.

In confinement principle, access control affects the server in two ways:

The goal of the service provider: The server must ensure that the resources that are being accessed on the behalf of the client include only those resources that the client is authorized for.
The goal of the service user: The server must ensure the privacy of the service user. The server should never disclose the client's data without the permission of the client. The client data could be seen by only those entities to whom the client is allowed to see.

Detour Unix User Ids Process

1. Detour is defined as few words about Unix user IDs and IDs associated with Unix processes.
2. Every user in Unix like operating system is identified by different integer number, this unique number is called as UserID.
3. There are three types of UID defined for a process, which can be dynamically changed as per the privilege of task.
4. The three different types of UIDS defined are :
À). Real UserID : It is account of owner of this process. It defines which files that this process has access to.
B). Effective UserID : It is normally same as real UserID, but sometimes it is changed to enable a non-privileged user to access files that can only be accessed by root.
C). Saved UserID: It is used when a process is running with elevated privileges (generally root) needs to do some under-privileged work, this can be achieved by temporarily switching to non-privileged account.

Confinement Techniques

1. Chroot (change root):

A. A chroot on Unix operating systems is an operation that changes the apparent root directory for the current running process and its children.
B. The programs that run in this modified environment cannot access the files outside the designated directory tree. This essentially limits their access to a directory tree and thus they get the name chroot jail.
C. The idea is that we create a directory tree where we copy or link in all the system files needed for a process to run.
D. We then use the chroot system call to change the root directory to be at the base of this new tree and start the process running in that chrooted environment.
E. Since it cannot actually reference paths outside the modified root, it cannot maliciously read or write to those locations.

2. Jailkits:

A. Jaillkit is a set of utilities to limit user accounts to specific files using chroot() or specific commands.
B. Setting up a chroot shell, a shell is limited to some specific command and can be automated using these utilities.
C. Jailkit is a specialized tool that is developed with a focus on security.
D. 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
E. Jailkit is known to be used in network security appliances.

System call interposition

System Call Interposition: In computing, a system call is the programmatic way in which a computer program requests a service from the kernel of the operating system it is executed on. A system call is a way for programs to interact with the operating system. A computer program makes a system call when it makes a request to the operating system's kernel. System call provides the services of the operating system to the user programs via Application Program Interface(API). It provides an interface between a process and operating system to allow user-level processes to request services of the operating system. System calls are the only entry points into the kernel system. All programs needing resources must use system calls.

Services Provided by System Calls:

1. Process creation and management
2. Main memory management
3. File Access, Directory and File system management
4. Device handling(I/O)
5. Protection
6. Networking, etc.

The interface between a process and an operating system is provided by system calls. In general, system calls are available as assembly language instructions. They are also included in the manuals used by the assembly level programmers.

System calls are usually made when a process in user mode requires access to a resource. Then it requests the kernel to provide the resource via a system call.

Types of System Calls

There are mainly five types of system calls. These are explained in detail as follows

Process Control

These system calls deal with processes such as process creation, process termination etc.

File Management

These system calls are responsible for file manipulation such as creating a file, reading a file, writing into a file etc.

Device Management

These system calls are responsible for device manipulation such as reading from device buffers, writing into device buffers etc.

Information Maintenance

These system calls handle information and its transfer between the operating system and the user program.

Communication

These system calls are useful for interprocess communication. They also deal with creating and deleting a communication connection.

Error 404 Hacking Digital India Part 2 Chase

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

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

VM isolation

A process VM is a virtual platform created for an individual process and destroyed once the process terminates. Virtually all operating systems provide a process VM for each one of the applications running. A VM is an isolated environment with access to a subset of physical resources of the computer system. Each VM appears to be running on the bare hardware, giving the appearance of multiple instances of the same computer, though all are supported by a single physical system.

Software Fault isolation

When protecting a computer system, it is often necessary to isolate an untrusted component into a separate protection domain and provide only controlled interaction between the domain and the rest of the system. Software-based Fault Isolation (SFI) establishes a logical protection domain by inserting dynamic checks before memory and control-transfer instructions. In this Program (tb be isolated), runs inside a dedicated isolated address space, called a sandbox.
Scenarios for Sandboxing

- Web Browser Plugins
    - o Security hole in plugin compromises browser
    - o Impose restrictions on plugin
- Downloaded executable applications from untrusted sources
- Packet Filter
    - o Can use callbacks to copy and filter packets in the application
        - Incurs a lot of overhead from context switching
    - o Put filtering logic in kernel
        - Danger of un trusted code running in supervisor mode

What Is a Rootkit?

A rootkit is a clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence. The term rootkit is a connection of the two words "root" and "kit." Originally, a rootkit was a collection of tools that enabled administrator-level access to a computer or network. Root refers to the Admin account on Unix and Linux systems, and kit refers to the software components that implement the tool. Today rootkits are generally associated with malware – such as Trojans, worms, viruses – that conceal their existence and actions from users and other system processes.

What Can a Rootkit Do?

A rootkit allows someone to maintain command and control over a computer without the computer user/owner knowing about it. Once a rootkit has been installed, the controller of the rootkit has the ability to remotely execute files and change system configurations on the host machine. A rootkit on an infected computer can also access log files and spy on the legitimate computer owner's usage.

Intrusion Detection System

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 the 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.

Classification of Intrusion Detection System

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 a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall. A network-based intrusion detection system is designed to help organizations monitor their cloud, on-premise and hybrid environments for suspicious events that could indicate a compromise. This includes policy violations and port scanning, plus unknown source and destination traffic.

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):

A protocol-based intrusion detection system (PIDS) is an intrusion detection system which is typically installed on a web server, and is used in the monitoring and analysis of the protocol in use by the computing system. Protocol-based intrusion detection system (PIDS) comprises 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:

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.

Anomaly-based Method:

Anomaly-based IDS was introduced to detect 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.