Intrusion Handling

Definition of intrusion

The act of intruding or the state of being intruded especially the act of wrongfully entering upon, seizing, or taking possession of the property of another is called intrusion and the person doing this act called intruder.

Intruders

Intruders are often referred to as hackers and are the most harmful factors contributing to the vulnerability of security. They have immense knowledge and an in-depth understanding of technology and security. Intruders breach the privacy of users and aim at stealing the confidential information of the users. The stolen information is then sold to third-party, which aim at misusing the information for their own personal or professional gains.

Intruders are divided into three categories:

- **Masquerader:** The category of individuals that are not authorized to use the system but still exploit user's privacy and confidential information by possessing techniques that give them control over the system, such category of intruders is referred to as Masquerader. Masqueraders are outsiders and hence they don't have direct access to the system, their aim is to attack unethically to steal data/ information.
- **Misfeasor:** The category of individuals that are authorized to use the system, but misuse the granted access and privilege. These are individuals that take undue advantage of the permissions and access given to them, such category of intruders is referred to as Misfeasor. Misfeasors are insiders and they have direct access to the system, which they aim to attack unethically for stealing data/ information.
- **Clandestine User:** The category of individuals those have supervision/administrative control over the system and misuse the authoritative power given to them. The misconduct of power is often done by superlative authorities for financial gains, such a category of intruders is referred to as Clandestine User. A Clandestine User can be any of the two, insiders or outsiders, and accordingly, they can have direct/ indirect access to the system, which they aim to attack unethically by stealing data/ information.

Below are the different ways adopted by intruders for cracking passwords for stealing confidential information:

- Regressively try all short passwords that may open the system for them.
- Try unlocking the system with default passwords, which will open the system if the user has not made any change to the default password.

- Try unlocking the system by personal information of the user such as their name, family member names, address, phone number in different combinations.
- Making use of Trojan horse for getting access to the system of the user.
- Attacking the connection of the host and remote user and getting entry through their connection gateway.
- Trying all the applicable information, relevant to the user such as plate numbers, room numbers, locality info.

To prevent intruders from attacking the computer system, it is extremely important to be aware of the preventive measures which leads to strengthening of the security posture.

Approaches to Intrusion Detection and Prevention:

1. Pre-emptive Blocking:

It is also called Banishment vigilance. It seeks to prevent intrusion from happening before they occur. The above method is done by observing any danger signs of imminent threats and then blocking user or IP address from which these signs originate. Example – This technique includes attempts to detect early foot-printing of an imminent intrusion then blocking IP or user that is source of foot-printing activity. If Admin finds that particular IP address is source of frequent port scans and other scans of their system then they will block that IP address at firewall. The above intrusion detection and avoidance can be quite complicated which could potentially block legitimate user by mistake. The complexity arises from distinguishing legitimate traffic from that indicative of an impending attack. This can lead to problem of false positives, in which system mistakenly identifies legitimate traffic as some form of attack.

- A software system will simply alert administrator that suspicious activity has taken place. The human admin then makes decision whether or not to block traffic.
- If software automatically blocks any addresses it deems suspicious, you run risk of blocking out legitimate users.
- It should also be noted that nothing prevents offending user from moving to different machine to continue attack.
- This sort of approach should only be one part of an overall intrusion-detection strategy and not entire strategy.

2. Anomaly Detection:

- It involves actual software that works to detect intrusion attempts and then notify the administrator.
- The general process is simple, system looks for any abnormal behaviour. Any activity that does not match pattern of normal user access is noted and logged. The software compares observed activity against expected normal usages profiles.
- Profiles are usually developed for specific user, group of users, or applications. Any activity that does not match definition of normal behaviour is considered an anomaly and is logged.

- Sometimes above situation is referred to as “traceback” detection or “traceback” process. We are able to establish from where this packet was delivered.

The specific ways in which an anomaly is detected includes Threshold Monitoring, Resource Profiling, User/Group Work Profiling, and Executable Profiling. These are explained as following below.

3. Threshold Monitoring:

Threshold monitoring pre-sets acceptable behaviour levels and observes whether these levels are exceeded. This could include something as simple as finite number of failed login attempts or something as complex as monitoring the time user is connected and amount of data user downloads. Threshold monitoring provide definition of acceptable behaviour. Characterizing intrusive behaviour only by threshold limits can be somewhat challenging. It is often quite difficult to establish proper threshold values or proper time frames at which to check those threshold values. This can result in high rate of false positives in which system misidentifies normal usage as probable attack.

4. Resource Profiling:

It measures the system-wide use of resources and develops historic usage profile. Abnormal readings can be indicative of illicit activity underway. It might be difficult to interpret meaning of changes in overall system usages. An increase in usage might simply indicate something benign like an increased workflow rather than an attempt to breach security.

5. User/Group Work Profiling:

Here, the IDS maintains individual work profiles about user and groups. These users and groups are expected to obey these profiles. As the user changes his/her activities, his/her expected work profile is updated to reflect those changes. Some systems attempt to monitor interaction of short-term versus long-term profiles. The short-term profiles capture recent changing work patterns, whereas long-term profiles provide view of usages over an extended period of time. However, it can be difficult to profile an irregular or dynamic user base. Profiles that are defined too broadly enable any activity to pass review, whereas profiles that are defined too narrowly may inhibit user work.

6. Executable Profiling:

Executable profiling seeks to measure and monitor how programs use system resources, paying particular attention to those whose activity can always be traced to specific originating user. Example – system services usually cannot be traced to specific user launching them. Viruses, Trojan horses, worms, Tap-doors and other software attacks are addressed by profiling how system objects such as files and printers are normally used, not only by the user but also by other system subjects on the part of users. If the viruses inherit all of privileges of user executing software. Software is not limited by the principle of least privilege but to only those privileges needed to properly execute. This openness architecture permits viruses to covertly change and infect totally unrelated parts of system. Executable profiling enables IDS to identify activity that might indicate an attack. Once potential danger is identified, method of notifying administrator, such as by network message or email, is specific to individual IDS.

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 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. 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 send 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 behaviour 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.
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 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 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 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 doesn't signal. An IDS describes a suspected intrusion once it has happened and then signals an alarm.

Intrusion Prevention System (IPS)

Intrusion Prevention System is also known as Intrusion Detection and Prevention System. It is a network security application that monitors network or system activities for malicious activity. Major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it and attempt to block or stop it.

Intrusion prevention systems are contemplated as augmentation of **Intrusion Detection Systems (IDS)** because both IPS and IDS operate network traffic and system activities for malicious activity.

IPS typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IPS can also respond to a detected threat by attempting to prevent it from succeeding. They use various response techniques, which involve the IPS stopping the attack itself, changing the security environment or changing the attack’s content.

Classification of Intrusion Prevention System (IPS):
Intrusion Prevention System (IPS) is classified into 4 types:

1. **Network-based intrusion prevention system (NIPS):**
   It monitors the entire network for suspicious traffic by analysing protocol activity.

2. **Wireless intrusion prevention system (WIPS):**
   It monitors a wireless network for suspicious traffic by analysing wireless networking protocols.

3. **Network behaviour analysis (NBA):**
   It examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service attacks, specific forms of malware and policy violations.

4. **Host-based intrusion prevention system (HIPS):**
   It is an inbuilt software package which operates a single host for doubtful activity by scanning events that occur within that host.

Comparison of Intrusion Prevention System (IPS) Technologies:

The Table below indicates various kinds of IPS Technologies:

IPS Technology Type	Types of Malicious Activity Detected	Scope per Sensor	Strengths
Network-Based	Network, transport, and application TCP/IP layer activity	Multiple network subnets and groups of hosts	Only IDPS which can analyse the widest range of application protocols;
Wireless	Wireless protocol activity; unauthorized wireless local area networks (WLAN) in use	Multiple WLANs and groups of wireless clients	Only IDPS able to predict wireless protocol activity
NBA	Network, transport, and application TCP/IP layer activity that causes anomalous network flows	Multiple network subnets and groups of hosts	Typically more effective than the others at identifying reconnaissance scanning and DoS attacks, and at reconstructing major malware infections
Host-Based	Host application and operating system (OS) activity; network, transport, and application TCP/IP layer activity	Individual host	Can analyse activity that was transferred in end-to-end encrypted communications

Detection Method of Intrusion Prevention System (IPS):

1. **Signature-based detection:**
   Signature-based IDS operates packets in the network and compares with pre-built and preordained attack patterns known as signatures.

2. **Statistical anomaly-based detection:**
   Anomaly based IDS monitors network traffic and compares it against an established baseline. The baseline will identify what is normal for that network and what protocols are used. However, It may raise a false alarm if the baselines are not intelligently configured.

3. **Stateful protocol analysis detection:**
   This IDS method recognizes divergence of protocols stated by comparing observed events with pre-built profiles of generally accepted definitions of not harmful activity.

Comparison of IPS with IDS:
The main difference between Intrusion Prevention System (IPS) with Intrusion Detection Systems (IDS) are:

1. Intrusion prevention systems are placed in-line and are able to actively prevent or block intrusions that are detected.
2. IPS can take such actions as sending an alarm, dropping detected malicious packets, resetting a connection or blocking traffic from the offending IP address.
3. IPS also can correct cyclic redundancy check (CRC) errors, defragment packet streams, mitigate TCP sequencing issues and clean up unwanted transport and network layer options.

Thank You