Unit 5

Q) Intrusion Detection Systems and its types

Intrusion Detection System is any hardware, software, or a combination of both that monitors a system or network of system against any malicious activity. This is mainly used for detecting break-ins or misuse of the network.

In short, we can say that IDS is the 'burglar alarm' for the network because

much like a burglar alarms, IDS detects the presence of an attack in the network and raises an alert. An IDS provides three functions: monitoring, detecting and generating an alert. IDS are often considered as the functionality of firewall. But there is a thin line of difference between them. A firewall must be regarded as a fence that protects the information flow and prevent intrusions whereas IDS detects if the network is under attack or if the security enforced by the firewall has breached. Together firewall and IDS enhance the security of network. Intrusion detection System uses a security policy (or rules) to detect unusual activity. These rules are defined by the administrator based on the needs of the organization. Any activity

What violates this security policy will be considered a security threat and will be reported to the administrator in the email on the page or as SNMP traps. These policies must be updated regularly to keep up with the threats and trends.

Of the security incidents that occur on a network the vast majority by up to 85 percent by known as threats come from inside the network. These attacks may consist of otherwise authorized users who are disgruntled employees. The remainder come from the outside in the form of denial of service attacks or attempts to penetrate a network infrastructure. Intrusion detection systems remain the only proactive means of detecting and responding to threats that stem from both inside and outside a corporate

network.

Types of IDS

There are three main types of Intrusion Detection Systems:

1) Host Based
2) Network Based
3) Stack Based
4) Signature Based
5) Anomaly Based

Host Based IDS

Intrusion Detection System is installed on a host in the network. HIDS collects and analyzes the traffic that is originated or is intended to that host. HIDS leverages their privileged access to monitor specific components of a host that are not readily accessible to other systems. Specific components of the operating system such as passwd files in UNIX and the Registry in

Windows can be watched for misuse. There is great risk in making these types of components available to NIDS to monitor. Although HIDS is far better than NIDS in detecting malicious activities for a particular host, they have limited view of entire network topology and they cannot detect attack that is targeted for a host in a network which does not have HIDS installed.

Network Based IDS

Network IDSs (NIDS) are placed in key areas of network infrastructure and monitors the traffic as it flows to other host. Unlike HIDS, NIDS have the capability of monitoring the network and detecting the malicious activities intended for that network. Monitoring criteria for a specific host is the

network can be increased or decreased with relative ease. NIDS should be capable of standing against large amount numbers of network traffic. As network traffic increases exponentially NIDS must grab all the traffic and analyze in a timely manner.

Stack Based IDS

Stack Based IDS is latest technology, which works by integrating closely with the TCP/IP stack, allowing packets to be watching as they traverse their way up the OSI layers watching the packet in this way allows the IDS to pull the packet from the stack before the OS or application has a chance to process the packets.

Signature-Based I.D.S.

- Signature-Based IDS use a ruleset to identify intrusions by watching for patterns of events specific to known and documented attacks.
- It is typically connected to a large database which houses attack signatures. It compares the information it gathers against those attack signatures to detect a match.
- These types of systems are normally presumed to be able to detect only attacks "known" to its database. Thus if the database is not updated with regularity, new attacks could slip through. It can, however, detect new attacks that share characteristics with old attacks eg., accessing 'cmd.exe' via a HTTP GET request. But, in case of new, uncataloged attacks this technique is

pretty porous.
Also, signature based IDS's may affect performance in cases when intrusion patterns match several attack signatures. On cases such as these, there is a noticeable performance lag. Signature definitions stored in the database need to be specific so that variations on known attacks are not missed. This sometimes leads to building up of huge databases which eat up a chunk of space.

Anomaly Based IDS

Anomaly Based IDS examines ongoing traffic activity, transactions and behavior in order to identify intrusions by detecting anomalies. It works on the notion that "attack behavior" differs enough from "normal user behavior"

such that it can be distinguished by cataloging and identifying the differences involved. In most anomaly-based IDS's the system administrator defines the baseline of normal behavior. This includes the state of the network's traffic load, breakdown protocol and typical packet size. Anomaly detectors monitor network segments to compare their state to the normal baseline and look for current behavior that deviate statistically from the normal. This capability theoretically gives anomaly-based IDS's abilities to detect new attacks that are neither known nor for which signatures have been created. On the other hand anomaly-based IDS systems have been known to be prone to a lot of false positives. In these cases, the attacks are reported based on

changes to the current system on which the IDS is installed. This is because there is a change in the normal state of the system which is not perceived by the IDS.

Sometimes, anomaly based IDS systems can cause heavy processing overheads on the computer system they are installed on. It takes a short period of time for anomaly based systems to create statistically significant baselines. During this period, they are relatively open to attack.

8] Prevention vs Detection / Intrusion Detection Systems (IDS) VS Intrusion Prevention System (IPS)

Intrusion Detection System (IDS) is a computer security system that

monitors network traffic for malicious activities and alert the network administrator when malicious activities detected. IDS performs a passive monitoring and implement in passive/promiscuous mode. IDS can detect the malicious activities but cannot prevent it. IDS have these capabilities include:

- Monitoring about malicious activities
- Auditing about malicious activities
- Forensics about malicious activities
- Reporting about malicious activities

Steps:-

1) Attacker sends a malicious traffic via internet to the target host.
2) Data packets will reach to both network and IDS
3) On IDS, packet will be inspected by sensor.

4) Store the log messages in management console.

Intrusion Prevention System (IPS) is a computer security mechanism that monitors network traffic for malicious activities (security threats or policy violations) and takes actions to prevent activities. IPS responsibilities include:

- Identify any malicious activity on the network.
- Send an alarm to the network administrator about malicious actions detected on the network system.
- Drop the malicious packets.
- Block the traffic from the source address that malicious packets originated.
- Record the activities in management console.
- Reset the connection.

IPS performs its actions monitoring and implement

...vision mode. IPS can be divided into two types: HIDS based IPS and network based IPS.

Steps:

1) Attacker sends a malicious traffic via internet to the target host.
2) Data packet will reach to IPS and will be inspected by sensor.
3) Store the log/report on management console and record actions.
4) Send the malicious packet to the bit bucket and drop it. Step 3 and 4 will happen at the same time.

IDS	IPS
Implement in passive/promiscuous mode	Implement in inline mode
Performs passive monitoring	Performs active monitoring

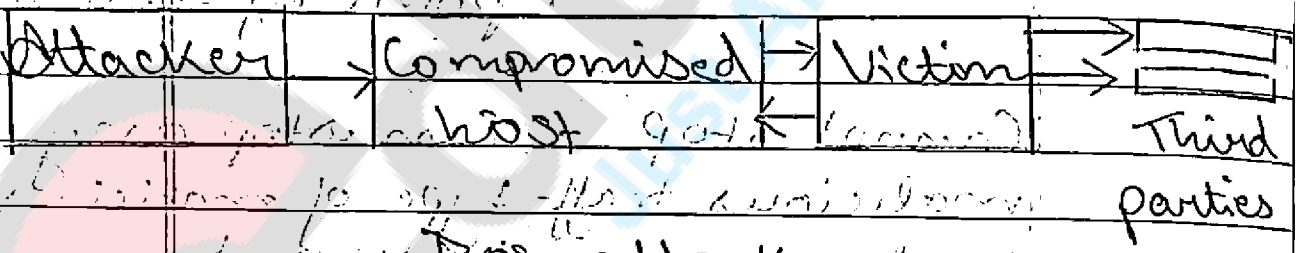
Can detect malicious traffics and alert about it in details	Can block malicious traffics and drop them into the bit bucket
No impact on the network performance, did even if sensor failure occurs	Some impact on the network performance, slow down the traffics on network and sensor failures stops the traffics flow (single point of failure)
Cannot stop malicious traffics from reaching the destination	Can stop any type of malicious traffics from reaching the destination

5) DOS attacks

Denial of Service attacks (DOS) are becoming highly popular mode of web attack these

days. It involves making the computer systems inaccessible by flooding servers, networks, or even end user systems with useless traffic so that legitimate users can no longer gain access to those resources.

A popular form of DOS attacks which happens worldwide is DDOS (Distributed Denial of Service) wherein multiple computer (also called zombies) participate in sending the traffic



DOS attack

Dos attacks exploit the asymmetric nature of certain types of network traffic. Therefore Dos attacks can be classified into three categories.

1) Bandwidth / Throughput Attacks

Ping flood attack	DDos attack	UDP flood attack
Saturate a network with ICMP echo requests	Focus the internet bandwidth of many machines upon one or few machines. In this way we create a large flood effect	Since UDP is a very simple unreliable protocol, an attacker simply creates enough packets to jam the network

2) Protocol Attacks

Smurf attack	DNS nameserver attacks
Here, spoofed (forged) IP packets with ICMP ECHO (ping) messages are sent with source address (forged) being the IP address of system to be attacked	It involves an intruder sending a large number of UDP-based DNS requests to a Nameserver using a spoofed source IP address. Any Nameserver responses are sent back to the

	spoofed IP address as the destination

3) Software Vulnerability Attacks

land attack	Ping of death attack	Teardrop attack
In this attack, an attacker sends spoofed TCP-SYN packets, with the same source and destination addresses as the victim's host address	Ping of death is an attempt by an attacker to crash, reboot or freeze a system by sending an illegal ICMP packet to the host under attack. The TCP/IP specification allows for a maximum packet size of up to 65536 octets. On some TCP/IP stack implementations those kinds of packets may cause the victim's host to crash or later	A normal packet is sent. A second packet is sent which has a fragmentation offset claiming to be inside the first fragment. This second fragment is too small to even extend outside the first fragment. This may cause an unexpected error condition

	Size may cause the victim's host to crash	to occur on the victim host

5) Flooding Attacks

Flooding is a Denial of Service (DOS) attack that is designed to bring a network or service down by flooding it with large amounts of traffic. Flood attacks occur when a network or service becomes so weighed down with packets initiating incomplete connection requests that it can no longer process genuine connection requests. By flooding a server or host with connections that cannot be completed, the flood attack eventually fills the hosts memory buffer. Once this buffer is full no further connections can be made, and the result is a Denial of Service.

PAGE NO.
DATE: / /

Q] DDoS attack prevention / Detection

DDoS Prevention

- Preventive measures at the victim side

One way of handling SYN attacks is to drop requests for TCP connection.

This can create problem if the victim is not able to distinguish between SYN packets from an attacker and a normal user.

One way to handle issue is
- Categorize IP addresses as "almost certainly genuine", "probably spoofed" etc
- under moderate load, all incoming packets are entertained
- when heavy load, packets with unfamilian source address are discarded

Another way
- under high load, allocate a full buffer of about 300 bytes for a given TCP connection request only upon completion of three way handshake protocol

• Preventive measures inside the network
- egress filtering
- Distribute Route filtering

Egress filtering
Let A be the set of all externally visible IP addresses within the network
Egress router examines the source address of each packet leaving it.
If the address doesn't match any address in A, it drops the packet.

2) Distribute Route filtering
A router is used for filtering packets with spoofed address
It uses packets source address to make decision
To implement RPF filter maintains set of source address from which packets arrive to some destination
If a packet with source IP address arrives via an interface that it should not have, that packet is discarded

PAGE NO.
DATE

DDoS Detection

Another approach to handle DDoS is to detect it and take remedial action.

In a TCP connection, we are having SYN packets and RST packets.

SYN - TCP connection request packet

FIN - TCP connection termination packet

RST - connection abort

To construct an anomaly detection system, we define some variables.

S_i = SYN packets arrives in the i^{th} interval

F_i = FIN packets arrives in the i^{th} interval

D_i = normalized difference between SYN and FYN packets in the i^{th} interval

i.e, $D_i = S_i - F_i / F_i$

T = threshold for detection

To construct an anomaly detection system, we define some

variables

S_i = SYN packets arrives in the i^{th} interval

F_i = FIN packet arrives in the i^{th} interval

D_i = normalized difference between SYN and FYN packets in the i^{th} interval

i.e $D_i = S_i - F_i / F_i$

T = threshold for detection

It is observed for different time series.

Different algorithms are used to detect attacks by monitoring the above series.

Algorithm 1

Raise an alert if the most recently computed detection variable D_i exceeds the threshold.

Problem

- may raise false alarms since decisions is based on point values.
- if cumulative value go beyond threshold, it won't raise an alarm.

PAGE NO.
DATE. / /

Algorithm 2
raise an alert if the "smoothed average" of previous D value exceeds threshold.
The smoothed average value, Ai is calculated as
$A_i = \alpha D_i + (1-\alpha) A_{i-1}$
where
$0 < \alpha < 1$ and $A_0 = 0$

Algorithm 3
Define a modified cumulative sum of previous values of D.
raise an alert if this value exceeds the threshold.

IP traceback
Usually source address is spoofed address
So we attempt to identify the path traversed by the attack packets.
Two approaches
- Packet marking
- Packet logging

Packet marking :- Packets keep track of the routers it has

visited.

Packet logging
Each router keeps track of the packets passing through it.

Q) Defenses Against Denial-of-Service Attacks

Infrastructure Improvements
First, consider increasing bandwidth and server performance. DDoS attacks attempt to overwhelm available resources so additional resources will allow you to withstand greater attacks. This involves having more server space or bandwidth than necessary. Such over-provisioning addresses the number one problem brought on by a DDoS attack, link and equipment saturation. Unfortunately, it can be difficult to determine how much extra

PAGE NO.....
DATE. ...../...../.....

hardware and bandwidth is necessary to sustain an attack as even some of the largest companies have succumbed to DDoS attacks. When attacks fail, attackers often gather a larger bot army and try again.

2) Traffic filtering :-
Consider configuring your firewall or IDS to filter DDoS traffic, if the functionality is available, or consider upgrading to a system that does. DDoS traffic filtering devices prevent SYN, TCP flooding and other types of DDoS attacks. Such devices typically analyze TCP flow control, conduct packet filtering and utilize blacklists and whitelists.

3) Real Time Monitoring :-
Another way to protect your data against a DDoS attack is through real-time monitoring. Real-time monitoring

can identify a DDoS attack early. Such a system must be actively monitored so that action can be taken quickly to resolve the situation. DDoS attacks can ramp up quickly so administrators might not have much time to respond once an alert comes in. Integration of site and device monitoring with SIEM can leverage existing technology to protect against this attack.

It should be noted that not all DDoS attacks happen immediately. Some attacks develop slowly so that they will not be noticed as easily. They gradually increase the number of requests made to resources until the resources become unavailable. It is important to have baselines of system performance and expected use so that these can be compared to active data in order to

classify traffic as legitimate or a potential DDoS attack. Consider monitoring log file sizes and growth rates. Some monitoring tools will create a more critical event and alert when a large number of informational events are generated so that administrators can stay on top of problem areas. Informational events might not appear in reports and individually they would not indicate a problem but collectively they could indicate a DDoS attempt or some other hacking activity.

4) Log Maintenance :-

Genuine users and DDoS attacks both log server events and this can cause some services to reject connections if the log files are as mentioned earlier, log file growth rates and sizes could indicate an attack but in order to prevent a full

log from making a system unavailable. You can either increase log file sizes, archive logs, or roll the logs over. If systems are set to refuse connections when the log is full, you should not implement log rollover because the refusal is a security mechanism meant to prevent unauthorized access. In this case you should either use archiving or larger log files to keep servers available.

Community:-

Finally, information security departments can work closely with the botnet hunter community. DDoS attacks rely on bots to perform their work, but if the bots are known about, control of the bots can potentially be wrested out of the attackers hands knowing who to call that

can nip the attack in the bud rather than allow it to get too big can save valuable time and effort. Know who to call at your upstream service provider to help filter attacks. Your ISP might have specialized equipment to help reduce DDoS attacks so put a plan in place to work with them to stop the attack.

[9] Malware Detection

Malware is a harmful software that pretends to be a legitimate program to infiltrate the computer. It is installed in different ways, but the most common are a phishing email, fake installer, injected attachment and phishing links. Hackers make malware presentable to convince users into installing them. Often, the users are unaware that the program is

malware because it looks legitimate. Bo
Once installed, malware hides in different folders in the computer. If it's an advanced type of malware, it can directly access the operating system. Then it starts to encrypt files and record personal information.
To detect malware, the process malware detection is created.

Malware detection is the process of scanning the computer and files to detect malware. It is effective at detecting malware because it involves multiple tools and approaches.
It is done using the following:-
1) Signature - Based Detection
Signature - based detection uses virus codes to identify malware. Malware carries a unique code that is used to identify it. When a file reaches the computer

The malware scanner collects the code and sends it to a cloud-based database. The database has a vast collection of virus codes. If the file code is found in the list, the database returns with a verdict that the file is malware. The anti-malware deletes the file from the computer and deletes it. If there's a new malware discovered, its code is added to the list.

3) Heuristic Analysis

Heuristics Analysis works differently. If Signature Based Detection relies on virus codes, Heuristics applies rules to identify malware. It has established certain rules that files cannot violate.

Some of the possible rules are:

Camera manipulation is prohibited.

Direct access to the hard drive is not allowed

Heuristics has also set a numerical value that determines if the file is suspicious If the score meets the assigned-point, it is flagged as a threat

3) Sandbox

Sandbox is a protected cell within the computer the antimalware creates to contain any suspicious or unknown file. This prevents malware injection because the file runs without injecting the other programs in the computer.

Inside the sandbox, the file is observed and analyzed further to determine if it's harmful or safe. If the file is legit, it is released, but if its malicious, it is denied.

4) Removal Tools

Lastly, when the threat is identified it must be deleted from the computer.

Here come the Removal Tools that eliminate the malware immediately. Now, the malicious file is deleted from the computer, the files and important information are perfectly safe.

The malware detection process ends here. The process starts every time a new file enters the computer. This must be done to prevent malware infection.

5) Anti Malware Software

Malware Detection is done using an anti malware software. The anti malware is a program that is designed to fight against malware. It protects the computer and ensures that it is malware free by scanning it regularly.

A computer without an anti malware software is vulnerable to malware attack. Hackers target computers

and networks with a poor security feature. ✍

Different types of malware are spread on the internet. The moment the user accesses the Internet, the risk of getting malware on the computer is there. Nowadays it is important to keep the computer security to avoid data loss.