11.1.2 Intrusion Detection System Facts

The intrusion detection system (IDS) is a software program or hardware appliance that monitors network traffic. The IDS creates an alert when it encounters a suspicious activity or known threat. It differs from an intrusion prevention system (IPS) in that the IPS takes action to prevent harmful events, while the IDS generates an alert. As an ethical hacker, you should be familiar IDSs, know how to avoid detection by an IDS when conducting a penetration test, and be able to recommend actions for IDS alerts.

This lesson covers the following topics:

- IDS roles
- Detection types
- IDS alert types

IDS Roles

An IDS gathers and analyzes information from within a computer or network. A Network Intrusion Detection Systems (NIDS) is designed to inspect each packet traversing the network for the presence of malicious or damaging behavior. A Host Intrusion Detection Systems (HIDS) is responsible for monitoring activities on a host system. It looks for misuse of a system, including insider misuses. An HIDS is more difficult to manage since it has to be maintained individually on each host system.

The following table identifies the roles of an IDS.

Role	Description
Analyze network traffic	An NIDS acts as a network sniffer to examine network traffic for: - Violations of security polices - Malicious activity on operations - Unauthorized access - Misuse of the organization's network - Signs of intrusions
Monitor log files	A Log File Monitor IDS (LFM IDS) searches log file for suspicious activity such as: - Blocked traffic due to failed or anonymous authentication - Repeated failed login attempts - Connections to known malicious sites - Activity during odd or non-business hours - Missing, short, or incomplete logs
Check file integrity	An IDS with file-checking mechanisms evaluates a specific system for the following: - New or unrecognized files, programs, or processes - Unexplained changes in file permissions - Unexplained changes in file size - Changes in configuration files - Presence of Trojan horse software

Detection Types

An IDS can perform many types of intrusion detections. The three common methods you should know are signature detection, anomaly detection, and protocol-based detection. Depending on the detection types implemented and the sophistication of the method of evasion used, a malicious attack may or may not generate an alert or be blocked from the network. The following table describes the three common types of intrusion detections:

Type	Description
Signature-based	A signature-based IDS analyzes network traffic for common patterns, referred to as signatures. Examples of signatures include byte sequences and malware instruction sequences. The IDS analyzes network traffic looking for signatures in the signature file database. Signature matching is the most basic form of detection and is used in many systems. When a match is found, the IDS logs and reports the attack. Be aware of the following regarding signature-based detection: - An attacker's intent is to exploit signatures by changing the attack so that the signature can no longer be recognized. - Signature recognition is effective at detecting known attacks, but poor at detecting attacks that aren't in the signature file database. - Signature-based detection systems are easy to implement and have a low false positive rate and a high true positive rate for known attacks. - Network traffic analysis can impact network performance.

Anomaly-based	Anomaly-based detection compares network behavior to baseline profiles or network behavior baselines. For example, if Internet Control Message Protocol (ICMP) traffic becomes greater than the baseline set, an alert is sent. Be aware of the following when you use an anomaly-based IDS: ▪ An anomaly-based IDS typically works by taking a baseline of the normal traffic taking place on the network. Then it measures the present state of traffic on the network against its baseline in order to detect patterns that are not normally present in the traffic. ▪ An anomaly-based approach can detect previously unknown threats by detecting deviations from normal baseline behavior. ▪ Anomaly-based methods can work very well when the system is configured to detect attacks that have been deliberately assembled to avoid an IDS. ▪ Anomaly-based profiles are similar to a white list because the anomaly-based IDS detects when behavior goes outside an acceptable range. ▪ A higher rate of false positives can occur with an anomaly-based IDS due to changing business needs or heightened workloads. This requires the system to be able to re-learn or update the baseline profiles constantly.
Protocol-based	Another type of detection looks specifically at protocols. Protocol-based detection can include malformed messages, sequencing errors, and similar variations from a protocol's known good behavior. Protocol detection can be useful against unknown or zero-day exploits, which might attempt to manipulate protocol behavior for malicious purposes. This type of detection is based on the anomalies that are specific to a given protocol. Detecting that a protocol is using an unusual port to operate its services is another way to check for protocol anomalies.

IDS Alert Types

An IDS may generate an alert on a network or host. Depending on how hardened the system security protocols are, there are four common outcomes:

- A true positive alert indicates a real attack, malicious activity, or suspicious traffic is detected and an alert is triggered.
- A false positive indicates an event triggers an alarm, but no actual attack is in progress.
- A true negative indicates activity that acceptable behavior or activity is recognized as authorized and accepted by the IDS. No alerts are triggered.
- A false negative is a condition that occurs when an IDS fails to react to an actual attack event. This indicates an attack has infiltrated the system undetected.