11.1.4 Avoid IDS Detection Facts

To be successful as a penetration tester of a network with an IDS, you must be able to avoid detection by the IDS or other security mechanisms. Familiarity with the network and IDS used is key to avoiding detection. Generally, a good rule of thumb is to avoid creating the signs of intrusion that a good system administrator looks for to keep the network safe.

This lesson covers the following topics:

- Signature detection avoidance
- Anomaly detection avoidance
- Protocol anomaly detection
- Host-based intrusion detection
- Network-based intrusion detection
- Other signs of system intrusion

Signature Detection Avoidance

Familiarity with signatures in the IDS will greatly enhance your chances of eluding detection. To avoid a signature-based IDS, you should:

- Design the threat to capitalize on weaknesses of the IDS.
- Avoid using known threat signatures.
- Use variations of known threat signatures that will allow you to bypass the IDS. Change the threat signature enough to fool the IDS and achieve your objective.

Anomaly Detection Avoidance

When penetration testing anomaly-based systems, obtain as much information as possible about the network behavior of the target. To avoid detection:

- Design attacks so that they make small, subtle changes to network behavior.
- Initiate activities to coincide with business activity changes and higher workloads. These situations can cause an anomaly-based IDS to generate a lot of false positives. A penetration tester can take advantage by planning attacks during those times.
- Distribute the connection requests from the attacker machine over many IPs. This is commonly done by malicious attackers through networks of compromised hosts. Other common methods are:
  - Using a system such as the Tor network to modify the IP of each packet.
  - Using an Infrastructure as a Service (IaaS) provider with a large IP space available for free to VM instances.
  - Using a product to change the source IP address.

Protocol Anomaly Detection

One means of avoiding detection when manipulating protocols is a cache poisoning attack. If using this method, keep in mind:

- Protocol detection requires the IDS to maintain its state information.
- A cache poisoning attack uses the Domain Name System (DNS) service, which is a two-step process.
- A protocol IDS can detect cache poisoning when a number of DNS responses occur without a DNS request.
- To effectively detect suspicious or abnormal behavior, a protocol IDS must re-implement a wide variety of application layer protocols.

Spoofing can also be used to avoid a protocol IDS. Spoofing an IP is the act of masking your identity and pretending to be another device by modifying the IP packet header and source address in order to bypass the IDS. Common spoofing targets include:

- Address Resolution Protocol (ARP)
- Domain Name Server (DNS)
- Internet Protocol (IP)
- Email addresses

Host-Based Intrusion Signs

To avoid detection when penetration testing a host-based IDS, avoid the following signs of intrusion:

- Unknown files inserted into the system
- Altered file attributes
- Unrecognized file extensions such as .ODIN, .OZD, .BUK in a Windows-based system
- Rogue suid or sgid files a Linux system
- Changes to the file or folder metadata
- Changes to the hidden status of files
- New files that do not match the existing naming scheme

Network-Based Intrusion Signs

Network intrusion signs are more focused on the network devices. These devices are going to be routers, switches, firewalls, proxy servers, and the security software and security devices that protect the network. Some intrusion signs include the following:

- Substantially increased network bandwidth. Use typical hours of peak activity to perform tests that will increase network bandwidth.
- New and/or unusual ports being used or open.
- New and/or unusual protocols and services being used.
- Connection attempts to closed ports or repeated login attempts from remote hosts.
- Unusual or unknown IP addresses or IPs outside the local network being used.
- Probes for services or systems running on the network by a remote device.
- Unknown or unexplained messages and warnings in log files.

Other Signs of System Intrusion

Other signs can appear that may indicate the presence of an intruder or a potential intrusion in progress. These signs include:

- Modifications to system software and configuration files
- Unfamiliar processes
- Decrease in system performance
- System reboots or crashes
- Noticeable changes to log files
- Incorrect permissions or ownership
- Anonymous logins
- New or unusual account names
- Changes to group membership
- Activity or logins during non-standard hours
- Discrepancies in system audit files or corrupt files
- Double file extensions
