11.1.7 IDS Penetration Testing Facts

This lesson covers the following topics:

- Signature-based detection
- Anomaly-based detection
- Protocol anomaly-based detection

Signature-based Detection

If the IDS uses signature-based detection, you should:

- Identify the scope of the signature-based IDS in view of the organization's network. Determine if there is any hardware, software, connectivity, or other mechanisms that can be exploited to bypass the IDS. Be sure to look for weaknesses in communications with remote offices, offsite locations, and wireless devices/networks.
- Determine if any exploits can be initiated or valuable information obtained through social engineering.
- Research the signatures (known threats) that the IDS has in its database.
- Determine if new threats exist and, if so, determine if the IDS has been updated to include them.
- Determine the IDS threshold for signature variance, and if possible, design an exploit that will not be detected.

Anomaly-base Detection

When penetration testing anomaly-based systems, obtain as much information as possible about the network behavior of the target. Then you should:

- Identify the scope of the anomaly-based IDS in view of the organization's network. Determine whether there are any hardware, software, or connectivity mechanisms that can be exploited to bypass the system. As with signature-based detection, look for weaknesses in communications with remote offices, offsite locations, and wireless devices/networks.
- Obtain as much information as possible about the organization's business processes, including the timing of business activity changes, employees' work hours, log file reviews, higher workload periods, backups, and scheduled system down time.
- Determine whether any exploits can be initiated or valuable information can be obtained through social engineering.
- Determine the IDS threshold for network behavior variance and, if possible, design an exploit within that variance.
- Identify activities, if any, that generate false positives. Determine if the false positives can obscure alerts triggered during penetration testing.

Protocol Anomaly-based Detection

For anomaly-based detection specific to protocols, keep the following in mind:

- Review the connectivity components of the network to expose any weaknesses in the implementation of protocols, encryption, hubs, switches, remote sites, remote servers, offsite locations, and wireless devices/networks.
- Determine if you can use any known attack types, such as:
  - Man-in-the-middle
  - DoS or DDoS
  - Cache poisoning
  - Spoofing
  - SYN flood