Lecture 10: Perimeter Security

QUESTION 1

A firewall is a component or set of components that restricts access between a protected network and other sets of networks and are often used to protect an organisation's networks from the Internet.

a. Briefly describe the operational characteristics of:
  • a simple packet filter;
  • a stateful packet filter;
  • a circuit level gateway;
  • an application gateway.
b. Briefly discuss the strengths and weaknesses of deploying:
  • a packet filter;
  • application gateway.

Answer

a. The characteristics are:
  • A packet filter examines each packet that attempts to pass through the filter. Each packet is examined independently of other packets that may be part of the same connection Packet filters examine each packet's headers and make decisions based on attributes such as:
    – Source or destination IP addresses
    – Source or destination port numbers
    – Protocol (UDP, TCP or ICMP)
    – ICMP message type
    – and which interface the packet arrived on
  • Stateful packet filters take account of the current state of a connection. Stateful packet filters are more 'intelligent' than simple packet filters. Stateful packet filters are able to recognise if a particular packet is part of an established connection by 'remembering' recent traffic history. This makes the definition of filtering rules easier to accomplish and therefore potentially more secure.
  • Application level gateway acts as a relay of application level traffic and is also known as an application proxy because the firewall needs to act on behalf of the client. ALG are usually configured to support only specific applications or specific features of an application. Each application is supported by a specific gateway.
  • A circuit level gateway is a special type of application level gateway with reduced security checking. It acts as a relay of TCP/UDP layer data rather than application data, and usually no analysis of the application layer data is performed. Connections are validated before allowing data to be exchanged. A particular packet can be identified as being part of a particular connection. There is limited additional security checking once packet has been identified.

b. Strengths and weaknesses:
  - Packet filter strengths
    – Low overhead and high throughput
    – Supports almost any application
  - Packet filter weaknesses:
    – Do not usually interpret application layer data/commands
    – may allow insecure operations to occur
    – Allows direct connection between hosts inside & outside firewall
    – Non-stateful packet filters only: less secure and more difficult to write complex rules
  - Application gateway strengths:
    – Easy logging and audit of all incoming traffic
    – Provides potential for best security through control of application layer data/commands
  - Application gateway weaknesses:
    – May require some time for vendor to write new gateways for new applications
    – Requires one more additional connection (including processing resources) for each new connection
    – Slower than packet filters

QUESTION 2

a. How can a firewall inspect TLS traffic?
b. How can a user know whether TLS traffic is being inspceted?

Answer

a. The firewall must be an application gateway with a TLS proxy. It requires the organisation to set up an internal PKI and issue internal proxy server certificates for every external TLS server that internal users will access. Each internal proxy certificate must contain the domain name of a specific external TLS server. The decryptio and the TLS gateway will be transparent to the user.
b. The user must know the difference between the external and internal root certificates used to validate the server certificate. This requires recording the characteristics/identity of each root certificate as is gets installed on the host (browser), and later use those recordings to tell certificates apart.

QUESTION 3

Intrusion detection systems (IDS) are automated systems (programs) that detect suspicious events.
a. An IDS can be either host-based or network-based. Briefly describe the operation of a host-based IDS and a network-based IDS.
b. Detection methods used by IDS are normally considered to be either misuse or anomaly-based. Briefly describe each of these detection methods.
c. Briefly discuss the strengths and weaknesses of misuse and anomaly-based IDS.
d. Briefly discuss the major operational issue associated with the deployment of an IDS.
e. Give typical reasons why many alarms can be ignored.

Answer

a. The operation principles are:
  - A host-based IDS is designed to detect intrusions only on the host it is installed on. HIDS monitors changes to host's operating system files and traffic sent to the host.
  - Network-based IDS are designed to detect intrusions on one or more network segments, and are usually deployed to protect a number of hosts. NIDS monitor network/s looking for suspicious traffic.
b. The detection methods are:
  - Misuse detection (sometimes called Signature detection) works by matching observed behaviour to known malicious behaviour. This is similar to most virus checkers.
  - Anomaly detection works by comparing observed behaviour with known good behaviour. If the behavior does not 'match', the behaviour is bad.
c. Operational issues:
  - Misuse Based IDS, Advantages:
    – Fast, only way to detect known intrusions at runtime
    – Have more True Positive results than False Positive results. Fewer false alarms
  - Misuse Based IDS, Disadvantages:
    – Cant detect new attacks that dont match existing signatures.
    – Requires manual administration. Must have signatures constantly updated
    – In DoS attacks, the IDS can be overwhelmed so that it cant function correctly.
  - Anomaly Based IDS, Advantages:
    – Can detect new attacks by identifying unusual behaviour
    – Information from anomaly based IDS can be used to develop signatures for misuse based IDS
  - Anomaly Based IDS, Disadvantages:
    – Usually generate many false positives (false alarms)
    – Usually require a lot of tuning to develop models of normal behaviour
d. Advantages and disadvantages. A major problem with IDS in general is the number of false positive alarms they generate Can lead to a sense of mistrust, then apathy by security administrator.
e. Detected attacks might attempt exploits that have been patched or which do not apply to the targeted system.

QUESTION 4

The so-called base rate fallacy is a common reason for false alarms in IDS.
a. What is meant by the base-rate fallacy?
b. In which other disciplines (other than information security) is the base-rate fallacy common?
c. What can be done to avoid the base-rate fallacy?

Answer

a. The base-rate fallacy means that the base rate of an event is ignored in the calculation of the probability of that event. More precisely, assume that the analyst needs to determine the probability of an event r based on knowing the probability of s, but that the analyst only knows the probability of s and the conditional probability $p(s|r)$. In order to derive $p(r|s)$, the base rate of r is needed. If the analyst doesn't take the base rate of s into account, he might make the approximation $p(r|s) = p(s|r)$. In case the base rate of is very low, this approximation is totally wrong.
b. The base rate fallacy is common in medical diagnostic and legal reasoning
c. The base-rate fallacy can be avoided by correctly applying the statistical and mathematical models to derive the probability of events.

QUESTION 5

a. What do the abbreviations BSS, ESS and DS mean in relation to IEEE 802.11 WLAN? Briefly describe each concept and how they are related.
b. List and briefly describe the 5 IEEE 802.11i phases of operation.

Answer

a. BSS: Basic service set; ESS: Extended Service Set; DS: Distributed System. The BSS is the smallest configuration of a WLAN, typically consisting of one AP (Access Point) and a dynamic set of mobile stations. ESS is two or more BSS that are interconnected via a DS.

b. **Discovery:** An AP uses messages called Beacons and Probe Responses to advertise its IEEE 802.11i security policy. The STA uses these to identify an AP for a WLAN with which it wishes to communicate. The STA associates with the AP, which it uses to select the cipher suite and authentication mechanism when the Beacons and Probe Responses present a choice. **Authentication**: During this phase, the STA and AS prove their identities to each other. The AP blocks non-authentication traffic between the STA and AS until the authentication transaction is successful. The AP does not participate in the authentication transaction other than forwarding traffic between the STA and AS. **Key generation and distribution**: The AP and the STA perform several operations that cause cryptographic keys to be generated and placed on the AP and the STA. Frames are exchanged between the AP and STA only **Protected data transfer**: Frames are exchanged between the STA and the end station through the AP. As denoted by the shading and the encryption module icon, secure data transfer occurs between the STA and the AP only; security is not provided end-to-end. **Connection termination**: The AP and STA exchange frames. During this phase, the secure connection is torn down and the connection is restored to the original state.