University of Oslo
INF3510 Information Security
Spring 2018
Workshop Questions and Answers

Lecture 11: Network 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 proxy;
   - an application layer proxy.

b. Briefly discuss the strengths and weaknesses of deploying:
   - a packet filter;
   - application layer proxy.

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.
   - A circuit level proxy acts as a relay of TCP/UDP layer data and does not inspect application data. Connections are validated before allowing data to be exchanged. A particular packet can be identified as being part of a particular connection. Through the proxy it can hide details of the internal network, e.g. through Ipv4 NAT (Network Address Translation).
   - An application layer proxy 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 separate proxy application, e.g. for http, smtp, ftp, ssh, etc. It can inspect the application data at any level of detail.

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 proxy strengths:
     – Easy logging and audit of all incoming traffic
     – Provides potential for best security through detailed inspection of application layer data/commands
   - Application proxy 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 inspected?

Answer

a. This is called TLS/SSL stripping. The firewall must be an application proxy with a TLS/SSL proxy module. It requires the organisation to set up an internal proxy PKI and install the proxy root certificate on every internal host. Whenever an internal host requests access to an external TLS server, then the proxy generates in real-time a proxy server certificate signed by the proxy root private key. To do this the proxy establishes a TLS connection to the external server, which includes receiving the external server certificate. The proxy copies attributes from the external server certificate when generating the proxy server certificate, such as the unique name (domain name) of the genuine external server certificate. However, the public key is necessarily different. The proxy sends the new proxy server certificate to the internal host to establish an internal TLS connection. This creates a cleartext gap at the proxy where all the traffic data can be read an inspected. The cleartext gap is transparent to the user, so he/she might wrongly think the TLS connection is end-to-end between internal host and the external server.
b. The user must know the difference between the external PKI root and internal proxy root certificates used to validate the received server certificate. Both root certificates are stored on the host. Since the proxy can copy every attribute from the genuine external root certificate to the proxy root certificate, except for the public key, only the public key itself can be used to identify the root with high certainty. So even if the unique name of the proxy root says “verisign.com” it is not necessarily “verisign.com”. The company running the proxy server decides what to fill in the various attributes of the proxy root certificate, as well as the proxy server certificates. So, if the user does not want to rely on any of the certificate attributes, she must be able to distinguish between the genuine external root certificate and the proxy root certificate by their public keys only. Each key is approximately 2000 bits long, which is a few lines of HEX digits. The user can inspect the signature path from the server certificate to the root certificate. The root certificate at the top of the certification path indicates whether the received server certificate is the genuine external server certificate, or the internal proxy server certificate.

Question 3

Intrusion detection systems (IDS) are automated systems (programs) that can detect suspicious activity.

a. An IDS can be either host-based or network-based. Briefly describe the operation of a host-based IDS, and of a network-based IDS.
b. Detection methods used by IDS are normally considered to be either misuse-based or anomaly-based. Briefly describe each of these detection methods.
c. Briefly discuss the strengths and weaknesses of misuse-based 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 known 'good' behavior, then the behaviour is considered 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 resulting in malfunction.
   - 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 a suspicious event or avtivity is ignored in the calculation of the probability of that event. More precisely, assume that the analyst needs to determine the conditional probability p(r|s), i.e. the probability of intrusion event r based on observing signature s, but that the analyst only knows the conditional probability p(s|r). In order to derive p(r|s), the base rate of r, denoted a(r) is needed. If the analyst doesn't take the base rate of r into account, he might make the approximation $p(r|s) \approx 1$. In case the base rate of r 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 for deriving the conditional 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. A 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 BSSs interconnected via a DS.
b. The 5 phases defined by IEEE 802.11i are:
    1. **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.
    2. **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.
    3. **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. After successful key installation, AP opens (connects) the controlled port, which gives STA access to the local network.
    4. **Protected data transfer**: Frames are exchanged between the STA and the destination host through the AP. Encrypted data transfer occurs between STA and AP only; security is not provided end-to-end.
    5. **Connection termination**: AP and STA exchange frames to express intention to end the wireless access. During this phase, the secure connection is torn down and the AP closes (disconnects) the controlled port.