Example of essay on software security assessment

Law, Security

Network Protocols

A network protocol is a set of rules that manage the communication between two or more computers within a given network. This set of rules determine given characteristics of a given network, such as allowed physical topologies, access method, speed of data transfer and types of cabling.

Common network protocols include:

- FDDI
- Token Ring
- Ethernet
- ATM (Asynchronous Transfer Mode)
- Telnet (Telephone Network)
- SSL (Secure Socket Layer)
- FTP*SMTP (Simple Mail Transfer Protocol)
- SFTP (Secure File Transfer Protocol)
- HTTP (Hyper Text Transfer Protocol)
- HTTPS (Secure Hyper Text Transfer Protocol)
- SSH (Secure Shell)
- NTP (Network Time Protocol)
- E6 (Ethernet Globalization Protocols)
- POP (Post Office Protocol)

Internet Protocol (IP)

For the internet protocol suite, the internet protocol (IP) is the primary communications protocol. It relays datagrams through network boundaries. It enables internetworking through the routing function, it foundationally

creates the internet. There exist four different types of layers within the Internet Protocol Suite, namely;

Application Layer

Application layers include the following:

- IMAP
- LDAP
- IRC
- MGCP
- BGP
- NNTP
- DHCP
- DHCPv6
- FTP
- DNS
- HTTP
- POP
- SNMP
- SMTP
- SOCKS
- RTP
- RTSP
- SIP
- RIP
- RPC

Transport Layer

Transport layers include the following:

- UDP

- SCTP

- TCP

- DCCP

- RSVP

Internet Layer

Internet layers include the following:

- ICMP

- ICMPv6

- ECN

- IP (IPv4. IPv6)

- IPsec

- IGMP

Link Layer

Link layers include the following:

- Tunnels (L2TP)

- NDP

- ARP/InARP

- OSPF

- Media Access Control (Ethernet. ISDN. DSL. FDDI)

- PPP

User Datagram Protocol

The UDP (User Datagram Protocol) belongs to the Internet network protocols set, it is one of the major members of the Internet Protocol Suite. This network protocol allows computers to send and receive messages in the form of datagrams to single or multiple hosts on an IP (Internet Protocol) network devoid of special transmission data paths or channels set up through prior communications.

- UDP has specific qualities that make it particularly suitable for given applications. These qualities include;

- Datagrams: It avails datagrams which are appropriate for the forming of other protocols, for example, Remote Procedure Call, the Network File System and IP Tunnelling.

- Transaction-Oriented: It is oriented for transactions, this makes it particularly fit for simple query-response protocols, for example, Network Time Protocol and the Domain Name System.

- Stateless: this makes it particularly favourable for a large number of clients as in the case of media streaming like IPTV

- Simple: makes it suitable for processes without a full protocol stack such as bootstrapping like Trivial File Transfer Protocol and DHCP

- Unidirectional: making it suitable for broadcast information.

- No Retransmission Delays: this makes it appropriate for real-time applications.

There are 4 fields that are involved in a UDP datagram header. These fields are 2-bytes each, namely:

- Destination Port Number
- Checksum
- Datagram Size
- Source Port Number

Transmission Control Protocol

TCP (Transmission Control Protocol) belongs to the Internet network protocols set, it is also one of the major members of the Internet Protocol Suite. This protocol offers an error-checked, ordered and reliable delivery of a torrent of octets between programs that are operational in computers within a LAN, intranet or public internet. The TCP exists at the transport layer. Throughout the TCP lifetime, the local end-point goes through a sequence of changes of state, namely;

- Listen
- Syn-Sent
- Syn-Received
- Established
- Fin-Wait-1
- Fin-Wait-2
- Close-Wait
- Closing
- Last-Ack
- Time-Wait
- Closed

Firewall

This is a hardware or software based network security system. A firewall is designed to control the data coming in and out of a given b= network by analysing and determining whether the given data packets should be authorized traffic flow founded on a given set of rules.

The stateful firewall keeps track of the state of network connections. This is common in UDP communications and TCP streams. This firewall executes a stateful packet inspection (SPI).

The stateless firewall needs less memory as compared to the stateless firewall. This is because it is much faster for modest filters. They are used in filtering of stateless network protocols as such protocols have no notion of a session.

Simple Stateful Firewall

The simple stateful firewall is configured and designed to identify the events below as anomalies. It the transfers them to the IDS software where they are processed.

IP address anomalies:

- Land attack (source IP equals destination IP).
- IP packet source is a broadcast or multicast.
- IP fragment overlap.
- IP fragmentation anomalies:
- IP packet length is more than 64 kilobytes (KB).
- Tiny fragment attack.

- IP fragment missed.

- IP fragment length error.

IP anomalies:

- IP version is not correct.

- IP header length is set larger than the entire packet.

- Packet has incorrect IP options.

- Time-to-live (TTL) equals 0.

- IP total length field is shorter than header length.

- IP header length field is too small.

- Internet Control Message Protocol (ICMP) packet length error.

- Bad header checksum.

TCP anomalies:

- TCP sequence number 0 and flags 0.

- TCP port 0.

- Bad TCP checksum.

- TCP flags with wrong combination (TCP FIN/RST or SYN/ (URG| FIN| RST).

- TCP sequence number 0 and FIN/PSH/RST flags set.

Anomalies found through stateful TCP or UDP checks:

- SYN followed by RST packets.

- Non-SYN first flow packet.

- SYN followed by SYN-ACK packets without ACK from initiator.

- ICMP unreachable errors for SYN packets.

- SYN without SYN-ACK.

- ICMP unreachable errors for UDP packets.

UDP anomalies:

- UDP header length check failed.

- UDP source or destination port 0.

- Bad UDP checksum.

Packets dropped according to stateful firewall rules.

References

Allen, J. H. (2008). Software security engineering: A guide for project managers. Upper Saddle River: Addison-Wesley.

McGraw, G. (2006). Software security: Building security in. Upper Saddle River: Addison-Wesley.

Vranken, H. E. (2012). Software security: Reader. (Software security.). Heerlen: Open Universiteit Nederland, Faculteit Informatica.

Wysopal, C. (2007). The art of software security testing: Identifying software security flaws. Upper Saddle River: Addison-Wesley.