Research
Week 09
CIT 288

Chaz Davis

BCTC
Spring 2020

March 6, 2020

Part 1: Chapter 09

i) Where would an application-level gateway exist physically in the network? Specifically - outside the firewall? Inside? Investigate. It appears that application level gateways exist to be entered vi telnet or ftp. Once you've gained access to the network. you can then specify the applications to gain access to within the host network, or the computer/server that you would like to access.

As for where in the network they exist, there are several configurations. The first version of the gateway-level application setup has it setup on the outside of the main firewall and router. The second configuration has a setup inside the main firewall but in front of the main router. The third and preferred variation has one inside the firewall and infront of the router, and one outside the firewall, with this configuration, you can add additional gateways in front of any subnet routers to protect access within those internal networks as well.

ii) What is the difference in a ALG and a CLG gateway?

APG is more secure than circuit-level, ALG uses a unique program for each applications, and CLG uses TCP connections, with know packet-filtering, ALG is good for authentication and logging, and CLG grants access by port address. ALG in not always transparent to users, CLG has no application level checking, ALG is used for email, ftp, telnet, www. CLG can understand what is carried in the packet.

iii) What is a SOCKS server?

It is a general purpose proxy server that establishes a TCP connection to another server on behalf of a client, then routes all the traffic back and forth between the client and server. It works for any kind of network protocol on any port. SOCKS V5 adds additional support for security and UDP.

iv) What is a DMZ network and what types of systems would you expect to find on such networks?

A DMZ network functions as asubnetwork containing an organization's exposed, outward-facing services. It acts as the exposed point to an untrusted network, comonly the Internet.

You would see it commonly used with web servers, mail servers, and ftp servers.

v) How does an IPS differ from a firewall?

An IPS, or intrusion prevention system, works with the firewall. It typically sits between the outside world and the firewall. IPS proactively denies nework traffic based on a security profile. If that packet represents a known security threat.

vi) How can an IPS attempt to block malicious activity?

It uses the security profile configured by the sys-admin or cyber security liason.

vii) What information is used by a typical packet filtering firewall?

- Source IP Address the IP Address of the system that originated the IP packet.

- Destination IP Address The IP Address of the system the IP packet is trying to reach,
- Source and destination Transport-Level Address The transport level (eg. TCP or UDP) port number, which defines applications such as SNMP or TELNET.
- IP Protocol field Defines the transport protocol
- Interface For a router with three or more ports, which interface of the router the packet came from or which interface of the router the packet is destined for.

viii) What are some weaknesses of a packet filtering firewall?

- They can be complex to configure
- They cannot prevent application-layer attacks
- They are susceptible to certain types of TCP/IP protocol attacks
- The don not support user authentication of connections
- the have limited logging capabilities

ix) What are the common characteristics of a bastion host?

- The bastion host hardware platform executes a secure os
- Only the services that the network admin considers esential are installed on the bastion host
- The bastion host may req. authentication before a user is allowed access to the proxy services
- Each proxy is configured to allow access to only soecific host systems
- Each proxy logs all traffic, each connection and its duration
- Each proxy is independent of the other proxies on the bastion host and runs in a private secured directory

x) Why is it useful to have host-based firewalls?
A host-based firewall is a software module used to secure an individual host.

- Filtering rules can be tailored to the host environment
- Protection is provided independent of topology
- Provides an additional layer of protection