A firewall is software which protects networked machines from malicious intrusion that could breach the confidentiality or data corruption. The program runs on a secure host computer and performs the basic function of inspecting packets to check if they match the criteria required to pass through to the protected network.

Firewalling protects the IDS and IPS from outside attacks such as worms, viruses, Trojan horses and so on. The firewall basically filters proxy data in a network and controls the traffic. However the chief limitation of a firewall is that it cannot secure against tunneling malicious packets over HTTP, SMTP and other protocols attempts, also applications that are secure can be "trojaned".

An intrusion detection system (IDS) in-turn inspects all incoming and outgoing network packets to identify suspicious activity that may be a possible network or system attack. An IDS software is more than a firewall since detects several types of malicious activities already in the system and alerts the users on any compromise in security. An IDS system is normally composed of three components; a sensor which sniffs packets off the network, a console which monitors events and alerts and controls the sensors and an engine that records events logged by the sensors in a database and uses a system of rules to engage alerts from the security events received.

Although they both operate towards network security, an IDS differs from a firewall in that a firewall detects malware in order to stop them from intruding however an IDS looks out for suspected intrusion and signals an alarm. An IDS also secures the system from internal attacks.

On the other hand A IPS, or intrusion prevention system is also used in computer security to provide system guidelines and policies for network traffic management along with an intrusion detection system for alerting system users to suspicious malware. However the IPS allows the user to provide the action upon being alerted. The IPS is designed to basically detect malicious data packets, stop intrusions and block malicious traffic automatically prior to any attacks taking place. Advanced IPS systems also prevent TCP sequencing issues, correct CRCs and unfragment packet streams

An IPS differs from an IDS system because aggressive and capable of responding in real time. It blocks any malicious activities before the overall network security can be compromised and subsequently sends out an alarm, drops the packet, resets the connection and blocks traffic from the source IP for some time.

What ways does snort resemble wireshark? Go on to explain how they differ.

Wireshark is an open source network protocol analyzer applicable in both Unix and Windows. It allows a user to look at data from a live network or from a capture file on disk

right into the level of the packet detail. Wireshark boasts a rich display filter language and the ability to view the reconstructed stream of a TCP session. It also supports hundreds of protocols and media types.

Snort is also an open source, real time network intrusion and protocol detection an traffic analyzer. It detects worms, port scams and suspicious behavior using a flexible rule-based language to describe traffic that should be collected or passed together with a modular detection engine.

They differ in that Snort is lightweight compared to wireshark and that it applies NIDS system to perform protocol analysis, content searching, and content matching. It can also be used to detect attacks in the OS fingerprinting attempts, common gateway interface, buffer overflows, server message block probes, and stealth port scans. Also wireshark has come under attack from remotely exploitable security holes.

Which is better - NIDS or HIDS? Justify your answer.

Both Host intrusion detection systems (HIDS) and network intrusion detection systems (NIDS) are tools used in security management for computers systems or networks. Basically in HIDS approach, anti-threat software is installed in every computer in the network that contains two-way access to volatile environment such as the Web. In NIDS, these anti-threat applications are installed only at strategic points such as servers that interface the unsafe environment and the network entity that is being protected.

Personally I think Host intrusion detection systems are very aggressive and versatile compared to NIDS since they pose a security check on all host machines. HIDS is applied on all types of machines within the protected network namely servers and workstations.Â Doing so provides an edge that NIDS does not have especially if the system has a segment that NIDS cannot reach beyond. Under HIDS Usually, Traffic conveyed to the host is scanned and forwarded onto the host if there are no potentially malicious packets within the data transmission.

HIDS also tends to protect the local machines more as compared to the NIDS.Â NIDS focuses more on the integrity of network which may be breached anytime from the exposure to malicious ware via any local machine. HIDS is also more platform specific meaning it performs strongly in the more common user friendly windows operating systems.Â

NIDS usage also gives rise a major hitch on switched networks when port spanning is not enabled.Â A switch functions on a high speed direct access principle only transmitting packets directly to the intended recipient of the packet and not the entire network like the legacy hub based networks. (Vijay 2006)Â Most security networks do not support port spanning in this scenario and therefore is recommended that sensors, be administered on

the sections that the spanning tree cannot be enabled on. In this way HIDS is much better than NIDS as it is host based.

List and explain the main features of a proxy server.

A proxy server is a computer that allows different users to access the internet at the same time on a single Internet connection. It intercepts requests from clients to the server in an organization where multiple users often download similar contents from the internet and provides caching thereby reducing access time and bandwidth requirements.

The main features of a proxy server are:

Caching: This happens when a user requests for a file. The proxy first browses its cache and forwards it if present; otherwise it forwards the request to the web server.

Connection sharing: Proxies facilitate users to share the internet connection by configuring them to access the web through it instead of providing a direct link to each user.

Filtering: Since the proxy servers handle all the users requests, it can therefore be used to restrict certain URLs.

Security: The proxy server assists in security by hiding the IP address of the users.

Scanning traffic: Sometimes proxies integrate with open source anti-virus software to scan the network traffic for viruses and worms.

Bandwidth Control: The proxies use delay pools to control bandwidth by allocating specific bandwidth to internet traffic. This helps prioritise traffic thus reducing the network overload.

What is a reverse proxy server?

A reverse proxy server is a server similar to a normal proxy server but it is located at the edge of the fire wall. This reverse proxy has its own external IP address on the external NIC and usually links it to one of the internal IP addresses. Reverse proxy's main aim is to shield the public users from directly accessing the web server by only accessing the reverse proxy server. The reverse Proxy server actually Places HTTP data on the network and forwards it to the users web server. The internal firewall is configured in such a way that the HTTPS data will be forwarded through the internal firewall only if it is sent from the reverse proxy server. The web server then accepts the request, processes it and sends a response back to the reverse proxy server which in turn sends the requested date back to the originating client. This setup prevents public users from contacting the web server directly for security reasons.