**CS 5601 Exam 3 Modules 13 through 15**

**Adam Hoffmeister**

1. **Describe at least two ways as to how to reduce the impact against a SYN Flood attack.**

Shorter timeouts on ACK responses and SYN cookies can be set to close the states quicker. Additionally, load balancing can be implemented to distribute connections evenly. This would allow more connections in total.

1. **Why, on today’s high speed Internet connections would a TCP Sequence Prediction attack be very difficult to accomplish from an external attacker that can only observe the traffic stream, that is, does not have an inline attack avenue?**

A TCP Sequence Prediction attack would be difficult to accomplish because you need to inject the correct TCP packet at the perfect time, right before the client gets it. This gets increasingly difficult the faster network connection the client has. Being external is difficult because intercepting the packet would be difficult with network latency. If they are too slow, the packet will be invalidated and the injection will fail.

1. **We discussed how ICMP Echo can be beneficial for determining if a device is reachable. Why would we want to block inbound ICMP Echo packets from our network (several answers possible. Choose one)?**

One reason ICMP Echo packets are blocked from networks is to prevent flood attacks. Thousands of packets can be sent from thousands of hosts, creating a denial of service attack.

1. **Why should all system event logs be sent to a central location?**

System event logs need to be securely protected. If the system is compromised, the attacker could edit the logs on the system. This would ruin the entire purpose of keeping the log.

1. **Your procurement manager, being helpful, has discovered a place where he can purchase a number of 100mbit network hubs. As the security officer, what are you going to tell him in regards to this purchase?**

Network hubs aren’t popular anymore due to their cons; I would tell him no and recommend switches.

1. **A vendor is pressing you to purchase a VPN appliance that supports SSL protocols only. It’s very reasonable compared to other VPN solutions which supports multiple protocols costing significantly more. Your environment must support multiple types of devices including smart phones and tablets. Is this a good solution for your organization? Explain your answer.**

This is a good solution for the organization. VPN solutions that have SSL tend to be more expensive, so a low-cost solution is optimal as there are benefits that come with switching. There shouldn’t be any issues using SSL for all devices, as they support it.

1. **Your organization has managed network devices (switches, routers, etc.) using public IP addresses to manage the devices along with all other systems. Why is this a bad design and how would you fix it?**

Using public IP addresses for private devices would allow them to be seen externally, opening the potential for attacks. The attacks could range from DoS or vulnerabilities.

This can be fixed by moving the network devices to a private IP subnet. If they are out of address space, they could implement a NAT firewall to translate private addresses into public addresses.

1. **Your organization has decided to deploy wireless access points in your building. A manager suggests that lots of money could be saved if they purchased inexpensive, older wireless units that support only 64/128 bit WEP. As the security officer for your organization what should your response be (good idea or bad idea and why)?**

WEP is not secure enough as the cryptography algorithm wasn’t implemented correctly. Once the key is obtained, all the traffic is available. I would recommend 802.1X, WPA, or WPA2 because of this.

1. **Why should an organization audit VPN authentication, authorization, account logs closely?**

VPNs allows employees remote access to the internal network of a company. If the employee’s personal machine was comprised, this could jeopardize portions of the company. An attacker could use their details to perform an exploit, transfer large amounts of data, etc.

1. **A good security design for remote access into the server requires system administrators to go through additional access gateways before access the data center servers. Why is this necessary?**

Multiple access gateways are used as multiple safe guards. One of the gateways could have a vulnerability that allows unauthorized users in; or the credentials for the gateway could be compromised. This is necessary to prevent attackers from getting in.

1. **As the security officer, you have advised your organization that you want to have 802.1x support per switch port. What are some arguments you could use to back this up?**

The IEEE 802.1x standard supports users authenticating prior to granting them access to the authorization server. This is an extra gateway that would secure the company from attackers.

Additionally, multiple methods of authentication are supported. So, one-time passwords, public keys, and smart cards could also be transmitted.

1. **If you were an attacker inside a network and find the network has non-managed switches, but did not have access to the wiring closet, how could you attack the network in such a way as to cause the switches to send you all traffic running through the switch?**

The MAC table can be overflowed which will force the switch to repeat traffic to all ports.

1. **Why should you control ICMP traffic from the Internet into your network (give at least 2 examples)?**

ICMP traffic is prone to a lot of different attacks. If the traffic isn’t controlled, they could ICMP Echo all the hosts (ping sweep) to find all available devices. Alternatively, they could send an ICMP reply packet before an open state. This would allow them to reverse map the network.

1. **Describe what a layer 7 firewall is and how it functions (10 pts)**

A layer 7 firewall is an application firewall. It controls I/O and access to a service. Packets are not allowed to traverse the firewall, but data flows up to the application that decides what to do with it. Connections are blocked if they don’t meet the configured policies.

1. **You need to extend a network connection to another office on the other side of town and you have lots of bandwidth through the Internet from both locations. Describe a way to securely connect the two networks so people in both buildings can see each other on the network without doing anything to connect their workstations to the other servers. (10 pts)**

An IPsec tunnel could be used to securely communicate between the two locations. This would provide an authenticated, encrypted tunnel. Since it is done between servers or routers, the employees will not have to do anything to their workstations.

1. **All of the devices listed below are all on the same network of behind one router and firewall. As the security officer describe how you would want the network redesigned (15 pts). You may assume everything is already behind a NAT already.**

The firewall should be equipped with packet filters, ACLs, application layers proxies, and network interface weighting. Wireless access points need to have 802.1x encryption. The VPNs should all use SSL and encrypt all traffic. Intrusion detection systems need to be deployed on all network-based and host-based systems. The IDS can be deployed between the firewall and router (where needed). The logs should be cent to an external central server.

The public webserver, web application server, DNS, and DHCP need to be placed in the DMZ with a static NAT. This is because they are accessed from the outside. Everything else should be placed behind the firewall, including the database server, financial server, routers, and switches. The financial server should only be accessed internally as the employees should only be modifying it during their day job. The database server should be bound to localhost only, only allowing connections by tunnel. Newer switches will be needed for DHCP guarding. A VPN or IPsec tunnel can be used to allow external employees the ability to maintain the public servers.

Internet <-> Outer Firewall <-> Web/Public servers (DMZ) <-> Firewall (With NAT) <-> Router:

-> Switch A <-> Machines, printers, VoIP, etc.

-> Switch B <-> IDS server <-> Financial/database server