CSc 4222/6222 – Assignment #4
Solutions

1. Jill lives in a large apartment complex and has a Wi-Fi access point that she keeps in her apartment. She likes her neighbors, so she doesn't put any password on her Wi0Fi and lets any of her neighbors use her Wi-Fi from their nearby apartments if they want to access the Internet. What kinds of security risks is Jill setting herself up for?

Solution: Jill is setting herself up for multiple problems. The neighbor could easily spoof Jill's IP address and it would appear as if a malicious transmission came from her. Any personal, confidential files on her network would be accessible by her neighbors. Also, if any of the neighbors downloaded or transmitted any illegal files, Jill would be responsible.

2. How many bytes are devoted to header and footer information (with respect to all layers of the IP protocol stack) of an Ethernet frame that contains a TCP packet inside it?

Solution: Ethernet frame for the link layer has 22 bytes for the header and 4 bytes for the checksum field in the footer. The network layer needs 20 bytes for the IPv4 packet and the transport layer needs 20 bytes for the TCP packet header. The total number of bytes needed for header and footer information is 66 bytes.

3. Suppose you suspect that your session with a server has been intercepted in a man-in-the-middle attack. You have a key, K, that you think you share with the server, but you might be only sharing it with an attacker. But the server also has a public key, K_p, which is widely known, and a private secret key, K_s, that goes with it. Describe how you can either confirm you share K with the server or discover that you share it only with a man-in-the-middle. Also, be sure your solution will not be discovered by a packet sniffer.

Solution: Ask the server to digitally sign your shared key, K, using his private key, K_S, and encrypt the result with K, so no one with a packet sniffer can read this. Then ask the server to send you the result. You can decrypt the package with K and verify the server's signature using his public key, K_P. If this was done correctly, you can verify everything. If you have a man-in-the middle, however, the message you get will either be garbled, or the signed shared key will not be the same.

4. You are the system administrator for a provider that owns a large network (e.g., at least 64,000 IP addresses). Show how you can use SYN cookies to perform a DOS attack on a web server. Show how to defend against this DOS attack.

Solution: The rogue administrator initiates a large number of TCP connections to the web server spoofing source IP addresses from his network. Also, he intercepts the SYN-ACK responses from the server and sends back spoofed ACKs to complete the handshakes for these connections. The web server has now created a large number of sessions that will remain open, using up resources, until they time out. This attack works even if the web server uses SYN cookies.

5. Suppose the transaction ID for DNS queries can take values from 1 to 65,536 and is randomly chosen for each DNS request. If an attacker sends 1,024 false replies per request, how many requests should he trigger to compromise the DNS cache of the victim with probability 99%?

Solution: The attacker has roughly a 1/64 chance of success with each request. That is, he has a failure rate of roughly 63/64. Thus, the probability of failing in k requests is roughly $(63/64)^k$. Therefore, he needs k to be large enough so that

$$(63/64)^k > 1/100.$$

That is,

$$(64/63)^k > 100,$$

Which implies that

$$k > \ln 100 / \ln(63/63) \approx 292.$$

6. Suppose DNS IDs were extended from 16 bits to 32 bits. Based on a birthday paradox analysis, how many DNS request and equal number of fake responses would an attacker need to make in order to get a 50% chance of succeeding in a DNS cache poisoning attack?

Solution: An attacker issuing a fake response will guess a transaction ID equal to one of n different 32-bit real IDs with probability $n/2^{32}$; hence she would fail to match one with probability $1 - n/2^{32}$. Thus, an attacker issuing n fake responses will fail to guess a transaction ID equal to one of n different 32-bit real IDs with probability

$$\left(1 - \frac{n}{2^{32}}\right)^n$$

By issuing at least 54580 DNS requests and an equal number of random fake responses, an attacker will have roughly at least a 50% chance that one of her random responses will match a real request.

7. During a *FIN scan*, a FIN packet is sent to each port of the target. If there is no response, then the port is open, but if an RST packet is sent in response, the port is closed. The success of this type of scan depends on the target operating systems – many OSs, including Windows, have changed the default behavior of their TCP/IP stacks to prevent this type of scan. How? Also, how could an intrusion detection system be configured to detect a FIN scan?

Solution: Windows sends a RST packet in response to any malformed or out of sync TCP packet. This will prevent an attacker from being able to distinguish between open and closed ports. An IDS can identify all out of sync and malformed packets by analyzing the headers. If it determines a packet is bad, it would signal an alert that an intruder is trying to perform a FIN scan.

Undergrads – answer any 3 of the following questions. Grads – answer all 5 of the following questions.

8. In the three-way handshake that initiates a TCP connections, if the SYN request has sequence number 156955003 and the SYN-ACK reply has sequence number 883790339, what are the sequence and acknowledgment numbers for the ACK response?

Solution: Sequence number = 156955004
Acknowledgement number = 883790340

9. Either party in an established TCP session is allowed to instantly kill their session just by sending a packet that has the reset bit, RST, set to 1. After receiving such a packet, all other packets for this session are discarded and no further packets for this session are acknowledged. Explain how

to use this fact in a way that allows a third party to kill an existing TCP connection between two others. This attack is called a *TCP reset attack.* Include both the case where the third party can sniff packets from the existing TCP connection and the case where he cannot.

Solution: An attacker would send a packet that contains the next sequence number, set the RST bit to 1 and he will need to spoof the IP source address. This will end the connection. If the attacker is not able to sniff the packets, he will not be able to guess the sequence number correctly and will not able to implement this attack.

10. Describe a firewall rule that can prevent IP spoofing on outgoing packets from its internal network.

Solution: One option is to prevent IP spoofing is for the firewall to check the source IP address of all outgoing packets. If the source address does not belong to the network, this packet will be dropped.

11. Explain why a large value for the TTL (time-to-live) of replies to DNS queries does not prevent a DNS cache poisoning attack.

Solution: Since DNS servers cache any entries they come across, they will be holding on to any possible poisoned entries for a longer period of time. Then, if they are queried in the future for the name resolution, if they still hold the entry, they will pass along this response, rather than check in with the authoritative name server.

12. Describe the types of rules that would be needed for a rule-based intrusion detection system to detect a smurf attack.

Solution: An IDS can be configured to block any incoming packets that had the broadcast address for the destination IP address. Or it can also monitor the outgoing messages and check the destination addresses of all the packets. In case a large number of packets are all destined for the same IP address, then it can block any other such packets from leaving the network.