Communication Vulnerabilities

Welcome back. In this video, we're going to take a look at some of the vulnerabilities that can happen within communication in a network. First up is packet sniffing. This is where an attacker can view information that is sent through a network. A packet sniffer is a program which monitors and logs all network traffic over the network they're on, not just the packets for their nodes.

Once the packet data has been captured, it needs to be analysed by the software and presented in a user-readable format. If you think about the web and the kind of information which is sent, such as e-commerce, passwords, financial information, and so forth, if this information is unencrypted, then the attacker can potentially access all of that information.

However, by default, that only works for one or either a hub or a switch. Which one do you think it is? Well, the answer is hub. This is because a hub sends all the packets to all the hosts on a network. Switches send packets to the correct nodes.

However, some switches can reduce themselves to hubs, and hence, become susceptible to sniffing. There are software programs available which can overload switches' internal tables, which relate connections to nodes. And hence, switches get into a mode called promiscuous mode, and they will act like hubs, sending all of their packets to all of the nodes on the network.

One important thing to note is that what we commonly call a router these days is actually a combination of multiple things, such as the router, modem, a switch, and a wireless access point. A network traffic analyser which is freely available is called Wireshark. As with port scanning, there are legitimate uses of this kind of software--

so for example, to identify a denial of service, to troubleshoot firewall problems, such as looking at communication from a node which isn't passed to another node when you would expect it to be. You can examine the details of traffic at a variety of levels using the software, ranging from connection-level information to the actual bits comprising a single packet.

Here is a screenshot from Wireshark, and you can see that the destination, IP address, username, and password are all sent in clear text, or in the clear. And this means that this information could potentially be used for an attack. Packet sniffing is what we call a passive attack.

It allows the attacker to read information which wouldn't normally pass through their computer. However, what if the switch wouldn't overload so the packets aren't getting passed to the attacker? One solution is to trick the victim's computer to connect with the attacker node rather than the actual destination. The attacker then opens a connection with the real destination and can pass the communication on between them in both directions.

This is called a man-in-the-middle attack. The attacker can just view the information that's been sent and resend it on, or the attacker can modify what is sent. So how does the attacker do this? The attacker can do this through something called spoofing. And spoofing is where you are pretending to be someone else, so for example, the destination server. One of the two common ways of achieving this is ARP spoofing or DNS spoofing. So on a local area network using address resolution protocol, ARP, this is used to map an IP address to a MAC address. You can change the mapping, and then the attacker's MAC is associated with the legitimate IP address of a node on that network. The attacker will then receive any data which is intended for the IP. But this, remember, works only on LANs using ARP.

The attacker opens an ARP spoofing tool and sets the tool IP address to match the IP subnet of a target. Examples of popular ARP spoofing software includes ARP Spoof, Cain and Abel, and Ettercap. The attacker uses the ARP spoofing tool to scan for the IP and MAC addresses of hosts in the target subnet. And the attacker then chooses its target and begins sending ARP packets across the LAN that contain the MAC address of the attacker and the target's IP address. As our hosts on the LAN cache the spoofed ARP packets, data that those hosts send to the victim will go to the attacker instead. From there, the attacker can then steal data or launch a more sophisticated follow-up attack.

On the internet, DNS protocol is used. So recall that when you type in a URL, the request goes to a domain name server, and this has a big list of URLs and corresponding IP addresses. If it finds the IP address, it will send it back to you. Otherwise, it asks another domain name server. In this approach, the attacker injects false domain name server replies, which map destination domains to the attacker's IP address. So the attacker then sends a response with their own IP address as an answer to a DNS query.

Another type of attack in networking with respect to communication is called a replay attack. In this attack, the attacker replays a stream of communication to one of the parties at a later time. So for example, if I was the attacker and I had monitored the transfer of the username and password to the legitimate server and I copied these packets, I could then potentially replay these at a later time.

So even if it is encrypted or hashed, it doesn't matter because the packet is still going to be the same. So say Alice wants to sign into myrecipes.com, who asks for a username and password. Alice sends this, but the man-in the-middle manages to get that information. The attacker can then replay this by sending the authentication packets to myrecipes.com.

Well, that's it for this video. We've had a look at packet sniffing, spoofing, and replay attacks. I hope you've enjoyed video, and I'll see you next time.