Lesson Plan 4 | Form 2 | LAN Chatting with Netcat and Wireshark

Objective

Students will chat with each other over the local lab network using the **nc** program. They will understand how their messages are transmitted over the network, and how they can be visualized using Wireshark.

Warm-up

None.

Presentation (requires local wireless network)

Have the central computer or gateway run Wireshark and show the students its general interface and how it can be used to capture and display messages being sent across the network. Point out different protocols, open various packets to point out familiar terms, compare the hexadecimal and ASCII representations, etc.

Then, have them ping their neighbors and watch the Wireshark window as it fills with ICMP messages. Stop Wireshark from recording and pause to open some of the captured packets, pointing out source and destination IP addresses and identifying the students associated with them.

Next, have students pair up with the person sitting directly in front of them. Ask each pair for a person A and a person B. Person A will run the following command:

nc -l 12345

and Person B will run the command:

nc <ip_addr_of_person_a> 12345

Give them some time to type messages to each other, and also have a few people surreptitiously send messages to other pairs to demonstrate how anyone can send messages to a device they know is listening. May also point them to **man nc** to independently learn more about what the program they're using.

After everyone has had some time to chat with their classmates, ask them to pause chatting, then start Wireshark on the central computer or gateway, and then record as they resume chatting. Open up various packets and show them that all of their chat messages can be viewed at the gateway. This is a good segue into security implications, real-life chat applications, etc.

Guided Practice

None.

Independent Practice

If time allows, have them run Wireshark on their own computers to capture packets themselves, then allow them to explore both the program and the captured packets independently. Note that since they're not on a hub, they won't be able to see messages destined for other machines, but they can monitor their own traffic and have others send traffic to them so as to see it in Wireshark. They can also run **ping -b 255.255.255.255** to broadcast a ping to everyone that all people can see on their Wireshark interface.

Closing

Remind students that they have just used fundamental networking tools and concepts that can be used to build communication applications of their own.

In Hindsight

01/24/2017: Students were enthusiastic about this lesson as expected due to the ability to chat with their friends. Some good questions were asked, specifically about what TCP is, why netcat interrupts the other person with a message from the sender while they're typing a message of their own, and whether support for multiple senders/receivers is provided by netcat. This was a good opportunity to talk about popular chat and messaging applications and the differences/similarities between them and low-level tools like netcat. Most students seemed to be getting the hang and enjoying using the command line, even some of those who noticeably lacked enthusiasm for ICT at the end of last year.

01/25/2017: Same observations as above for the second stream, many students wrote things down without being prompted and showed enthusiasm for the topic.