Lab 8a – Packets – Packet Capturing

By

Lukas Fuller

IAE-201-D02

IA-201: Introduction to Information Assurance

**Abstract**

The objective of this lab is to introduce students to Wireshark and packet capturing. The students will be able to use Wireshark to capture packets on a network. Students will also be introduced to what network packets are.

**Materials**

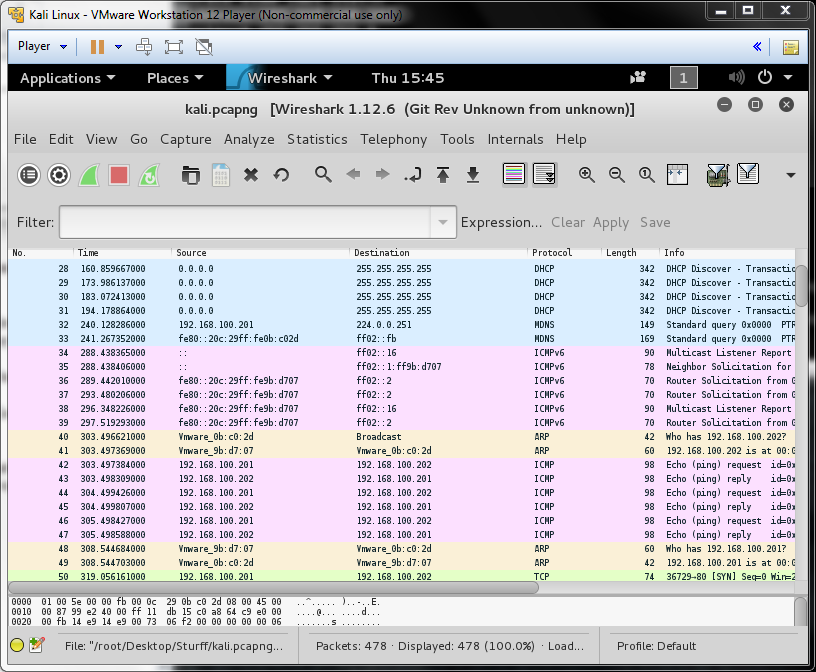
1. Backtrack 4 Virtual Machine (Kali)
2. Metasploitable Virtual Machine

**Conclusion**

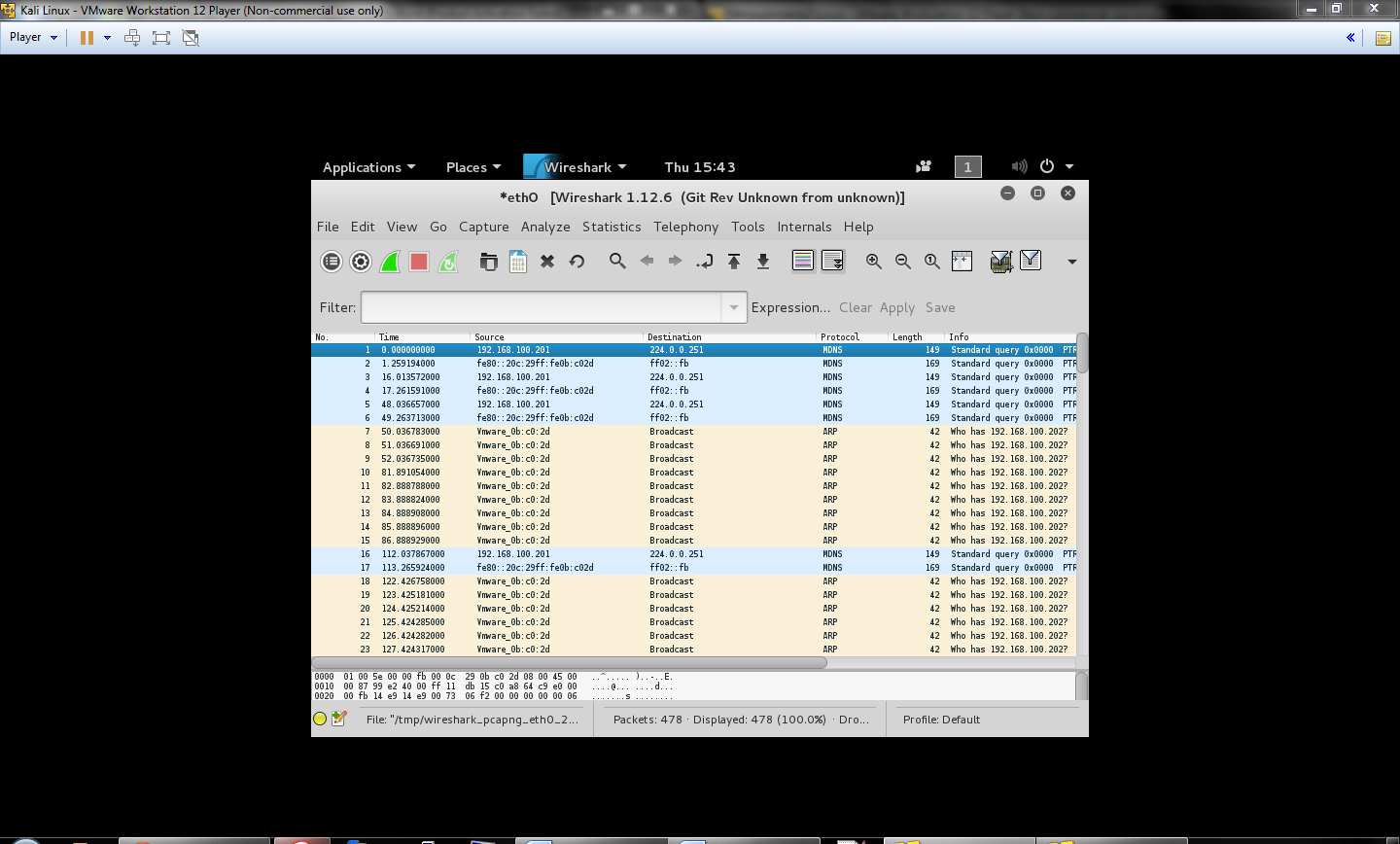
Thankfully this time I didn’t run into any major issues since I finished the lab on the desktops in the cyber-battle-lab. Also, it was rather simple to maneuver through wireshark, and seeing the requests happen as I’m creating them was pretty cool. Another part of wireshark that was interesting was it captured the data packets almost instantaneously as they were being transmitted, which might be only because it was on the same server, but regardless was interesting to note. Lastly, seeing each packet broken down was rather interesting, since you can see the client and server conversation. Overall, this lab helped me understand how to use wireshark and visually see how packets appear.

**Screenshots**

1. Screenshot of Wireshark session with successful capture.



2. Pcap of your lab session.



**Questions:**

1. What is Wireshark? **Wireshark is a software used to capture packets of data on the internet**
2. What is a packet frame? **A container for a packet which allows the packet to be sent and received**
3. What is a packet? **It contains data that is sent between networked computers**
4. What is TCP? **It is inside a IP packet, and it shows if there are any flags and if there is acknowledgement between the two computers as well as other basic information**
5. What is UDP? **It is inside the IP packet, and it shows the: destination port, source port, sequence number, checksum, and data**
6. What is ICMP? **Packets that are created when you ping other hosts**
7. What is a pcap? **An application programming interface for capturing network packets**