CYBS 7357 Lab 02 Quiz

\* Answers are highlighted in yellow

1. Which of the following statements is true?

a. The Wireshark protocol analyzer has limited capabilities and is not considered multi-faceted.

b. Wireshark is used to find anomalies in network traffic as well as to troubleshoot application performance issues.

c. Both Wireshark and NetWitness Investigator are expensive tools that are cost-prohibitive for most organizations.

d. NetWitness Investigator is available at no charge while Wireshark is a commercial product.

2. Wireshark capture files, like the DemoCapturepcap file found in this lab, have a \_\_\_\_\_\_\_\_\_\_ extension, which stands for packet capture, next generation.

a. .packcng

b. .paccapnextg

c. .pcnextgen

d. .pcapng

3. The Wireless Toolbar (View > Wireless Toolbar) is used only:

a. when using a pre-captured file.

b. when capturing live traffic.

c. when reviewing wireless traffic.

d. in a virtual lab environment.

4. In the frame detail pane, which of the following was a field unique to wireless traffic, confirming that it is a wireless packet?

a. The Encapsulation type: Per-Packet Information header

b. The Arrival time: May 11, 2007 15:30:37 041165000 Pacific Daylight Time

c. The Capture Length: 181 bytes

d. The Epoch Time: 1178922637.041165000 seconds

5. Which of the following tools provides information about the antennae signal strengths, noise ratios, and other antennae information during a captured transmission?

a. Windows Explorer

b. DemoCapture

c. Wireshark

d. NetWitness

6. Which of the following can be used to map who is able to communicate with whom, the measured strength of signals, and what frequencies are used, as well as be used for jamming certain frequencies and for determining which devices were likely used to set off remote bombs and Improvised Explosive Devices (IEDs)?

a. MAC+PHY (MAC and Physical Layer)

b. IEEE Layer

c. Flags fields

d. Quality of Service information

7. In the IEEE 802.11 Quality of Service information and Flags fields, Wireshark displays information about the \_\_\_\_\_\_\_\_\_\_, which enables the network administrator to determine which Media Access Control (MAC) addresses match each of them.

a. antennae and signal strength

b. transmitters and receivers of the data

c. payload and frame information

d. Domain System and Internet Protocol version

8. In the lab, Wireshark displayed the transmitter/receiver address in both full hexadecimal (00:14:a5:cd:74:7b) and a kind of shorthand, which was:

a. IEEE 802.11.

b. GemtekTe\_IEEE.

c. GemtekTe\_00:14:a5.

d. GemtekTe\_cd:74:7b.

9. Matching the \_\_\_\_\_\_\_\_\_\_ to their appropriate transmitter and receiver addresses can provide the needed forensic evidence of which devices are involved in a particular communication.

a. MAC addresses

b. IP addresses

c. brand names

d. IEEE numbers

10. Which of the following statements is true regarding the fields displayed in Wireshark?

a. There are hundreds of fields of data available and there are many different ways to interpret them.

b. There are a few dozen fields of data available but there are many different ways to interpret them.

c. There are very few fields of data available and most administrators will interpret them in the same or a similar way.

d. Although there are very few fields of data available, most administrators will interpret them differently.

11. Which of the following is a packet capture add-on that is frequently installed with Wireshark that enables the capture of more wireless information?

a. 3Com

b. QoS

c. GemtekTE

d. AirPcap

12. Regardless of whether the packet is sent through the air or on a wire, the ultimate payload in an investigation is:

a. information regarding the transmitters and receivers of the data.

b. detail about the Internet Protocol version.

c. a Domain Name System query.

d. evidence of any suspicious activity.

13. In the lab, the DNS query indicated an IP address of \_\_\_\_\_\_\_\_\_\_ for www.polito.it.

a. 172.30.0.100

b. 130.192.73.1

c. 177.390.13.6

d. 172.30.121.1

14. What is the actual web host name to which www.polito.it is resolved?

a. web01.polito.gov

b. web01.polito.it

c. web01.polito.com

d. www.polito.com

15. In order to use NetWitness Investigator to analyze the same packets that you analyzed with Wireshark, you first had to save the DemoCapturepcap.pcapng file in the older \_\_\_\_\_\_\_\_\_\_ format.

a. .libpcap

b. .tcpdump-libcap

c. .pcapng

d. .pcap

16. Which of the following statements is true regarding NetWitness Investigator?

a. NetWitness Investigator is available for free so it is only used for some initial analysis.

b. NetWitness Investigator is often used only by skilled analysts for specific types of analysis.

c. Investigators with little training typically can capture needed information using NetWitness Investigator.

d. Wireshark provides a more in-depth, security-focused analysis than NetWitness Investigator.

17. Which of the following statements is true regarding NetWitness Investigator reports?

a. NetWitness reports contain only low-level wireless information, such as command and control.

b. NetWitness reports do not provide the kind of sophisticated analysis that is found within Wireshark.

c. NetWitness and Wireshark both provide the same information but the two tools differ in how that information is displayed.

d. NetWitness is unable to provide information about the geographic location of the transmitter and receiver.

18. Which of the following tools displays the MAC address and IP address information and enables them to be correlated for a given capture transmission?

a. DemoCapture

b. Wireshark

c. NetWitness Investigator

d. Both Wireshark and NetWitness Investigator

19. When you were using NetWitness Investigator in the lab, the Destination City report indicated that the Destination Organization of www.polito.it was recorded as:

a. Turin Polytechnic.

b. Politecnico de Tourino.

c. Republic of Italia.

d. Turin, Italy.

20. Which of the following statements is true regarding the information in the Destination City report?

a. The Top-Level Domain (TLD) “.it” belongs to Italy.

b. The Top-Level Domain (TLD) “.it” is proof that the web site is physically located in Italy.

c. The Top-Level Domain (TLD) was actually registered in the United States.

d. It indicates that it will be impossible to determine the actual physical location of the server.

NAME:

Natnael kebede