Name: _____ Class: _____ Date: _____

Module 02: Analyzing Network Reconnaissance

Multiple Choice

1. A threat actor has gone to a local coffee shop and opened a program that can analyze traffic being sent and received on the network. He finds that someone on the network is sending emails using SMTP without encryption, and he can see the contents of the emails. Which of the following programs is he most likely using?

a. netstat
b. dig
c. Wireshark
d. Nessus

ANSWER: c

FEEDBACK:

a. Incorrect. Netstat can show a variety of information about a network connection, but it does not perform any type of packet sniffing.
b. Incorrect.The dig command is used on UNIX and Linux machines to query DNS servers.
c. Correct.Wireshark is a packet analysis tool that allows a user to see the traffic being sent and received on a network. If the traffic is unencrypted, the user can see the contents of the packets as well.
d. Incorrect. Nessus is a popular vulnerability scanner. It does not perform packet capture and analysis.

POINTS: 1

QUESTION TYPE: Multiple Choice

HAS VARIABLES: False

DATE CREATED: 6/17/2020 6:55 AM

DATE MODIFIED: 6/17/2020 6:57 AM

2. Umberto works for an organization that has created a policy prohibiting the use of open source software unless there is no alternative. He wants to sniff packets on the network, but most of the sniffer applications are open source. Which of the following software packages would adhere to the company's policy?

a. Wireshark
b. EtherApe
c. NetworkMiner
d. Network General

ANSWER: d

FEEDBACK:

a. Incorrect. Wireshark is an open source packet capture application.
b. Incorrect. EtherApe is an open source packet capture application.
c. Incorrect. NetworkMiner is an open source packet capture application.
d. Correct. Network General is a proprietary software application that performs packet capturing.

POINTS: 1

QUESTION TYPE: Multiple Choice

HAS VARIABLES: False

Name: _____ Class: _____ Date: _____

Module 02: Analyzing Network Reconnaissance

DATE CREATED: 6/17/2020 6:58 AM
DATE MODIFIED: 6/17/2020 6:59 AM

3. A cybersecurity analyst is researching syslog for possible implementation at his organization. He is reading about the elements that syslog messages contain and sees the priority and header fields. Which of the following fields contains the contents of the messages?

a. MSG
b. CONTENT
c. VALUE
d. STAT

ANSWER: a
FEEDBACK:
a. Correct. The MSG field contains the contents of syslog messages.
b. Incorrect. There is not a CONTENT field in syslog messages.
c. Incorrect. There is not a VALUE field in syslog messages.
d. Incorrect. There is not a STAT field in syslog messages.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 6/17/2020 7:09 AM
DATE MODIFIED: 6/17/2020 7:13 AM

4. Ian, a cybersecurity analyst, wants to use a system to identify when employees are using Telnet on the network by examining only the headers of packets as they traverse the network. Which of the following might he decide to implement to meet this goal?

a. Packet analysis
b. Protocol analysis
c. Traffic analysis
d. Wireless analysis

ANSWER: b
FEEDBACK:
a. Incorrect. Packet analysis examines the entire contents of packets, not just the headers.
b. Correct. Protocol analysis only examines the headers of packets to determine the protocol in use.
c. Incorrect. Traffic analysis examines a collection of data to find performance bottlenecks. It does not examine only the headers to determine which protocol is being used.
d. Incorrect. Wireless analysis is used to analyze the RF spectrum to find and detect wireless networks.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 6/17/2020 7:13 AM

Module 02: Analyzing Network Reconnaissance

DATE MODIFIED: 6/17/2020 7:14 AM

5. Morena wants to use Wireshark to analyze the types of traffic being sent across her company's network. Which of the following types of analysis does she want to perform?

a. Wireless analysis
b. Traffic analysis
c. Packet analysis
d. Protocol analysis

ANSWER: c

FEEDBACK:

a. Incorrect. Wireshark is not used to analyze the RF spectrum. It is used to analyze the packets moving across a network.
b. Incorrect. Traffic analysis is used to examine the performance of a network and identify bottlenecks.
c. Correct. Wireshark is an application used to analyze the contents of packets on a network; this is known as packet analysis.
d. Incorrect. Protocol analysis only examines the headers of packets. Wireshark can analyze the entire contents of packets.

POINTS: 1

QUESTION TYPE: Multiple Choice

HAS VARIABLES: False

DATE CREATED: 6/17/2020 7:14 AM

DATE MODIFIED: 6/17/2020 7:16 AM

6. Talera believes an evil twin might be planted somewhere around her company's office. Which of the following is the best method of finding where it might be located?

a. Protocol analysis
b. Traffic analysis
c. Packet analysis
d. Wireless analysis

ANSWER: d

FEEDBACK:

a. Incorrect. Protocol analysis is used to examine the headers of packets on a network and determine which protocols are being used.
b. Incorrect. Traffic analysis is used to examine network performance and find bandwidth bottlenecks.
c. Incorrect. Packet analysis is used to examine the contents of packets moving across a network. It might help detect an evil twin, but it doesn't help track down the evil twin's location as easily as a wireless analysis tool would.
d. Correct. Wireless analysis can be used to identify the signal strength of wireless access points, which will help locate an evil twin.

Name: _____ Class: _____ Date: _____

Module 02: Analyzing Network Reconnaissance

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 6/17/2020 7:16 AM
DATE MODIFIED: 6/17/2020 7:18 AM

7. Jorge is analyzing the event logs on a server and sees that someone attempted to log into a user account twice with the incorrect password before logging in successfully. In which of the following general types of logs were these events most likely captured?

a. System
b. Security
c. Application
d. Authentication

ANSWER: b

FEEDBACK:

a. Incorrect. System logs include events logged by the operating system, such as hardware failures.
b. Correct. Security logs are specifically logged by the operating system; they include login failures.
c. Incorrect. Application logs include events logged by applications.
d. Incorrect. Some systems may have an authentication event log type, but it is not one of the three general log types that are present in all systems.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 6/17/2020 7:18 AM
DATE MODIFIED: 6/17/2020 7:20 AM

8. Tina wants to determine the fault toleranceof the servers in her data center, and is reviewing the previous 24 months of logs using an analysis tool. Which of the following types of analysis is Tina most likely performing?

a. Conditional analysis
b. Anomaly analysis
c. Behavioral analysis
d. Availability analysis

ANSWER: d

FEEDBACK:

a. Incorrect. A conditional analysis seeks to uncover one or more events that violate predefined rules. It does not analyze the availability of a system that might have individual

component failures over a period of time.

b. Incorrect. While a component failure could be considered an anomaly by some systems, it is not the best answer here. Some systems may note a component failure, but they wouldn't note whether the system as a whole became unavailable.

c. Incorrect. While the results of a component failure might show up in a behavioral analysis, it is not the best answer here. Some systems may note a component failure, but they wouldn't note whether the system as a whole became unavailable.

d. Correct. Availability analysis is a data correlation analysis that examines whether a network device or service is properly functioning to provide resources to users. In this case, even if a component fails, Tina wants to determine whether the systems are fault tolerant and thus still available to users.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 6/17/2020 7:20 AM
DATE MODIFIED: 6/17/2020 7:22 AM

9. Thierry wants to implement a method of analyzing network traffic to detect attacks by using a database of known attacks for comparison. Which of the following methods of analysis meets his goal?

a. Signature analysis
b. Behavioral analysis
c. Availability analysis
d. Anomaly analysis

ANSWER: a
FEEDBACK:

a. Correct. Signature analysis uses a database of signatures for comparison to determine whether network activity may be part of an attack.

b. Incorrect. Behavioral analysis does not use a database of attacks for comparison to determine whether network activity is part of an attack.

c. Incorrect. Availability analysis does not use a database of attacks for comparison to determine whether network activity is part of an attack.

d. Incorrect. Anomaly analysis uses a baseline to compare network activity against, not a database.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 6/17/2020 7:23 AM
DATE MODIFIED: 6/17/2020 7:25 AM

Module 02: Analyzing Network Reconnaissance

10. Jonquil, a cybersecurityanalyst, has been asked to implement a system that collects information for analysis about traffic flowing through the routers and switches on her company's network. Which of the following protocols should she considerto implement this type of setup?

a. IDS
b. Resource Monitor
c. NetFlow
d. SIEM

ANSWER: c

FEEDBACK:
a. Incorrect. An intrusion detection system is not a protocol.
b. Incorrect. Resource Monitor is not a protocol; it is an application.
c. Correct. NetFlow is a protocol developed by Cisco that is used to collect information about traffic flowing through devices on a network.
d. Incorrect. SIEM is not a protocol; it is a product.

POINTS: 1

QUESTION TYPE: Multiple Choice

HAS VARIABLES: False

DATE CREATED: 6/17/2020 7:26 AM

DATE MODIFIED: 6/17/2020 7:27 AM

11. Neo wants to consolidate real-time monitoring and management of security-related information with analysis and reporting of events. Which of the following might he want to implement?

a. IGRP
b. SERP
c. SIEM
d. IMEI

ANSWER: c

FEEDBACK:
a. Incorrect. The Interior Gateway Routing Protocol is not used to consolidate monitoring and management of security information and events.
b. Incorrect. Search engine results pages do not provide real-time monitoring and management of security-related information.
c. Correct. Security Information and Event Management products consolidate real-time monitoring and management of security information with analysis and reporting of security events.
d. Incorrect. AnInternational Mobile Equipment Identity is a way of identifying a mobile phone. It would not be helpful in consolidating real-time monitoring and management of security-related information.

POINTS: 1

QUESTION TYPE: Multiple Choice

Module 02: Analyzing Network Reconnaissance

HAS VARIABLES: False
DATE CREATED: 6/17/2020 7:28 AM
DATE MODIFIED: 6/17/2020 7:29 AM

12. Nichole, a cybersecurity analyst, has received an alert about a potential ping flood on one of the company's Windows servers. She is able to connect to the server via an out-of-band management network. Which of the following native tools might help her verify what is occurring on the server at the moment?

a. Resource Monitor
b. tcpdump
c. Wireshark
d. Network General

ANSWER: a

FEEDBACK:

a. Correct. Resource Monitor is a tool built into Windows that allows the administrator to view disk, network, CPU, and memory usage. Ping floods are typically visible in Resource Monitor when you see a spike in network and CPU usage.
b. Incorrect. The tcpdump command is not native to Windows. There is a clone version available for Windows from a third party.
c. Incorrect. Wireshark is not a native tool to Windows. It is a third-party tool that can be installed.
d. Incorrect. Network General is a third-party utility; it is not a native built-in tool for Windows.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 6/17/2020 7:29 AM
DATE MODIFIED: 6/17/2020 7:31 AM

13. Cyndi, a cybersecurity researcher, has been hired to comb through historical data at a large organization after an APT was discovered. She needs to determine the extent of the attack and be able to view various parts of the network's logs to give her the full context of what occurred. Which of the following might best describe the type of analysis she is performing?

a. Packet analysis
b. Retrospective network analysis
c. Signature analysis
d. Anomaly analysis

ANSWER: b

FEEDBACK:

a. Incorrect. While packet analysis may be used in the scenario, the best answer is retrospective network analysis.

b. Correct. Retrospective network analysis allows you to observe data breaches and attacks exactly as they occurred within the context of other network activity.

c. Incorrect. While signature analysis may help detect attacks when they occur, and may be used with historical data at times, the best answer for the scenario described is retrospective network analysis.

d. Incorrect. While anomaly analysis may be used in the scenario, the best answer is retrospective network analysis.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 6/17/2020 7:31 AM
DATE MODIFIED: 6/17/2020 7:33 AM

Matching

Match each of the following output types with the command switch used with nmap to generate that type of output:

a. (Default)
b. -oN
c. -oX
d. -oG

QUESTION TYPE: Matching
HAS VARIABLES: False
DATE CREATED: 6/17/2020 6:59 AM
DATE MODIFIED: 6/17/2020 7:08 AM

14. Interactive
ANSWER: a
POINTS: 1

15. Interactive output stored in a file
ANSWER: b
POINTS: 1

16. Output in Extensible Markup Language
ANSWER: c
POINTS: 1

17. Output that can be manipulated using Linux command-line tools
ANSWER: d
POINTS: 1