X

Unit 8 - Week 6

Assignment 6

The due date for submitting this assignment has passed. **Due on 2018-03-21, 23:59 IST.**

Submitted assignment

1) In network forensics the most important activity among others is *1 point*

- collecting the evidence
- destroying the foot-prints
- securing the network
- preserving the evidence

No, the answer is incorrect.
Score: 0

Accepted Answers:
preserving the evidence

2) List the one that is not a part of network based evidence *1 point*

- Name server
- OS logs
- Switches and Routers
- Application servers

No, the answer is incorrect.
Score: 0

Accepted Answers:
OS logs

3) Queries and response of name servers traverse in a _____ fashion. *1 point*

- Relational
- Network
- Hierarchical
- Distributed

No, the answer is incorrect.
Score: 0

Accepted Answers:
Hierarchical

4) Some examples of directory services are *1 point*

- TCP/IP, ICMP
- Linux, Ubuntu, Windows NT, Windows 7
- TACACS+, RADIUS, DIAMETER
- LDAP, AD

No, the answer is incorrect.
Score: 0

Accepted Answers:
LDAP, AD

5) The library used in Linux to capture data packets is **1 point**

- libpcap
- libmcap
- libscap
- libc

No, the answer is incorrect.
Score: 0

Accepted Answers:
libpcap

6) Identify one tool in the list that is not a packet capture tool **1 point**

- tcpdump
- sftp
- tshark
- dumpcap

No, the answer is incorrect.
Score: 0

Accepted Answers:
sftp

7) The wireshark interface screen has 3 main partitions, namely, **1 point**

- Source, Destination addresses and length of packets
- Packet list, packet details, and packet bytes
- TCP/IP, RIP, NTP
- partition 1, 2 and 3

No, the answer is incorrect.
Score: 0

Accepted Answers:
Packet list, packet details, and packet bytes

8) It is most advisable to **1 point**

- Do live analysis of the network
- Capture packets all the time in the network
- Store a copy of important packets in a packet capture file and use it for analysis
- Discard original packet capture file

No, the answer is incorrect.
Score: 0

Accepted Answers:
Store a copy of important packets in a packet capture file and use it for analysis

9) After capturing the packets, identify one activity that cannot be done immediately on the captured packets. **1 point**

- Documented Protocol analysis

- Undocumented Protocol Analysis
- Stream Reconstruction
- Packet analysis

No, the answer is incorrect.
Score: 0

Accepted Answers:
Undocumented Protocol Analysis

10) RFC is expanded to **1 point**

- Request for Comments
- Request for Classes
- Raising Formatted Protocols
- Rather Funny Conclusion

No, the answer is incorrect.
Score: 0

Accepted Answers:
Request for Comments

11) Examination of a sequence of related packets is called **1 point**

- Flow analysis
- Deep packet Inspection
- Packet analysis
- Field scanning

No, the answer is incorrect.
Score: 0

Accepted Answers:
Flow analysis

12) In the case study large amount of packets have been sent from the local machine to **1 point**

- local address
- internal ip address
- home postal address
- external ip address

No, the answer is incorrect.
Score: 0

Accepted Answers:
external ip address

13) In the case study a multicast was identified using **1 point**

- data packets traversing between multiple destination
- source sending data to different IP addresses
- the reserved address range
- guess work

No, the answer is incorrect.
Score: 0

Accepted Answers:
the reserved address range

14) The instant messaging protocol that was reverse engineered to develop the tool was **1 point**

- SIMPLE
- XMPP
- OSCAR

- AIM

No, the answer is incorrect.
Score: 0

Accepted Answers:
OSCAR

15) XXD is used for **1 point**

- data capture
- data correlation
- linking conversations during forensic analysis
- creating a hex dump of a file

No, the answer is incorrect.
Score: 0

Accepted Answers:
creating a hex dump of a file

Previous Page End