NAME : _____

CLASS : _____

DATE : _____

Cyber Range Pre-Experiment

14 Questions

1. What is the main task of a Security Information and Event Management (SIEM)?

☐ a) Treats malware according to the virus scan.

☐ b) Generates alarms from security events (parsed log files).

☐ c) Conducts cyberhacking operations.

☐ d) Generates and reports the status of the current tasks of the cybersecurity team.

2. What does the tag "title" describe in a SIEM dashboard?

☐ a) The type of the attack.

☐ b) The name of the hacker.

☐ c) The title of the malware.

☐ d) Information of what the event is about.

3. What is a plugin sid in a SIEM?

☐ a) The ID that matches to the specific ID of an event type.

☐ b) The ID of the plugins that we can install within a SIEM.

☐ c) The ID of the plugins that are already installed within a SIEM.

☐ d) None of the choices.

4. Regarding headers of a directive and the rules:

☐ a) A directive can be either a header or a rule.

☐ b) The rules include headers.

☐ c) A directive defines rules that includes a header.

☐ d) A directive defines a header and include the corresponding rules.

5. What is the purpose of stages in a SIEM?

☐ a) They define the state of the attack.

☐ b) Stages are not used in a SIEM.

☐ c) Stages are the steps which have to be followed from the incident response team.

☐ d) Stages are conditions that define when the alarm will be triggered.

6. What is a timeout in a SIEM?

- ☐ a) Defines how long a rule is valid for going to the next stage of the rule.
- ☐ b) Defines how long the attacker maintained access before being identified by the SIEM.
- ☐ c) Defines how long the directive is valid.
- ☐ d) None of the choices.

7. What does occurence define in a SIEM rule?

- ☐ a) Defines how many events of the exact event type need to occur to fulfill a rule.
- ☐ b) Defines the number of occurrences of a specific attack.
- ☐ c) Defines the severity level of a ransomware that occurred in the past.
- ☐ d) Occurrence is the obscureness.

8. How does ARP Spoofing work?

- ☐ a) ARP spoofing is about the HTTP protocol and how to intercept messages.
- ☐ b) Enabling the monitoring of the keystrokes of the victim.
- ☐ c) Installing a malware on the victim's side.
- ☐ d) Linking the attacker's MAC address with the IP of the victim.

9. What is a Man in the Middle Attack?

- ☐ a) It is a social engineering attack where a person tries to collect information from the victims.
- ☐ b) The attacker is able to collect password by using e-mails.
- ☐ c) The two parties believe that they have a direct communication while the attacker intercepts or eavesdrops the messages.
- ☐ d) The attack is executed once a middleware is installed.

10. What could be the reason for an attacker deleting the log files?

- ☐ a) The attacker tries to infiltrate other systems by deleting the log files.
- ☐ b) This is called log file manipulation for hiding the traces from the malicious action.
- ☐ c) This task is not important since the attacker does not want to actually delete files but to access the main system.
- ☐ d) The attacker likes very much to delete files whenever she can.

11. Ping requests/commands are used using the ICMP protocol. What are the potential malicious actions?

☐ a) ARP Poisoning
☐ b) Cross-site scripting (XSS) attack
☐ c) Denial Of Service Attacks
☐ d) Password Attacks

12. What is a directive within dSIEM (a specific SIEM product)?

☐ a) Directives include the ransomware payload and their intention is to proceed with a malware scanning.
☐ b) Directives include the main directions that have to be forwarded to the cyberoperation teams for responding to an incident.
☐ c) Directives include among others the conditions that have to be met for triggering an alarm.
☐ d) Directives are the security and privacy guidelines that a SIEM must comply with.

13. What is the direct benefit of using a SIEM?

☐ a) Removes ransomware from a computer.
☐ b) Blocks the ports that are insecure or limits the network ports which will be exposed to the internet.
☐ c) Checks if an e-mail is a phishing e-mail and supports the common user to open or delete the e-mail.
☐ d) Correlates data from across the entire network, and analyzes it to trigger an alarm in order to detect incidents.

14. Have you ever used or seen any educational content regarding SIEMs in the past?

☐ a) Yes
☐ b) No

Answer Key

1. b
2. d
3. a
4. d
5. d
6. a
7. a
8. d
9. c
10. b
11. c
12. c
13. d
14. n/a