Free Questions for 312-39 by braindumpscollection

Shared by Willis on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following attack can be eradicated by disabling of "allow_url_fopen and allow_url_include" in the php.ini file?

Options:

A- File Injection Attacks

B- URL Injection Attacks

C- LDAP Injection Attacks

D- Command Injection Attacks

Answer:

A

Question 2

Question Type: MultipleChoice

In which log collection mechanism, the system or application sends log records either on the local disk or over the network.

Options:

A- rule-based

B- pull-based

C- push-based

D- signature-based

Answer:

C

Question 3

Question Type: **MultipleChoice**

Identify the attack in which the attacker exploits a target system through publicly known but still unpatched vulnerabilities.

Options:

A- Slow DoS Attack

B- DHCP Starvation

C- Zero-Day Attack

D- DNS Poisoning Attack

Answer:

C

Question 4

Question Type: **MultipleChoice**

Peter, a SOC analyst with Spade Systems, is monitoring and analyzing the router logs of the company and wanted to check the logs that are generated by access control list numbered 210.

What filter should Peter add to the 'show logging' command to get the required output?

Options:

A- show logging | access 210

B- show logging | forward 210

C- show logging | include 210

D- show logging | route 210

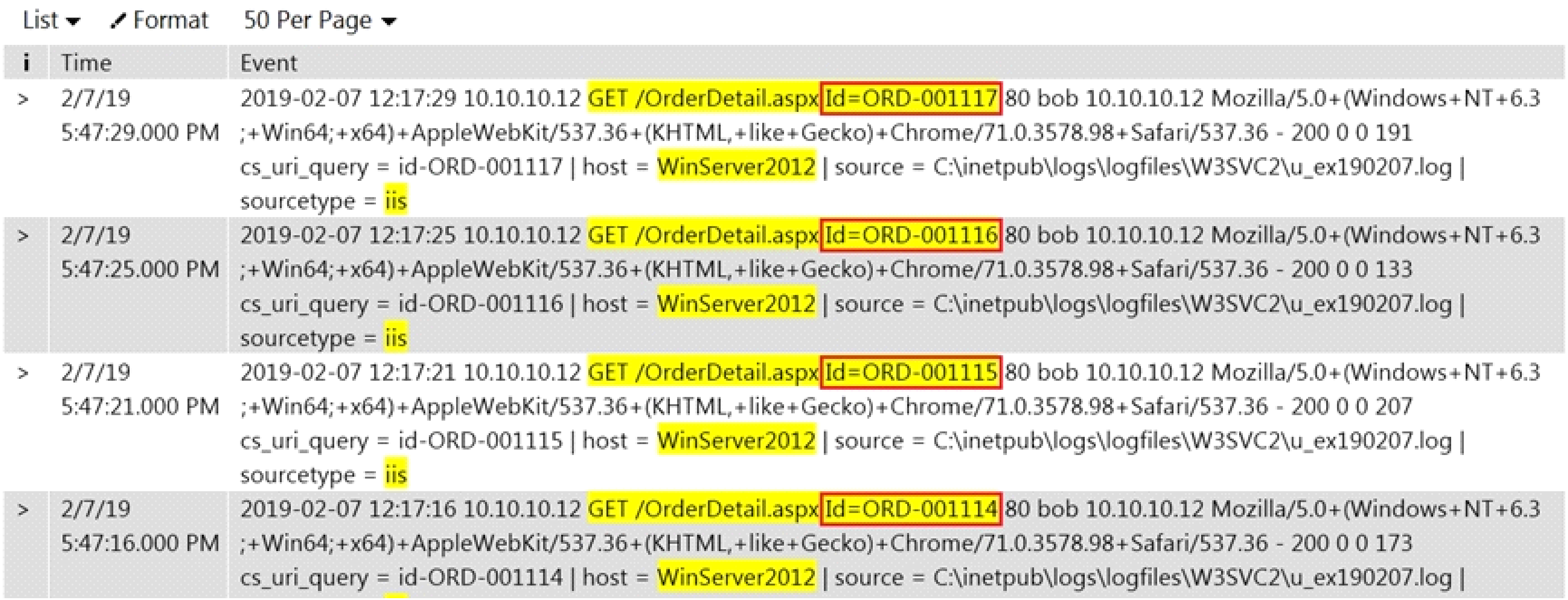
Answer:

C

Question 5

Question Type: MultipleChoice

Rinni, SOC analyst, while monitoring IDS logs detected events shown in the figure below.



```
i   Time            Event
>   2/7/19          2019-02-07 12:17:29 10.10.10.12 GET /OrderDetail.aspx Id=ORD-001117 80 bob 10.10.10.12 Mozilla/5.0+(Windows+NT+6.3
    5:47:29.000 PM  ;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/71.0.3578.98+Safari/537.36 - 200 0 0 191
                    cs_uri_query = id-ORD-001117 | host = WinServer2012 | source = C:\inetpub\logs\logfiles\W3SVC2\u_ex190207.log |
                    sourcetype = iis
>   2/7/19          2019-02-07 12:17:25 10.10.10.12 GET /OrderDetail.aspx Id=ORD-001116 80 bob 10.10.10.12 Mozilla/5.0+(Windows+NT+6.3
    5:47:25.000 PM  ;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/71.0.3578.98+Safari/537.36 - 200 0 0 133
                    cs_uri_query = id-ORD-001116 | host = WinServer2012 | source = C:\inetpub\logs\logfiles\W3SVC2\u_ex190207.log |
                    sourcetype = iis
>   2/7/19          2019-02-07 12:17:21 10.10.10.12 GET /OrderDetail.aspx Id=ORD-001115 80 bob 10.10.10.12 Mozilla/5.0+(Windows+NT+6.3
    5:47:21.000 PM  ;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/71.0.3578.98+Safari/537.36 - 200 0 0 207
                    cs_uri_query = id-ORD-001115 | host = WinServer2012 | source = C:\inetpub\logs\logfiles\W3SVC2\u_ex190207.log |
                    sourcetype = iis
>   2/7/19          2019-02-07 12:17:16 10.10.10.12 GET /OrderDetail.aspx Id=ORD-001114 80 bob 10.10.10.12 Mozilla/5.0+(Windows+NT+6.3
    5:47:16.000 PM  ;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/71.0.3578.98+Safari/537.36 - 200 0 0 173
                    cs_uri_query = id-ORD-001114 | host = WinServer2012 | source = C:\inetpub\logs\logfiles\W3SVC2\u_ex190207.log |
```

What does this event log indicate?

Options:

A- Directory Traversal Attack

B- XSS Attack

C- SQL Injection Attack

D- Parameter Tampering Attack

Answer:

D

Question 6

Question Type: **MultipleChoice**

Which of the following is a correct flow of the stages in an incident handling and response (IH&R) process?

Options:

A- Containment --> Incident Recording --> Incident Triage --> Preparation --> Recovery --> Eradication --> Post-Incident Activities

B- Preparation --> Incident Recording --> Incident Triage --> Containment --> Eradication --> Recovery --> Post-Incident Activities

C- Incident Triage --> Eradication --> Containment --> Incident Recording --> Preparation --> Recovery --> Post-Incident Activities

D- Incident Recording --> Preparation --> Containment --> Incident Triage --> Recovery --> Eradication --> Post-Incident Activities

Answer:

B