200-201 Q&As

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Pass Cisco 200-201 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

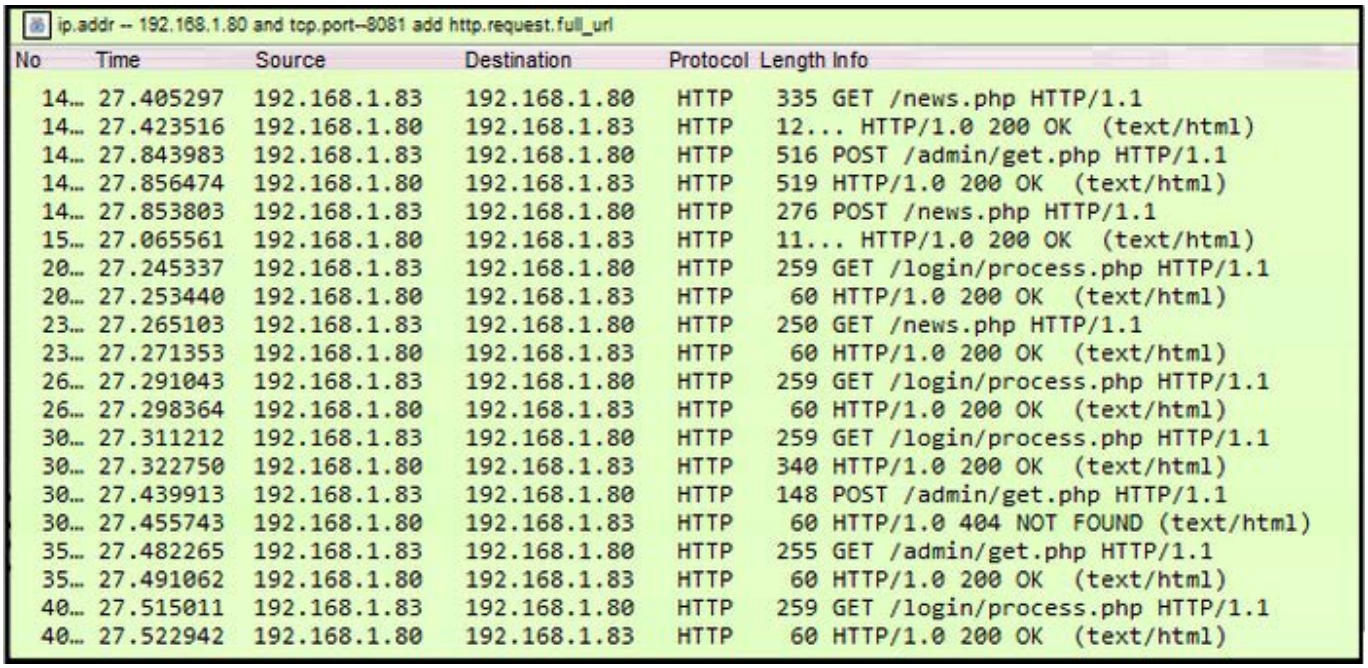
https://www.passapply.com/200-201.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

Refer to the exhibit.


ip.addr -- 192.168.1.80 and tcp.port--8081 add http.request.full_url

No	Time	Source	Destination	Protocol	Length	Info
14…	27.405297	192.168.1.83	192.168.1.80	HTTP	335	GET /news.php HTTP/1.1
14…	27.423516	192.168.1.80	192.168.1.83	HTTP	12...	HTTP/1.0 200 OK (text/html)
14…	27.843983	192.168.1.83	192.168.1.80	HTTP	516	POST /admin/get.php HTTP/1.1
14…	27.856474	192.168.1.80	192.168.1.83	HTTP	519	HTTP/1.0 200 OK (text/html)
14…	27.853803	192.168.1.83	192.168.1.80	HTTP	276	POST /news.php HTTP/1.1
15…	27.065561	192.168.1.80	192.168.1.83	HTTP	11...	HTTP/1.0 200 OK (text/html)
20…	27.245337	192.168.1.83	192.168.1.80	HTTP	259	GET /login/process.php HTTP/1.1
20…	27.253440	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)
23…	27.265103	192.168.1.83	192.168.1.80	HTTP	250	GET /news.php HTTP/1.1
23…	27.271353	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)
26…	27.291043	192.168.1.83	192.168.1.80	HTTP	259	GET /login/process.php HTTP/1.1
26…	27.298364	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)
30…	27.311212	192.168.1.83	192.168.1.80	HTTP	259	GET /login/process.php HTTP/1.1
30…	27.322750	192.168.1.80	192.168.1.83	HTTP	340	HTTP/1.0 200 OK (text/html)
30…	27.439913	192.168.1.83	192.168.1.80	HTTP	148	POST /admin/get.php HTTP/1.1
30…	27.455743	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 404 NOT FOUND (text/html)
35…	27.482265	192.168.1.83	192.168.1.80	HTTP	255	GET /admin/get.php HTTP/1.1
35…	27.491062	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)
40…	27.515011	192.168.1.83	192.168.1.80	HTTP	259	GET /login/process.php HTTP/1.1
40…	27.522942	192.168.1.80	192.168.1.83	HTTP	60	HTTP/1.0 200 OK (text/html)

A network administrator is investigating suspicious network activity by analyzing captured traffic. An engineer notices abnormal behavior and discovers that the default user agent is present in the headers of requests and data being transmitted What is occurring?

A. indicators of denial-of-service attack due to the frequency of requests

B. garbage flood attack attacker is sending garbage binary data to open ports

C. indicators of data exfiltration HTTP requests must be plain text

D. cache bypassing attack: attacker is sending requests for noncacheable content

Correct Answer: C

QUESTION 2

What is an example of social engineering attacks?

A. receiving an unexpected email from an unknown person with an attachment from someone in the same company

B. receiving an email from human resources requesting a visit to their secure website to update contact information

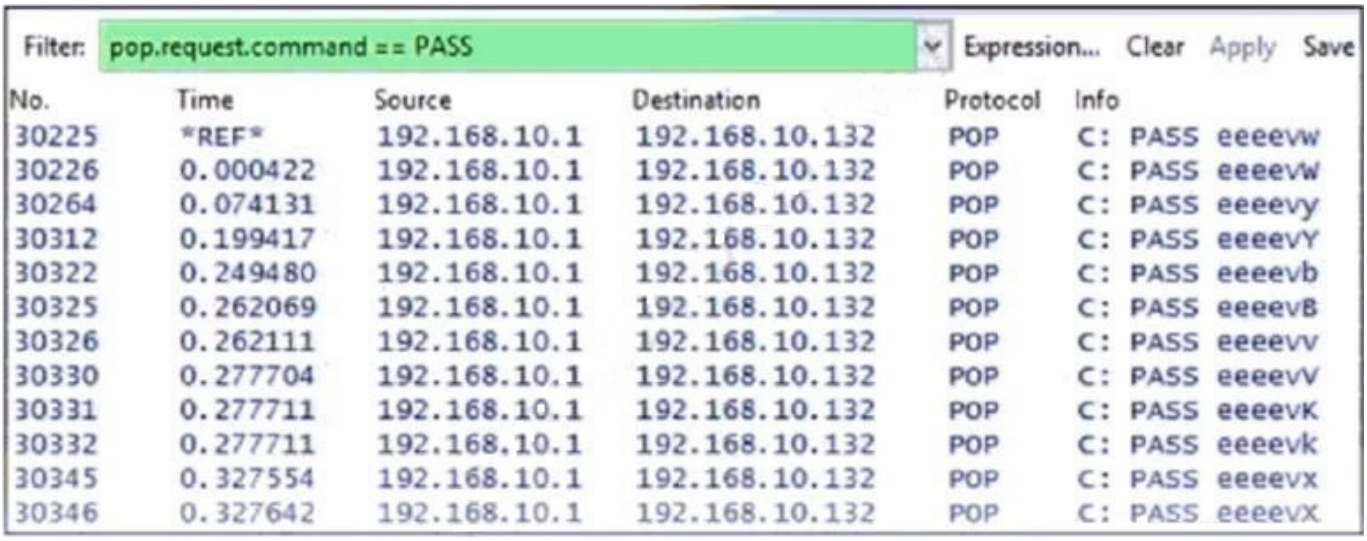
C. sending a verbal request to an administrator who knows how to change an account password

D. receiving an invitation to the department\\'s weekly WebEx meeting

Correct Answer: C

QUESTION 3

Refer to the exhibit.


Filter: pop.request.command == PASS Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Info
30225	*REF*	192.168.10.1	192.168.10.132	POP	C: PASS eeeevw
30226	0.000422	192.168.10.1	192.168.10.132	POP	C: PASS eeeevW
30264	0.074131	192.168.10.1	192.168.10.132	POP	C: PASS eeeevy
30312	0.199417	192.168.10.1	192.168.10.132	POP	C: PASS eeeevY
30322	0.249480	192.168.10.1	192.168.10.132	POP	C: PASS eeeevb
30325	0.262069	192.168.10.1	192.168.10.132	POP	C: PASS eeeevB
30326	0.262111	192.168.10.1	192.168.10.132	POP	C: PASS eeeevv
30330	0.277704	192.168.10.1	192.168.10.132	POP	C: PASS eeeevV
30331	0.277711	192.168.10.1	192.168.10.132	POP	C: PASS eeeevK
30332	0.277711	192.168.10.1	192.168.10.132	POP	C: PASS eeeevk
30345	0.327554	192.168.10.1	192.168.10.132	POP	C: PASS eeeevx
30346	0.327642	192.168.10.1	192.168.10.132	POP	C: PASS eeeevX

Which alert is identified from this packet capture?

A. man-in-the-middle attack

B. brute-force attack

C. ARP poisoning

D. SQL injection

Correct Answer: B

QUESTION 4

Refer to the exhibit.

Where is the executable file?

A. info

B. tags

C. MIME

D. name

Correct Answer: C

QUESTION 5

How does statistical detection differ from rule-based detection?

A. Statistical detection involves the evaluation of events, and rule-based detection requires an evaluated set of events to function.

B. Statistical detection defines legitimate data over time, and rule-based detection works on a predefined set of rules

C. Rule-based detection involves the evaluation of events, and statistical detection requires an evaluated set of events to function Rule-based detection defines

D. legitimate data over a period of time, and statistical detection works on a predefined set of rules

Correct Answer: B