GCIH Q&As

GIAC Certified Incident Handler

Pass GIAC GCIH Exam with 100% Guarantee

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

https://www.passapply.com/gcih.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

You are the Administrator for a corporate network. You are concerned about denial of service attacks.

Which of the following would be the most help against Denial of Service (DOS) attacks?

A. Packet filtering firewall

B. Network surveys.

C. Honey pot

D. Stateful Packet Inspection (SPI) firewall

Correct Answer: D

QUESTION 2

Analyze the data shown below. Where does this data originate from?

```
? (172.16.62.254) at 00:50:56:e8:b1:4b [ether] on eth0
? (172.16.62.2) at 00:50:56:e8:68:e7 [ether] on eth0
? (172.16.62.84) at 04:b0:77:81:90:5f [ether] on eth0
? (172.16.62.102) at 30:40:50:d3:14:af [ether] on eth0
```

A. Established connections

B. Routing table

C. ARP cache

D. Network interfaces

Correct Answer: C

Reference: https://petri.com/csc_arp_cache

QUESTION 3

A helpdesk ticket has been escalated to the incident response team. According to the FIRST organization classification guidelines, during which incident response phase should the team document the following information?

Category: Compromised Intellectual Property Criticality: High Sensitivity: Restricted to response team and management

A. Preparation

B. Eradication

C. Lessons Learned

D. Containment

Correct Answer: D

It is important to document various characteristics of the incident early on in the Containment phase. The FIRST organization distributes an incident Case Classification document that recommends characterizing an incident based on three areas: it\\'s general category, the criticality of impacted systems and data, and the sensitivity with which information about the case itself should be treated.

QUESTION 4

During which phase of incident response would an analyst review the data below?

```
root@kali:~# tcpdump -nn port 27017
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:53:01.588720 IP 172.16.66.133.36502 > 10.0.1.1.27017: Flags [S]
13:53:01.589156 IP 172.16.66.133.36502 > 10.0.1.2.27017: Flags [S]
13:53:01.589428 IP 172.16.66.133.36502 > 10.0.1.3.27017: Flags [S]
13:53:01.589693 IP 172.16.66.133.36502 > 10.0.1.4.27017: Flags [S]
13:53:01.589952 IP 172.16.66.133.36502 > 10.0.1.5.27017: Flags [S]
13:53:01.590213 IP 172.16.66.133.36502 > 10.0.1.6.27017: Flags [S]
13:53:01.590557 IP 172.16.66.133.36502 > 10.0.1.7.27017: Flags [S]
13:53:01.590914 IP 172.16.66.133.36502 > 10.0.1.8.27017: Flags [S]
13:53:01.591183 IP 172.16.66.133.36502 > 10.0.1.9.27017: Flags [S]
13:53:01.591254 IP 10.0.1.1.27017 > 172.16.66.133.36502: Flags [R.]
13:53:01.591598 IP 172.16.66.133.36502 > 10.0.1.10.27017: Flags [S]
13:53:01.594403 IP 172.16.66.133.36502 > 10.0.1.13.27017: Flags [S]
13:53:01.594725 IP 172.16.66.133.36502 > 10.0.1.14.27017: Flags [S]
```

A. Preparation

B. Reconnaissance

C. Detection

D. Enumeration

Correct Answer: A

Reference: https://www.securitymetrics.com/blog/6-phases-incident-response-plan

QUESTION 5

You see the career section of a company\\'s Web site and analyze the job profile requirements. You conclude that the company wants professionals who have a sharp knowledge of Windows server 2003 and Windows active directory installation and placement. Which of the following steps are you using to perform hacking?

A. Scanning

B. Covering tracks

C. Reconnaissance

D. Gaining access

Correct Answer: C