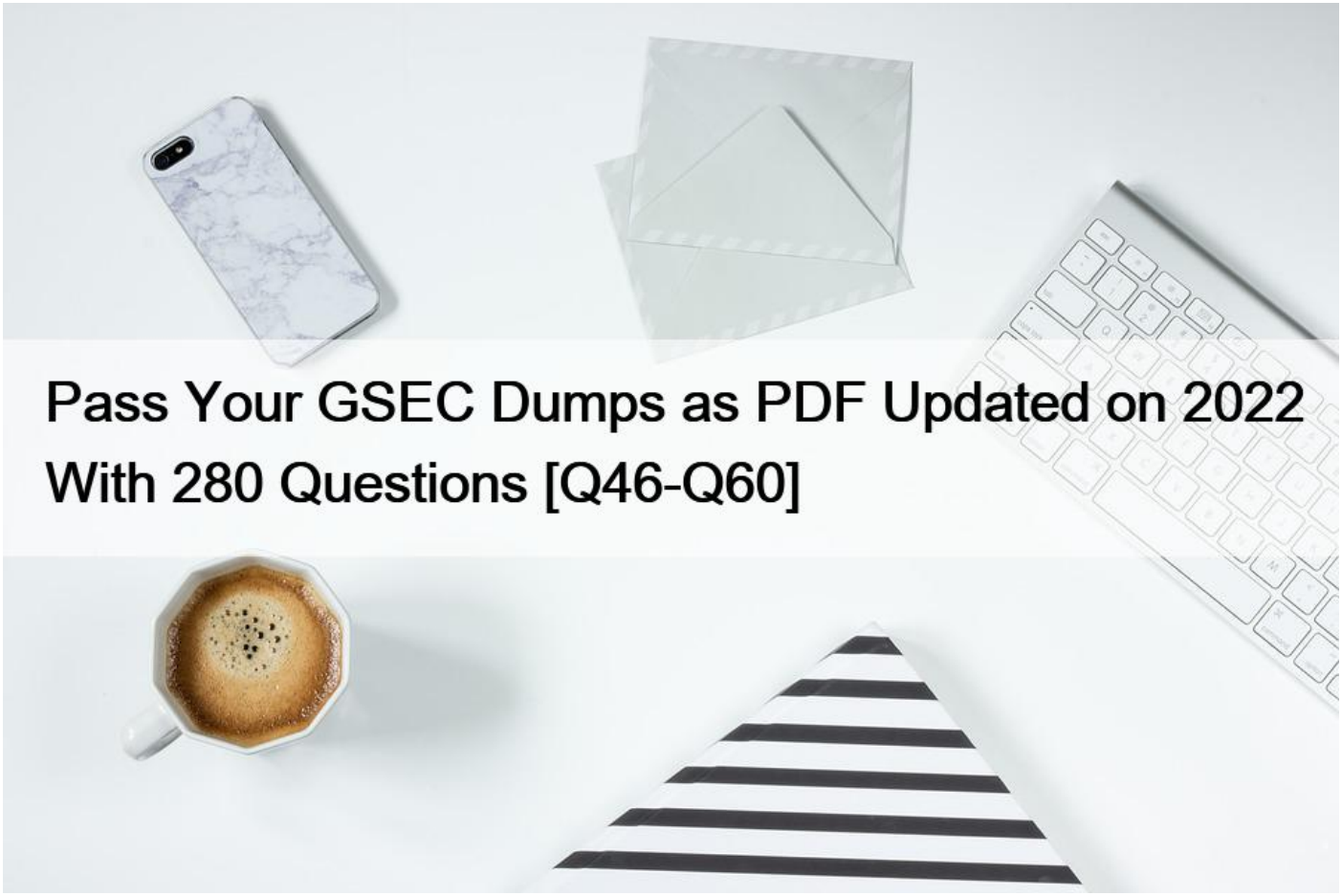
Pass Your GSEC Dumps as PDF Updated on 2022 With 280 Questions [Q46-Q60



Pass Your GSEC Dumps as PDF Updated on 2022 With 280 Questions
GIAC GSEC Real Exam Questions and Answers FREE

Concluding Thoughts

It is no longer a doubt that many employers will prioritize experienced IT professionals when looking for new candidates to fill the vacant roles. And what better way to gain the required skills than becoming certified?
GIAC training paths empower IT professionals to propel their careers to new heights, in a field of security that's widely perceived to be competitive. The GIAC GSEC certification is all about equipping security specialists with the fundamental skills they need to protect networks and information systems from digital attacks. And the more security professionals we have, the safer our systems will be. So, if you want to assure your employer that you are the most suitable candidate for the position, get accredited today! This is also the surest path to realizing your income goals since GSEC certified individuals earn about $92k annually, according to PayScale.

NO.46 Which of the following statements about Network Address Translation (NAT) are true? Each correct answer represents a complete solution. Choose two.
* It reduces the need for globally unique IP addresses.
* It allows external network clients access to internal services.

* It allows the computers in a private network to share a global, ISP assigned address to connect to the Internet.
* It provides added security by using Internet access to deny or permit certain traffic from the Bastion Host.

NO.47 While using Wire shark to investigate complaints of users being unable to login to a web application, you come across an HTTP POST submitted through your web application. The contents of the POST are listed below.

Based on what you see below, which of the following would you recommend to prevent future damage to your database?

```
POST /samplelogin.cfm HTTP/1.1
Host: www.example.com
User-Agent: Mozilla/5.0 (X11; U; en-US;) Gecko/200910 Ubuntu 8.4
Firefox/2.6
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.example.com/
Cookie: SID=026DCB9CBBF2339C2CBFAEBA8F1DD656;
Content-Type: application/x-www-form-urlencoded
Content-Length: 64
username='a'&password=DROP+TABLE+members;+--
```


* Use ssh to prevent a denial of service attack
* Sanitize user inputs to prevent injection attacks
* Authenticate users to prevent hackers from using your database
* Use https to prevent hackers from inserting malware

NO.48 You are doing some analysis of malware on a Unix computer in a closed test network. The IP address of the computer is 192.168.1.120. From a packet capture, you see the malware is attempting to do a DNS query for a server called iamabadserver.com so that it can connect to it. There is no DNS server on the test network to do name resolution. You have another computer, whose IP is 192.168.1.115, available on the test network that you would like for the malware connect to it instead. How do you get the malware to connect to that computer on the test network?
* You modify the HOSTS file on the computer you want the malware to connect to and add an entry that reads: 192.168.1.120 iamabadserver iamabadserver.com
* You modify the HOSTS file on the Unix computer your malware is running on and add an entry that reads: 192.168.1.115 iamabadserveriamabadserver.com
* You modify the HOSTS file on the Unix computer your malware is running on and add an entry that reads: 192.168.1.120 iamabadserver iamabadserver.com
* You modify the HOSTS file on the computer you want the malware to connect to and add an entry that reads: 192.168.1.115 iamabadserver iamabadserver.com

NO.49 Which of the following Linux commands can change both the username and group name a file belongs to?
* chown
* chgrp
* chmod
* newgrp

NO.50 Included below is the output from a resource kit utility run against local host.

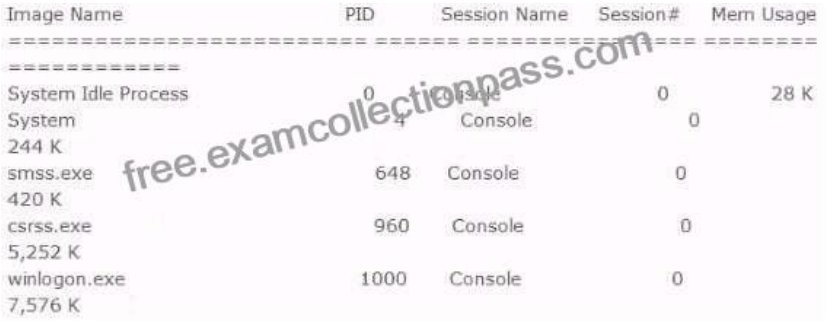


Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Console	0	28 K
System	4	Console	0	244 K
smss.exe	648	Console	0	420 K
csrss.exe	960	Console	0	5,252 K
winlogon.exe	1000	Console	0	7,576 K

Which command could have produced this output?
* Schtasks
* Task kill
* SC
* Task list

Explanation/Reference:

NO.51 What will be displayed as the output by using the following command? TAIL /var/log/messages
* An error message because of insufficient parameters.
* The last ten lines of the /var/log/messages log file.
* The first ten lines of the /var/log/messages log file.
* All lines of the /var/log/messages log file.

NO.52 Which of the following statements about a hoax are true?

Each correct answer represents a complete solution. Choose two.
* It spreads through e-mail messages.
* It is a false warning about a virus.
* It is a boot sector virus.
* It corrupts DLL files.

NO.53 Which of the following is a Layer 3 device that will typically drop directed broadcast traffic?
* Hubs
* Bridges
* Routers
* Switches

NO.54 Included below is the output from a resource kit utility run against local host.

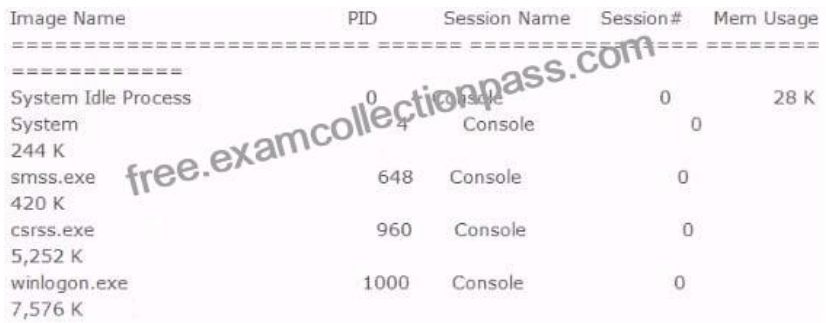


Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Console	0	28 K
System	4	Console	0	244 K
smss.exe	648	Console	0	420 K
csrss.exe	960	Console	0	5,252 K
winlogon.exe	1000	Console	0	7,576 K

Which command could have produced this output?
* Schtasks
* Task kill
* SC
* Task list

NO.55 Which of the following statements are true about satellite broadband Internet access? Each correct answer represents a complete solution. Choose two.
* It is among the least expensive way of gaining broadband Internet access.
* It is among the most expensive way of gaining broadband Internet access.
* This type of internet access has low latency compared to other broadband services.
* This type of internet access has high latency compared to other broadband services.

NO.56 Which of the following is a signature-based intrusion detection system (IDS) ?
* RealSecure
* Snort
* StealthWatch
* Tripwire

NO.57 What is the function of the TTL (Time to Live) field in IPv4 and the Hop Limit field in IPv6 In an IP Packet header?
* These fields are decremented each time a packet is retransmitted to minimize the possibility of routing loops.
* These fields are initialized to an initial value to prevent packet fragmentation and fragmentation attacks.
* These fields are recalculated based on the required time for a packet to arrive at its destination.
* These fields are incremented each time a packet is transmitted to indicate the number of routers that an IP packet has traversed.

NO.58 IPS devices that are classified as “In-line NIDS” devices use a combination of anomaly analysis, signature-based rules, and what else to identify malicious events on the network?
* Firewall compatibility rules
* Application analysis
* ICMP and UDP active scanning
* MAC address filtering

NO.59 Which of the following processes is known as sanitization?
* Assessing the risk involved in discarding particular information.
* Verifying the identity of a person, network host, or system process.
* Physically destroying the media and the information stored on it.
* Removing the content from the media so that it is difficult to restore.

NO.60 Which of the following proxy servers provides administrative controls over the content?
* Content filtering web proxy server
* Caching proxy server
* Forced proxy server
* Web proxy server

Explanation/Reference:

Pass GIAC GSEC Exam Info and Free Practice Test:
https://www.examcollectionpass.com/GIAC/GSEC-practice-exam-dumps.html]