Digital Forensics Quiz 2

1. Only USE your SVNIT E-mail ID to open google MCQ form/Exam
2. You need to compulsory submit the test/exam before the due/end time. Your response will not be recorded, If you don't submit the test.

EMAIL *

u21cs089@coed.svnit.ac.in

PHONE NUMBER *

7977569777

NAME

Garvit Shah

ADMISSION NUMBER *

U21CS089

Untitled Section

Marks : 20
Questions : 20

What can an attacker do with directory traversal? *

- (●) Once attackers access the root directory, they can enter other parts of the computer system.
- ( ) Attackers can also gain control of access control lists which administrators use to grant various levels of file access to users.
- ( ) They may also be able to read and write arbitrary files on the server enabling them to manipulate applications and associated data, read sensitive information like password files or take control of the server.
- ( ) All of the above

Reason to perform log analysis? *

- ( ) Compliance with security policies
- ( ) System troubleshooting
- ( ) Security incident response
- (●) All of the given

ABC Corp. is an e-commerce company that relies heavily on its online platform for sales. During a major holiday sale event, the company experiences a sudden and significant increase in website traffic. However, shortly after the sale begins, the website becomes unresponsive, and customers start reporting difficulties accessing the site. The IT team suspects a DDoS attack. What is the most appropriate initial step for ABC Corp. to take in response to the suspected DDoS attack? *

- ○ Notify customers about the issue and apologize for the inconvenience.
- ◉ Investigate the network traffic to confirm the presence of a DDoS attack
- ○ Contact the web hosting provider for assistance in handling the increased traffic.
- ○ Implement rate limiting or traffic filtering to mitigate the impact of the attack.

Evidences in a mobile device are *

- ☑ Sim card
- ☑ SD Card
- ☑ Web Browsing
- ☑ IMEI information

SAM uses cryptographic measures to prevent forbidden users to gain access to the system. *

- ◉ True
- ○ False

Choose the correct option *

- (●) Example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.
- ( ) An example of HIDS usage can be seen on mission-critical machines, which are expected to change their layout.
- ( ) An example of APIDS is monitor the SQL protocol explicitly to the middleware as it transacts with the database in the web server.
- ( ) None of the above

A _____ is a series of HTTP requests submitted by a visitor with the maximum time between requests not exceeding a certain amount configured by the webmaster. *

- ( ) Host
- ( ) User agent
- (●) Visit
- ( ) Page

As an investigator, you need to collect data from which sources *

- [x] Hosts
- [x] Routers
- [x] Firewalls
- [x] Switch
- [x] Wifi

When handling computers for legal purposes, investigators increasingly are faced with four main types of problems, except: *

- How to recover data from computers while preserving evidential integrity
- How to keep your data and information safe from theft or accidental loss
- How to securely store and handle recovered data
- How to find the significant information in a large volume of data

What are the correct password cracking methods? *

- Hybrid attack
- Rule based attack
- Dictionary searches
- All of the above

What is meant by the term 'cyber-crime'? *

- Any crime that uses computers to jeopardise or attempt to jeopardise national security
- The use of computer networks to commit financial or identity fraud
- The theft of digital information
- Any crime that involves computers and networks

Which of the following is not a type of volatile evidence *

- [ ] routing tables
- [ ] Main memory
- [x] Log files
- [ ] Cached data

File carving is the process of trying to recover files without this metadata. *

- [x] True
- [ ] False

You own an company and someone has replaced the original content of the website with their own messages and replaced your image with some other image. What possible attack would this be? *

- [ ] Cross site scripting (XSS)
- [x] Web defacement Attack
- [ ] SQL injection
- [ ] Buffer overflow

The process of documenting the seizure of digital evidence and, in particular, when that evidence changes hands, is known as: *

- (●) Chain of custody
- ( ) Field notes
- ( ) Interim report
- ( ) None of the above

Choose the correct option: *
Statement 1 : Local port mirroring involves copying traffic from one switch port to another on the different switch
Statement 2 : Remote port mirroring involves copying traffic from one switch port to another on the same switch

- ( ) Statement 1 is True and Statement 2 is false
- ( ) Statement 1 is False and Statement 2 is True
- ( ) Both statements are true
- (●) Both statements are false

The following are what it really costs to replace a * stolen computer, except:

- ( ) The price of the replacement hardware
- ( ) The price of replacing the software
- ( ) The cost of creating data
- (●) The cost of lost production time or instruction tim

Someone has accessed your Instagram's server and and sent inflammatory information to others under the guise of one of your top managers. This is known as *

- (●) Repudiation
- ( ) Non - Repudiation
- ( ) Privacy attack
- ( ) None of the above

Which of the below is a popular victim of cyber attackers looking to gain the IP address of a target or victim user? *

- (●) emails
- ( ) websites
- ( ) IP tracer
- ( ) web pages

Consider someone wiretap a phone line by cutting into the phone wires outside an individual's home, assuming the wire can be accessed without incident. The type of attack is *

- (●) Eavesdropping
- ( ) Spoofing
- ( ) Phishing
- ( ) Hacking

Google Forms