212-82$^{Q\&As}$

Certified Cybersecurity Technician(C|CT)

QUESTION 1

As a cybersecurity technician, you were assigned to analyze the file system of a Linux image captured from a device that has been attacked recently. Study the forensic image \\'Evidenced.img" in the Documents folder of the "Attacker Machine-1" and identify a user from the image file.

A. smith

B. attacker

C. roger

D. john

Correct Answer: B

Explanation: The attacker is a user from the image file in the above scenario. A file system is a method or structure that organizes and stores files and data on a storage device, such as a hard disk, a flash drive, etc. A file system can have

different types based on its format or features, such as FAT, NTFS, ext4, etc. A file system can be analyzed to extract various information, such as file names, sizes, dates, contents, etc. A Linux image is an image file that contains a copy or a

snapshot of a Linux-based file system . A Linux image can be analyzed to extract various information about a Linux-based system or device . To analyze the file system of a Linux image captured from a device that has been attacked recently

and identify a user from the image file, one has to follow these steps:

Navigate to Documents folder of Attacker Machine-1. Right-click on Evidenced.img file and select Mount option. Wait for the image file to be mounted and assigned a drive letter. Open File Explorer and navigate to the mounted drive. Open

etc folder and open passwd file with a text editor.

Observe the user accounts listed in the file.

The user accounts listed in the file are:

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin

man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/

var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin

nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:

systemd-network:x: systemd-resolve:x: systemd-bus-proxy:x: syslog:x: _apt:x:

messagebus:x: uuidd:x: lightdm:x: whoopsie:x: avahi-autoipd:x: avahi:x: dnsmasq:x:

colord:x: speech-dispatcher:x: hplip:x: kernoops:x: saned:x: nm-openvpn:x: nm- openconnect:x: pulse:x: rtkit:x: sshd:x: attacker::1000 The user account that is not a system or service account is attacker, which is a user from the image file.

QUESTION 2

Sam, a software engineer, visited an organization to give a demonstration on a software tool that helps in business development. The administrator at the organization created a least privileged account on a system and allocated that system to Sam for the demonstration. Using this account, Sam can only access the files that are required for the demonstration and cannot open any other file in the system.

Which of the following types of accounts the organization has given to Sam in the above scenario?

A. Service account

B. Guest account

C. User account

D. Administrator account

Correct Answer: B

Explanation: The correct answer is B, as it identifies the type of account that the organization has given to Sam in the above scenario. A guest account is a type of account that allows temporary or limited access to a system or network for visitors or users who do not belong to the organization. A guest account typically has minimal privileges and permissions and can only access certain files or applications. In the above scenario, the organization has given Sam a guest account for the demonstration. Using this account, Sam can only access the files that are required for the demonstration and cannot open any other file in the system. Option A is incorrect, as it does not identify the type of account that the organization has given to Sam in the above scenario. A service account is a type of account that allows applications or services to run on a system or network under a specific identity. A service account typically has high privileges and permissions and can access various files or applications. In the above scenario, the organization has not given Sam a service account for the demonstration. Option C is incorrect, as it does not identify the type of account that the organization has given to Sam in the above scenario. A user account is a type of account that allows regular access to a system or network for employees or members of an organization. A user account typically has moderate privileges and permissions and can access various files or applications depending on their role. In the above scenario, the organization has not given Sam a user account for the demonstration. Option D is incorrect, as it does not identify the type of account that the organization has given to Sam in the above scenario. An administrator account is a type of account that allows full access to a system or network for administrators or managers of an organization. An administrator account typically has the highest privileges and permissions and can access and modify any files or applications. In the above scenario, the organization has not given Sam an administrator account for the demonstration. References: , Section 4.1

QUESTION 3

An FTP server has been hosted in one of the machines in the network. Using Cain and Abel the attacker was able to poison the machine and fetch the FTP credentials used by the admin. You\\'re given a task to validate the credentials that were stolen using Cain and Abel and read the file flag.txt

A. white@hat

B. red@hat

C. hat@red

D. blue@hat

Correct Answer: C

Explanation: hat@red is the FTP credential that was stolen using Cain and Abel in the above scenario. FTP (File Transfer Protocol) is a protocol that allows transferring files between a client and a server over a network. FTP requires a

username and a password to authenticate the client and grant access to the server . Cain and Abel is a tool that can perform various network attacks, such as ARP poisoning, password cracking, sniffing, etc. Cain and Abel can poison the

machine and fetch the FTP credentials used by the admin by intercepting and analyzing the network traffic . To validate the credentials that were stolen using Cain and Abel and read the file flag.txt, one has to follow these steps:

Navigate to the Documents folder of Attacker-1 machine. Double-click on Cain.exe file to launch Cain and Abel tool.

Click on Sniffer tab.

Click on Start/Stop Sniffer icon.

Click on Configure icon.

Select the network adapter and click on OK button.

Click on + icon to add hosts to scan.

Select All hosts in my subnet option and click on OK button.

Wait for the hosts to appear in the list.

Right-click on 20.20.10.26 (FTP server) and select Resolve Host Name option.

Note down the host name as ftpserver.movieabc.com

Click on Passwords tab.

Click on + icon to add items to list.

Select Network Passwords option.

Select FTP option from Protocol drop-down list.

Click on OK button.

Wait for the FTP credentials to appear in the list. Note down the username as hat and the password as red Open a web browser and type ftp://hat:red@ftpserver.movieabc.com Press Enter key to access the FTP server using the stolen

credentials.

Navigate to flag.txt file and open it.

Read the file content.

QUESTION 4

Gideon, a forensic officer, was examining a victim\\'s Linux system suspected to be involved in online criminal activities. Gideon navigated to a directory containing a log file that recorded information related to user login/logout. This information helped Gideon to determine the current login state of cyber criminals in the victim system, identify the Linux log file accessed by Gideon in this scenario.

A. /va r/l og /mysq Id. log

B. /va r/l og /wt m p

C. /ar/log/boot.iog

D. /var/log/httpd/

Correct Answer: B

Explanation: /var/log/wtmp is the Linux log file accessed by Gideon in this scenario. /var/log/wtmp is a log file that records information related to user login/logout, such as username, terminal, IP address, and login time. /var/log/wtmp can be used to determine the current login state of users in a Linux system. /var/log/wtmp can be viewed using commands such as last, lastb, or utmpdump1. References: Linux Log Files

QUESTION 5

A software company develops new software products by following the best practices for secure application development. Dawson, a software analyst, is responsible for checking the performance of applications in the client\\'s network to determine any issue faced by end users while accessing the application.

Which of the following tiers of the secure application development lifecycle involves checking the application performance?

A. Development

B. Staging

C. Testing

D. Quality assurance (QA)

Correct Answer: C

Explanation: Testing is the tier of the secure application development lifecycle that involves checking the application performance in the above scenario. Secure application development is a process that involves designing, developing, deploying, and maintaining software applications that are secure and resilient to threats and attacks. Secure application development can be based on various models or frameworks, such as SDLC (Software Development Life Cycle), OWASP (Open Web Application Security Project), etc. Secure application development consists of various tiers or stages that perform different tasks or roles. Testing is a tier of the secure application development lifecycle that involves verifying and validating the functionality and security of software applications before releasing them to end users. Testing can include various types of tests, such as unit testing, integration testing, system testing, performance testing, security testing, etc. Testing can be used to check the application performance and identify any errors, bugs, or vulnerabilities in the software applications. In the scenario, a software company develops new software products by following the best practices for secure application development. Dawson, a software analyst, is responsible for checking the performance of applications in the client\\'s network to determine any issue faced by end users while accessing the application. This means that he performs testing for this purpose. Development is a tier of the secure application development lifecycle that involves creating and coding software applications according to the design and specifications. Staging is a tier of the secure application development lifecycle that involves deploying software applications to a simulated or pre-production environment for testing or evaluation purposes. Quality assurance (QA) is a tier of the secure application development lifecycle that involves ensuring that software applications meet the quality standards and expectations of end users and stakeholders