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

Certified Cybersecurity Technician(C|CT)

Pass EC-COUNCIL 212-82 Exam with 100% Guarantee

QUESTION 1

A web application www.movieabc.com was found to be prone to SQL injection attack. You are given a task to exploit the web application and fetch the user credentials. Select the UID which is mapped to user john in the database table.

Note: Username: sam Pass: test

A. 5

B. 3

C. 2

D. 4

Correct Answer: D

Explanation: 4 is the UID that is mapped to user john in the database table in the above scenario. SQL injection is a type of web application attack that exploits a vulnerability in a web application that allows an attacker to inject malicious SQL

statements into an input field, such as a username or password field, and execute them on the database server. SQL injection can be used to bypass authentication, access or modify sensitive data, execute commands, etc. To exploit the web

application and fetch the user credentials, one has to follow these steps:

Open a web browser and type www.movieabc.com

Press Enter key to access the web application.

Enter sam as username and test as password.

Click on Login button.

Observe that a welcome message with username sam is displayed.

Click on Logout button.

Enter sam\\' or `1\\'=\\'1 as username and test as password.

Click on Login button.

Observe that a welcome message with username admin is displayed, indicating that SQL injection was successful.

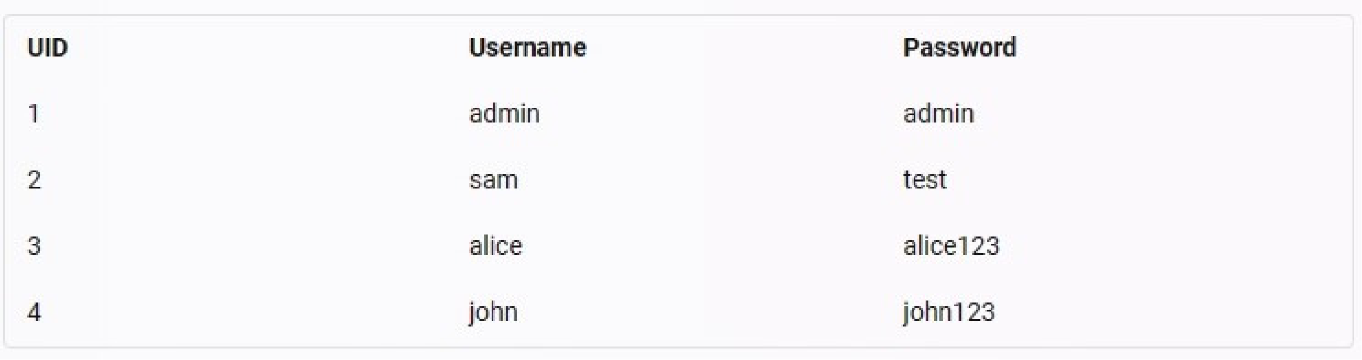
Click on Logout button.

Enter sam\\'; SELECT * FROM users; ?as username and test as password.

Click on Login button.

Observe that an error message with user credentials from users table is displayed.

The user credentials from users table are:



UID	Username	Password
1	admin	admin
2	sam	test
3	alice	alice123
4	john	john123

The UID that is mapped to user john is 4.

QUESTION 2

A software team at an MNC was involved in a project aimed at developing software that could detect the oxygen levels of a person without physical contact, a helpful solution for pandemic situations. For this purpose, the team used a wireless technology that could digitally transfer data between two devices within a short range of up to 5 m and only worked in the absence of physical blockage or obstacle between the two devices, identify the technology employed by the software team in the above scenario.

A. Infrared

B. USB

C. CPS

D. Satcom

Correct Answer: A

Explanation: of

QUESTION 3

Giovanni, a system administrator, was tasked with configuring permissions for employees working on a new project. Hit organization used active directories (ADs) to grant/deny permissions to resources Giovanni created a folder for AD users with the required permissions and added all employees working on the new project in it. Identify the type of account created by Giovanni in this scenario.

A. Third-party account

B. Croup-based account

C. Shared account

D. Application account

Correct Answer: B

Explanation: Group-based account is the type of account created by Giovanni in this scenario. An account is a set of credentials, such as a username and a password, that allows a user to access a system or network. An account can have different types based on its purpose or usage. A group-based account is a type of account that allows multiple users to access a system or network with the same credentials and permissions. A group-based account can be used to simplify the management of users and resources by assigning them to groups based on their roles or functions. In the scenario, Giovanni was tasked with configuring permissions for employees working on a new project. His organization used active directories (ADs) to grant/deny permissions to resources. Giovanni created a folder for AD users with the required permissions and added all employees working on the new project in it. This means that he created a group-based account for those employees. A third-party account is a type of account that allows an external entity or service to access a system or network with limited permissions or scope. A shared account is a type of account that allows multiple users to access a system or network with the same credentials but different permissions. An application account is a type of account that allows an application or software to access a system or network with specific permissions or functions.

QUESTION 4

in a security incident, the forensic investigation has isolated a suspicious file named "security_update.exe". You are asked to analyze the file in the Documents folder of the "Attacker Machine-1" to determine whether it is malicious. Analyze the suspicious file and identify the malware signature.

A. Stuxnet

B. KLEZ

C. ZEUS

D. Conficker

Correct Answer: A

Explanation: Stuxnet is the malware signature of the suspicious file in the above scenario. Malware is malicious software that can harm or compromise the security or functionality of a system or network. Malware can include various types, such as viruses, worms, trojans, ransomware, spyware, etc. Malware signature is a unique pattern or characteristic that identifies a specific malware or malware family. Malware signature can be used to detect or analyze malware by comparing it with known malware signatures in databases or repositories. To analyze the suspicious file and identify the malware signature, one has to follow these steps: Navigate to Documents folder of Attacker Machine-1. Right-click on security_update.exe file and select Scan with VirusTotal option. Wait for VirusTotal to scan the file and display the results. Observe the detection ratio and details. The detection ratio is 59/70, which means that 59 out of 70 antivirus engines detected the file as malicious. The details show that most antivirus engines detected the file as Stuxnet, which is a malware signature of a worm that targets industrial control systems (ICS). Stuxnet can be used to sabotage or damage ICS by modifying their code or behavior. Therefore, Stuxnet is the malware signature of the suspicious file. KLEZ is a malware signature of a worm that spreads via email and network shares. KLEZ can be used to infect or overwrite files, disable antivirus software, or display fake messages. ZEUS is a malware signature of a trojan that targets banking and financial systems. ZEUS can be used to steal or modify banking credentials, perform fraudulent transactions, or install other malware. Conficker is a malware signature of a worm that exploits a vulnerability in Windows operating systems. Conficker can be used to create a botnet, disable security services, or download other malware

QUESTION 5

Identify a machine in the network with 5SH service enabled. Initiate an SSH Connection to the machine, find the file, ttag.txt. in the machine, and enter the tile\\'s content as the answer. The credentials tor SSH login are sam/adm(admin@123.

A. sam@bob

B. bob2@sam

C. sam2@bob D. bobt@sam

Correct Answer: D

Explanation: bob1@sam is the file\\'s content as the answer. To find the machine with SSH service enabled, one can use a network scanning tool such as Nmap to scan the network for port 22, which is the default port for SSH. For example, the command nmap -p 22 192.168.0.0/24 will scan the network range 192.168.0.0/24 for port 22 and display the results2. To initiate an SSH connection to the machine, one can use a command-line tool such as ssh or an SSH client such as PuTTY to connect to the machine using the credentials sam/admin@123. For example, the command ssh sam@192.168.0.10 will connect to the machine with IP address 192.168.0.10 using the username sam and prompt for the password admin@1233. To find the file flag.txt in the machine, one can use a file searching tool such as find or locate to search for the file name in the machine\\'s file system. For example, the command find / -name flag.txt will search for the file flag.txt from the root directory (/) and display its location4. To enter the file\\'s content as the answer, one can use a file viewing tool such as cat or less to display the content of the file flag.txt. For example, the command cat /home/sam/flag.txt will display the content of the file flag.txt located in /home/sam/ directory5. The screenshot below shows an example of performing these steps: ![Screenshot of performing these steps] References: Nmap Tutorial, SSH Tutorial, Find Command Tutorial, Cat Command Tutorial, [Screenshot of performing these steps]