Free Questions for PT0-003 by braindumpscollection

Shared by Moore on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A penetration tester would like to leverage a CSRF vulnerability to gather sensitive details from an application's end users. Which of the following tools should the tester use for this task?

Options:

A- Browser Exploitation Framework

B- Maltego

C- Metasploit

D- theHarvester

Cross-Site Request Forgery (CSRF) vulnerabilities can be leveraged to trick authenticated users into performing unwanted actions on a web application. The right tool for this task would help in exploiting web-based vulnerabilities, particularly those related to web browsers and interactions.

Browser Exploitation Framework (BeEF) (Answer: A):

Answer:

A

Explanation:

Capabilities: BeEF is equipped with modules to create CSRF attacks, capture session tokens, and gather sensitive information from the target user's browser session.

Drawbacks: While useful for reconnaissance, Maltego is not designed for exploiting web vulnerabilities like CSRF.

Metasploit (Option C):

Capabilities: While Metasploit can exploit some web vulnerabilities, it is not specifically tailored for CSRF attacks as effectively as BeEF.

Drawbacks: It does not provide capabilities for exploiting CSRF vulnerabilities.

Conclusion: The Browser Exploitation Framework (BeEF) is the most suitable tool for leveraging a CSRF vulnerability to gather sensitive details from an application's end users. It is specifically designed for browser-based exploitation, making it the best choice for this task.

Maltego (Option B):

theHarvester (Option D):

Question 2

Question Type: **MultipleChoice**

A penetration tester performs a service enumeration process and receives the following result after scanning a server using the Nmap tool:

PORT STATE SERVICE

22/tcp open ssh

25/tcp filtered smtp

111/tcp open rpcbind

2049/tcp open nfs

Based on the output, which of the following services provides the best target for launching an attack?

Options:

A- Database

B- Remote access

C- Email

D- File sharing

Based on the Nmap scan results, the services identified on the target server are as follows:
22/tcp open ssh:
Service: SSH (Secure Shell)
Function: Provides encrypted remote access.
Attack Surface: Brute force attacks or exploiting vulnerabilities in outdated SSH implementations. However, it is generally considered

secure if properly configured.
25/tcp filtered smtp:
Service: SMTP (Simple Mail Transfer Protocol)
Function: Email transmission.
Attack Surface: Potential for email-related attacks such as spoofing, but the port is filtered, indicating that access may be restricted or protected by a firewall.
111/tcp open rpcbind:
Service: RPCBind (Remote Procedure Call Bind)
Function: Helps in mapping RPC program numbers to network addresses.
Attack Surface: Can be exploited in specific configurations, but generally not a primary target compared to others.
2049/tcp open nfs:
Service: NFS (Network File System)
Function: Allows for file sharing over a network.
Attack Surface: NFS can be a significant target for attacks due to potential misconfigurations that can allow unauthorized access to file shares or exploitation of vulnerabilities in NFS services.
Conclusion: The NFS service (2049/tcp) provides the best target for launching an attack. File sharing services like NFS often contain sensitive data and can be vulnerable to misconfigurations that allow unauthorized access or privilege escalation.

Answer:

D

Question 3

Question Type: MultipleChoice

A penetration tester is getting ready to conduct a vulnerability scan as part of the testing process. The tester will evaluate an environment that consists of a container orchestration cluster. Which of the following tools should the tester use to evaluate the cluster?

Options:

A- Trivy

B- Nessus

C- Grype

D- Kube-hunter

Evaluating a container orchestration cluster, such as Kubernetes, requires specialized tools designed to assess the security and configuration of container environments. Here's an analysis of each tool and why Kube-hunter is the best choice:

Trivy (Option A):

Answer:

D

Explanation:

Capabilities: While effective at scanning container images for vulnerabilities, it is not specifically designed to assess the security of a container orchestration cluster itself.

Nessus (Option B):

Capabilities: It is not tailored for container orchestration environments and may miss specific issues related to Kubernetes or other orchestration systems.

Grype (Option C):

Capabilities: Similar to Trivy, it focuses on identifying vulnerabilities in container images rather than assessing the overall security posture of a container orchestration cluster.

Kube-hunter (Answer: D):

Capabilities: It scans the Kubernetes cluster for a wide range of security issues, including misconfigurations and vulnerabilities specific to Kubernetes environments.

Conclusion: Kube-hunter is the most appropriate tool for evaluating a container orchestration cluster, such as Kubernetes, due to its specialized focus on identifying security vulnerabilities and misconfigurations specific to such environments.

Question 4

Question Type: **MultipleChoice**

Which of the following OT protocols sends information in cleartext?

Options:

A- TTEthernet

B- DNP3

C- Modbus

D- PROFINET

Operational Technology (OT) protocols are used in industrial control systems (ICS) to manage and automate physical processes. Here's an analysis of each protocol regarding whether it sends information in cleartext:

TTEthernet (Option A):

Answer:

C

Explanation:

Security: It includes mechanisms for reliable and deterministic data transfer, not typically sending information in cleartext.

DNP3 (Option B):

Security: While the original DNP3 protocol transmits data in cleartext, the DNP3 Secure Authentication extensions provide cryptographic security features.

Modbus (Answer: C):

Security: Modbus transmits data in cleartext, which makes it susceptible to interception and unauthorized access.

Security: PROFINET includes several security features, including support for encryption, which means it doesn't necessarily send information in cleartext.

Conclusion: Modbus is the protocol that most commonly sends information in cleartext, making it vulnerable to eavesdropping and interception.

PROFINET (Option D):

Question 5

Question Type: MultipleChoice

Which of the following post-exploitation activities allows a penetration tester to maintain persistent access in a compromised system?

Options:

A- Creating registry keys

B- Installing a bind shell

C- Executing a process injection

D- Setting up a reverse SSH connection

Answer:

A

Explanation:

Maintaining persistent access in a compromised system is a crucial goal for a penetration tester after achieving initial access. Here's an explanation of each option and why creating registry keys is the preferred method:

Creating registry keys (Answer: A):

Advantages: This method is stealthy and can be effective in maintaining access over long periods, especially on Windows systems.

Example: Adding a new entry to the HKLM\Software\Microsoft\Windows\CurrentVersion\Run registry key to execute a malicious script upon system boot.

Drawbacks: This method is less stealthy and can be easily detected by network monitoring tools. It also requires an open port, which might be closed or filtered by firewalls.

Executing a process injection (Option C):

Drawbacks: While effective for evading detection, it doesn't inherently provide persistence. The injected code will typically be lost when the process terminates or the system reboots.

Setting up a reverse SSH connection (Option D):

Drawbacks: This method can be useful for maintaining a session but is less reliable for long-term persistence. It can be disrupted by network changes or monitoring tools.

Conclusion: Creating registry keys is the most effective method for maintaining persistent access in a compromised system, particularly in Windows environments, due to its stealthiness and reliability.

Installing a bind shell (Option B):

Question 6

Question Type: **MultipleChoice**

Which of the following is the most efficient way to infiltrate a file containing data that could be sensitive?

Options:

A- Use steganography and send the file over FTP

B- Compress the file and send it using TFTP

C- Split the file in tiny pieces and send it over dnscat

D- Encrypt and send the file over HTTPS

Answer:

D

Explanation:

When considering efficiency and security for exfiltrating sensitive data, the chosen method must ensure data confidentiality and minimize the risk of detection. Here's an analysis of each option:

Use steganography and send the file over FTP (Option A):

Drawbacks: FTP is not secure as it transmits data in clear text, making it susceptible to interception. Steganography can add an extra layer of obfuscation, but the use of FTP makes this option insecure.

Compress the file and send it using TFTP (Option B):

Drawbacks: TFTP is inherently insecure because it does not support encryption, making it easy for attackers to intercept the data during transfer.

Split the file in tiny pieces and send it over dnscat (Option C):

Drawbacks: While effective at evading detection by using DNS, splitting the file and managing the reassembly adds complexity. Additionally, large data transfers over DNS can raise suspicion.

Encrypt and send the file over HTTPS (Answer: D):

Advantages: HTTPS is widely used and trusted, making it less likely to raise suspicion. Encryption ensures the data remains confidential during transit.

The use of HTTPS for secure data transfer is a standard practice in cybersecurity, providing both encryption and integrity of the data being transmitted.

Conclusion: Encrypting the file and sending it over HTTPS is the most efficient and secure method for exfiltrating sensitive data, ensuring both confidentiality and reducing the risk of detection.