Vendor: CompTIA

Exam Code:PT0-001

Exam Name: CompTIA PenTest+ Exam

Version: Demo

QUESTION 1

After successfully capturing administrator credentials to a remote Windows machine, a penetration tester attempts to access the system using PSExec but is denied permission. Which of the following shares must be accessible for a successful PSExec connection?

A. IPCS and C$

B. C$ and ADMINS

C. SERVICES and ADMINS

D. ADMINS and IPCS

Correct Answer: B

QUESTION 2

A security analyst was provided with a detailed penetration report, which was performed against the organization\\'s DMZ environment. It was noted on the report that a finding has a CVSS base score of 10.0.

Which of the following levels of difficulty would be required to exploit this vulnerability?

A. Very difficult; perimeter systems are usually behind a firewall.

B. Somewhat difficult; would require significant processing power to exploit.

C. Trivial; little effort is required to exploit this finding.

D. Impossible; external hosts are hardened to protect against attacks.

Correct Answer: C

Reference https://nvd.nist.gov/vuln-metrics/cvss

QUESTION 3

A penetration tester is able to move laterally throughout a domain with minimal roadblocks after compromising a single workstation. Which of the following mitigation strategies would be BEST to recommend in the report? (Select THREE).

A. Randomize local administrator credentials for each machine.

B. Disable remote logons for local administrators.

C. Require multifactor authentication for all logins.

D. Increase minimum password complexity requirements.

E. Apply additional network access control.

F. Enable full-disk encryption on every workstation.

G. Segment each host into its own VLAN.

Correct Answer: CDE

QUESTION 4

When performing active information reconnaissance, which of the following should be tested FIRST before starting the exploitation process?

A. SQLmap

B. TLS configuration

C. HTTP verbs

D. Input fields

Correct Answer: A

QUESTION 5

A security consultant finds a folder in "C VProgram Files" that has writable permission from an unprivileged user account Which of the following can be used to gam higher privileges?

A. Retrieving the SAM database

B. Kerberoasting

C. Retrieving credentials in LSASS

D. DLL hijacking

E. VM sandbox escape

Correct Answer: C

QUESTION 6

At the information gathering stage, a penetration tester is trying to passively identify the technology running on a client\\'s website. Which of the following approached should the penetration tester take?

A. Run a spider scan in Burp Suite.

B. Use web aggregators such as BuiltWith and Netcraft

C. Run a web scraper and pull the website\\'s content.

D. Use Nmap to fingerprint the website\\'s technology.

Correct Answer: A

Reference: https://relevant.software/blog/penetration-testing-for-web-applications/

QUESTION 7

A penetration tester has gained physical access to a facility and connected directly into the internal network. The penetration tester now wants to pivot into the server VLAN. Which of the following would accomplish this?

A. Spoofing a printer\\'s MAC address

B. Abusing DTP negotiation

C. Performing LLMNR poisoning

D. Conducting an STP attack

Correct Answer: D

QUESTION 8

A penetration tester has been asked to conduct OS fingerprinting with Nmap using a company-provide text file that contain a list of IP addresses.

Which of the following are needed to conduct this scan? (Select TWO).

A. -O

B. _iL

C. _sV

D. -sS

E. -oN

F. -oX

Correct Answer: AB

Reference https://securitytrails.com/blog/top-15-nmap-commands-to-scan-remote-hosts#six-scan-hosts-and-ip-addresses-reading-from-a-text-file

---

QUESTION 9

During a penetration test, a tester runs a phishing campaign and receives a shell from an internal PC running Windows 10 OS. The tester wants to perform credential harvesting with Mimikatz.

Which of the following registry changes would allow for credential caching in memory?

A. reg add HKLM\System\ControlSet002\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d

0

B. reg add HKCU\System\CurrentControlSet\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 1

C. reg add HKLM\Software\CurrentControlSet\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 1

D. reg add HKLM\System\CurrentControlSet\Control\SecurityProviders\WDigest /v userLogoCredential /t REG_DWORD /d 1

Correct Answer: A

QUESTION 10

Which of the following are MOST important when planning for an engagement? (Select TWO).

A. Goals/objectives

B. Architectural diagrams

C. Tolerance to impact

D. Storage time for a report

E. Company policies

Correct Answer: AC

QUESTION 11

A penetration tester identifies prebuilt exploit code containing Windows imports for VirtualAllocEx and LoadLibraryA functions. Which of the following techniques is the exploit code using?

A. DLL hijacking

B. DLL sideloading

C. DLL injection

D. DLL function hooking

Correct Answer: A

Reference: https://trustfoundry.net/what-is-dll-hijacking/

QUESTION 12

A penetration tester has a full shell to a domain controller and wants to discover any user account that has not

authenticated to the domain in 21 days. Which of the following commands would BEST accomplish this?

A. dsrm -users "DN=compony.com; OU=hq CN=usera"

B. dsuser -name -account -limit 3

C. dsquery uaer -inactive 3

D. dsquery -o -rein -limit 21

Correct Answer: D

Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

Average 99.9% Success Rate

More than 800,000 Satisfied Customers Worldwide

Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: