BraindumpsQA

http://www.braindumpsqa.com

IT Exam Study materials / Braindumps

Exam : **PT0-001**

Title : CompTIA PenTest+ Certification Exam

Vendor : CompTIA

Version : DEMO

NO.1 An attacker receives a DHCP address and notices the hostname was populated in the corporate DNS server.
Which of the following BEST describes how the attacker can use this information?
A. DCSync operation
B. WPAD attack
C. VLAN hopping
D. Setting custom SRV records
Answer: B

NO.2 A company performed an annual penetration test of its environment.
In addition to several new findings, all of the previously identified findings persisted on the latest report.
Which of the following is the MOST likely reason?
A. Infrastructure is being replaced with similar hardware and software.
B. The organization is not taking action to remediate identified findings.
C. Systems administrators are applying the wrong patches.
D. The penetration testing tools were misconfigured.
Answer: B

NO.3 A security guard observes an individual entering the building after scanning a badge.
The facility has a strict badge-in and badge-out requirement with a turnstile.
The security guard then audits the badge system and finds two log entries for the badge in the following has MOST likely occurred?
A. The employee lost the badge.
B. The system reached the crossover error rate.
C. The physical access control server is malfunctioning.
D. The badge was cloned.
Answer: D

NO.4 A penetration tester observes that several high numbered ports are listening on a public web server.
However, the system owner says the application only uses port 443.
Which of the following would be BEST to recommend?
A. Transition the application to another port
B. Disable unneeded services.
C. Implement a web application firewall
D. Filter port 443 to specific IP addresses
Answer: B

NO.5 When calculating the sales price of a penetration test to a client, which of the following is the MOST important aspect to understand?
A. The operating cost
B. The required scope of work
C. The non-disclosure agreement

D. The client's budget
Answer: B

NO.6 A penetration tester has been asked to conduct OS fingering with Nmap using a company-provided text file that contains a list of IP addresses. Which of the following are needed to conduct this scan? (Choose two.).
A. -oX
B. -O
C. -iL
D. -V
E. oN
F. -sS
Answer: C,E
Explanation:
Reference https://securitytrails.com/blog/top-15-nmap-commands-to-scan-remote-hosts#six-scan-hosts-and-ip-addresses-reading-from-a-text-file

NO.7 Which of the following commands will allow a tester to enumerate potential unquoted services paths on a host?
A. wmic service get /format:hform > c:\temp\services.html
B. wmic service get name, displayname, patchname, startmode | findstr /i "auto" | findstr /i /v "c:\windows\\" | findstr /i /v """
C. wmic startup get caption, location, command | findstr /i "service" | findstr /v /i "%"
D. wmic environment get name, variablevalue, username / findstr /i "Path" | findstr /i "service"
Answer: B
Reference:
c7a011a8d8ae

NO.8 A penetration tester is required to perform OSINT on staff at a target company after completing the infrastructure aspect. Which of the following would be the BEST step for the penetration tester to take?
A. Obtain staff information by calling the company and using social engineering techniques.
B. Send spoofed emails to staff to see if staff will respond with sensitive information.
C. Visit the client and use impersonation to obtain information from staff.
D. Search the Internet for information on staff such as social networking sites.
Answer: D

NO.9 A penetration tester attempts to perform a UDP port scan against a remote target using an Nmap tool installed onto a non-Kali Linux image. For some reason, the UDP scan falls to start. Which of the following would MOST likely help to resolve the issue?
A. Enable both IPv4 and IPv6 forwarding.
B. Install the latest version of the tool.
C. Review local iptables for existing drop rules.
D. Relaunch the tool with elevated privileges.

Answer: A

NO.10 A penetration tester reviews the scan results of a web application. Which of the following vulnerabilities is MOST critical and should be prioritized for exploitation?
A. Clickjacking
B. Expired certificate
C. Stored XSS
D. Fill path disclosure
Answer: C
Explanation:
References https://www.owasp.org/index.php/Top_10_2010-A2-Cross-Site_Scripting_(XSS)

NO.11 A penetration tester is performing a code review. Which of the following testing techniques is being performed?
A. Dynamic analysis
B. Fuzzing analysis
C. Static analysis
D. Run-time analysis
Answer: C

NO.12 A web application scanner reports that a website is susceptible to clickjacking. Which of the following techniques would BEST prove exploitability?
A. Redirect the user with a CSRF.
B. Pull server headers.
C. Launch the website in an iFRAME.
D. Capture and replay a session I
Answer: C

NO.13 A penetration tester has discovered through automated scanning that a Tomcat server allows for the use of default credentials. Using default credentials, the tester is able to upload WAR files to the server. Which of the following is the MOST likely post-exploitation step?
A. Connect via SSH using default credentials.
B. Monitor network traffic
C. Install web shell on the server.
D. Upload a customized /etc/shadow file.
Answer: C

NO.14 Which of the following would be BEST for performing passive reconnaissance on a target's external domain?
A. OpenVAS
B. CeWL
C. Shodan
D. Peach

Answer: C

NO.15 Which of the following describe a susceptibility present in Android-based commercial mobile devices when organizations are not employing MDM services? (Choose two.)
A. The default device log facility does not record system actions.
B. Unsigned apps can be installed.
C. End users have root access to devices by default.
D. IPSec VPNs are not configurable.
E. Push notification services require Internet access.
F. Configurations are user-customizable.
Answer: B,F

NO.16 A penetration tester locates a few unquoted service paths during an engagement. Which of the following can the tester attempt to do with these?
A. Attempt DLL hijacking attacks.
B. Attempt to locate weak file and folder permissions.
C. Attempt to crack the service account passwords.
D. Attempt privilege escalation attacks.
Answer: D

NO.17 A penetration tester has compromised a host. Which of the following would be the correct syntax to create a Netcat listener on the device?
A. nc -l -p 4444 /bin/bash
B. nc -lp 4444 -e /bin/bash
C. nc -vp 4444 /bin/bash
D. nc -p 4444 /bin/bash
Answer: A

NO.18 A penetration tester needs to use Nmap to scan a host with a very low speed so the WAF or IPS/IDS is not triggered. Which of the following command-line parameters should be added to the Nmap command?
A. -t 1
B. -t 5
C. -sV
D. -sP 10
Answer: A

NO.19 During an internal penetration test, several multicast and broadcast name resolution requests are observed traversing the network. Which of the following tools could be used to impersonate network resources and collect authentication requests?
A. Responder
B. Medusa
C. Tcpdump

D. Ettercap
Answer: A

NO.20 A company requested a penetration tester review the security of an in-house-developed Android application. The penetration tester received an APK file to support the assessment. The penetration tester wants to run SAST on the APK file. Which of the following preparatory steps must the penetration tester do FIRST? (Select TWO)
A. Convert JAR files to DEX
B. Cross-compile the application
C. Re-sign the APK
D. Decompile
E. Attach to ADB
F. Convert to JAR
Answer: D

NO.21 A penetration tester has successfully exploited an application vulnerability and wants to remove the command history from the Linux session. Which of the following will accomplish this successfully?
A. history -c
B. rm -f ./history
C. history --remove
D. cat history I clear
Answer: A

NO.22 Prior to a security assessment of a company's user population via spear phishing, which of the following is the MOST appropriate method to de-escalate any incidents or consequences?
A. Determine the appropriate format and content of the spear-phishing emails.
B. Provide limited but necessary communication prior to the assessment.
C. Carefully prioritize the list of targeted users, excluding high value targets.
D. Send follow-up communication to spear-phishing targets to notify of the assessment.
Answer: A

NO.23 After gaining initial low-privilege access to a Linux system, a penetration tester identifies an interesting binary in a user's folder titled "changepass"
-sr -xr -x 1 root root 6443 Oct 18 2017 /home/user/changepass
Using "strings" to print ASCII printable characters from changepass, the tester notes the following:
$ strings changepass
Exit
setuid
strmp
GLINC _2.0
ENV_PATH
%s/changepw
malloc

strlen
Given this information, which of the following is the MOST likely path of exploitation to achieve root privileges on the machines?

A. Run changepass within the current directory with sudo after exporting the ENV_PATH environmental variable to the path of '/usr/local/bin'

B. Export the ENV_PATH environmental variable to the path of a writable directory that contains a token-stealing binary title changepw

C. Copy changepass to a writable directory and export the ENV_PATH environmental variable to the path of a token-stealing binary titled changepw. Then run changepass

D. Create a copy of changepass in the same directory, naming it changpw. Export the ENV_PATH environmental variable to the path "/home/user'. Then run changepass

Answer: A

NO.24 During a physical security review, a detailed penetration testing report was obtained, which was issued to a security analyst and then discarded in the trash. The report contains validated critical risk exposures. Which of the following processes would BEST protect this information from being disclosed in the future?

A. Require only electronic copies of all documents to be maintained.

B. Install surveillance cameras near all garbage disposal areas.

C. Restrict access to physical copies to authorized personnel only.

D. Ensure corporate policies include guidance on the proper handling of sensitive information.

Answer: D

NO.25 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. Segment each host into its own VLAN.

B. Apply additional network access control.

C. Disable remote logons for local administrators.

D. Enable full-disk encryption on every workstation.

E. Randomize local administrator credentials for each machine.

F. Increase minimum password complexity requirements.

G. Require multifactor authentication for all logins.

Answer: A,F,G