[Lead2pass New Lead2pass EC-Council 312-50v9 Exam Dumps Free Download (361-380)

Lead2pass 2017 November New EC-Council 312-50v9 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! The EC-Council 312-50v9 PDF, 312-50v9 VCE and 312-50v9 exam questions and answers at Lead2pass are written and prepared by EC-Council affiliated trainers and lecturers with decades of experience in the IT field. This ensures that you are equipped with the latest and most current information to give you a better chance of passing the EC-Council 312-50v9 exam. Following questions and answers are all new published by EC-Council Official Exam Center: https://www.lead2pass.com/312-50v9.html QUESTION 361 What is the best Nmap command to use when you want to list all devices in the same network quickly after you successfully identified a server whose IP address is 10.10.0.5? A. nmap -T4 -F 10.10.0.0/24B. nmap -T4 -q 10.10.0.0/24C. nmap -T4 -O 10.10.0.0/24D. nmap -T4 -r 10.10.1.0/24Answer: C QUESTION 362You've just discovered a server that is currently active within the same network with the machine you recently compromised. You ping it but it did not respond. What could be the case? A. TCP/IP doesn't support ICMPB. ARP is disabled on the target serverC. ICMP could be disabled on the target serverD. You need to run the ping command with root privileges Answer: C QUESTION 363What tool should you use when you need to analyze extracted metadata from files you collected when you were in the initial stage of penetration test (information gathering)? A. ArmitageB. DimitryC. MetagoofilD. cdpsnarf Answer: C QUESTION 364Which of the following is NOT an ideal choice for biometric controls? A. Iris patternsB. FingerprintsC. Height and weightD. Voice Answer: C QUESTION 365While you were gathering information as part of security assessments for one of your clients, you were able to gather data that show your client is involved with fraudulent activities. What should you do? A. Immediately stop work and contact the proper legal authoritiesB. Ignore the data and continue the assessment until completed as agreedC. Confront the client in a respectful manner and ask her about the dataD. Copy the data to removable media and keep it in case you need it Answer: A QUESTION 366In order to prevent particular ports and applications from getting packets into an organization, what does a firewall check? A. Network layer headers and the session layer port numbersB. Presentation layer headers and the session layer port numbersC. Application layer port numbers and the transport layer headersD. Transport layer port numbers and application layer headers Answer: D QUESTION 367 Suppose you've gained access to your client's hybrid network. On which port should you listen to in order to know which Microsoft Windows workstations has its file sharing enabled? A. 1433B. 161C. 445D. 3389 Answer: C QUESTION 368Which of the following BEST describes the mechanism of a Boot Sector Virus? A. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBRB. Moves the MBR to another location on the RAM and copies itself to the original location of the MBRC. Overwrites the original MBR and only executes the new virus codeD. Modifies directory table entries so that directory entries point to the virus code instead of the actual program Answer: A QUESTION 369What is the term coined for logging, recording and resolving events in a company? A. Internal ProcedureB. Security PolicyC. Incident Management ProcessD. Metrics Answer: C QUESTION 370XOR is a common cryptographic tool. 10110001 XOR 00111010 is? A. 10111100B. 11011000C. 10011101D. 10001011 Answer: D QUESTION 371A server has been infected by a certain type of Trojan. The hacker intended to utilize it to send and host junk mails. What type of Trojan did the hacker use? A. Turtle Trojans B. Ransomware TrojansC. Botnet TrojanD. Banking Trojans Answer: C QUESTION 372First thing you do every office day is to check your email inbox. One morning, you received an email from your best friend and the subject line is quite strange. What should you do? A. Delete the email and pretend nothing happened.B. Forward the message to your supervisor and ask for her opinion on how to handle the situation.C. Forward the message to your company's security response team and permanently delete the message from your computer.D. Reply to the sender and ask them for more information about the message contents. Answer: C QUESTION 373LM hash is a compromised password hashing function. Which of the following parameters describe LM Hash:? I. The maximum password length is 14 characters.II. There are no distinctions between uppercase and lowercase. III. It's a simple algorithm, so 10,000,000 hashes can be generated per second. A. IB. I, II, and IIIC. IID. I and II Answer: BExplanation: QUESTION 374Defining rules, collaborating human workforce, creating a backup plan, and testing the plans are within what phase of the Incident Handling Process? A. Preparation phaseB. Containment phaseC. Recovery phaseD. Identification phase Answer: A QUESTION 375Which of the following BEST describes how Address Resolution Protocol (ARP) works? A. It sends a reply packet for a specific IP, asking for the MAC addressB. It sends a reply packet to all the network elements, asking for the MAC address from a specific IPC. It sends a request packet to all the network elements, asking for the domain name from a specific IPD. It sends a request packet to all the network elements, asking for the MAC address from a specific IP Answer: D QUESTION 376Which of the following is a form of penetration testing that relies heavily on human interaction and often involves tricking people into breaking normal security procedures? A. Social EngineeringB. PiggybackingC. TailgatingD.

Eavesdropping Answer: A QUESTION 377What tool and process are you going to use in order to remain undetected by an IDS while pivoting and passing traffic over a server you've compromised and gained root access to? A. Install and use Telnet to encrypt all outgoing traffic from this server.B. Install Cryptcat and encrypt outgoing packets from this server.C. Use HTTP so that all traffic can be routed via a browser, thus evading the internal Intrusion Detection Systems.D. Use Alternate Data Streams to hide the outgoing packets from this server. Answer: B QUESTION 378You've just gained root access to a Centos 6 server after days of trying. What tool should you use to maintain access? A. Disable Key ServicesB. Create User AccountC. Download and Install NetcatD. Disable IPTables Answer: B QUESTION 379What type of malware is it that restricts access to a computer system that it infects and demands that the user pay a certain amount of money, cryptocurrency, etc. to the operators of the malware to remove the restriction? A. RansomwareB. RiskwareC. AdwareD. Spyware Answer: A QUESTION 380The following are types of Bluetooth attack EXCEPT_____? A. BluejackingB. BluesmakingC. BluesnarfingD. Bluedriving Answer: D More free Lead2pass 312-50v9 exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDTVZJRHRvblhycms Lead2pass guarantees your 312-50v9 exam success with our exam resources. Our 312-50v9 braindumps are the latest and developed by experienced IT certification professionals working in today's prospering companies and data centers. All our 312-50v9 braindumps include 312-50v9 real exam questions which guarantee your 100% success of 312-50v9 exam in your first try. 2017 EC-Council 312-50v9 (All 589 Q&As) exam dumps (PDF&VCE) from Lead2pass: https://www.lead2pass.com/312-50v9.html [100% Exam Pass Guaranteed]