Free Download Latest 2014 Pass4sure&Lead2pass CompTIA SY0-401 Dumps (231-240)

QUESTION 231 During a penetration test from the Internet, Jane, the system administrator, was able to establish a connection to an internal router, but not successfully log in to it. Which ports and protocols are MOST likely to be open on the firewall? (Select FOUR). A.   21 B.   22 C.   23 D.   69 E.   3389 F.   SSH G.   Terminal services H.   Rlogin I.   Rsync J.   Telnet Answer: BCFJ QUESTION 232 Which of the following is an application security coding problem? A.   Error and exception handling B.   Patch management C.   Application hardening D.   Application fuzzing Answer: A QUESTION 233 An IT security technician needs to establish host based security for company workstations. Which of the following will BEST meet this requirement? A.   Implement IIS hardening by restricting service accounts. B.   Implement database hardening by applying vendor guidelines. C.   Implement perimeter firewall rules to restrict access. D.   Implement OS hardening by applying GPOs. Answer: D QUESTION 234 Which of the following is the MOST specific plan for various problems that can arise within a system? A.   Business Continuity Plan B.   Continuity of Operation Plan C.   Disaster Recovery Plan D.   IT Contingency Plan Answer: D QUESTION 235 Which of the following BEST describes the weakness in WEP encryption? A.   The initialization vector of WEP uses a crack-able RC4 encryption algorithm. Once enough packets are captured an XOR operation can be performed and the asymmetric keys can be derived. B.   The WEP key is stored in plain text and split in portions across 224 packets of random data. Once enough packets are sniffed the IV portion of the packets can be removed leaving the plain text key. C.   The WEP key has a weak MD4 hashing algorithm used. A simple rainbow table can be used to generate key possibilities due to MD4 collisions. D.   The WEP key is stored with a very small pool of random numbers to make the cipher text. As the random numbers are often reused it becomes easy to derive the remaining WEP key. Answer: D QUESTION 236 Sara, the Chief Security Officer (CSO), has had four security breaches during the past two years. Each breach has cost the company $3,000. A third party vendor has offered to repair the security hole in the system for $25,000. The breached system is scheduled to be replaced in five years. Which of the following should Sara do to address the risk? A.   Accept the risk saving $10,000. B.   Ignore the risk saving $5,000. C.   Mitigate the risk saving $10,000. D.   Transfer the risk saving $5,000. Answer: D QUESTION 237 Which of the following is an authentication and accounting service that uses TCP for connecting to routers and switches? A.   DIAMETER B.   RADIUS C.   TACACS+ D.   Kerberos Answer: C QUESTION 238 Which of the following can BEST help prevent cross-site scripting attacks and buffer overflows on a production system? A.   Input validation B.   Network intrusion detection system C.   Anomaly-based HIDS D.   Peer review Answer: A QUESTION 239 Pete, an IT Administrator, needs to secure his server room. Which of the following mitigation methods would provide the MOST physical protection? A.   Sign in and sign out logs B.   Mantrap C.   Video surveillance D.   HVAC Answer: B QUESTION 240 Which of the following should be connected to the fire alarm system in order to help prevent the spread of a fire in a server room without data loss to assist in an FM-200 deployment? A.   Water base sprinkler system B.   Electrical C.   HVAC D.   Video surveillance Answer: C If you want to pass CompTIA SY0-401 successfully, donot missing to read latest lead2pass CompTIA SY0-401 dumps. If you can master all lead2pass questions you will able to pass 100% guaranteed.
http://www.lead2pass.com/SY0-401.html