312-50V11 Q&As

Certified Ethical Hacker v11 Exam

Pass EC-COUNCIL 312-50V11 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/312-50v11.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

A company\\'s policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as display filter to find unencrypted file transfers?

A. tcp.port = = 21

B. tcp.port = 23

C. tcp.port = = 21 | | tcp.port = =22

D. tcp.port ! = 21

Correct Answer: A

QUESTION 2

in this form of encryption algorithm, every Individual block contains 64-bit data, and three keys are used, where each key consists of 56 bits. Which is this encryption algorithm?

A. IDEA

B. Triple Data Encryption standard

C. MDS encryption algorithm

D. AES

Correct Answer: B

Triple DES is another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. In Stealth, you merely type within the entire 192-bit (24 character) key instead of entering each of the three keys individually. The Triple DES DLL then breaks the user-provided key into three subkeys, padding the keys if necessary in order that they are each 64 bits long. The procedure for encryption is strictly an equivalent as regular DES, but it\\'s repeated 3 times , hence the name Triple DES. the info is encrypted with the primary key, decrypted with the second key, and eventually encrypted again with the third key.Triple DES runs 3 times slower than DES, but is far safer if used properly. The procedure for decrypting something is that the same because the procedure for encryption, except it\\'s executed in reverse. Like DES, data is encrypted and decrypted in 64-bit chunks. Although the input key for DES is 64 bits long, the particular key employed by DES is merely 56 bits long . the smallest amount significant (rightmost) bit in each byte may be a parity , and will be set in order that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most vital bits of every byte are used, leading to a key length of 56 bits. this suggests that the effective key strength for Triple DES is really 168 bits because each of the three keys contains 8 parity bits that aren\\'t used during the encryption process.Triple DES ModesTriple ECB (Electronic Code Book)?This variant of Triple DES works precisely the same way because the ECB mode of DES.?this is often the foremost commonly used mode of operation.Triple CBC (Cipher Block Chaining)?This method is extremely almost like the quality DES CBC mode.?like Triple ECB, the effective key length is 168 bits and keys are utilized in an equivalent manner, as described above, but the chaining features of CBC mode also are employed.?the primary 64-bit key acts because the Initialization Vector to DES.?Triple ECB is then executed for one 64-bit block of plaintext.?The resulting ciphertext is then XORed with subsequent plaintext block to be encrypted, and therefore the procedure is repeated.?This method adds an additional layer of security to Triple DES and is therefore safer than Triple ECB, although it\\'s not used as widely as Triple ECB.

QUESTION 3

Bill is a network administrator. He wants to eliminate unencrypted traffic inside his company\\'s network. He

decides to setup a SPAN port and capture all traffic to the datacenter. He immediately discovers

unencrypted traffic in port UDP 161.

what protocol is this port using and how can he secure that traffic?

A. it is not necessary to perform any actions, as SNMP is not carrying important information.

B. SNMP and he should change it to SNMP V3

C. RPC and the best practice is to disable RPC completely

D. SNMP and he should change it to SNMP v2, which is encrypted

Correct Answer: B

We have various articles already in our documentation for setting up SNMPv2 trap handling in Opsview, but SNMPv3 traps are a whole new ballgame. They can be quite confusing and complicated to set up the first time you go through the process, but when you understand what is going on, everything should make more sense. SNMP has gone through several revisions to improve performance and security (version 1, 2c and 3). By default, it is a UDP port based protocol where communication is based on a `fire and forget\\' methodology in which network packets are sent to another device, but there is no check for receipt of that packet (versus TCP port when a network packet must be acknowledged by the other end of the communication link). There are two modes of operation with SNMP ?get requests (or polling) where one device requests information from an SNMP enabled device on a regular basis (normally using UDP port 161), and traps where the SNMP enabled device sends a message to another device when an event occurs (normally using UDP port 162). The latter includes instances such as someone logging on, the device powering up or down, or a wide variety of other problems that would need this type of investigation. This blog covers SNMPv3 traps, as polling and version 2c traps are covered elsewhere in our documentation. SNMP trapsSince SNMP is primarily a UDP port based system, traps may be `lost\\' when sending between devices; the sending device does not wait to see if the receiver got the trap. This means if the configuration on the sending device is wrong (using the wrong receiver IP address or port) or the receiver isn\\'t listening for traps or rejecting them out of hand due to misconfiguration, the sender will never know. The SNMP v2c specification introduced the idea of splitting traps into two types; the original `hope it gets there\\' trap and the newer `INFORM\\' traps. Upon receipt of an INFORM, the receiver must send an acknowledgement back. If the sender doesn\\'t get the acknowledgement back, then it knows there is an existing problem and can log it for sysadmins to find when they interrogate the device.

QUESTION 4

Attacker Rony Installed a rogue access point within an organization\\'s perimeter and attempted to Intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack. What is the type of vulnerability assessment performed by Johnson in the above scenario?

A. Distributed assessment

B. Wireless network assessment

C. Most-based assessment

D. Application assessment

Correct Answer: B

Expanding your network capabilities are often done well using wireless networks, but it also can be a source of harm to your data system . Deficiencies in its implementations or configurations can allow tip to be accessed in an unauthorized manner.This makes it imperative to closely monitor your wireless network while also conducting periodic Wireless Network assessment.It identifies flaws and provides an unadulterated view of exactly how vulnerable your systems are to malicious and unauthorized accesses.Identifying misconfigurations and inconsistencies in wireless implementations and rogue access points can improve your security posture and achieve compliance with regulatory frameworks.

QUESTION 5

What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?

A. 110

B. 135

C. 139

D. 161

E. 445

F. 1024

Correct Answer: BCE