Exam Code: 642-553

Exam Name: Implementing Cisco Intrusion Prevention System (IPS)

Vendor: CISCO

Version: DEMO

2: Which method is of gaining access to a system that bypasses normal security measures?
A.Creating a back door
B.Starting a Smurf attack
C.Conducting social engineering
D.Launching a DoS attack
Correct Answers: A

This question is to examine the methods of sabotaging network security.
3: Which statement is true about a Smurf attack?
A.It sends ping requests to a subnet, requesting that devices on that subnet send ping replies to a target system.
B.It intercepts the third step in a TCP three-way handshake to hijack a session.
C.It uses Trojan horse applications to create a distributed collection of "zombie" computers, which can be used to launch a coordinated DDoS attack.
D.It sends ping requests in segments of an invalid size.
Correct Answers: A

5: Which one is the most important based on the following common elements of a network design?
A.Business needs
B.Best practices
C.Risk analysis
D.Security policy
Correct Answers: A

6: What are four methods used by hackers? (Choose four.)
A.Social engineering attack
B.Trojan horse attack
C.Front door attacks
D.Buffer Unicode attack
E.Privilege escalation attack
F.Footprint analysis attack
Correct Answers: A B E F

7: For the following options, which feature is the foundation of Cisco Self-Defending Network technology?
A.policy management
B.secure connectivity
C.threat control and containment
D.secure network platform
Correct Answers: D

9: Which item is the great majority of software vulnerabilities that have been discovered?
A.Stack vulnerabilities

B.Software overflows
C.Heap overflows
D.Buffer overflows
Correct Answers: D

10: What will be enabled by the scanning technology-The Dynamic Vector Streaming (DVS)?
A.Firmware-level virus detection
B.Layer 4 virus detection
C.Signature-based spyware filtering
D.Signature-based virus filtering
Correct Answers: C

11: Which statement is not a reason for an organization to incorporate a SAN in its enterprise infrastructure?
A.To increase the performance of long-distance replication, backup, and recovery
B.To decrease the threat of viruses and worm attacks against data storage devices
C.To decrease both capital and operating expenses associated with data storage
D.To meet changing business priorities, applications, and revenue growth
Correct Answers: B