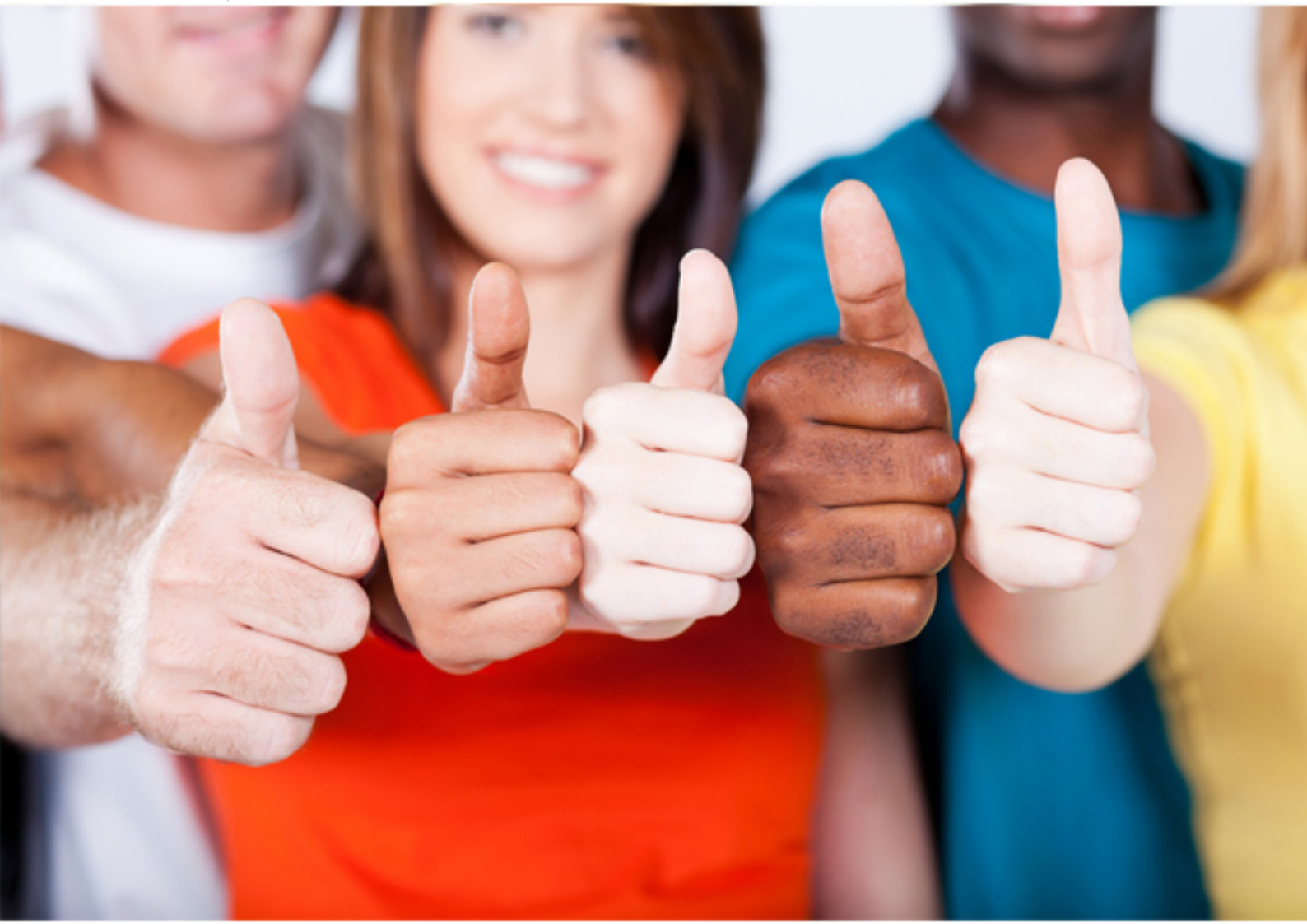
QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

SY0-501 Dumps
SY0-501 Braindumps
SY0-501 Real Questions
SY0-501 Practice Test
SY0-501 dumps free



CompTIA

SY0-501

CompTIA Security+

Question: 847

Which of the following documents would provide specific guidance regarding ports and protocols that should be disabled on an operating system?

A. Regulatory requirements
B. Secure configuration guide
C. Application installation guides
D. User manuals

Answer: B

Question: 848

A security analyst is investigating a call from a user regarding one of the websites receiving a 503: Service Unavailable error. The analyst runs a netstat-an command to discover if the web server is up and listening. The analyst receives the following output: TCP 10.1.5.2:80 192.168.2.112:60973 TIME_WAIT TCP 10.1.5.2:80 192.168.2.112:60974 TIME_WAIT TCP 10.1.5.2:80 192.168.2.112:60975 TIME_WAIT TCP 10.1.5.2:80 192.168.2.112:60976 TIME_WAIT TCP 10.1.5.2:80 192.168.2.112:60977 TIME_WAIT TCP 10.1.5.2:80 192.168.2.112:60978 TIME_WAIT Which of the following types of attack is the analyst seeing?

A. Buffer overflow
B. Domain hijacking
C. Denial of service
D. ARP poisoning

Answer: C

Question: 849

Which of the following serves to warn users against downloading and installing pirated software on company devices?

A. AUP
B. NDA
C. ISA
D. BPA

Answer: A

Question: 850

An organization wants to set up a wireless network in the most secure way. Budget is not a major consideration, and the organization is willing to accept some

complexity when clients are connecting. It is also willing to deny wireless connectivity for clients who cannot be connected in the most secure manner. Which of the following would be the MOST secure setup that conforms to the organization's requirements?

A. Enable WPA2-PSK for older clients and WPA2-Enterprise for all other clients.
B. Enable WPA2-PSK, disable all other modes, and implement MAC filtering along with port security.
C. Use WPA2-Enterprise with RADIUS and disable pre-shared keys.
D. Use WPA2-PSK with a 24-character complex password and change the password monthly.

Answer: C

Question: 851

A first responder needs to collect digital evidence from a compromised headless virtual host. Which of the following should the first responder collect FIRST?

A. Virtual memory
B. BIOS configuration
C. Snapshot
D. RAM

Answer: C

Question: 852

Which of the following BEST explains the difference between a credentialed scan and a non-credentialed scan?

A. D. credentialed scan sees the system the way an authorized user sees the system, while a non-credentialed scan sees the system as a guest.
B. A credentialed scan will not show up in system logs because the scan is running with the necessary authorization, while non-credentialed scan activity will appear in the logs.
C. A credentialed scan generates significantly more false positives, while a non-credentialed scan generates fewer false positives.
D. A credentialed scan sees the system the way an authorized user sees the system, while a non-credentialed scan sees the system as a guest.

Answer: D

Question: 853

Using a one-time code that has been texted to a smartphone is an example of:

A. something you have.
B. something you know.
C. something you do.
D. something you are.

Answer: A

Question: 854

The exploitation of a buffer-overrun vulnerability in an application will MOST likely lead to:

A. arbitrary code execution.
B. resource exhaustion.
C. exposure of authentication credentials.
D. dereferencing of memory pointers.

Answer: A

Question: 855

A security professional wants to test a piece of malware that was isolated on a user's computer to document its effect on a system. Which of the following is the FIRST step the security professional should take?

A. Create a sandbox on the machine.
B. Open the file and run it.
C. Create a secure baseline of the system state.
D. Harden the machine.

Answer: C

Question: 856

In highly secure environments where the risk of malicious actors attempting to steal data is high, which of the following is the BEST reason to deploy Faraday cages?

A. To provide emanation control to prevent credential harvesting
B. To minimize signal attenuation over distances to maximize signal strength
C. To minimize external RF interference with embedded processors
D. To protect the integrity of audit logs from malicious alteration
F. C. To minimize external Rinterference with embedded processors

Answer: C

Question: 857

Which of the following is the proper use of a Faraday cage?

A. To block electronic signals sent to erase a cell phone
B. To capture packets sent to a honeypot during an attack
C. To protect hard disks from access during a forensics investigation

D. To restrict access to a building allowing only one person to enter at a time

Answer: A

Question: 858

A security administrator found the following piece of code referenced on a domain controller's task scheduler: $var = GetDomainAdmins If $var != "ÿfabio' SetDomainAdmins = NULL - With which of the following types of malware is the code associated?

A. RAT
B. Backdoor
C. Logic bomb
D. Crypto-malware

Answer: C

Question: 859

An email recipient is unable to open a message encrypted through PKI that was sent from another organization. Which of the following does the recipient need to decrypt the message?

A. The sender's private key
B. The recipient's private key
C. The recipient's public key
D. The CA's root certificate
E. The sender's public key
F. An updated CRL

Answer: E

Question: 860

An employee opens a web browser and types a URL into the address bar. Instead of reaching the requested site, the browser opens a completely different site. Which of the following types of attacks have MOST likely occurred? (Choose two.)

A. DNS hijacking
B. Cross-site scripting
C. Domain hijacking
D. Man-in-the-browser
E. Session hijacking

Answer: A,E

For More exams visit https://killexams.com/vendors-exam-list