

QUESTIONS & ANSWERS

Kill your exam at first Attempt



ST0-095 Dumps
ST0-095 Braindumps
ST0-095 Real Questions
ST0-095 Practice Test
ST0-095 dumps free



Symantec

ST0-095

*Symantec Technical Foundations- Security(R) Solutions
1.0*



QUESTION: 132

A cybercriminal is trying to get a foothold into an organization by exploiting a weakness in their web servers. What is the most common website vulnerability that can be used by cybercriminals?

- A. limited user accounts
- B. default credentials
- C. open shares
- D. excessive directory access rights

Answer: B

QUESTION: 133

Which global trade does the United States Federal Bureau of Investigation (FBI) say is smaller than the global market for illegally-obtained information, according to the Security Solutions 1.0 course?

- A. illegal drug trade
- B. arms trafficking trade
- C. human trafficking trade
- D. money laundering trade

Answer: A

QUESTION: 134

Which method would a cybercriminal most likely use in a drive-by download?

- A. spam with an attachment
- B. whaling with a link to click on
- C. SQL injection
- D. cross-site request forgery

Answer: D

QUESTION: 135

What is the most common method bots use to extract data?

- A. RSS

- B. IRC
- C. FTP
- D. P2P

Answer: C

QUESTION: 136

Which method did the MetaFisher bot use to extract data from a system?

- A. RSS
- B. FTP
- C. peer to peer
- D. IRC

Answer: B

QUESTION: 137

A cybercriminal wants to maintain future access to a compromised system. Which tool would the cybercriminal incorporate into malware to accomplish this?

- A. rootkit
- B. keylogger
- C. backdoor
- D. screen scraper

Answer: C

QUESTION: 138

Malware that contains a backdoor is placed on a system that will later be used by the cybercriminal to gain access to the system. The cybercriminal was successful in which phase of the breach?

- A. capture
- B. discovery
- C. incursion
- D. exfiltration

Answer: C

QUESTION: 139

According to the Symantec research shared in the Security Solutions 1.0 course, which group is the number one source of IT security attacks?

- A. corporate competitors
- B. organized criminals
- C. well-meaning insiders
- D. malicious insiders

Answer: B

QUESTION: 140

Why would a cybercriminal avoid using a trojan if they were trying to infect a lot of systems?

- A. Trojans are easily caught by antivirus products.
- B. End-users are aware of clicking on non-trusted executables
- C. Trojans only infect one system at a time.
- D. Trojans rarely carry payloads.

Answer: C

QUESTION: 141

An employee has become disgruntled with their employer, a payroll software manufacturer, and one of the employee's friends works for a competitor. The employee copies some highly- confidential source code to a USB drive and gives the USB drive to their friend after work. Which source(s) of a breach are involved in this scenario?

- A. malicious insider only
- B. organized criminal only
- C. malicious insider and organized criminal
- D. well-meaning insider and malicious insider

Answer: A

QUESTION: 142

Which type of attack does a cybercriminal use to convince individuals to respond with sensitive information?

- A. phishing
- B. malware
- C. cross-scripting
- D. spam

Answer: D



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



Kill your exam at First Attempt....Guaranteed!