

# T estpassport Q&A



---

*La meilleure qualité le meilleur service*

<http://www.testpassport.fr>

Service de mise à jour gratuit pendant un an

**Exam** : **ST0-192**

**Title** : Symantec Technical  
Foundations: Security  
Solutions 2.0 Technical  
Assessment

**Version** : DEMO

1.Which group is the number one source of IT security attacks according to the Symantec research shared in the Security Solutions 2.0 course?

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

**Answer: B**

2.Which global trade is determined by the United States Federal Bureau of Investigation (FBI) to be smaller than the global market for illegally-obtained information, according to the Security Solutions 2.0 course?

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

**Answer: A**

3.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**

4.The security team of a major government agency discovers a breach involving employee data that has been leaked outside the agency. They discover that a software developer for the agency transferred employee data from a secure primary system to a secondary system, for the purpose of software development and testing. This secondary system was the target of a hacker.

Which type of breach source(s) is this?

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

**Answer: C**

5.What is the cybercriminal hoping to accomplish during the incursion phase?

- A.obtain authorized access to data or a system
- B.gain unauthorized access to data or a system
- C.use social media sites to gather information on the target
- D.perform scans to identify targets in the environment

**Answer: B**

6. Malware that contains a backdoor is placed on a system that will later be used by the cybercriminal to gain access to the system.

Which phase of the breach does this represent?

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

**Answer: C**

7. A cybercriminal wants to maintain future access to a compromised system.

Which tool would the cybercriminal use to accomplish this?

- A. rootkit
- B. keylogger
- C. backdoor
- D. trojan

**Answer: C**

8. A cybercriminal wants to break into an organization using a SQL injection attack.

What will the cybercriminal do to start the attack?

- A. initiate port scanning
- B. locate a user input field on the company's web page
- C. gain administrative access to the database
- D. identify database version

**Answer: B**

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

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

**Answer: C**

10. What is the leading root cause for successful malicious attacks?

- A. guest user access
- B. default system configurations
- C. exposed network configurations
- D. ineffective security software

**Answer: B**

11. 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 cybercriminals can use?

- A. guest user accounts

- B.default credentials
- C.open shares
- D.excessive directory access rights

**Answer: B**

12.Which method does the MetaFisher bot use to extract data from a system?

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

**Answer: B**

13.What does a cybercriminal insert into a web page to perform a cross-site scripting attack?

- A.client side scripts
- B.Java applications
- C.server side scripts
- D.Flash-based applications

**Answer: A**

14.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**

15.Why would a cybercriminal avoid using a trojan in a widespread attack?

- 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.execution of trojans are dependent on the operating system

**Answer: C**

16.What are the three types of scans used to identify systems?

- A.port, network, and vulnerability
- B.protocol, hardware, and services
- C.port, network, and protocol
- D.hardware, network, and vulnerability

**Answer: A**

17.Which type of attack would be most successful against the password T63k#s23A?

- A.cross site scripting
- B.brute-force
- C.keyword

D.special character guessing

**Answer: B**

18.Which condition would require performing a remote exploit on a machine?

- A.presence of a malicious insider
- B.end-users leaking sensitive data
- C.unpatched system
- D.anonymous FTP login allowed

**Answer: C**

19.Which properly illustrates the basic steps of exploit hacking?

- A.phishing, breaking in, and looting
- B.taking inventory, breaking in, and phishing
- C.port scanning, breaking in, and looting
- D.escalation of privileges, breaking in, and looting

**Answer: C**

20.What properly describes the process of generating password hashes?

- A.taking a cryptographic algorithm and running it through a password
- B.taking a user name and running it through an exploit
- C.taking a password and running it through a cryptographic algorithm
- D.taking a user name and running it through a remote debugger

**Answer: C**