

# EC0-479

## ECCouncil

### EC-Council Certified Security Analyst (ECSA)

*OfficialCerts.com is a reputable IT certification examination guide, study guides and audio exam provider. We ensure that you pass your EC0-479 exam in first attempt and also get high scores to acquire ECCouncil certification.*

*If you use OfficialCerts EC0-479 Certification questions and answers, you will experience actual EC0-479 exam questions/answers. We know exactly what is needed and have all the exam preparation material required to pass the exam. Our ECCouncil exam prep covers over 95% of the questions and answers that may be appeared in your EC0-479 exam. Every point from pass4sure EC0-479 PDF, EC0-479 review will help you take ECCouncil EC0-479 exam much easier and become ECCouncil certified.*

*Here's what you can expect from the OfficialCerts ECCouncil EC0-479 course:*

- \* Up-to-Date ECCouncil EC0-479 questions as experienced in the real exam.*
- \* 100% correct ECCouncil EC0-479 answers you simply can't find in other EC0-479 courses.*
- \* All of our tests are easy to download. Your file will be saved as a EC0-479 PDF.*
- \* ECCouncil EC0-479 brain dump free content featuring the real EC0-479 test questions.*

*ECCouncil EC0-479 certification exam is of core importance both in your Professional life and ECCouncil certification path. With ECCouncil certification you can get a good job easily in the market and get on your path for success. Professionals who passed ECCouncil EC0-479 exam training are an absolute favorite in the industry.*

*You will pass ECCouncil EC0-479 certification test and career opportunities will be open for you.*

<http://news.ift.org/?newsid=exams.asp?examcode=EC0-479>



**QUESTION: 1**

When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

- A. Passive IDS
- B. Active IDS
- C. Progressive IDS
- D. NIPS

**Answer: B**

**QUESTION: 2**

Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr commands using DIG. What is Simon trying to accomplish here?

- A. Send DOS commands to crash the DNS servers
- B. Perform DNS poisoning
- C. Perform a zone transfer
- D. Enumerate all the users in the domain

**Answer: C**

**QUESTION: 3**

What will the following command produce on a website login page?

```
SELECT email, passwd, login_id, full_name
```

```
FROM members
```

```
WHERE email = 'someone@somehwere.com'; DROP TABLE members; --'
```

- A. Deletes the entire members table
- B. Inserts the Error! Reference source not found. email address into the members table
- C. Retrieves the password for the first user in the members table
- D. This command will not produce anything since the syntax is incorrect

**Answer: A**

**QUESTION: 4**

You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall

changes are to blame. What ports should you open for SNMP to work through Firewalls (Select 2)

- A. 162
- B. 161
- C. 163
- D. 160

**Answer:** A, B

**QUESTION: 5**

You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities: `<script>alert("This is a test.")</script>`. When you type this and click on search, you receive a pop-up window that says: "This is a test." What is the result of this test?

- A. Your website is vulnerable to CSS
- B. Your website is not vulnerable
- C. Your website is vulnerable to SQL injection
- D. Your website is vulnerable to web bugs

**Answer:** A

**QUESTION: 6**

If an attacker's computer sends an IPID of 31400 to a zombie computer on an open port in IDLE scanning, what will be the response?

- A. The zombie will not send a response
- B. 31402
- C. 31399
- D. 31401

**Answer:** D

**QUESTION: 7**

Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state

are these ports?

- A. Closed
- B. Open
- C. Stealth
- D. Filtered

**Answer: B**

**QUESTION: 8**

You are assisting a Department of Defense contract company to become compliant with the stringent security policies set by the DoD. One such strict rule is that firewalls must only allow incoming connections that were first initiated by internal computers. What type of firewall must you implement to abide by this policy?

- A. Packet filtering firewall
- B. Circuit-level proxy firewall
- C. Application-level proxy firewall
- D. Statefull firewall

**Answer: D**

**QUESTION: 9**

Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?

- A. Tracert
- B. Smurf scan
- C. Ping trace
- D. ICMP ping sweep

**Answer: D**

**QUESTION: 10**

You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing passive footprinting against their Web servers. What tool should you use?

## OfficialCerts.com Certification Exam Full Version Features;

- Verified answers researched by industry experts.
- Exams **updated** on regular basis.
- Questions, Answers are downloadable in **PDF** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success **Guarantee**.
- **Fast**, helpful support 24x7.

View list of All exams we offer;

<http://www.officialcerts.com/allexams.asp>

To contact our Support;

<http://www.officialcerts.com/support.asp>

View FAQs

<http://www.officialcerts.com/faq.asp>

Download All Exams Samples

<http://www.officialcerts.com/samples.asp>

To purchase Full Version and updated exam;

<http://www.officialcerts.com/allexams.asp>



Shop now using **PayPal**



3COM	CompTIA	Filemaker	IBM	LPI	OMG	Sun
ADOBE	ComputerAssociates	Fortinet	IISFA	McAfee	Oracle	Sybase
APC	CWNP	Foundry	Intel	McData	PMI	Symantec
Apple	DELL	Fujitsu	ISACA	Microsoft	Polycom	TeraData
BEA	ECCouncil	GuidanceSoftware	ISC2	Mile2	RedHat	TIA
BICSI	EMC	HDI	ISEB	NetworkAppliance	Sair	Tibco
CheckPoint	Enterasys	Hitachi	ISM	Network-General	SASInstitute	TruSecure
Cisco	ExamExpress	HP	Juniper	Nokia	SCP	Veritas
Citrix	Exin	Huawei	Legato	Nortel	See-Beyond	Vmware
CIW	ExtremeNetworks	Hyperion	Lotus	Novell	Google	

*You have made the*  
**Right Choice**

You are becoming member of most comprehensive, accurate, highest quality and lowest cost certification resource in the world.

