312-50

ECCouncil
Certified Ethical Hacker

Thousands of IT Professionals before you have already passed their 312-50 certification exams using the ECCouncil 312-50 Practice Exam from ipass4sure.com. Once you start using our 312-50 exam questions you simply can't stop! You are guaranteed to pass your ECCouncil 312-50 test with ease and in your first attempt.

Here's what you can expect from the ipass4sure ECCouncil 312-50 course:

* Up-to-Date ECCouncil 312-50 questions designed to familiarize you with the real exam.
* 100% correct ECCouncil 312-50 answers you simply can't find in other 312-50 courses.
* All of our tests are easy to download. Your file will be saved as a 312-50 PDF.
* ECCouncil 312-50 brain dump free content featuring the real 312-50 test questions.

ECCouncil 312-50 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 312-50 Certification Exam are an absolute favorite in the industry. If you pass ECCouncil 312-50 Certification Exam then career opportunities are open for you.

Our 312-50 Questions & Answers provide you an easy solution to your ECCouncil 312-50 Exam Preparation. Our 312-50 Q&As contains the most updated ECCouncil 312-50 real tests. You can use our 312-50 Q&As on any PC with most versions of Acrobat Reader and prepare the exam easily.

QUESTION 1:

What is the essential difference between an 'Ethical Hacker' and a 'Cracker'?

A. The ethical hacker does not use the same techniques or skills as a cracker.
B. The ethical hacker does it strictly for financial motives unlike a cracker.
C. The ethical hacker has authorization from the owner of the target.
D. The ethical hacker is just a cracker who is getting paid.

Answer: C

Explanation: The ethical hacker uses the same techniques and skills as a cracker and the motive is to find the security breaches before a cracker does. There is nothing that says that a cracker does not get paid for the work he does, a ethical hacker has the owners authorization and will get paid even if he does not succeed to penetrate the target.

QUESTION 2:

What does the term "Ethical Hacking" mean?

A. Someone who is hacking for ethical reasons.
B. Someone who is using his/her skills for ethical reasons.
C. Someone who is using his/her skills for defensive purposes.
D. Someone who is using his/her skills for offensive purposes.

Answer: C

Explanation: Ethical hacking is only about defending your self or your employer against malicious persons by using the same techniques and skills.

QUESTION 3:

Who is an Ethical Hacker?

A. A person whohacksfor ethical reasons
B. A person whohacksfor an ethical cause
C. A person whohacksfor defensive purposes
D. A person whohacksfor offensive purposes

Answer: C

Explanation: The Ethical hacker is a security professional who applies his hacking skills for defensive purposes.

QUESTION 4:

What is "Hacktivism"?

A. Hacking for a cause
B. Hacking ruthlessly
C. An association which groups activists
D. None of the above

Answer: A

Explanation: The term was coined by author/critic Jason Logan Bill Sack in an article about media artist Shu Lea Cheang. Acts of hacktivism are carried out in the belief that proper use of code will have leveraged effects similar to regular activism or civil disobedience.

QUESTION 5:

Where should a security tester be looking for information that could be used by an attacker against an organization? (Select all that apply)

A. CHAT rooms
B. WHOIS database
C. News groups
D. Web sites
E. Search engines
F. Organization's own web site

Answer: A, B, C, D, E, F

Explanation: A Security tester should search for information everywhere that he/she can access. You never know where you find that small piece of information that could penetrate a strong defense.

QUESTION 6:

What are the two basic types of attacks?(Choose two.

A. DoS
B. Passive
C. Sniffing
D. Active
E. Cracking

Answer: B, D

Explanation: Passive and active attacks are the two basic types of attacks.

QUESTION 7:

You are footprinting Acme.com to gather competitive intelligence. You visit the acme.com websire for contact information and telephone number numbers but do not find it listed there. You know that they had the entire staff directory listed on their website 12 months ago but now it is not there. How would it be possible for you to retrieve information from the website that is outdated?

A. Visit google search engine and view the cached copy.
B. Visit Archive.org site to retrieve the Internet archive of the acme website.
C. Crawl the entire website and store them into your computer.
D. Visit the company's partners and customers website for this information.

Answer: B

Explanation: The Internet Archive (
IA) is a non-profit organization dedicated to maintaining an archive of Web and multimedia resources. Located at the Presidio in San Francisco, California, this archive includes "snapshots of the World Wide Web" (archived copies of pages, taken at various points in time), software, movies, books, and audio recordings (including recordings of live concerts from bands that allow it). This site is found at www.archive.org.

QUESTION 8:

User which Federal Statutes does FBI investigate for computer crimes involving e-mail scams and mail fraud?

A. 18 U.S.C 1029 Possession of Access Devices
B. 18 U.S.C 1030 Fraud and related activity in connection with computers
C. 18 U.S.C 1343 Fraud by wire, radio or television
D. 18 U.S.C 1361 Injury to Government Property
E. 18 U.S.C 1362 Government communication systems
F. 18 U.S.C 1831 Economic Espionage Act
G. 18 U.S.C 1832 Trade Secrets Act

Answer: B

Explanation:
http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001030----000-.html

---

QUESTION 9:

Which of the following activities will NOT be considered as passive footprinting?

A. Go through the rubbish to find out any information that might have been discarded.
B. Search on financial site such as Yahoo Financial to identify assets.
C. Scan the range of IP address found in the target DNS database.
D. Perform multiples queries using a search engine.

Answer: C

Explanation:
Passive footprinting is a method in which the attacker never makes contact with the target systems. Scanning the range of IP addresses found in the target DNS is considered making contact to the systems behind the IP addresses that is targeted by the scan.

QUESTION 10:

Which one of the following is defined as the process of distributing incorrect Internet Protocol (IP) addresses/names with the intent of diverting traffic?

A. Network aliasing
B. Domain Name Server (DNS) poisoning
C. Reverse Address Resolution Protocol (ARP)
D. Port scanning

Answer: B

Explanation:
This reference is close to the one listed DNS poisoning is the correct answer.
This is how DNS DOS attack can occur. If the actual DNS records are unattainable to the attacker for him to alter in this fashion, which they should be, the attacker can insert this data into the cache of there server instead of replacing the actual records, which is referred to as cache poisoning.

QUESTION 11:

You are footprinting an organization to gather competitive intelligence. You visit the company's website for contact information and telephone numbers but do not find it listed there. You know that they had the entire staff directory listed on their website 12 months ago but not it is not there.
How would it be possible for you to retrieve information from the website that is outdated?

A. Visit google's search engine and view the cached copy.
B. Visit Archive.org web site to retrieve the Internet archive of the company's website.
C. Crawl the entire website and store them into your computer.

D. Visit the company's partners and customers website for this information.

Answer: B

Explanation: Archive.org mirrors websites and categorizes them by date and month depending on the crawl time. Archive.org dates back to 1996, Google is incorrect because the cache is only as recent as the latest crawl, the cache is over-written on each subsequent crawl. Download the websiteis incorrect because that's the same as what you see online. Visiting customer partners websites is just bogus. The answer is then Firmly, C, archive.org

---

QUESTION 12:

A Certkiller security System Administrator is reviewing the network system log files.
He notes the following:
- Network log files are at 5 MB at 12:00 noon.
- At 14:00 hours, the log files at 3 MB.
What should he assume has happened and what should he do about the situation?

A. He should contact the attacker's ISP as soon as possible and have the connection disconnected.
B. He should log the event as suspicious activity, continue to investigate, and take further steps according to site security policy.
C. He should log the file size, and archive the information, because the router crashed.
D. He should run a file system check, because the Syslog server has a self correcting file system problem.
E. He should disconnect from the Internet discontinue any further unauthorized use, because an attack has taken place.

Answer: B

Explanation: You should never assume a host has been compromised without verification. Typically, disconnecting a server is an extreme measure and should only be done when it is confirmed there is a compromise or the server contains such sensitive data that the loss of service outweighs the risk. Never assume that any administrator or automatic process is making changes to a system. Always investigate the root cause of the change on the system and follow your organizations security policy.

QUESTION 13:

To what does "message repudiation" refer to what concept in the realm of email security?

A. Message repudiation means a user can validate which mail server or servers a message was passed through.

Pass4sure $89 Lifetime Membership Features;

- Pass4sure $89 Lifetime Membership includes Over **2100** Exams in One Price.
- **All** Pass4sure Questions and Answers are included in $89 package.
- **All** Pass4sure audio exams are included **free** in $89 package (See List).
- **All** Pass4sure study guides are included **free** in $89 package (See List).
- **Lifetime** login access, no hidden fee, no login expiry.
- **Free updates** for Lifetime.
- **Free Download Access** to All new exams added in future.
- Accurate answers with explanations (If applicable).
- Verified answers researched by industry experts.
- Study Material **updated** on regular basis.
- Questions, Answers and Study Guides are downloadable in **PDF** format.
- Audio Exams are downloadable in **MP3** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success *Guarantee*.
- **Fast**, helpful support 24x7.

View list of All exams (Q&A) provided in $89 membership;
http://www.ipass4sure.com/allexams.asp

View list of All Study Guides (SG) provided FREE for members;
http://www.ipass4sure.com/study-guides.asp

View list of All Audio Exams (AE) provided FREE for members;
http://www.ipass4sure.com/audio-exams.asp

Download All Exams Sample QAs.
http://www.ipass4sure.com/samples.asp

To purchase $89 Lifetime Full Access Membership click here (One time fee)
https://www.regnow.com/softsell/nph-softsell.cgi?item=30820-3

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	SNIA	

and many others.. See complete list Here