312-50Q&As

Ethical Hacker Certified

Pass EC-COUNCIL 312-50 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/312-50.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

_____ will let you assume a users identity at a dynamically generated web page or site.

A. SQL attack

B. Injection attack

C. Cross site scripting

D. The shell attack

E. Winzapper

Correct Answer: C

Cross site scripting is also referred to as XSS or CSS. You must know the user is online and you must scam that user into clicking on a link that you have sent in order for this hack attack to work.

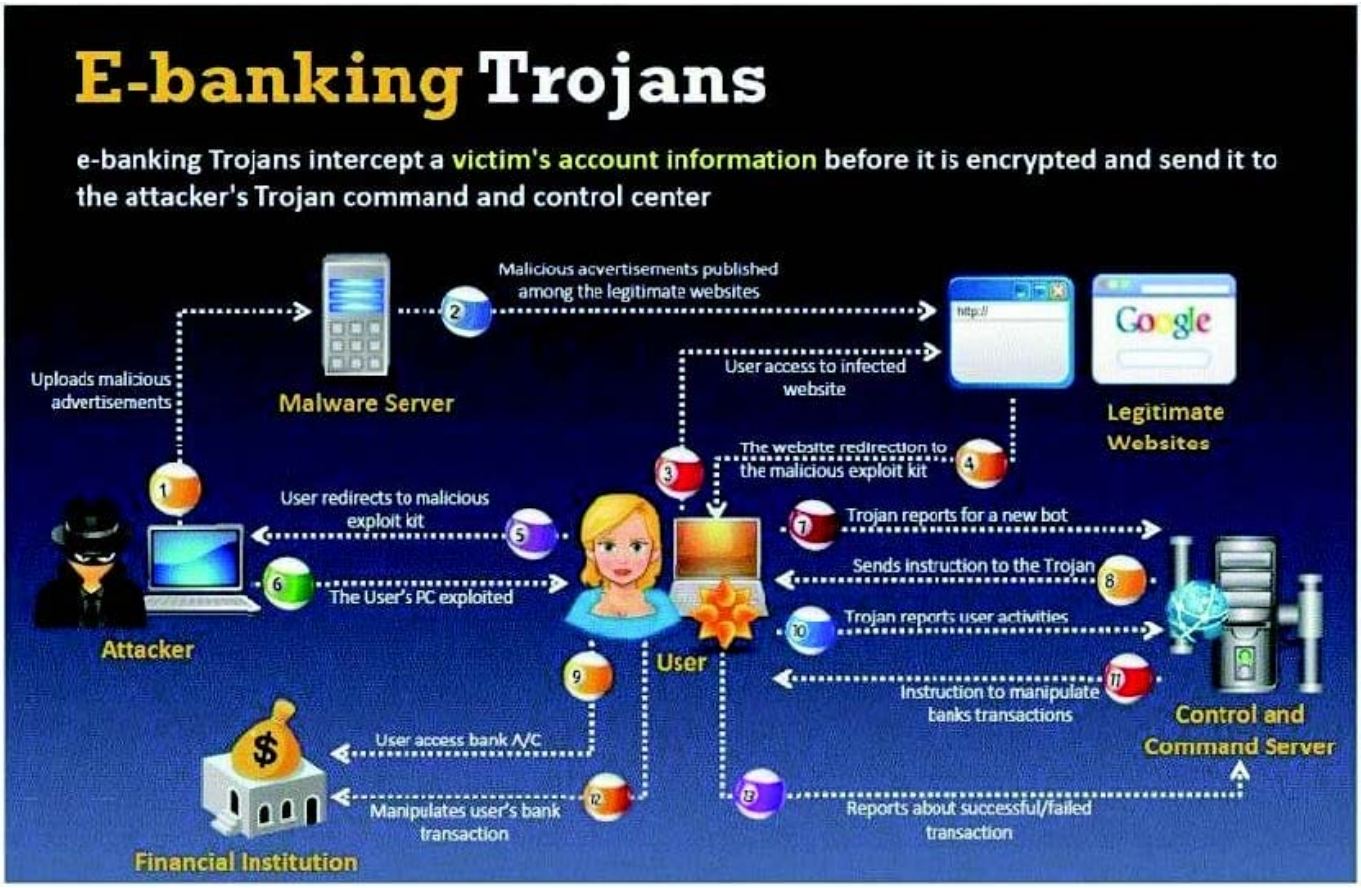
QUESTION 2

BankerFox is a Trojan that is designed to steal users\\' banking data related to certain banking entities.

When they access any website of the affected banks through the vulnerable Firefox 3.5 browser, the Trojan is activated and logs the information entered by the user. All the information entered in that website will be logged by the Trojan and

transmitted to the attacker\\'s machine using covert channel.

BankerFox does not spread automatically using its own means. It needs an attacking user\\'s intervention in order to reach the affected computer.



What is the most efficient way an attacker located in remote location to infect this banking Trojan on a victim\\'s machine?

A. Physical access - the attacker can simply copy a Trojan horse to a victim\\'s hard disk infecting the machine via Firefox add-on extensions

B. Custom packaging - the attacker can create a custom Trojan horse that mimics the appearance of a program that is unique to that particular computer

C. Custom packaging - the attacker can create a custom Trojan horse that mimics the appearance of a program that is unique to that particular computer

D. Custom packaging - the attacker can create a custom Trojan horse that mimics the appearance of a program that is unique to that particular computer

E. Downloading software from a website? An attacker can offer free software, such as shareware programs and pirated mp3 files

Correct Answer: E

QUESTION 3

Who is an Ethical Hacker?

A. A person who hacks for ethical reasons

B. A person who hacks for an ethical cause

C. A person who hacks for defensive purposes

D. A person who hacks for offensive purposes

Correct Answer: C

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

QUESTION 4

According to the CEH methodology, what is the next step to be performed after footprinting?

A. Enumeration

B. Scanning

C. System Hacking

D. Social Engineering

E. Expanding Influence

Correct Answer: B

Once footprinting has been completed, scanning should be attempted next. Scanning should take place on two distinct levels: network and host.

QUESTION 5

#define MAKE_STR_FROM_RET(x) ((x)and0xff), (((x)and0xff00)8), (((x)and0xff0000)16), (((x)and0xff000000)24) char infin_loop[]=

/* for testing purposes */

"\xEB\xFE";

char bsdcode[] =

/* Lam3rZ chroot() code rewritten for FreeBSD by venglin */
"\x31\xc0\x50\x50\x50\xb0\x7e\xcd\x80\x31\xdb\x31\xc0\x43" "\x43\x53\x4b\x53\x53\xb0\x5a\xcd\x80
\xeb\x77\x5e\x31\xc0" "\x8d\x5e\x01\x88\x46\x04\x66\x68\xff\xff\x01\x53\x53

\xb0" "\x88\xcd\x80\x31\xc0\x8d\x5e\x01\x53\x53\xb0\x3d\xcd\x80" "\x31\xc0\x31\xdb
\x8d\x5e\x08\x89\x43\x02\x31\xc9\xfe\xc9" "\x31\xc0\x8d\x5e\x08\x53\x53\xb0\x0c\xcd\x80\xfe\xc9\x75"
"\xf1\x31\xc0\x88\x46\x09\x8d\x5e\x08\x53\x53\xb0

\x3d \xcd" "\x80\xfe\x0e\xb0\x30\xfe\xc8\x88\x46\x04\x31\xc0\x88\x46"
"\x07\x89\x76\x08\x89\x46\x0c\x89\xf3\x8d\x4e\x08\x8d\x56" "\x0c\x52\x51\x53\x53\xb0\x3b\xcd
\x80\x31\xc0\x31\xdb\x53" "\x53\xb0\x01\xcd\x80\xe8\x84\xff\xff\xff\xff\x01

\xff\xff\x30" "\x62\x69\x6e\x30\x73\x68\x31\x2e\x2e\x31\x31\x76\x65\x6e" "\x67\x6c\x69 \x6e";static int magic[MAX_MAGIC],magic_d[MAX_MAGIC]; static char *magic_str=NULL;

int before_len=0;

char *target=NULL, *username="user", *password=NULL;

struct targets getit;

The following exploit code is extracted from what kind of attack?

A. Remote password cracking attack

B. SQL Injection

C. Distributed Denial of Service

D. Cross Site Scripting

E. Buffer Overflow

Correct Answer: E

This is a buffer overflow with it\\'s payload in hex format.