EC-Council 312-92

EC-Council Certified Secure Programmer (ECSP)

Version: 4.0

QUESTION NO: 1

Harold is programming an application that needs to be incorporate data encryption. Harold decides to utilize an encryption algorithm that uses 4-bit working registers instead of the usual 2-bit working registers. What encryption algorithm has Harold decided to use?

A. Blowfish
B. RC5
C. RC4
D. RC6

Answer: D
Explanation:

QUESTION NO: 2

What security package is implemented with the following code?

```
dwStatus = DsMakSpn
(
“ldap”,
“MyServer.Mydomain.com”,
NULL,
0,
NULL,
&pcSpnLength,
pszSpn
);
rpcStatus = RpcServerRegisterAuthInfo
(
psz
RPC_C_AUTHN_GSS_NEGOTIATE,
NULL,
```

NULL

);

A. Diffie-Hellman encryption
B. Repurposing
C. SSPI
D. SMDT

Answer: A
Explanation:

QUESTION NO: 3

Steve is using the libcap library to create scripts for capturing and analyzing network traffic.

Steve has never used libcap before and is struggling with finding out the correct functions to use. Steve is trying to pick the default network interface in his script and does not know which function to use. Which function would he use to correctly choose the default interface in the script?

A. pcap_open_live
B. pcap_int_default
C. pcap_lookupdev
D. pcap_use_int

Answer: C
Explanation:

QUESTION NO: 4

Processes having the “CAP_NET_BIND_SERVICE” can listen on which ports?

A. Any TCP port over 1024
B. Any UDP port under 1024
C. Any TCP port under 1024
D. Any UDP port over 1024

Answer: C
Explanation:

QUESTION NO: 5

David is an applications developer working for Dewer and Sons law firm in Los Angeles David just completed a course on writing secure code and was enlightened by all the intricacies of how code must be rewritten many times to ensure its security. David decides to go through all the applications he has written and change them to be more secure. David comes across the following snippet in one of his programs:

```
#include <stdio.h>

int main(int argc, char **argv)

{

int number = 5;

printf(argv[1]);

putchar('\n');

printf("number (%p) is equal to %d\n",

&value, value);

}
```

What could David change, add, or delete to make this code more secure?

A. Change putchar('\n') to putchar("%s", '\n')
B. Change printf(argv[1]) to printf("%s", argv[1])
C. Change printf(argv[1]) to printf(constv [0])
D. Change int number = 5 to const number = ""

Answer: B
Explanation:

QUESTION NO: 6

Which Linux command will securely delete a file by overwriting its contents?

A. rm –rf /
B. Shred
C. ps –rm
D. del –rm

Answer: B

Explanation:

QUESTION NO: 7

Shayla is designing a web-based application that will pass data to and from a company extranet. This data is very sensitive and must be protected at all costs. Shayla will use a digital certificate and a digital signature to protect the data. The digital signature she has chosen to use is based on the difficulty in computing discrete logarithms. Which digital signature has she chosen?

A. Rabin
B. Diffie-Hellman
C. SA-PSS
D. ElGamal

Answer: D

Explanation:

QUESTION NO: 8

After learning from an external auditor that his code was susceptible to attack, George decided to rewrite some of his code to look like the following. What is George preventing by changing the code?

```
public voif doContent(...) {

...

String s;

if ((s = getUsernameByID(“userid”)) != null) {

s = StringUtils.encodeToHTML(s, 50);

response.write(“<br>Applicant:<u>” + s +

“</u>”);

}

...

}
```

A. Query string manipulation
B. XSS attack
C. Cookie poisoning
D. SQL injection

Answer: B
Explanation:

QUESTION NO: 9

Fred is planning on using the windows socket application ClientApp.exe program to create a client-side application that his employees will use. This program will access backend programs from two different remote sites over WAN connections. If Fred does not make any modifications to the ClientApp.exe default settings, what port must he have the network engineer open in order for the application to communicate?

A. 21
B. 23
C. 25
D. 80

Answer: D
Explanation:

QUESTION NO: 10

What would be the result of the following code?

```
#include <stdio.h>

#include <stdlib.h>

int main(int argc, char *argv[])

{

char *input=malloc(20);

char *output=malloc(20);

strcpy(output, “normal output”);

strcpy(input, argv[1]);
```

```
printf("input at %p: %s\n", input, input);

printf("output at %p: %s\n", output, output);

printf("\n\n%s\n", output);

}
```

A. Stack buffer overflow
B. Heap overflow
C. Query string manipulation
D. Pointer Subterfuge

Answer: B
Explanation:

QUESTION NO: 11

Wayne is a gaming software developer for a large video gaming company in Los Angeles. Wayne has just completed developing a new action/adventure game for the company that is to be released soon. To protect the company's copyright on the game, Wayne would like to incorporate a technology that will restrict the use of the digital files by controlling access, altering, sharing, copying, printing, and saving. What technology does Wayne want to use?

A. ARM
B. WRM
C. DRM
D. Diffusion

Answer: C
Explanation:

QUESTION NO: 12

Kenny is the CIO for Fredrickson Entertainment, a gaming software company in Omaha. The developers in Kenny's company have just finished creating a 3D first person shooter game that will be released to the market within the next couple of months. Kenny is trying to decide what type of license or activation code structure they should use for the game to prevent piracy and protect their product. Kenny decides to go with an approach that will allow each sold copy to be activated online up to five times because he knows his users might have multiple PCs or might need to reinstall the product at some point.

What type of activation policy has Kenny decided to go with?

A. Loose license enforced – reasonable use
B. License terms enforced – fair use
C. Strict license terms enforced
D. Monitor only mode

Answer: A
Explanation:

QUESTION NO: 13

John is creating a website using ASP. John's web pages will have a number of calculations, so he decides to create an include file that the pages will call so he does not have to rewrite the formula numerous times. John's website will be hosted by a server running IIS. John wants to ensure that the include source code is not revealed when the pages are viewed, so he gives the include an .asp extension.

When IIS processes the include file, which system file will be used to hide the include source code?

A. ASP.dll
B. Include.dll
C. IISASP.dll
D. IIS.dll

Answer: A
Explanation:

QUESTION NO: 14

Devon is an applications developer that just got back from a conference on how to correctly write code. Devon has a number of programs he has written that access data across WAN links, so he is particularly concerned about their security. Devon writes a script in C++ to check the security of the programs running on his internal servers. What will the following code from Devon's script accomplish?

#include <iostream>

#include <socket.cpp>

```
#include <util.h>

using namespace std;

bool tryPort(int p);

string target("");

int main(int argC, char *argV[])

{

printf("PlagueZ port scanner 0.1\n");

int startPort = getInt("start Port: ");

int endPort = getInt("end Port: ");

target = getString("Host: ");

printf("[Processing port %d to %d]\n",

startPort, endPort);

for(int i=0; i<endPort; i++)

{

printf("[Trying port: %d]\n", i);

if(tryPort(i)) // port open

printf("[Port %d is open]\n", i);

}

printf("------Scan Finished-------\n");

system("pause");

return 0;

}

bool tryPort(int p)

{

SocketClient *scan;

try

{
```

```
scan = new SocketClient(target, p);

}

catch(int e) { delete &scan; return

false; }

delete &scan;

return true;

}
```

A. Scan the perimeter firewall for DoS vulnerabilities
B. Create socket connections to the remote sites to check their security
C. Close off any ports used by malicious code
D. Scan for open ports

Answer: D
Explanation:

QUESTION NO: 15

Travis, a senior systems developer for YNY Services, received an email recently from an unknown source. Instead of opening the email on his normal production machine, Travis decides to copy the email to a thumb drive and examine it from a quarantined PC not on the network. Travis examines the email and discovers a link that is supposed to take him to http://scarysite.com. Travis decides to get back on his production computer and examine the code of that site.

From the following code snippet, what has Travis discovered?

```
<script>

function object() {

this.email setter = captureobject

}

function captureobject(x) {

var objstring = “”

for(fld in this) {
```