EC-COUNCIL.312-50v10.v2022-05-02.q353

Exam Code:	312-50v10
Exam Name:	Certified Ethical Hacker Exam (CEH v10)
Certification Provider:	EC-COUNCIL
Free Question Number:	353
Version:	v2022-05-02
# of views:	5868
# of Questions views:	3530
https://www.freeqas.com/qa/EC-COUNCIL/312-50v10/EC-COUNCIL.312-50v10.v2022-05-02.q353.html	

NEW QUESTION: 1
Which NMAP feature can a tester implement or adjust while scanning for open ports to avoid detection by the network's IDS?
A. ICMP ping sweep to determine which hosts on the network are not available
B. Timing options to slow the speed that the port scan is conducted
C. Fingerprinting to identify which operating systems are running on the network
D. Traceroute to control the path of the packets sent during the scan
Answer: B (LEAVE A REPLY)

NEW QUESTION: 2
A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed. Which security policy must the security analyst check to see if dial-out modems are allowed?
A. Firewall-management policy
B. Permissive policy
C. Acceptable-use policy
D. Remote-access policy
Answer: (SHOW ANSWER)

NEW QUESTION: 3
When security and confidentiality of data within the same LAN is of utmost priority, which IPSec mode should you implement?
A. AH Tunnel mode
B. ESP confidential
C. ESP transport mode
D. AH promiscuous
Answer: C (LEAVE A REPLY)

NEW QUESTION: 4
_____ is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.
A. RootKit
B. Trojan
C. Backdoor
D. DoS tool
E. Scanner
Answer: A (LEAVE A REPLY)

NEW QUESTION: 5
.....is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there.
Fill in the blank with appropriate choice.
A. Evil Twin Attack
B. Sinkhole Attack
C. Collision Attack
D. Signal Jamming Attack
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 6
Which of the following is a low-tech way of gaining unauthorized access to systems?
A. Social Engineering
B. Sniffing
C. Eavesdropping
D. Scanning
Answer: A (LEAVE A REPLY)
Explanation
Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access.
References: https://en.wikipedia.org/wiki/Social_engineering_(security)

NEW QUESTION: 7
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: (SHOW ANSWER)
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-attack-likelihood.pdf

NEW QUESTION: 8
An attacker attaches a rogue router in a network. He wants to redirect traffic to a LAN attached to his router as part of a man-in-the-middle attack. What measure on behalf of the legitimate admin can mitigate this attack?
A. Redirection of the traffic cannot happen unless the admin allows it explicitly.
B. Only using OSPFv3 will mitigate this risk.
C. Disable all routing protocols and only use static routes
D. Make sure that legitimate network routers are configured to run routing protocols with authentication.
Answer: (SHOW ANSWER)

NEW QUESTION: 9
Firewalls are the software or hardware systems that are able to control and monitor the traffic coming in and out the target network based on pre-defined set of rules.
Which of the following types of firewalls can protect against SQL injection attacks?
A. Stateful firewall
B. Packet firewall
C. Data-driven firewall
D. Web application firewall
Answer: D (LEAVE A REPLY)

NEW QUESTION: 10
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. Delete the email and pretend nothing happened.
C. Forward the message to your supervisor and ask for her opinion on how to handle the situation.
D. Reply to the sender and ask them for more information about the message contents.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 11
Which command line switch would be used in NMAP to perform operating system detection?
A. -OS
B. -O
C. -sP
D. -sO
Answer: B (LEAVE A REPLY)

NEW QUESTION: 12
You have the SOA presented below in your Zone.
Your secondary servers have not been able to contact your primary server to synchronize information. How long will the secondary servers attempt to contact the primary server before it considers that zone is dead and stops responding to queries?
collegae.edu.SOA, cikkye.edu ipad.college.edu. (200302028 3600 3600 604800 3600)
A. One month
B. One day
C. One week
D. One hour
Answer: C (LEAVE A REPLY)

NEW QUESTION: 13
(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.). 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?
What is odd about this attack? Choose the best answer.
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: OXA1D95 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** Seq: 0XA1D95 Ack: 0x53 Win: 0x400
freeqas.com
EC-Council
A. These packets were crafted by a tool, they were not created by a standard IP stack.
B. This is back orifice activity as the scan comes from port 31337.
C. This is not a spoofed packet as the IP stack has increasing numbers for the three flags.
D. The attacker wants to avoid creating a sub-carries connection that is not normally valid.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 14
Which of the following is designed to identify malicious attempts to penetrate systems?

A. Intrusion Detection System
B. Firewall
C. Proxy
D. Router
Answer: A (LEAVE A REPLY)
Explanation
An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces electronic reports to a management station.
References: https://en.wikipedia.org/wiki/Intrusion_detection_system

NEW QUESTION: 15
Which of the following parameters enables NMAP's operating system detection feature?
A. NMAP -oS
B. NMAP -O
C. NMAP -sV
D. NMAP -sR
Answer: B (LEAVE A REPLY)

NEW QUESTION: 16
During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network.
What is this type of DNS configuration commonly called?
A. DNS Scheme
B. Split DNS
C. DNSSEC
D. DynDNS
Answer: B (LEAVE A REPLY)

Valid 312-50v10 Dumps shared by PrepPdf.com for Helping Passing 312-50v10 Exam! PrepPdf.com now offer the **newest 312-50v10 exam dumps**, the PrepPdf.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-50v10 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-50v10-prepaway-exam-dumps.html (**745** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 17
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 attack 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. WLAN-crack
B. Aircrack-ng
C. wificracker
D. Airguard
Answer: B (LEAVE A REPLY)

NEW QUESTION: 18
Why is a penetration test considered to be more thorough than vulnerability scan?
A. The tools used by penetration testers tend to have much more comprehensive vulnerability databases.
B. It is not - a penetration test is often performed by an automated tool, while a vulnerability scan requires active engagement.
C. A penetration test actively exploits vulnerabilities in the targeted infrastructure, while a vulnerability scan does not typically involve active exploitation.
D. Vulnerability scans only do host discovery and port scanning by default.
Answer: (SHOW ANSWER)

NEW QUESTION: 19
Which of the following security operations is used for determining the attack surface of an organization?
A. Running a network scan to detect network services in the corporate DMZ
B. Training employees on the security policy regarding social engineering
C. Reviewing the need for a security clearance for each employee
D. Using configuration management to determine when and where to apply security patches
Answer: A (LEAVE A REPLY)
Explanation
For a network scan the goal is to document the exposed attack surface along with any easily detected vulnerabilities.
References:
http://meisecurity.com/home/consulting/consulting-network-scanning/

NEW QUESTION: 20
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
```

freeqas.com
EC-Council

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 (LEAVE A REPLY)
Explanation
The Internet Printing Protocol (IPP) uses port 631.
References: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

NEW QUESTION: 21
What is GINA?
A. Gateway Interface Network Application
B. Global Internet National Authority (G-USA)
C. GUI Installed Network Application CLASS
D. Graphical Identification and Authentication DLL
Answer: (SHOW ANSWER)

NEW QUESTION: 22
A hacker was able to sniff packets on a company's wireless network. The following information was discovered:

```
The Key 10110010 01001011
The Cyphertext 01100101 01011010
```

Using the Exlcusive OR, what was the original message?
A. 11010111 00010001
B. 11110010 01011011
C. 00101000 11101110
D. 00001101 10100100
Answer: A (LEAVE A REPLY)

NEW QUESTION: 23
Shellshock allowed an unauthorized user to gain access to a server. It affected many Internet-facing services, which OS did it not directly affect?
A. Unix
B. Linux
C. Windows
D. OS X
Answer: (SHOW ANSWER)

NEW QUESTION: 24
An IT security engineer notices that the company's web server is currently being hacked. What should the engineer do next?

A. Unplug the network connection on the company's web server.
B. Perform a system restart on the company's web server.
C. Record as much information as possible from the attack.
D. Determine the origin of the attack and launch a counterattack.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 25
Scenario:
1. Victim opens the attacker's web site.
2. Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make $1000 in a day?'.
3. Victim clicks to the interesting and attractive content URL.
4. Attacker creates a transparent 'iframe' in front of the URL which victim attempts to click, so victim thinks that he/she clicks to the 'Do you want to make $1000 in a day?' url but actually he/she clicks to the content or UPL that exists in the transparent 'iframe' which is setup by the attacker.
What is the name of the attack which is mentioned in the scenario?
A. Session Fixation
B. Clickjacking Attack
C. HTTP Parameter Pollution
D. HTML Injection
Answer: B (LEAVE A REPLY)

NEW QUESTION: 26
Which of the following settings enables Nessus to detect when it is sending too many packets and the network pipe is approaching capacity?
A. Silent Dependencies
B. Netstat WMI Scan
C. Reduce parallel connections on congestion
D. Consider unscanned ports as closed
Answer: C (LEAVE A REPLY)

NEW QUESTION: 27
In Trojan terminology, what is a covert channel?



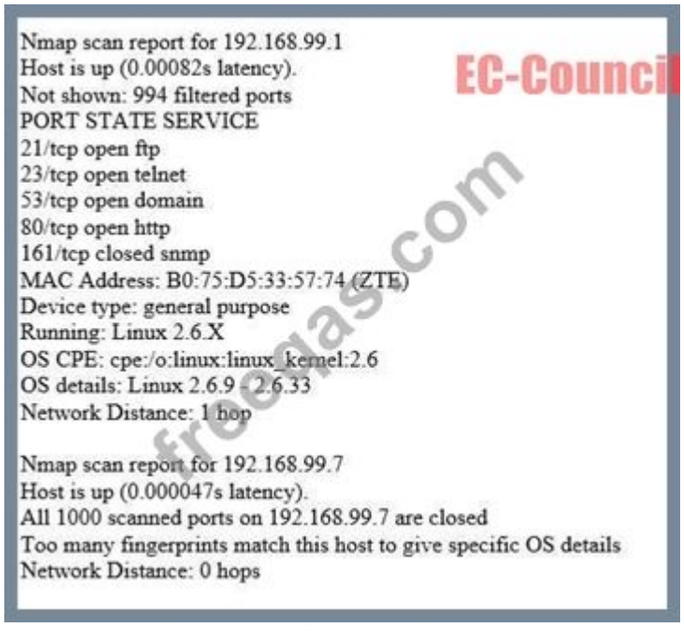
A. It is a kernel operation that hides boot processes and services to mask detection

B. A channel that transfers information within a computer system or network in a way that violates the security policy
C. It is Reverse tunneling technique that uses HTTPS protocol instead of HTTP protocol to establish connections
D. A legitimate communication path within a computer system or network for transfer of data
Answer: (SHOW ANSWER)

NEW QUESTION: 28
Rebecca commonly sees an error on her Windows system that states that a Data Execution Prevention (DEP) error has taken place. Which of the following is most likely taking place?
A. A page fault is occuring, which forces the operating system to write data from the hard drive.
B. Malware is executing in either ROM or a cache memory area.
C. A race condition is being exploited, and the operating system is containing the malicious process.
D. Malicious code is attempting to execute instruction a non-executable memory region.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 29
Which statement best describes a server type under an N-tier architecture?
A. A group of servers with a unique role
B. A single server at a specific layer
C. A group of servers at a specific layer
D. A single server with a specific role
Answer: A (LEAVE A REPLY)

NEW QUESTION: 30
Emil uses nmap to scan two hosts using this command:
nmap -sS -T4 -O 192.168.99.1 192.168.99.7
He receives this output:



What is his conclusion?

A. Host 192.168.99.7 is down.

B. Host 192.168.99.7 is an iPad.

C. He performed a SYN scan and OS scan on hosts 192.168.99.1 and 192.168.99.7

D. Host 192.168.99.1 is the host that he launched the scan from.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 31

Security Policy is a definition of what it means to be secure for a system, organization or other entity. For Information Technologies, there are sub-policies like Computer Security Policy, Information Protection Policy, Information Security Policy, network Security Policy, Physical Security Policy, Remote Access Policy, and User Account Policy.

What is the main theme of the sub-policies for Information Technologies?

A. Authenticity, Confidentiality, Integrity

B. Availability, Non-repudiation, Confidentiality

C. Authenticity, Integrity, Non-repudiation

D. Confidentiality, Integrity, Availability

Answer: D (LEAVE A REPLY)

Valid 312-50v10 Dumps shared by PrepPdf.com for Helping Passing 312-50v10 Exam! PrepPdf.com now offer the **newest 312-50v10 exam dumps**, the PrepPdf.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-50v10 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-50v10-prepaway-exam-dumps.html (**745** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 32
You have successfully compromised a machine on the network and found a server that is alive on the same network. You tried to ping it but you didn't get any response back.
What is happening?
A. ICMP could be disabled on the target server.
B. The ARP is disabled on the target server.
C. TCP/IP doesn't support ICMP.
D. You need to run the ping command with root privileges.
Answer: (SHOW ANSWER)
Explanation
The ping utility is implemented using the ICMP "Echo request" and "Echo reply" messages.
Note: The Internet Control Message Protocol (ICMP) is one of the main protocols of the internet protocol suite. It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached.
References: https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

NEW QUESTION: 33
Risks = Threats x Vulnerabilities is referred to as the:
A. Risk equation
B. Threat assessment
C. BIA equation
D. Disaster recovery formula
Answer: A (LEAVE A REPLY)
Explanation
The most effective way to define risk is with this simple equation:
Risk = Threat x Vulnerability x Cost
This equation is fundamental to all information security.
References:
http://www.icharter.org/articles/risk_equation.html

NEW QUESTION: 34
In cryptanalysis and computer security, 'pass the hash' is a hacking technique that allows an attacker to authenticate to a remote server/service by using the underlying NTLM and/or LanMan hash of a user's password, instead of requiring the associated plaintext password as is normally the case.
Metasploit Framework has a module for this technique: psexec. The psexec module is often used by penetration testers to obtain access to a given system that you already know the credentials for. It was written by sysinternals and has been integrated within the framework. Often as penetration testers, successfully gain access to a system through some exploit, use meterpreter to grab the passwords or other methods like fgdump, pwdump, or cachedump and then utilize rainbowtables to crack those hash values.
Which of the following is true hash type and sort order that is using in the psexec module's 'smbpass'?
A. NTLM:LM

B. LM:NTLM
C. LM:NT
D. NT:LM
Answer: C (LEAVE A REPLY)

NEW QUESTION: 35
Which specific element of security testing is being assured by using hash?
A. Authentication
B. Integrity
C. Availability
D. Confidentiality
Answer: B (LEAVE A REPLY)

NEW QUESTION: 36
What type of vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?
A. Server side request forgery
B. Session hijacking
C. Cross-site request forgery
D. Cross-site scripting
Answer: C (LEAVE A REPLY)

NEW QUESTION: 37
A consultant is hired to do physical penetration testing at a large financial company. In the first day of his assessment, the consultant goes to the company`s building dressed like an electrician and waits in the lobby for an employee to pass through the main access gate, then the consultant follows the employee behind to get into the restricted area. Which type of attack did the consultant perform?
A. Social engineering
B. Tailgating
C. Man trap
D. Shoulder surfing
Answer: (SHOW ANSWER)

NEW QUESTION: 38
What is the code written for?

```
#!/usr/bin/python
import socket
buffer=["A"]
counter=50
while len(buffer)<=100:
buffer.apend ("A"*counter)
counter=counter+50
commands=["HELP","STATS.","RTIME.","LTIME.","SRUN.","TRUN.","GMO
N.","GDOG.","KSTET.","GTER.","HTER.","LTER.","KSTAN."]
for command in commands:
 for buffstring in buffer:
  print "Exploiting" +command+":"+str(len(buffstring))
  s=socket.socket(socket.AF_INET.socket.SOCK_STREAM)
  s.connect(('127.0.0.1',9999))
  s.recv(50)
  s.send(command+buffstring)
  s.close()
```

freeqas.com
EC-Council

A. Bruteforce
B. Denial-of-service (Dos)
C. Buffer Overflow
D. Encryption
Answer: C (LEAVE A REPLY)

NEW QUESTION: 39
In which phase of the ethical hacking process can Google hacking be employed? This is a technique that involves manipulating a search string with specific operators to search for vulnerabilities.
Example:
allintitle: root passwd
A. Maintaining Access
B. Gaining Access
C. Scanning and Enumeration
D. Reconnaissance
Answer: D (LEAVE A REPLY)

NEW QUESTION: 40
Which of the following programming languages is most susceptible to buffer overflow attacks, due to its lack of a built-in-bounds checking mechanism?
Code:
#include <string.h>
int main(){
char buffer[8];

strcpy(buffer, ""11111111111111111111111111111"");
}
Output:
Segmentation fault
A. Java
B. Python
C. C#
D. C++
Answer: D (LEAVE A REPLY)

NEW QUESTION: 41
Which type of scan measures a person's external features through a digital video camera?
A. Iris scan
B. Facial recognition scan
C. Retinal scan
D. Signature kinetics scan
Answer: B (LEAVE A REPLY)

NEW QUESTION: 42
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 = 23
B. tcp.port != 21
C. tcp.port ==21 || tcp.port ==22
D. tcp.port ==21
Answer: C (LEAVE A REPLY)

NEW QUESTION: 43
Which of the following processes evaluates the adherence of an organization to its stated security policy?
A. Security auditing
B. Risk assessment
C. Vulnerability assessment
D. Penetration testing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 44
Insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key.

Suppose a malicious user Rob tries to get access to the account of a benign user Ned.
Which of the following requests best illustrates an attempt to exploit an insecure direct object reference vulnerability?

A. "GET/restricted/goldtransfer?to=Rob&from=1 or 1=1' HTTP/1.1Host: westbank.com"

B. "GET/restricted/accounts/?name=Ned HTTP/1.1 Host: westbank.com"

C. "GET/restricted/\r\n\%00account%00Ned%00access HTTP/1.1 Host: westbank.com"

D. "GET/restricted/bank.getaccount('Ned') HTTP/1.1 Host: westbank.com"

Answer: B (LEAVE A REPLY)

NEW QUESTION: 45

Take a look at the following attack on a Web Server using obstructed URL:



How would you protect from these attacks?

A. Use SSL authentication on Web Servers

B. Create rules in IDS to alert on strange Unicode requests

C. Enable Active Scripts Detection at the firewall and routers

D. Configure the Web Server to deny requests involving "hex encoded" characters

Answer: B (LEAVE A REPLY)

NEW QUESTION: 46

Which component of IPsec performs protocol-level functions that are required to encrypt and decrypt the packets?

A. Internet Key Exchange (IKE)

B. IPsec driver

C. IPsec Policy Agent

D. Oakley

Answer: (SHOW ANSWER)

Valid 312-50v10 Dumps shared by PrepPdf.com for Helping Passing 312-50v10 Exam! PrepPdf.com now offer the **newest 312-50v10 exam dumps**, the PrepPdf.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-50v10 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-50v10-prepaway-exam-dumps.html (**745** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 47
Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small sized packets to the target computer, making it very difficult for an IDS to detect the attack signatures. Which tool can be used to perform session splicing attacks?
A. tcpsplice
B. Burp
C. Whisker
D. Hydra
Answer: C (LEAVE A REPLY)

NEW QUESTION: 48
When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerability scanners. What proxy tool will help you find web vulnerabilities?
A. Maskgen
B. Dimitry
C. Proxychains
D. Burpsuite
Answer: (SHOW ANSWER)

NEW QUESTION: 49
Name two software tools used for OS guessing? (Choose two.)
A. NetBus
B. Snadboy
C. UserInfo
D. Queso
E. Nmap
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 50
Which of the following incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an organization?
A. Identification phase
B. Preparation phase
C. Containment phase
D. Recovery phase
Answer: B (LEAVE A REPLY)

NEW QUESTION: 51

What is the way to decide how a packet will move from an untrusted outside host to a protected inside that is behind a firewall, which permits the hacker to determine which ports are open and if the packets can pass through the packet-filtering of the firewall.

A. Firewalking

B. Session hijacking

C. Network sniffing

D. Man-in-the middle attack

Answer: A (LEAVE A REPLY)

NEW QUESTION: 52

What is a "Collision attack" in cryptography?

A. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key

B. Collision attacks try to find two inputs producing the same hash

C. Collision attacks try to get the public key

D. Collision attacks try to break the hash into three parts to get the plaintext value

Answer: B (LEAVE A REPLY)

NEW QUESTION: 53

Which of the following describes the characteristics of a Boot Sector Virus?

A. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR

B. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR

C. Modifies directory table entries so that directory entries point to the virus code instead of the actual program

D. Overwrites the original MBR and only executes the new virus code

Answer: A (LEAVE A REPLY)

A boot sector virus is a computer virus that infects a storage device's master boot record (MBR). The virus moves the boot sector to another location on the hard drive.

References: https://www.techopedia.com/definition/26655/boot-sector-virus

NEW QUESTION: 54

The company ABC recently contract a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it. What is the following options can be useful to ensure the integrity of the data?

A. The CFO can use a hash algorithm in the document once he approved the financial statements

B. The document can be sent to the accountant using an exclusive USB for that document

C. The financial statements can be sent twice, one by email and the other delivered in USB and the accountant can compare both to be sure is the same document

D. The CFO can use an excel file with a password

Answer: A (LEAVE A REPLY)

NEW QUESTION: 55
You have compromised a server and successfully gained a root access. You want to pivot and pass traffic undetected over the network and evade any possible Intrusion Detection System.
What is the best approach?
A. Install Cryptcat and encrypt outgoing packets from this server.
B. Install and use Telnet to encrypt all outgoing traffic from this server.
C. Use Alternate Data Streams to hide the outgoing packets from this server.
D. Use HTTP so that all traffic can be routed via a browser, thus evading the internal Intrusion Detection Systems.
Answer: A (LEAVE A REPLY)
Explanation
Cryptcat enables us to communicate between two systems and encrypts the communication between them with twofish.
References:
http://null-byte.wonderhowto.com/how-to/hack-like-pro-create-nearly-undetectable-backdoor-with-cryptcat-0149

NEW QUESTION: 56
A Security Engineer at a medium-sized accounting firm has been tasked with discovering how much information can be obtained from the firm's public facing web servers. The engineer decides to start by using netcat to port 80.
The engineer receives this output:
HTTP/1.1 200 OK
Server: Microsoft-IIS/6
Expires: Tue, 17 Jan 2011 01:41:33 GMT
Date: Mon, 16 Jan 2011 01:41:33 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Wed, 28 Dec 2010 15:32:21 GMT
ETag: "b0aac0542e25c31:89d"
Content-Length: 7369
Which of the following is an example of what the engineer performed?
A. Banner grabbing
B. Who is database query
C. Cross-site scripting
D. SQL injection
Answer: A (LEAVE A REPLY)

NEW QUESTION: 57
What information should an IT system analysis provide to the risk assessor?
A. Threat statement
B. Management buy-in

C. Impact analysis
D. Security architecture
Answer: (SHOW ANSWER)

NEW QUESTION: 58
While scanning with Nmap, Patin found several hosts which have the IP ID of incremental sequences. He then decided to conduct: nmap -Pn -p- -si kiosk.adobe.com www.riaa.com.
kiosk.adobe.com is the host with incremental IP ID sequence. What is the purpose of using
"-si" with Nmap?
A. Conduct silent scan
B. Conduct IDLE scan
C. Conduct ICMP scan
D. Conduct stealth scan
Answer: (SHOW ANSWER)

NEW QUESTION: 59
If a token and 4-digit personal identification number (PIN) are used to access a computer system and the token performs off-line checking for the correct PIN, what type of attack is possible?
A. Birthday
B. Man-in-the-middle
C. Brute force
D. Smurf
Answer: (SHOW ANSWER)

NEW QUESTION: 60
When discussing passwords, what is considered a brute force attack?
A. You threaten to use the rubber hose on someone unless they reveal their password
B. You wait until the password expires
C. You create hashes of a large number of words and compare it with the encrypted passwords
D. You load a dictionary of words into your cracking program
E. You attempt every single possibility until you exhaust all possible combinations or discover the password
Answer: (SHOW ANSWER)

NEW QUESTION: 61
The company ABC recently contracted a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it.
What of the following options can be useful to ensure the integrity of the data?
A. The CFO can use an excel file with a password.
B. The CFO can use a hash algorithm in the document once he approved the financial statements.

C. The document can be sent to the accountant using an exclusive USB for that document.
D. The financial statements can be sent twice, one by email and the other delivered in USB and the accountant can compare both to be sure it is the same document.
Answer: B (LEAVE A REPLY)

Valid 312-50v10 Dumps shared by PrepPdf.com for Helping Passing 312-50v10 Exam! PrepPdf.com now offer the **newest 312-50v10 exam dumps**, the PrepPdf.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-50v10 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-50v10-prepaway-exam-dumps.html (**745** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 62
You are the Systems Administrator for a large corporate organization. You need to monitor all network traffic on your local network for suspicious activities and receive notifications when an attack is occurring. Which tool would allow you to accomplish this goal?
A. Network-based IDS
B. Firewall
C. Proxy
D. Host-based IDS
Answer: (SHOW ANSWER)
A network-based intrusion detection system (NIDS) is used to monitor and analyze network traffic to protect a system from network-based threats.
A NIDS reads all inbound packets and searches for any suspicious patterns. When threats are discovered, based on its severity, the system can take action such as notifying administrators, or barring the source IP address from accessing the network.
References: https://www.techopedia.com/definition/12941/network-based-intrusion- detection-system-nids

NEW QUESTION: 63
The "white box testing" methodology enforces what kind of restriction?
A. The internal operation of a system is completely known to the tester.
B. Only the external operation of a system is accessible to the tester.
C. Only the internal operation of a system is known to the tester.
D. The internal operation of a system is only partly accessible to the tester.
Answer: (SHOW ANSWER)
White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases.
References: https://en.wikipedia.org/wiki/White-box_testing

NEW QUESTION: 64
Which of the following is a preventive control?
A. Smart card authentication
B. Security policy
C. Audit trail
D. Continuity of operations plan
Answer: A (LEAVE A REPLY)

NEW QUESTION: 65
In Trojan terminology, what is a covert channel?



A. A channel that transfers information within a computer system or network in a way that violates the security policy
B. A legitimate communication path within a computer system or network for transfer of data
C. It is a kernel operation that hides boot processes and services to mask detection
D. It is Reverse tunneling technique that uses HTTPS protocol instead of HTTP protocol to establish connections
Answer: A (LEAVE A REPLY)

NEW QUESTION: 66
A company has five different subnets: 192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0 and 192.168.5.0. How can NMAP be used to scan these adjacent Class C networks?
A. NMAP -P 192.168.1/17
B. NMAP -P 192.168.1.0,2.0,3.0,4.0,5.0
C. NMAP -P 192.168.1-5.
D. NMAP -P 192.168.0.0/16
Answer: C (LEAVE A REPLY)

NEW QUESTION: 67
You are working as a Security Analyst in a company XYZ that owns the whole subnet range of 23.0.0.0/8 and 192.168.0.0/8.
While monitoring the data, you find a high number of outbound connections. You see that IP's owned by XYZ (Internal) and private IP's are communicating to a Single Public IP. Therefore, the Internal IP's are sending data to the Public IP.

After further analysis, you find out that this Public IP is a blacklisted IP, and the internal communicating devices are compromised.
What kind of attack does the above scenario depict?
A. Rootkit Attack
B. Spear Phishing Attack
C. Advanced Persistent Threats
D. Botnet Attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 68
Ricardo wants to send secret messages to a competitor company. To secure these messages, he uses a technique of hiding a secret message within an ordinary message. The technique provides 'security through obscurity'.
What technique is Ricardo using?
A. RSA algorithm
B. Encryption
C. Public-key cryptography
D. Steganography
Answer: (SHOW ANSWER)

NEW QUESTION: 69
What is attempting an injection attack on a web server based on responses to True/False questions called?
A. Blind SQLi
B. DMS-specific SQLi
C. Classic SQLi
D. Compound SQLi
Answer: A (LEAVE A REPLY)

NEW QUESTION: 70
An unauthorized individual enters a building following an employee through the employee entrance after the lunch rush. What type of breach has the individual just performed?
A. Announced
B. Reverse Social Engineering
C. Tailgating
D. Piggybacking
Answer: C (LEAVE A REPLY)

NEW QUESTION: 71
While performing ping scans into a target network you get a frantic call from the organization's security team. They report that they are under a denial of service attack. When you stop your scan, the smurf attack event stops showing up on the organization's IDS monitor.

How can you modify your scan to prevent triggering this event in the IDS?
A. Only scan the Windows systems.
B. Do not scan the broadcast IP.
C. Scan more slowly.
D. Spoof the source IP address.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 72
Which of the following is a passive wireless packet analyzer that works on Linux-based systems?
A. OpenVAS
B. Burp Suite
C. tshark
D. Kismet
Answer: (SHOW ANSWER)

NEW QUESTION: 73
An attacker scans a host with the below command. Which three flags are set? (Choose three.)
#nmap -sX host.domain.com
A. This is SYN scan. SYN flag is set
B. This is ACK scan. ACK flag is set
C. This is Xmas scan. SYN and ACK flags are set
D. This is Xmas scan. URG, PUSH and FIN are set
Answer: (SHOW ANSWER)

NEW QUESTION: 74
Initiating an attack against targeted businesses and organizations, threat actors compromise a carefully selected website by inserting an exploit resulting in malware infection. The attackers run exploits on well-known and trusted sites likely to be visited by their targeted victims. Aside from carefully choosing sites to compromise, these attacks are known to incorporate zero-day exploits that target unpatched vulnerabilities. Thus, the targeted entities are left with little or no defense against these exploits.
What type of attack is outlined in the scenario?
A. Watering Hole Attack
B. Heartbleed Attack
C. Shellshock Attack
D. Spear Phising Attack
Answer: (SHOW ANSWER)
Watering Hole is a computer attack strategy, in which the victim is a particular group (organization, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some member of the targeted group gets infected.

NEW QUESTION: 75

Which United States legislation mandates that the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO) must sign statements verifying the completeness and accuracy of financial reports?
A. Federal Information Security Management Act (FISMA)
B. Fair and Accurate Credit Transactions Act (FACTA)
C. Gramm-Leach-Bliley Act (GLBA)
D. Sarbanes-Oxley Act (SOX)
Answer: (SHOW ANSWER)

NEW QUESTION: 76
Gavin owns a white-hat firm and is performing a website security audit for one of his clients. He begins by running a scan which looks for common misconfigurations and outdated software versions. Which of the following tools is he most likely using?
A. Metasploit
B. Nikto
C. Armitage
D. Nmap
Answer: (SHOW ANSWER)

Valid 312-50v10 Dumps shared by PrepPdf.com for Helping Passing 312-50v10 Exam! PrepPdf.com now offer the **newest 312-50v10 exam dumps**, the PrepPdf.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-50v10 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-50v10-prepaway-exam-dumps.html (**745** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 77
How can a rootkit bypass Windows 7 operating system's kernel mode, code signing policy?
A. Attaching itself to the master boot record in a hard drive and changing the machine's boot sequence/options
B. Defeating the scanner from detecting any code change at the kernel
C. Performing common services for the application process and replacing real applications with fake ones
D. Replacing patch system calls with its own version that hides the rootkit (attacker's) actions
Answer: A (LEAVE A REPLY)

NEW QUESTION: 78
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. SQL injection
C. Cross-site scripting
D. Command injection
Answer: (SHOW ANSWER)

NEW QUESTION: 79
What type of vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?
A. Cross-site request forgery
B. Server side request forgery
C. Session hijacking
D. Cross-site scripting
Answer: (SHOW ANSWER)

NEW QUESTION: 80
The Open Web Application Security Project (OWASP) is the worldwide not-for-profit charitable organization focused on improving the security of software. What item is the primary concern on OWASP's Top Ten Project Most Critical Web Application Security Risks?
A. Injection
B. Cross Site Scripting
C. Path disclosure
D. Cross Site Request Forgery
Answer: (SHOW ANSWER)

NEW QUESTION: 81
Ricardo wants to send secret messages to a competitor company. To secure these messages, he uses a technique of hiding a secret message within an ordinary message. The technique provides 'security through obscurity'.
What technique is Ricardo using?
A. Steganography
B. Public-key cryptography
C. RSA algorithm
D. Encryption
Answer: A (LEAVE A REPLY)
Explanation
Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video.
References: https://en.wikipedia.org/wiki/Steganography

NEW QUESTION: 82
An attacker uses a communication channel within an operating system that is neither designed nor intended to transfer information. What is the name of the communications channel?
A. Encrypted
B. Covert
C. Classified
D. Overt
Answer: B (LEAVE A REPLY)

NEW QUESTION: 83
What is the main disadvantage of the scripting languages as opposed to compiled programming languages?
A. Scripting languages are slower because they require an interpreter to run the code.
B. Scripting languages cannot be used to create graphical user interfaces.
C. Scripting languages are hard to learn.
D. Scripting languages are not object-oriented.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 84
Which of the following areas is considered a strength of symmetric key cryptography when compared with asymmetric algorithms?
A. Scalability
B. Key distribution
C. Speed
D. Security
Answer: C (LEAVE A REPLY)

NEW QUESTION: 85
Bob, your senior colleague, has sent you a mail regarding aa deal with one of the clients. You are requested to accept the offer and you oblige.
After 2 days, Bob denies that he had ever sent a mail.
What do you want to "know" to prove yourself that it was Bob who had send a mail?
A. Integrity
B. Authentication
C. Confidentiality
D. Non-Repudiation
Answer: D (LEAVE A REPLY)

NEW QUESTION: 86
Study the snort rule given below and interpret the rule. alert tcp any any --> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msG. "mountd access";)

A. An alert is generated when a TCP packet originating from any IP address is seen on the network and destined for any IP address on the 192.168.1.0 subnet on port 111
B. An alert is generated when any packet other than a TCP packet is seen on the network and destined for the 192.168.1.0 subnet
C. An alert is generated when a TCP packet is generated from any IP on the 192.168.1.0 subnet and destined to any IP on port 111
D. An alert is generated when a TCP packet is originated from port 111 of any IP address to the 192.168.1.0 subnet
Answer: A (LEAVE A REPLY)

NEW QUESTION: 87
What type of OS fingerprinting technique sends specially crafted packets to the remote OS and analyzes the received response?
A. Reflective
B. Distributive
C. Passive
D. Active
Answer: (SHOW ANSWER)

NEW QUESTION: 88
The tools which receive event logs from servers, network equipment, and applications, and perform analysis and correlation on those logs, and can generate alarms for security relevant issues, are known as what?
A. Network Sniffer
B. Vulnerability Scanner
C. Intrusion Prevention Server
D. Security Incident and Event Monitoring
Answer: D (LEAVE A REPLY)
Explanation

NEW QUESTION: 89
Session splicing is an IDS evasion technique 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 be used to perform session splicing attacks?
A. Whisker
B. tcpsplice
C. Burp
D. Hydra
Answer: A (LEAVE A REPLY)
Explanation
One basic technique is to split the attack payload into multiple small packets, so that the IDS must reassemble the packet stream to detect the attack. A simple way of splitting packets is by fragmenting them, but an

adversary can also simply craft packets with small payloads. The 'whisker' evasion tool calls crafting packets with small payloads 'session splicing'.
References:
https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques#Fragmentation_and_small_packet

NEW QUESTION: 90
Which of the following represents the initial two commands that an IRC client sends to join an IRC network?
A. USER, PASS
B. LOGIN, USER
C. USER, NICK
D. LOGIN, NICK
Answer: (SHOW ANSWER)

NEW QUESTION: 91
Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?
A. Macro virus
B. Polymorphic virus
C. Stealth/ Tunneling virus
D. Cavity virus
Answer: C (LEAVE A REPLY)

Valid 312-50v10 Dumps shared by PrepPdf.com for Helping Passing 312-50v10 Exam! PrepPdf.com now offer the **newest 312-50v10 exam dumps**, the PrepPdf.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-50v10 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-50v10-prepaway-exam-dumps.html (**745** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 92
This configuration allows NIC to pass all traffic it receives to the Central Processing Unit (CPU), instead of passing only the frames that the controller is intended to receive. Select the option that BEST describes the above statement.
A. Port forwarding
B. Promiscuous mode
C. Multi-cast mode
D. WEM
Answer: (SHOW ANSWER)

NEW QUESTION: 93

You are monitoring the network of your organizations. You notice that:
1. There are huge outbound connections from your Internal Network to External IPs
2. On further investigation, you see that the external IPs are blacklisted
3. Some connections are accepted, and some are dropped
4. You find that it is a CnC communication
Which of the following solution will you suggest?
A. Update the Latest Signatures on your IDS/IPS
B. Block the Blacklist IP's @ Firewall
C. Block the Blacklist IP's @ Firewall as well as Clean the Malware which are trying to Communicate with the External Blacklist IP's.
D. Clean the Malware which are trying to Communicate with the External Blacklist IP's
Answer: (SHOW ANSWER)

NEW QUESTION: 94
Which of the following is an adaptive SQL Injection testing technique used to discover coding errors by inputting massive amounts of random data and observing the changes in the output?
A. Static Testing
B. Dynamic Testing
C. Function Testing
D. Fuzzing Testing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 95
When conducting a penetration test, it is crucial to use all means to get all available information about the target network. One of the ways to do that is by sniffing the network. Which of the following cannot be performed by the passive network sniffing?
A. Identifying operating systems, services, protocols and devices
B. Collecting unencrypted information about usernames and passwords
C. Capturing a network traffic for further analysis
D. Modifying and replaying captured network traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 96
An IT employee got a call from one our best customers. The caller wanted to know about the company's network infrastructure, systems, and team. New opportunities of integration are in sight for both company and customer. What should this employee do?
A. The employee should not provide any information without previous management authorization
B. The employee can not provide any information: but, anyway, he/she will provide the name of the person in charge
C. Since the company's policy is all about Customer Service. he/she will provide information
D. Disregarding the call, the employee should hang up

Answer: A (LEAVE A REPLY)

NEW QUESTION: 97
You have successfully logged on a Linux system. You want to now cover your track. Your login attempt may be logged on several files located in /var/log. Which file does NOT belong to the list:
A. btmp
B. wtmp
C. user.log
D. auth.log
Answer: C (LEAVE A REPLY)

NEW QUESTION: 98
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. Social engineering
B. Tailgating
C. Piggybacking
D. Eavesdropping
Answer: A (LEAVE A REPLY)
Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

NEW QUESTION: 99
During a penetration test, a tester finds a target that is running MS SQL 2000 with default credentials. The tester assumes that the service is running with Local System account.
How can this weakness be exploited to access the system?
A. Invoking the stored procedure xp_cmdshell to spawn a Windows command shell
B. Invoking the stored procedure cmd_shell to spawn a Windows command shell
C. Using the Metasploit psexec module setting the SA / Admin credential
D. Invoking the stored procedure xp_shell to spawn a Windows command shell
Answer: A (LEAVE A REPLY)

NEW QUESTION: 100

You work as a Security Analyst for a retail organization. In securing the company's network, you set up a firewall and an IDS. However, hackers are able to attack the network. After investigating, you discover that your IDS is not configured properly and therefore is unable to trigger alarms when needed. What type of alert is the IDS giving?

A. False Negative

B. False Positive

C. True Negative

D. True Positive

Answer: A (LEAVE A REPLY)

Explanation

A false negative error, or in short false negative, is where a test result indicates that a condition failed, while it actually was successful. I.e. erroneously no effect has been assumed.

References: https://en.wikipedia.org/wiki/False_positives_and_false_negatives#False_negative_error

NEW QUESTION: 101

Which of the following is the greatest threat posed by backups?

A. A backup is the source of Malware or illicit information.

B. A backup is unavailable during disaster recovery.

C. A backup is incomplete because no verification was performed.

D. An un-encrypted backup can be misplaced or stolen.

Answer: D (LEAVE A REPLY)

Explanation

If the data written on the backup media is properly encrypted, it will be useless for anyone without the key.

References:

http://resources.infosecinstitute.com/backup-media-encryption/

NEW QUESTION: 102

You are a security officer of a company. You had an alert from IDS that indicates that one PC on your Intranet is connected to a blacklisted IP address (C2 Server) on the Internet. The IP address was blacklisted just before the alert. You are staring an investigation to roughly analyze the severity of the situation. Which of the following is appropriate to analyze?

A. Event logs on the PC

B. Internet Firewall/Proxy log

C. Event logs on domain controller

D. IDS log

Answer: B (LEAVE A REPLY)

NEW QUESTION: 103

Why would you consider sending an email to an address that you know does not exist within the company you are performing a Penetration Test for?

A. To perform a DoS

B. To illicit a response back that will reveal information about email servers and how they treat undeliverable mail
C. To test for virus protection
D. To create needless SPAM
E. To determine who is the holder of the root account
Answer: B (LEAVE A REPLY)

NEW QUESTION: 104
Matthew, a black hat, has managed to open a meterpreter session to one of the kiosk machines in Evil Corp's lobby. He checks his current SID, which is S-1-5-21-1223352397-1872883824-861252104-501. What needs to happen before Matthew has full administrator access?
A. He needs to gain physical access.
B. He must perform privilege escalation.
C. He already has admin privileges, as shown by the "501" at the end of the SID.
D. He needs to disable antivirus protection.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 105
It is a short-range wireless communication technology intended to replace the cables connecting portable of fixed devices while maintaining high levels of security. It allows mobile phones, computers and other devices to connect and communicate using a short-range wireless connection. Which of the following terms best matches the definition?
A. Radio-Frequency identification
B. InfraRed
C. Bluetooth
D. WLAN
Answer: (SHOW ANSWER)

NEW QUESTION: 106
Which of the following tools can be used to perform a zone transfer?
A. Neotrace
B. Netcat
C. Sam Spade
D. NSLookup
E. Finger
F. Host
G. Dig
Answer: C,D,F,G (LEAVE A REPLY)

Valid 312-50v10 Dumps shared by PrepPdf.com for Helping Passing 312-50v10 Exam! PrepPdf.com now offer the **newest 312-50v10 exam dumps**, the PrepPdf.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-50v10 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-50v10-prepaway-exam-dumps.html (**745** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 107
Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?
A. ESP transport mode
B. AH permiscuous
C. ESP confidential
D. AH Tunnel mode
Answer: (SHOW ANSWER)
Explanation
When transport mode is used, IPSec encrypts only the IP payload. Transport mode provides the protection of an IP payload through an AH or ESP header. Encapsulating Security Payload (ESP) provides confidentiality (in addition to authentication, integrity, and anti-replay protection) for the IP payload.

NEW QUESTION: 108
The following is part of a log file taken from the machine on the network with the IP address of 192.168.1.106:

```
Time:Mar 13 17:30:15 Port:20 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:17 Port:21 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:19 Port:22 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:21 Port:23 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:22 Port:25 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:23 Port:80 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:30 Port:443 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
```

freeqas.com
EC-Council

What type of activity has been logged?

A. Denial of service attack targeting 192.168.1.103
B. Port scan targeting 192.168.1.106
C. Port scan targeting 192.168.1.103
D. Teardrop attack targeting 192.168.1.106
Answer: B (LEAVE A REPLY)

NEW QUESTION: 109
Which of the following parameters describe LM Hash (see exhibit):
Exhibit:
I - The maximum password length is 14 characters.

II - There are no distinctions between uppercase and lowercase.

III - It's a simple algorithm, so 10,000,000 hashes can be generated per second.

EC-Council freeqas.com

A. I, II, and III
B. I
C. II
D. I and II
Answer: A (LEAVE A REPLY)
Explanation
The LM hash is computed as follows:
1. The user's password is restricted to a maximum of fourteen characters.
2. The user's password is converted to uppercase.
Etc.
14 character Windows passwords, which are stored with LM Hash, can be cracked in five seconds.
References: https://en.wikipedia.org/wiki/LM_hash

NEW QUESTION: 110
What is one of the advantages of using both symmetric and asymmetric cryptogrsphy in SSL/TLS?
A. Symmetric algorithms such as AES provide a failsafe when asymmetric methods fail.
B. Supporting both types of algorithms allows less-powerful devices such as mobile phones to use symmetric encryption instead.
C. Asymmetric cryptography is computationally expensive in comparison. However, it is well-suited to securely negotiate keys for use with symmetric cryptography.
D. Symmetric encryption allows the server to security transmit the session keys out-of-band.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 111
Which of the following is a vulnerability in GNU's bash shell (discovered in September of 2014) that gives attackers access to run remote commands on a vulnerable system?

A. Rootshock
B. Shellshock
C. Shellbash
D. Rootshell
Answer: B (LEAVE A REPLY)

NEW QUESTION: 112
A consultant has been hired by the V.P. of a large financial organization to assess the company's security posture. During the security testing, the consultant comes across child pornography on the V.P.'s computer. What is the consultant's obligation to the financial organization?
A. Delete the pornography, say nothing, and continue security testing.
B. Say nothing and continue with the security testing.
C. Stop work immediately and contact the authorities.
D. Bring the discovery to the financial organization's human resource department.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 113
Jimmy is standing outside a secure entrance to a facility. He is pretending to have a tense conversation on his cell phone as an authorized employee badges in. Jimmy, while still on the phone, grabs the door as it begins to close.
What just happened?
A. Masquerading
B. Tailgating
C. Phishing
D. Whaling
Answer: B (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 114
Using Windows CMD, how would an attacker list all the shares to which the current user context has access?
A. NET USE
B. NET CONFIG
C. NET FILE
D. NET VIEW
Answer: (SHOW ANSWER)
Connects a computer to or disconnects a computer from a shared resource, or displays information about computer connections. The command also controls persistent net connections. Used without parameters, net use retrieves a list of network connections.
References: https://technet.microsoft.com/en-us/library/bb490717.aspx

NEW QUESTION: 115

From the two screenshots below, which of the following is occurring?

First one:

```
1 [10.0.0.253]# nmap -sP 10.0.0.0/24
3 Starting Nmap
5 Host 10.0.0.1 appears to be up.
6 MAC Address: 00:09:5B:29:FD:96 (Netgear)
7 Host 10.0.0.2 appears to be up.
8 MAC Address: 00:0F:B5:96:38:5D (Netgear)
9 Host 10.0.0.4 appears to be up.
10 Host 10.0.0.5 appears to be up.
11 MAC Address: 00:14:2A:B1:1E:2E (Elitegroup Computer System Co.)
12 Nmap finished: 256 IP addresses (4 hosts up) scanned in 5.399
seconds
```

Second one:

```
1 [10.0.0.252]# nmap -sO 10.0.0.2
3 Starting Nmap 4.01 at 2006-07-14 12:56 BST
4 Interesting protocols on 10.0.0.2:
5 (The 251 protocols scanned but not shown below are
6 in state: closed)
7 PROTOCOL STATE SERVICE
8 1 open icmp
9 2 open|filtered igmp
10 6 open tcp
11 17 open udp
12 255 open|filtered unknown
14 Nmap finished: 1 IP address (1 host up) scanned in
15 1.259 seconds
1 [10.0.0.253]# nmap -sP
1 [10.0.0.253]# nmap -sP
```

EC-Council freeeas.com

A. 10.0.0.253 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against 10.0.0.2.

B. 10.0.0.252 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2.

C. 10.0.0.253 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2.

D. 10.0.0.2 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against 10.0.0.2.

Answer: (SHOW ANSWER)

NEW QUESTION: 116

When creating a security program, which approach would be used if senior management is supporting and enforcing the security policy?

A. A senior creation approach

B. An IT assurance approach

C. A top-down approach

D. A bottom-up approach

Answer: C (LEAVE A REPLY)

NEW QUESTION: 117
While you were gathering information as part of security assessments for one of your clients, you were able to gather data that show your client is involved with fraudulent activities. What should you do?
A. Ignore the data and continue the assessment until completed as agreed
B. Immediately stop work and contact the proper legal authorities
C. Copy the data to removable media and keep it in case you need it
D. Confront the client in a respectful manner and ask her about the data
Answer: B (LEAVE A REPLY)

NEW QUESTION: 118
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. Do not transfer the money but steal the bitcoins.
D. Transfer money from the administrator's account to another account.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 119
In Wireshark, the packet bytes panes show the data of the current packet in which format?
A. Hexadecimal
B. Decimal
C. ASCII only
D. Binary
Answer: A (LEAVE A REPLY)

NEW QUESTION: 120
env x=`(){ :;};echo exploit` bash -c 'cat /etc/passwd'
What is the Shellshock bash vulnerability attempting to do on a vulnerable Linux host?
A. Display passwd content to prompt
B. Removes the passwd file
C. Changes all passwords in passwd
D. Add new user to the passwd file
Answer: A (LEAVE A REPLY)
Explanation
To extract private information, attackers are using a couple of techniques. The simplest extraction attacks are in the form:
() {:;}; /bin/cat /etc/passwd

That reads the password file /etc/passwd, and adds it to the response from the web server. So an attacker injecting this code through the Shellshock vulnerability would see the password file dumped out onto their screen as part of the web page returned.
References: https://blog.cloudflare.com/inside-shellshock/

NEW QUESTION: 121
During an Xmas scan, what indicates a port is closed?
A. RST
B. SYN
C. ACK
D. No return response
Answer: (SHOW ANSWER)

Valid 312-50v10 Dumps shared by PrepPdf.com for Helping Passing 312-50v10 Exam! PrepPdf.com now offer the **newest 312-50v10 exam dumps**, the PrepPdf.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-50v10 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-50v10-prepaway-exam-dumps.html (**745** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 122
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 as wardriving.
Which Algorithm is this referring to?
A. Wired Equivalent Privacy (WEP)
B. Wi-Fi Protected Access (WPA)
C. Wi-Fi Protected Access 2 (WPA2)
D. Temporal Key Integrity Protocol (TKIP)
Answer: (SHOW ANSWER)
WEP is the currently most used protocol for securing 802.11 networks, also called wireless lans or wlans. In 2007, a new attack on WEP, the PTW attack, was discovered, which allows an attacker to recover the secret key in less than 60 seconds in some cases.
Note: Wardriving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer, smartphone or personal digital assistant (PDA).
References: https://events.ccc.de/camp/2007/Fahrplan/events/1943.en.html

NEW QUESTION: 123
DHCP snooping is a great solution to prevent rogue DHCP servers on your network. Which security feature on switchers leverages the DHCP snooping database to help prevent man-in-the-middle attacks?

A. Port security
B. Dynamic ARP Inspection (DAI)
C. Layer 2 Attack Prevention Protocol (LAPP)
D. Spanning tree
Answer: B (LEAVE A REPLY)

NEW QUESTION: 124
You just set up a security system in your network. In what kind of system would you find the following string of characters used as a rule within its configuration? alert tcp any any ->192.168.100.0/24 21 (msg:""FTP on the network!"";)
A. A Router IPTable
B. A firewall IPTable
C. FTP Server rule
D. An Intrusion Detection System
Answer: D (LEAVE A REPLY)

NEW QUESTION: 125
Your business has decided to add credit card numbers to the data it backs up to tape. Which of the following represents the best practice your business should observe?
A. Encrypt backup tapes that are sent off-site.
B. Hire a security consultant to provide direction.
C. Do not back up cither the credit card numbers or then hashes.
D. Back up the hashes of the credit card numbers not the actual credit card numbers.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 126
Which of the following conditions must be given to allow a tester to exploit a Cross-Site Request Forgery (CSRF) vulnerable web application?
A. The victim user must open the malicious link with an Internet Explorer prior to version 8.
B. The victim user must open the malicious link with a Firefox prior to version 3.
C. The web application should not use random tokens.
D. The session cookies generated by the application do not have the HttpOnly flag set.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 127
It is an entity or event with the potential to adversely impact a system through unauthorized access, destruction, disclosure, denial of service or modification of data.
Which of the following terms best matches the definition?
A. Threat
B. Attack
C. Vulnerability

D. Risk

Answer: (SHOW ANSWER)

A threat is at any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.

References: https://en.wikipedia.org/wiki/Threat_(computer)

NEW QUESTION: 128

Which of the following is the BEST approach to prevent Cross-site Scripting (XSS) flaws?

A. Validate and escape all information sent to a server.

B. Verify access right before allowing access to protected information and UI controls.

C. Use digital certificates to authenticate a server prior to sending data.

D. Verify access right before allowing access to protected information and UI controls.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 129

Which vital role does the U.S. Computer Security Incident Response Team (CSIRT) provide?

A. Measurement of key vulnerability assessments on behalf of the Department of Defense (DOD) and State Department, as well as private sectors

B. Maintenance of the nation's Internet infrastructure, builds out new Internet infrastructure, and decommissions old Internet infrastructure

C. Incident response services to any user, company, government agency, or organization in partnership with the Department of Homeland Security

D. Registration of critical penetration testing for the Department of Homeland Security and public and private sectors

Answer: C (LEAVE A REPLY)

NEW QUESTION: 130

Bob is doing a password assessment for one of his clients. Bob suspects that security policies are not in place. He also suspects that weak passwords are probably the norm throughout the company he is evaluating. Bob is familiar with password weaknesses and key loggers.

Which of the following options best represents the means that Bob can adopt to retrieve passwords from his clients hosts and servers?

A. Hardware and Software Keyloggers.

B. Passwords are always best obtained using Hardware key loggers.

C. Hardware, Software, and Sniffing.

D. Software only, they are the most effective.

Answer: (SHOW ANSWER)

NEW QUESTION: 131

You are a Penetration Tester and are assigned to scan a server. You need to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for.
Which of the below scanning technique will you use?
A. Inverse TCP flag scanning
B. IP Fragment Scanning
C. ACK flag scanning
D. TCP Scanning
Answer: B (LEAVE A REPLY)

NEW QUESTION: 132
Which of the following Nmap commands would be used to perform a stack fingerprinting?
A. Nmap -hU -Q<host(s.>
B. Nmap -sS -0p targe
C. Nmap -O -p80 <host(s.>
D. Nmap -sT -p <host(s.>
E. Nmap -u -o -w2 <host>
Answer: A (LEAVE A REPLY)

NEW QUESTION: 133
What is the process of logging, recording, and resolving events that take place in an organization?
A. Incident Management Process
B. Internal Procedure
C. Security Policy
D. Metrics
Answer: A (LEAVE A REPLY)

NEW QUESTION: 134
In order to show improvement of security over time, what must be developed?
A. Reports
B. Testing tools
C. Metrics
D. Taxonomy of vulnerabilities
Answer: C (LEAVE A REPLY)
Explanation
Today, management demands metrics to get a clearer view of security.
Metrics that measure participation, effectiveness, and window of exposure, however, offer information the organization can use to make plans and improve programs.
References:
http://www.infoworld.com/article/2974642/security/4-security-metrics-that-matter.html

NEW QUESTION: 135
It is a short-range wireless communication technology intended to replace the cables connecting portable of fixed devices while maintaining high levels of security. It allows mobile phones, computers and other devices to connect and communicate using a short-range wireless connection.
Which of the following terms best matches the definition?
A. Bluetooth
B. Radio-Frequency Identification
C. WLAN
D. InfraRed
Answer: A (LEAVE A REPLY)
Explanation
Bluetooth is a standard for the short-range wireless interconnection of mobile phones, computers, and other electronic devices.
References:
http://www.bbc.co.uk/webwise/guides/about-bluetooth

NEW QUESTION: 136
What is the most common method to exploit the "Bash Bug" or "ShellShock" vulnerability?
A. Through Web servers utilizing CGI (Common Gateway Interface) to send a malformed environment variable to a vulnerable Web server
B. Manipulate format strings in text fields
C. SSH
D. SYN Flood
Answer: A (LEAVE A REPLY)
Explanation
Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell.
One specific exploitation vector of the Shellshock bug is CGI-based web servers.
Note: When a web server uses the Common Gateway Interface (CGI) to handle a document request, it passes various details of the request to a handler program in the environment variable list. For example, the variable HTTP_USER_AGENT has a value that, in normal usage, identifies the program sending the request. If the request handler is a Bash script, or if it executes one for example using the system call, Bash will receive the environment variables passed by the server and will process them. This provides a means for an attacker to trigger the Shellshock vulnerability with a specially crafted server request.
References: https://en.wikipedia.org/wiki/Shellshock_(software_bug)#Specific_exploitation_vectors

Valid 312-50v10 Dumps shared by PrepPdf.com for Helping Passing 312-50v10 Exam! PrepPdf.com now offer the **newest 312-50v10 exam dumps**, the PrepPdf.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-50v10 dumps with Test

Engine here: https://www.preppdf.com/EC-COUNCIL/312-50v10-prepaway-exam-dumps.html (**745** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 137
To send a PGP encrypted message, which piece of information from the recipient must the sender have before encrypting the message?
A. Master encryption key
B. Recipient's public key
C. Sender's public key
D. Recipient's private key
Answer: (SHOW ANSWER)

NEW QUESTION: 138
Matthew, a black hat, has managed to open a meterpreter session to one of the kiosk machines in Evil Corp's lobby. He checks his current SID, which is S-1-5-21-1223352397-1872883824-861252104-501. What needs to happen before Matthew has full administrator access?
A. He needs to gain physical access.
B. He needs to disable antivirus protection.
C. He already has admin privileges, as shown by the "501" at the end of the SID.
D. He must perform privilege escalation.
Answer: (SHOW ANSWER)

NEW QUESTION: 139
If you want only to scan fewer ports than the default scan using Nmap tool, which option would you use?
A. -sP
B. -F
C. -P
D. -r
Answer: B (LEAVE A REPLY)

NEW QUESTION: 140
Which of the following Nmap commands will produce the following output?

Output:

```
Staring Nmap 6.47 (http://nmap.org) at 2015-05-26 12:50 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00042s latency).
Not shown: 65530 open | filtered ports, 65529 filtered ports
PORT STATE SERVICE
111/tcp open rpcbind
999/tcp open garcon
1017/tcp open unknown
1021/tcp open exp1
1023/tcp open netvenuechat
2049/tcp open nfs
17501/tcp open unknown
111/udp open rpcbind
123/udp open ntp
137/udp open netbios-ns
2049/udp open zeroconf
17501/udp open|filtered unknown
51857/udp open|filtered unknown
54358/udp open|filtered unknown
56228/udp open|filtered unknown
57598/udp open|filtered unknown
59488/udp open|filtered unknown
60027/udp open|filtered unknown
```

freeqas.com

A. nmap -sS -Pn 192.168.1.1

B. nmap -sT -sX -Pn -p 1-65535 192.168.1.1

C. nmap -sS -sU -Pn -p 1-65535 192.168.1.1

D. nmap -sN -Ps -T4 192.168.1.1

Answer: C (LEAVE A REPLY)

NEW QUESTION: 141

You are a Penetration Tester and are assigned to scan a server. You need to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for.

Which of the below scanning technique will you use?

A. ACK flag scanning

B. TCP Scanning

C. IP Fragment Scanning

D. Inverse TCP flag scanning

Answer: C (LEAVE A REPLY)

NEW QUESTION: 142
You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.
What is the best Nmap command you will use?
A. nmap -T4 -F 10.10.0.0/24
B. nmap -T4 -r 10.10.1.0/24
C. nmap -T4 -O 10.10.0.0/24
D. nmap -T4 -q 10.10.0.0/24
Answer: A (LEAVE A REPLY)

NEW QUESTION: 143
Which of the following programs is usually targeted at Microsoft Office products?
A. Polymorphic virus
B. Multipart virus
C. Macro virus
D. Stealth virus
Answer: C (LEAVE A REPLY)
A macro virus is a virus that is written in a macro language: a programming language which is embedded inside a software application (e.g., word processors and spreadsheet applications). Some applications, such as Microsoft Office, allow macro programs to be embedded in documents such that the macros are run automatically when the document is opened, and this provides a distinct mechanism by which malicious computer instructions can spread.
References: https://en.wikipedia.org/wiki/Macro_virus

NEW QUESTION: 144
Which tool can be used to silently copy files from USB devices?
A. USB Sniffer
B. USB Grabber
C. USB Snoopy
D. USB Dumper
Answer: D (LEAVE A REPLY)

NEW QUESTION: 145
During a wireless penetration test, a tester detects an access point using WPA2 encryption. Which of the following attacks should be used to obtain the key?
A. The tester must change the MAC address of the wireless network card and then use the AirTraf tool to obtain the key.
B. The tester must capture the WPA2 authentication handshake and then crack it.
C. The tester cannot crack WPA2 because it is in full compliance with the IEEE 802.11i standard.
D. The tester must use the tool inSSIDer to crack it using the ESSID of the network.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 146
The Open Web Application Security Project (OWASP) testing methodology addresses the need to secure web applications by providing which one of the following services?
A. An extensible security framework named COBIT
B. A list of flaws and how to fix them
C. Web application patches
D. A security certification for hardened web applications
Answer: (SHOW ANSWER)

NEW QUESTION: 147
Employees in a company are no longer able to access Internet web sites on their computers. The network administrator is able to successfully ping IP address of web servers on the Internet and is able to open web sites by using an IP address in place of the URL. The administrator runs the nslookup command for www.eccouncil.org and receives an error message stating there is no response from the server. What should the administrator do next?
A. Configure the firewall to allow traffic on TCP port 53.
B. Configure the firewall to allow traffic on TCP port 8080.
C. Configure the firewall to allow traffic on TCP ports 53 and UDP port 53.
D. Configure the firewall to allow traffic on TCP ports 80 and UDP port 443.
Answer: (SHOW ANSWER)

NEW QUESTION: 148
In IPv6 what is the major difference concerning application layer vulnerabilities compared to IPv4?
A. Vulnerabilities in the application layer are independent of the network layer. Attacks and mitigation techniques are almost identical.
B. Due to the extensive security measures built in IPv6, application layer vulnerabilities need not be addresses.
C. Implementing IPv4 security in a dual-stack network offers protection from IPv6 attacks too.
D. Vulnerabilities in the application layer are greatly different from IPv4.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 149
A penetration test was done at a company. After the test, a report was written and given to the company's IT authorities. A section from the report is shown below:
According to the section from the report, which of the following choice is true?
A. MAC Spoof attacks cannot be performed.
B. There is access control policy between VLANs.
C. Possibility of SQL Injection attack is eliminated.
D. A stateful firewall can be used between intranet (LAN) and DMZ.
Answer: (SHOW ANSWER)

NEW QUESTION: 150
Sam is working as s pen-tester in an organization in Houston. He performs penetration testing on IDS in order to find the different ways an attacker uses to evade the IDS. Sam sends a large amount of packets to the target IDS that generates alerts, which enable Sam to hide the real traffic. What type of method is Sam using to evade IDS?
A. Insertion Attack
B. False Positive Generation
C. Denial-of-Service
D. Obfuscating
Answer: B (LEAVE A REPLY)

NEW QUESTION: 151
You are the Network Admin, and you get a compliant that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL.
What may be the problem?
A. Traffic is Blocked on TCP Port 54
B. Traffic is Blocked on UDP Port 80
C. Traffic is Blocked on TCP Port 80
D. Traffic is Blocked on UDP Port 53
Answer: (SHOW ANSWER)

Valid 312-50v10 Dumps shared by PrepPdf.com for Helping Passing 312-50v10 Exam! PrepPdf.com now offer the **newest 312-50v10 exam dumps**, the PrepPdf.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-50v10 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-50v10-prepaway-exam-dumps.html (**745** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 152
What are the three types of compliance that the Open Source Security Testing Methodology Manual (OSSTMM) recognizes?
A. Audit, standards based, regulatory
B. Legislative, contractual, standards based
C. Legal, performance, audit
D. Contractual, regulatory, industry
Answer: (SHOW ANSWER)

NEW QUESTION: 153

Eve stole a file named secret.txt, transferred it to her computer and she just entered these commands:



What is she trying to achieve?

A. She is encrypting the file.

B. She is using John the Ripper to view the contents of the file.

C. She is using ftp to transfer the file to another hacker named John.

D. She is using John the Ripper to crack the passwords in the secret.txt file.

Answer: (SHOW ANSWER)

NEW QUESTION: 154

A network administrator received an administrative alert at 3:00 a.m. from the intrusion detection system. The alert was generated because a large number of packets were coming into the network over ports 20 and 21. During analysis, there were no signs of attack on the FTP servers. How should the administrator classify this situation?

A. True negatives

B. False negatives

C. False positives

D. True positives

Answer: C (LEAVE A REPLY)

NEW QUESTION: 155

>NMAP -sn 192.168.11.200-215 The NMAP command above performs which of the following?

A. A port scan

B. A ping scan

C. A trace sweep

D. An operating system detect

Answer: (SHOW ANSWER)

NEW QUESTION: 156

The following is a sample of output from a penetration tester's machine targeting a machine with the IP address of 192.168.1.106:



What is most likely taking place?

A. Ping sweep of the 192.168.1.106 network

B. Denial of service attack on 192.168.1.106

C. Remote service brute force attempt

D. Port scan of 192.168.1.106

Answer: C (LEAVE A REPLY)

NEW QUESTION: 157

Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

A. Nessus

B. Tcpdump

C. Jack the ripper

D. Ethereal

Answer: (SHOW ANSWER)

NEW QUESTION: 158

You are attempting to man-in-the-middle a session. Which protocol will allow you to guess a sequence number?

A. TCP

B. ICMP

C. UPD

D. UPX

Answer: (SHOW ANSWER)

NEW QUESTION: 159

You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.

What is the best nmap command you will use?

A. nmap -T4 -F 10.10.0.0/24

B. nmap -T4 -r 10.10.1.0/24

C. nmap -T4 -O 10.10.0.0/24

D. nmap -T4 -q 10.10.0.0/24

Answer: A (LEAVE A REPLY)

command = nmap -T4 -F
description = This scan is faster than a normal scan because it uses the aggressive timing template and scans fewer ports.
References: https://svn.nmap.org/nmap/zenmap/share/zenmap/config/scan_profile.usp

NEW QUESTION: 160
Fingerprinting an Operating System helps a cracker because:
A. It opens a security-delayed window based on the port being scanned
B. It informs the cracker of which vulnerabilities he may be able to exploit on your system
C. It defines exactly what software you have installed
D. It doesn't depend on the patches that have been applied to fix existing security holes
Answer: B (LEAVE A REPLY)

NEW QUESTION: 161
Gavin owns a white-hat firm and is performing a website security audit for one of his clients. He begins by running a scan which looks for common misconfigurations and outdated software versions. Which of the following tools is he most likely using?
A. Metasploit
B. Armitage
C. Nikto
D. Nmap
Answer: C (LEAVE A REPLY)

NEW QUESTION: 162
Which of the following Secure Hashing Algorithm (SHA) produces a 160-bit digest from a message with a maximum length of (264-1) bits and resembles the MD5 algorithm?
A. SHA-2
B. SHA-1
C. SHA-3
D. SHA-0
Answer: (SHOW ANSWER)

NEW QUESTION: 163
You need a tool that can do network intrusion prevention and intrusion detection, function as a network sniffer, and record network activity. What tool would you most likely select?
A. Nmap
B. Snort
C. Nessus
D. Cain & Abel
Answer: B (LEAVE A REPLY)

NEW QUESTION: 164
Which system consists of a publicly available set of databases that contain domain name registration contact information?
A. WHOIS
B. IANA
C. IETF
D. CAPTCHA
Answer: A (LEAVE A REPLY)

NEW QUESTION: 165
Which of the following is designed to identify malicious attempts to penetrate systems?
A. Intrusion Detection System
B. Firewall
C. Proxy
D. Router
Answer: A (LEAVE A REPLY)
An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces electronic reports to a management station.
References: https://en.wikipedia.org/wiki/Intrusion_detection_system

NEW QUESTION: 166
Which of the following tools are used for enumeration? (Choose three.)
A. Cheops
B. DumpSec
C. SID2USER
D. SolarWinds
E. USER2SID
Answer: B,C,E (LEAVE A REPLY)

Valid 312-50v10 Dumps shared by PrepPdf.com for Helping Passing 312-50v10 Exam! PrepPdf.com now offer the **newest 312-50v10 exam dumps**, the PrepPdf.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-50v10 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-50v10-prepaway-exam-dumps.html (**745** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 167
When utilizing technical assessment methods to assess the security posture of a network, which of the following techniques would be most effective in determining whether end-user security training would be beneficial?

A. Vulnerability scanning
B. Social engineering
C. Network sniffing
D. Application security testing
Answer: (SHOW ANSWER)

NEW QUESTION: 168
Sophia travels a lot and worries that her laptop containing confidential documents might be stolen. What is the best protection that will work for her?
A. Disk encryption
B. BIOS password
C. Hidden folders
D. Password protected files
Answer: A (LEAVE A REPLY)

NEW QUESTION: 169
Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drown based on these scan results?
TCP port 21 - no response
TCP port 22 - no response
TCP port 23 - Time-to-live exceeded
A. The scan on port 23 passed through the filtering device. This indicates that port 23 was not blocked at the firewall
B. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server
C. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error
D. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host
Answer: (SHOW ANSWER)

NEW QUESTION: 170
Which of the following is a strong post designed to stop a car?
A. Fence
B. Gate
C. Bollard
D. Reinforced rebar
Answer: C (LEAVE A REPLY)

NEW QUESTION: 171

When a security analyst prepares for the formal security assessment - what of the following should be done in order to determine inconsistencies in the secure assets database and verify that system is compliant to the minimum security baseline?

A. Interviewing employees and network engineers

B. Source code review

C. Data items and vulnerability scanning

D. Reviewing the firewalls configuration

Answer: C (LEAVE A REPLY)

NEW QUESTION: 172

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. Polymorphism

C. Escrow

D. Collusion

Answer: A (LEAVE A REPLY)

NEW QUESTION: 173

Which type of security document is written with specific step-by-step details?

A. Paradigm

B. Policy

C. Procedure

D. Process

Answer: C (LEAVE A REPLY)

NEW QUESTION: 174

While reviewing the result of scanning run against a target network you come across the following:

```
system.sysDescr.0 : DISPLAY STRING- (ascii): Cisco Internetwork Operating
System Software
IOS (tm) 4500 Software (C4500-IS-M), Version 12.0(9), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2000 by Cisco Systems, Inc.
Compiled Tue 25-Jan-00 04:28 by bettyl
system.sysObjectID.0 : OBJECT IDENTIFIER:
.iso.org.dod.internet.Private.enter  .Cisco.c  .Cisco4700
system.sysUpTime.0 : Timeticks: (1563980  18 days, 2:26:20.17
system.sysContact.0 : DISPLAY STRING- (ascii):
system.sysName.0 : DISPLAY STRING- (ascii): somerroutername
system.sysLocation.0 : DISPLAY STRING- (ascii):
system.sysServices.0 : INTEGER: 6
system.sysORLastChange.0 : Timeticks: (0) 0:00:00.00
```

EC-Council
Pleqas.com

Which among the following can be used to get this output?
A. An SNMP walk
B. A Bo2k system query.
C. nmap protocol scan
D. A sniffer
Answer: A (LEAVE A REPLY)

NEW QUESTION: 175
A virus that attempts to install itself inside the file it is infecting is called?
A. Tunneling virus
B. Stealth virus
C. Cavity virus
D. Polymorphic virus
Answer: C (LEAVE A REPLY)

NEW QUESTION: 176
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 (LEAVE A REPLY)
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

NEW QUESTION: 177
A network admin contacts you. He is concerned that ARP spoofing or poisoning might occur on his network. What are some things he can do to prevent it? Select the best answers.
A. Use a firewall between all LAN segments.
B. Use port security on his switches.
C. Use only static IP addresses on all PC's.
D. Use a tool like ARPwatch to monitor for strange ARP activity.
E. If you have a small network, use static ARP entries.
Answer: B,D,E (LEAVE A REPLY)

NEW QUESTION: 178
Risks=Threats x Vulnerabilities is referred to as the:
A. Threat assessment

B. Risk equation
C. Disaster recovery formula
D. BIA equation
Answer: (SHOW ANSWER)

NEW QUESTION: 179
Assume a business-crucial web-site of some company that is used to sell handsets to the customers worldwide. All the developed components are reviewed by the security team on a monthly basis. In order to drive business further, the web-site developers decided to add some 3rd party marketing tools on it. The tools are written in JavaScript and can track the customer's activity on the site. These tools are located on the servers of the marketing company.
What is the main security risk associated with this scenario?
A. External scripts increase the outbound company data traffic which leads greater financial losses
B. External scripts have direct access to the company servers and can steal the data from there
C. External script contents could be maliciously modified without the security team knowledge
D. There is no risk at all as the marketing services are trustworthy
Answer: C (LEAVE A REPLY)

NEW QUESTION: 180
Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?
A. Nikto
B. Snort
C. John the Ripper
D. Dsniff
Answer: A (LEAVE A REPLY)
Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/CGIs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.
References: https://en.wikipedia.org/wiki/Nikto_Web_Scanner

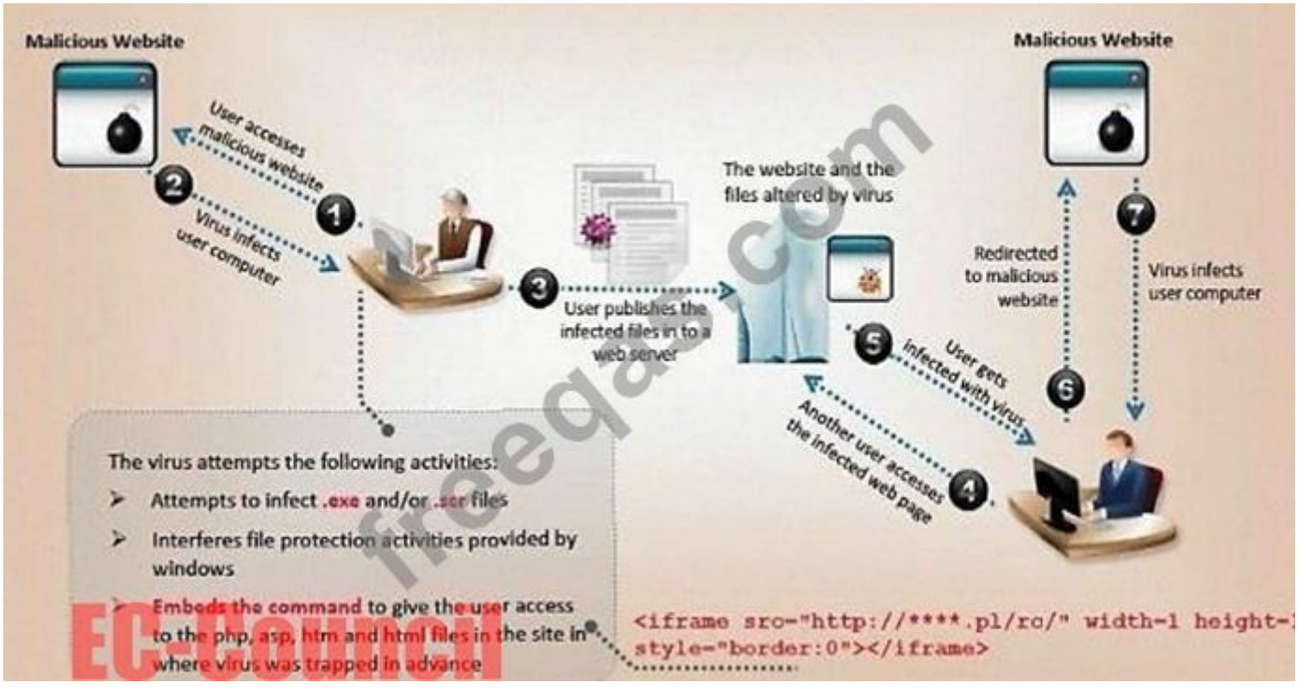
NEW QUESTION: 181
> NMAP -sn 192.168.11.200-215
The NMAP command above performs which of the following?
A. A ping scan
B. A trace sweep
C. An operating system detect
D. A port scan
Answer: A (LEAVE A REPLY)

Explanation
NMAP -sn (No port scan)
This option tells Nmap not to do a port scan after host discovery, and only print out the available hosts that responded to the host discovery probes. This is often known as a "ping scan", but you can also request that traceroute and NSE host scripts be run.
References: https://nmap.org/book/man-host-discovery.html

Valid 312-50v10 Dumps shared by PrepPdf.com for Helping Passing 312-50v10 Exam! PrepPdf.com now offer the **newest 312-50v10 exam dumps**, the PrepPdf.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-50v10 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-50v10-prepaway-exam-dumps.html (**745** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 182
In many states sending spam is illegal. Thus, the spammers have techniques to try and ensure that no one knows they sent the spam out to thousands of users at a time. Which of the following best describes what spammers use to hide the origin of these types of e-mails?
A. A blacklist of companies that have their mail server relays configured to allow traffic only to their specific domain name.
B. Mail relaying, which is a technique of bouncing e-mail from internal to external mails servers continuously.
C. A blacklist of companies that have their mail server relays configured to be wide open.
D. Tools that will reconfigure a mail server's relay component to send the e-mail back to the spammers occasionally.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 183
ViruXine.W32 virus hides their presence by changing the underlying executable code.
This Virus code mutates while keeping the original algorithm intact, the code changes itself each time it runs, but the function of the code (its semantics) will not change at all.



Here is a section of the Virus code:

```
1.  lots of encrypted code
2.  …
3.  Decryption_Code:
4.  C=C+1
5.  A=Encrypted
6.  Loop:
7.  B=*A
8.  C=3214*A
9.  B=B XOR CryptoKey
10. *A=B
11. C=1
12. C=A+B
13. A=A+1
14. GOTO Loop IF NOT A=Decryption_Code
15. C=C^2
16. GOTO Encrypted
17. CryptoKey:
18. some_random_number
```

What is this technique called?

A. Stealth Virus

B. Dravidic Virus

C. Polymorphic Virus

D. Metamorphic Virus

Answer: C (LEAVE A REPLY)

NEW QUESTION: 184

Take a look at the following attack on a Web Server using obstructed URL:



How would you protect from these attacks?

A. Create rules in IDS to alert on strange Unicode requests

B. Configure the Web Server to deny requests involving "hex encoded" characters

C. Enable Active Scripts Detection at the firewall and routers

D. Use SSL authentication on Web Servers

Answer: (SHOW ANSWER)

NEW QUESTION: 185

Jesse receives an email with an attachment labeled "Court_Notice_21206.zip". Inside the zip file is a file named "Court_Notice_21206.docx.exe" disguised as a word document. Upon execution, a window appears stating, "This word document is corrupt." In the background, the file copies itself to Jesse APPDATA\local directory and begins to beacon to a C2 server to download additional malicious binaries.

What type of malware has Jesse encountered?

A. Trojan

B. Worm

C. Macro Virus

D. Key-Logger

Answer: A (LEAVE A REPLY)

Explanation

In computing, Trojan horse, or Trojan, is any malicious computer program which is used to hack into a computer by misleading users of its true intent. Although their payload can be anything, many modern forms act as a backdoor, contacting a controller which can then have unauthorized access to the affected computer.

References: https://en.wikipedia.org/wiki/Trojan_horse_(computing)

NEW QUESTION: 186

Insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key.

Suppose a malicious user Rob tries to get access to the account of a benign user Ned.

Which of the following requests best illustrates an attempt to exploit an insecure direct object reference vulnerability?

A. "GET/restricted/accounts/?name=Ned HTTP/1.1 Host: westbank.com"

B. "GET/restricted/bank.getaccount('Ned') HTTP/1.1 Host: westbank.com"

C. "GET/restricted/\r\n\%00account%00Ned%00access HTTP/1.1 Host: westbank.com"

D. "GET/restricted/goldtransfer?to=Rob&from=1 or 1=1' HTTP/1.1Host: westbank.com"

Answer: A (LEAVE A REPLY)

NEW QUESTION: 187
Which of the following Bluetooth hacking techniques does an attacker use to send messages to users without the recipient's consent, similar to email spamming?
A. Bluejacking
B. Bluesniffing
C. Bluesmacking
D. Bluesnarfing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 188
You have successfully gained access to a linux server and would like to ensure that the succeeding outgoing traffic from this server will not be caught by a Network Based Intrusion Detection Systems (NIDS).
What is the best way to evade the NIDS?
A. Encryption
B. Protocol Isolation
C. Alternate Data Streams
D. Out of band signalling
Answer: (SHOW ANSWER)
When the NIDS encounters encrypted traffic, the only analysis it can perform is packet level analysis, since the application layer contents are inaccessible. Given that exploits against today's networks are primarily targeted against network services (application layer entities), packet level analysis ends up doing very little to protect our core business assets.
References: http://www.techrepublic.com/article/avoid-these-five-common-ids- implementation-errors/

NEW QUESTION: 189
Which of the following tools can be used for passive OS fingerprinting?
A. tcpdump
B. tracert
C. nmap
D. ping
Answer: A (LEAVE A REPLY)

NEW QUESTION: 190
Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients.
You are requested to accept the offer and you oblige. After 2 days. Bob denies that he had ever sent a mail.
What do you want to ""know"" to prove yourself that it was Bob who had send a mail?
A. Authentication
B. Confidentiality
C. Integrity
D. Non-Repudiation

Answer: (SHOW ANSWER)

NEW QUESTION: 191
Analyst is investigating proxy logs and found out that one of the internal user visited website storing suspicious java scripts. After opening one of them, he noticed that it is very hard to understand the code and that all codes differ from the typical java script. What is the name of this technique to hide the code and extend analysis time?
A. Steganography
B. Obfuscation
C. Code encoding
D. Encryption
Answer: B (LEAVE A REPLY)

NEW QUESTION: 192
Bob is going to perform an active session hijack against Brownies Inc. He has found a target that allows session oriented connections (Telnet) and performs the sequence prediction on the target operating system. He manages to find an active session due to the high level of traffic on the network. What is Bob supposed to do next?
A. Take one of the parties offline
B. Take over the session
C. Reverse sequence prediction
D. Guess the sequence numbers
Answer: D (LEAVE A REPLY)

NEW QUESTION: 193
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 (LEAVE A REPLY)
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

NEW QUESTION: 194
Which of the following statements is FALSE with respect to Intrusion Detection Systems?
A. Intrusion Detection Systems can be configured to distinguish specific content in network packets
B. Intrusion Detection Systems can easily distinguish a malicious payload in an encrypted traffic
C. Intrusion Detection Systems require constant update of the signature library
D. Intrusion Detection Systems can examine the contents of the data n context of the network protocol

Answer: B (LEAVE A REPLY)

NEW QUESTION: 195
How do employers protect assets with security policies pertaining to employee surveillance activities?
A. Employers use informal verbal communication channels to explain employee monitoring activities to employees.
B. Employers promote monitoring activities of employees as long as the employees demonstrate trustworthiness.
C. Employers provide employees written statements that clearly discuss the boundaries of monitoring activities and consequences.
D. Employers use network surveillance to monitor employee email traffic, network access, and to record employee keystrokes.
Answer: C (LEAVE A REPLY)

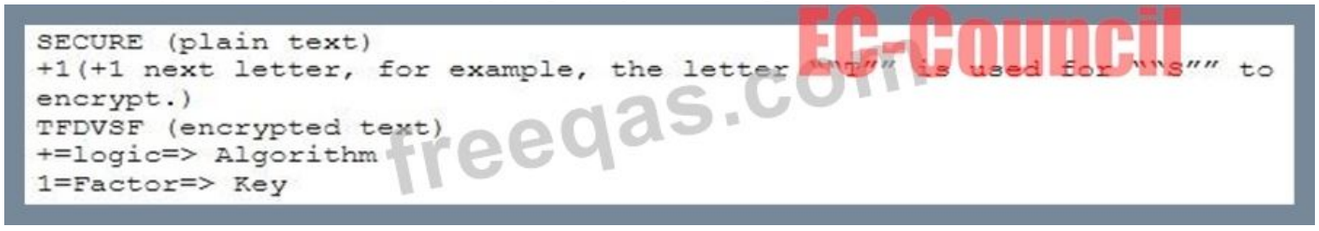
NEW QUESTION: 196
In which of the following password protection technique, random strings of characters are added to the password before calculating their hashes?
A. Keyed Hashing
B. Key Stretching
C. Salting
D. Double Hashing
Answer: C (LEAVE A REPLY)
Explanation

Valid 312-50v10 Dumps shared by PrepPdf.com for Helping Passing 312-50v10 Exam! PrepPdf.com now offer the **newest 312-50v10 exam dumps**, the PrepPdf.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-50v10 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-50v10-prepaway-exam-dumps.html (**745** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 197
Which of the following steps for risk assessment methodology refers to vulnerability identification?
A. Identifies sources of harm to an IT system (Natural, Human, Environmental)
B. Assigns values to risk probabilities; Impact values
C. Determines if any flaws exist in systems, policies, or procedures
D. Determines risk probability that vulnerability will be exploited (High, Medium, Low)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 198

Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries.) More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and that are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.
Basic example to understand how cryptography works is given below:



EC-Council
freeqas.com

Which of the following choices is true about cryptography?
A. Symmetric-key algorithms are a class of algorithms for cryptography that use the different cryptographic keys for both encryption of plaintext and decryption of ciphertext.
B. Public-key cryptography, also known as asymmetric cryptography, public key is for decrypt, private key is for encrypt.
C. Algorithm is not the secret, key is the secret.
D. Secure Sockets Layer (SSL) use the asymmetric encryption both (public/private key pair) to deliver the shared session key and to achieve a communication way.
Answer: (SHOW ANSWER)

NEW QUESTION: 199
In which of the following password protection technique, random strings of characters are added to the password before calculating their hashes?
A. Double Hashing
B. Key Stretching
C. Keyed Hashing
D. Salting
Answer: D (LEAVE A REPLY)

NEW QUESTION: 200
In an internal security audit, the white hat hacker gains control over a user account and attempts to acquire access to another account's confidential files and information. How can he achieve this?
A. Port Scanning
B. Privilege Escalation
C. Shoulder-Surfing
D. Hacking Active Directory
Answer: B (LEAVE A REPLY)

NEW QUESTION: 201

During the security audit of IT processes, an IS auditor found that there were no documented security procedures. What should the IS auditor do?
A. Identify and evaluate existing practices
B. Terminate the audit
C. Create a procedures document
D. Conduct compliance testing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 202
Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drown based on these scan results?
TCP port 21 - no response
TCP port 22 - no response
TCP port 23 - Time-to-live exceeded
A. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error
B. The scan on port 23 passed through the filtering device. This indicates that port 23 was not blocked at the firewall
C. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server
D. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host
Answer: B (LEAVE A REPLY)

NEW QUESTION: 203
Which protocol is used for setting up secure channels between two devices, typically in VPNs?
A. PPP
B. IPSEC
C. PEM
D. SET
Answer: (SHOW ANSWER)

NEW QUESTION: 204
Which of the below hashing functions are not recommended for use?
A. MD5, SHA-1
B. SHA-2. SHA-3
C. SHA-1.ECC
D. MD5. SHA-5
Answer: (SHOW ANSWER)

NEW QUESTION: 205
Based on the below log, which of the following sentences are true?

Mar 1, 2016, 7:33:28 AM 10.240.250.23 - 54373 10.249.253.15 - 22 tcp_ip

A. Application is FTP and 10.240.250.23 is the client and 10.249.253.15 is the server

B. Application is SSH and 10.240.250.23 is the server and 10.249.253.15 is the server

C. SSH communications are encrypted it's impossible to know who is the client or the server

D. Application is SSH and 10.240.250.23 is the client and 10.249.253.15 is the server

Answer: D (LEAVE A REPLY)

NEW QUESTION: 206

Emil uses nmap to scan two hosts using this command.

nmap -sS -T4 -O 192.168.99.1 192.168.99.7

He receives this output:

```
Nmap scan report for 192.168.99.1
Host is up (0.00082s latency).
Not shown: 994 filtered ports
PORT STATE SERVICE
21/tcp open ftp
23/tcp open telnet
53/tcp open domain
80/tcp open http
161/tcp closed snmp
MAC Address: B0:75:D5:33:57:74 (ZTE)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

Nmap scan report for 192.168.99.7
Host is up (0.000047s latency).
All 1000 scanned ports on 192.168.99.7 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
```

What is his conclusion?

A. He performed a SYN scan and OS scan on hosts 192.168.99.1 and 192.168.99.7.

B. Host 192.168.99.7 is down.

C. Host 192.168.99.7 is an iPad.

D. Host 192.168.99.1 is the host that he launched the scan from.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 207

Elliot is in the process of exploiting a web application that uses SQL as a back-end database. He is determined that the application is vulnerable to SQL injection and has introduced conditional timing delays into injected queries to determine whether they are successful. What type of SQL injection is Elliot most likely performing?

A. Error-based SQL injection

B. NoSQL injection
C. Union-based SQL injection
D. Blind SQL injection
Answer: (SHOW ANSWER)

NEW QUESTION: 208
Gavin owns a white-hat firm and is performing a website security audit for one of his clients. He begins by running a scan which looks for common misconfigurations and outdated software versions. Which of the following tools is he most likely using?
A. Metasploit
B. Nikto
C. Nmap
D. Armitage
Answer: (SHOW ANSWER)

NEW QUESTION: 209
Shellshock had the potential for an unauthorized user to gain access to a server. It affected many internet-facing services, which OS did it not directly affect?
A. Linux
B. Unix
C. Windows
D. OS X
Answer: C (LEAVE A REPLY)

NEW QUESTION: 210
Your team has won a contract to infiltrate an organization. The company wants to have the attack be as realistic as possible; therefore, they did not provide any information besides the company name. What should be the first step in security testing the client?
A. Reconnaissance
B. Escalation
C. Scanning
D. Enumeration
Answer: A (LEAVE A REPLY)
Explanation

NEW QUESTION: 211
What type of vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?
A. Cross-site request forgery
B. Cross-site scripting
C. Session hijacking

D. Server side request forgery
Answer: A (LEAVE A REPLY)
Explanation/Reference:

Valid 312-50v10 Dumps shared by PrepPdf.com for Helping Passing 312-50v10 Exam! PrepPdf.com now offer the **newest 312-50v10 exam dumps**, the PrepPdf.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-50v10 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-50v10-prepaway-exam-dumps.html (**745** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 212
When you are collecting information to perform a data analysis, Google commands are very useful to find sensitive information and files. These files may contain information about passwords, system functions, or documentation. What command will help you to search files using Google as a search engine?
A. site: target.com filetype:xls username password email
B. inurl: target.com filename:xls username password email
C. domain: target.com archieve:xls username password email
D. site: target.com file:xls username password email
Answer: (SHOW ANSWER)

NEW QUESTION: 213
Initiating an attack against targeted businesses and organizations, threat actors compromise a carefully selected website by inserting an exploit resulting in malware infection. The attackers run exploits on well-known and trusted sites likely to be visited by their targeted victims. Aside from carefully choosing sites to compromise, these attacks are known to incorporate zero-day exploits that target unpatched vulnerabilities. Thus, the targeted entities are left with little or no defense against these exploits.
What type of attack is outlined in the scenario?
A. Watering Hole Attack
B. Heartbleed Attack
C. Shellshock Attack
D. Spear Phising Attack
Answer: (SHOW ANSWER)
Explanation
Watering Hole is a computer attack strategy, in which the victim is a particular group (organization, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some member of the targeted group gets infected.

NEW QUESTION: 214

A security consultant decides to use multiple layers of anti-virus defense, such as end user desktop anti-virus and E-mail gateway. This approach can be used to mitigate which kind of attack?

A. Scanning attack

B. Social engineering attack

C. Forensic attack

D. ARP spoofing attack

Answer: (SHOW ANSWER)

NEW QUESTION: 215

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 need to modify?

A. Networks

B. Boot.ini

C. Hosts

D. Sudoers

Answer: (SHOW ANSWER)

NEW QUESTION: 216

Which of the following statements is FALSE with respect to Intrusion Detection Systems?

A. Intrusion Detection Systems can be configured to distinguish specific content in network packets

B. Intrusion Detection Systems require constant update of the signature library

C. Intrusion Detection Systems can examine the contents of the data in context of the network protocol

D. Intrusion Detection Systems can easily distinguish a malicious payload in an encrypted traffic

Answer: D (LEAVE A REPLY)

NEW QUESTION: 217

To maintain compliance with regulatory requirements, a security audit of the systems on a network must be performed to determine their compliance with security policies. Which one of the following tools would most likely be used in such an audit?

A. Vulnerability scanner

B. Protocol analyzer

C. Port scanner

D. Intrusion Detection System

Answer: A (LEAVE A REPLY)

Explanation

A vulnerability scanner is a computer program designed to assess computers, computer systems, networks or applications for weaknesses.

They can be run either as part of vulnerability management by those tasked with protecting systems - or by black hat attackers looking to gain unauthorized access.

References: https://en.wikipedia.org/wiki/Vulnerability_scanner

NEW QUESTION: 218
The network administrator contacts you and tells you that she noticed the temperature on the internal wireless router increases by more than 20% during weekend hours when the office was closed. She asks you to investigate the issue because she is busy dealing with a big conference and she doesn't have time to perform the task.
What tool can you use to view the network traffic being sent and received by the wireless router?
A. Wireshark
B. Nessus
C. Netcat
D. Netstat
Answer: A (LEAVE A REPLY)
Explanation
Wireshark is a Free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

NEW QUESTION: 219
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 (LEAVE A REPLY)
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

NEW QUESTION: 220
Which of the following describes the characteristics of a Boot Sector Virus?
A. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR
B. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR
C. Modifies directory table entries so that directory entries point to the virus code instead of the actual program
D. Overwrites the original MBR and only executes the new virus code
Answer: A (LEAVE A REPLY)
Explanation
A boot sector virus is a computer virus that infects a storage device's master boot record (MBR). The virus moves the boot sector to another location on the hard drive.
References: https://www.techopedia.com/definition/26655/boot-sector-virus

NEW QUESTION: 221
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. Man-in-the-middle attack
B. Replay attack
C. Traffic analysis attack
D. Meet-in-the-middle attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 222
When tuning security alerts, what is the best approach?
A. Decrease False negatives
B. Tune to avoid False positives and False Negatives
C. Rise False positives Rise False Negatives
D. Decrease the false positives
Answer: B (LEAVE A REPLY)

NEW QUESTION: 223
Steve, a scientist who works in a governmental security agency, developed a technological solution to identify people based on walking patterns and implemented this approach to a physical control access.
A camera captures people walking and identifies the individuals using Steve's approach.
After that, people must approximate their RFID badges. Both the identifications are required to open the door.
In this case, we can say:
A. Biological motion cannot be used to identify people
B. Although the approach has two phases, it actually implements just one authentication factor
C. The solution will have a high level of false positives
D. The solution implements the two authentication factors: physical object and physical characteristic
Answer: (SHOW ANSWER)

NEW QUESTION: 224
Which command can be used to show the current TCP/IP connections?
A. Net use connection
B. Netsh
C. Netstat
D. Net use
Answer: B (LEAVE A REPLY)

NEW QUESTION: 225
What type of OS fingerprinting technique sends specially crafted packets to the remote OS and analyzes the received response?

A. Passive
B. Active
C. Reflective
D. Distributive
Answer: B (LEAVE A REPLY)
Explanation

NEW QUESTION: 226
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. 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
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. Launch DDOS attacks against Merclyn Barley Bank's routers and firewall systems using 100, 000 or more "zombies" and "bots"
D. 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
Answer: (SHOW ANSWER)

Valid 312-50v10 Dumps shared by PrepPdf.com for Helping Passing 312-50v10 Exam! PrepPdf.com now offer the **newest 312-50v10 exam dumps**, the PrepPdf.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-50v10 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-50v10-prepaway-exam-dumps.html (**745** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 227

ping -* 6 192.168.0.101
output
Pinging 192.168.0.101 with 32 bytes of data:
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.0.101:
Packets: Sent=6, Received=6, Lost=0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum=0ms, Maximum=0ms, Average=0ms
What does the option * indicate?

A. t

B. n

C. s

D. a

Answer: B (LEAVE A REPLY)

NEW QUESTION: 228

One of your team members has asked you to analyze the following SOA record. What is the version?
Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800
2400.) (Choose four.)

A. 4800

B. 200303028

C. 60

D. 2400

E. 3600

F. 604800

Answer: B (LEAVE A REPLY)

NEW QUESTION: 229

You are performing a penetration test for a client and have gained shell access to a Windows machine on the internal network. You intend to retrieve all DNS records for the internal domain. If the DNS server is at 192.168.10.2 and the domain name is abccorp.local, what command would you type at the nslookup prompt to attempt a zone transfer?

A. ls -d accorp.local

B. list server=192.168.10.2 type=all

C. list domain=abccorp.local type=zone

D. lserver 192.168.10.2 -t all

Answer: A (LEAVE A REPLY)

NEW QUESTION: 230
What is the proper response for a NULL scan if the port is open?
A. No response
B. FIN
C. SYN
D. ACK
E. PSH
F. RST
Answer: A (LEAVE A REPLY)

NEW QUESTION: 231
Chandler works as a pen-tester in an IT-firm in New York. As a part of detecting viruses in the systems, he uses a detection method where the anti-virus executes the malicious codes on a virtual machine to simulate CPU and memory activities.
Which type of virus detection method did Chandler use in this context?
A. Code Emulation
B. Integrity checking
C. Heuristic Analysis
D. Scanning
Answer: (SHOW ANSWER)

NEW QUESTION: 232
Which of the following is used to indicate a single-line comment in structured query language (SQL)?
A. ||
B. %%
C. --
D. "
Answer: C (LEAVE A REPLY)

NEW QUESTION: 233
Which of the following is an application that requires a host application for replication?
A. Micro
B. Worm
C. Trojan
D. Virus
Answer: D (LEAVE A REPLY)
Explanation
Computer viruses infect a variety of different subsystems on their hosts. A computer virus is a malware that, when executed, replicates by reproducing itself or infecting other programs by modifying them. Infecting

computer programs can include as well, data files, or the boot sector of the hard drive. When this replication succeeds, the affected areas are then said to be "infected".
References: https://en.wikipedia.org/wiki/Computer_virus

NEW QUESTION: 234
Which of the following can take an arbitrary length of input and produce a message digest output of 160 bit?
A. HAVAL
B. MD4
C. SHA-1
D. MD5
Answer: C (LEAVE A REPLY)

NEW QUESTION: 235
You have successfully compromised a machine on the network and found a server that is alive on the same network. You tried to ping it but you didn't get any response back.
What is happening?
A. ICMP could be disabled on the target server.
B. The ARP is disabled on the target server.
C. TCP/IP doesn't support ICMP.
D. You need to run the ping command with root privileges.
Answer: A (LEAVE A REPLY)
Explanation

NEW QUESTION: 236
What is one thing a tester can do to ensure that the software is trusted and is not changing or tampering with critical data on the back end of a system it is loaded on?
A. Systems security and architecture review
B. Proper testing
C. Secure coding principles
D. Analysis of interrupts within the software
Answer: (SHOW ANSWER)

NEW QUESTION: 237
To maintain compliance with regulatory requirements, a security audit of the systems on a network must be performed to determine their compliance with security policies. Which one of the following tools would most likely be used in such an audit?
A. Protocol analyzer
B. Vulnerability scanner
C. Intrusion Detection System
D. Port scanner
Answer: B (LEAVE A REPLY)

NEW QUESTION: 238
A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the Prometric Online Testing - Reports https://ibt1.prometric.com/users/custom/report_queue/rq_str... corporate network. What tool should the analyst use to perform a Blackjacking attack?
A. BBProxy
B. Bloover
C. Paros Proxy
D. BBCrack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 239
You've just discovered a server that is currently active within the same network with the machine you recently compromised. You ping it but it did not respond. What could be the case?
A. ARP is disabled on the target server
B. ICMP could be disabled on the target server
C. You need to run the ping command with root privileges
D. TCP/IP doesn't support ICMP
Answer: B (LEAVE A REPLY)

NEW QUESTION: 240
If an e-commerce site was put into a live environment and the programmers failed to remove the secret entry point that was used during the application development, what is this secret entry point known as?
A. Honey pot
B. SDLC process
C. Trap door
D. SQL injection
Answer: C (LEAVE A REPLY)

NEW QUESTION: 241
Which of the following statements is TRUE?
A. Sniffers operate on Layer 2 of the OSI model
B. Sniffers operate on Layer 3 of the OSI model
C. Sniffers operate on both Layer 2 & Layer 3 of the OSI model.
D. Sniffers operate on the Layer 1 of the OSI model.
Answer: A (LEAVE A REPLY)
The OSI layer 2 is where packet sniffers collect their data.
References: https://en.wikipedia.org/wiki/Ethernet_frame

Valid 312-50v10 Dumps shared by PrepPdf.com for Helping Passing 312-50v10 Exam! PrepPdf.com now offer the **newest 312-50v10 exam dumps**, the PrepPdf.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-50v10 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-50v10-prepaway-exam-dumps.html (**745** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 242
Which of the following is a restriction being enforced in "white box testing?"
A. Only the internal operation of a system is known 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. The internal operation of a system is only partly accessible to the tester
Answer: (SHOW ANSWER)

NEW QUESTION: 243
You are tasked to configure the DHCP server to lease the last 100 usable IP addresses in subnet 10.1.4.0/23.
Which of the following IP addresses could be leased as a result of the new configuration?
A. 10.1.4.254
B. 10.1.4.156
C. 10.1.255.200
D. 10.1.5.200
Answer: D (LEAVE A REPLY)

NEW QUESTION: 244
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. Tailgating
B. Social engineering
C. Piggybacking
D. Eavesdropping
Answer: B (LEAVE A REPLY)

NEW QUESTION: 245

Which of the following is the greatest threat posed by backups?
A. A backup is the source of Malware or illicit information.
B. A backup is unavailable during disaster recovery.
C. A backup is incomplete because no verification was performed.
D. An un-encrypted backup can be misplaced or stolen.
Answer: (SHOW ANSWER)
If the data written on the backup media is properly encrypted, it will be useless for anyone without the key.
References: http://resources.infosecinstitute.com/backup-media-encryption/

NEW QUESTION: 246
The establishment of a TCP connection involves a negotiation called 3 way handshake.
What type of message sends the client to the server in order to begin this negotiation?
A. RST
B. SYN-ACK
C. ACK
D. SYN
Answer: D (LEAVE A REPLY)

NEW QUESTION: 247
Windows file servers commonly hold sensitive files, databases, passwords and more. Which of the following choices would be a common vulnerability that usually exposes them?
A. CRLF injection
B. Missing patches
C. SQL injection
D. Cross-site scripting
Answer: B (LEAVE A REPLY)

NEW QUESTION: 248
In many states sending spam is illegal. Thus, the spammers have techniques to try and ensure that no one knows they sent the spam out to thousands of users at a time. Which of the following best describes what spammers use to hide the origin of these types of e-mails?
A. A blacklist of companies that have their mail server relays configured to be wide open.
B. Tools that will reconfigure a mail server's relay component to send the e-mail back to the spammers occasionally.
C. A blacklist of companies that have their mail server relays configured to allow traffic only to their specific domain name.
D. Mail relaying, which is a technique of bouncing e-mail from internal to external mails servers continuously.
Answer: (SHOW ANSWER)

NEW QUESTION: 249
>NMAP -sn 192.168.11.200-215 The NMAP command above performs which of the following?

A. A trace sweep
B. A ping scan
C. A port scan
D. An operating system detect
Answer: C (LEAVE A REPLY)

NEW QUESTION: 250
Perspective clients want to see sample reports from previous penetration tests.
What should you do next?
A. Decline but, provide references.
B. Share full reports, not redacted.
C. Share full reports with redactions.
D. Share reports, after NDA is signed.
Answer: A (LEAVE A REPLY)
Explanation
Penetration tests data should not be disclosed to third parties.

NEW QUESTION: 251
The change of a hard drive failure is once every three years. The cost to buy a new hard drive is $300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns $10/hour. Calculate the SLE, ARO, and ALE. Assume the EF = 1(100%). What is the closest approximate cost of this replacement and recovery operation per year?
A. $100
B. $146
C. $1320
D. $440
Answer: B (LEAVE A REPLY)

NEW QUESTION: 252
Trinity needs to scan all hosts on a /16 network for TCP port 445 only. What is the fastest way she can accomplish this with Nmap? Stealth is not a concern.
A. nmap -s 445 -sU -T5 10.1.0.0/16
B. nmap -p 445 -n -T4 -open 10.1.0.0/16
C. nmap -p 445 -max -Pn 10.1.0.0/16
D. nmap -sn -sF 10.1.0.0/16 445
Answer: (SHOW ANSWER)

NEW QUESTION: 253
Password cracking programs reverse the hashing process to recover passwords.
(True/False.)

A. True
B. False
Answer: (SHOW ANSWER)

NEW QUESTION: 254
A possibly malicious sequence of packets that were sent to a web server has been captured by an Intrusion Detection System (IDS) and was saved to a PCAP file. As a network administrator, you need to determine whether this packets are indeed malicious. What tool are you going to use?
A. Vulnerability scanner
B. Protocol analyzer
C. Network sniffer
D. Intrusion Prevention System (IPS)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 255
What does a firewall check to prevent particular ports and applications from getting packets into an organization?
A. Transport layer port numbers and application layer headers
B. Presentation layer headers and the session layer port numbers
C. Network layer headers and the session layer port numbers
D. Application layer port numbers and the transport layer headers
Answer: (SHOW ANSWER)
Newer firewalls can filter traffic based on many packet attributes like source IP address, source port, destination IP address or transport layer port, destination service like WWW or FTP. They can filter based on protocols, TTL values, netblock of originator, of the source, and many other attributes.
Application layer firewalls are responsible for filtering at 3, 4, 5, 7 layer. Because they analyze the application layer headers, most firewall control and filtering is performed actually in the software.
References:
https://en.wikipedia.org/wiki/Firewall_(computing)#Network_layer_or_packet_filters
http://howdoesinternetwork.com/2012/application-layer-firewalls

NEW QUESTION: 256
Which of the following is an example of IP spoofing?
A. Cross-site scripting
B. Man-in-the-middle
C. ARP poisoning
D. SQL injections
Answer: B (LEAVE A REPLY)

Valid 312-50v10 Dumps shared by PrepPdf.com for Helping Passing 312-50v10 Exam! PrepPdf.com now offer the **newest 312-50v10 exam dumps**, the PrepPdf.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-50v10 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-50v10-prepaway-exam-dumps.html (**745** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 257
A tester has been hired to do a web application security test. The tester notices that the site is dynamic and must make use of a back end database. In order for the tester to see if SQL injection is possible, what is the first character that the tester should use to attempt breaking a valid SQL request?
A. Double quote
B. Single quote
C. Exclamation mark
D. Semicolon
Answer: (SHOW ANSWER)

NEW QUESTION: 258
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. Hierarchical, Relational
B. Simple, Complex
C. Relational, Hierarchical
D. Strict, Abstract
Answer: A (LEAVE A REPLY)

NEW QUESTION: 259
During a wireless penetration test, a tester detects an access point using WPA2 encryption.
Which of the following attacks should be used to obtain the key?
A. The tester must capture the WPA2 authentication handshake and then crack it.
B. The tester cannot crack WPA2 because it is in full compliance with the IEEE 802.11i standard.
C. The tester must change the MAC address of the wireless network card and then use the AirTraf tool to obtain the key.
D. The tester must use the tool inSSIDer to crack it using the ESSID of the network.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 260
Which of the following can the administrator do to verify that a tape backup can be recovered in its entirety?
A. Read the last 512 bytes of the tape

B. Perform a full restore
C. Read the first 512 bytes of the tape
D. Restore a random file
Answer: B (LEAVE A REPLY)

NEW QUESTION: 261
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 as wardriving.
Which Algorithm is this referring to?
A. Temporal Key Integrity Protocol (TKIP)
B. Wi-Fi Protected Access 2 (WPA2)
C. Wired Equivalent Privacy (WEP)
D. Wi-Fi Protected Access (WPA)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 262
Ricardo wants to send secret messages to a competitor company. To secure these messages, he uses a technique of hiding a secret message within an ordinary message.
The technique provides 'security through obscurity'.
What technique is Ricardo using?
A. Steganography
B. Public-key cryptography
C. RSA algorithm
D. Encryption
Answer: A (LEAVE A REPLY)
Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video.
References: https://en.wikipedia.org/wiki/Steganography

NEW QUESTION: 263
It is an entity or event with the potential to adversely impact a system through unauthorized access, destruction, disclosure, denial of service or modification of data.
Which of the following terms best matches the definition?
A. Threat
B. Attack
C. Vulnerability
D. Risk
Answer: A (LEAVE A REPLY)
Explanation

A threat is at any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.
References: https://en.wikipedia.org/wiki/Threat_(computer)

NEW QUESTION: 264
A penetration tester is hired to do a risk assessment of a company's DMZ. The rules of engagement states that the penetration test be done from an external IP address with no prior knowledge of the internal IT systems.
What kind of test is being performed?
A. white box
B. red box
C. black box
D. grey box
Answer: C (LEAVE A REPLY)

NEW QUESTION: 265
Pentest results indicate that voice over IP traffic is traversing a network. Which of the following tools will decode a packet capture and extract the voice conversations?
A. Cain
B. Hping
C. John the Ripper
D. Nikto
Answer: (SHOW ANSWER)

NEW QUESTION: 266
Seth is starting a penetration test from inside the network. He hasn't been given any information about the network. What type of test is he conducting?
A. Internal, Blackbox
B. External, Whitebox
C. External, Blackbox
D. Internal, Whitebox
Answer: A (LEAVE A REPLY)

NEW QUESTION: 267
A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.
What kind of Web application vulnerability likely exists in their software?
A. Cross-site scripting vulnerability
B. Cross-site Request Forgery vulnerability

C. SQL injection vulnerability
D. Web site defacement vulnerability
Answer: A (LEAVE A REPLY)
Many operators of particular web applications (e.g. forums and webmail) allow users to utilize a limited subset of HTML markup. When accepting HTML input from users (say, very large), output encoding (such as very large) will not suffice since the user input needs to be rendered as HTML by the browser (so it shows as "very large", instead of "very large"). Stopping an XSS attack when accepting HTML input from users is much more complex in this situation. Untrusted HTML input must be run through an HTML sanitization engine to ensure that it does not contain cross-site scripting code.
References: https://en.wikipedia.org/wiki/Cross-site_scripting#Safely_validating_untrusted_HTML_input

NEW QUESTION: 268
Why should the security analyst disable/remove unnecessary ISAPI filters?
A. To defend against webserver attacks
B. To defend against wireless attacks
C. To defend against jailbreaking
D. To defend against social engineering attacks
Answer: A (LEAVE A REPLY)

NEW QUESTION: 269
A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?
A. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.
B. Attempts by attackers to access the user and password information stored in the company's SQL database.
C. Attempts by attackers to access passwords stored on the user's computer without the user's knowledge.
D. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.
Answer: (SHOW ANSWER)
Explanation
Cookies can store passwords and form content a user has previously entered, such as a credit card number or an address.
Cookies can be stolen using a technique called cross-site scripting. This occurs when an attacker takes advantage of a website that allows its users to post unfiltered HTML and JavaScript content.
References: https://en.wikipedia.org/wiki/HTTP_cookie#Cross-site_scripting_.E2.80.93_cookie_theft

NEW QUESTION: 270
You've gained physical access to a Windows 2008 R2 server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your tool kit you have an

Ubuntu 9.10 Linux LiveCD. Which Linux based tool has the ability to change any user's password or to activate disabled Windows accounts?

A. CHNTPW

B. Cain & Abel

C. SET

D. John the Ripper

Answer: A (LEAVE A REPLY)

chntpw is a software utility for resetting or blanking local passwords used by Windows NT, 2000, XP, Vista, 7, 8 and 8.1. It does this by editing the SAM database where Windows stores password hashes.

References: https://en.wikipedia.org/wiki/Chntpw

NEW QUESTION: 271

Which of the following is the successor of SSL?

A. RSA

B. IPSec

C. GRE

D. TLS

Answer: (SHOW ANSWER)

Valid 312-50v10 Dumps shared by PrepPdf.com for Helping Passing 312-50v10 Exam! PrepPdf.com now offer the **newest 312-50v10 exam dumps**, the PrepPdf.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-50v10 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-50v10-prepaway-exam-dumps.html (**745** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 272

In which of the following password protection technique, random strings of characters are added to the password before calculating their hashes?

A. Salting

B. Double Hashing

C. Key Stretching

D. Keyed Hashing

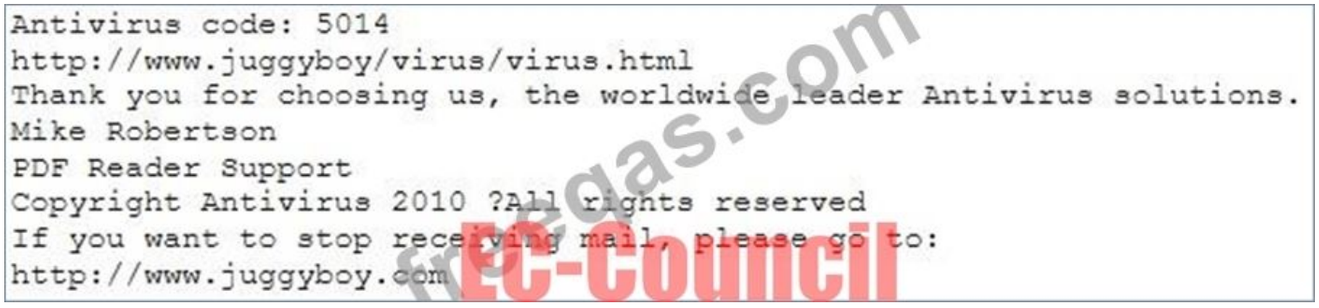
Answer: A (LEAVE A REPLY)

NEW QUESTION: 273

You receive an e-mail like the one shown below. When you click on the link contained in the mail, you are redirected to a website seeking you to download free Anti-Virus software.

Dear valued customers,

We are pleased to announce the newest version of Antivirus 2010 for Windows which will probe you with total security against the latest spyware, malware, viruses, Trojans and other online threats. Simply visit the link below and enter your antivirus code:



freedas.com
ec-Council

or you may contact us at the following address:

Media Internet Consultants, Edif. Neptuno, Planta

Baja, Ave. Ricardo J. Alfaro, Tumba Muerto, n/a Panama

How will you determine if this is Real Anti-Virus or Fake Anti-Virus website?

A. Download and install Anti-Virus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a malware

B. Look at the website design, if it looks professional then it is a Real Anti-Virus website

C. Download and install Anti-Virus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a malware

D. Connect to the site using SSL, if you are successful then the website is genuine

E. Search using the URL and Anti-Virus product name into Google and lookout for suspicious warnings against this site

Answer: E (LEAVE A REPLY)

NEW QUESTION: 274

Joseph was the Web site administrator for the Mason Insurance in New York, who's main Web site was located at www.masonins.com. Joseph uses his laptop computer regularly to administer the Web site. One night, Joseph received an urgent phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker's message "Hacker Message: You are dead! Freaks!" From his office, which was directly connected to Mason Insurance's internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact.

No changes were apparent. Joseph called a friend of his at his home to help troubleshoot the problem. The Web site appeared defaced when his friend visited using his DSL connection. So, while Smith and his friend could see the defaced page, Joseph saw the intact Mason Insurance web site. To help make sense of this problem, Joseph decided to access the Web site using hisdial-up ISP. He disconnected his laptop from the corporate internal network and used his modem to dial up the same ISP used by Smith. After his modem connected, he quickly typed www.masonins.com in his browser to reveal the following web page:

```
H@cker Mess@ge:
YOu @re De@d! Fre@ks!
```

After seeing the defaced Web site, he disconnected his dial-up line, reconnected to the internal network, and used Secure Shell (SSH) to log in directly to the Web server. He ran Tripwire against the entire Web site, and determined that every system file and all the Web content on the server were intact. How did the attacker accomplish this hack?

A. ARP spoofing

B. Routing table injection

C. DNS poisoning

D. SQL injection

Answer: C (LEAVE A REPLY)

NEW QUESTION: 275

A user on your Windows 2000 network has discovered that he can use L0phtcrack to sniff the SMB exchanges which carry user logons. The user is plugged into a hub with 23 other systems.

However, he is unable to capture any logons though he knows that other users are logging in.

What do you think is the most likely reason behind this?

A. There is a NIDS present on that segment.

B. Kerberos is preventing it.

C. Windows logons cannot be sniffed.

D. L0phtcrack only sniffs logons to web servers.

Answer: (SHOW ANSWER)

NEW QUESTION: 276

The configuration allows a wired or wireless network interface controller to pass all traffic it receives to the central processing unit (CPU), rather than passing only the frames that the controller is intended to receive.

Which of the following is being described?

A. promiscuous mode

B. port forwarding

C. multi-cast mode

D. WEM

Answer: (SHOW ANSWER)

Promiscuous mode refers to the special mode of Ethernet hardware, in particular network interface cards (NICs), that allows a NIC to receive all traffic on the network, even if it is not addressed to this NIC. By default, a NIC ignores all traffic that is not addressed to it, which is done by comparing the destination address of the Ethernet packet with the hardware address (a.k.a. MAC) of the device. While this makes perfect sense for networking, non- promiscuous mode makes it difficult to use network monitoring and analysis software for diagnosing connectivity issues or traffic accounting.

References: https://www.tamos.com/htmlhelp/monitoring/

NEW QUESTION: 277

Which of the following describes a component of Public Key Infrastructure (PKI) where a copy of a private key is stored to provide third-party access and to facilitate recovery operations?

A. Key escrow
B. Directory
C. Key registry
D. Recovery agent
Answer: (SHOW ANSWER)

NEW QUESTION: 278
Which of the following Linux commands will resolve a domain name into IP address?
A. >host -t soa hackeddomain.com
B. >host -t AXFR hackeddomain.com
C. >host-t ns hackeddomain.com
D. >host-t a hackeddomain.com
Answer: D (LEAVE A REPLY)

NEW QUESTION: 279
Which of the following algorithms provides better protection against brute force attacks by using a 160-bit message digest?
A. RC4
B. SHA-1
C. MD5
D. MD4
Answer: (SHOW ANSWER)

NEW QUESTION: 280
Which of the following statements regarding ethical hacking is incorrect?
A. Testing should be remotely performed offsite.
B. An organization should use ethical hackers who do not sell vendor hardware/software or other consulting services
C. Ethical hackers should never use tools or methods that have the potential of exploiting vulnerabilities in an organization's systems
D. Ethical hacking should not involve writing to or modifying the target systems.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 281
When a normal TCP connection starts, a destination host receives a SYN (synchronize/start) packet from a source host and sends back a SYN/ACK (synchronize acknowledge). The destination host must then hear an ACK (acknowledge) of the SYN/ACK before the connection is established. This is referred to as the "TCP three-way handshake." While waiting for the ACK to the SYN ACK, a connection queue of finite size on the destination host keeps track of connections waiting to be completed. This queue typically empties quickly since the ACK is expected to arrive a few milliseconds after the SYN ACK. How would an attacker exploit this design by launching TCP SYN attack?

A. Attacker floods TCP SYN packets with random source addresses towards a victim host
B. Attacker generates TCP ACK packets with random source addresses towards a victim host
C. Attacker generates TCP RST packets with random source addresses towards a victim host
D. Attacker generates TCP SYN packets with random destination addresses towards a victim host
Answer: (SHOW ANSWER)

NEW QUESTION: 282
Sid is a judge for a programming contest. Before the code reaches him it goes through a restricted OS and is tested there. If it passes, then it moves onto Sid. What is this middle step called?
A. Fuzzy-testing the code
B. String validating the code
C. Third party running the code
D. Sandboxing the code
Answer: A (LEAVE A REPLY)

NEW QUESTION: 283
Which of the following items is unique to the N-tier architecture method of designing software applications?
A. Data security is tied into each layer and must be updated for all layers when any upgrade is performed.
B. Application layers can be written in C, ASP.NET, or Delphi without any performance loss.
C. Application layers can be separated, allowing each layer to be upgraded independently from other layers.
D. It is compatible with various databases including Access, Oracle, and SQL.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 284
Which of the following is the BEST way to protect Personally Identifiable Information (PII) from being exploited due to vulnerabilities of varying web applications?
A. Use full disk encryption on all hard drives to protect PII
B. Use cryptographic storage to store all PII
C. Use encrypted communications protocols to transmit PII
D. Use a security token to log into all Web applications that use PII
Answer: (SHOW ANSWER)

NEW QUESTION: 285
Which of the following is considered an acceptable option when managing a risk?
A. Deny the risk.
B. Initiate the risk.
C. Reject the risk.
D. Mitigate the risk.
Answer: (SHOW ANSWER)

NEW QUESTION: 286

Which of the following levels of algorithms does Public Key Infrastructure (PKI) use?
A. AES 512 bit strength
B. RSA 1024 bit strength
C. AES 1024 bit strength
D. RSA 512 bit strength
Answer: B (LEAVE A REPLY)

Valid 312-50v10 Dumps shared by PrepPdf.com for Helping Passing 312-50v10 Exam! PrepPdf.com now offer the **newest 312-50v10 exam dumps**, the PrepPdf.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-50v10 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-50v10-prepaway-exam-dumps.html (**745** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 287
As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing.
What document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester?
A. Terms of Engagement
B. Non-Disclosure Agreement
C. Project Scope
D. Service Level Agreement
Answer: A (LEAVE A REPLY)

NEW QUESTION: 288
Which among the following is a Windows command that a hacker can use to list all the shares to which the current user context has access?
A. NET VIEW
B. NET USE
C. NET CONFIG
D. NET FILE
Answer: (SHOW ANSWER)

NEW QUESTION: 289
What network security concept requires multiple layers of security controls to be placed throughout an IT infrastructure, which improves the security posture of an organization to defend against malicious attacks or potential vulnerabilities?
A. Defense in depth
B. Host-Based Intrusion Detection System

C. Security through obscurity
D. Network-Based Intrusion Detection System
Answer: (SHOW ANSWER)

NEW QUESTION: 290
Which of the following statements is TRUE?
A. Sniffers operate on Layer 2 of the OSI model
B. Sniffers operate on Layer 3 of the OSI model
C. Sniffers operate on both Layer 2 & Layer 3 of the OSI model.
D. Sniffers operate on the Layer 1 of the OSI model.
Answer: A (LEAVE A REPLY)
Explanation

NEW QUESTION: 291
What are two things that are possible when scanning UDP ports? (Choose two.)
A. Nothing
B. A reset will be returned
C. An ICMP message will be returned
D. An RFC 1294 message will be returned
E. The four-way handshake will not be completed
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 292
A new wireless client is configured to join an 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client. What is a possible source of this problem?
A. The wireless client is not configured to use DHCP
B. Client is configured for the wrong channel
C. The WAP does not recognize the client's MAC address
D. The client cannot see the SSID of the wireless network
Answer: (SHOW ANSWER)

NEW QUESTION: 293
What kind of detection techniques is being used in antivirus softwares that identifies malware by collecting data from multiple protected systems and instead of analyzing files locally it's made on the provider's environment.
A. Cloud based
B. Honypot based
C. Heuristics based
D. Behavioral based
Answer: A (LEAVE A REPLY)

NEW QUESTION: 294

(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.). 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?

What is odd about this attack? Choose the best answer.



A. This is not a spoofed packet as the IP stack has increasing numbers for the three flags.

B. The attacker wants to avoid creating a sub-carries connection that is not normally valid.

C. This is back orifice activity as the scan comes from port 31337.

D. These packets were crafted by a tool, they were not created by a standard IP stack.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 295

Which of the following is not a Bluetooth attack?

A. Bluesmacking

B. Bluejacking

C. Bluedriving

D. Bluesnarfing

Answer: C (LEAVE A REPLY)

NEW QUESTION: 296

You are working as a Security Analyst in a company XYZ that owns the whole subnet range of 23.0.0.0/8 and 192.168.0.0/8.

While monitoring the data, you find a high number of outbound connections. You see that IP's owned by XYZ (Internal) and private IP's are communicating to a Single Public IP.

Therefore, the Internal IP's are sending data to the Public IP.

After further analysis, you find out that this Public IP is a blacklisted IP, and the internal communicating devices are compromised.

What kind of attack does the above scenario depict?

A. Rootkit Attack

B. Advanced Persistent Threats

C. Spear Phishing Attack

D. Botnet Attack

Answer: D (LEAVE A REPLY)

NEW QUESTION: 297
You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.
What is the best nmap command you will use?
A. nmap -T4 -O 10.10.0.0/24
B. nmap -T4 -q 10.10.0.0/24
C. nmap -T4 -F 10.10.0.0/24
D. nmap -T4 -r 10.10.1.0/24
Answer: C (LEAVE A REPLY)

NEW QUESTION: 298
.....is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there.
Fill in the blank with appropriate choice.
A. Collision Attack
B. Evil Twin Attack
C. Signal Jamming Attack
D. Sinkhole Attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 299
Which of the following is one of the most effective ways to prevent Cross-site Scripting (XSS) flaws in software applications?
A. Verify access right before allowing access to protected information and UI controls.
B. Validate and escape all information sent to a server.
C. Use digital certificates to authenticate a server prior to sending data.
D. Use security policies and procedures to define and implement proper security settings.
Answer: (SHOW ANSWER)

NEW QUESTION: 300
The chance of a hard drive failure is once every three years. The cost to buy a new hard drive is $300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns $10/hour. Calculate the SLE, ARO, and ALE. Assume the EF = 1 (100%).
What is the closest approximate cost of this replacement and recovery operation per year?
A. $146
B. $1320

C. $440
D. $100
Answer: A (LEAVE A REPLY)
Explanation
The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE).
Suppose than an asset is valued at $100,000, and the Exposure Factor (EF) for this asset is 25%. The single loss expectancy (SLE) then, is 25% * $100,000, or $25,000.
In our example the ARO is 33%, and the SLE is 300+14*10 (as EF=1). The ALO is thus: 33%*(300+14*10) which equals 146.
References: https://en.wikipedia.org/wiki/Annualized_loss_expectancy

NEW QUESTION: 301
Which of the following is an adaptive SQL Injection testing technique used to discover coding errors by inputting massive amounts of random data and observing the changes in the output?
A. Fuzzing Testing
B. Static Testing
C. Function Testing
D. Dynamic Testing
Answer: A (LEAVE A REPLY)

Valid 312-50v10 Dumps shared by PrepPdf.com for Helping Passing 312-50v10 Exam! PrepPdf.com now offer the **newest 312-50v10 exam dumps**, the PrepPdf.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-50v10 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-50v10-prepaway-exam-dumps.html (**745** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 302
An attacker is using nmap to do a ping sweep and a port scanning in a subnet of 254 addresses.
In which order should he perform these steps?
A. The port scan alone is adequate. This way he saves time.
B. The sequence does not matter. Both steps have to be performed against all hosts.
C. First the port scan to identify interesting services and then the ping sweep to find hosts responding to icmp echo requests.
D. First the ping sweep to identify live hosts and then the port scan on the live hosts. This way he saves time.
Answer: (SHOW ANSWER)

NEW QUESTION: 303

Which of the following is considered an exploit framework and has the ability to perform automated attacks on services, ports, applications and unpatched security flaws in a computer system?

A. Wireshark

B. Maltego

C. Nessus

D. Metasploit

Answer: D (LEAVE A REPLY)

NEW QUESTION: 304

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 (LEAVE A REPLY)

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

NEW QUESTION: 305

Jack was attempting to fingerprint all machines in the network using the following Nmap syntax:

invictus@victim_server:~$ nmap -T4 -0 10.10.0.0/24

TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx. QUITTING!

Obviously, it is not going through. What is the issue here?

A. OS Scan requires root privileges

B. The nmap syntax is wrong.

C. This is a common behavior for a corrupted nmap application

D. The outgoing TCP/IP fingerprinting is blocked by the host firewall

Answer: (SHOW ANSWER)

NEW QUESTION: 306

Your next door neighbor, that you do not get along with, is having issues with their network, so he yells to his spouse the network's SSID and password and you hear them both clearly. What do you do with this information?

A. Only use his network when you have large downloads so you don't tax your own network.

B. Nothing, but suggest to him to change the network's SSID and password.

C. Sell his SSID and password to friends that come to your house, so it doesn't slow down your network.

D. Log onto to his network, after all it's his fault that you can get in.
Answer: (SHOW ANSWER)

NEW QUESTION: 307
A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?
A. The gateway is not routing to a public IP address.
B. The computer is not using a private IP address.
C. The gateway and the computer are not on the same network.
D. The computer is using an invalid IP address.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 308
You have gained physical access to a Windows 2008 R2 server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your toolkit, you have an Ubuntu 9.10 Linux LiveCD. Which Linux-based tool can change any user's password or activate disabled Windows accounts?
A. CHNTPW
B. SET
C. Cain & Abel
D. John the Ripper
Answer: A (LEAVE A REPLY)

NEW QUESTION: 309
Sandra has been actively scanning the client network on which she is doing a vulnerability assessment test. While conducting a port scan she notices open ports in the range of 135 to 139.
What protocol is most likely to be listening on those ports?
A. Finger
B. FTP
C. SMB
D. Samba
Answer: C (LEAVE A REPLY)

NEW QUESTION: 310
Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and that are related to various aspects in information security such as data confidentially, data integrity, authentication, and non-repudiation. Modern cryptography intersects the

disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.
Basic example to understand how cryptography works is given below:

SECURE (plain text)
+1 (+1 next letter.for example , the letter""T"" is used for "S" to encrypt.)
TFDVSF (encrypted text)
+=logic=>Algorithm
1=Factor=>Key

Which of the following choices true about cryptography?
A. Algorithm is not the secret; key is the secret.
B. Public-key cryptography, also known as asymmetric cryptography, public key is for decrypt, private key is for encrypt.
C. Secure Sockets Layer (SSL) use the asymmetric encryption both (public/private key pair) to deliver the shared session key and to achieve a communication way.
D. Symmetric-key algorithms are a class of algorithms for cryptography that use the different cryptographic keys for both encryption of plaintext and decryption of ciphertext.
Answer: (SHOW ANSWER)
Explanation

NEW QUESTION: 311
In both pharming and phishing attacks an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims. What is the difference between pharming and phishing attacks?
A. In a phishing attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a phishing attack an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name.
B. Both pharming and phishing attacks are identical.
C. In a pharming attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a phishing attack an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name.
D. Both pharming and phishing attacks are purely technical and are not considered forms of social engineering
Answer: C (LEAVE A REPLY)

NEW QUESTION: 312
The establishment of a TCP connection involves a negotiation called three-way handshake. What type of message does the client send to the server in order to begin this negotiation?
A. SYN-ACK
B. SYN
C. RST
D. ACK
Answer: (SHOW ANSWER)

NEW QUESTION: 313
A new wireless client is configured to join an 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect.
A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client. What is a possible source of this problem?
A. The client cannot see the SSID of the wireless network
B. Client is configured for the wrong channel
C. The wireless client is not configured to use DHCP
D. The WAP does not recognize the client's MAC address
Answer: (SHOW ANSWER)

NEW QUESTION: 314
Which type of security feature stops vehicles from crashing through the doors of a building?
A. Turnstile
B. Bollards
C. Mantrap
D. Receptionist
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 315
You are a security officer of a company. You had an alert from IDS that indicates that one PC on your Intranet is connected to a blacklisted IP address (C2 Server) on the Internet.
The IP address was blacklisted just before the alert. You are staring an investigation to roughly analyze the severity of the situation. Which of the following is appropriate to analyze?
A. Internet Firewall/Proxy log
B. IDS log
C. Event logs on the PC
D. Event logs on domain controller
Answer: A (LEAVE A REPLY)

NEW QUESTION: 316
You receive an e-mail like the one shown below. When you click on the link contained in the mail, you are redirected to a website seeking you to download free Anti-Virus software.
Dear valued customers,
We are pleased to announce the newest version of Antivirus 2010 for Windows which will probe you with total security against the latest spyware, malware, viruses, Trojans and other online threats. Simply visit the link below and enter your antivirus code:



or you may contact us at the following address:
Media Internet Consultants, Edif. Neptuno, Planta
Baja, Ave. Ricardo J. Alfaro, Tumba Muerto, n/a Panama
How will you determine if this is Real Anti-Virus or Fake Anti-Virus website?

A. Search using the URL and Anti-Virus product name into Google and lookout for suspicious warnings against this site

B. Look at the website design, if it looks professional then it is a Real Anti-Virus website

C. Connect to the site using SSL, if you are successful then the website is genuine

D. Download and install Anti-Virus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a malware

E. Download and install Anti-Virus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a malware

Answer: (SHOW ANSWER)

Valid 312-50v10 Dumps shared by PrepPdf.com for Helping Passing 312-50v10 Exam! PrepPdf.com now offer the **newest 312-50v10 exam dumps**, the PrepPdf.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-50v10 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-50v10-prepaway-exam-dumps.html (**745** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 317

When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, PUT, DELETE, TRACE) using NMAP script engine.
What nmap script will help you with this task?

A. http-methods

B. http enum

C. http-headers

D. http-git

Answer: A (LEAVE A REPLY)

Explanation

You can check HTTP method vulnerability using NMAP.
Example: #nmap -script=http-methods.nse 192.168.0.25
References:
http://solutionsatexperts.com/http-method-vulnerability-check-using-nmap/

NEW QUESTION: 318
An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next?
A. He will repeat this action so that it escalates to a DoS attack.
B. He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.
C. He will activate OSPF on the spoofed root bridge.
D. He will repeat the same attack against all L2 switches of the network.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 319
Which of the following are well known password-cracking programs?
A. NetCat
B. Jack the Ripper
C. L0phtcrack
D. John the Ripper
E. Netbus
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 320
You have successfully gained access to a Linux server and would like to ensure that the succeeding outgoing traffic from this server will not be caught by Network-Based Intrusion Detection Systems (NIDS).
What is the best way to evade the NIDS?
A. Protocol Isolation
B. Encryption
C. Alternate Data Streams
D. Out of band signaling
Answer: (SHOW ANSWER)

NEW QUESTION: 321
Which of the following is designed to verify and authenticate individuals taking part in a data exchange within an enterprise?
A. PKI
B. Single-Sign On
C. SOA
D. Biometrics
Answer: A (LEAVE A REPLY)

NEW QUESTION: 322
Scenario:
What is the name of the attack which is mentioned in the scenario?
A. HTTP Parameter Pollution
B. HTML Injection
C. ClickJacking Attack
D. Session Fixation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 323
Internet Protocol Security IPSec is actually a suite of protocols. Each protocol within the suite provides different functionality. Collective IPSec does everything except.
A. Work at the Data Link Layer
B. Protect the payload and the headers
C. Authenticate
D. Encrypt
Answer: A (LEAVE A REPLY)

NEW QUESTION: 324
Take a look at the following attack on a Web Server using obstructed URL:

```
http://www.certifiedhacker.com/script.ext?
template=%2e%2e%2f%2e%2e%2f%2e%2e%2f%65%74%63%2f%70%61%73%73%77%64
This request is made up of:
%2e%2e%2f%2e%2f%2e%2e%2f = ../ ../ ../
%65%74%63 = etc
%2f = /
%70%61%73%73%77%64 = passwd
```

How would you protect from these attacks?
A. Use SSL authentication on Web Servers
B. Create rules in IDS to alert on strange Unicode requests
C. Configure the Web Server to deny requests involving "hex encoded" characters
D. Enable Active Scripts Detection at the firewall and routers
Answer: B (LEAVE A REPLY)

NEW QUESTION: 325
Which method of password cracking takes the most time and effort?
A. Dictionary attack
B. Brute force
C. Shoulder surfing
D. Rainbow tables
Answer: B (LEAVE A REPLY)

NEW QUESTION: 326
A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.
What kind of Web application vulnerability likely exists in their software?
A. Cross-site scripting vulnerability
B. SQL injection vulnerability
C. Cross-site Request Forgery vulnerability
D. Session management vulnerability
Answer: A (LEAVE A REPLY)

NEW QUESTION: 327
A company has five different subnets: 192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0 and 192.168.5.0.
How can NMAP be used to scan these adjacent Class C networks?
A. NMAP -P 192.168.0.0/16
B. NMAP -P 192.168.1-5.
C. NMAP -P 192.168.1/17
D. NMAP -P 192.168.1.0,2.0,3.0,4.0,5.0
Answer: B (LEAVE A REPLY)

NEW QUESTION: 328
An attacker sniffs encrypted traffic from the network and is subsequently able to decrypt it. The attacker can now use which cryptanalytic technique to attempt to discover the encryption key?
A. Chosen ciphertext attack
B. Birthday attack
C. Plaintext attack
D. Meet in the middle attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 329
Which of the following is the most important phase of ethical hacking wherein you need to spend considerable amount of time?
A. Escalating privileges
B. Gaining access
C. Footprinting
D. Network mapping
Answer: C (LEAVE A REPLY)

NEW QUESTION: 330
What is a "Collision attack" in cryptography?
A. Collision attacks try to find two inputs producing the same hash.

B. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key.
C. Collision attacks try to get the public key.
D. Collision attacks try to break the hash into three parts to get the plaintext value.
Answer: A (LEAVE A REPLY)
Explanation
A Collision Attack is an attempt to find two input strings of a hash function that produce the same hash result.
References: https://learncryptography.com/hash-functions/hash-collision-attack

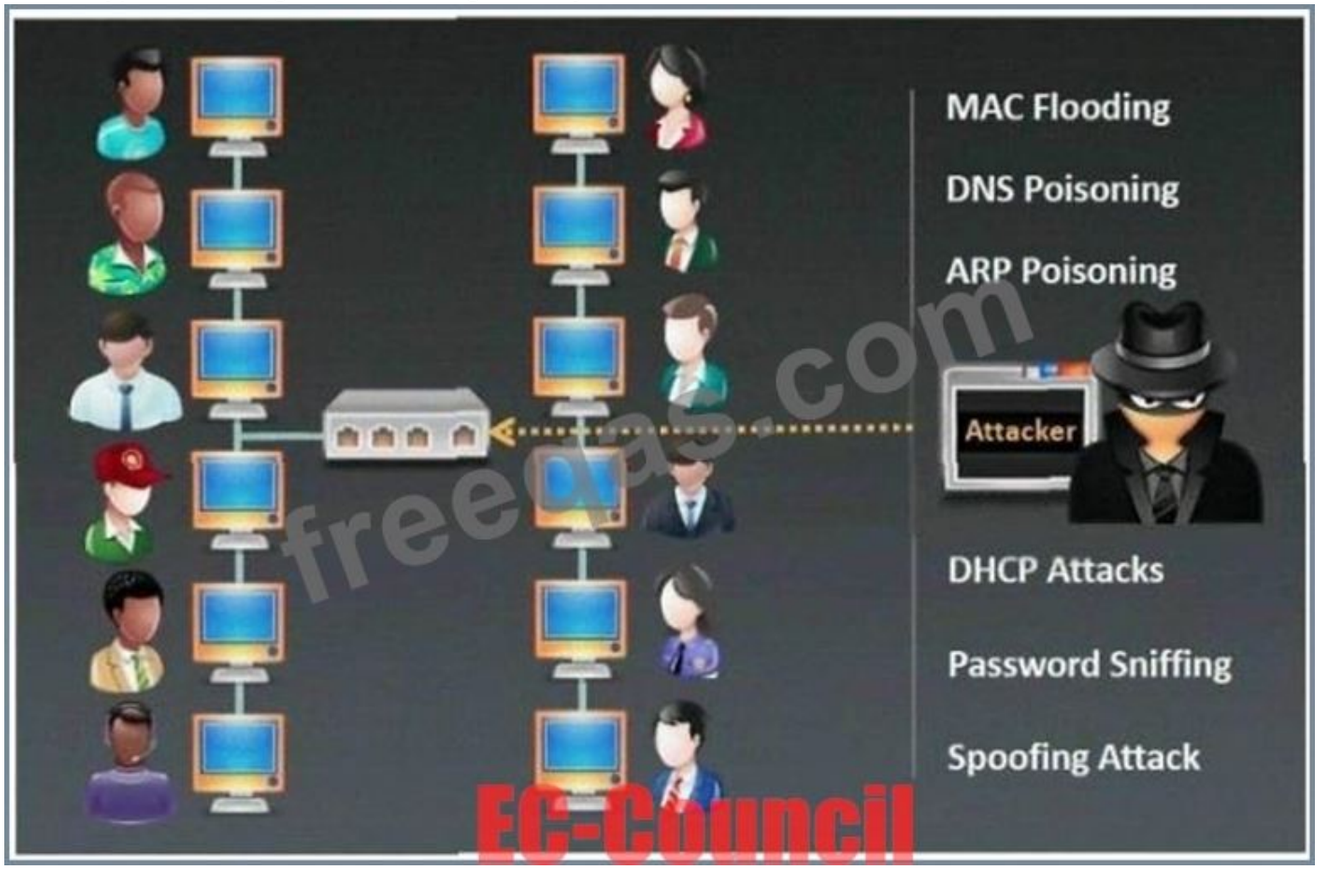
NEW QUESTION: 331
Fred is the network administrator for his company. Fred is testing an internal switch.
From an external IP address, Fred wants to try and trick this switch into thinking it already has established a session with his computer. How can Fred accomplish this?
A. Fred can accomplish this by sending an IP packet with the RST/SIN bit and the source address of his computer.
B. He can send an IP packet with the SYN bit and the source address of his computer.
C. Fred can send an IP packet with the ACK bit set to zero and the source address of the switch.
D. Fred can send an IP packet to the switch with the ACK bit and the source address of his machine.
Answer: D (LEAVE A REPLY)

Valid 312-50v10 Dumps shared by PrepPdf.com for Helping Passing 312-50v10 Exam! PrepPdf.com now offer the **newest 312-50v10 exam dumps**, the PrepPdf.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-50v10 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-50v10-prepaway-exam-dumps.html (**745** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 332
Suppose your company has just passed a security risk assessment exercise. The results display that the risk of the breach in the main company application is 50%. Security staff has taken some measures and implemented the necessary controls. After that another security risk assessment was performed showing that risk has decreased to 10%. The risk threshold for the application is 20%.
Which of the following risk decisions will be the best for the project in terms of its successful continuation with most business profit?
A. Introduce more controls to bring risk to 0%
B. Avoid the risk
C. Mitigate the risk
D. Accept the risk
Answer: (SHOW ANSWER)

NEW QUESTION: 333

Which type of sniffing technique is generally referred as MiTM attack?



A. Mac Flooding
B. Password Sniffing
C. DHCP Sniffing
D. ARP Poisoning
Answer: D (LEAVE A REPLY)

NEW QUESTION: 334
_____ is a set of extensions to DNS that provide to DNS clients (resolvers) origin authentication of DNS data to reduce the threat of DNS poisoning, spoofing, and similar attacks types.
A. Zone transfer
B. DNSSEC
C. Resource records
D. Resource transfer
Answer: B (LEAVE A REPLY)

NEW QUESTION: 335
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. tracert

C. ping
D. tcpdump
Answer: (SHOW ANSWER)

NEW QUESTION: 336
Which method can provide a better return on IT security investment and provide a thorough and comprehensive assessment of organizational security covering policy, procedure design, and implementation?
A. Access control list reviews
B. Vulnerability scanning
C. Social engineering
D. Penetration testing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 337
Log monitoring tools performing behavioral analysis have alerted several suspicious logins on a Linux server occurring during non-business hours. After further examination of all login activities, it is noticed that none of the logins have occurred during typical work hours. A Linux administrator who is investigating this problem realizes the system time on the Linux server is wrong by more than twelve hours. What protocol used on Linux servers to synchronize the time has stopped working?
A. PPP
B. NTP
C. OSPP
D. Time Keeper
Answer: (SHOW ANSWER)

NEW QUESTION: 338
If an attacker uses the command SELECT*FROM user WHERE name = 'x' AND userid IS NULL; --'; which type of SQL injection attack is the attacker performing?
A. Tautology
B. UNION SQL Injection
C. End of Line Comment
D. Illegal/Logically Incorrect Query
Answer: C (LEAVE A REPLY)

NEW QUESTION: 339
Sophia travels a lot and worries that her laptop containing confidential documents might be stolen. What is the best protection that will work for her?
A. Hidden folders
B. BIOS password
C. Password protected files
D. Full Disk encryption

Answer: D (LEAVE A REPLY)

NEW QUESTION: 340
You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?
A. hping2 host.domain.com
B. hping2 -i host.domain.com
C. hping2 -1 host.domain.com
D. hping2 --set-ICMP host.domain.com
Answer: C (LEAVE A REPLY)

NEW QUESTION: 341
Susan has attached to her company's network. She has managed to synchronize her boss's sessions with that of the file server. She then intercepted his traffic destined for the server, changed it the way she wanted to and then placed it on the server in his home directory.
What kind of attack is Susan carrying on?
A. A spoofing attack
B. A man in the middle attack
C. A denial of service attack
D. A sniffing attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 342
You are attempting to man-in-the-middle a session. Which protocol will allow you to guess a sequence number?
A. UPX
B. UPD
C. TCP
D. ICMP
Answer: C (LEAVE A REPLY)

NEW QUESTION: 343
Bob is doing a password assessment for one of his clients. Bob suspects that security policies are not in place. He also suspects that weak passwords are probably the norm throughout the company he is evaluating. Bob is familiar with password weaknesses and key loggers.
Which of the following options best represents the means that Bob can adopt to retrieve passwords from his clients hosts and servers?
A. Hardware and Software Keyloggers.
B. Passwords are always best obtained using Hardware key loggers.
C. Hardware, Software, and Sniffing.
D. Software only, they are the most effective.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 344
Study the log below and identify the scan type.



A. nmap -sS 192.168.1.10
B. nmap -sO -T 192.168.1.10
C. nmap -sR 192.168.1.10
D. nmap -sV 192.168.1.10
Answer: B (LEAVE A REPLY)

NEW QUESTION: 345
A software tester is randomly generating invalid inputs in an attempt to crash the program.
Which of the following is a software testing technique used to determine if a software program properly handles a wide range of invalid input?
A. Fuzzing
B. Randomizing
C. Mutating
D. Bounding
Answer: A (LEAVE A REPLY)

NEW QUESTION: 346
When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's Computer to update the router configuration. What type of an alert is this?
A. False negative
B. True negative
C. True positive
D. False positive
Answer: D (LEAVE A REPLY)

Valid 312-50v10 Dumps shared by PrepPdf.com for Helping Passing 312-50v10 Exam! PrepPdf.com now offer the **newest 312-50v10 exam dumps**, the PrepPdf.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-50v10 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-50v10-prepaway-exam-dumps.html (**745** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 347
A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?
A. The computer is using an invalid IP address.
B. The computer is not using a private IP address.
C. The gateway and the computer are not on the same network.
D. The gateway is not routing to a public IP address.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 348
During a blackbox pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded.
What type of firewall is inspecting outbound traffic?
A. Application
B. Circuit
C. Stateful
D. Packet Filtering
Answer: A (LEAVE A REPLY)
Explanation
An application firewall is an enhanced firewall that limits access by applications to the operating system (OS) of a computer. Conventional firewalls merely control the flow of data to and from the central processing unit (CPU), examining each packet and determining whether or not to forward it toward a particular destination.
An application firewall offers additional protection by controlling the execution of files or the handling of data by specific applications.
References:
http://searchsoftwarequality.techtarget.com/definition/application-firewall

NEW QUESTION: 349
You are attempting to run an Nmap port scan on a web server. Which of the following commands would result in a scan of common ports with the least amount of noise in order to evade IDS?
A. nmap -A - Pn
B. nmap -sT -O -T0

C. nmap -sP -p-65535-T5
D. nmap -A --host-timeout 99-T1
Answer: B (LEAVE A REPLY)

NEW QUESTION: 350
SOAP services use which technology to format information?
A. XML
B. SATA
C. PCI
D. ISDN
Answer: A (LEAVE A REPLY)

NEW QUESTION: 351
When setting up a wireless network, an administrator enters a pre-shared key for security. Which of the following is true?
A. The key is an RSA key used to encrypt the wireless data.
B. The key entered is a symmetric key used to encrypt the wireless data.
C. The key entered is based on the Diffie-Hellman method.
D. The key entered is a hash that is used to prove the integrity of the wireless data.
Answer: (SHOW ANSWER)

NEW QUESTION: 352
During a security audit of IT processes, an IS auditor found that there were no documented security procedures. What should the IS auditor do?
A. Identify and evaluate existing practices
B. Create a procedures document
C. Conduct compliance testing
D. Terminate the audit
Answer: (SHOW ANSWER)
The auditor should first evaluated existing policies and practices to identify problem areas and opportunities.

NEW QUESTION: 353
As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?
A. Use split-horizon operation for DNS servers
B. Restrict Zone transfers
C. Harden DNS servers
D. Use the same machines for DNS and other applications
E. Have subnet diversity between DNS servers
Answer: (SHOW ANSWER)

Valid 312-50v10 Dumps shared by PrepPdf.com for Helping Passing 312-50v10 Exam! PrepPdf.com now offer the **newest 312-50v10 exam dumps**, the PrepPdf.com 312-50v10 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-50v10 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-50v10-prepaway-exam-dumps.html (**745** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)