EC-COUNCIL.312-50v10.v2021-11-17.q164

Exam Code:	312-50v10
Exam Name:	Certified Ethical Hacker Exam (CEH v10)
Certification Provider:	EC-COUNCIL
Free Question Number:	164
Version:	v2021-11-17
# of views:	3609
# of Questions views:	1640
https://www.freepdfdumps.com/EC-COUNCIL.312-50v10.v2021-11-17.q164.html	

NEW QUESTION: 1
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. Tailgating
B. Announced
C. Piggybacking
D. Reverse Social Engineering
Answer: (SHOW ANSWER)

NEW QUESTION: 2
An organization hires a tester to do a wireless penetration test. Previous reports indicate that the last test did not contain management or control packets in the submitted traces.
Which of the following is the most likely reason for lack of management or control packets?
A. The wrong network card drivers were in use by Wireshark.
B. The wireless card was not turned on.
C. Certain operating systems and adapters do not collect the management or control packets.
D. On Linux and Mac OS X, only 802.11 headers are received in promiscuous mode.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 3
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: A (LEAVE A REPLY)
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: 4
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. ARP spoofing attack
B. Forensic attack
C. Social engineering attack
D. Scanning attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 5
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 can not provide any information: but, anyway, he/she will provide the name of the
person in charge
B. Disregarding the call, the employee should hang up
C. Since the company's policy is all about Customer Service. he/she will provide information
D. The employee should not provide any information without previous management authorization
Answer: (SHOW ANSWER)

NEW QUESTION: 6
What two conditions must a digital signature meet?
A. Must be unique and have special characters.
B. Has to be legible and neat.
C. Has to be unforgeable, and has to be authentic.

D. Has to be the same number of characters as a physical signature and must be unique.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 7
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: A (LEAVE A REPLY)
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: 8
Under the "Post-attack Phase and Activities", it is the responsibility of the tester to restore the systems to a pre-test state.
Which of the following activities should not be included in this phase? (see exhibit) Exhibit:

A. III
B. IV
C. III and IV
D. All should be included.
Answer: (SHOW ANSWER)
The post-attack phase revolves around returning any modified system(s) to the pretest state.
Examples of such activities:
References: Computer and Information Security Handbook, John R. Vacca (2012), page 531

NEW QUESTION: 9
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: (SHOW ANSWER)
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: 10
Bob learned that his username and password for a popular game has been compromised. He contacts the
company and resets all the information. The company suggests he use two-factor authentication; which
option below offers that?
A. His username and a stronger password
B. A new username and password
C. A fingerprint scanner and his username and password
D. Disable his username and use just a fingerprint scanner
Answer: C (LEAVE A REPLY)

NEW QUESTION: 11
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 sequence does not matter. Both steps have to be performed against all hosts.
B. The port scan alone is adequate. This way he saves time.
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: D (LEAVE A REPLY)

NEW QUESTION: 12
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: (SHOW ANSWER)
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: 13
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)
Explanation
The auditor should first evaluated existing policies and practices to identify problem areas and opportunities.

NEW QUESTION: 14
You are logged in as a local admin on a Windows 7 system and you need to launch the Computer Management Console from command line.
Which command would you use?
A. c:\compmgmt.msc
B. c:\services.msc
C. c:\ncpa.cp

D. c:\gpedit
Answer: A (LEAVE A REPLY)
Explanation
To start the Computer Management Console from command line just type compmgmt.msc /computer:computername in your run box or at the command line and it should automatically open the Computer Management console.
References:
http://www.waynezim.com/tag/compmgmtmsc/

NEW QUESTION: 15
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, ""1111111111111111111111111111"");
}
Output:
Segmentation fault
A. Java
B. Python
C. C#
D. C++
Answer: D (LEAVE A REPLY)

NEW QUESTION: 16
Which DNS resource record can indicate how long any "DNS poisoning" could last?
A. MX
B. TIMEOUT
C. SOA
D. NS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 17
Craig received a report of all the computers on the network that showed all the missing patches and weak passwords. What type of software generated this report?
A. a virus scanner
B. a malware scanner
C. a vulnerability scanner
D. a port scanner
Answer: C (LEAVE A REPLY)

NEW QUESTION: 18
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. Authentication
B. Non-Repudiation
C. Confidentiality
D. Integrity
Answer: (SHOW ANSWER)

NEW QUESTION: 19
You have compromised a server on a network and successfully opened a shell. You aimed to identify all operating systems running on the network. However, as you attempt to fingerprint all machines in the network using the nmap syntax below, it is not going through.

```
invictus@victim_server:~$ nmap -T4 -O 10.10.0.0/24
TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx.
QUITTING!
```

What seems to be wrong?
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: A (LEAVE A REPLY)
You requested a scan type which requires root privileges.
References: http://askubuntu.com/questions/433062/using-nmap-for-information-regarding- web-host

NEW QUESTION: 20

Which one of the following Google advanced search operators allows an attacker to restrict the results to
those websites in the given domain?
A. [site:]
B. [inurl:]
C. [link:]
D. [cache:]
Answer: A (LEAVE A REPLY)

NEW QUESTION: 21
A pentester is using Metasploit to exploit an FTP server and pivot to a LAN. How will the pentester pivot using Metasploit?
A. Issue the pivot exploit and set the meterpreter.
B. Reconfigure the network settings in the meterpreter.
C. Create a route statement in the meterpreter.
D. Set the payload to propagate through the meterpreter.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 22
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. Man trap
C. Shoulder surfing
D. Tailgating
Answer: D (LEAVE A REPLY)

NEW QUESTION: 23
At a Windows Server command prompt, which command could be used to list the running services?
A. Sc config
B. Sc query type= running
C. Sc query \\servername
D. Sc query
Answer: D (LEAVE A REPLY)

NEW QUESTION: 24

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

NEW QUESTION: 25
Which of the following open source tools would be the best choice to scan a network for potential targets?
A. CAIN
B. NIKTO
C. NMAP
D. John the Ripper
Answer: C (LEAVE A REPLY)

NEW QUESTION: 26
Which of the following cryptography attack methods is usually performed without the use of a computer?
A. Chosen key attack
B. Rainbow table attack
C. Ciphertext-only attack
D. Rubber hose attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 27
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
```


A. 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.
B. 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.
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. 10.0.0.253 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.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 28
John the Ripper is a technical assessment tool used to test the weakness of which of the following?
A. Firewall rulesets
B. Usernames
C. Passwords
D. File permissions

Answer: C (LEAVE A REPLY)

NEW QUESTION: 29
What hacking attack is challenge/response authentication used to prevent?
A. Replay attacks
B. Scanning attacks
C. Session hijacking attacks
D. Password cracking attacks
Answer: A (LEAVE A REPLY)

NEW QUESTION: 30
Which of the following does proper basic configuration of snort as a network intrusion detection system require?
A. Limit the packets captured to the snort configuration file.
B. Capture every packet on the network segment.
C. Limit the packets captured to the /var/log/snort directory.
D. Limit the packets captured to a single segment.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 31
Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?
A. tcptrace
B. tcptraceroute
C. Nessus
D. OpenVAS
Answer: (SHOW ANSWER)
tcptrace is a tool for analysis of TCP dump files. It can take as input the files produced by several popular packet-capture programs, including tcpdump/WinDump/Wireshark, snoop, EtherPeek, and Agilent NetMetrix.
References: https://en.wikipedia.org/wiki/Tcptrace

NEW QUESTION: 32
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. The solution will have a high level of false positives
C. The solution implements the two authentication factors: physical object and physical characteristic
D. Although the approach has two phases, it actually implements just one authentication factor
Answer: C (LEAVE A REPLY)

NEW QUESTION: 33
Which of the following is designed to verify and authenticate individuals taking part in a data exchange within an enterprise?
A. Biometrics
B. SOA
C. Single-Sign On
D. PKI
Answer: D (LEAVE A REPLY)

NEW QUESTION: 34
The security administrator of ABC needs to permit Internet traffic in the host 10.0.0.2 and UDP traffic in the host 10.0.0.3. He also needs to permit all FTP traffic to the rest of the network and deny all other traffic. After he applied his ACL configuration in the router, nobody can access to the ftp, and the permitted hosts cannot access the Internet.
According to the next configuration, what is happening in the network?

```
access-list 102 deny tcp any any
access-list 104 permit udp host 10.0.0.3 any
access-list 110 permit tcp host 10.0.0.2 eq www any
access-list 108 permit tcp any eq ftp any
```

A. The ACL for FTP must be before the ACL 110
B. The ACL 110 needs to be changed to port 80
C. The ACL 104 needs to be first because is UDP
D. The first ACL is denying all TCP traffic and the other ACLs are being ignored by the router
Answer: D (LEAVE A REPLY)

NEW QUESTION: 35
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
```


What type of activity has been logged?

A. Teardrop attack targeting 192.168.1.106

B. Denial of service attack targeting 192.168.1.103

C. Port scan targeting 192.168.1.106

D. Port scan targeting 192.168.1.103

Answer: C (LEAVE A REPLY)

NEW QUESTION: 36

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. Unix

B. OS X

C. Windows

D. Linux

Answer: C (LEAVE A REPLY)

NEW QUESTION: 37

Which technical characteristic do Ethereal/Wireshark, TCPDump, and Snort have in common?

A. They use the same packet capture utility.

B. They are written in Java.

C. They send alerts to security monitors.

D. They use the same packet analysis engine.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 38

It is an entity or event with the potential to adversely impact a system through unauthorized acces,

destruction, disclosure, denial of service or modification of data. Which of the following terms best matches
the definition?
A. Threat
B. Vulnerability
C. Attack
D. Risk
Answer: A (LEAVE A REPLY)

NEW QUESTION: 39
Which of the following is a common Service Oriented Architecture (SOA) vulnerability?
A. SQL injection
B. VPath injection
C. Cross-site scripting
D. XML denial of service issues
Answer: D (LEAVE A REPLY)

NEW QUESTION: 40
While checking the settings on the internet browser, a technician finds that the proxy server settings have been checked and a computer is trying to use itself as a proxy server. What specific octet within the subnet does the technician see?
A. 192.168.1.1
B. 127.0.0.1
C. 192.168.168.168
D. 10.10.10.10
Answer: B (LEAVE A REPLY)

NEW QUESTION: 41
A company has hired a security administrator to maintain and administer Linux and Windows-based systems.
Written in the nightly report file is the following:
Firewall log files are at the expected value of 4 MB. The current time is 12am. Exactly two hours later the size has decreased considerably. Another hour goes by and the log files have shrunk in size again.
Which of the following actions should the security administrator take?
A. Run an anti-virus scan because it is likely the system is infected by malware.
B. Log the event as suspicious activity, continue to investigate, and act according to the site's security policy.
C. Log the event as suspicious activity, call a manager, and report this as soon as possible.
D. Log the event as suspicious activity and report this behavior to the incident response team immediately.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 42
What type of analysis is performed when an attacker has partial knowledge of inner-workings of the application?
A. Black-box
B. White-box
C. Announced
D. Grey-box
Answer: D (LEAVE A REPLY)

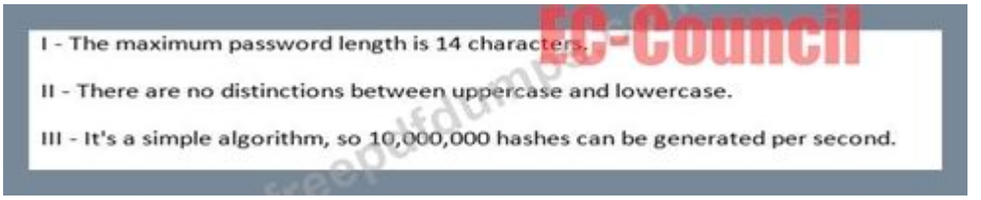
NEW QUESTION: 43
As an Ethical Hacker you are capturing traffic from your customer network with Wireshark and you need to
find and verify just SMTP traffic. What command in Wireshark will help you to find this kind of traffic?
A. smtp port
B. request smtp 25
C. tcp.port eq 25
D. tcp.contains port 25
Answer: C (LEAVE A REPLY)

NEW QUESTION: 44
What does a firewall check to prevent particular ports and applications from getting packets into an organization?
A. Application layer port numbers and the transport layer headers
B. Presentation layer headers and the session layer port numbers
C. Network layer headers and the session layer port numbers
D. Transport layer port numbers and application layer headers
Answer: (SHOW ANSWER)

NEW QUESTION: 45
Which type of antenna is used in wireless communication?
A. Parabolic
B. Omnidirectional
C. Uni-directional
D. Bi-directional
Answer: B (LEAVE A REPLY)

NEW QUESTION: 46
Which of the following parameters describe LM Hash (see exhibit):

Exhibit:



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: 47
The purpose of a _____ is to deny network access to local area networks and other information assets by unauthorized wireless devices.
A. Wireless Intrusion Prevention System
B. Wireless Access Point
C. Wireless Access Control List
D. Wireless Analyzer
Answer: A (LEAVE A REPLY)
A wireless intrusion prevention system (WIPS) is a network device that monitors the radio spectrum for the presence of unauthorized access points (intrusion detection), and can automatically take countermeasures (intrusion prevention).
References: https://en.wikipedia.org/wiki/Wireless_intrusion_prevention_system

NEW QUESTION: 48
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. lserver 192.168.10.2 -t all
C. list server=192.168.10.2 type=all
D. list domain=abccorp.local type=zone
Answer: A (LEAVE A REPLY)

NEW QUESTION: 49
A regional bank hires your company to perform a security assessment on their network after a recent data breach. The attacker was able to steal financial data from the bank by compromising only a single server.
Based on this information, what should be one of your key recommendations to the bank?
A. Place a front-end web server in a demilitarized zone that only handles external web traffic
B. Require all employees to change their passwords immediately
C. Move the financial data to another server on the same IP subnet
D. Issue new certificates to the web servers from the root certificate authority
Answer: (SHOW ANSWER)
A DMZ or demilitarized zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external network node only has direct access to equipment in the DMZ, rather than any other part of the network.
References: https://en.wikipedia.org/wiki/DMZ_(computing)

NEW QUESTION: 50
Some clients of TPNQM SA were redirected to a malicious site when they tried to access the TPNQM main
site. Bob, a system administrator at TPNQM SA, found that they were victims of DNS Cache Poisoning.
What should Bob recommend to deal with such a threat?
A. The use of double-factor authentication
B. The use of security agents in clients' computers
C. Client awareness
D. The use of DNSSEC
Answer: D (LEAVE A REPLY)

NEW QUESTION: 51
During the process of encryption and decryption, what keys are shared?
During the process of encryption and decryption, what keys are shared?
A. Public keys
B. Private keys
C. User passwords
D. Public and private keys
Answer: A (LEAVE A REPLY)

NEW QUESTION: 52
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: 53
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: (SHOW ANSWER)
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: 54
Which results will be returned with the following Google search query? site:target.com site:Marketing.target.com accounting

A. Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting.
B. Results matching "accounting" in domain target.com but not on the site Marketing.target.com
C. Results for matches on target.com and Marketing,target.com that include the word "accounting"
D. Results matching all words in the query.
Answer: (SHOW ANSWER)

NEW QUESTION: 55
You have several plain-text firewall logs that you must review to evaluate network traffic. You know that in order to do fast, efficient searches of the logs you must use regular expressions. Which command-line utility are you most likely to use?
A. Grep
B. Notepad
C. MS Excel
D. Relational Database
Answer: A (LEAVE A REPLY)
Explanation
grep is a command-line utility for searching plain-text data sets for lines matching a regular expression.
References: https://en.wikipedia.org/wiki/Grep

NEW QUESTION: 56
Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?
A. AH Tunnel mode
B. ESP confidential
C. ESP transport mode
D. AH permiscuous
Answer: C (LEAVE A REPLY)

NEW QUESTION: 57
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. Heuristics based
B. Behavioral based
C. Cloud based
D. Honypot based

Answer: (SHOW ANSWER)

NEW QUESTION: 58
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. Shellshock
B. Shellbash
C. Rootshock
D. Rootshell
Answer: A (LEAVE A REPLY)

NEW QUESTION: 59
The "black box testing" methodology enforces which kind of restriction?
A. Only the external operation of a system is accessible to the tester.
B. Only the internal operation of a system is known to the tester.
C. The internal operation of a system is only partly accessible to the tester.
D. The internal operation of a system is completely known to the tester.
Answer: A (LEAVE A REPLY)
Explanation
Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings.
References: https://en.wikipedia.org/wiki/Black-box_testing

NEW QUESTION: 60
The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124.
An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is:
nmap 192.168.1.64/28.
Why he cannot see the servers?
A. He needs to add the command ""ip address"" just before the IP address.
B. He needs to change the address to 192.168.1.0 with the same mask.
C. The network must be down and the nmap command and IP address are ok.
D. He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are not in that range.
Answer: (SHOW ANSWER)

NEW QUESTION: 61
An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections.

When users accessed any page, the applet ran and exploited many machines.
Which one of the following tools the hacker probably used to inject HTML code?
A. Aircrack-ng
B. Tcpdump
C. Ettercap
D. Wireshark
Answer: (SHOW ANSWER)

NEW QUESTION: 62
Which method of password cracking takes the most time and effort?
A. Brute force
B. Rainbow tables
C. Dictionary attack
D. Shoulder surfing
Answer: A (LEAVE A REPLY)
Brute-force cracking, in which a computer tries every possible key or password until it succeeds, is typically very time consuming. More common methods of password cracking, such as dictionary attacks, pattern checking, word list substitution, etc. attempt to reduce the number of trials required and will usually be attempted before brute force.
References: https://en.wikipedia.org/wiki/Password_cracking

NEW QUESTION: 63
Which of the following is the least-likely physical characteristic to be used in biometric control that supports a large company?
A. Height and Weight
B. Voice
C. Fingerprints
D. Iris patterns
Answer: A (LEAVE A REPLY)
There are two main types of biometric identifiers:

Examples of physiological characteristics used for biometric authentication include fingerprints; DNA; face, hand, retina or ear features; and odor. Behavioral characteristics are related to the pattern of the behavior of a person, such as typing rhythm, gait, gestures and voice.
References: http://searchsecurity.techtarget.com/definition/biometrics

NEW QUESTION: 64
What is the broadcast address for the subnet 190.86.168.0/22?
A. 190.86.171.255
B. 190.86.169.255
C. 190.86.255.255
D. 190.86.168.255
Answer: (SHOW ANSWER)

NEW QUESTION: 65
Which of the following tools is used to detect wireless LANs using the 802.11 a/b/g/n WLAN standards on a linux platform?
A. Kismet
B. Netstumbler
C. Nessus
D. Abel
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 66
It 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. The malicious software can take control of an infected machine, launch denial-of-service attacks to disrupt websites, and scan for other vulnerable devices (including routers).
Which of the following vulnerabilities is being described?
A. Shellshock
B. Rootshock
C. Rootshell
D. Shellbash
Answer: A (LEAVE A REPLY)
Explanation
Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell, the first of which was disclosed on 24 September 2014.
References: https://en.wikipedia.org/wiki/Shellshock_(software_bug)

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. Botnet Attack
B. Spear Phishing Attack
C. Advanced Persistent Threats
D. Rootkit Attack
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 68
A developer for a company is tasked with creating a program that will allow customers to update their billing and shipping information. The billing address field used is limited to 50 characters. What pseudo code would the developer use to avoid a buffer overflow attack on the billing address field?
A. if (billingAddress != 50) {update field} else exit
B. if (billingAddress >= 50) {update field} else exit
C. if (billingAddress <= 50) {update field} else exit
D. if (billingAddress = 50) {update field} else exit
Answer: C (LEAVE A REPLY)

NEW QUESTION: 69
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. black box
C. red box
D. grey box
Answer: (SHOW ANSWER)

NEW QUESTION: 70
Which access control mechanism allows for multiple systems to use a central authentication server (CAS) that permits users to authenticate once and gain access to multiple systems?

A. Discretionary Access Control (DAC)
B. Single sign-on
C. Windows authentication
D. Role Based Access Control (RBAC)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 71
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. Event logs on domain controller
C. Internet Firewall/Proxy log
D. IDS log
Answer: C (LEAVE A REPLY)

NEW QUESTION: 72
Which is the first step followed by Vulnerability Scanners for scanning a network?
A. OS Detection
B. Firewall detection
C. TCP/UDP Port scanning
D. Checking if the remote host is alive
Answer: (SHOW ANSWER)

NEW QUESTION: 73
Log monitoring tools performing behavioral analysis have alerted several suspicious logins on a Linux server occuring during non-business hours. After further examination of all login activities, it is notices that none of the logins have occurred during typical work hours. A Linux administrator who is investigating this problem realized the system time on the Linux server is wrong by more than twelve hours. What protocol used on Linux serves to synchronize the time has stopped working?
A. TimeKeeper
B. NTP
C. PPP
D. OSPF
Answer: B (LEAVE A REPLY)

NEW QUESTION: 74

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. Path disclosure

B. Cross Site Request Forgery

C. Injection

D. Cross Site Scripting

Answer: (SHOW ANSWER)

NEW QUESTION: 75

Which of the following is designed to identify malicious attempts to penetrate systems?

A. Intrusion Detection System

B. Firewall

C. Proxy

D. Router

Answer: (SHOW ANSWER)

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: 76

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. An Intrusion Detection System

B. A firewall IPTable

C. A Router IPTable

D. FTP Server rule

Answer: (SHOW ANSWER)

NEW QUESTION: 77
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()
```

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

NEW QUESTION: 78
Eve stole a file named secret.txt, transferred it to her computer and she just entered these commands:

```
[eve@localhost ~]$ john secret.txt
Loaded 2 password hashes with no different salts (LM [DES 128/128 SSE2-
16])
Press 'q' or Ctrl-C to abort. almost any other key for status
0g 0:00:00:03 3/3 0g/s 86168p/s 86168c/s 172336C/s MERO..SAMPLUI
0g 0:00:00:04 3/3 0g/s 3296Kp/s 3296Kc/s 6592KC/s GOS..KARIS4
0g 0:00:00:07 3/3 0g/s 8154Kp/s 8154Kc/s 16309KC/s NY180K..NY1837
0g 0:00:00:10 3/3 0g/s 7958Kp/s 7958Kc/s 1591KC/s SHAGRN..SHENY9
```

What is she trying to achieve?
A. She is using ftp to transfer the file to another hacker named John.
B. She is encrypting the file.
C. She is using John the Ripper to crack the passwords in the secret.txt file.
D. She is using John the Ripper to view the contents of the file.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 79
What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?
A. Impact risk
B. Residual risk
C. Inherent risk
D. Deferred risk
Answer: B (LEAVE A REPLY)

NEW QUESTION: 80
Fingerprinting an Operating System helps a cracker because:
A. It defines exactly what software you have installed
B. It opens a security-delayed window based on the port being scanned
C. It doesn't depend on the patches that have been applied to fix existing security holes
D. It informs the cracker of which vulnerabilities he may be able to exploit on your system
Answer: D (LEAVE A REPLY)

NEW QUESTION: 81
What is the role of test automation in security testing?
A. It should be used exclusively. Manual testing is outdated because of low speed and possible test setup inconsistencies.
B. Test automation is not usable in security due to the complexity of the tests.
C. It can accelerate benchmark tests and repeat them with a consistent test setup. But it cannot replace manual testing completely.
D. It is an option but it tends to be very expensive.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 82
As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?
A. Have subnet diversity between DNS servers
B. Restrict Zone transfers
C. Harden DNS servers
D. Use split-horizon operation for DNS servers
E. Use the same machines for DNS and other applications
Answer: A,B,C,D (LEAVE A REPLY)

NEW QUESTION: 83

Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

A. tcptrace

B. tcptraceroute

C. Nessus

D. OpenVAS

Answer: A (LEAVE A REPLY)

Explanation

tcptrace is a tool for analysis of TCP dump files. It can take as input the files produced by several popular packet-capture programs, including tcpdump/WinDump/Wireshark, snoop, EtherPeek, and Agilent NetMetrix.

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

NEW QUESTION: 84

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. Encryption

B. Steganography

C. RSA algorithm

D. Public-key cryptography

Answer: (SHOW ANSWER)

NEW QUESTION: 85

The network administrator at Spears Technology, Inc has configured the default gateway Cisco router's access-list as below:

You are hired to conduct security testing on their network.

You successfully brute-force the SNMP community string using a SNMP crack tool.

The access-list configured at the router prevents you from establishing a successful connection.

You want to retrieve the Cisco configuration from the router. How would you proceed?

A. Run Generic Routing Encapsulation (GRE) tunneling protocol from your computer to the router masking your IP address

B. Run a network sniffer and capture the returned traffic with the configuration file from the router

C. Send a customized SNMP set request with a spoofed source IP address in the range - 192.168.1.0

D. Use the Cisco's TFTP default password to connect and download the configuration file

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 86
You are logged in as a local admin on a Windows 7 system and you need to launch the Computer Management Console from command line.
Which command would you use?
A. c:\compmgmt.msc
B. c:\services.msc
C. c:\ncpa.cp
D. c:\gpedit
Answer: A (LEAVE A REPLY)
To start the Computer Management Console from command line just type compmgmt.msc /computer:computername in your run box or at the command line and it should automatically open the Computer Management console.
References: http://www.waynezim.com/tag/compmgmtmsc/

NEW QUESTION: 87
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. Determines risk probability that vulnerability will be exploited (High. Medium, Low)
C. Determines if any flaws exist in systems, policies, or procedures
D. Assigns values to risk probabilities; Impact values.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 88
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 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
C. The document can be sent to the accountant using an exclusive USB for that document
D. The CFO can use an excel file with a password
Answer: (SHOW ANSWER)

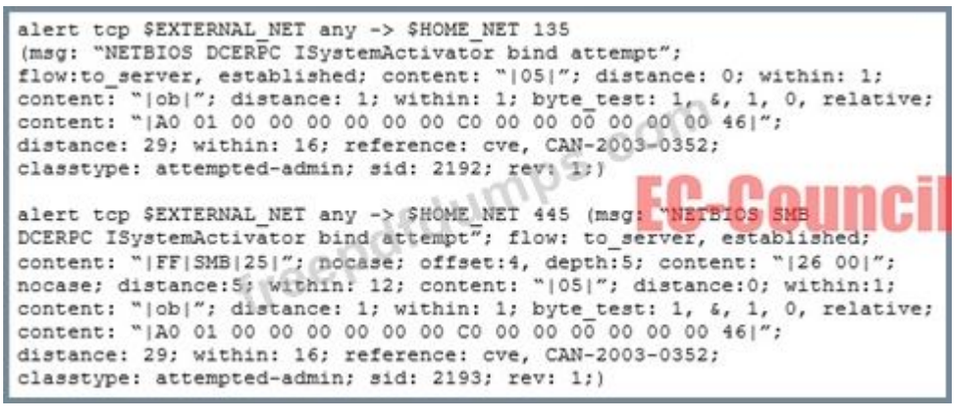
NEW QUESTION: 89
Which tier in the N-tier application architecture is responsible for moving and processing data between the
tiers?
A. Data tier

B. Application Layer
C. Presentation tier
D. Logic tier
Answer: D (LEAVE A REPLY)

NEW QUESTION: 90
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. Preparation phase
B. Containment phase
C. Identification phase
D. Recovery phase
Answer: A (LEAVE A REPLY)
Explanation
There are several key elements to have implemented in preparation phase in order to help mitigate any potential problems that may hinder one's ability to handle an incident. For the sake of brevity, the following should be performed:
References: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

NEW QUESTION: 91
Which of the following is a form of penetration testing that relies heavily on human interaction and often involves tricking people into breaking normal security procedures?
A. Piggybacking
B. Social Engineering
C. Tailgating
D. Eavesdropping
Answer: B (LEAVE A REPLY)

NEW QUESTION: 92
Study the snort rule given below:



From the options below, choose the exploit against which this rule applies.

A. MS Blaster

B. WebDav

C. MyDoom

D. SQL Slammer

Answer: A (LEAVE A REPLY)

NEW QUESTION: 93

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: 94

Tremp is an IT Security Manager, and he is planning to deploy an IDS in his small company. He is looking for an IDS with the following characteristics: - Verifies success or failure of an attack - Monitors system activities Detects attacks that a network-based IDS fails to detect - Near real-time detection and response - Does not require additional hardware - Lower entry cost Which type of IDS is best suited for Tremp's requirements?

A. Gateway-based IDS

B. Open source-based

C. Network-based IDS

D. Host-based IDS
Answer: (SHOW ANSWER)

NEW QUESTION: 95
Which of the following resources does NMAP need to be used as a basic vulnerability scanner covering several vectors like SMB, HTTP and FTP?
A. SAINT scripting engine
B. Nessus scripting engine
C. Metasploit scripting engine
D. NMAP scripting engine
Answer: (SHOW ANSWER)

NEW QUESTION: 96
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. Spear Phishing Attack
B. Advanced Persistent Threats
C. Botnet Attack
D. Rootkit Attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 97
Let's imagine three companies (A, B and C), all competing in a challenging global environment. Company A and B are working together in developing a product that will generate a major competitive advantage for them. Company A has a secure DNS server while company B has a DNS server vulnerable to spoofing. With a spoofing attack on the DNS server of company B, company C gains access to outgoing e-mails from company B.
How do you prevent DNS spoofing?
A. Install DNS logger and track vulnerable packets
B. Disable DNS timeouts
C. Install DNS Anti-spoofing
D. Disable DNS Zone Transfer
Answer: C (LEAVE A REPLY)

NEW QUESTION: 98
Which one of the following Google advanced search operators allows an attacker to restrict the results to those websites in the given domain?
A. [cache:]
B. [site:]
C. [inurl:]
D. [link:]
Answer: B (LEAVE A REPLY)

NEW QUESTION: 99
A large mobile telephony and data network operator has a data center that houses network elements.
These are essentially large computers running on Linux. The perimeter of the data center is secured with
firewalls and IPS systems.
What is the best security policy concerning this setup?
A. Network elements must be hardened with user ids and strong passwords. Regular security tests and
audits should be performed.
B. The operator knows that attacks and down time are inevitable and should have a backup site.
C. As long as the physical access to the network elements is restricted, there is no need for additional
measures.
D. There is no need for specific security measures on the network elements as long as firewalls and IPS
systems exist.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 100
Which tool allows analysts and pen testers to examine links between data using graphs and link analysis?
A. Maltego
B. Cain & Abel
C. Metasploit
D. Wireshark
Answer: A (LEAVE A REPLY)
Maltego is proprietary software used for open-source intelligence and forensics, developed by Paterva. Maltego focuses on providing a library of transforms for discovery of data from open sources, and visualizing that information in a graph format, suitable for link analysis and data mining.
References: https://en.wikipedia.org/wiki/Maltego

NEW QUESTION: 101
>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: A (LEAVE A REPLY)

NEW QUESTION: 102
In IPv6 what is the major difference concerning application layer vulnerabilities compared to IPv4?
A. Implementing IPv4 security in a dual-stack network offers protection from IPv6 attacks too.
B. Vulnerabilities in the application layer are greatly different from IPv4.
C. Vulnerabilities in the application layer are independent of the network layer. Attacks and mitigation techniques are almost identical.
D. Due to the extensive security measures built in IPv6, application layer vulnerabilities need not be addresses.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 103
Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to
VHF and UHF?
A. Dipole antenna
B. Yagi antenna
C. Parabolic grid antenna
D. Omnidirectional antenna
Answer: B (LEAVE A REPLY)

NEW QUESTION: 104
Low humidity in a data center can cause which of the following problems?
A. Corrosion
B. Static electricity
C. Airborne contamination
D. Heat
Answer: B (LEAVE A REPLY)

NEW QUESTION: 105
What kind of risk will remain even if all theoretically possible safety measures would be applied?
A. Residual risk

B. Deferred risk
C. Inherent risk
D. Impact risk
Answer: A (LEAVE A REPLY)

NEW QUESTION: 106
Within the context of Computer Security, which of the following statements describes Social Engineering best?
A. Social Engineering is the means put in place by human resource to perform time accounting
B. Social Engineering is the act of getting needed information from a person rather than breaking into a system
C. Social Engineering is the act of publicly disclosing information
D. Social Engineering is a training program within sociology studies
Answer: B (LEAVE A REPLY)

NEW QUESTION: 107
An engineer is learning to write exploits in C++ and is using the exploit tool Backtrack. The engineer wants to compile the newest C++ exploit and name it calc.exe. Which command would the engineer use to accomplish this?
A. g++ hackersExploit.cpp -o calc.exe
B. g++ -i hackersExploit.pl -o calc.exe
C. g++ --compile -i hackersExploit.cpp -o calc.exe
D. g++ hackersExploit.py -o calc.exe
Answer: A (LEAVE A REPLY)

NEW QUESTION: 108
Which results will be returned with the following Google search query?
site:target.com -site:Marketing.target.com accounting
A. Results for matches on target.com and Marketing.target.com that include the word "accounting"
B. Results matching all words in the query
C. Results matching "accounting" in domain target.com but not on the site Marketing.target.com

D. Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting
Answer: (SHOW ANSWER)

NEW QUESTION: 109
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: A (LEAVE A REPLY)
Explanation
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: 110
You are monitoring the network of your organizations. You notice that:
There are huge outbound connections from your Internal Network to External IPs
- On further investigation, you see that the external IPs are blacklisted
- Some connections are accepted, and some are dropped
- You find that it is a CnC communication
- Which of the following solution will you suggest?

A. Block the Blacklist IP's @ Firewall
B. Clean the Malware which are trying to Communicate with the External Blacklist IP's
C. Update the Latest Signatures on your IDS/IPS
D. Both B and C
Answer: (SHOW ANSWER)

NEW QUESTION: 111
What kind of detection techniques is being used in antivirus software 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. Behavioral based

B. Honypot based
C. Heuristics based
D. Cloud based
Answer: D (LEAVE A REPLY)

NEW QUESTION: 112
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)
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: 113
This phase will increase the odds of success in later phases of the penetration test. It is also the very first step in Information Gathering, and it will tell you what the "landscape" looks like.
What is the most important phase of ethical hacking in which you need to spend a considerable amount of time?
A. footprinting
B. network mapping
C. gaining access
D. escalating privileges
Answer: (SHOW ANSWER)
Explanation
Footprinting is a first step that a penetration tester used to evaluate the security of any IT infrastructure, footprinting means to gather the maximum information about the computer system or a network and about the devices that are attached to this network.
References:
http://www.ehacking.net/2011/02/footprinting-first-step-of-ethical.html

NEW QUESTION: 114
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

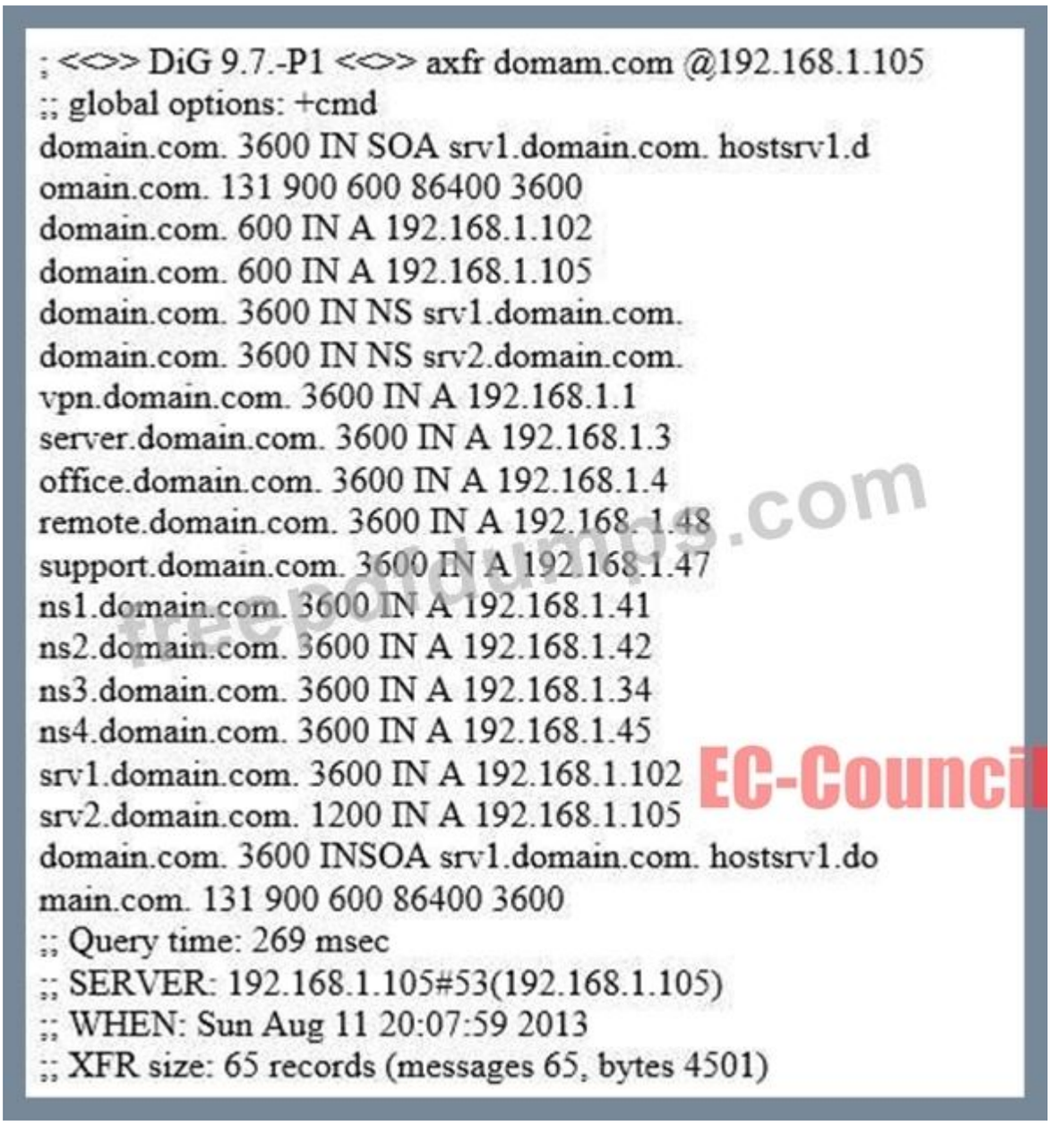
B. Invoking the stored procedure xp_shell to spawn a Windows command shell
C. Using the Metasploit psexec module setting the SA / Admin credential
D. Invoking the stored procedure cmd_shell to spawn a Windows command shell
Answer: A (LEAVE A REPLY)

NEW QUESTION: 115
Which of the following provides a security professional with most information about the system's security posture?
A. Social engineering, company site browsing, tailgating
B. Phishing, spamming, sending trojans
C. Wardriving, warchalking, social engineering
D. Port scanning, banner grabbing, service identification
Answer: (SHOW ANSWER)

NEW QUESTION: 116
An attacker tries to do banner grabbing on a remote web server and executes the following command.

Service
detection performed. Please report any incorrect results at http://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 6.42 seconds
What did the hacker accomplish?
A. The hacker failed to do banner grabbing as he didn't get the version of the Apache web server.
B. nmap can't retrieve the version number of any running remote service.
C. The hacker successfully completed the banner grabbing.
D. The hacker should've used nmap -O host.domain.com.
Answer: (SHOW ANSWER)

NEW QUESTION: 117
Look at the following output. What did the hacker accomplish?



A. The hacker listed DNS records on his own domain.

B. The hacker used who is to gather publicly available records for the domain.

C. The hacker used the "fierce" tool to brute force the list of available domains.

D. The hacker successfully transferred the zone and enumerated the hosts.

Answer: (SHOW ANSWER)

NEW QUESTION: 118

Company XYZ has asked you to assess the security of their perimeter email gateway. From your office in New York, you craft a specially formatted email message and send it across the Internet to an employee of Company XYZ. The employee of Company XYZ is aware of your test.

Your email message looks like this:

From: jim_miller@companyxyz.com

To: michelle_saunders@companyxyz.com

Subject: Test message

Date: 4/3/2017 14:37
The employee of Company XYZ receives your email message. This proves that Company XYZ's email gateway doesn't prevent what?
A. Email Harvesting
B. Email Phishing
C. Email Masquerading
D. Email Spoofing
Answer: (SHOW ANSWER)

NEW QUESTION: 119
You are monitoring the network of your organizations. You notice that:
Which of the following solution will you suggest?
A. Both B and C
B. Block the Blacklist IP's @ Firewall
C. Clean the Malware which are trying to Communicate with the External Blacklist IP's
D. Update the Latest Signatures on your IDS/IPS
Answer: A (LEAVE A REPLY)

NEW QUESTION: 120
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. Bloover
B. BBProxy
C. Paros Proxy
D. BBCrack
Answer: (SHOW ANSWER)

NEW QUESTION: 121
What is the best description of SQL Injection?
A. It is an attack used to gain unauthorized access to a database.
B. It is an attack used to modify code in an application.
C. It is a Man-in-the-Middle attack between your SQL Server and Web App Server.
D. It is a Denial of Service Attack.
Answer: (SHOW ANSWER)

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).
References: https://en.wikipedia.org/wiki/SQL_injection

NEW QUESTION: 122
An attacker runs netcat tool to transfer a secret file between two hosts.

```
Machine A: netcat -l -p 1234 < secretfile
Machine B: netcat 192.168.3.4 > 1234
```

He is worried about information being sniffed on the network.
How would the attacker use netcat to encrypt the information before transmitting onto the wire?
A. Machine A: netcat -l -p 1234 < testfile -pw passwordMachine B: netcat <machine A IP> 1234 -pw password
B. Use cryptcat instead of netcat
C. Machine A: netcat -l -p -s password 1234 < testfileMachine B: netcat <machine A IP> 1234
D. Machine A: netcat -l -e magickey -p 1234 < testfileMachine B: netcat <machine A IP> 1234
Answer: B (LEAVE A REPLY)

NEW QUESTION: 123
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 document can be sent to the accountant using an exclusive USB for that document.
B. 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.
C. The CFO can use a hash algorithm in the document once he approved the financial statements.
D. The CFO can use an excel file with a password.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 124
Port scanning can be used as part of a technical assessment to determine network vulnerabilities. The TCP XMAS scan is used to identify listening ports on the targeted system.
If a scanned port is open, what happens?
A. The port will ignore the packets.
B. The port will send an RST.
C. The port will send an ACK.
D. The port will send a SYN.
Answer: A (LEAVE A REPLY)
Explanation
An attacker uses a TCP XMAS scan to determine if ports are closed on the target machine. This scan type is accomplished by sending TCP segments with the all flags sent in the packet header, generating packets that are illegal based on RFC 793. The RFC 793 expected behavior is that any TCP segment with an out-of-state Flag sent to an open port is discarded, whereas segments with out-of-state flags sent to closed ports should be handled with a RST in response. This behavior should allow an attacker to scan for closed ports by sending certain types of rule-breaking packets (out of sync or disallowed by the TCB) and detect closed ports via RST packets.
References: https://capec.mitre.org/data/definitions/303.html

NEW QUESTION: 125
Which of the following security policies defines the use of VPN for gaining access to an internal corporate network?
A. Information protection policy
B. Access control policy
C. Remote access policy
D. Network security policy
Answer: C (LEAVE A REPLY)

NEW QUESTION: 126
Which method of password cracking takes the most time and effort?
A. Brute force
B. Rainbow tables
C. Dictionary attack
D. Shoulder surfing
Answer: A (LEAVE A REPLY)
Explanation
Brute-force cracking, in which a computer tries every possible key or password until it succeeds, is typically very time consuming. More common methods of password cracking, such as dictionary attacks, pattern checking, word list substitution, etc. attempt to reduce the number of trials required and will usually be attempted before brute force.
References: https://en.wikipedia.org/wiki/Password_cracking

NEW QUESTION: 127
LM hash is a compromised password hashing function. Which of the following parameters describe LM Hash:?
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.
A. II
B. I, II, and III
C. I
D. I and II
Answer: B (LEAVE A REPLY)

NEW QUESTION: 128
You work for Acme Corporation as Sales Manager. The company has tight network security restrictions. You are trying to steal data from the company's Sales database (Sales.xls) and transfer them to your home computer. Your company filters and monitors traffic that leaves from the internal network to the Internet. How will you achieve this without raising suspicion?
A. Change the extension of Sales.xls to sales.txt and upload them as attachment to your hotmail account
B. You can conceal the Sales.xls database in another file like photo.jpg or other files and send it out in an innocent looking email or file transfer using Steganography techniques
C. Encrypt the Sales.xls using PGP and e-mail it to your personal gmail account
D. Package the Sales.xls using Trojan wrappers and telnet them back your home computer
Answer: (SHOW ANSWER)

NEW QUESTION: 129
A network security administrator is worried about potential man-in-the-middle attacks when users access a corporate web site from their workstations. Which of the following is the best remediation against this type of attack?
A. Implementing server-side PKI certificates for all connections
B. Mandating only client-side PKI certificates for all connections
C. Requiring client and server PKI certificates for all connections
D. Requiring strong authentication for all DNS queries
Answer: C (LEAVE A REPLY)

NEW QUESTION: 130
A security engineer is attempting to map a company's internal network. The engineer enters in the following NMAP command:
NMAP -n -sS -P0 -p 80 ***.***.**.**
What type of scan is this?

A. Comprehensive scan
B. Quick scan
C. Stealth scan
D. Intense scan
Answer: C (LEAVE A REPLY)

NEW QUESTION: 131
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
```

What type of activity has been logged?
A. Denial of service attack targeting 192.168.1.103
B. Port scan targeting 192.168.1.103
C. Teardrop attack targeting 192.168.1.106
D. Port scan targeting 192.168.1.106
Answer: D (LEAVE A REPLY)

NEW QUESTION: 132
env x='(){ :;};echo exploit' bash -c 'cat/etc/passwd'
What is the Shellshock bash vulnerability attempting to do a vulnerable Linux host?
A. Display passwd content to prompt
B. Changes all passwords in passwd
C. Add new user to the passwd file
D. Removes the passwd file
Answer: A (LEAVE A REPLY)

NEW QUESTION: 133
How can you determine if an LM hash you extracted contains a password that is less than 8 characters long?
A. The right most portion of the hash is always the same
B. The left most portion of the hash is always the same
C. There is no way to tell because a hash cannot be reversed

D. A portion of the hash will be all 0's
E. The hash always starts with AB923D
Answer: A (LEAVE A REPLY)

NEW QUESTION: 134
A security engineer has been asked to deploy a secure remote access solution that will allow employees to connect to the company's internal network. Which of the following can be implemented to minimize the opportunity for the man-in-the-middle attack to occur?
A. IPSec
B. Mutual authentication
C. Static IP addresses
D. SSL
Answer: A (LEAVE A REPLY)

NEW QUESTION: 135
Which of these options is the most secure procedure for storing backup tapes?
A. In a cool dry environment
B. On a different floor in the same building
C. Inside the data center for faster retrieval in a fireproof safe
D. In a climate controlled facility offsite
Answer: D (LEAVE A REPLY)

NEW QUESTION: 136
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. Whaling
D. Phishing
Answer: (SHOW ANSWER)

NEW QUESTION: 137
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 activate OSPF on the spoofed root bridge.
B. He will repeat the same attack against all L2 switches of the network.
C. He will repeat this action so that is escalates to a DoS attack.
D. He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 138
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 Xmas scan. URG, PUSH and FIN are set
C. This is Xmas scan. SYN and ACK flags are set
D. This is ACK scan. ACK flag is set
Answer: (SHOW ANSWER)

NEW QUESTION: 139
The following is part of a log file taken from the machine on the network with the IP address of 192.168.0.110:

```
Time:June 16 17:30:15 Port:20 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:17 Port:21 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:19 Port:22 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:21 Port:23 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:22 Port:25 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:23 Port:80 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:30 Port:443 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
```

What type of activity has been logged?
A. Teardrop attack targeting 192.168.0.110
B. Port scan targeting 192.168.0.105
C. Port scan targeting 192.168.0.110
D. Denial of service attack targeting 192.168.0.105
Answer: C (LEAVE A REPLY)

NEW QUESTION: 140

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, ""1111111111111111111111111111"");
}
```


Output:
Segmentation fault

A. Java
B. Python
C. C++
D. C#
Answer: C (LEAVE A REPLY)

NEW QUESTION: 141
Port scanning can be used as part of a technical assessment to determine network vulnerabilities. The
TCP XMAS scan is used to identify listening ports on the targeted system.
If a scanned port is open, what happens?

A. The port will send a SYN.
B. The port will send an RST.
C. The port will ignore the packets.
D. The port will send an ACK.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 142
Which security strategy requires using several, varying methods to protect IT systems against attacks?

A. Exponential backoff algorithm
B. Three-way handshake
C. Defense in depth
D. Covert channels
Answer: C (LEAVE A REPLY)

NEW QUESTION: 143
What is the role of test automation in security testing?

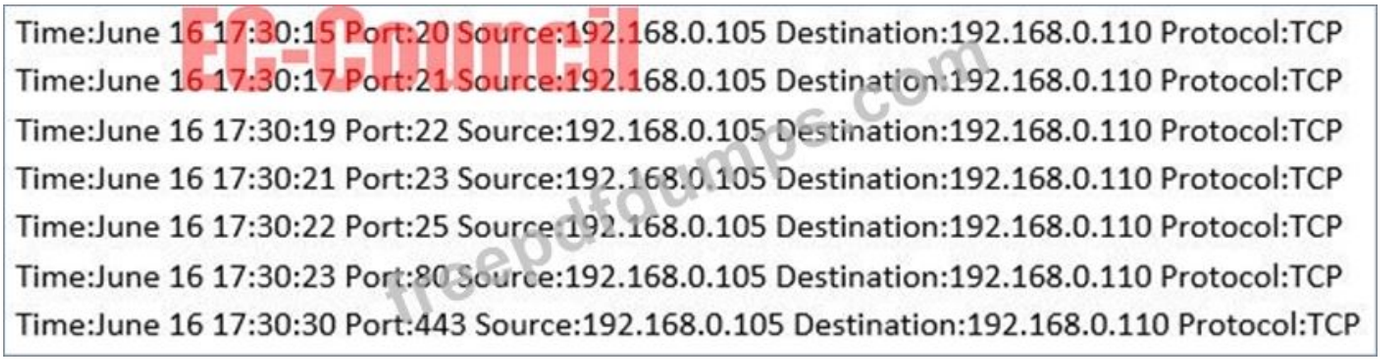
A. Test automation is not usable in security due to the complexity of the tests.

B. It can accelerate benchmark tests and repeat them with a consistent test setup. But it cannot replace manual testing completely.
C. It is an option but it tends to be very expensive.
D. It should be used exclusively. Manual testing is outdated because of low spend and possible test setup inconsistencies.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 144
If executives are found liable for not properly protecting their company's assets and information systems,
what type of law would apply in this situation?
A. Criminal
B. International
C. Civil
D. Common
Answer: C (LEAVE A REPLY)

NEW QUESTION: 145
Null sessions are un-authenticated connections (not using a username or password.) to an NT or 2000 system. Which TCP and UDP ports must you filter to check null sessions on your network?
A. 139 and 443
B. 139 and 445
C. 137 and 139
D. 137 and 443
Answer: B (LEAVE A REPLY)

NEW QUESTION: 146
The following is part of a log file taken from the machine on the network with the IP address of 192.168.0.110:



What type of activity has been logged?
A. Port scan targeting 192.168.0.110
B. Teardrop attack targeting 192.168.0.110
C. Denial of service attack targeting 192.168.0.105

D. Port scan targeting 192.168.0.105
Answer: A (LEAVE A REPLY)

NEW QUESTION: 147
When setting up a wireless network, an administrator enters a pre-shared key for security. Which of the following is true?
A. The key entered is a hash that is used to prove the integrity of the wireless data.
B. The key entered is based on the Diffie-Hellman method.
C. The key entered is a symmetric key used to encrypt the wireless data.
D. The key is an RSA key used to encrypt the wireless data.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 148
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. LM:NT
B. LM:NTLM
C. NTLM:LM
D. NT:LM
Answer: (SHOW ANSWER)

NEW QUESTION: 149
(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. The attacker wants to avoid creating a sub-carries connection that is not normally valid.
B. These packets were crafted by a tool, they were not created by a standard IP stack.
C. This is back orifice activity as the scan comes from port 31337.
D. This is not a spoofed packet as the IP stack has increasing numbers for the three flags.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 150
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. Piggybacking
B. Masqurading
C. Phishing
D. Whaling
Answer: A (LEAVE A REPLY)
Explanation
In security, piggybacking refers to when a person tags along with another person who is authorized to gain entry into a restricted area, or pass a certain checkpoint.
References: https://en.wikipedia.org/wiki/Piggybacking_(security)

NEW QUESTION: 151
A regional bank hires your company to perform a security assessment on their network after a recent data breach. The attacker was able to steal financial data from the bank by compromising only a single server.
Based on this information, what should be one of your key recommendations to the bank?
A. Issue new certificates to the web servers from the root certificate authority
B. Move the financial data to another server on the same IP subnet
C. Require all employees to change their passwords immediately
D. Place a front-end web server in a demilitarized zone that only handles external web traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 152
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. DynDNS
C. Split DNS
D. DNSSEC
Answer: C (LEAVE A REPLY)

NEW QUESTION: 153
Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?
A. Dipole antenna
B. Omnidirectional antenna
C. Parabolic grid antenna
D. Yagi antenna
Answer: D (LEAVE A REPLY)

NEW QUESTION: 154
You are analyzing a traffic on the network with Wireshark. You want to routinely run a cron job which will run the capture against a specific set of IPs. - 192.168.8.0/24. What command you would use?
A. wireshark -fetch "192.168.8/*"
B. wireshark -capture -local -masked 192.168.8.0 -range 24
C. sudo tshark -f "net 192.168.8.0/24"
D. tshark -net 192.255.255.255 mask 192.168.8.0
Answer: (SHOW ANSWER)

NEW QUESTION: 155
To reach a bank web site, the traffic from workstations must pass through a firewall. You have been asked to review the firewall configuration to ensure that workstations in network 10.10.10.0/24 can only reach the bank web site 10.20.20.1 using https. Which of the following firewall rules meets this requirement?
A. If (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit

B. If (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 80 or 443) then permit
C. If (source matches 10.20.20.1 and destination matches 10.10.10.0/24 and port matches 443) then permit
D. If (source matches 10.10.10.0 and destination matches 10.20.20.1 and port matches 443) then permit
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 156
_____ 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. Resource transfer
C. DNSSEC
D. Resource records
Answer: (SHOW ANSWER)

NEW QUESTION: 157
The following is an entry captured by a network IDS. You are assigned the task of analyzing this entry. You notice the value 0x90, which is the most common NOOP instruction for the Intel processor. You figure that the attacker is attempting a buffer overflow attack.
You also notice "/bin/sh" in the ASCII part of the output.
As an analyst what would you conclude about the attack?

```
45 00 01 ce 28 1e 40 00 32 06 96 92 d1 3a 18 09 86 9f 18 97 E..Î(.@.2...Ñ:......
06 38 02 03 6f 54 4f a9 01 af fe 78 50 18 7d 78 76 dd 00 00 .8..oTO©.¯þxP.}xv..
Application "Calculator" "%path:..\dtsapps\calc\dcalc.exe%" " " size 0.75in 0.25in 0.50in
0.05inxvÝ..
42 42 20 f7 ff bf 21 f7 ff bf 22 f7 ff bf 23 f7 ff bf 58 58 BB ÷ÿ¿!÷ÿ¿"÷ÿ¿#÷ÿ¿XX
58 58 58 58 58 58 58 58 58 58 58 58 58 58 25 2e 32 32 XXXXXXXXXXXXXX%.22
34 75 25 33 30 30 24 6e 25 2e 32 31 33 75 25 33 30 31 24 6e 4u%300$n%.213u%301$n
73 65 63 75 25 33 30 32 24 6e 25 2e 31 39 32 75 25 33 30 33 secu%302$n%.192u%303
24 6e 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 $n..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..................
90 90 31 db 31 c9 31 c0 b0 46 cd 80 89 e5 31 d2 b2 66 89 d0 ..1Û1É1À°FÍ..å1Ò²f.Ð
31 c9 89 cb 43 89 5d f8 43 89 5d f4 4b 89 4d fc 8d 4d f4 cd 1É.ËC.]øC.]ôK.Mü.MôÍ
80 31 c9 89 45 f4 43 66 89 5d ec 66 c7 45 ee 0f 27 89 4d f0 .1É.EôCf.]ìfÇEî.'.Mð
8d 45 ec 89 45 f8 c6 45 fc 10 89 d0 8d 4d f4 cd 80 89 d0 43 .Eì.Eø.Eü..Ð.MôÍ..ÐC
43 cd 80 89 d0 43 cd 80 89 c3 31 c9 b2 3f 89 d0 cd 80 89 d0 CÍ..ÐCÍ..Ã1É²?.ÐÍ..Ð
41 cd 80 eb 18 5e 89 75 08 31 c0 88 46 07 89 45 0c b0 0b 89 AÍ.ë.^.u.1À.F..E.°..
f3 8d 4d 08 8d 55 0c cd 80 e8 e3 ff ff ff 2f 62 69 6e 2f 73 ó.M..U.Í.èãÿÿÿ/bin/s
68 0a h.
EVENT4: [NOOP:X86] (tcp,dp=515,sp=1592)
```

A. The attacker is attempting an exploit that launches a command-line shell

B. The attacker is attempting a buffer overflow attack and has succeeded
C. The attacker is creating a directory on the compromised machine
D. The buffer overflow attack has been neutralized by the IDS
Answer: A (LEAVE A REPLY)

NEW QUESTION: 158
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 S100 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 attempt to click, so victim thinks that he/she clicks to the 'Do you want to make $1000 in a day?' url but actually he/sne clicks to the content or url 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. HTML Injection
D. HTTP Parameter Pollution
Answer: B (LEAVE A REPLY)

NEW QUESTION: 159
An attacker is trying to redirect the traffic of a small office. That office is using their own mail server, DNS
server and NTP server because of the importance of their job. The attacker gain access to the DNS server
and redirect the direction www.google.com to his own IP address. Now when the employees of the office
wants to go to Google they are being redirected to the attacker machine. What is the name of this kind of
attack?
A. DNS spoofing
B. Smurf Attack
C. ARP Polsoning
D. MAC Flooding
Answer: A (LEAVE A REPLY)

NEW QUESTION: 160
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. An Intrusion Detection System

B. A firewall IPTable
C. A Router IPTable
D. FTP Server rule
Answer: (SHOW ANSWER)
Snort is an open source network intrusion detection system (NIDS) for networks .
Snort rule example:
This example is a rule with a generator id of 1000001.
alert tcp any any -> any 80 (content:"BOB"; gid:1000001; sid:1; rev:1;) References: http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node31.html

NEW QUESTION: 161
In the software security development life cycle process, threat modeling occurs in which phase?
A. Verification
B. Requirements
C. Design
D. Implementation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 162
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. There is no risk at all as the marketing services are trustworthy
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. External scripts increase the outbound company data traffic which leads greater financial losses
Answer: C (LEAVE A REPLY)

NEW QUESTION: 163
In Trojan terminology, what is a covert channel?

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

NEW QUESTION: 164
It is a widely used standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. This protocol is specifically designed for transporting event messages.
Which of the following is being described?
A. SYSLOG
B. SNMP
C. SMS
D. ICMP
Answer: A (LEAVE A REPLY)