

EC-Council

Exam Questions 312-50v11

Certified Ethical Hacker Exam (CEH v11)



NEW QUESTION 1

Which of the following allows attackers to draw a map or outline the target organization's network infrastructure to know about the actual environment that they are going to hack.

- A. Enumeration
- B. Vulnerability analysis
- C. Malware analysis
- D. Scanning networks

Answer: D

NEW QUESTION 2

Jude, a pen tester working in Keiltech Ltd., performs sophisticated security testing on his company's network infrastructure to identify security loopholes. In this process, he started to circumvent the network protection tools and firewalls used in the company. He employed a technique that can create forged TCP sessions by carrying out multiple SYN, ACK, and RST or FIN packets. Further, this process allowed Jude to execute DDoS attacks that can exhaust the network resources. What is the attack technique used by Jude for finding loopholes in the above scenario?

- A. UDP flood attack
- B. Ping-of-death attack
- C. Spoofed session flood attack
- D. Peer-to-peer attack

Answer: C

NEW QUESTION 3

What is the proper response for a NULL scan if the port is open?

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

Answer: F

NEW QUESTION 4

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 want to go to Google they are being redirected to the attacker machine. What is the name of this kind of attack?

- A. MAC Flooding
- B. Smurf Attack
- C. DNS spoofing
- D. ARP Poisoning

Answer: C

NEW QUESTION 5

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

NEW QUESTION 6

A security analyst uses Zenmap to perform an ICMP timestamp ping scan to acquire information related to the current time from the target host machine. Which of the following Zenmap options must the analyst use to perform the ICMP timestamp ping scan?

- A. -PY
- B. -PU
- C. -PP
- D. -Pn

Answer: C

NEW QUESTION 7

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. \$1320
- B. \$440
- C. \$100
- D. \$146

Answer: D

NEW QUESTION 8

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. Nikto
- B. Nmap
- C. Metasploit
- D. Armitage

Answer: B

NEW QUESTION 9

Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?

- A. Yagi antenna
- B. Dipole antenna
- C. Parabolic grid antenna
- D. Omnidirectional antenna

Answer: A

NEW QUESTION 10

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 the most business profit?

- A. Accept the risk
- B. Introduce more controls to bring risk to 0%
- C. Mitigate the risk
- D. Avoid the risk

Answer: A

NEW QUESTION 10

To invisibly maintain access to a machine, an attacker utilizes a toolkit that sits undetected in the core components of the operating system. What is this type of rootkit an example of?

- A. Hypervisor rootkit
- B. Kernel toolkit
- C. Hardware rootkit
- D. Firmware rootkit

Answer: B

Explanation:

Kernel-mode rootkits run with the best operating system privileges (Ring 0) by adding code or replacement parts of the core operating system, as well as each the kernel and associated device drivers. Most operative systems support kernel-mode device drivers, that execute with a similar privileges because the software itself. As such, several kernel-mode rootkits square measure developed as device drivers or loadable modules, like loadable kernel modules in Linux or device drivers in Microsoft Windows. This category of rootkit has unrestricted security access, however is tougher to jot down. The quality makes bugs common, and any bugs in code operative at the kernel level could seriously impact system stability, resulting in discovery of the rootkit. one amongst the primary wide familiar kernel rootkits was developed for Windows NT four.0 and discharged in Phrack magazine in 1999 by Greg Hoglund. Kernel rootkits is particularly tough to observe and take away as a result of they operate at a similar security level because the software itself, and square measure therefore able to intercept or subvert the foremost sure software operations. Any package, like antivirus package, running on the compromised system is equally vulnerable. during this scenario, no a part of the system is sure.

NEW QUESTION 13

This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.

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

What is this attack?

- A. Cross-site-scripting attack
- B. SQL Injection
- C. URL Traversal attack
- D. Buffer Overflow attack

Answer: A

NEW QUESTION 17

Daniel is a professional hacker who is attempting to perform an SQL injection attack on a target website. www.movlescope.com. During this process, he encountered an IDS that detects SQL Injection attempts based on predefined signatures. To evade any comparison statement, he attempted placing characters such as "or '1'='1'" in any basic injection statement such as "or 1=1." Identify the evasion technique used by Daniel in the above scenario.

- A. Null byte
- B. IP fragmentation
- C. Char encoding
- D. Variation

Answer: D

Explanation:

One may append the comment "--" operator along with the String for the username and whole avoid executing the password segment of the SQL query. Everything when the -- operator would be considered as comment and not dead.

To launch such an attack, the value passed for name could be 'OR '1'='1' ; --Statement = "SELECT * FROM 'CustomerDB' WHERE 'name' = ' " + userName + " ' AND 'password' = ' " + passwd + " ' ;"

Statement = "SELECT * FROM 'CustomerDB' WHERE 'name' = ' ' OR '1'='1';-- + " ' AND 'password' = ' " + passwd + " ' ;"

All the records from the customer database would be listed.

Yet, another variation of the SQL Injection Attack can be conducted in dbms systems that allow multiple SQL injection statements. Here, we will also create use of the vulnerability in some dbms whereby a user provided field isn't strongly used in or isn't checked for sort constraints.

This could take place once a numeric field is to be employed in a SQL statement; but, the programmer makes no checks to validate that the user supplied input is numeric.

Variation is an evasion technique whereby the attacker can easily evade any comparison statement. The attacker does this by placing characters such as "" or '1'='1'" in any basic injection statement such as "or 1=1" or with other accepted SQL comments.

Evasion Technique: Variation Variation is an evasion technique whereby the attacker can easily evade any comparison statement. The attacker does this by placing characters such as "" or '1'='1'" in any basic injection statement such as "or 1=1" or with other accepted SQL comments. The SQL interprets this as a comparison between two strings or characters instead of two numeric values. As the evaluation of two strings yields a true statement, similarly, the evaluation of two numeric values yields a true statement, thus rendering the evaluation of the complete query unaffected. It is also possible to write many other signatures; thus, there are infinite possibilities of variation as well. The main aim of the attacker is to have a WHERE statement that is always evaluated as "true" so that any mathematical or string comparison can be used, where the SQL can perform the same.

NEW QUESTION 20

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 sniffing attack
- B. A spoofing attack
- C. A man in the middle attack
- D. A denial of service attack

Answer: C

NEW QUESTION 21

Gerard, a disgruntled ex-employee of Sunglass IT Solutions, targets this organization to perform sophisticated attacks and bring down its reputation in the market. To launch the attacks process, he performed DNS footprinting to gather information about DNS servers and to identify the hosts connected in the target network. He used an automated tool that can retrieve information about DNS zone data including DNS domain names, computer names, IP addresses, DNS records, and network Whois records. He further exploited this information to launch other sophisticated attacks. What is the tool employed by Gerard in the above scenario?

- A. Knative
- B. zANTI
- C. Towelroot
- D. Bluto

Answer: D

Explanation:

<https://www.darknet.org.uk/2017/07/bluto-dns-recon-zone-transfer-brute-forcer/>

"Attackers also use DNS lookup tools such as DNSdumpster.com, Bluto, and Domain Dossier to retrieve DNS records for a specified domain or hostname. These tools retrieve information such as domains and IP addresses, domain Whois records, DNS records, and network Whois records." CEH Module 02 Page 138

NEW QUESTION 22

Email is transmitted across the Internet using the Simple Mail Transport Protocol. SMTP does not encrypt email, leaving the information in the message vulnerable to being read by an unauthorized person. SMTP can upgrade a connection between two mail servers to use TLS. Email transmitted by SMTP over TLS is encrypted. What is the name of the command used by SMTP to transmit email over TLS?

- A. OPPORTUNISTICTLS
- B. UPGRADETLS
- C. FORCETLS
- D. STARTTLS

Answer: D

NEW QUESTION 24

Morris, a professional hacker, performed a vulnerability scan on a target organization by sniffing the traffic on the network to identify the active systems, network services, applications, and vulnerabilities. He also obtained the list of the users who are currently accessing the network. What is the type of vulnerability assessment that Morris performed on the target organization?

- A. internal assessment

- B. Passive assessment
- C. External assessment
- D. Credentialed assessment

Answer: B

Explanation:

Passive Assessment Passive assessments sniff the traffic present on the network to identify the active systems, network services, applications, and vulnerabilities. Passive assessments also provide a list of the users who are currently accessing the network.

NEW QUESTION 29

How does a denial-of-service attack work?

- A. A hacker prevents a legitimate user (or group of users) from accessing a service
- B. A hacker uses every character, word, or letter he or she can think of to defeat authentication
- C. A hacker tries to decipher a password by using a system, which subsequently crashes the network
- D. A hacker attempts to imitate a legitimate user by confusing a computer or even another person

Answer: A

NEW QUESTION 33

Which of the following DoS tools is used to attack target web applications by starvation of available sessions on the web server? The tool keeps sessions at halt using never-ending POST transmissions and sending an arbitrarily large content-length header value.

- A. My Doom
- B. Astacheldraht
- C. R-U-Dead-Yet?(RUDY)
- D. LOIC

Answer: C

NEW QUESTION 35

Which of the following represents the initial two commands that an IRC client sends to join an IRC network?

- A. USER, NICK
- B. LOGIN, NICK
- C. USER, PASS
- D. LOGIN, USER

Answer: A

NEW QUESTION 36

The network team has well-established procedures to follow for creating new rules on the firewall. This includes having approval from a manager prior to implementing any new rules. While reviewing the firewall configuration, you notice a recently implemented rule but cannot locate manager approval for it. What would be a good step to have in the procedures for a situation like this?

- A. Have the network team document the reason why the rule was implemented without prior manager approval.
- B. Monitor all traffic using the firewall rule until a manager can approve it.
- C. Do not roll back the firewall rule as the business may be relying upon it, but try to get manager approval as soon as possible.
- D. Immediately roll back the firewall rule until a manager can approve it

Answer: D

NEW QUESTION 41

While performing an Nmap scan against a host, Paola determines the existence of a firewall. In an attempt to determine whether the firewall is stateful or stateless, which of the following options would be best to use?

- A. -sA
- B. -sX
- C. -sT
- D. -sF

Answer: A

NEW QUESTION 44

Bobby, an attacker, targeted a user and decided to hijack and intercept all their wireless communications. He installed a fake communication tower between two authentic endpoints to mislead the victim. Bobby used this virtual tower to interrupt the data transmission between the user and real tower, attempting to hijack an active session, upon receiving the users request. Bobby manipulated the traffic with the virtual tower and redirected the victim to a malicious website. What is the attack performed by Bobby in the above scenario?

- A. Wardriving
- B. KRACK attack
- C. jamming signal attack
- D. aLTER attack

Answer: D

Explanation:

aLTER attacks are usually performed on LTE devices. Attacker installs a virtual (fake) communication tower between two authentic endpoints intending to mislead the victim. This virtual tower is used to interrupt the data transmission between the user and real tower attempting to hijack the active session.

NEW QUESTION 46

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. Service Level Agreement
- B. Project Scope
- C. Rules of Engagement
- D. Non-Disclosure Agreement

Answer: C

NEW QUESTION 48

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. Bluesmacking
- B. BlueSniffing
- C. Bluejacking
- D. Bluesnarfing

Answer: C

NEW QUESTION 49

The network users are complaining because their systems are slowing down. Further, every time they attempt to go to a website, they receive a series of pop-ups with advertisements. What types of malware have the system been infected with?

- A. Virus
- B. Spyware
- C. Trojan
- D. Adware

Answer: D

Explanation:

Adware, or advertising supported computer code, is computer code that displays unwanted advertisements on your PC. Adware programs can tend to serve you pop-up ads, will modify your browser's homepage, add spyware and simply bombard your device with advertisements. Adware may be an additional summary name for doubtless unwanted programs. It's roughly a virulent disease and it's going to not be as clearly malicious as a great deal of different problematic code floating around on the net. Create no mistake concerning it, though, that adware has to return off of no matter machine it's on. Not solely will adware be extremely annoying whenever you utilize your machine, it might additionally cause semipermanent problems for your device.

Adware a network user the browser to gather your internet browsing history so as to 'target' advertisements that appear tailored to your interests. At their most innocuous, adware infections square measure simply annoying. As an example, adware barrages you with pop-up ads that may create your net expertise markedly slower and additional labor intensive.

NEW QUESTION 53

Which of the following tools are used for enumeration? (Choose three.)

- A. SolarWinds
- B. USER2SID
- C. Cheops
- D. SID2USER
- E. DumpSec

Answer: BDE

NEW QUESTION 57

What is the minimum number of network connections in a multihomed firewall?

- A. 3
- B. 5
- C. 4
- D. 2

Answer: A

NEW QUESTION 60

You are the Network Admin, and you get a complaint 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 UDP Port 53
- B. Traffic is Blocked on TCP Port 80
- C. Traffic is Blocked on TCP Port 54
- D. Traffic is Blocked on UDP Port 80

Answer: A

NEW QUESTION 63

Heather's company has decided to use a new customer relationship management tool. After performing the appropriate research, they decided to purchase a subscription to a cloud-hosted solution. The only administrative task that Heather will need to perform is the management of user accounts. The provider will take care of the hardware, operating system, and software administration including patching and monitoring. Which of the following is this type of solution?

- A. SaaS
- B. IaaS
- C. CaaS
- D. PaaS

Answer: A

Explanation:

Software as a service (SaaS) allows users to attach to and use cloud-based apps over the web. Common examples are email, calendaring and workplace tool (such as Microsoft Workplace 365).

SaaS provides a whole software solution that you get on a pay-as-you-go basis from a cloud service provider. You rent the use of an app for your organisation and your users connect with it over the web, typically with an internet browser. All of the underlying infrastructure, middleware, app software system and app knowledge are located within the service provider's knowledge center. The service provider manages the hardware and software system and with the appropriate service agreement, can make sure the availability and also the security of the app and your data as well. SaaS allows your organisation to induce quickly up and running with an app at token upfront cost.

Common SaaS scenarios This tool having used a web-based email service like Outlook, Hotmail or Yahoo! Mail, then you have got already used a form of SaaS. With these services, you log into your account over the web, typically from an internet browser. The e-mail software system is found on the service provider's network and your messages are held on there moreover. You can access your email and hold on messages from an internet browser on any laptop or Internet-connected device.

The previous examples are free services for personal use. For organisational use, you can rent productivity apps, like email, collaboration and calendaring; and sophisticated business applications like client relationship management (CRM), enterprise resource planning (ERP) and document management. You buy the use of those apps by subscription or per the level of use.

Advantages of SaaS Gain access to stylish applications. To supply SaaS apps to users, you don't need to purchase, install, update or maintain any hardware, middleware or software system. SaaS makes even sophisticated enterprise applications, like ERP and CRM, affordable for organisations that lack the resources to shop for, deploy and manage the specified infrastructure and software system themselves.

Pay just for what you utilize. You furthermore may economize because the SaaS service automatically scales up and down per the level of usage.

Use free shopper software system. Users will run most SaaS apps directly from their web browser without needing to transfer and install any software system, though some apps need plugins. This suggests that you simply don't need to purchase and install special software system for your users.

Mobilise your hands simply. SaaS makes it simple to "mobilise" your hands as a result of users will access SaaS apps and knowledge from any Internet-connected laptop or mobile device. You don't need to worry concerning developing apps to run on differing types of computers and devices as a result of the service supplier has already done therefore. Additionally, you don't need to bring special experience aboard to manage the safety problems inherent in mobile computing. A fastidiously chosen service supplier can make sure the security of your knowledge, no matter the sort of device intense it.

Access app knowledge from anyplace. With knowledge held on within the cloud, users will access their info from any Internet-connected laptop or mobile device. And once app knowledge is held on within the cloud, no knowledge is lost if a user's laptop or device fails.

NEW QUESTION 66

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. Although the approach has two phases, it actually implements just one authentication factor
- B. The solution implements the two authentication factors: physical object and physical characteristic
- C. The solution will have a high level of false positives
- D. Biological motion cannot be used to identify people

Answer: B

NEW QUESTION 71

What is the first step for a hacker conducting a DNS cache poisoning (DNS spoofing) attack against an organization?

- A. The attacker queries a nameserver using the DNS resolver.
- B. The attacker makes a request to the DNS resolver.
- C. The attacker forges a reply from the DNS resolver.
- D. The attacker uses TCP to poison the DNS resolver.

Answer: A

NEW QUESTION 74

Attacker Lauren has gained the credentials of an organization's internal server system, and she was often logging in during irregular times to monitor the network activities. The organization was skeptical about the login times and appointed security professional Robert to determine the issue. Robert analyzed the compromised device to find incident details such as the type of attack, its severity, target, impact, method of propagation, and vulnerabilities exploited. What is the incident handling and response (IH&R) phase, in which Robert has determined these issues?

- A. Preparation
- B. Eradication
- C. Incident recording and assignment
- D. Incident triage

Answer: D

Explanation:

Triage is that the initial post-detection incident response method any responder can execute to open an event or false positive. Structuring an efficient and correct triage method can reduce analyst fatigue, reduce time to reply to and right incidents, and ensure that solely valid alerts are promoted to "investigation or incident" status.

Every part of the triage method should be performed with urgency, as each second counts once in the inside of a crisis. However, triage responders face the intense challenge of filtering an unwieldy input supply into a condensed trickle of events. Here are some suggestions for expediting analysis before knowledge is validated:

- Organization: reduce redundant analysis by developing a workflow that may assign tasks to responders. Avoid sharing an email box or email alias between multiple responders. Instead use a workflow tool, like those in security orchestration, automation, and response (SOAR) solutions, to assign tasks. Implement a method to re-assign or reject tasks that are out of scope for triage.
 - Correlation: Use a tool like a security info and event management (SIEM) to mix similar events. Link potentially connected events into one useful event.
 - Data Enrichment: automate common queries your responders perform daily, like reverse DNS lookups, threat intelligence lookups, and IP/domain mapping. Add this knowledge to the event record or make it simply accessible.
- Moving full speed ahead is that the thanks to get through the initial sorting method however a a lot of detailed, measured approach is necessary throughout event verification. Presenting a robust case to be accurately evaluated by your security operations center (SOC) or cyber incident response team (CIRT) analysts is key. Here are many tips for the verification:
- Adjacent Data: Check the data adjacent to the event. for example, if an end has a virus signature hit, look to visualize if there's proof the virus is running before career for more response metrics.
 - Intelligence Review: understand the context around the intelligence. simply because an ip address was flagged as a part of a botnet last week doesn't mean it still is an element of a botnet today.
 - Initial Priority: Align with operational incident priorities and classify incidents appropriately. ensure the right level of effort is applied to every incident.
 - Cross Analysis: look for and analyze potentially shared keys, like science addresses or domain names, across multiple knowledge sources for higher knowledge acurity.

NEW QUESTION 76

Shiela is an information security analyst working at HiTech Security Solutions. She is performing service version discovery using Nmap to obtain information about the running services and their versions on a target system.

Which of the following Nmap options must she use to perform service version discovery on the target host?

- A. -SN
- B. -SX
- C. -sV
- D. -SF

Answer: C

NEW QUESTION 81

Which of the following is the primary objective of a rootkit?

- A. It opens a port to provide an unauthorized service
- B. It creates a buffer overflow
- C. It replaces legitimate programs
- D. It provides an undocumented opening in a program

Answer: C

NEW QUESTION 86

Ron, a security professional, was pen testing web applications and SaaS platforms used by his company. While testing, he found a vulnerability that allows hackers to gain unauthorized access to API objects and perform actions such as view, update, and delete sensitive data of the company. What is the API vulnerability revealed in the above scenario?

- A. Code injections
- B. Improper use of CORS
- C. No ABAC validation
- D. Business logic flaws

Answer: B

NEW QUESTION 89

Sam is a penetration tester hired by Inception Tech, a security organization. He was asked to perform port scanning on a target host in the network. While performing the given task, Sam sends FIN/ACK probes and determines that an RST packet is sent in response by the target host, indicating that the port is closed. What is the port scanning technique used by Sam to discover open ports?

- A. Xmas scan
- B. IDLE/IPID header scan
- C. TCP Maimon scan
- D. ACK flag probe scan

Answer: C

Explanation:

TCP Maimon scan

This scan technique is very similar to NULL, FIN, and Xmas scan, but the probe used here is

FIN/ACK. In most cases, to determine if the port is open or closed, the RST packet should be generated as a response to a probe request. However, in many BSD systems, the port is open if the packet gets dropped in response to a probe.

<https://nmap.org/book/scan-methods-maimon-scan.html> How Nmap interprets responses to a Maimon scan probe Probe Response Assigned State

No response received (even after retransmissions) open|filtered TCP RST packet closed
 ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13) filtered

NEW QUESTION 94

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, Bab 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. Non-Repudiation
- B. Integrity
- C. Authentication
- D. Confidentiality

Answer: A

NEW QUESTION 97

Mirai malware targets IoT devices. After infiltration, it uses them to propagate and create botnets that then used to launch which types of attack?

- A. MITM attack
- B. Birthday attack
- C. DDoS attack
- D. Password attack

Answer: C

NEW QUESTION 100

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. Nessus
- C. OpenVAS
- D. tcptraceroute

Answer: A

NEW QUESTION 103

Study the following log extract and identify the attack.

```
12/26-07:06:22:31.167035 207.219.207.240:1882 -> 172.16.1.106:80
TCP TTL:13 TTL:50 TOS:0x0 IP:53476 DFF
***AP*** Seq: 0x2BDC107 Ack: 0x1CB9F186 Win: 0x2238 TcpLen: 20
47 45 54 20 2F 6D 73 61 64 63 2F 2E 2E C0 AF 2E GET /msadc/.....
2E 2F 2E 2E C0 AF 2E 2E 2F 2E 2E C0 AF 2E 2E 2F ./...../...../
77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 63 winnt/system32/c
6D 64 2E 65 78 65 3F 2F 63 2B 64 69 72 2B 63 3A md.exe?/c+dir+c:
5C 20 48 54 54 50 2F 31 2E 31 0D 0A 41 63 63 65 \ HTTP/1.1..Acce
70 74 3A 20 69 6D 61 67 65 2F 67 69 66 2C 20 69 pt: image/gif, i
6D 61 67 65 2F 78 2D 78 62 69 74 6D 61 70 2C 20 mage/x-xbitmap
69 6D 61 67 65 2F 6A 70 65 67 2C 20 69 6D 61 67 image/jpeg, imag
65 2F 70 6A 70 65 67 2C 20 61 70 70 6C 69 63 61 e/jpeg, applica
74 69 6F 6E 2F 76 6E 64 2E 6D 73 2D 65 78 63 65 tion/vnd.ms-exce
6C 2C 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 6D l, application/m
73 77 6F 72 64 2C 20 61 70 70 6C 69 63 61 74 69 sword, applicati
6F 6E 2F 76 6E 64 2E 6D 73 2D 70 6F 77 65 72 70 on/vnd.ms-powerp
6F 69 6E 74 2C 20 2A 2F 2A 0D 0A 41 63 63 65 70 oint, =/?.Accep
74 2D 4C 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70ozilla/age: en-u
73 0D 0A 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30 atible;pt-EncodD
6E 67 3A 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A l; Windo, deflat
65 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D e..User-Agent: M
6F 7A 69 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70ozilla/4.0 (comp
61 74 69 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30 atible; MSIE 5.0
31 3B 20 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A l; Windows 95)..
48 6F 73 74 3A 20 6C 61 62 2E 77 69 72 65 74 72 Host: lib.bvxttr
69 70 2E 6E 65 74 0D 0A 43 6F 6E 6E 65 63 74 69 ip.org..Connecti
6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A on: Keep-Alive..
43 6F 6F 6B 69 65 3A 20 41 53 50 53 45 53 53 49 Cookie: ASPSESSI
4F 4E 49 44 47 51 51 51 51 51 5A 55 3D 4B 4E 4F ONIDGQQQQZU=KNO
48 4D 4F 4A 41 4B 50 46 4F 50 48 4D 4C 41 50 4E HMOJAKPFOPHMLAPN
49 46 49 46 42 0D 0A 0D 0A 41 50 4E 49 46 49 46 IFIFB....APNIFIF
42 0D 0A 0D 0A B....
```

- A. Hexcode Attack

- B. Cross Site Scripting
- C. Multiple Domain Traversal Attack
- D. Unicode Directory Traversal Attack

Answer: D

NEW QUESTION 105

Which command can be used to show the current TCP/IP connections?

- A. Netsh
- B. Netstat
- C. Net use connection
- D. Net use

Answer: A

NEW QUESTION 106

Which of the following tactics uses malicious code to redirect users' web traffic?

- A. Spimming
- B. Pharming
- C. Phishing
- D. Spear-phishing

Answer: B

NEW QUESTION 108

infesting a system with malware and using phishing to gain credentials to a system or web application are examples of which phase of the ethical hacking methodology?

- A. Reconnaissance
- B. Maintaining access
- C. Scanning
- D. Gaining access

Answer: D

Explanation:

This phase having the hacker uses different techniques and tools to realize maximum data from the system. they're → Password cracking – Methods like Bruteforce, dictionary attack, rule-based attack, rainbow table a used. Bruteforce is trying all combinations of the password. Dictionary attack is trying an inventory of meaningful words until the password matches. Rainbow table takes the hash value of the password and compares with pre-computed hash values until a match is discovered. • Password attacks – Passive attacks like wire sniffing, replay attack. Active online attack like Trojans, keyloggers, hash injection, phishing. Offline attacks like pre-computed hash, distributed network and rainbow. Non electronic attack like shoulder surfing, social engineering and dumpster diving.

NEW QUESTION 109

Which file is a rich target to discover the structure of a website during web-server footprinting?

- A. Document root
- B. Robots.txt
- C. domain.txt
- D. index.html

Answer: B

NEW QUESTION 110

Your company performs penetration tests and security assessments for small and medium-sized business in the local area. During a routine security assessment, you discover information that suggests your client is involved with human trafficking.

What should you do?

- A. Confront the client in a respectful manner and ask her about the data.
- B. Copy the data to removable media and keep it in case you need it.
- C. Ignore the data and continue the assessment until completed as agreed.
- D. Immediately stop work and contact the proper legal authorities.

Answer: D

NEW QUESTION 114

which of the following protocols can be used to secure an LDAP service against anonymous queries?

- A. SSO
- B. RADIUS
- C. WPA
- D. NTLM

Answer: D

Explanation:

In a Windows network, nongovernmental organization (New Technology) local area network Manager (NTLM) could be a suite of Microsoft security protocols supposed to produce authentication, integrity, and confidentiality to users. NTLM is that the successor to the authentication protocol in Microsoft local area network Manager (LANMAN), Associate in Nursing older Microsoft product. The NTLM protocol suite is enforced in an exceedingly Security Support supplier, which mixes the local area network Manager authentication protocol, NTLMv1, NTLMv2 and NTLM2 Session protocols in an exceedingly single package. whether or not these protocols area unit used or will be used on a system is ruled by cluster Policy settings, that totally different|completely different} versions of Windows have different default settings. NTLM passwords area unit thought-about weak as a result of they will be brute-forced very simply with fashionable hardware. NTLM could be a challenge-response authentication protocol that uses 3 messages to authenticate a consumer in an exceedingly affiliation orientating setting (connectionless is similar), and a fourth extra message if integrity is desired.

- > First, the consumer establishes a network path to the server and sends a NEGOTIATE_MESSAGE advertising its capabilities.
- > Next, the server responds with CHALLENGE_MESSAGE that is employed to determine the identity of the consumer.
- > Finally, the consumer responds to the challenge with Associate in Nursing AUTHENTICATE_MESSAGE.

The NTLM protocol uses one or each of 2 hashed word values, each of that are keep on the server (or domain controller), and that through a scarcity of seasoning area unit word equivalent, that means that if you grab the hash price from the server, you'll evidence while not knowing the particular word. the 2 area unit the lm Hash (a DES-based operate applied to the primary fourteen chars of the word born-again to the standard eight bit laptop charset for the language), and also the nt Hash (MD4 of the insufficient endian UTF-16 Unicode password). each hash values area unit sixteen bytes (128 bits) every.

The NTLM protocol additionally uses one among 2 a method functions, looking on the NTLM version. National Trust LanMan and NTLM version one use the DES primarily based LanMan a method operate (LMOWF), whereas National TrustLMv2 uses the NT MD4 primarily based a method operate (NTOWF).

NEW QUESTION 117

Which Intrusion Detection System is the best applicable for large environments where critical assets on the network need extra scrutiny and is ideal for observing sensitive network segments?

- A. Honeypots
- B. Firewalls
- C. Network-based intrusion detection system (NIDS)
- D. Host-based intrusion detection system (HIDS)

Answer: C

NEW QUESTION 121

Abel, a cloud architect, uses container technology to deploy applications/software including all its dependencies, such as libraries and configuration files, binaries, and other resources that run independently from other processes in the cloud environment. For the containerization of applications, he follows the five-tier container technology architecture. Currently, Abel is verifying and validating image contents, signing images, and sending them to the registries. Which of the following tiers of the container technology architecture is Abel currently working in?

- A. Tier-1: Developer machines
- B. Tier-4: Orchestrators
- C. Tier-3: Registries
- D. Tier-2: Testing and accreditation systems

Answer: D

Explanation:

The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

formal declaration by a designated accrediting authority (DAA) or principal accrediting authority (PAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. See authorization to operate (ATO).

Rationale: The Risk Management Framework uses a new term to refer to this concept, and it is called authorization.

Identifies the information resources covered by an accreditation decision, as distinguished from separately accredited information resources that are interconnected or with which information is exchanged via messaging. Synonymous with Security Perimeter.

For the purposes of identifying the Protection Level for confidentiality of a system to be accredited, the system has a conceptual boundary that extends to all intended users of the system, both directly and indirectly connected, who receive output from the system. See authorization boundary. Rationale: The Risk Management Framework uses a new term to refer to the concept of accreditation, and it is called authorization. Extrapolating, the accreditation boundary would then be referred to as the authorization boundary.

NEW QUESTION 126

Which DNS resource record can indicate how long any "DNS poisoning" could last?

- A. MX
- B. SOA
- C. NS
- D. TIMEOUT

Answer: B

NEW QUESTION 130

Garry is a network administrator in an organization. He uses SNMP to manage networked devices from a remote location. To manage nodes in the network, he uses MIB. which contains formal descriptions of all network objects managed by SNMP. He accesses the contents of MIB by using a web browser either by entering the IP address and Lseries.mlb or by entering the DNS library name and Lseries.mlb. He is currently retrieving information from an MIB that contains object types for workstations and server services. Which of the following types of MIB is accessed by Garry in the above scenario?

- A. LNMIB2.MIB
- B. WINS.MIB
- C. DHCP.MIS
- D. MIB_II.MIB

Answer: A

Explanation:

DHCP.MIB: Monitors network traffic between DHCP servers and remote hosts
HOSTMIB.MIB: Monitors and manages host resources
LNMIB2.MIB: Contains object types for workstation and server services
MIBJI.MIB: Manages TCP/IP-based Internet using a simple architecture and system
WINS.MIB: For the Windows Internet Name Service (WINS)

NEW QUESTION 133

Which of the following program infects the system boot sector and the executable files at the same time?

- A. Polymorphic virus
- B. Stealth virus
- C. Multipartite Virus
- D. Macro virus

Answer: C

NEW QUESTION 138

You are using a public Wi-Fi network inside a coffee shop. Before surfing the web, you use your VPN to prevent intruders from sniffing your traffic. If you did not have a VPN, how would you identify whether someone is performing an ARP spoofing attack on your laptop?

- A. You should check your ARP table and see if there is one IP address with two different MAC addresses.
- B. You should scan the network using Nmap to check the MAC addresses of all the hosts and look for duplicates.
- C. You should use netstat to check for any suspicious connections with another IP address within the LAN.
- D. You cannot identify such an attack and must use a VPN to protect your traffic, r

Answer: A

NEW QUESTION 143

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 security agents in clients' computers
- B. The use of DNSSEC
- C. The use of double-factor authentication
- D. Client awareness

Answer: B

NEW QUESTION 146

Under what conditions does a secondary name server request a zone transfer from a primary name server?

- A. When a primary SOA is higher than a secondary SOA
- B. When a secondary SOA is higher than a primary SOA
- C. When a primary name server has had its service restarted
- D. When a secondary name server has had its service restarted
- E. When the TTL falls to zero

Answer: A

NEW QUESTION 147

A group of hackers were roaming around a bank office building in a city, driving a luxury car. They were using hacking tools on their laptop with the intention to find a free-access wireless network. What is this hacking process known as?

- A. GPS mapping
- B. Spectrum analysis
- C. Wardriving
- D. Wireless sniffing

Answer: C

NEW QUESTION 151

A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer's software and hardware without the owner's permission. Their intention can either be to simply gain knowledge or to illegally make changes.

Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?

- A. White Hat
- B. Suicide Hacker
- C. Gray Hat
- D. Black Hat

Answer: C

NEW QUESTION 153

Bob is acknowledged as a hacker of repute and is popular among visitors of "underground" sites.

Bob is willing to share his knowledge with those who are willing to learn, and many have expressed their interest in learning from him. However, this knowledge has a risk associated with it, as it can be used for malevolent attacks as well.

In this context, what would be the most effective method to bridge the knowledge gap between the "black" hats or crackers and the "white" hats or computer security professionals? (Choose the test answer.)

- A. Educate everyone with books, articles and training on risk analysis, vulnerabilities and safeguards.
- B. Hire more computer security monitoring personnel to monitor computer systems and networks.
- C. Make obtaining either a computer security certification or accreditation easier to achieve so more individuals feel that they are a part of something larger than life.
- D. Train more National Guard and reservist in the art of computer security to help out in times of emergency or crises.

Answer: A

NEW QUESTION 155

Identify the correct terminology that defines the above statement.

"Testing the network using the same methodologies and tools employed by attackers"

- A. Vulnerability Scanning
- B. Penetration Testing
- C. Security Policy Implementation
- D. Designing Network Security

Answer: B

NEW QUESTION 157

Sam, a professional hacker, targeted an organization with intention of compromising AWS IAM credentials. He attempted to lure one of the employees of the organization by initiating fake calls while posing as a legitimate employee. Moreover, he sent phishing emails to steal the AWS IAM credentials and further compromise the employee's account. What is the technique used by Sam to compromise the AWS IAM credentials?

- A. Social engineering
- B. insider threat
- C. Password reuse
- D. Reverse engineering

Answer: A

Explanation:

Just like any other service that accepts usernames and passwords for logging in, AWS users are vulnerable to social engineering attacks from attackers. fake emails, calls, or any other method of social engineering, may find yourself with an AWS users' credentials within the hands of an attacker.

If a user only uses API keys for accessing AWS, general phishing techniques could still use to gain access to other accounts or their pc itself, where the attacker may then pull the API keys for aforementioned AWS user.

With basic opensource intelligence (OSINT), it's usually simple to collect a list of workers of an organization that use AWS on a regular basis. This list will then be targeted with spear phishing to do and gather credentials. an easy technique may include an email that says your bill has spiked 500th within the past 24 hours, "click here for additional information", and when they click the link, they're forwarded to a malicious copy of the AWS login page designed to steal their credentials.

An example of such an email will be seen within the screenshot below. it's exactly like an email that AWS would send to you if you were to exceed the free tier limits, except for a few little changes. If you clicked on any of the highlighted regions within the screenshot, you'd not be taken to the official AWS web site and you'd instead be forwarded to a pretend login page setup to steal your credentials.

These emails will get even more specific by playing a touch bit additional OSINT before causing them out. If an attacker was ready to discover your AWS account ID on-line somewhere, they could use methods we at rhino have free previously to enumerate what users and roles exist in your account with none logs contact on your side. they could use this list to more refine their target list, further as their emails to reference services they will know that you often use.

For reference, the journal post for using AWS account IDs for role enumeration will be found here and the journal post for using AWS account IDs for user enumeration will be found here.

During engagements at rhino, we find that phishing is one in all the fastest ways for us to achieve access to an AWS environment.

NEW QUESTION 158

When purchasing a biometric system, one of the considerations that should be reviewed is the processing speed. Which of the following best describes what it is meant by processing?

- A. The amount of time and resources that are necessary to maintain a biometric system
- B. How long it takes to setup individual user accounts
- C. The amount of time it takes to be either accepted or rejected from when an individual provides identification and authentication information
- D. The amount of time it takes to convert biometric data into a template on a smart card

Answer: C

NEW QUESTION 159

Jason, an attacker, targeted an organization to perform an attack on its Internet-facing web server with the intention of gaining access to backend servers, which are protected by a firewall. In this process, he used a URL <https://xyz.com/feed.php?url:externalsile.com/feed/to> to obtain a remote feed and altered the URL input to the local host to view all the local resources on the target server. What is the type of attack Jason performed in the above scenario?

- A. website defacement
- B. Server-side request forgery (SSRF) attack
- C. Web server misconfiguration
- D. web cache poisoning attack

Answer: B

Explanation:

Server-side request forgery (also called SSRF) is a net security vulnerability that allows an assaulter to induce the server-side application to make http requests to associate arbitrary domain of the attacker's choosing.

In typical SSRF examples, the attacker might cause the server to make a connection back to itself, or to other web-based services among the organization's infrastructure, or to external third-party systems.

Another type of trust relationship that often arises with server-side request forgery is where the application server is able to interact with different back-end systems that aren't directly reachable by users. These systems typically have non-routable private informatics addresses. Since the back-end systems normally ordinarily protected by the topology, they typically have a weaker security posture. In several cases, internal back-end systems contain sensitive functionality that may be accessed while not authentication by anyone who is able to act with the systems.

In the preceding example, suppose there's an body interface at the back-end url <https://192.168.0.68/admin>. Here, an attacker will exploit the SSRF vulnerability to access the executive interface by submitting the following request:

```
POST /product/stock HTTP/1.0
```

```
Content-Type: application/x-www-form-urlencoded Content-Length: 118 stockApi=http://192.168.0.68/admin
```

NEW QUESTION 162

Calvin, a grey-hat hacker, targets a web application that has design flaws in its authentication mechanism. He enumerates usernames from the login form of the web application, which requests users to feed data and specifies the incorrect field in case of invalid credentials. Later, Calvin uses this information to perform social engineering.

Which of the following design flaws in the authentication mechanism is exploited by Calvin?

- A. Insecure transmission of credentials
- B. Verbose failure messages
- C. User impersonation
- D. Password reset mechanism

Answer: D

NEW QUESTION 167

John is an incident handler at a financial institution. His steps in a recent incident are not up to the standards of the company. John frequently forgets some steps and procedures while handling responses as they are very stressful to perform. Which of the following actions should John take to overcome this problem with the least administrative effort?

- A. Create an incident checklist.
- B. Select someone else to check the procedures.
- C. Increase his technical skills.
- D. Read the incident manual every time it occurs.

Answer: C

NEW QUESTION 170

Sam is working as a system administrator in an organization. He captured the principal characteristics of a vulnerability and produced a numerical score to reflect its severity using CVSS v3.0 to properly assess and prioritize the organization's vulnerability management processes. The base score that Sam obtained after performing cvss rating was 4.0. What is the CVSS severity level of the vulnerability discovered by Sam in the above scenario?

- A. Medium
- B. Low
- C. Critical
- D. High

Answer: A

Explanation:

Rating CVSS Score None 0.0

Low 0.1 - 3.9

Medium 4.0 - 6.9

High 7.0 - 8.9

Critical 9.0 - 10.0

NEW QUESTION 172

_____ is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

- A. Trojan
- B. RootKit
- C. DoS tool
- D. Scanner
- E. Backdoor

Answer: B

NEW QUESTION 173

Which of the following statements is TRUE?

- A. Packet Sniffers operate on the Layer 1 of the OSI model.
- B. Packet Sniffers operate on Layer 2 of the OSI model.
- C. Packet Sniffers operate on both Layer 2 & Layer 3 of the OSI model.
- D. Packet Sniffers operate on Layer 3 of the OSI model.

Answer: B

NEW QUESTION 177

There are multiple cloud deployment options depending on how isolated a customer's resources are from those of other customers. Shared environments share the costs and allow each customer to enjoy lower operations expenses. One solution is for a customer to join with a group of users or organizations to share a cloud environment. What is this cloud deployment option called?

- A. Hybrid
- B. Community
- C. Public
- D. Private

Answer: B

Explanation:

The purpose of this idea is to permit multiple customers to figure on joint projects and applications that belong to the community, where it's necessary to possess a centralized clouds infrastructure. In other words, Community Cloud may be a distributed infrastructure that solves the precise problems with business sectors by integrating the services provided by differing types of clouds solutions.

The communities involved in these projects, like tenders, business organizations, and research companies, specialise in similar issues in their cloud interactions. Their shared interests may include concepts and policies associated with security and compliance considerations, and therefore the goals of the project also .

Community Cloud computing facilitates its users to spot and analyze their business demands better. Community Clouds could also be hosted during a data center, owned by one among the tenants, or by a third-party cloud services provider and may be either on-site or off-site.

Community Cloud Examples and Use CasesCloud providers have developed Community Cloud offerings, and a few organizations are already seeing the advantages . the subsequent list shows a number of the most scenarios of the Community Cloud model that's beneficial to the participating organizations.

➤ Multiple governmental departments that perform transactions with each other can have their processing systems on shared infrastructure. This setup makes it cost-effective to the tenants, and may also reduce their data traffic.

Benefits of Community CloudsCommunity Cloud provides benefits to organizations within the community, individually also as collectively. Organizations don't need to worry about the safety concerns linked with Public Cloud due to the closed user group.

This recent cloud computing model has great potential for businesses seeking cost-effective cloud services to collaborate on joint projects, because it comes with multiple advantages.

Openness and ImpartialityCommunity Clouds are open systems, and that they remove the dependency organizations wear cloud service providers. Organizations are able to do many benefits while avoiding the disadvantages of both public and personal clouds.

➤ Ensures compatibility among each of its users, allowing them to switch properties consistent with their individual use cases. They also enable companies to interact with their remote employees and support the utilization of various devices, be it a smartphone or a tablet. This makes this sort of cloud solution more flexible to users' demands.

➤ Consists of a community of users and, as such, is scalable in several aspects like hardware resources, services, and manpower. It takes under consideration demand growth, and you simply need to increase the user-base.

Flexibility and ScalabilityHigh Availability and ReliabilityYour cloud service must be ready to make sure the availability of knowledge and applications in the least times. Community Clouds secure your data within the same way as the other cloud service, by replicating data and applications in multiple secure locations to guard them from unforeseen circumstances.

Cloud possesses redundant infrastructure to form sure data is out there whenever and wherever you would like it. High availability and reliability are critical concerns for any sort of cloud solution.

Security and ComplianceTwo significant concerns discussed when organizations believe cloud computing are data security and compliance with relevant regulatory authorities. Compromising each other's data security isn't profitable to anyone during a Community Cloud.

➤ the power to dam users from editing and downloading specific datasets.

➤ Making sensitive data subject to strict regulations on who has access to Sharing sensitive data unique to a specific organization would bring harm to all or any the members involved.

➤ What devices can store sensitive data.

Users can configure various levels of security for his or her data. Common use cases:Convenience and ControlConflicts associated with convenience and control don't arise during a Community Cloud. Democracy may be a crucial factor the Community Cloud offers as all tenants share and own the infrastructure and make decisions collaboratively. This setup allows organizations to possess their data closer to them while avoiding the complexities of a personal Cloud.

Less Work for the IT DepartmentHaving data, applications, and systems within the cloud means you are doing not need to manage them entirely. This convenience eliminates the necessity for tenants to use extra human resources to manage the system. Even during a self-managed solution, the work is split among the participating organizations.

Environment SustainabilityIn the Community Cloud, organizations use one platform for all their needs, which dissuades them from investing in separate cloud facilities. This shift introduces a symbiotic relationship between broadening and shrinking the utilization of cloud among clients. With the reduction of organizations using different clouds, resources are used more efficiently, thus resulting in a smaller carbon footprint.

NEW QUESTION 180

Taylor, a security professional, uses a tool to monitor her company's website, analyze the website's traffic, and track the geographical location of the users visiting the company's website. Which of the following tools did Taylor employ in the above scenario?

- A. WebSite Watcher
- B. web-Stat
- C. Webroot
- D. WAFW00F

Answer: B

Explanation:

Increase your web site's performance and grow! Add Web-Stat to your site (it's free!) and watch individuals act together with your pages in real time.

Learn how individuals realize your web site. Get details concerning every visitor's path through your web site and track pages that flip browsers into consumers.

One-click install. observe locations, in operation systems, browsers and screen sizes and obtain alerts for new guests and conversions

NEW QUESTION 185

This TCP flag instructs the sending system to transmit all buffered data immediately.

- A. SYN

- B. RST
- C. PSH
- D. URG
- E. FIN

Answer: C

NEW QUESTION 189

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. Privilege Escalation
- B. Shoulder-Surfing
- C. Hacking Active Directory
- D. Port Scanning

Answer: A

NEW QUESTION 191

Widespread fraud at Enron, WorldCom, and Tyco led to the creation of a law that was designed to improve the accuracy and accountability of corporate disclosures. It covers accounting firms and third parties that provide financial services to some organizations and came into effect in 2002. This law is known by what acronym?

- A. Fed RAMP
- B. PCIDSS
- C. SOX
- D. HIPAA

Answer: C

Explanation:

The Sarbanes-Oxley Act of 2002 could be a law the U.S. Congress passed on July thirty of that year to assist defend investors from fallacious money coverage by companies. Also called the SOX Act of 2002 and also the company Responsibility Act of 2002, it mandated strict reforms to existing securities rules and obligatory powerful new penalties on law breakers.

The Sarbanes-Oxley law Act of 2002 came in response to money scandals within the early 2000s involving in public listed corporations like Enron Corporation, Tyco International plc, and WorldCom. The high-profile frauds cask capitalist confidence within the trustiness of company money statements Associate in Nursing light-emitting diode several to demand an overhaul of decades-old restrictive standards.

NEW QUESTION 193

On performing a risk assessment, you need to determine the potential impacts when some of the critical business processes of the company interrupt its service. What is the name of the process by which you can determine those critical businesses?

- A. Emergency Plan Response (EPR)
- B. Business Impact Analysis (BIA)
- C. Risk Mitigation
- D. Disaster Recovery Planning (DRP)

Answer: B

NEW QUESTION 195

Richard, an attacker, targets an MNC. In this process, he uses a footprinting technique to gather as much information as possible. Using this technique, he gathers domain information such as the target domain name, contact details of its owner, expiry date, and creation date. With this information, he creates a map of the organization's network and misleads domain owners with social engineering to obtain internal details of its network. What type of footprinting technique is employed by Richard?

- A. VoIP footprinting
- B. VPN footprinting
- C. Whois footprinting
- D. Email footprinting

Answer: C

Explanation:

WHOIS (pronounced because the phrase who is) may be a query and response protocol and whois footprinting may be a method for glance information about ownership of a website name as following:• name details• Contact details contain phone no. and email address of the owner• Registration date for the name• Expire date for the name• name servers

NEW QUESTION 197

Which of the following Linux commands will resolve a domain name into IP address?

- A. >host -t a hackeddomain.com
- B. >host -t ns hackeddomain.com
- C. >host -t soa hackeddomain.com
- D. >host -t AXFR hackeddomain.com

Answer: A

NEW QUESTION 201

Alex, a cloud security engineer working in Eyecloud Inc. is tasked with isolating applications from the underlying infrastructure and stimulating communication via well-defined channels. For this purpose, he used an open-source technology that helped him in developing, packaging, and running applications; further, the technology provides PaaS through OS-level visualization, delivers containerized software packages, and promotes fast software delivery. What is the cloud technology employed by Alex in the above scenario?

- A. Virtual machine
- B. Serverless computing
- C. Docker
- D. Zero trust network

Answer: C

NEW QUESTION 206

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 premises environment

- A. VCloud based
- B. Honypot based
- C. Behaviour based
- D. Heuristics based

Answer: A

NEW QUESTION 211

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. Web site defacement vulnerability
- D. Cross-site Request Forgery vulnerability

Answer: A

NEW QUESTION 213

Which of the following algorithms can be used to guarantee the integrity of messages being sent, in transit, or stored?

- A. symmetric algorithms
- B. asymmetric algorithms
- C. hashing algorithms
- D. integrity algorithms

Answer: C

NEW QUESTION 218

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 his dial-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@g@:
Y0u @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. SQL injection
- C. DNS poisoning
- D. Routing table injection

Answer: C

NEW QUESTION 220

Gilbert, a web developer, uses a centralized web API to reduce complexity and increase the Integrity of updating and changing data. For this purpose, he uses a web service that uses HTTP methods such as PUT, POST, GET, and DELETE and can improve the overall performance, visibility, scalability, reliability, and portability of an application. What is the type of web-service API mentioned in the above scenario?

- A. JSON-RPC
- B. SOAP API

- C. RESTful API
- D. REST API

Answer: C

Explanation:

*REST is not a specification, tool, or framework, but instead is an architectural style for web services that serves as a communication medium between various systems on the web. *RESTful APIs, which are also known as RESTful services, are designed using REST principles and HTTP communication protocols RESTful is a collection of resources that use HTTP methods such as PUT, POST, GET, and DELETE

RESTful API: RESTful API is a RESTful service that is designed using REST principles and HTTP communication protocols. RESTful is a collection of resources that use HTTP methods such as PUT, POST, GET, and DELETE. RESTful API is also designed to make applications independent to improve the overall performance, visibility, scalability, reliability, and portability of an application. APIs with the following features can be referred to as RESTful APIs: o Stateless: The client end stores the state of the session; the server is restricted to save data during the request processing o Cacheable: The client should save responses (representations) in the cache. This feature can enhance API performance pg. 1920 CEHv11 manual.

<https://cloud.google.com/files/apigee/apigee-web-api-design-the-missing-link-ebook.pdf>

The HTTP methods GET, POST, PUT or PATCH, and DELETE can be used with these templates to read, create, update, and delete description resources for dogs and their owners. This API style has become popular for many reasons. It is straightforward and intuitive, and learning this pattern is similar to learning a programming language API. APIs like this one are commonly called RESTful APIs, although they do not display all of the characteristics that define REST (more on REST later).

NEW QUESTION 221

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 port security on his switches.
- B. Use a tool like ARPwatch to monitor for strange ARP activity.
- C. Use a firewall between all LAN segments.
- D. If you have a small network, use static ARP entries.
- E. Use only static IP addresses on all PC's.

Answer: ABD

NEW QUESTION 224

in this form of encryption algorithm, every Individual block contains 64-bit data, and three keys are used, where each key consists of 56 bits. Which is this encryption algorithm?

- A. IDEA
- B. Triple Data Encryption standard
- C. MDS encryption algorithm
- D. AES

Answer: B

Explanation:

Triple DES is another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. In Stealth, you merely type within the entire 192-bit (24 character) key instead of entering each of the three keys individually. The Triple DES DLL then breaks the user-provided key into three subkeys, padding the keys if necessary in order that they are each 64 bits long. The procedure for encryption is strictly an equivalent as regular DES, but it's repeated 3 times, hence the name Triple DES. the info is encrypted with the primary key, decrypted with the second key, and eventually encrypted again with the third key. Triple DES runs 3 times slower than DES, but is far safer if used properly. The procedure for decrypting something is that the same because the procedure for encryption, except it's executed in reverse. Like DES, data is encrypted and decrypted in 64-bit chunks. Although the input key for DES is 64 bits long, the particular key employed by DES is merely 56 bits long. the smallest amount significant (right-most) bit in each byte may be a parity, and will be set in order that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most vital bits of every byte are used, leading to a key length of 56 bits. this suggests that the effective key strength for Triple DES is really 168 bits because each of the three keys contains 8 parity bits that aren't used during the encryption process. Triple DES Modes Triple ECB (Electronic Code Book)• This variant of Triple DES works precisely the same way because the ECB mode of DES. • this is often the foremost commonly used mode of operation. Triple CBC (Cipher Block Chaining)• This method is extremely almost like the quality DES CBC mode. • like Triple ECB, the effective key length is 168 bits and keys are utilized in an equivalent manner, as described above, but the chaining features of CBC mode also are employed. • the primary 64-bit key acts because the Initialization Vector to DES. • Triple ECB is then executed for one 64-bit block of plaintext. • The resulting ciphertext is then XORed with subsequent plaintext block to be encrypted, and therefore the procedure is repeated. • This method adds an additional layer of security to Triple DES and is therefore safer than Triple ECB, although it's not used as widely as Triple ECB.

NEW QUESTION 227

Which method of password cracking takes the most time and effort?

- A. Dictionary attack
- B. Shoulder surfing
- C. Rainbow tables
- D. Brute force

Answer: D

NEW QUESTION 229

What useful information is gathered during a successful Simple Mail Transfer Protocol (SMTP) enumeration?

- A. The two internal commands VRFY and EXPN provide a confirmation of valid users, email addresses, aliases, and mailing lists.
- B. Reveals the daily outgoing message limits before mailboxes are locked
- C. The internal command RCPT provides a list of ports open to message traffic.
- D. A list of all mail proxy server addresses used by the targeted host

Answer: A

NEW QUESTION 230

Which of the following is not a Bluetooth attack?

- A. Bluedriving
- B. Bluesmacking
- C. Bluejacking
- D. Bluesnarfing

Answer: A

NEW QUESTION 235

Which of the following steps for risk assessment methodology refers to vulnerability identification?

- A. Determines if any flaws exist in systems, policies, or procedures
- B. Assigns values to risk probabilities; Impact values.
- C. Determines risk probability that vulnerability will be exploited (High, Medium, Low)
- D. Medium, Low
- E. Identifies sources of harm to an IT system
- F. (Natural, Human, Environmental)
- G. Environmental

Answer: C

NEW QUESTION 237

John, a professional hacker, performs a network attack on a renowned organization and gains unauthorized access to the target network. He remains in the network without being detected for a long time and obtains sensitive information without sabotaging the organization. Which of the following attack techniques is used by John?

- A. Advanced persistent threat
- B. threat Diversion theft
- C. Spear-phishing sites
- D. insider threat

Answer: A

Explanation:

An advanced persistent threat (APT) may be a broad term used to describe an attack campaign within which an intruder, or team of intruders, establishes a bootleg, long presence on a network so as to mine sensitive knowledge. The targets of those assaults, that square measure terribly fastidiously chosen and researched, usually embrace massive enterprises or governmental networks. the implications of such intrusions square measure huge, and include:

- Intellectual property thieving (e.g., trade secrets or patents)
- Compromised sensitive info (e.g., worker and user personal data)
- The sabotaging of essential structure infrastructures (e.g., information deletion)
- Total website takeovers

Executing an APT assault needs additional resources than a regular internet application attack. The perpetrators square measure typically groups of intimate cybercriminals having substantial resource. Some APT attacks square measure government-funded and used as cyber warfare weapons.

APT attacks dissent from ancient internet application threats, in that:

- They're considerably additional advanced.
- They're not hit and run attacks—once a network is infiltrated, the culprit remains so as to realize the maximum amount info as potential.
- They're manually dead (not automated) against a selected mark and indiscriminately launched against an outsized pool of targets.
- They typically aim to infiltrate a complete network, as opposition one specific half.

More common attacks, like remote file inclusion (RFI), SQL injection and cross-site scripting (XSS), square measure oftentimes employed by perpetrators to ascertain a footing in a very targeted network. Next, Trojans and backdoor shells square measure typically wont to expand that foothold and make a persistent presence inside the targeted perimeter.

NEW QUESTION 242

CyberTech Inc. recently experienced SQL injection attacks on its official website. The company appointed Bob, a security professional, to build and incorporate defensive strategies against such attacks. Bob adopted a practice whereby only a list of entities such as the data type, range, size, and value, which have been approved for secured access, is accepted. What is the defensive technique employed by Bob in the above scenario?

- A. Output encoding
- B. Enforce least privileges
- C. Whitelist validation
- D. Blacklist validation

Answer: C

NEW QUESTION 244

Which of the following is a passive wireless packet analyzer that works on Linux-based systems?

- A. Burp Suite
- B. OpenVAS
- C. tshark
- D. Kismet

Answer: C

NEW QUESTION 248

You are attempting to crack LM Manager hashed from Windows 2000 SAM file. You will be using LM Brute force hacking tool for decryption. What encryption algorithm will you be decrypting?

- A. MD4
- B. DES
- C. SHA
- D. SSL

Answer: B

NEW QUESTION 250

Peter extracts the SIDs list from Windows 2000 Server machine using the hacking tool "SIDExtractor". Here is the output of the SIDs:

```
s-1-5-21-1125394485-807628933-54978560-100Johns  
s-1-5-21-1125394485-807628933-54978560-652Rebecca  
s-1-5-21-1125394485-807628933-54978560-412Sheela  
s-1-5-21-1125394485-807628933-54978560-999Shawn  
s-1-5-21-1125394485-807628933-54978560-777Somia  
s-1-5-21-1125394485-807628933-54978560-500chang  
s-1-5-21-1125394485-807628933-54978560-555Micah
```

From the above list identify the user account with System Administrator privileges.

- A. John
- B. Rebecca
- C. Sheela
- D. Shawn
- E. Somia
- F. Chang
- G. Micah

Answer: F

NEW QUESTION 255

A pen tester is configuring a Windows laptop for a test. In setting up Wireshark, what driver and library are required to allow the NIC to work in promiscuous mode?

- A. Libpcap
- B. Awincap
- C. Winprom
- D. Winpcap

Answer: D

NEW QUESTION 260

Steve, an attacker, created a fake profile on a social media website and sent a request to Stella. Stella was enthralled by Steve's profile picture and the description given for his profile, and she initiated a conversation with him soon after accepting the request. After a few days, Steve started asking about her company details and eventually gathered all the essential information regarding her company. What is the social engineering technique Steve employed in the above scenario?

- A. Diversion theft
- B. Baiting
- C. Honey trap
- D. Piggybacking

Answer: C

Explanation:

The honey trap is a technique where an attacker targets a person online by pretending to be an attractive person and then begins a fake online relationship to obtain confidential information about the target company. In this technique, the victim is an insider who possesses critical information about the target organization.

Baiting is a technique in which attackers offer end users something alluring in exchange for important information such as login details and other sensitive data. This technique relies on the curiosity and greed of the end-users. Attackers perform this technique by leaving a physical device such as a USB flash drive containing malicious files in locations where people can easily find them, such as parking lots, elevators, and bathrooms. This physical device is labeled with a legitimate company's logo, thereby tricking end-users into trusting it and opening it on their systems. Once the victim connects and opens the device, a malicious file downloads. It infects the system and allows the attacker to take control.

For example, an attacker leaves some bait in the form of a USB drive in the elevator with the label "Employee Salary Information 2019" and a legitimate company's logo. Out of curiosity and greed, the victim picks up the device and opens it up on their system, which downloads the bait. Once the bait is downloaded, a piece of malicious software installs on the victim's system, giving the attacker access.

NEW QUESTION 261

MX record priority increases as the number increases. (True/False.)

- A. True
- B. False

Answer: B

NEW QUESTION 265

In an attempt to damage the reputation of a competitor organization, Hailey, a professional hacker, gathers a list of employee and client email addresses and other related information by using various search engines, social networking sites, and web spidering tools. In this process, she also uses an automated tool to gather a list of words from the target website to further perform a brute-force attack on the previously gathered email addresses. What is the tool used by Hailey for gathering a list of words from the target website?

- A. Shadowsocks
- B. CeWL
- C. Psiphon
- D. Orbot

Answer: B

NEW QUESTION 269

Within the context of Computer Security, which of the following statements describes Social Engineering best?

- A. Social Engineering is the act of publicly disclosing information
- B. Social Engineering is the means put in place by human resource to perform time accounting
- C. Social Engineering is the act of getting needed information from a person rather than breaking into a system
- D. Social Engineering is a training program within sociology studies

Answer: C

NEW QUESTION 272

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 must perform privilege escalation.
- B. He needs to disable antivirus protection.
- C. He needs to gain physical access.
- D. He already has admin privileges, as shown by the "501" at the end of the SID.

Answer: A

NEW QUESTION 276

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%2e%2f = ../ ../ ../
%65%74%63 = etc
%2f = /
%70%61%73%73%77%64 = passwd
```

How would you protect from these attacks?

- A. Configure the Web Server to deny requests involving "hex encoded" characters
- B. Create rules in IDS to alert on strange Unicode requests
- C. Use SSL authentication on Web Servers
- D. Enable Active Scripts Detection at the firewall and routers

Answer: B

NEW QUESTION 279

Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

- A. ESP transport mode
- B. ESP confidential
- C. AH permiscuous
- D. AH Tunnel mode

Answer: A

NEW QUESTION 281

What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?

- A. 110
- B. 135
- C. 139
- D. 161
- E. 445
- F. 1024

Answer: BCE

NEW QUESTION 285

A zone file consists of which of the following Resource Records (RRs)?

- A. DNS, NS, AXFR, and MX records
- B. DNS, NS, PTR, and MX records
- C. SOA, NS, AXFR, and MX records
- D. SOA, NS, A, and MX records

Answer: D

NEW QUESTION 290

SQL injection (SQLi) attacks attempt to inject SQL syntax into web requests, which may Bypass authentication and allow attackers to access and/or modify data attached to a web application.

Which of the following SQLi types leverages a database server's ability to make DNS requests to pass data to an attacker?

- A. Union-based SQLi
- B. Out-of-band SQLi
- C. In-band SQLi
- D. Time-based blind SQLi

Answer: B

Explanation:

Out-of-band SQL injection occurs when an attacker is unable to use an equivalent channel to launch the attack and gather results. ... Out-of-band SQLi techniques would believe the database server's ability to form DNS or HTTP requests to deliver data to an attacker. Out-of-band SQL injection is not very common, mostly because it depends on features being enabled on the database server being used by the web application.

Out-of-band SQL injection occurs when an attacker is unable to use the same channel to launch the attack and gather results.

Out-of-band techniques, offer an attacker an alternative to inferential time-based techniques, especially if the server responses are not very stable (making an inferential time-based attack unreliable).

Out-of-band SQLi techniques would rely on the database server's ability to make DNS or HTTP requests to deliver data to an attacker. Such is the case with Microsoft SQL Server's xp_dirtree command, which can be used to make DNS requests to a server an attacker controls; as well as Oracle Database's UTL_HTTP

package, which can be used to send HTTP requests from SQL and PL/SQL to a server an attacker controls.

NEW QUESTION 292

```
#!/usr/bin/python import socket buffer=["A"] counter=50 while len(buffer)<=100: buffer.append ("A"*counter) counter=counter+50 commands= ["HELP","STATS .","RTIME .","LTIME .","SRUN .","TRUN .","GMON .","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()
```

What is the code written for?

- A. Denial-of-service (DOS)
- B. Buffer Overflow
- C. Bruteforce
- D. Encryption

Answer: B

NEW QUESTION 297

Your organization has signed an agreement with a web hosting provider that requires you to take full responsibility of the maintenance of the cloud-based resources. Which of the following models covers this?

- A. Platform as a service
- B. Software as a service
- C. Functions as a
- D. service Infrastructure as a service

Answer: C

NEW QUESTION 298

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 that 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:8

- A. The host is likely a Linux machine.
- B. The host is likely a printer.
- C. The host is likely a router.
- D. The host is likely a Windows machine.

Answer: B

NEW QUESTION 302

Your company was hired by a small healthcare provider to perform a technical assessment on the network. What is the best approach for discovering vulnerabilities on a Windows-based computer?

- A. Use the built-in Windows Update tool
- B. Use a scan tool like Nessus
- C. Check MITRE.org for the latest list of CVE findings
- D. Create a disk image of a clean Windows installation

Answer: B

NEW QUESTION 305

BitLocker encryption has been implemented for all the Windows-based computers in an organization. You are concerned that someone might lose their cryptographic key. Therefore, a mechanism was implemented to recover the keys from Active Directory. What is this mechanism called in cryptography?

- A. Key archival
- B. Key escrow.
- C. Certificate rollover
- D. Key renewal

Answer: B

NEW QUESTION 306

At what stage of the cyber kill chain theory model does data exfiltration occur?

- A. Actions on objectives
- B. Weaponization
- C. installation
- D. Command and control

Answer: A

Explanation:

The longer an adversary has this level of access, the greater the impact. Defenders must detect this stage as quickly as possible and deploy tools which can enable them to gather forensic evidence. One example would come with network packet captures, for damage assessment. Only now, after progressing through the primary six phases, can intruders take actions to realize their original objectives. Typically, the target of knowledge exfiltration involves collecting, encrypting and extracting information from the victim(s) environment; violations of knowledge integrity or availability are potential objectives also. Alternatively, and most ordinarily, the intruder may only desire access to the initial victim box to be used as a hop point to compromise additional systems and move laterally inside the network. Once this stage is identified within an environment, the implementation of prepared reaction plans must be initiated. At a minimum, the plan should include a comprehensive communication plan, detailed evidence must be elevated to the very best ranking official or board, the deployment of end-point security tools to dam data loss and preparation for briefing a CIRT Team. Having these resources well established beforehand may be a "MUST" in today's quickly evolving landscape of cybersecurity threats

NEW QUESTION 308

Becky has been hired by a client from Dubai to perform a penetration test against one of their remote offices. Working from her location in Columbus, Ohio, Becky runs her usual reconnaissance scans to obtain basic information about their network. When analyzing the results of her Whois search, Becky notices that the IP was allocated to a location in Le Havre, France. Which regional Internet registry should Becky go to for detailed information?

- A. ARIN
- B. APNIC
- C. RIPE
- D. LACNIC

Answer: C

Explanation:

Regional Internet Registries (RIRs):

ARIN (American Registry for Internet Numbers) AFRINIC (African Network Information Center) APNIC (Asia Pacific Network Information Center)

RIPE (Réseaux IP Européens Network Coordination Centre)

LACNIC (Latin American and Caribbean Network Information Center)

NEW QUESTION 313

What is a "Collision attack" in cryptography?

- A. Collision attacks try to get the public key
- B. Collision attacks try to break the hash into three parts to get the plaintext value
- C. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key
- D. Collision attacks try to find two inputs producing the same hash

Answer: D

NEW QUESTION 318

What did the following commands determine?

```
C: user2sid \earth guest
8-1-5-21-343818398-789336058-1343024091-501
C:sid2user 5 21 343818398 789336058 1343024091 500
Name is Joe
Domain is EARTH
```

- A. That the Joe account has a SID of 500
- B. These commands demonstrate that the guest account has NOT been disabled
- C. These commands demonstrate that the guest account has been disabled
- D. That the true administrator is Joe
- E. Issued alone, these commands prove nothing

Answer: D

NEW QUESTION 321

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. Data items and vulnerability scanning
- B. Interviewing employees and network engineers
- C. Reviewing the firewalls configuration
- D. Source code review

Answer: A

NEW QUESTION 325

George is a security professional working for iTech Solutions. He was tasked with securely transferring sensitive data of the organization between industrial systems. In this process, he used a short-range communication protocol based on the IEEE 203.15.4 standard. This protocol is used in devices that transfer data infrequently at a low rate in a restricted area, within a range of 10-100 m. What is the short-range wireless communication technology George employed in the above scenario?

- A. MQTT
- B. LPWAN
- C. Zigbee
- D. NB-IoT

Answer: C

Explanation:

Zigbee could be a wireless technology developed as associate open international normal to deal with the unique desires of affordable, low-power wireless IoT networks. The Zigbee normal operates on the IEEE 802.15.4 physical radio specification and operates in unauthorised bands as well as a pair of 4 GHz, 900 MHz and 868 MHz.

The 802.15.4 specification upon that the Zigbee stack operates gained confirmation by the Institute of Electrical and physical science Engineers (IEEE) in 2003. The specification could be a packet-based radio protocol supposed for affordable, battery-operated devices. The protocol permits devices to speak in an exceedingly kind of network topologies and may have battery life lasting many years.

The Zigbee three.0 Protocol

The Zigbee protocol has been created and ratified by member corporations of the Zigbee Alliance. Over three hundred leading semiconductor makers, technology corporations, OEMs and repair corporations comprise the Zigbee Alliance membership. The Zigbee protocol was designed to supply associate easy-to-use wireless information answer characterised by secure, reliable wireless network architectures.

THE ZIGBEE ADVANTAGE

The Zigbee 3.0 protocol is intended to speak information through rip-roaring RF environments that area unit common in business and industrial applications. Version 3.0 builds on the prevailing Zigbee normal however unifies the market-specific application profiles to permit all devices to be wirelessly connected within the same network, no matter their market designation and performance. what is more, a Zigbee 3.0 certification theme ensures the ability of product from completely different makers. Connecting Zigbee three.0 networks to the information science domain unveil observance and management from devices like smartphones and tablets on a local area network or WAN, as well as the web, and brings verity net of Things to fruition.

Zigbee protocol options include:

- Support for multiple network topologies like point-to-point, point-to-multipoint and mesh networks
- Low duty cycle – provides long battery life
- Low latency
- Direct Sequence unfold Spectrum (DSSS)
- Up to 65,000 nodes per network
- 128-bit AES encryption for secure information connections
- Collision avoidance, retries and acknowledgements

This is another short-range communication protocol based on the IEEE 203.15.4 standard. Zig-Bee is used in devices that transfer data infrequently at a low rate in a restricted area and within a range of 10–100 m.

NEW QUESTION 330

Morris, an attacker, wanted to check whether the target AP is in a locked state. He attempted using different utilities to identify WPS-enabled APs in the target wireless network. Ultimately, he succeeded with one special command-line utility. Which of the following command-line utilities allowed Morris to discover the WPS-enabled APs?

- A. wash
- B. ntptrace
- C. macof
- D. net View

Answer: A

NEW QUESTION 333

You want to analyze packets on your wireless network. Which program would you use?

- A. Wireshark with Airpcap
- B. Aircrack-ng with Airpcap
- C. Wireshark with Winpcap
- D. Ethereal with Winpcap

Answer: A

NEW QUESTION 336

In an attempt to increase the security of your network, you implement a solution that will help keep your wireless network undiscoverable and accessible only to those that know it. How do you accomplish this?

- A. Delete the wireless network
- B. Remove all passwords
- C. Lock all users
- D. Disable SSID broadcasting

Answer: D

NEW QUESTION 337

These hackers have limited or no training and know how to use only basic techniques or tools. What kind of hackers are we talking about?

- A. Black-Hat Hackers
- B. Script Kiddies
- C. White-Hat Hackers
- D. Gray-Hat Hacker

Answer: B

Explanation:

Script Kiddies: These hackers have limited or no training and know how to use only basic techniques or tools. Even then they may not understand any or all of what they are doing.

NEW QUESTION 342

Richard, an attacker, aimed to hack IoT devices connected to a target network. In this process, Richard recorded the frequency required to share information between connected devices. After obtaining the frequency, he captured the original data when commands were initiated by the connected devices. Once the original data were collected, he used free tools such as URH to segregate the command sequence. Subsequently, he started injecting the segregated command sequence on the same frequency into the IoT network, which repeats the captured signals of the devices. What is the type of attack performed by Richard in the above scenario?

- A. Side-channel attack
- B. Replay attack
- C. Cryptanalysis attack
- D. Reconnaissance attack

Answer: B

Explanation:

Replay Attack could be a variety of security attack to the info sent over a network. In this attack, the hacker or a person with unauthorized access, captures the traffic and sends communication to its original destination, acting as the original sender. The receiver feels that it's a genuine message however it's really the message sent by the aggressor. The most feature of the Replay Attack is that the consumer would receive the message double, hence the name, Replay Attack.

Prevention from Replay Attack : 1. Timestamp technique –Prevention from such attackers is feasible, if timestamp is employed at the side of the info. Supposedly, the timestamp on an information is over a precise limit, it may be discarded, and sender may be asked to send the info once more. 2. Session key technique –Another way of hindrance, is by victimisation session key. This key may be used one time (by sender and receiver) per dealing, and can't be reused.

NEW QUESTION 346

Suppose that you test an application for the SQL injection vulnerability. You know that the backend database is based on Microsoft SQL Server. In the login/password form, you enter the following credentials: Username: attack' or 1=1 Password: 123456

Based on the above credentials, which of the following SQL commands are you expecting to be executed by the server, if there is indeed an SQL injection vulnerability?

- A. `select * from Users where UserName = 'attack' or 1=1 -- and UserPassword = '123456'`
- B. `select * from Users where UserName = 'attack' or 1=1 -- and UserPassword = '123456'`
- C. `select * from Users where UserName = 'attack or 1=1 -- and UserPassword = '123456'`
- D. `select * from Users where UserName = 'attack' or 1=1 --' and UserPassword = '123456'`

Answer: A

NEW QUESTION 349

Allen, a professional pen tester, was hired by xpertTech solutions to perform an attack simulation on the organization's network resources. To perform the attack,

he took advantage of the NetBIOS API and targeted the NetBIOS service. B/enumerating NetBIOS, he found that port 139 was open and could see the resources that could be accessed or viewed on a remote system. He came across many NetBIOS codes during enumeration. identify the NetBIOS code used for obtaining the messenger service running for the logged-in user?

- A. <1B>
- B. <00>
- C. <03>
- D. <20>

Answer: C

Explanation:

<03>Windows Messenger administration Courier administration is an organization based framework notice Windows administration by Microsoft that was remembered for some prior forms of Microsoft Windows. This resigned innovation, despite the fact that it has a comparable name, isn't connected in any capacity to the later, Internet-based Microsoft Messenger administration for texting or to Windows Messenger and Windows Live Messenger (earlier named MSN Messenger) customer programming. The Messenger Service was initially intended for use by framework managers to tell Windows clients about their networks.[1] It has been utilized malevolently to introduce spring up commercials to clients over the Internet (by utilizing mass-informing frameworks which sent an ideal message to a predetermined scope of IP addresses). Despite the fact that Windows XP incorporates a firewall, it isn't empowered naturally. Along these lines, numerous clients got such messages. Because of this maltreatment, the Messenger Service has been debilitated as a matter of course in Windows XP Service Pack 2.

NEW QUESTION 350

Harris is attempting to identify the OS running on his target machine. He inspected the initial TTL in the IP header and the related TCP window size and obtained the following results:

TTL: 64 Window Size: 5840

What is the OS running on the target machine?

- A. Solaris OS
- B. Windows OS
- C. Mac OS
- D. Linux OS

Answer: D

NEW QUESTION 351

Which of the following is a low-tech way of gaining unauthorized access to systems?

- A. Social Engineering
- B. Eavesdropping
- C. Scanning
- D. Sniffing

Answer: A

NEW QUESTION 353

In the field of cryptanalysis, what is meant by a "rubber-hose" attack?

- A. Attempting to decrypt cipher text by making logical assumptions about the contents of the original plain text.
- B. Extraction of cryptographic secrets through coercion or torture.
- C. Forcing the targeted key stream through a hardware-accelerated device such as an ASIC.
- D. A backdoor placed into a cryptographic algorithm by its creator.

Answer: B

NEW QUESTION 354

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 anti-virus program with a new one
- 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: A

NEW QUESTION 355

which type of virus can change its own code and then cipher itself multiple times as it replicates?

- A. Stealth virus
- B. Tunneling virus
- C. Cavity virus
- D. Encryption virus

Answer: A

Explanation:

A stealth virus may be a sort of virus malware that contains sophisticated means of avoiding detection by antivirus software. After it manages to urge into the now-infected machine a stealth viruses hides itself by continually renaming and moving itself round the disc. Like other viruses, a stealth virus can take hold of the many

parts of one's PC. When taking control of the PC and performing tasks, antivirus programs can detect it, but a stealth virus sees that coming and can rename then copy itself to a special drive or area on the disc, before the antivirus software. Once moved and renamed a stealth virus will usually replace the detected 'infected' file with a clean file that doesn't trigger anti-virus detection. It's a never-ending game of cat and mouse. The intelligent architecture of this sort of virus about guarantees it's impossible to completely rid oneself of it once infected. One would need to completely wipe the pc and rebuild it from scratch to completely eradicate the presence of a stealth virus. Using regularly-updated antivirus software can reduce risk, but, as we all know, antivirus software is additionally caught in an endless cycle of finding new threats and protecting against them.
<https://www.techslang.com/definition/what-is-a-stealth-virus/>

NEW QUESTION 357

An organization decided to harden its security against web-application and web-server attacks. John, a security personnel in the organization, employed a security scanner to automate web-application security testing and to guard the organization's web infrastructure against web-application threats. Using that tool, he also wants to detect XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks. Which of the following security scanners will help John perform the above task?

- A. AlienVault®OSSIM™
- B. Syhunt Hybrid
- C. Saleae Logic Analyzer
- D. Cisco ASA

Answer: B

NEW QUESTION 361

In the field of cryptanalysis, what is meant by a "rubber-hose" attack?

- A. Forcing the targeted keystream through a hardware-accelerated device such as an ASIC.
- B. A backdoor placed into a cryptographic algorithm by its creator.
- C. Extraction of cryptographic secrets through coercion or torture.
- D. Attempting to decrypt ciphertext by making logical assumptions about the contents of the original plaintext.

Answer: C

NEW QUESTION 366

Which utility will tell you in real time which ports are listening or in another state?

- A. Netstat
- B. TCPView
- C. Nmap
- D. Loki

Answer: B

NEW QUESTION 368

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. Multi-cast mode
- B. Promiscuous mode
- C. WEM
- D. Port forwarding

Answer: B

NEW QUESTION 370

Which of these is capable of searching for and locating rogue access points?

- A. HIDS
- B. WISS
- C. WIPS
- D. NIDS

Answer: C

NEW QUESTION 375

What is the most common method to exploit the "Bash Bug" or "Shellshock" vulnerability?

- A. SYN Flood
- B. SSH
- C. Through Web servers utilizing CGI (Common Gateway Interface) to send a malformed environment variable to a vulnerable Web server
- D. Manipulate format strings in text fields

Answer: C

NEW QUESTION 379

Clark, a professional hacker, attempted to perform a Btlejacking attack using an automated tool, Btlejack, and hardware tool, micro:bit. This attack allowed Clark to hijack, read, and export sensitive information shared between connected devices. To perform this attack, Clark executed various btlejack commands. Which of the following commands was used by Clark to hijack the connections?

- A. btlejack -f 0x129f3244-j
- B. btlejack -c any
- C. btlejack -d /dev/ttyACM0 -d /dev/ttyACM2 -s
- D. btlejack -f 0x9c68fd30 -t -m 0x1 ffffffff

Answer: D

NEW QUESTION 380

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

- A. How do you prevent DNS spoofing?
- B. Install DNS logger and track vulnerable packets
- C. Disable DNS timeouts
- D. Install DNS Anti-spoofing
- E. Disable DNS Zone Transfer

Answer: C

NEW QUESTION 384

DNS cache snooping is a process of determining if the specified resource address is present in the DNS cache records. It may be useful during the examination of the network to determine what software update resources are used, thus discovering what software is installed.

What command is used to determine if the entry is present in DNS cache?

- A. nslookup -fullrecursive update.antivirus.com
- B. dnsnooping -rt update.antivirus.com
- C. nslookup -norecursive update.antivirus.com
- D. dns --snoop update.antivirus.com

Answer: C

NEW QUESTION 387

John, a disgruntled ex-employee of an organization, contacted a professional hacker to exploit the organization. In the attack process, the professional hacker installed a scanner on a machine belonging to one of the victims and scanned several machines on the same network to identify vulnerabilities to perform further exploitation. What is the type of vulnerability assessment tool employed by John in the above scenario?

- A. Proxy scanner
- B. Agent-based scanner
- C. Network-based scanner
- D. Cluster scanner

Answer: B

Explanation:

Knowing when to include agents into your vulnerability management processes isn't an easy decision. Below are common use cases for agent-based vulnerability scanning to assist you build out your combined scanning strategy.

➤ Intermittent or Irregular Connectivity: Vulnerability management teams are now tasked with scanning devices that access the company network remotely using public or home-based Wi-Fi connections. These connections are often unreliable and intermittent leading to missed network-based scans. Fortunately, the scanning frequency of agents doesn't require a network connection. The agent detects when the device is back online, sending scan data when it's ready to communicate with the VM platform.

➤ Connecting Non-Corporate Devices to Corporate Networks: With the increased use of private devices, company networks are more exposed to malware and infections thanks to limited IT and security teams' control and visibility. Agent-based scanning gives security teams insight into weaknesses on non-corporate endpoints, keeping them informed about professional hacker is potential attack vectors in order that they can take appropriate action.

➤ Endpoints Residing Outside of Company Networks: Whether company-issued or BYOD, remote assets frequently hook up with the web outside of traditional network bounds. An agent that resides on remote endpoints conducts regular, authenticated scans checking out system changes and unpatched software. The results are then sent back to the VM platform and combined with other scan results for review, prioritization, and mitigation planning.

Agent-Based Scanner: Agent-based scanners reside on a single machine but can scan several machines on the same network.

NEW QUESTION 391

Due to a slowdown of normal network operations, the IT department decided to monitor internet traffic for all of the employees. From a legal standpoint, what would be troublesome to take this kind of measure?

- A. All of the employees would stop normal work activities
- B. IT department would be telling employees who the boss is
- C. Not informing the employees that they are going to be monitored could be an invasion of privacy.
- D. The network could still experience traffic slow down.

Answer: C

NEW QUESTION 392

A penetration tester is performing the footprinting process and is reviewing publicly available information about an organization by using the Google search engine. Which of the following advanced operators would allow the pen tester to restrict the search to the organization's web domain?

- A. [allinurl:]
- B. [location:]

- C. [site:]
- D. [link:]

Answer: C

NEW QUESTION 393

Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?

- A. msfpayload
- B. msfcli
- C. msfd
- D. msfencode

Answer: D

NEW QUESTION 396

By using a smart card and pin, you are using a two-factor authentication that satisfies

- A. Something you are and something you remember
- B. Something you have and something you know
- C. Something you know and something you are
- D. Something you have and something you are

Answer: B

NEW QUESTION 398

joe works as an it administrator in an organization and has recently set up a cloud computing service for the organization. To implement this service, he reached out to a telecom company for providing Internet connectivity and transport services between the organization and the cloud service provider, in the NIST cloud deployment reference architecture, under which category does the telecom company fall in the above scenario?

- A. Cloud booker
- B. Cloud consumer
- C. Cloud carrier
- D. Cloud auditor

Answer: C

Explanation:

A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers.

Cloud carriers provide access to consumers through network, telecommunication and other access devices. for instance, cloud consumers will obtain cloud services through network access devices, like computers, laptops, mobile phones, mobile web devices (MIDs), etc.

The distribution of cloud services is often provided by network and telecommunication carriers or a transport agent, wherever a transport agent refers to a business organization that provides physical transport of storage media like high-capacity hard drives.

Note that a cloud provider can started SLAs with a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers, and will require the cloud carrier to provide dedicated and secure connections between cloud consumers and cloud providers.

NEW QUESTION 399

Windows LAN Manager (LM) hashes are known to be weak.

Which of the following are known weaknesses of LM? (Choose three.)

- A. Converts passwords to uppercase.
- B. Hashes are sent in clear text over the network.
- C. Makes use of only 32-bit encryption.
- D. Effective length is 7 characters.

Answer: ABD

NEW QUESTION 402

Robert, a professional hacker, is attempting to execute a fault injection attack on a target IoT device. In this process, he injects faults into the power supply that can be used for remote execution, also causing the skipping of key instructions. He also injects faults into the clock network used for delivering a synchronized signal across the chip.

Which of the following types of fault injection attack is performed by Robert in the above scenario?

- A. Frequency/voltage tampering
- B. Optical, electromagnetic fault injection (EMFI)
- C. Temperature attack
- D. Power/clock/reset glitching

Answer: D

Explanation:

These types of attacks occur when faults or glitches are INJECTED into the Power supply that can be used for remote execution.

NEW QUESTION 406

Abel, a security professional, conducts penetration testing in his client organization to check for any security loopholes. He launched an attack on the DHCP servers by broadcasting forged DHCP requests and leased all the DHCP addresses available in the DHCP scope until the server could not issue any more IP

addresses. This led to a Dos attack, and as a result, legitimate employees were unable to access the clients network. Which of the following attacks did Abel perform in the above scenario?

- A. VLAN hopping
- B. DHCP starvation
- C. Rogue DHCP server attack
- D. STP attack

Answer: B

Explanation:

A DHCP starvation assault is a pernicious computerized assault that objectives DHCP workers. During a DHCP assault, an unfriendly entertainer floods a DHCP worker with false DISCOVER bundles until the DHCP worker debilitates its stock of IP addresses. When that occurs, the aggressor can deny genuine organization clients administration, or even stock an other DHCP association that prompts a Man-in-the-Middle (MITM) assault.

In a DHCP Starvation assault, a threatening entertainer sends a huge load of false DISCOVER parcels until the DHCP worker thinks they've used their accessible pool. Customers searching for IP tends to find that there are no IP addresses for them, and they're refused assistance. Furthermore, they may search for an alternate DHCP worker, one which the unfriendly entertainer may give. What's more, utilizing a threatening or sham IP address, that unfriendly entertainer would now be able to peruse all the traffic that customer sends and gets.

In an unfriendly climate, where we have a malevolent machine running some sort of an instrument like Yersinia, there could be a machine that sends DHCP DISCOVER bundles. This malevolent customer doesn't send a modest bunch – it sends a great many vindictive DISCOVER bundles utilizing sham, made-up MAC addresses as the source MAC address for each solicitation.

In the event that the DHCP worker reacts to every one of these false DHCP DISCOVER parcels, the whole IP address pool could be exhausted, and that DHCP worker could trust it has no more IP delivers to bring to the table to legitimate DHCP demands.

When a DHCP worker has no more IP delivers to bring to the table, ordinarily the following thing to happen would be for the aggressor to get their own DHCP worker. This maverick DHCP worker at that point starts giving out IP addresses.

The advantage of that to the assailant is that if a false DHCP worker is distributing IP addresses, including default DNS and door data, customers who utilize those IP delivers and begin to utilize that default passage would now be able to be directed through the aggressor's machine. That is all that an unfriendly entertainer requires to play out a man-in-the-center (MITM) assault.

NEW QUESTION 408

Nedved is an IT Security Manager of a bank in his country. One day, he found out that there is a security breach to his company's email server based on analysis of a suspicious connection from the email server to an unknown IP Address.

What is the first thing that Nedved needs to do before contacting the incident response team?

- A. Leave it as it is and contact the incident response team right away
- B. Block the connection to the suspicious IP Address from the firewall
- C. Disconnect the email server from the network
- D. Migrate the connection to the backup email server

Answer: C

NEW QUESTION 409

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:

Antivirus code: 5014

<http://www.juggyboy/virus/virus.html>

Thank you for choosing us, the worldwide leader Antivirus solutions.

Mike Robertson

PDF Reader Support

Copyright Antivirus 2010 ?All rights reserved

If you want to stop receiving mail, please go to:

<http://www.juggyboy.com>

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. Look at the website design, if it looks professional then it is a Real Anti-Virus website
- B. Connect to the site using SSL, if you are successful then the website is genuine
- C. Search using the URL and Anti-Virus product name into Google and lookout for suspicious warnings against this site
- 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: C

NEW QUESTION 410

A "Server-Side Includes" attack refers to the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary code remotely. Which web-page file type, if it exists on the web server, is a strong indication that the server is vulnerable to this kind of attack?

- A. .stm
- B. .html
- C. .rss
- D. .cms

Answer: A

NEW QUESTION 415

When considering how an attacker may exploit a web server, what is web server footprinting?

- A. When an attacker implements a vulnerability scanner to identify weaknesses
- B. When an attacker creates a complete profile of the site's external links and file structures
- C. When an attacker gathers system-level data, including account details and server names
- D. When an attacker uses a brute-force attack to crack a web-server password

Answer: B

NEW QUESTION 417

What is the file that determines the basic configuration (specifically activities, services, broadcast receivers, etc.) in an Android application?

- A. AndroidManifest.xml
- B. APK.info
- C. resources.asrc
- D. classes.dex

Answer: A

Explanation:

The AndroidManifest.xml file contains information of your package, including components of the appliance like activities, services, broadcast receivers, content providers etc. It performs another tasks also:• it's responsible to guard the appliance to access any protected parts by providing the permissions. • It also declares the android api that the appliance goes to use. • It lists the instrumentation classes. The instrumentation classes provides profiling and other informations. These informations are removed just before the appliance is published etc. This is the specified xml file for all the android application and located inside the basis directory.

NEW QUESTION 418

Which of the following is the least-likely physical characteristic to be used in biometric control that supports a large company?

- A. Iris patterns
- B. Voice
- C. Height and Weight
- D. Fingerprints

Answer: C

NEW QUESTION 420

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

312-50v11 Practice Exam Features:

- * 312-50v11 Questions and Answers Updated Frequently
- * 312-50v11 Practice Questions Verified by Expert Senior Certified Staff
- * 312-50v11 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 312-50v11 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 312-50v11 Practice Test Here](#)