

EC-Council

Exam Questions 312-50v13

Certified Ethical Hacker v13



NEW QUESTION 1

- (Topic 1)

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 2

- (Topic 1)

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 3

- (Topic 1)

Let's imagine three companies (A, B and C), all competing in a challenging global environment. Company A and B are working together in developing a product that will generate a major competitive advantage for them. Company A has a secure DNS server while company B has a DNS server vulnerable to spoofing. With a spoofing attack on the DNS server of company B, company C gains access to outgoing e-mails from company B. How do you prevent DNS spoofing?

- A. Install DNS logger and track vulnerable packets
- B. Disable DNS timeouts
- C. Install DNS Anti-spoofing
- D. Disable DNS Zone Transfer

Answer: C

NEW QUESTION 4

- (Topic 1)

Study the snort rule given below:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 135
(msg: "NETBIOS DCERPC ISystemActivator bind attempt";
flow:to_server, established; content: "|05|"; distance: 0; within: 1;
content: "|0b|"; distance: 1; within: 1; byte_test: 1, &, 1, 0, relative;
content: "|A0 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46|";
distance: 29; within: 16; reference: cve, CAN-2003-0352;
classtype: attempted-admin; sid: 2192; rev: 1;)
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg: "NETBIOS SMB
DCERPC ISystemActivator bind attempt"; flow: to_server, established;
content: "|FF|SMB|25|"; nocase; offset:4, depth:5; content: "|26 00|";
nocase; distance:5; within: 12; content: "|05|"; distance:0; within:1;
content: "|0b|"; distance: 1; within: 1; byte_test: 1, &, 1, 0, relative;
content: "|A0 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46|";
distance: 29; within: 16; reference: cve, CAN-2003-0352;
classtype: attempted-admin; sid: 2193; rev: 1;)
```

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

- A. WebDav
- B. SQL Slammer
- C. MS Blaster
- D. MyDoom

Answer: C

NEW QUESTION 5

- (Topic 1)

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 6

- (Topic 1)

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

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

Answer: A

NEW QUESTION 7

- (Topic 1)

During a black-box pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded. What type of firewall is inspecting outbound traffic?

- A. Circuit
- B. Stateful
- C. Application
- D. Packet Filtering

Answer: C

Explanation:

https://en.wikipedia.org/wiki/Internet_Relay_Chat

Internet Relay Chat (IRC) is an application layer protocol that facilitates communication in text. The chat process works on a client/server networking model. IRC clients are computer programs that users can install on their system or web-based applications running either locally in the browser or on a third-party server. These clients communicate with chat servers to transfer messages to other clients.

IRC is a plaintext protocol that is officially assigned port 194, according to IANA. However, running the service on this port requires running it with root-level permissions, which is inadvisable. As a result, the well-known port for IRC is 6667, a high-number port that does not require elevated privileges. However, an IRC server can also be configured to run on other ports as well.

You can't tell if an IRC server is designed to be malicious solely based on port number. Still, if you see an IRC server running on port a WKP such as 80, 8080, 53, 443, it's almost always going to be malicious; the only real reason for IRCD to be running on port 80 is to try to evade firewalls.

https://en.wikipedia.org/wiki/Application_firewall

An application firewall is a form of firewall that controls input/output or system calls of an application or service. It operates by monitoring and blocking communications based on a configured policy, generally with predefined rule sets to choose from. The application firewall can control communications up to the OSI model's application layer, which is the highest operating layer, and where it gets its name. The two primary categories of application firewalls are network-based and host-based.

Application layer filtering operates at a higher level than traditional security appliances. This allows packet decisions to be made based on more than just source/destination IP Addresses or ports. It can also use information spanning across multiple connections for any given host.

Network-based application firewalls

Network-based application firewalls operate at the application layer of a TCP/IP stack. They can understand certain applications and protocols such as File Transfer Protocol (FTP), Domain Name System (DNS), or Hypertext Transfer Protocol (HTTP). This allows it to identify unwanted applications or services using a non-standard port or detect if an allowed protocol is being abused.

Host-based application firewalls

A host-based application firewall monitors application system calls or other general system communication. This gives more granularity and control but is limited to only protecting the host it is running on. Control is applied by filtering on a per-process basis. Generally, prompts are used to define rules for processes that have not yet received a connection. Further filtering can be done by examining the process ID of the owner of the data packets. Many host-based application firewalls are combined or used in conjunction with a packet filter.

NEW QUESTION 8

- (Topic 1)

Which of the following is a component of a risk assessment?

- A. Administrative safeguards
- B. Physical security
- C. DMZ
- D. Logical interface

Answer: A

NEW QUESTION 9

- (Topic 1)

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 promiscuous
- D. AH Tunnel mode

Answer: A

NEW QUESTION 10

- (Topic 1)

Which of the following is not a Bluetooth attack?

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

Answer: A

Explanation:

<https://github.com/verovaleros/bluedriving>

Bluedriving is a bluetooth wardriving utility. It can capture bluetooth devices, lookup their services, get GPS information and present everything in a nice web page. It can search for and show a lot of information about the device, the GPS address and the historic location of devices on a map. The main motivation of this tool is to research about the targeted surveillance of people by means of its cellular phone or car. With this tool you can capture information about bluetooth devices and show, on a map, the points where you have seen the same device in the past.

NEW QUESTION 10

- (Topic 1)

Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students.

He identified this when the IDS alerted for malware activities in the network. What should Bob do to avoid this problem?

- A. Disable unused ports in the switches
- B. Separate students in a different VLAN
- C. Use the 802.1x protocol
- D. Ask students to use the wireless network

Answer: C

NEW QUESTION 12

- (Topic 1)

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

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

- A. Hardware, Software, and Sniffing.
- B. Hardware and Software Keyloggers.
- C. Passwords are always best obtained using Hardware key loggers.
- D. Software only, they are the most effective.

Answer: A

NEW QUESTION 13

- (Topic 1)

Bob, a system administrator at TPNQM SA, concluded one day that a DMZ is not needed if he properly configures the firewall to allow access just to servers/ports, which can have direct internet access, and block the access to workstations.

Bob also concluded that DMZ makes sense just when a stateful firewall is available, which is not the case of TPNQM SA.

In this context, what can you say?

- A. Bob can be right since DMZ does not make sense when combined with stateless firewalls
- B. Bob is partially right
- C. He does not need to separate networks if he can create rules by destination IPs, one by one
- D. Bob is totally wrong
- E. DMZ is always relevant when the company has internet servers and workstations
- F. Bob is partially right
- G. DMZ does not make sense when a stateless firewall is available

Answer: C

NEW QUESTION 16

- (Topic 1)

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 17

- (Topic 1)

An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to "www.MyPersonalBank.com", the user is directed to a phishing site.

Which file does the attacker need to modify?

- A. Boot.ini
- B. Sudoers
- C. Networks
- D. Hosts

Answer: D

NEW QUESTION 20

- (Topic 1)

Identify the UDP port that Network Time Protocol (NTP) uses as its primary means of communication?

- A. 113
- B. 69
- C. 123
- D. 161

Answer: C

Explanation:

https://en.wikipedia.org/wiki/Network_Time_Protocol

The Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. NTP is intended to synchronize all participating computers within a few milliseconds of Coordinated Universal Time (UTC). It uses the intersection algorithm, a modified version of Marzullo's algorithm, to select accurate time servers and is designed to mitigate variable network latency effects. NTP can usually maintain time to within tens of milliseconds over the public Internet and achieve better than one millisecond accuracy in local area networks. Asymmetric routes and network congestion can cause errors of 100 ms or more. The protocol is usually described in terms of a client-server model but can easily be used in peer-to-peer relationships where both peers consider the other to be a potential time source. Implementations send and receive timestamps using the User Datagram Protocol (UDP) on port number 123.

NEW QUESTION 25

- (Topic 1)

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 26

- (Topic 1)

PGP, SSL, and IKE are all examples of which type of cryptography?

- A. Digest
- B. Secret Key
- C. Public Key
- D. Hash Algorithm

Answer: C

NEW QUESTION 31

- (Topic 1)

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

- A. True
- B. False

Answer: B

NEW QUESTION 35

- (Topic 1)

A company??s policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as display filter to find unencrypted file transfers?

- A. tcp.port == 21
- B. tcp.port == 23
- C. tcp.port == 21 || tcp.port == 22
- D. tcp.port != 21

Answer: A

NEW QUESTION 39

- (Topic 1)

What does a firewall check to prevent particular ports and applications from getting packets into an organization?

- A. Transport layer port numbers and application layer headers
- B. Presentation layer headers and the session layer port numbers
- C. Network layer headers and the session layer port numbers
- D. Application layer port numbers and the transport layer headers

Answer: A

NEW QUESTION 40

- (Topic 1)

You just set up a security system in your network. In what kind of system would you find the following string of characters used as a rule within its configuration?
alert tcp any any -> 192.168.100.0/24 21 (msg: ???FTP on the network!???)

- A. A firewall IPTable
- B. FTP Server rule
- C. A Router IPTable
- D. An Intrusion Detection System

Answer: D

NEW QUESTION 42

- (Topic 1)

Eve is spending her day scanning the library computers. She notices that Alice is using a computer whose port 445 is active and listening. Eve uses the ENUM tool to enumerate Alice machine. From the command prompt, she types the following command.

```
For /f "tokens=1 %%a in (hackfile.txt) do net use *  
\\10.1.2.3\c$ /user:"Administrator" %%a
```

What is Eve trying to do?

- A. Eve is trying to connect as a user with Administrator privileges
- B. Eve is trying to enumerate all users with Administrative privileges
- C. Eve is trying to carry out a password crack for user Administrator
- D. Eve is trying to escalate privilege of the null user to that of Administrator

Answer: C

NEW QUESTION 43

- (Topic 1)

You have gained physical access to a Windows 2008 R2 server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your toolkit, you have an Ubuntu 9.10 Linux LiveCD. Which Linux-based tool can change any user's password or activate disabled Windows accounts?

- A. John the Ripper
- B. SET
- C. CHNTPW
- D. Cain & Abel

Answer: C

NEW QUESTION 46

- (Topic 1)

Which of the following statements about a zone transfer is correct? (Choose three.)

- A. A zone transfer is accomplished with the DNS
- B. A zone transfer is accomplished with the nslookup service
- C. A zone transfer passes all zone information that a DNS server maintains
- D. A zone transfer passes all zone information that a nslookup server maintains
- E. A zone transfer can be prevented by blocking all inbound TCP port 53 connections
- F. Zone transfers cannot occur on the Internet

Answer: ACE

NEW QUESTION 48

- (Topic 1)

As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?

- A. Use the same machines for DNS and other applications
- B. Harden DNS servers
- C. Use split-horizon operation for DNS servers
- D. Restrict Zone transfers
- E. Have subnet diversity between DNS servers

Answer: BCDE

NEW QUESTION 49

- (Topic 1)

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 53

- (Topic 1)

Shellshock allowed an unauthorized user to gain access to a server. It affected many Internet-facing services, which OS did it not directly affect?

- A. Linux
- B. Unix
- C. OS X
- D. Windows

Answer: D

NEW QUESTION 55

- (Topic 1)

Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?

- A. Kismet
- B. Abel
- C. Netstumbler
- D. Nessus

Answer: A

Explanation:

[https://en.wikipedia.org/wiki/Kismet_\(software\)](https://en.wikipedia.org/wiki/Kismet_(software))

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

NEW QUESTION 60

- (Topic 1)

Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system?

- A. A biometric system that bases authentication decisions on behavioral attributes.
- B. A biometric system that bases authentication decisions on physical attributes.
- C. An authentication system that creates one-time passwords that are encrypted with secret keys.
- D. An authentication system that uses passphrases that are converted into virtual passwords.

Answer: C

NEW QUESTION 61

- (Topic 1)

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 63

- (Topic 1)

A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client. What is a possible source of this problem?

- A. The WAP does not recognize the client's MAC address
- B. The client cannot see the SSID of the wireless network
- C. Client is configured for the wrong channel
- D. The wireless client is not configured to use DHCP

Answer: A

Explanation:

https://en.wikipedia.org/wiki/MAC_filtering

MAC filtering is a security method based on access control. Each address is assigned a 48-bit address, which is used to determine whether we can access a network or not. It helps in listing a set of allowed devices that you need on your Wi-Fi and the list of denied devices that you don't want on your Wi-Fi. It helps in preventing unwanted access to the network. In a way, we can blacklist or white list certain computers based on their MAC address. We can configure the filter to allow connection only to those devices included in the white list. White lists provide greater security than blacklists because the router grants access only to selected devices.

It is used on enterprise wireless networks having multiple access points to prevent clients from communicating with each other. The access point can be configured only to allow clients to talk to the default gateway, but not other wireless clients. It increases the efficiency of access to a network.

The router allows configuring a list of allowed MAC addresses in its web interface, allowing you to choose which devices can connect to your network. The router has several functions designed to improve the network's security, but not all are useful. Media access control may seem advantageous, but there are certain flaws. On a wireless network, the device with the proper credentials such as SSID and password can authenticate with the router and join the network, which gets an IP address and access to the internet and any shared resources.

MAC address filtering adds an extra layer of security that checks the device's MAC address

against a list of agreed addresses. If the client's address matches one on the router's list, access is granted; otherwise, it doesn't join the network.

NEW QUESTION 65

- (Topic 1)

Why is a penetration test considered to be more thorough than vulnerability scan?

- A. Vulnerability scans only do host discovery and port scanning by default.
- B. A penetration test actively exploits vulnerabilities in the targeted infrastructure, while a vulnerability scan does not typically involve active exploitation.
- C. It is not – a penetration test is often performed by an automated tool, while a vulnerability scan requires active engagement.
- D. The tools used by penetration testers tend to have much more comprehensive vulnerability databases.

Answer: B

NEW QUESTION 70

- (Topic 1)

Which system consists of a publicly available set of databases that contain domain name registration contact information?

- A. WHOIS
- B. CAPTCHA
- C. IANA
- D. IETF

Answer: A

NEW QUESTION 72

- (Topic 1)

Which of the following is assured by the use of a hash?

- A. Authentication
- B. Confidentiality
- C. Availability
- D. Integrity

Answer: D

NEW QUESTION 76

- (Topic 1)

Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?

- A. Nikto
- B. John the Ripper
- C. Dsniff
- D. Snort

Answer: A

Explanation:

[https://en.wikipedia.org/wiki/Nikto_\(vulnerability_scanner\)](https://en.wikipedia.org/wiki/Nikto_(vulnerability_scanner))

Nikto is a free software command-line vulnerability scanner that scans web servers for dangerous files/CGIs, outdated server software, and other problems. It performs generic and server types specific checks. It also captures and prints any cookies received. The Nikto code itself is free software, but the data files it uses to drive the program are not.

NEW QUESTION 78

- (Topic 1)

What is not a PCI compliance recommendation?

- A. Use a firewall between the public network and the payment card data.
- B. Use encryption to protect all transmission of card holder data over any public network.
- C. Rotate employees handling credit card transactions on a yearly basis to different departments.
- D. Limit access to card holder data to as few individuals as possible.

Answer: C

Explanation:

https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security Build and Maintain a Secure Network

* 1. Install and maintain a firewall configuration to protect cardholder data.

- * 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data
- * 3. Protect stored cardholder data.
- * 4. Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program
- * 5. Use and regularly update anti-virus software or programs.
- * 6. Develop and maintain secure systems and applications.
Implement Strong Access Control Measures
- * 7. Restrict access to cardholder data by business need-to-know.
- * 8. Assign a unique ID to each person with computer access.
- * 9. Restrict physical access to cardholder data.
Regularly Monitor and Test Networks
- * 10. Track and monitor all access to network resources and cardholder data.
- * 11. Regularly test security systems and processes.
Maintain an Information Security Policy
- * 12. Maintain a policy that addresses information security for employees and contractors.

NEW QUESTION 83

- (Topic 1)

The following is an entry captured by a network IDS. You are assigned the task of analyzing this entry. You notice the value 0x90, which is the most common NOOP instruction for the Intel processor. You figure that the attacker is attempting a buffer overflow attack.

You also notice "/bin/sh" in the ASCII part of the output. As an analyst what would you conclude about the attack?

```
45 00 01 ce 28 1e 40 00 32 06 96 92 d1 3a 18 09 86 9f 18 97 E..î(.ø.2...Ñ:.....
06 38 02 03 6f 54 4f a9 01 af fe 78 50 18 7d 78 76 dd 00 00 .8...oTO@.̣pxP.\)
Application "Calculator" "%path:..\dtsapps\calc\dcalc.exe%" " " size 0.75in 0.25in 0.50in
0.05inxvÝ..
42 42 20 f7 ff bf 21 f7 ff bf 22 f7 ff bf 23 f7 ff bf 58 58 BB ÷ÿ!÷ÿ"÷ÿ#÷ÿXX
58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 25 2e 32 32 XXXXXXXXXXXXXXXXXXXX%.22
34 75 25 33 30 30 24 6e 25 2e 32 31 33 75 25 33 30 31 24 6e 4u%300$n%.213u%301$n
73 65 63 75 25 33 30 32 24 6e 25 2e 31 39 32 75 25 33 30 33 secu%302$n%.192u%303
24 6e 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 $n.....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 31 db 31 c9 31 c0 b0 46 cd 80 89 e5 31 d2 b2 66 89 d0 ..1Û1É1à°FÍ..Å1Ô*f.Đ
31 c9 89 cb 43 89 5d f8 43 89 5d f4 4b 89 4d fc 8d 4d f4 cd 1É.ËC.]øC.]ôK.Mù.MôÍ
80 31 c9 89 45 f4 43 66 89 5d ec 66 c7 45 ee 0f 27 89 4d f0 .1É.EôCf.]ifÇEi.'.Mô
8d 45 ec 89 45 f8 c6 45 fc 10 89 d0 8d 4d f4 cd 80 89 d0 43 .Ei.EøEEù..Đ.MôÍ..ĐC
43 cd 80 89 d0 43 cd 80 89 c3 31 c9 b2 3f 89 d0 cd 80 89 d0 CÍ..ĐCÍ..Ã1É*?.ĐÍ..Đ
41 cd 80 eb 18 5e 89 75 08 31 c0 88 46 07 89 45 0c b0 0b 89 AÍ.è.^.u.1à.F..E.°..
f3 8d 4d 08 8d 55 0c cd 80 e8 e3 ff ff ff 2f 62 69 6e 2f 73 ó.M..U.Í.èäÿÿÿ/bin/s
68 0a h.
EVENT4: [NOOP:X86] (tcp,dp=515,sp=1592)
```

- A. The buffer overflow attack has been neutralized by the IDS
- B. The attacker is creating a directory on the compromised machine
- C. The attacker is attempting a buffer overflow attack and has succeeded
- D. The attacker is attempting an exploit that launches a command-line shell

Answer: D

NEW QUESTION 86

- (Topic 1)

Bob received this text message on his mobile phone: ??Hello, this is Scott Smelby from the Yahoo Bank. Kindly contact me for a vital transaction on: scottsmelby@yahoo.com??. Which statement below is true?

- A. This is a scam as everybody can get a @yahoo address, not the Yahoo customer service employees.
- B. This is a scam because Bob does not know Scott.
- C. Bob should write to scottmelby@yahoo.com to verify the identity of Scott.
- D. This is probably a legitimate message as it comes from a respectable organization.

Answer: A

NEW QUESTION 90

- (Topic 1)

You need to deploy a new web-based software package for your organization. The package requires three separate servers and needs to be available on the Internet. What is the recommended architecture in terms of server placement?

- A. All three servers need to be placed internally
- B. A web server facing the Internet, an application server on the internal network, a database server on the internal network
- C. A web server and the database server facing the Internet, an application server on the internal network
- D. All three servers need to face the Internet so that they can communicate between themselves

Answer: B

NEW QUESTION 93

- (Topic 1)

Which definition among those given below best describes a covert channel?

- A. A server program using a port that is not well known.
- B. Making use of a protocol in a way it is not intended to be used.
- C. It is the multiplexing taking place on a communication link.
- D. It is one of the weak channels used by WEP which makes it insecure

Answer: B

NEW QUESTION 94

- (Topic 1)

Why should the security analyst disable/remove unnecessary ISAPI filters?

- A. To defend against social engineering attacks
- B. To defend against webserver attacks
- C. To defend against jailbreaking
- D. To defend against wireless attacks

Answer: B

NEW QUESTION 97

- (Topic 1)

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 102

- (Topic 1)

Scenario1:

* 1. Victim opens the attacker's web site.

* 2. Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make \$1000 in a day?'.

* 3. Victim clicks to the interesting and attractive content URL.

* 4. Attacker creates a transparent 'iframe' in front of the URL which victim attempts to click, so victim thinks that he/she clicks to the 'Do you want to make \$1000 in a day?' URL but actually he/she clicks to the content or URL that exists in the transparent 'iframe' which is setup by the attacker.

What is the name of the attack which is mentioned in the scenario?

- A. Session Fixation
- B. HTML Injection
- C. HTTP Parameter Pollution
- D. Clickjacking Attack

Answer: D

Explanation:

<https://en.wikipedia.org/wiki/Clickjacking>

Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online.

Typically, clickjacking is performed by displaying an invisible page or HTML element, inside an iframe, on top of the page the user sees. The user believes they are clicking the visible page but in fact they are clicking an invisible element in the additional page transposed on top of it.

NEW QUESTION 103

- (Topic 1)

Which type of security feature stops vehicles from crashing through the doors of a building?

- A. Bollards
- B. Receptionist

C. Mantrap
D. Turnstile

Answer: A

NEW QUESTION 107

- (Topic 1)

Which is the first step followed by Vulnerability Scanners for scanning a network?

- A. OS Detection
- B. Firewall detection
- C. TCP/UDP Port scanning
- D. Checking if the remote host is alive

Answer: D

Explanation:

Vulnerability scanning solutions perform vulnerability penetration tests on the organizational network in three steps:

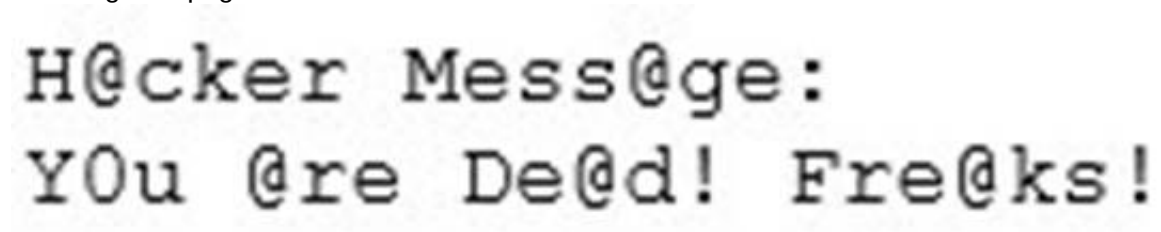
- * 1. Locating nodes: The first step in vulnerability scanning is to locate live hosts in the target network using various scanning techniques.
- * 2. Performing service and OS discovery on them: After detecting the live hosts in the target network, the next step is to enumerate the open ports and services and the operating system on the target systems.
- * 3. Testing those services and OS for known vulnerabilities: Finally, after identifying the open services and the operating system running on the target nodes, they are tested for known vulnerabilities.

NEW QUESTION 109

- (Topic 1)

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:



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 112

- (Topic 1)

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 113

- (Topic 1)

What is the following command used for? `net use \targetipc$ "" /u:""`

- A. Grabbing the etc/passwd file
- B. Grabbing the SAM
- C. Connecting to a Linux computer through Samba.
- D. This command is used to connect as a null session
- E. Enumeration of Cisco routers

Answer: D

NEW QUESTION 118

- (Topic 1)

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 119

- (Topic 1)

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

- A. nessus
- B. tcpdump
- C. ethereal
- D. jack the ripper

Answer: B

Explanation:

Tcpdump is a data-network packet analyzer computer program that runs under a command-line interface. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Distributed under the BSD license, tcpdump is free software.

<https://www.wireshark.org/>

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

NOTE: Wireshark is very similar to tcpdump, but has a graphical front-end, plus some integrated sorting and filtering options.

NEW QUESTION 121

- (Topic 1)

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

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

Answer: B

Explanation:

Dynamic ARP inspection (DAI) protects switching devices against Address Resolution Protocol (ARP) packet spoofing (also known as ARP poisoning or ARP cache poisoning). DAI inspects ARPs on the LAN and uses the information in the DHCP snooping database on the switch to validate ARP packets and to protect against ARP spoofing. ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made based on the results of those comparisons. When an attacker tries to use a forged ARP packet to spoof an address, the switch compares the address with entries in the database. If the media access control (MAC) address or IP address in the ARP packet does not match a valid entry in the DHCP snooping database, the packet is dropped.

NEW QUESTION 123

- (Topic 1)

Null sessions are un-authenticated connections (not using a username or password.) to an NT or 2000 system. Which TCP and UDP ports must you filter to check null sessions on your network?

- A. 137 and 139
- B. 137 and 443
- C. 139 and 443
- D. 139 and 445

Answer: D

NEW QUESTION 127

- (Topic 1)

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 131

- (Topic 1)

The collection of potentially actionable, overt, and publicly available information is known as

- A. Open-source intelligence
- B. Real intelligence
- C. Social intelligence
- D. Human intelligence

Answer: A

NEW QUESTION 135

- (Topic 1)

Which address translation scheme would allow a single public IP address to always correspond to a single machine on an internal network, allowing "server publishing"?

- A. Overloading Port Address Translation
- B. Dynamic Port Address Translation
- C. Dynamic Network Address Translation
- D. Static Network Address Translation

Answer: D

NEW QUESTION 140

- (Topic 1)

```
env x=??(){ :};echo exploit?? bash -c ??cat/etc/passwd??
```

What is the Shellshock bash vulnerability attempting to do on a vulnerable Linux host?

- A. Removes the passwd file
- B. Changes all passwords in passwd
- C. Add new user to the passwd file
- D. Display passwd content to prompt

Answer: D

NEW QUESTION 142

- (Topic 1)

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?

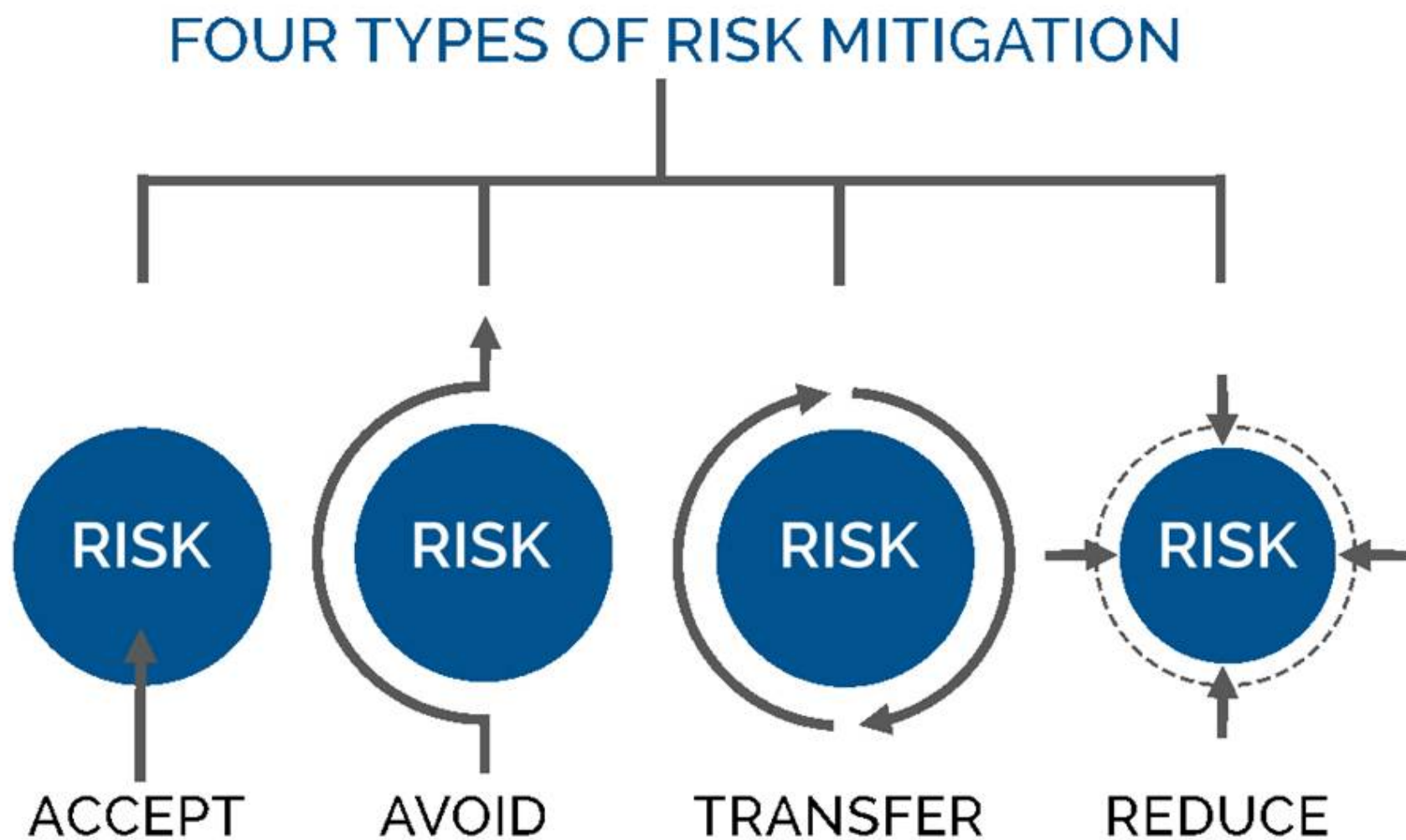
- A. Accept the risk
- B. Introduce more controls to bring risk to 0%
- C. Mitigate the risk
- D. Avoid the risk

Answer: A

Explanation:

Risk Mitigation

Risk mitigation can be defined as taking steps to reduce adverse effects. There are four types of risk mitigation strategies that hold unique to Business Continuity and Disaster Recovery. When mitigating risk, it's important to develop a strategy that closely relates to and matches your company's profile.



A picture containing diagram

Description automatically generated

Risk Acceptance

Risk acceptance does not reduce any effects; however, it is still considered a strategy. This strategy is a common option when the cost of other risk management options such as avoidance or limitation may outweigh the cost of the risk itself. A company that doesn't want to spend a lot of money on avoiding risks that do not have a high possibility of occurring will use the risk acceptance strategy.

Risk Avoidance

Risk avoidance is the opposite of risk acceptance. It is the action that avoids any exposure to the risk whatsoever. It's important to note that risk avoidance is usually the most expensive of all risk mitigation options.

Risk Limitation

Risk limitation is the most common risk management strategy used by businesses. This strategy limits a company's exposure by taking some action. It is a strategy employing a bit of risk acceptance and a bit of risk avoidance or an average of both. An example of risk limitation would be a company accepting that a disk drive may fail and avoiding a long period of failure by having backups.

Risk Transference

Risk transference is the involvement of handing risk off to a willing third party. For example, numerous companies outsource certain operations such as customer service, payroll

services, etc. This can be beneficial for a company if a transferred risk is not a core competency of that company. It can also be used so a company can focus more on its core competencies.

NEW QUESTION 145

- (Topic 1)

Although FTP traffic is not encrypted by default, which layer 3 protocol would allow for end-to-end encryption of the connection?

- A. SFTP
- B. Ipsec
- C. SSL
- D. FTPS

Answer: B

Explanation:

<https://en.wikipedia.org/wiki/IPsec>

Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs). IPsec includes protocols for establishing mutual authentication between agents at the beginning of a session and negotiation of cryptographic keys to use during the session. IPsec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks. It supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection. The initial IPv4 suite was developed with few security provisions. As a part of the IPv4 enhancement, IPsec is a layer 3 OSI model or internet layer end-to-end security scheme. In contrast, while some other Internet security systems in widespread use operate above layer 3, such as Transport Layer Security (TLS) that operates at the Transport Layer and Secure Shell (SSH) that operates at the Application layer, IPsec can automatically secure applications at the IP layer.

NEW QUESTION 146

- (Topic 1)

What is the role of test automation in security testing?

- A. It is an option but it tends to be very expensive.
- B. It should be used exclusively

- C. Manual testing is outdated because of low speed and possible test setup inconsistencies.
- D. Test automation is not usable in security due to the complexity of the tests.
- E. It can accelerate benchmark tests and repeat them with a consistent test setu
- F. But it cannot replace manual testing completely.

Answer: D

NEW QUESTION 147

- (Topic 1)

A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named "nc." The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server's software. The ??ps?? command shows that the ??nc?? file is running as process, and the netstat command shows the ??nc?? process is listening on a network port.

What kind of vulnerability must be present to make this remote attack possible?

- A. File system permissions
- B. Privilege escalation
- C. Directory traversal
- D. Brute force login

Answer: A

Explanation:

File system permissions

Processes may automatically execute specific binaries as part of their functionality or to perform other actions. If the permissions on the file system directory containing a target binary, or permissions on the binary itself, are improperly set, then the target binary may be overwritten with another binary using user-level permissions and executed by the original process. If the original process and thread are running under a higher permissions level, then the replaced binary will also execute under higher-level permissions, which could include SYSTEM.

Adversaries may use this technique to replace legitimate binaries with malicious ones as a means of executing code at a higher permissions level. If the executing process is set to run at a specific time or during a certain event (e.g., system startup) then this technique can also be used for persistence.

NEW QUESTION 152

- (Topic 1)

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 153

- (Topic 1)

An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next?

- A. He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.
- B. He will activate OSPF on the spoofed root bridge.
- C. He will repeat this action so that it escalates to a DoS attack.
- D. He will repeat the same attack against all L2 switches of the network.

Answer: A

NEW QUESTION 156

- (Topic 1)

During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network.

What is this type of DNS configuration commonly called?

- A. DynDNS
- B. DNS Scheme
- C. DNSSEC
- D. Split DNS

Answer: D

NEW QUESTION 159

- (Topic 2)

which of the following information security controls creates an appealing isolated environment for hackers to prevent them from compromising critical targets while simultaneously gathering information about the hacker?

- A. intrusion detection system
- B. Honeypot
- C. Botnet D Firewall

Answer: B

Explanation:

A honeypot may be a trap that an IT pro lays for a malicious hacker, hoping that they will interact with it during a way that gives useful intelligence. It's one among the oldest security measures in IT, but beware: luring hackers onto your network, even on an isolated system, are often a dangerous game. A honeypot may be a good starting place: A honeypot may be a computer or computing system intended to mimic likely targets of cyberattacks. Often a honeypot are going to be deliberately configured with known vulnerabilities in situation to form a more tempting or obvious target for attackers. A honeypot won't contain production data or participate in legitimate traffic on your network — that's how you'll tell anything happening within it's a results of an attack. If someone's stopping by, they're up to no good. That definition covers a various array of systems, from bare-bones virtual machines that only offer a couple of vulnerable systems to ornately constructed fake networks spanning multiple servers. and therefore the goals of these who build honeypots can vary widely also, starting from defense thorough to academic research. additionally, there's now an entire marketing category of deception technology that, while not meeting the strict definition of a honeypot, is certainly within the same family. But we'll get thereto during a moment. Honeypots aim to permit close analysis of how hackers do their dirty work. The team controlling the honeypot can watch the techniques hackers use to infiltrate systems, escalate privileges, and otherwise run amok through target networks. These sorts of honeypots are found out by security companies, academics, and government agencies looking to look at the threat landscape. Their creators could also be curious about learning what kind of attacks are out there, getting details on how specific sorts of attacks work, or maybe trying to lure a specific hackers within the hopes of tracing the attack back to its source. These systems are often inbuilt fully isolated lab environments, which ensures that any breaches don't end in non-honeypot machines falling prey to attacks. Production honeypots, on the opposite hand, are usually deployed in proximity to some organization's production infrastructure, though measures are taken to isolate it the maximum amount as possible. These honeypots often serve both as bait to distract hackers who could also be trying to interrupt into that organization's network, keeping them faraway from valuable data or services; they will also function a canary within the coalpit, indicating that attacks are underway and are a minimum of partially succeeding.

NEW QUESTION 164

- (Topic 2)

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 165

- (Topic 2)

Harry, a professional hacker, targets the IT infrastructure of an organization. After preparing for the attack, he attempts to enter the target network using techniques such as sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Using these techniques, he successfully deployed malware on the target system to establish an outbound connection. What is the APT lifecycle phase that Harry is currently executing?

- A. Preparation
- B. Cleanup
- C. Persistence
- D. initial intrusion

Answer: A

Explanation:

After the attacker completes preparations, subsequent step is an effort to realize an edge within the target's environment. a particularly common entry tactic is that the use of spearphishing emails containing an internet link or attachment. Email links usually cause sites where the target's browser and related software are subjected to varied exploit techniques or where the APT actors plan to social engineer information from the victim which will be used later. If a successful exploit takes place, it installs an initial malware payload on the victim's computer. Figure 2 illustrates an example of a spearphishing email that contains an attachment. Attachments are usually executable malware, a zipper or other archive containing malware, or a malicious Office or Adobe PDF (Portable Document Format) document that exploits vulnerabilities within the victim's applications to ultimately execute malware on the victim's computer. Once the user has opened a malicious file using vulnerable software, malware is executing on the target system. These phishing emails are often very convincing and difficult to differentiate from legitimate email messages. Tactics to extend their believability include modifying legitimate documents from or associated with the organization. Documents are sometimes stolen from the organization or their collaborators during previous exploitation operations. Actors modify the documents by adding exploits and malicious code then send them to the victims. Phishing emails are commonly sent through previously compromised email servers, email accounts at organizations associated with the target or public email services. Emails also can be sent through mail relays with modified email headers to form the messages appear to possess originated from legitimate sources. Exploitation of vulnerabilities on public-facing servers is another favorite technique of some APT groups. Though this will be accomplished using exploits for known vulnerabilities, 0-days are often developed or purchased to be used in intrusions as required. Gaining an edge within the target environment is that the primary goal of the initial intrusion. Once a system is exploited, the attacker usually places malware on the compromised system and uses it as a jump point or proxy for further actions. Malware placed during the initial intrusion phase is usually an easy downloader, basic Remote Access Trojan or an easy shell. Figure 3 illustrates a newly infected system initiating an outbound connection to notify the APT actor that the initial intrusion attempt was successful which it's able to accept commands.

NEW QUESTION 169

- (Topic 2)

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 172

- (Topic 2)

How is the public key distributed in an orderly, controlled fashion so that the users can be sure of the sender's identity?

- A. Hash value
- B. Private key
- C. Digital signature
- D. Digital certificate

Answer: D

NEW QUESTION 174

- (Topic 2)

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: D

NEW QUESTION 176

- (Topic 2)

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 181

- (Topic 2)

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 are 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 are 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 184

- (Topic 2)

You are a penetration tester tasked with testing the wireless network of your client Brakeme SA. You are attempting to break into the wireless network with the SSID "Brakeme-Internal." You realize that this network uses WPA3 encryption, which of the following vulnerabilities is the promising to exploit?

- A. Dragonblood
- B. Cross-site request forgery
- C. Key reinstallation attack
- D. AP Myconfiguration

Answer: A

Explanation:

Dragonblood allows an attacker in range of a password-protected Wi-Fi network to get the password and gain access to sensitive information like user credentials, emails and mastercard numbers. consistent with the published report:??The WPA3 certification aims to secure Wi-Fi networks, and provides several advantages over its predecessor WPA2, like protection against offline dictionary attacks and forward secrecy. Unfortunately, we show that WPA3 is suffering from several design flaws, and analyze these flaws both theoretically and practically. Most prominently, we show that WPA3??s Simultaneous Authentication of Equals (SAE) handshake, commonly referred to as Dragonfly, is suffering from password partitioning attacks.??Our Wi-Fi researchers at WatchGuard are educating businesses globally that WPA3 alone won??t stop the Wi-Fi hacks that allow attackers to steal information over the air (learn more in our recent blog post on the topic). These Dragonblood vulnerabilities impact alittle amount of devices that were released with WPA3 support, and makers are currently making patches available. one among the most important takeaways for businesses of all sizes is to know that a long-term fix might not be technically feasible for devices with lightweight processing capabilities like IoT and embedded systems. Businesses got to consider adding products that enable a Trusted Wireless Environment for all kinds of devices and users alike. Recognizing that vulnerabilities like KRACK and Dragonblood require attackers to initiate these attacks by bringing an ??Evil Twin?? Access Point or a Rogue Access Point into a Wi-Fi environment, we??ve been that specialize in developing Wi-Fi security solutions that neutralize these threats in order that these attacks can never occur. The Trusted Wireless Environment framework protects against the ??Evil Twin?? Access Point and Rogue Access Point. one among these hacks is required to initiate the 2 downgrade or side-channel attacks referenced in Dragonblood. What??s next? WPA3 is an improvement over WPA2 Wi-Fi encryption protocol, however, as we predicted, it still doesn??t provide protection from the six known Wi-Fi threat categories. It??s highly likely that we??ll see more WPA3 vulnerabilities announced within the near future. To help reduce Wi-Fi vulnerabilities, we??re asking all of you to hitch the Trusted Wireless Environment movement and advocate for a worldwide security standard for Wi-Fi.

NEW QUESTION 188

- (Topic 2)

What is one of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS?

- A. Symmetric algorithms such as AES provide a failsafe when asymmetric methods fail.
- B. Asymmetric cryptography is computationally expensive in compariso
- C. However, it is well-suited to securely negotiate keys for use with symmetric cryptography.
- D. Symmetric encryption allows the server to securely transmit the session keys out-of- band.
- E. Supporting both types of algorithms allows less-powerful devices such as mobile phones to use symmetric encryption instead.

Answer: D

NEW QUESTION 190

- (Topic 2)

During an Xmas scan what indicates a port is closed?

- A. No return response
- B. RST
- C. ACK
- D. SYN

Answer: B

NEW QUESTION 192

- (Topic 2)

The Payment Card Industry Data Security Standard (PCI DSS) contains six different categories of control objectives. Each objective contains one or more requirements, which must be followed in order to achieve compliance. Which of the following requirements would best fit under the objective, "Implement strong access control measures"?

- A. Regularly test security systems and processes.
- B. Encrypt transmission of cardholder data across open, public networks.
- C. Assign a unique ID to each person with computer access.
- D. Use and regularly update anti-virus software on all systems commonly affected by malware.

Answer: C

NEW QUESTION 193

- (Topic 2)

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 802.15.4 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 802.15.4 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 195

- (Topic 2)

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 199

- (Topic 2)

in the Common Vulnerability Scoring System (CVSS) v3.1 severity ratings, what range does medium vulnerability fall in?

- A. 3.0-6.9
- B. 4.0-6.0

- C. 4.0-6.9
- D. 3.9-6.9

Answer: C

Explanation:

CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Severity	Base Score Range	Severity	Base Score Range
		None	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

NEW QUESTION 202

- (Topic 2)

which of the following Bluetooth hacking techniques refers to the theft of information from a wireless device through Bluetooth?

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

Answer: D

Explanation:

Bluesnarfing is the unauthorized access of information from a wireless device through aBluetooth connection, often between phones, desktops, laptops, and PDAs (personal digital assistant).

NEW QUESTION 205

- (Topic 2)

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 premiers environment-

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

Answer: A

NEW QUESTION 207

- (Topic 2)

Larry, a security professional in an organization, has noticed some abnormalities In the user accounts on a web server. To thwart evolving attacks, he decided to harden the security of the web server by adopting a countermeasures to secure the accounts on the web server.

Which of the following countermeasures must Larry implement to secure the user accounts on the web server?

- A. Enable unused default user accounts created during the installation of an OS
- B. Enable all non-interactive accounts that should exist but do not require interactive login
- C. Limit the administrator or toot-level access to the minimum number of users
- D. Retain all unused modules and application extensions

Answer: C

NEW QUESTION 208

- (Topic 2)

What is the purpose of DNS AAAA record?

- A. Authorization, Authentication and Auditing record
- B. Address prefix record
- C. Address database record
- D. IPv6 address resolution record

Answer: D

NEW QUESTION 211

- (Topic 2)

Bella, a security professional working at an IT firm, finds that a security breach has occurred while transferring important files. Sensitive data, employee usernames, and passwords are shared in plaintext, paving the way for hackers to perform successful session hijacking. To address this situation, Bella implemented a protocol that sends data using encryption and digital certificates. Which of the following protocols is used by Bella?

- A. FTP
- B. HTTPS
- C. FTPS
- D. IP

Answer: C

Explanation:

The File Transfer Protocol (FTP) is a standard organization convention utilized for the exchange of PC records from a worker to a customer on a PC organization. FTP is based on a customer worker model engineering utilizing separate control and information associations between the customer and the server.[1] FTP clients may validate themselves with an unmistakable book sign-in convention, ordinarily as a username and secret key, however can interface namelessly if the worker is designed to permit it. For secure transmission that ensures the username and secret phrase, and scrambles the substance, FTP is frequently made sure about with SSL/TLS (FTPS) or supplanted with SSH File Transfer Protocol (SFTP).

The primary FTP customer applications were order line programs created prior to working frameworks had graphical UIs, are as yet dispatched with most Windows, Unix, and Linux working systems.[2][3] Many FTP customers and mechanization utilities have since been created for working areas, workers, cell phones, and equipment, and FTP has been fused into profitability applications, for example, HTML editors.

NEW QUESTION 213

- (Topic 2)

Wilson, a professional hacker, targets an organization for financial benefit and plans to compromise its systems by sending malicious emails. For this purpose, he uses a tool to track the emails of the target and extracts information such as sender identities, mail servers, sender IP addresses, and sender locations from different public sources. He also checks if an email address was leaked using the haveibeenpwned.com API. Which of the following tools is used by Wilson in the above scenario?

- A. Factiva
- B. Netcraft
- C. infoga
- D. Zoominfo

Answer: C

Explanation:

Infoga may be a tool gathering email accounts informations (ip,hostname,country,??) from completely different public supply (search engines, pgp key servers and shodan) and check if email was leaked using haveibeenpwned.com API. is a really simple tool, however very effective for the first stages of a penetration test or just to know the visibility of your company within the net.

NEW QUESTION 216

- (Topic 2)

Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days, Bob denies that he had ever sent a mail. What do you want to "know" to prove yourself that it was Bob who had sent a mail?

- A. Authentication
- B. Confidentiality
- C. Integrity
- D. Non-Repudiation

Answer: D

Explanation:

Non-repudiation is the assurance that someone cannot deny the validity of something.

Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data. In other words, non-repudiation makes it very difficult to successfully deny who/where a message came from as well as the authenticity and integrity of that message.

NEW QUESTION 218

- (Topic 2)

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 A
- 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 220

- (Topic 2)

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 because the original sender.

The receiver feels that it??s Associate in Nursing 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, thence 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 221

- (Topic 2)

E-mail scams and mail fraud are regulated by which of the following?

- A. 18 U.S.
- B. pa
- C. 1030 Fraud and Related activity in connection with Computers
- D. 18 U.S.
- E. pa
- F. 1029 Fraud and Related activity in connection with Access Devices
- G. 18 U.S.
- H. pa
- I. 1362 Communication Lines, Stations, or Systems
- J. 18 U.S.
- K. pa
- L. 2510 Wire and Electronic Communications Interception and Interception of Oral Communication

Answer: A

NEW QUESTION 222

- (Topic 2)

Which of the following LM hashes represent a password of less than 8 characters? (Choose two.)

- A. BA810DBA98995F1817306D272A9441BB
- B. 44EFCE164AB921CQAAD3B435B51404EE
- C. 0182BD0BD4444BF836077A718CCDF409
- D. CEC52EB9C8E3455DC2265B23734E0DAC
- E. B757BF5C0D87772FAAD3B435B51404EE
- F. E52CAC67419A9A224A3B108F3FA6CB6D

Answer: BE

NEW QUESTION 225

- (Topic 2)

jane, an ethical hacker. Is testing a target organization's web server and website to identity security loopholes. In this process, she copied the entire website and its content on a local drive to view the complete profile of the site's directory structure, file structure, external links, images, web pages, and so on. This information helps jane map the website's directories and gain valuable information. What is the attack technique employed by Jane in the above scenario?

- A. website mirroring
- B. Session hijacking
- C. Web cache poisoning
- D. Website defacement

Answer: A

Explanation:

A mirror site may be a website or set of files on a computer server that has been copied to a different computer server in order that the location or files are available from quite one place. A mirror site has its own URL, but is otherwise just like the principal site. Load-balancing devices allow high-volume sites to scale easily, dividing the work between multiple mirror sites. A mirror site is typically updated frequently to make sure it reflects the contents of the first site. In some cases, the first site may arrange for a mirror site at a bigger location with a better speed connection and, perhaps, a better proximity to an outsized audience. If the first site generates an excessive amount of traffic, a mirror site can ensure better availability of the web site or files. For websites that provide copies or updates of widely used software, a mirror site allows the location to handle larger demands and enables the downloaded files to arrive more quickly. Microsoft, Sun Microsystems and other companies have mirror sites from which their browser software are often downloaded. Mirror sites are wont to make site access faster when the first site could also be geographically distant from those accessing it. A mirrored web server is usually located on a special continent from the principal site, allowing users on the brink of the mirror site to urge faster and more reliable access. Mirroring an internet site also can be done to make sure that information are often made available to places where access could also be unreliable or censored. In 2013, when Chinese authorities blocked access to foreign media outlets just like the Wall Street Journal and Reuters, site mirroring was wont to restore access and circumvent government censorship.

NEW QUESTION 230

- (Topic 2)

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:

Incident Handling and Response Incident handling and response (IH&R) is the process of taking organized and careful steps when reacting to a security incident or cyberattack. Steps involved in the IH&R process: 3. Incident Triage - The IH&R team further analyzes the compromised device to find incident details such as the type of attack, its severity, target, impact, and method of propagation, and any vulnerabilities it exploited. (P.84/68)

NEW QUESTION 232

- (Topic 2)

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 235

- (Topic 2)

What is the main security service a cryptographic hash provides?

- A. Integrity and ease of computation
- B. Message authentication and collision resistance
- C. Integrity and collision resistance
- D. Integrity and computational in-feasibility

Answer: D

NEW QUESTION 240

- (Topic 2)

What do Trinoo, TFN2k, WinTrinoo, T-Sight, and Stracheldraht have in common?

- A. All are hacking tools developed by the legion of doom
- B. All are tools that can be used not only by hackers, but also security personnel
- C. All are DDOS tools
- D. All are tools that are only effective against Windows
- E. All are tools that are only effective against Linux

Answer: C

NEW QUESTION 242

- (Topic 2)

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: B

Explanation:

https://ru.wikipedia.org/wiki/DNS_spoofing

DNS spoofing is a threat that copies the legitimate server destinations to divert the domain's traffic. Ignorant these attacks, the users are redirected to malicious websites, which results in insensitive and personal data being leaked. It is a method of attack where your DNS server is tricked into saving a fake DNS entry. This will make the DNS server recall a fake site for you, thereby posing a threat to vital information stored on your server or computer.

The cache poisoning codes are often found in URLs sent through spam emails. These emails are sent to prompt users to click on the URL, which infects their computer. When the computer is poisoned, it will divert you to a fake IP address that looks like a real thing. This way, the threats are injected into your systems as well.

Different Stages of Attack of DNS Cache Poisoning:

- The attacker proceeds to send DNS queries to the DNS resolver, which forwards the Root/TLD authoritative DNS server request and awaits an answer.
- The attacker overloads the DNS with poisoned responses that contain several IP addresses of the malicious website. To be accepted by the DNS resolver, the attacker's response should match a port number and the query ID field before the DNS response. Also, the attackers can force its response to increasing their

chance of success.

- If you are a legitimate user who queries this DNS resolver, you will get a poisoned response from the cache, and you will be automatically redirected to the malicious website.

NEW QUESTION 243

- (Topic 2)

Bob is going to perform an active session hijack against Brownies Inc. He has found a target that allows session oriented connections (Telnet) and performs the sequence prediction on the target operating system. He manages to find an active session due to the high level of traffic on the network. What is Bob supposed to do next?

- A. Take over the session
- B. Reverse sequence prediction
- C. Guess the sequence numbers
- D. Take one of the parties offline

Answer: C

NEW QUESTION 246

- (Topic 2)

Clark is a professional hacker. He created and configured multiple domains pointing to the same host to switch quickly between the domains and avoid detection. Identify the behavior of the adversary In the above scenario.

- A. use of command-line interface
- B. Data staging
- C. Unspecified proxy activities
- D. Use of DNS tunneling

Answer: C

Explanation:

A proxy server acts as a gateway between you and therefore the internet. It's an intermediary server separating end users from the websites they browse. Proxy servers provide varying levels of functionality, security, and privacy counting on your use case, needs, or company policy. If you're employing a proxy server, internet traffic flows through the proxy server on its thanks to the address you requested. A proxy server is essentially a computer on the web with its own IP address that your computer knows. once you send an internet request, your request goes to the proxy server first. The proxy server then makes your web request on your behalf, collects the response from the online server, and forwards you the online page data so you'll see the page in your browser.

NEW QUESTION 250

- (Topic 2)

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 ONS 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 Who is 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 255

- (Topic 2)

This kind of password cracking method uses word lists in combination with numbers and special characters:

- A. Hybrid
- B. Linear
- C. Symmetric
- D. Brute Force

Answer: A

NEW QUESTION 259

- (Topic 2)

Johnson, an attacker, performed online research for the contact details of reputed cybersecurity firms. He found the contact number of sibertech.org and dialed the number, claiming himself to represent a technical support team from a vendor. He warned that a specific server is about to be compromised and requested sibertech.org to follow the provided instructions. Consequently, he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical Information to Johnson's machine. What is the social engineering technique Steve employed in the above scenario?

- A. Quid pro quo
- B. Diversion theft
- C. Elicitation
- D. Phishing

Answer: A

Explanation:

<https://www.eccouncil.org/what-is-social-engineering/>

This Social Engineering scam involves an exchange of information that can benefit both the victim and the trickster. Scammers would make the prey believe that a fair exchange will be present between both sides, but in reality, only the fraudster stands to benefit, leaving the victim hanging on to nothing. An example of a Quid Pro Quo is a scammer pretending to be an IT support technician. The con artist asks for the login credentials of the company's computer saying that the company is going to receive technical support in return. Once the victim has provided the credentials, the scammer now has control over the company's computer and may possibly load malware or steal personal information that can be a motive to commit identity theft.

"A quid pro quo attack (aka something for something?? attack) is a variant of baiting. Instead of baiting a target with the promise of a good, a quid pro quo attack promises a service or a benefit based on the execution of a specific action." <https://resources.infosecinstitute.com/topic/common-social-engineering-attacks/#:~:text=A%20quid%20pro%20quo%20attack,execution%20of%20a%20specific%20action.>

NEW QUESTION 264

- (Topic 2)

A friend of yours tells you that he downloaded and executed a file that was sent to him by a coworker. Since the file did nothing when executed, he asks you for help because he suspects that he may have installed a trojan on his computer. what tests would you perform to determine whether his computer Is Infected?

- A. Use ExifTool and check for malicious content.
- B. You do not check; rather, you immediately restore a previous snapshot of the operating system.
- C. Upload the file to VirusTotal.
- D. Use netstat and check for outgoing connections to strange IP addresses or domains.

Answer: D

NEW QUESTION 269

- (Topic 2)

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 271

- (Topic 2)

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. Mypervisor 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 273

- (Topic 2)

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

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

Answer: D

NEW QUESTION 274

- (Topic 2)

What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?

- A. Copy the system files from a known good system
- B. Perform a trap and trace
- C. Delete the files and try to determine the source
- D. Reload from a previous backup
- E. Reload from known good media

Answer: E

NEW QUESTION 277

- (Topic 2)

Steven connected his iPhone to a public computer that had been infected by Clark, an attacker. After establishing the connection with the public computer, Steven enabled iTunes Wi-Fi sync on the computer so that the device could continue communication with that computer even after being physically disconnected. Now, Clark gains access to Steven's iPhone through the infected computer and is able to monitor and read all of Steven's activity on the iPhone, even after the device is out of the communication zone.

Which of the following attacks is performed by Clark in above scenario?

- A. IOS trustjacking
- B. IOS Jailbreaking
- C. Exploiting SS7 vulnerability
- D. Man-in-the-disk attack

Answer: A

Explanation:

An iPhone client's most noticeably terrible bad dream is to have somebody oversee his/her gadget, including the capacity to record and control all action without waiting be in a similar room. In this blog entry, we present another weakness called ??Trustjacking??, which permits an aggressor to do precisely that.

This weakness misuses an iOS highlight called iTunes Wi-Fi sync, which permits a client to deal with their iOS gadget without genuinely interfacing it to their PC. A solitary tap by the iOS gadget proprietor when the two are associated with a similar organization permits an assailant to oversee the gadget. Furthermore, we will stroll through past related weaknesses and show the progressions that iPhone has made to alleviate them, and why these are adequately not to forestall comparative assaults.

After interfacing an iOS gadget to another PC, the clients are being found out if they trust the associated PC or not. Deciding to believe the PC permits it to speak with the iOS gadget by means of the standard iTunes APIs.

This permits the PC to get to the photographs on the gadget, perform reinforcement, introduce applications and considerably more, without requiring another affirmation from the client and with no recognizable sign. Besides, this permits enacting the ??iTunes Wi-Fi sync?? highlight, which makes it conceivable to proceed with this sort of correspondence

with the gadget even after it has been detached from the PC, as long as the PC and the iOS gadget are associated with a similar organization. It is intriguing to take note of that empowering ??iTunes Wi-Fi sync?? doesn't need the casualty's endorsement and can be directed simply from the PC side.

Getting a live stream of the gadget's screen should be possible effectively by consistently requesting screen captures and showing or recording them distantly.

It is imperative to take note of that other than the underlying single purpose of disappointment, approving the vindictive PC, there is no other component that forestalls this proceeded with access. Likewise, there isn't anything that informs the clients that by approving the PC they permit admittance to their gadget even in the wake of detaching the USB link.

NEW QUESTION 281

- (Topic 2)

Which of the following commands checks for valid users on an SMTP server?

- A. RCPT
- B. CHK
- C. VRFY
- D. EXPN

Answer: C

Explanation:

The VRFY commands enables SMTP clients to send an invitation to an SMTP server to verify that mail for a selected user name resides on the server. The VRFY command is defined in RFC 821. The server sends a response indicating whether the user is local or not, whether mail are going to be forwarded, and so on. A response of 250 indicates that the user name is local; a response of 251 indicates that the user name isn't local, but the server can forward the message. The server response includes the mailbox name.

NEW QUESTION 283

- (Topic 2)

Security administrator John Smith has noticed abnormal amounts of traffic coming from local computers at night. Upon reviewing, he finds that user data have been exfiltrated by an attacker. AV tools are unable to find any malicious software, and the IDS/IPS has not reported on any non-whitelisted programs, what type of malware did the attacker use to bypass the company's application whitelisting?

- A. Phishing malware
- B. Zero-day malware
- C. File-less malware
- D. Logic bomb malware

Answer: C

Explanation:

<https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html>

Fileless malware can easily evade various security controls, organizations need to focus on monitoring, detecting, and preventing malicious activities instead of using traditional approaches such as scanning for malware through file signatures. Also known as non- malware, infects legitimate software, applications, and other protocols existing in the system to perform various malicious activities. It resides in the system's RAM. It injects malicious code into the running processes.

(P.966/950)

NEW QUESTION 286

- (Topic 2)

In this attack, a victim receives an e-mail claiming from PayPal stating that their account has been disabled and confirmation is required before activation. The attackers then scam to collect not one but two credit card numbers, ATM PIN number and other personal details. Ignorant users usually fall prey to this scam. Which of the following statement is incorrect related to this attack?

- A. Do not reply to email messages or popup ads asking for personal or financial information
- B. Do not trust telephone numbers in e-mails or popup ads
- C. Review credit card and bank account statements regularly
- D. Antivirus, anti-spyware, and firewall software can very easily detect these type of attacks
- E. Do not send credit card numbers, and personal or financial information via e-mail

Answer: D

NEW QUESTION 291

- (Topic 2)

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 is 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 294

- (Topic 2)

What port number is used by LDAP protocol?

- A. 110
- B. 389
- C. 464
- D. 445

Answer: B

NEW QUESTION 297

- (Topic 2)

A newly joined employee, Janet, has been allocated an existing system used by a previous employee. Before issuing the system to Janet, it was assessed by Martin, the administrator. Martin found that there were possibilities of compromise through user directories, registries, and other system parameters. He also identified vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. What is the type of vulnerability assessment performed by Martin?

- A. Credentialed assessment
- B. Database assessment
- C. Host-based assessment
- D. Distributed assessment

Answer: C

Explanation:

The host-based vulnerability assessment (VA) resolution arose from the auditors' got to periodically review systems. Arising before the net becoming common, these tools typically take an administrator's eye read of the setting by evaluating all of the knowledge that an administrator has at his or her disposal. Uses Host VA tools verify system configuration, user directories, file systems, registry settings, and all forms of other info on a number to gain information about it. Then, it evaluates the chance of compromise. it should also live compliance to a predefined company policy so as to satisfy an annual audit. With administrator access, the scans are unit less possible to disrupt traditional operations since the computer code has the access it has to see into the complete configuration of the system.

What it Measures Host

VA tools will examine the native configuration tables and registries to spot not solely apparent vulnerabilities, however additionally dormant vulnerabilities – those weak or misconfigured systems and settings which will be exploited when an initial entry into the setting. Host VA solutions will assess the safety settings of a user account table; the access management lists related to sensitive files or data; and specific levels of trust applied to other systems. The host VA resolution will a lot of accurately verify the extent of the danger by determinant however way any specific exploit could also be ready to get.

Types of Vulnerability Assessment Host-based assessments are a type of security check that involve conducting a configuration-level check to identify system configurations, user directories, file systems, registry settings, and other parameters to evaluate the possibility of compromise. Host-based scanners assess systems to identify vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. (P.528/512)

NEW QUESTION 301

- (Topic 2)

Ralph, a professional hacker, targeted Jane, who had recently bought new systems for her company. After a few days, Ralph contacted Jane while masquerading as a legitimate customer support executive, informing that her systems need to be serviced for proper functioning and that customer support will send a computer technician. Jane promptly replied positively. Ralph entered Jane's company using this opportunity and gathered sensitive information by scanning terminals for

passwords, searching for important documents in desks, and rummaging bins. What is the type of attack technique Ralph used on Jane?

- A. Dumpster diving
- B. Eavesdropping
- C. Shoulder surfing
- D. impersonation

Answer: D

NEW QUESTION 302

- (Topic 2)

What are common files on a web server that can be misconfigured and provide useful information for a hacker such as verbose error messages?

- A. httpd.conf
- B. administration.config
- C. idq.dll
- D. php.ini

Answer: D

Explanation:

The php.ini file may be a special file for PHP. It's where you declare changes to your PHP settings. The server is already configured with standard settings for PHP, which your site will use by default. Unless you would like to vary one or more settings, there's no need to create or modify a php.ini file. If you'd wish to make any changes to settings, please do so through the MultiPHP INI Editor.

NEW QUESTION 306

- (Topic 2)

You work for Acme Corporation as Sales Manager. The company has tight network security restrictions. You are trying to steal data from the company's Sales database (Sales.xls) and transfer them to your home computer. Your company filters and monitors traffic that leaves from the internal network to the Internet. How will you achieve this without raising suspicion?

- A. Encrypt the Sales.xls using PGP and e-mail it to your personal gmail account
- B. Package the Sales.xls using Trojan wrappers and telnet them back your home computer
- C. You can conceal the Sales.xls database in another file like photo.jpg or other files and send it out in an innocent looking email or file transfer using Steganography techniques
- D. Change the extension of Sales.xls to sales.txt and upload them as attachment to your hotmail account

Answer: C

NEW QUESTION 309

- (Topic 2)

Bill is a network administrator. He wants to eliminate unencrypted traffic inside his company's network. He decides to setup a SPAN port and capture all traffic to the datacenter. He immediately discovers unencrypted traffic in port UDP 161. What protocol is this port using and how can he secure that traffic?

- A. It is not necessary to perform any actions, as SNMP is not carrying important information.
- B. SNMP and he should change it to SNMP V3
- C. RPC and the best practice is to disable RPC completely
- D. SNMP and he should change it to SNMP v2, which is encrypted

Answer: B

Explanation:

We have various articles already in our documentation for setting up SNMPv2 trap handling in Opsview, but SNMPv3 traps are a whole new ballgame. They can be quite confusing and complicated to set up the first time you go through the process, but when you understand what is going on, everything should make more sense. SNMP has gone through several revisions to improve performance and security (version 1, 2c and 3). By default, it is a UDP port based protocol where communication is based on a "fire and forget" methodology in which network packets are sent to another device, but there is no check for receipt of that packet (versus TCP port when a network packet must be acknowledged by the other end of the communication link). There are two modes of operation with SNMP – get requests (or polling) where one device requests information from an SNMP enabled device on a regular basis (normally using UDP port 161), and traps where the SNMP enabled device sends a message to another device when an event occurs (normally using UDP port 162). The latter includes instances such as someone logging on, the device powering up or down, or a wide variety of other problems that would need this type of investigation. This blog covers SNMPv3 traps, as polling and version 2c traps are covered elsewhere in our documentation. SNMP traps Since SNMP is primarily a UDP port based system, traps may be "lost" when sending between devices; the sending device does not wait to see if the receiver got the trap. This means if the configuration on the sending device is wrong (using the wrong receiver IP address or port) or the receiver isn't listening for traps or rejecting them out of hand due to misconfiguration, the sender will never know. The SNMP v2c specification introduced the idea of splitting traps into two types; the original "hope it gets there" trap and the newer "INFORM" traps. Upon receipt of an INFORM, the receiver must send an acknowledgement back. If the sender doesn't get the acknowledgement back, then it knows there is an existing problem and can log it for sysadmins to find when they interrogate the device.

NEW QUESTION 313

- (Topic 2)

In the context of Windows Security, what is a 'null' user?

- A. A user that has no skills
- B. An account that has been suspended by the admin
- C. A pseudo account that has no username and password
- D. A pseudo account that was created for security administration purpose

Answer: C

NEW QUESTION 315

- (Topic 2)

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

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

How would you protect from these attacks?

- A. 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 319

- (Topic 2)

Henry is a cyber security specialist hired by BlackEye - Cyber security solutions. He was tasked with discovering the operating system (OS) of a host. He used the Unkornscan tool to discover the OS of the target system. As a result, he obtained a TTL value, which indicates that the target system is running a Windows OS. Identify the TTL value Henry obtained, which indicates that the target OS is Windows.

- A. 64
- B. 128
- C. 255
- D. 138

Answer: B

Explanation:

Windows TTL 128, Linux TTL 64, OpenBSD 255 ... <https://subinsb.com/default-device-ttl-values/>

Time to Live (TTL) represents the number of 'hops' a packet can take before it is considered invalid. For Windows/Windows Phone, this value is 128. This value is 64 for Linux/Android.

NEW QUESTION 323

- (Topic 2)

Alice, a professional hacker, targeted an organization's cloud services. She infiltrated the target's MSP provider by sending spear-phishing emails and distributed custom-made malware to compromise user accounts and gain remote access to the cloud service. Further, she accessed the target customer profiles with her MSP account, compressed the customer data, and stored them in the MSP. Then, she used this information to launch further attacks on the target organization. Which of the following cloud attacks did Alice perform in the above scenario?

- A. Cloud hopper attack
- B. Cloud cryptojacking
- C. Cloudborne attack
- D. Man-in-the-cloud (MITC) attack

Answer: A

Explanation:

Operation Cloud Hopper was an in-depth attack and theft of data in 2017 directed at MSP within the UK (U.K.), US (U.S.), Japan, Canada, Brazil, France, Switzerland, Norway, Finland, Sweden, South Africa, India, Thailand, South Korea, and Australia. The group used MSP as intermediaries to accumulate assets and trade secrets from MSP client engineering, MSP industrial manufacturing, retail, energy, pharmaceuticals, telecommunications, and government agencies. Operation Cloud Hopper used over 70 variants of backdoors, malware, and trojans. These were delivered through spear-phishing emails. The attacks scheduled tasks or leveraged services/utilities to continue Microsoft Windows systems albeit the PC system was rebooted. It installed malware and hacking tools to access systems and steal data.

NEW QUESTION 325

- (Topic 2)

Susan, a software developer, wants her web API to update other applications with the latest information. For this purpose, she uses a user-defined HTTP tailback or push APIs that are raised based on trigger events: when invoked, this feature supplies data to other applications so that users can instantly receive real-time information.

Which of the following techniques is employed by Susan?

- A. web shells
- B. Webhooks
- C. REST API
- D. SOAP API

Answer: B

Explanation:

Webhooks are one of a few ways internet applications will communicate with one another. It allows you to send real-time data from one application to another whenever a given event happens. For example, let's say you've created an application using the Foursquare API that tracks when people check into your restaurant. You ideally wish to be able to greet customers by name and provide a complimentary drink when they check in. What a webhook will is notify you any time someone checks in, therefore you'd be able to run any processes that you simply had in your application once this event is triggered. The data is then sent over the web from the application wherever the event originally occurred, to the receiving application that handles the data. Here's a visual representation of what that looks like:



A webhook url is provided by the receiving application, and acts as a phone number that the other application will call once an event happens. Only it's more complicated than a phone number, because data about the event is shipped to the webhook url in either JSON or XML format. this is known as the payload. Here's an example of what a webhook url looks like with the payload it's carrying:



What are Webhooks? Webhooks are user-defined HTTP callback or push APIs that are raised based on events triggered, such as comment received on a post and pushing code to the registry. A webhook allows an application to update other applications with the latest information. Once invoked, it supplies data to the other applications, which means that users instantly receive real-time information. Webhooks are sometimes called "Reverse APIs" as they provide what is required for API specification, and the developer should create an API to use a webhook. A webhook is an API concept that is also used to send text messages and notifications to mobile numbers or email addresses from an application when a specific event is triggered. For instance, if you search for something in the online store and the required item is out of stock, you click on the "Notify me" bar to get an alert from the application when that item is available for purchase. These notifications from the applications are usually sent through webhooks.

NEW QUESTION 329

- (Topic 2)

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 330

- (Topic 2)

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

Explanation:

Information Gathering from Robots.txt File A website owner creates a robots.txt file to list the files or directories a web crawler should index for providing search results. Poorly written robots.txt files can cause the complete indexing of website files and directories. If confidential files and directories are indexed, an attacker may easily obtain information such as passwords, email addresses, hidden links, and membership areas. If the owner of the target website writes the robots.txt file without allowing the indexing of restricted pages for providing search results, an attacker can still view the robots.txt file of the site to discover restricted files and then view them to gather information. An attacker types URL/robots.txt in the address bar of a browser to view the target website's robots.txt file. An attacker can also download the robots.txt file of a target website using the Wget tool. Certified Ethical Hacker(CEH) Version 11 pg 1650

NEW QUESTION 332

- (Topic 2)

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 335

- (Topic 2)

There have been concerns in your network that the wireless network component is not sufficiently secure. You perform a vulnerability scan of the wireless network and find that it is using an old encryption protocol that was designed to mimic wired encryption, what encryption protocol is being used?

- A. WEP
- B. RADIUS
- C. WPA
- D. WPA3

Answer: A

Explanation:

Wired Equivalent Privacy (WEP) may be a security protocol, laid out in the IEEE wireless local area network (Wi-Fi) standard, 802.11b, that's designed to supply a wireless local area network (WLAN) with A level of security and privacy like what's usually expected of a wired LAN. A wired local area network (LAN) is usually protected by physical security mechanisms (controlled access to a building, for example) that are effective for a controlled physical environment, but could also be ineffective for WLANs because radio waves aren't necessarily bound by the walls containing the network. WEP seeks to determine similar protection thereto offered by the wired network's physical security measures by encrypting data transmitted over the WLAN. encoding protects the vulnerable wireless link between clients and access points; once this measure has been taken, other typical LAN security mechanisms like password protection, end-to-end encryption, virtual private networks (VPNs), and authentication are often put in situ to make sure privacy. A research group from the University of California at Berkeley recently published a report citing ??major security flaws?? in WEP that left WLANs using the protocol susceptible to attacks (called wireless equivalent privacy attacks). within the course of the group's examination of the technology, they were ready to intercept and modify transmissions and gain access to restricted networks. The Wireless Ethernet Compatibility Alliance (WECA) claims that WEP– which is included in many networking products – was never intended to be the only security mechanism for a WLAN, and that, in conjunction with traditional security practices, it's very effective.

NEW QUESTION 340

- (Topic 2)

Alice needs to send a confidential document to her coworker. Bryan. Their company has public key infrastructure set up. Therefore. Alice both encrypts the message and digitally signs it. Alice uses to encrypt the message, and Bryan uses to confirm the digital signature.

- A. Bryan's public key; Bryan's public key
- B. Alice's public key; Alice's public key
- C. Bryan's private key; Alice's public key
- D. Bryan's public key; Alice's public key

Answer: D

Explanation:

PKI uses public-key cryptography, which is widely used on the Internet to encrypt messages or authenticate message senders. In public-key cryptography, a CA generates public and private keys with the same algorithm simultaneously. The private key is held only by the subject (user, company, or system) mentioned in the certificate, while the public key is made publicly available in a directory that all parties can access. The subject keeps the private key secret and uses it to decrypt the text encrypted by someone else using the corresponding public key (available in a public directory). Thus, others encrypt messages for the user with the user's

public key, and the user decrypts it with his/her private key.

NEW QUESTION 344

- (Topic 2)

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 347

- (Topic 2)

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 348

.....

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

312-50v13 Practice Exam Features:

- * 312-50v13 Questions and Answers Updated Frequently
- * 312-50v13 Practice Questions Verified by Expert Senior Certified Staff
- * 312-50v13 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 312-50v13 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 312-50v13 Practice Test Here](#)