

EC-Council

Exam Questions 312-50v12

Certified Ethical Hacker Exam



NEW QUESTION 1

- (Exam Topic 3)

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

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

Answer: A**NEW QUESTION 2**

- (Exam Topic 3)

Insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key. Suppose a malicious user Rob tries to get access to the account of a benign user Ned.

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

- A. "GET /restricted/goldtransfer?to=Rob&from=1 or 1=1' HTTP/1.1Host: westbank.com"
- B. "GET /restricted/\r\n\%00account%00Ned%00access HTTP/1.1 Host: westbank.com"
- C. "GET /restricted/accounts/?name=Ned HTTP/1.1 Host westbank.com"
- D. "GET /restricted/ HTTP/1.1 Host: westbank.com"

Answer: C**Explanation:**

This question shows a classic example of an IDOR vulnerability. Rob substitutes Ned's name in the "name" parameter and if the developer has not fixed this vulnerability, then Rob will gain access to Ned's account. Below you will find more detailed information about IDOR vulnerability.

Insecure direct object references (IDOR) are a cybersecurity issue that occurs when a web application developer uses an identifier for direct access to an internal implementation object but provides no additional access control and/or authorization checks. For example, an IDOR vulnerability would happen if the URL of a transaction could be changed through client-side user input to show unauthorized data of another transaction.

Most web applications use simple IDs to reference objects. For example, a user in a database will usually be referred to via the user ID. The same user ID is the primary key to the database column containing user information and is generated automatically. The database key generation algorithm is very simple: it usually uses the next available integer. The same database ID generation mechanisms are used for all other types of database records.

The approach described above is legitimate but not recommended because it could enable the attacker to enumerate all users. If it's necessary to maintain this approach, the developer must at least make absolutely sure that more than just a reference is needed to access resources. For example, let's say that the web application displays transaction details using the following URL:

> <https://www.example.com/transaction.php?id=74656>

A malicious hacker could try to substitute the id parameter value 74656 with other similar values, for example

> <https://www.example.com/transaction.php?id=74657>

The 74657 transaction could be a valid transaction belonging to another user. The malicious hacker should not be authorized to see it. However, if the developer made an error, the attacker would see this transaction and hence we would have an insecure direct object reference vulnerability.

NEW QUESTION 3

- (Exam Topic 3)

Which type of malware spreads from one system to another or from one network to another and causes similar types of damage as viruses do to the infected system?

- A. Rootkit
- B. Trojan
- C. Worm
- D. Adware

Answer: C**NEW QUESTION 4**

- (Exam Topic 3)

Harper, a software engineer, is developing an email application. To ensure the confidentiality of email messages, Harper uses a symmetric-key block cipher having a classical 12- or 16-round Feistel network with a block size of 64 bits for encryption, which includes large 8 x 32-bit S-boxes (S1, S2, S3, S4) based on bent functions, modular addition and subtraction, key-dependent rotation, and XOR operations. This cipher also uses a masking key(Km1)and a rotation key (Kr1) for performing its functions. What is the algorithm employed by Harper to secure the email messages?

- A. CAST-128
- B. AES
- C. GOST block cipher
- D. DES

Answer: A**NEW QUESTION 5**

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 6

- (Exam Topic 3)

You have been authorized to perform a penetration test against a website. You want to use Google dorks to footprint the site but only want results that show file extensions. What Google dork operator would you use?

- A. filetype
- B. ext
- C. inurl
- D. site

Answer: A

Explanation:

Restrict results to those of a certain filetype. E.g., PDF, DOCX, TXT, PPT, etc. Note: The "ext:" operator can also be used—the results are identical.

Example: apple filetype:pdf / apple ext:pdf

NEW QUESTION 7

- (Exam Topic 3)

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

- A. Cross-site scripting vulnerability
- B. SQL injection vulnerability
- C. Web site defacement vulnerability
- D. Cross-site Request Forgery vulnerability

Answer: A

Explanation:

There is no single, standardized classification of cross-site scripting flaws, but most experts distinguish between at least two primary flavors of XSS flaws: non-persistent and persistent. In this issue, we consider the non-persistent cross-site scripting vulnerability.

The non-persistent (or reflected) cross-site scripting vulnerability is by far the most basic type of web vulnerability. These holes show up when the data provided by a web client, most commonly in HTTP query parameters (e.g. HTML form submission), is used immediately by server-side scripts to parse and display a page of results for and to that user, without properly sanitizing the content.

Because HTML documents have a flat, serial structure that mixes control statements, formatting, and the actual content, any non-validated user-supplied data included in the resulting page without proper HTML encoding, may lead to markup injection. A classic example of a potential vector is a site search engine: if one searches for a string, the search string will typically be redisplayed verbatim on the result page to indicate what was searched for. If this response does not properly escape or reject HTML control characters, a cross-site scripting flaw will ensue.

NEW QUESTION 8

- (Exam Topic 3)

John, a professional hacker, decided to use DNS to perform data exfiltration on a target network, in this process, he embedded malicious data into the DNS protocol packets that even DNSSEC cannot detect. Using this technique, John successfully injected malware to bypass a firewall and maintained communication with the victim machine and C&C server. What is the technique employed by John to bypass the firewall?

- A. DNS cache snooping
- B. DNSSEC zone walking
- C. DNS tunneling method
- D. DNS enumeration

Answer: C

Explanation:

DNS tunneling may be a method used to send data over the DNS protocol, a protocol which has never been intended for data transfer. Due to that, people tend to overlook it and it's become a well-liked but effective tool in many attacks. Most popular use case for DNS tunneling is obtaining free internet through bypassing captive portals at airports, hotels, or if you are feeling patient the not-so-cheap on the wing Wi-Fi. On those shared internet hotspots HTTP traffic is blocked until a username/password is provided, however DNS traffic is usually still allowed within the background: we will encode our HTTP traffic over DNS and voilà, we've internet access. This sounds fun but reality is, browsing anything on DNS tunneling is slow. Like, back to 1998 slow. Another more dangerous use of DNS tunneling would be bypassing network security devices (Firewalls, DLP appliances...) to line up an immediate and unmonitored communications channel on an organisation's network. Possibilities here are endless: Data exfiltration, fixing another penetration testing tool... you name it. To make it even more worrying, there's an outsized amount of easy to use DNS tunneling tools out there. There's even a minimum of one VPN over DNS protocol provider (warning: the planning of the web site is hideous, making me doubt on the legitimacy of it). As a pentester all this is often great, as a network admin not such a lot.

How does it work: For those that ignoramus about DNS protocol but still made it here, I feel you deserve a really brief explanation on what DNS does: DNS is sort of a phonebook for the web, it translates URLs (human-friendly language, the person's name), into an IP address (machine-friendly language, the phone number). That helps us remember many websites, same as we will remember many people's names. For those that know what DNS is I might suggest looking here for a fast refresh on DNS protocol, but briefly what you would like to understand is:

- A Record: Maps a website name to an IP address. example.com ? 12.34.52.67
- NS Record (a.k.a. Nameserver record): Maps a website name to an inventory of DNS servers, just in case our website is hosted in multiple servers. example.com ? server1.example.com, server2.example.com
- Who is involved in DNS tunneling?
 - Client. Will launch DNS requests with data in them to a website.
 - One Domain that we will configure. So DNS servers will redirect its requests to an outlined server of our own.
 - Server. This is often the defined nameserver which can ultimately receive the DNS requests.

The 6 Steps in DNS tunneling (simplified):

1. The client encodes data during a DNS request. The way it does this is often by prepending a bit of knowledge within the domain of the request. For instance: mypieceofdata.server1.example.com
2. The DNS request goes bent a DNS server.
3. The DNS server finds out the A register of your domain with the IP address of your server.
4. The request for

mypieceofdata.server1.example.com is forwarded to the server.5. The server processes regardless of the mypieceofdata was alleged to do. Let's assume it had been an HTTP request.6. The server replies back over DNS and woop woop, we've got signal.

Bypassing Firewalls through the DNS Tunneling Method DNS operates using UDP, and it has a 255-byte limit on outbound queries. Moreover, it allows only alphanumeric characters and hyphens. Such small size constraints on external queries allow DNS to be used as an ideal choice to perform data exfiltration by various malicious entities. Since corrupt or malicious data can be secretly embedded into the DNS protocol packets, even DNSSEC cannot detect the abnormality in DNS tunneling. It is effectively used by malware to bypass the firewall to maintain communication between the victim machine and the C&C server. Tools such as NSTX (<https://sourceforge.net>), Heyoka (<http://heyoka.sourceforge.net>), and Iodine (<https://code.kryo.se>) use this technique of tunneling traffic across DNS port 53. CEH v11 Module 12 Page 994

NEW QUESTION 9

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 10

- (Exam Topic 3)

Roma is a member of a security team. She was tasked with protecting the internal network of an organization from imminent threats. To accomplish this task, Roma fed threat intelligence into the security devices in a digital format to block and identify inbound and outbound malicious traffic entering the organization's network.

Which type of threat intelligence is used by Roma to secure the internal network?

- A. Technical threat intelligence
- B. Operational threat intelligence
- C. Tactical threat intelligence
- D. Strategic threat intelligence

Answer: A

NEW QUESTION 10

- (Exam Topic 3)

To create a botnet, the attacker can use several techniques to scan vulnerable machines. The attacker first collects information about a large number of vulnerable machines to create a list. Subsequently, they infect the machines. The list is divided by assigning half of the list to the newly compromised machines. The scanning process runs simultaneously. This technique ensures the spreading and installation of malicious code in little time.

Which technique is discussed here?

- A. Hit-list-scanning technique
- B. Topological scanning technique
- C. Subnet scanning technique
- D. Permutation scanning technique

Answer: A

Explanation:

One of the biggest problems a worm faces in achieving a very fast rate of infection is "getting off the ground." although a worm spreads exponentially throughout the early stages of infection, the time needed to infect say the first 10,000 hosts dominates the infection time.

There is a straightforward way for an active worm to overcome this obstacle, that we term hit-list scanning. Before the worm is free, the worm author collects a listing of say ten,000 to 50,000 potentially vulnerable machines, ideally ones with sensible network connections. The worm, when released onto an initial machine on this hit-list, begins scanning down the list. once it infects a machine, it divides the hit-list in half, communicating half to the recipient worm, keeping the other half.

This fast division ensures that even if only 10-20% of the machines on the hit-list are actually vulnerable, an active worm can quickly bear the hit-list and establish itself on all vulnerable machines in only some seconds. though the hit-list could begin at 200 kilobytes, it quickly shrinks to nothing during the partitioning. This provides a great benefit in constructing a quick worm by speeding the initial infection.

The hit-list needn't be perfect: a simple list of machines running a selected server sort could serve, though larger accuracy can improve the unfold. The hit-list itself is generated victimization one or many of the following techniques, ready well before, typically with very little concern of detection.

➤ Stealthy scans. Portscans are so common and then wide ignored that even a quick scan of the whole net would be unlikely to attract law enforcement attention or over gentle comment within the incident response community. However, for attackers wish to be particularly careful, a randomised sneaky scan taking many months would be not possible to attract much attention, as most intrusion detection systems are not currently capable of detecting such low-profile scans. Some portion of the scan would be out of date by the time it had been used, however abundant of it'd not.

➤ Distributed scanning. an assailant might scan the web using a few dozen to some thousand already-compromised "zombies," the same as what DDOS attackers assemble in a very fairly routine fashion. Such distributed scanning has already been seen within the wild—Lawrence Berkeley National Laboratory received ten throughout the past year.

➤ DNS searches. Assemble a list of domains (for example, by using wide offered spam mail lists, or trolling the address registries). The DNS will then be searched for the science addresses of mail-servers (via mx records) or net servers (by looking for www.domain.com).

➤ Spiders. For net server worms (like Code Red), use Web-crawling techniques the same as search engines so as to produce a list of most Internet-connected web sites. this would be unlikely to draw in serious attention.

➤ Public surveys. for many potential targets there may be surveys available listing them, like the Netcraft survey.

➤ Just listen. Some applications, like peer-to-peer networks, wind up advertising many of their servers.

Similarly, many previous worms effectively broadcast that the infected machine is vulnerable to further attack. easy, because of its widespread scanning, during the Code Red I infection it was easy to select up the addresses of upwards of 300,000 vulnerable IIS servers—because each came knock on everyone's door!

NEW QUESTION 11

- (Exam Topic 3)

Samuel, a professional hacker, monitored and intercepted already established traffic between Bob and a host machine to predict Bob's ISN. Using this ISN, Samuel sent spoofed packets with Bob's IP address to the host machine. The host machine responded with a packet having an incremented ISN. Consequently, Bob's connection got hung, and Samuel was able to communicate with the host machine on behalf of Bob. What is the type of attack performed by Samuel in the above scenario?

- A. UDP hijacking
- B. Blind hijacking
- C. TCP/IP hacking
- D. Forbidden attack

Answer: C

Explanation:

A TCP/IP hijack is an attack that spoofs a server into thinking it's talking with a sound client, once actually it's communication with an assaulter that has condemned (or hijacked) the tcp session. Assume that the client has administrator-level privileges, which the attacker needs to steal that authority so as to form a brand new account with root-level access of the server to be used afterward. A tcp Hijacking is sort of a two-phased man-in-the-middle attack. The man-in-the-middle assaulter lurks within the circuit between a shopper and a server so as to work out what port and sequence numbers are being employed for the conversation.

First, the attacker knocks out the client with an attack, like Ping of Death, or ties it up with some reasonably ICMP storm. This renders the client unable to transmit any packets to the server. Then, with the client crashed, the attacker assumes the client's identity so as to talk with the server. By this suggests, the attacker gains administrator-level access to the server.

One of the most effective means of preventing a hijack attack is to want a secret, that's a shared secret

between the shopper and also the server. Looking on the strength of security desired, the key may be used for random exchanges. This is often once a client and server periodically challenge each other, or it will occur with each exchange, like Kerberos.

NEW QUESTION 14

- (Exam Topic 3)

The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124. An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is: nmap 192.168.1.64/28.

Why he cannot see the servers?

- A. He needs to add the command "ip address" just before the IP address
- B. He needs to change the address to 192.168.1.0 with the same mask
- C. He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are not in that range
- D. The network must be down and the nmap command and IP address are ok

Answer: C

Explanation:

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

This is a fairly simple question. You must understand what a subnet mask is and how it works.

A subnetwork or subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting.

Computers that belong to the same subnet are addressed with an identical most-significant bit-group in their IP addresses. This results in the logical division of an IP address into two fields: the network number or routing prefix and the rest field or host identifier. The rest field is an identifier for a specific host or network interface.

The routing prefix may be expressed in Classless Inter-Domain Routing (CIDR) notation written as the first address of a network, followed by a slash character (/), and ending with the bit-length of the prefix. For example, 198.51.100.0/24 is the prefix of the Internet Protocol version 4 network starting at the given address, having 24 bits allocated for the network prefix, and the remaining 8 bits reserved for host addressing. Addresses in the range 198.51.100.0 to 198.51.100.255 belong to this network. The IPv6 address specification 2001:db8::/32 is a large address block with 296 addresses, having a 32-bit routing prefix.

For IPv4, a network may also be characterized by its subnet mask or netmask, which is the bitmask that when applied by a bitwise AND operation to any IP address in the network, yields the routing prefix. Subnet masks are also expressed in dot-decimal notation like an address. For example, 255.255.255.0 is the subnet mask for the prefix 198.51.100.0/24.

Table Description automatically generated

IPv4 CIDR				
CIDR	The last IP address on the subnet	Subnet mask	Number of addresses in a subnet	Number of hosts in the subnet
a.b.c.d/32	0.0.0.0	255.255.255.255	1	0
a.b.c.d/31	0.0.0.1	255.255.255.254	2	0
a.b.c.d/30	0.0.0.3	255.255.255.252	4	2
a.b.c.d/29	0.0.0.7	255.255.255.248	8	6
a.b.c.d/28	0.0.0.15	255.255.255.240	16	14
a.b.c.d/27	0.0.0.31	255.255.255.224	32	30
a.b.c.d/26	0.0.0.63	255.255.255.192	64	62
a.b.c.d/25	0.0.0.127	255.255.255.128	128	126
a.b.c.0/24	0.0.0.255	255.255.255.000	256	254
a.b.c.0/23	0.0.1.255	255.255.254.000	512	510
a.b.c.0/22	0.0.3.255	255.255.252.000	1024	1022
a.b.c.0/21	0.0.7.255	255.255.248.000	2048	2046
a.b.c.0/20	0.0.15.255	255.255.240.000	4096	4094
a.b.c.0/19	0.0.31.255	255.255.224.000	8192	8190
a.b.c.0/18	0.0.63.255	255.255.192.000	16384	16382
a.b.c.0/17	0.0.127.255	255.255.128.000	32768	32766
a.b.0.0/16	0.0.255.255	255.255.000.000	65536	65534
a.b.0.0/15	0.1.255.255	255.254.000.000	131072	131070
a.b.0.0/14	0.3.255.255	255.252.000.000	262144	262142
a.b.0.0/13	0.7.255.255	255.248.000.000	524288	524286
a.b.0.0/12	0.15.255.255	255.240.000.000	1048576	1048574
a.b.0.0/11	0.31.255.255	255.224.000.000	2097152	2097150
a.b.0.0/10	0.63.255.255	255.192.000.000	4194304	4194302
a.b.0.0/9	0.127.255.255	255.128.000.000	8388608	8388606
a.0.0.0/8	0.255.255.255	255.000.000.000	16777216	16777214
a.0.0.0/7	1.255.255.255	254.000.000.000	33554432	33554430
a.0.0.0/6	3.255.255.255	252.000.000.000	67108864	67108862
a.0.0.0/5	7.255.255.255	248.000.000.000	134217728	134217726
a.0.0.0/4	15.255.255.255	240.000.000.000	268435456	268435454
a.0.0.0/3	31.255.255.255	224.000.000.000	536870912	536870910
a.0.0.0/2	63.255.255.255	192.000.000.000	1073741824	1073741822
a.0.0.0/1	127.255.255.255	128.000.000.000	2147483648	2147483646
0.0.0.0/0	255.255.255.255	000.000.000.000	4294967296	4294967294

NEW QUESTION 15

- (Exam Topic 3)

Kevin, an encryption specialist, implemented a technique that enhances the security of keys used for encryption and authentication. Using this technique, Kevin input an initial key to an algorithm that generated an enhanced key that is resistant to brute-force attacks. What is the technique employed by Kevin to improve the security of encryption keys?

- A. Key derivation function
- B. Key reinstallation
- C. A Public key infrastructure
- D. Key stretching

Answer: D**NEW QUESTION 19**

- (Exam Topic 3)

Henry is a penetration tester who works for XYZ organization. While performing enumeration on a client organization, he queries the DNS server for a specific cached DNS record. Further, by using this cached record, he determines the sites recently visited by the organization's user. What is the enumeration technique used by Henry on the organization?

- A. DNS zone walking
- B. DNS cache snooping
- C. DNS SEC zone walking
- D. DNS cache poisoning

Answer: B**NEW QUESTION 21**

- (Exam Topic 3)

Kate dropped her phone and subsequently encountered an issue with the phone's internal speaker. Thus, she is using the phone's loudspeaker for phone calls and other activities. Bob, an attacker, takes advantage of this vulnerability and secretly exploits the hardware of Kate's phone so that he can monitor the loudspeaker's output from data sources such as voice assistants, multimedia messages, and audio files by using a malicious app to breach speech privacy. What is the type of attack Bob performed on Kate in the above scenario?

- A. Man-in-the-disk attack
- B. aLTER attack
- C. SIM card attack
- D. Spearphone attack

Answer: D

NEW QUESTION 25

- (Exam Topic 3)

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

- A. Wireshark with Airpcap
- B. Aircnort with Airpcap
- C. Wireshark with Winpcap
- D. Ethereal with Winpcap

Answer: A

Explanation:

<https://support.riverbed.com/content/support/software/steelcentral-npm/airpcap.html>

Since this question refers specifically to analyzing a wireless network, it is obvious that we need an option with AirPcap (Riverbed AirPcap USB-based adapters capture 802.11 wireless traffic for analysis). Since it works with two traffic analyzers SteelCentral Packet Analyzer (Cascade Pilot) or Wireshark, the correct option would be "Wireshark with Airpcap."

NOTE: AirPcap adapters no longer available for sale effective January 1, 2018, but a question on this topic may occur on your exam.

NEW QUESTION 26

- (Exam Topic 3)

Jane is working as a security professional at CyberSol Inc. She was tasked with ensuring the authentication and integrity of messages being transmitted in the corporate network. To encrypt the messages, she implemented a security model in which every user in the network maintains a ring of public keys. In this model, a user needs to encrypt a message using the receiver's public key, and only the receiver can decrypt the message using their private key. What is the security model implemented by Jane to secure corporate messages?

- A. Zero trust network
- B. Transport Layer Security (TLS)
- C. Secure Socket Layer (SSL)
- D. Web of trust (WOT)

Answer: D

NEW QUESTION 27

- (Exam Topic 3)

Which tool can be used to silently copy files from USB devices?

- A. USB Grabber
- B. USB Snoopy
- C. USB Sniffer
- D. Use Dumper

Answer: D

NEW QUESTION 28

- (Exam Topic 3)

Which wireless security protocol replaces the personal pre-shared key (PSK) authentication with Simultaneous Authentication of Equals (SAE) and is therefore resistant to offline dictionary attacks?

- A. WPA3-Personal
- B. WPA2-Enterprise
- C. Bluetooth
- D. ZigBee

Answer: A

NEW QUESTION 29

- (Exam Topic 3)

Jacob works as a system administrator in an organization. He wants to extract the source code of a mobile application and disassemble the application to analyze its design flaws. Using this technique, he wants to fix any bugs in the application, discover underlying vulnerabilities, and improve defense strategies against attacks.

What is the technique used by Jacob in the above scenario to improve the security of the mobile application?

- A. Reverse engineering
- B. App sandboxing
- C. Jailbreaking
- D. Social engineering

Answer: A

NEW QUESTION 30

- (Exam Topic 3)

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

- A. -sA

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

Answer: A

NEW QUESTION 31

- (Exam Topic 3)

To hide the file on a Linux system, you have to start the filename with a specific character. What is the character?

- A. Exclamation mark (!)
- B. Underscore (_)
- C. Tilde H
- D. Period (.)

Answer: D

NEW QUESTION 35

- (Exam Topic 3)

Kevin, a professional hacker, wants to penetrate CyberTech Inc.'s network. He employed a technique, using which he encoded packets with Unicode characters. The company's IDS cannot recognize the packet, but the target web server can decode them.

What is the technique used by Kevin to evade the IDS system?

- A. Desynchronization
- B. Obfuscating
- C. Session splicing
- D. Urgency flag

Answer: B

Explanation:

Adversaries could decide to build an possible or file difficult to find or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. this is often common behavior which will be used across totally different platforms and therefore the network to evade defenses.

Payloads may be compressed, archived, or encrypted so as to avoid detection. These payloads may be used throughout Initial Access or later to mitigate detection. typically a user's action could also be needed to open and Deobfuscate/Decode Files or info for User Execution. The user can also be needed to input a parole to open a parole protected compressed/encrypted file that was provided by the mortal. Adversaries can also used compressed or archived scripts, like JavaScript.

Portions of files can even be encoded to cover the plain-text strings that will otherwise facilitate defenders

with discovery. Payloads can also be split into separate, ostensibly benign files that solely reveal malicious practicality once reassembled.

Adversaries can also modify commands dead from payloads or directly via a Command and Scripting Interpreter. surroundings variables, aliases, characters, and different platform/language specific linguistics may be wont to evade signature based mostly detections and application management mechanisms.

NEW QUESTION 38

- (Exam Topic 3)

An attacker identified that a user and an access point are both compatible with WPA2 and WPA3 encryption. The attacker installed a rogue access point with only WPA2 compatibility in the vicinity and forced the victim to go through the WPA2 four-way handshake to get connected. After the connection was established, the attacker used automated tools to crack WPA2-encrypted messages. What is the attack performed in the above scenario?

- A. Timing-based attack
- B. Side-channel attack
- C. Downgrade security attack
- D. Cache-based attack

Answer: B

NEW QUESTION 39

- (Exam Topic 3)

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

- A. [allinurl:]
- B. [location:]
- C. [site:]
- D. [link:]

Answer: C

Explanation:

Google hacking or Google dorking https://en.wikipedia.org/wiki/Google_hacking

It is a hacker technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites are using. Google dorking could also be used for OSINT.

Search syntax https://en.wikipedia.org/wiki/Google_Search

Google's search engine has its own built-in query language. The following list of queries can be run to find a list of files, find information about your competition, track people, get information about SEO backlinks, build email lists, and of course, discover web vulnerabilities.

- [site:] - Search within a specific website

NEW QUESTION 40

- (Exam Topic 3)

The security administrator of ABC needs to permit Internet traffic in the host 10.0.0.2 and UDP traffic in the host 10.1.1.3. He also needs to permit all FTP traffic to the rest of the network and deny all other traffic. After he applied his ACL configuration in the router, nobody can access the ftp, and the permitted hosts cannot access the Internet. According to the next configuration, what is happening in the network?

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

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

Answer: B

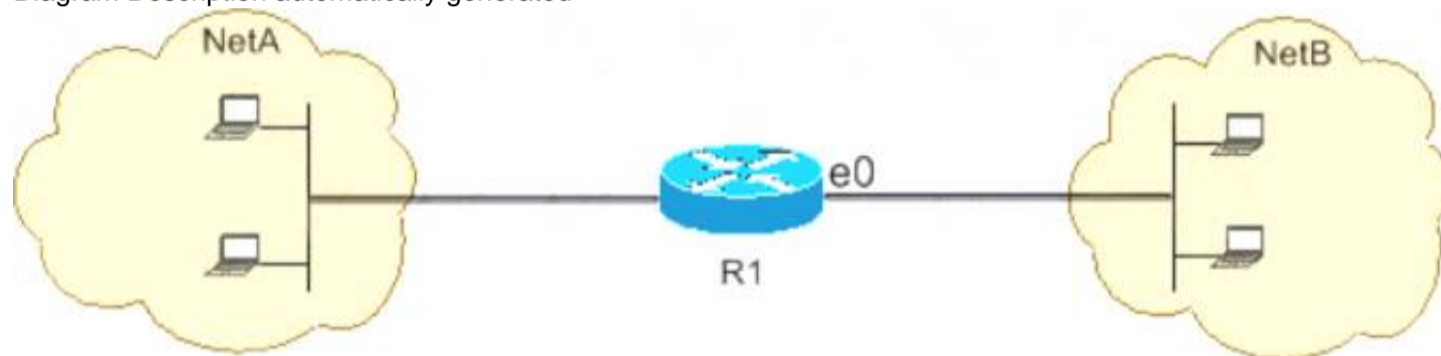
Explanation:

<https://www.cisco.com/c/en/us/support/docs/ip/access-lists/26448-ACLsamples.html>

Since the first line prohibits any TCP traffic (access-list 102 deny tcp any any), the lines below will simply be ignored by the router. Below you will find the example from CISCO documentation.

This figure shows that FTP (TCP, port 21) and FTP data (port 20) traffic sourced from NetB destined to NetA is denied, while all other IP traffic is permitted.

Diagram Description automatically generated



FTP uses port 21 and port 20. TCP traffic destined to port 21 and port 20 is denied and everything else is explicitly permitted.

- > access-list 102 deny tcp any any eq ftp
- > access-list 102 deny tcp any any eq ftp-data
- > access-list 102 permit ip any any

NEW QUESTION 42

- (Exam Topic 3)

What would you enter if you wanted to perform a stealth scan using Nmap?

- A. nmap -sM
- B. nmap -sU
- C. nmap -sS
- D. nmap -sT

Answer: C

NEW QUESTION 43

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 44

- (Exam Topic 3)

Attempting an injection attack on a web server based on responses to True/False QUESTION NO:s is called which of the following?

- A. Compound SQLi
- B. Blind SQLi
- C. Classic SQLi
- D. DMS-specific SQLi

Answer: B

Explanation:

https://en.wikipedia.org/wiki/SQL_injection#Blind_SQL_injection

Blind SQL injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker. The page with the vulnerability may not be one that displays data but will display differently depending on the results of a logical statement injected into the legitimate SQL statement called for that page. This type of attack has traditionally been considered time-intensive because a new statement needed to be crafted for each bit recovered, and depending on its structure, the attack may consist of many unsuccessful requests. Recent advancements have allowed each request to recover multiple bits, with no unsuccessful requests, allowing for more consistent and efficient extraction.

NEW QUESTION 45

- (Exam Topic 3)

An unauthorized individual enters a building following an employee through the employee entrance after the lunch rush. What type of breach has the individual just performed?

- A. Reverse Social Engineering
- B. Tailgating
- C. Piggybacking
- D. Announced

Answer: B**Explanation:**

- Identifying operating systems, services, protocols and devices,
- Collecting unencrypted information about usernames and passwords,
- Capturing network traffic for further analysis

are passive network sniffing methods since with the help of them we only receive information and do not make any changes to the target network. When modifying and replaying the captured network traffic, we are already starting to make changes and actively interact with it.

NEW QUESTION 49

- (Exam Topic 3)

Bob wants to ensure that Alice can check whether his message has been tampered with. He creates a checksum of the message and encrypts it using asymmetric cryptography. What key does Bob use to encrypt the checksum for accomplishing this goal?

- A. Alice's private key
- B. Alice's public key
- C. His own private key
- D. His own public key

Answer: B**NEW QUESTION 54**

- (Exam Topic 3)

An attacker utilizes a Wi-Fi Pineapple to run an access point with a legitimate-looking SSID for a nearby business in order to capture the wireless password. What kind of attack is this?

- A. MAC spoofing attack
- B. Evil-twin attack
- C. War driving attack
- D. Phishing attack

Answer: B**NEW QUESTION 56**

- (Exam Topic 3)

This type of injection attack does not show any error message. It is difficult to exploit as it returns information when the application is given SQL payloads that elicit a true or false response from the server. By observing the response, an attacker can extract sensitive information. What type of attack is this?

- A. Time-based SQL injection
- B. Union SQL injection
- C. Error-based SQL injection
- D. Blind SQL injection

Answer: D**NEW QUESTION 58**

- (Exam Topic 3)

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

- A. Wireshark
- B. Maltego
- C. Metasploit
- D. Nessus

Answer: C**Explanation:**

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

The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. It is owned by Boston, Massachusetts-based security company Rapid7.

Its best-known sub-project is the open-source Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shellcode archive and related research.

The Metasploit Project includes anti-forensic and evasion tools, some of which are built into the Metasploit Framework. Metasploit is pre-installed in the Kali Linux operating system.

The basic steps for exploiting a system using the Framework include.

* 1. Optionally checking whether the intended target system is vulnerable to an exploit.

* 2. Choosing and configuring an exploit (code that enters a target system by taking advantage of one of its bugs; about 900 different exploits for Windows, Unix/Linux and macOS systems are included).

* 3. Choosing and configuring a payload (code that will be executed on the target system upon successful entry; for instance, a remote shell or a VNC server). Metasploit often recommends a payload that should work.

* 4. Choosing the encoding technique so that hexadecimal opcodes known as "bad characters" are removed from the payload, these characters will cause the exploit to fail.

* 5. Executing the exploit.

This modular approach – allowing the combination of any exploit with any payload – is the major advantage of the Framework. It facilitates the tasks of attackers, exploit writers and payload writers.

NEW QUESTION 60

- (Exam Topic 3)

Mr. Omkar performed tool-based vulnerability assessment and found two vulnerabilities. During analysis, he found that these issues are not true vulnerabilities. What will you call these issues?

- A. False positives
- B. True negatives
- C. True positives
- D. False negatives

Answer: A

Explanation:

False Positives occur when a scanner, Web Application Firewall (WAF), or Intrusion Prevention System (IPS) flags a security vulnerability that you do not have. A false negative is the opposite of a false positive, telling you that you don't have a vulnerability when, in fact, you do.

A false positive is like a false alarm; your house alarm goes off, but there is no burglar. In web application security, a false positive is when a web application security scanner indicates that there is a vulnerability on your website, such as SQL Injection, when, in reality, there is not. Web security experts and penetration testers use automated web application security scanners to ease the penetration testing process. These tools help them ensure that all web application attack surfaces are correctly tested in a reasonable amount of time. But many false positives tend to break down this process. If the first 20 variants are false, the penetration tester assumes that all the others are false positives and ignore the rest. By doing so, there is a good chance that real web application vulnerabilities will be left undetected.

When checking for false positives, you want to ensure that they are indeed false. By nature, we humans tend to start ignoring false positives rather quickly. For example, suppose a web application security scanner detects 100 SQL Injection vulnerabilities. If the first 20 variants are false positives, the penetration tester assumes that all the others are false positives and ignore all the rest. By doing so, there are chances that real web application vulnerabilities are left undetected. This is why it is crucial to check every vulnerability and deal with each false positive separately to ensure false positives.

NEW QUESTION 64

- (Exam Topic 3)

You are a penetration tester and are about to perform a scan on a specific server. The agreement that you signed with the client contains the following specific condition for the scan: "The attacker must scan every port on the server several times using a set of spoofed sources IP addresses." Suppose that you are using Nmap to perform this scan. What flag will you use to satisfy this requirement?

- A. The -A flag
- B. The -g flag
- C. The -f flag
- D. The -D flag

Answer: D

Explanation:

flags `--source-port` and `-g` are equivalent and instruct nmap to send packets through a selected port. this option is used to try to cheat firewalls whitelisting traffic from specific ports. the following example can scan the target from the port twenty to ports eighty, 22, 21,23 and 25 sending fragmented packets to LinuxHint.

NEW QUESTION 67

- (Exam Topic 3)

An Internet Service Provider (ISP) has a need to authenticate users connecting via analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network.

Which AAA protocol is the most likely able to handle this requirement?

- A. TACACS+
- B. DIAMETER
- C. Kerberos
- D. RADIUS

Answer: D

Explanation:

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

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service.

RADIUS is a client/server protocol that runs in the application layer, and can use either TCP or UDP. Network access servers, which control access to a network, usually contain a RADIUS client component that communicates with the RADIUS server. RADIUS is often the back-end of choice for 802.1X authentication. A RADIUS server is usually a background process running on UNIX or Microsoft Windows.

Authentication and authorization

The user or machine sends a request to a Network Access Server (NAS) to gain access to a particular network resource using access credentials. The credentials are passed to the NAS device via the link-layer protocol—for example, Point-to-Point Protocol (PPP) in the case of many dialup or DSL providers or posted in an HTTPS secure web form.

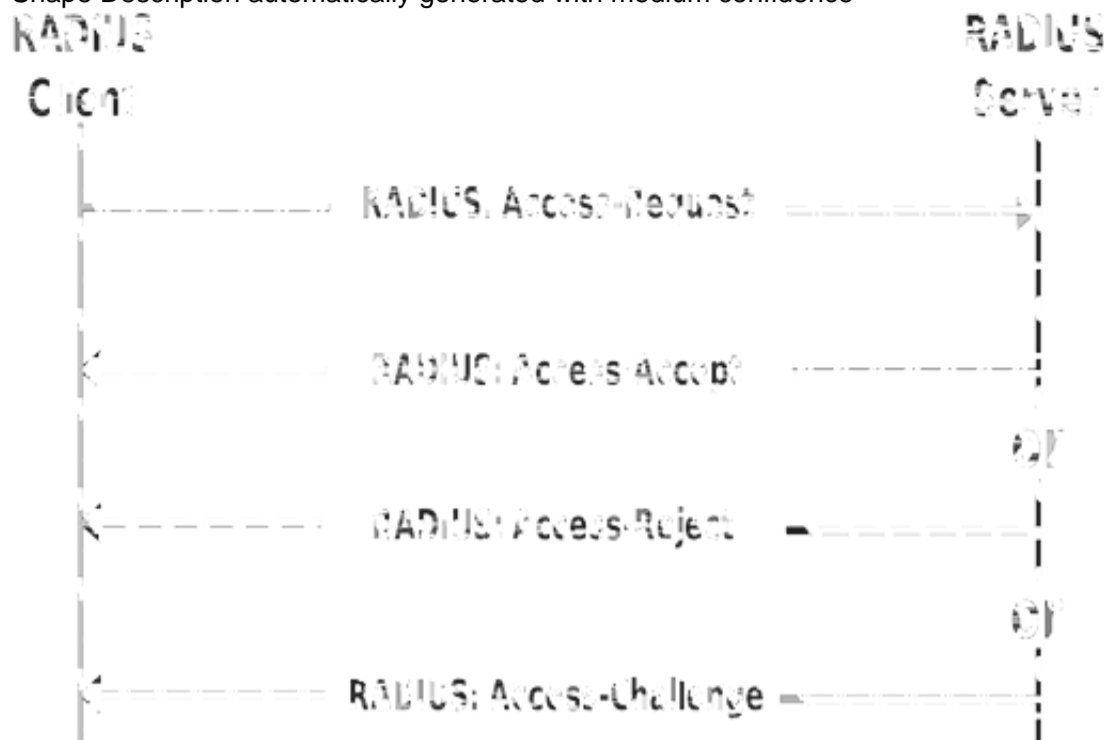
In turn, the NAS sends a RADIUS Access Request message to the RADIUS server, requesting authorization to grant access via the RADIUS protocol.

This request includes access credentials, typically in the form of username and password or security certificate provided by the user. Additionally, the request may contain other information which the NAS knows about the user, such as its network address or phone number, and information regarding the user's physical point of attachment to the NAS.

The RADIUS server checks that the information is correct using authentication schemes such as PAP, CHAP or EAP. The user's proof of identification is verified,

along with, optionally, other information related to the request, such as the user's network address or phone number, account status, and specific network service access privileges. Historically, RADIUS servers checked the user's information against a locally stored flat-file database. Modern RADIUS servers can do this or can refer to external sources—commonly SQL, Kerberos, LDAP, or Active Directory servers—to verify the user's credentials.

Shape Description automatically generated with medium confidence



The RADIUS server then returns one of three responses to the NAS:

- 1) Access-Reject,
- 2) Access-Challenge,
- 3) Access-Accept.

Access-Reject

The user is unconditionally denied access to all requested network resources. Reasons may include failure to provide proof of identification or an unknown or inactive user account.

Access-Challenge

Requests additional information from the user such as a secondary password, PIN, token, or card.

Access-Challenge is also used in more complex authentication dialogs where a secure tunnel is established between the user machine and the Radius Server in a way that the access credentials are hidden from the NAS.

Access-Accept

The user is granted access. Once the user is authenticated, the RADIUS server will often check that the user is authorized to use the network service requested. A given user may be allowed to use a company's wireless network, but not its VPN service, for example. Again, this information may be stored locally on the RADIUS server or may be looked up in an external source such as LDAP or Active Directory.

NEW QUESTION 69

- (Exam 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 Unkn0rnsCan 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 71

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 73

- (Exam Topic 2)

An attacker runs netcat tool to transfer a secret file between two hosts.

```
Machine A: netcat -l -p 1234 < secretfile
```

```
Machine B: netcat 192.168.3.4 > 1234
```

He is worried about information being sniffed on the network.

How would the attacker use netcat to encrypt the information before transmitting onto the wire?

- A. Machine A: netcat -l -p -s password 1234 < testfileMachine B: netcat <machine A IP> 1234
 B. Machine A: netcat -l -e magickey -p 1234 < testfileMachine B: netcat <machine A IP> 1234
 C. Machine A: netcat -l -p 1234 < testfile -pw passwordMachine B: netcat <machine A IP> 1234 -pw password
 D. Use cryptcat instead of netcat

Answer: D

NEW QUESTION 77

- (Exam Topic 2)

Ethical hacker Jane Doe is attempting to crack the password of the head of the IT department of ABC company. She is utilizing a rainbow table and notices upon entering a password that extra characters are added to the password after submitting. What countermeasure is the company using to protect against rainbow tables?

- A. Password key hashing
 B. Password salting
 C. Password hashing
 D. Account lockout

Answer: B

Explanation:

Passwords are usually delineated as "hashed and salted". salting is simply the addition of a unique, random string of characters renowned solely to the site to every parole before it's hashed, typically this "salt" is placed in front of each password.

The salt value needs to be hold on by the site, which means typically sites use the same salt for each parole. This makes it less effective than if individual salts are used.

The use of unique salts means that common passwords shared by multiple users – like "123456" or "password" – aren't revealed revealed when one such hashed password is known – because despite the passwords being the same the immediately and hashed values are not.

Large salts also protect against certain methods of attack on hashes, including rainbow tables or logs of hashed passwords previously broken.

Both hashing and salting may be repeated more than once to increase the issue in breaking the security.

NEW QUESTION 80

- (Exam Topic 2)

John wants to send Marie an email that includes sensitive information, and he does not trust the network that he is connected to. Marie gives him the idea of using PGP. What should John do to communicate correctly using this type of encryption?

- A. Use his own public key to encrypt the message.
 B. Use Marie's public key to encrypt the message.
 C. Use his own private key to encrypt the message.
 D. Use Marie's private key to encrypt the message.

Answer: B

Explanation:

When a user encrypts plaintext with PGP, PGP first compresses the plaintext. The session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext. Once the data is encrypted, the session key is then encrypted to the recipient's public key

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

Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography, and finally public-key cryptography; each step uses one of several supported algorithms. Each public key is bound to a username or an e-mail address.

https://en.wikipedia.org/wiki/Public-key_cryptography

Public key encryption uses two different keys. One key is used to encrypt the information and the other is used to decrypt the information. Sometimes this is referred to as asymmetric encryption because two keys are required to make the system and/or process work securely. One key is known as the public key and should be shared by the owner with anyone who will be securely communicating with the key owner. However, the owner's secret key is not to be shared and considered a private key. If the private key is shared with unauthorized recipients, the encryption mechanisms protecting the information must be considered compromised.

NEW QUESTION 82

- (Exam 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 83

- (Exam 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 command 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 is 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 85

- (Exam 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: D

Explanation:

After the attacker completes preparations, the subsequent step is an effort to realize an edge within the target's environment. A particularly common entry tactic is 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 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.



Figure 2. APT actor sends spearphishing email to target with malicious content

NEW QUESTION 87

- (Exam 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 90

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 95

- (Exam Topic 2)

Robin, a professional hacker, targeted an organization's network to sniff all the traffic. During this process, Robin plugged in a rogue switch to an unused port in the LAN with a priority lower than any other switch in

the network so that he could make it a root bridge that will later allow him to sniff all the traffic in the network.

What is the attack performed by Robin in the above scenario?

- A. ARP spoofing attack
- B. VLAN hopping attack
- C. DNS poisoning attack
- D. STP attack

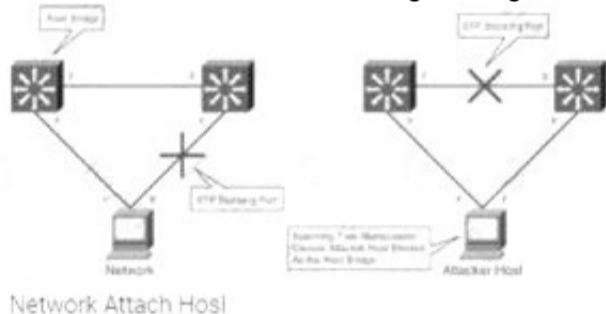
Answer: D

Explanation:

STP prevents bridging loops in a redundant switched network environment. By avoiding loops, you can ensure that broadcast traffic does not become a traffic storm.

STP is a hierarchical tree-like topology with a "root" switch at the top. A switch is elected as root based on the lowest configured priority of any switch (0 through 65,535). When a switch boots up, it begins a process of identifying other switches and determining the root bridge. After a root bridge is elected, the topology is established from its perspective of the connectivity. The switches determine the path to the root bridge, and all redundant paths are blocked. STP sends configuration and topology change notifications and acknowledgments (TCN/TCA) using bridge protocol data units (BPDU).

An STP attack involves an attacker spoofing the root bridge in the topology. The attacker broadcasts out an STP configuration/topology change BPDU in an attempt to force an STP recalculation. The BPDU sent out announces that the attacker's system has a lower bridge priority. The attacker can then see a variety of frames forwarded from other switches to it. STP recalculation may also cause a denial-of-service (DoS) condition on the network by causing an interruption of 30 to 45 seconds each time the root bridge changes. An attacker using STP network topology changes to force its host to be elected as the root bridge.



switch

NEW QUESTION 96

- (Exam 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 97

- (Exam Topic 2)

John, a professional hacker, targeted an organization that uses LDAP for accessing distributed directory services. He used an automated tool to anonymously query the LDAP service for sensitive information such as usernames, addresses, departmental details, and server names to launch further attacks on the target organization.

What is the tool employed by John to gather information from the LDAP service?

- A. jxplorer
- B. Zabasearch
- C. EarthExplorer
- D. lke-scan

Answer: A

Explanation:

JXplorer could be a cross platform LDAP browser and editor. it's a standards compliant general purpose LDAP client which will be used to search, scan and edit any commonplace LDAP directory, or any directory service with an LDAP or DSML interface.

It is extremely flexible and can be extended and custom in a very number of the way. JXplorer is written in java, and also the source code and source code build system are obtainable via svn or as a packaged build for users who wish to experiment or any develop the program.

JX is available in 2 versions; the free open source version under an OSI Apache two style licence, or within the JXWorkBench Enterprise bundle with inbuilt reporting, administrative and security tools.

JX has been through a number of different versions since its creation in 1999; the foremost recent stable release is version 3.3.1, the August 2013 release.

JXplorer could be an absolutely useful LDAP consumer with advanced security integration and support for the harder and obscure elements of the LDAP protocol. It's been tested on Windows, Solaris, Linux and OSX, packages are obtainable for HP-UX, AIX, BSD and it should run on any Java supporting OS.

NEW QUESTION 101

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 106

- (Exam 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 the 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 to 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 proceeding 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 110

- (Exam 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 comparison.
- 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 111

- (Exam Topic 2)

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

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

Answer: C

Explanation:

Network-based scanner

A network-based vulnerability scanner, in simplistic terms, is the process of identifying loopholes on a computer's network or IT assets, which hackers and threat actors can exploit. By implementing this process, one can successfully identify their organization's current risk(s). This is not where the buck stops; one can also

verify the effectiveness of your system's security measures while improving internal and external defenses. Through this review, an organization is well equipped to take an extensive inventory of all systems, including operating systems, installed software, security patches, hardware, firewalls, anti-virus software, and much more.

Agent-based scanner

Agent-based scanners make use of software scanners on each and every device; the results of the scans are reported back to the central server. Such scanners are well equipped to find and report out on a range of vulnerabilities.

NOTE: This option is not suitable for us, since for it to work, you need to install a special agent on each computer before you start collecting data from them.

NEW QUESTION 113

- (Exam 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 117

- (Exam 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 121

- (Exam Topic 2)

You are analysing traffic on the network with Wireshark. You want to routinely run a cron job which will run the capture against a specific set of IPs - 192.168.8.0/24. What command would you use?

- A. wireshark --fetch "192.168.8**"
- B. wireshark --capture --local masked 192.168.8.0 ---range 24
- C. tshark -net 192.255.255.255 mask 192.168.8.0
- D. sudo tshark -f"net 192 .68.8.0/24"

Answer: D

NEW QUESTION 126

- (Exam 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 reinstatement 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 a little 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 127

- (Exam Topic 2)

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

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

Answer: A

Explanation:

A stealth virus may be a sort of virus malware that contains sophisticated means of avoiding detection by antivirus software. After it manages to urge into the now-infected machine a stealth viruses hides itself by continually renaming and moving itself round the disc. Like other viruses, a stealth virus can take hold of the many parts of one's PC. When taking control of the PC and performing tasks, antivirus programs can detect it, but a stealth virus sees that coming and can rename then copy itself to a special drive or area on the disc, before the antivirus software. Once moved and renamed a stealth virus will usually replace the detected 'infected' file with a clean file that doesn't trigger anti-virus detection. It's a never-ending game of cat and mouse. The intelligent architecture of this sort of virus about guarantees it's impossible to completely rid oneself of it once infected. One would need to completely wipe the pc and rebuild it from scratch to completely eradicate the presence of a stealth virus. Using regularly-updated antivirus software can reduce risk, but, as we all know, antivirus software is additionally caught in an endless cycle of finding new threats and protecting against them.

<https://www.techslang.com/definition/what-is-a-stealth-virus/>

NEW QUESTION 131

- (Exam Topic 2)

Samuel a security administrator, is assessing the configuration of a web server. He noticed that the server permits SSLv2 connections, and the same private key certificate is used on a different server that allows SSLv2 connections. This vulnerability makes the web server vulnerable to attacks as the SSLv2 server can leak key information.

Which of the following attacks can be performed by exploiting the above vulnerability?

- A. DROWN attack
- B. Padding oracle attack
- C. Side-channel attack
- D. DUHK attack

Answer: A

Explanation:

DROWN is a serious vulnerability that affects HTTPS and other services that deem SSL and TLS, some of the essential cryptographic protocols for net security. These protocols allow everyone on the net to browse the net, use email, look on-line, and send instant messages while not third-parties being able to browse the communication.

DROWN allows attackers to break the encryption and read or steal sensitive communications, as well as passwords, credit card numbers, trade secrets, or financial data. At the time of public disclosure on March 2016, our measurements indicated thirty third of all HTTPS servers were vulnerable to the attack. fortuitously, the vulnerability is much less prevalent currently. As of 2019, SSL Labs estimates that one.2% of HTTPS servers are vulnerable.

What will the attackers gain? Any communication between users and the server. This typically includes, however isn't limited to, usernames and passwords, credit card numbers, emails, instant messages, and sensitive documents. under some common scenarios, an attacker can also impersonate a secure web site and intercept or change the content the user sees.

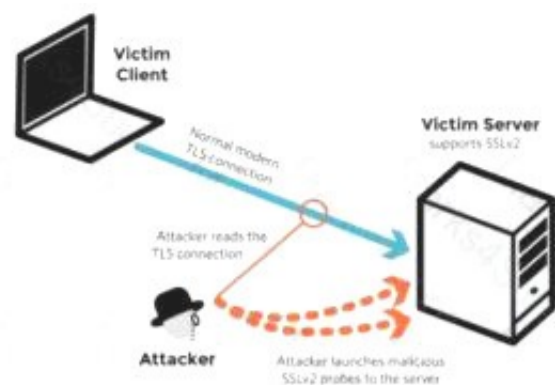
Who is vulnerable? Websites, mail servers, and other TLS-dependent services are in danger for the DROWN attack. At the time of public disclosure, many popular sites were affected. we used Internet-wide scanning to live how many sites are vulnerable:

SSLv2	Vulnerable at Disclosure (March 2016)
HTTPS — Top one million domains	25%
HTTPS — All browser-trusted sites	22%
HTTPS — All sites	33%

Operators of vulnerable servers got to take action. there's nothing practical that browsers or end-users will do on their own to protect against this attack.

Is my site vulnerable? Modern servers and shoppers use the TLS encryption protocol. However, because of misconfigurations, several servers also still support SSLv2, a 1990s-era precursor to TLS. This support did not matter in practice, since no up-to-date clients really use SSLv2. Therefore, despite the fact that SSLv2 is thought to be badly insecure, until now, simply supporting SSLv2 wasn't thought of a security problem, is a clients never used it.

DROWN shows that merely supporting SSLv2 may be a threat to fashionable servers and clients. It modern associate degree attacker to modern fashionable TLS connections between up-to-date clients and servers by sending probes to a server that supports SSLv2 and uses the same private key.

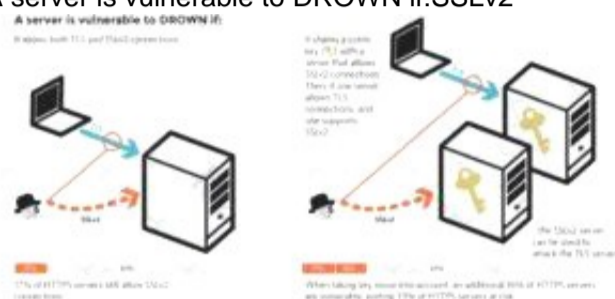


SSLv2

- It allows SSLv2 connections. This is surprisingly common, due to misconfiguration and inappropriate default settings.
- Its private key is used on any other server that allows SSLv2 connections, even for another protocol.

Many companies reuse the same certificate and key on their web and email servers, for instance. In this case, if the email server supports SSLv2 and the web server does not, an attacker can take advantage of the email server to break TLS connections to the web server.

A server is vulnerable to DROWN if: SSLv2



How do I protect my server? To protect against DROWN, server operators need to ensure that their private keys software used anywhere with server computer code that enables SSLv2 connections. This includes net servers, SMTP servers, IMAP and POP servers, and the other software that supports SSL/TLS.

Disabling SSLv2 is difficult and depends on the particular server software. we offer instructions here for many common products:

OpenSSL: OpenSSL may be a science library employed in several server merchandise. For users of OpenSSL, the simplest and recommended solution is to upgrade to a recent OpenSSL version. OpenSSL 1.0.2 users ought to upgrade to 1.0.2g. OpenSSL 1.0.1 users ought to upgrade to one.0.1s. Users of older OpenSSL versions ought to upgrade to either one in every of these versions. (Updated March thirteenth, 16:00 UTC) **Microsoft IIS (Windows Server):** Support for SSLv2 on the server aspect is enabled by default only on the OS versions that correspond to IIS 7.0 and IIS seven.5, particularly Windows scene, Windows Server 2008, Windows seven and Windows Server 2008R2. This support is disabled within the appropriate SSLv2 subkey for 'Server', as outlined in KB245030. albeit users haven't taken the steps to disable SSLv2, the export-grade and 56-bit ciphers that build DROWN possible don't seem to be supported by default.

Network Security Services (NSS): NSS may be a common science library designed into several server merchandise. NSS versions three.13 (released back in 2012) and higher than ought to have SSLv2 disabled by default. (A little variety of users might have enabled SSLv2 manually and can got to take steps to disable it.) Users of older versions ought to upgrade to a more modern version. we tend to still advocate checking whether or not your non-public secret is exposed elsewhere

Other affected software and in operation systems:

Instructions and data for: Apache, Postfix, Nginx, Debian, Red Hat

Browsers and other consumers: practical nothing practical that net browsers or different client computer code will do to stop DROWN. only server operators are ready to take action to guard against the attack.

NEW QUESTION 134

- (Exam Topic 2)

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

- A. Intrusion Detection Systems can be configured to distinguish specific content in network packets
- B. Intrusion Detection Systems can easily distinguish a malicious payload in an encrypted traffic
- C. Intrusion Detection Systems require constant update of the signature library
- D. Intrusion Detection Systems can examine the contents of the data in context of the network protocol

Answer: B

NEW QUESTION 136

- (Exam 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. UsesHost 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 area 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.

NEW QUESTION 141

- (Exam Topic 2)

While browsing his Facebook feed, Matt sees a picture one of his friends posted with the caption. "Learn more about your friends!", as well as a number of personal questions. Matt is suspicious and texts his friend, who confirms that he did indeed post it. With assurance that the post is legitimate. Matt responds to the questions on the post, a few days later. Matt's bank account has been accessed, and the password has been changed. What most likely happened?

- A. Matt inadvertently provided the answers to his security questions when responding to the post.
- B. Matt's bank-account login information was brute forced.
- C. Matt inadvertently provided his password when responding to the post.
- D. Matt's computer was infected with a keylogger.

Answer: A

NEW QUESTION 143

- (Exam Topic 2)

Every company needs a formal written document which spells out to employees precisely what they are allowed to use the company's systems for, what is prohibited, and what will happen to them if they break the rules. Two printed copies of the policy should be given to every employee as soon as possible after they join the organization. The employee should be asked to sign one copy, which should be safely filed by the company. No one should be allowed to use the company's computer systems until they have signed the policy in acceptance of its terms.

What is this document called?

- A. Information Audit Policy (IAP)
- B. Information Security Policy (ISP)
- C. Penetration Testing Policy (PTP)
- D. Company Compliance Policy (CCP)

Answer: B

NEW QUESTION 148

- (Exam Topic 2)

what is the port to block first in case you are suspicious that an IoT device has been compromised?

- A. 22
- B. 443
- C. 48101
- D. 80

Answer: C

Explanation:

TCP port 48101 uses the Transmission management Protocol. transmission control protocol is one in all the most protocols in TCP/IP networks. transmission control protocol could be a connection-oriented protocol, it needs acknowledgement to line up end-to-end communications. only a association is about up user's knowledge may be sent bi-directionally over the association.

Attention! transmission control protocol guarantees delivery of knowledge packets on port 48101 within the same order during which they were sent. bonded communication over transmission control protocol port 48101 is that the main distinction between transmission control protocol and UDP. UDP port 48101 wouldn't have bonded communication as transmission control protocol.

UDP on port 48101 provides Associate in Nursing unreliable service and datagrams might arrive duplicated, out of order, or missing unexpectedly. UDP on port 48101 thinks that error checking and correction isn't necessary or performed within the application, avoiding the overhead of such process at the network interface level.

UDP (User Datagram Protocol) could be a borderline message-oriented Transport Layer protocol (protocol is documented in IETF RFC 768).

Application examples that always use UDP: vocalisation IP (VoIP), streaming media and period multiplayer games. several internet applications use UDP, e.g. the name System (DNS), the Routing info Protocol (RIP), the Dynamic Host Configuration Protocol (DHCP), the straightforward Network Management Protocol (SNMP).

NEW QUESTION 149

- (Exam Topic 2)

Emily, an extrovert obsessed with social media, posts a large amount of private information, photographs, and location tags of recently visited places. Realizing this. James, a professional hacker, targets Emily and her acquaintances, conducts a location search to detect their geolocation by using an automated tool, and gathers information to perform other sophisticated attacks. What is the tool employed by James in the above scenario?

- A. ophcrack
- B. Hootsuite
- C. VisualRoute
- D. HULK

Answer: B

Explanation:

Hootsuite may be a social media management platform that covers virtually each side of a social media manager's role.

With only one platform users area unit ready to do the easy stuff like reverend cool content and schedule posts on social media in all the high to managing team members and measure ROI.

There area unit many totally different plans to decide on from, from one user set up up to a bespoke enterprise account that's appropriate for much larger organizations.

Conducting location search on social media sites such as Twitter, Instagram, and Facebook helps attackers to detect the geolocation of the target. This information further helps attackers to perform various social engineering and non-technical attacks. Many online tools such as Followerwonk, Hootsuite, and Sysomos are available to search for both geotagged and non-geotagged information on social media sites. Attackers search social media sites using these online tools using keywords, usernames, date, time, and so on...

NEW QUESTION 151

- (Exam Topic 2)

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

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

Answer: B**NEW QUESTION 155**

- (Exam Topic 2)

During the enumeration phase, Lawrence performs banner grabbing to obtain information such as OS details and versions of services running. The service that he enumerated runs directly on TCP port 445.

Which of the following services is enumerated by Lawrence in this scenario?

- A. Server Message Block (SMB)
- B. Network File System (NFS)
- C. Remote procedure call (RPC)
- D. Telnet

Answer: A**Explanation:**

Worker Message Block (SMB) is an organization document sharing and information texture convention. SMB is utilized by billions of gadgets in a different arrangement of working frameworks, including Windows, MacOS, iOS, Linux, and Android. Customers use SMB to get to information on workers. This permits sharing of records, unified information the board, and brought down capacity limit needs for cell phones. Workers additionally use SMB as a feature of the Software-characterized Data Center for outstanding burdens like grouping and replication.

Since SMB is a far off record framework, it requires security from assaults where a Windows PC may be fooled into reaching a pernicious worker running inside a confided in organization or to a far off worker outside the organization edge. Firewall best practices and arrangements can upgrade security keeping malevolent traffic from leaving the PC or its organization.

For Windows customers and workers that don't have SMB shares, you can obstruct all inbound SMB traffic utilizing the Windows Defender Firewall to keep far off associations from malignant or bargained gadgets. In the Windows Defender Firewall, this incorporates the accompanying inbound principles.

Name	Profile	Enabled
File and Printer Sharing (SMB-In)	All	No
Netlogon Service (NP-In)	All	No
Remote Event Log Management (NP-In)	All	No
Remote Service Management (NP-In)	All	No

You should also create a new blocking rule to override any other inbound firewall rules. Use the following suggested settings for any Windows clients or servers that do not host SMB Shares:

- > Name: Block all inbound SMB 445
- > Description: Blocks all inbound SMB TCP 445 traffic. Not to be applied to domain controllers or computers that host SMB shares.
- > Action: Block the connection
- > Programs: All
- > Remote Computers: Any
- > Protocol Type: TCP
- > Local Port: 445
- > Remote Port: Any
- > Profiles: All
- > Scope (Local IP Address): Any
- > Scope (Remote IP Address): Any
- > Edge Traversal: Block edge traversal

You must not globally block inbound SMB traffic to domain controllers or file servers. However, you can restrict access to them from trusted IP ranges and devices to lower their attack surface. They should also be restricted to Domain or Private firewall profiles and not allow Guest/Public traffic.

NEW QUESTION 160

- (Exam Topic 2)

While examining audit logs, you discover that people are able to telnet into the SMTP server on port 25. You would like to block this, though you do not see any evidence of an attack or other wrong doing. However, you are concerned about affecting the normal functionality of the email server. From the following options choose how best you can achieve this objective?

- A. Block port 25 at the firewall.
- B. Shut off the SMTP service on the server.
- C. Force all connections to use a username and password.
- D. Switch from Windows Exchange to UNIX Sendmail.
- E. None of the above.

Answer: E**NEW QUESTION 163**

- (Exam 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: A

NEW QUESTION 166

- (Exam 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's responsible to guard the appliance to access any protected parts by providing the permissions.
- It also declares the android api that the appliance goes to use.
- It lists the instrumentation classes. The instrumentation classes provides profiling and other informations. These informations are removed just before the appliance is published etc.

This is the specified xml file for all the android application and located inside the basis directory.

NEW QUESTION 171

- (Exam Topic 2)

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

You are hired to conduct security testing on their network.

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

The access-list configured at the router prevents you from establishing a successful connection. You want to retrieve the Cisco configuration from the router. How would you proceed?

- A. Use the Cisco's TFTP default password to connect and download the configuration file
- B. Run a network sniffer and capture the returned traffic with the configuration file from the router
- C. Run Generic Routing Encapsulation (GRE) tunneling protocol from your computer to the router masking your IP address
- D. Send a customized SNMP set request with a spoofed source IP address in the range -192.168.1.0

Answer: BD

NEW QUESTION 175

- (Exam Topic 2)

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

How would an attacker exploit this design by launching TCP SYN attack?

- A. Attacker generates TCP SYN packets with random destination addresses towards a victim host
- B. Attacker floods TCP SYN packets with random source addresses towards a victim host
- C. Attacker generates TCP ACK packets with random source addresses towards a victim host
- D. Attacker generates TCP RST packets with random source addresses towards a victim host

Answer: B

NEW QUESTION 176

- (Exam 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:

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

Every part of the triage method should be performed with urgency, as each second counts once in the inside of a crisis. However, triage responders face the

intense challenge of filtering an unwieldy input supply into a condensed trickle of events. Here are some suggestions for expediting analysis before knowledge is validated:

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

NEW QUESTION 181

- (Exam Topic 2)

Abel, a security professional, conducts penetration testing in his client organization to check for any security loopholes. He launched an attack on the DHCP servers by broadcasting forged DHCP requests and leased all the DHCP addresses available in the DHCP scope until the server could not issue any more IP addresses. This led to a Dos attack, and as a result, legitimate employees were unable to access the clients network. Which of the following attacks did Abel perform in the above scenario?

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

Answer: B

Explanation:

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

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

In an unfriendly climate, where we have a malevolent machine running some sort of an instrument like Yersinia, there could be a machine that sends DHCP DISCOVER bundles. This malevolent customer doesn' send a modest bunch – it sends a great many vindictive DISCOVER bundles utilizing sham, made-up MAC addresses as the source MAC address for each solicitation.

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

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

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

NEW QUESTION 183

- (Exam 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 188

- (Exam 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 189

- (Exam 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 192

- (Exam 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 197

- (Exam Topic 1)

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

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

Answer: C

Explanation:

A powerful and often the most effective cryptanalysis method in which the attack is directed at the most vulnerable link in the cryptosystem - the person. In this attack, the cryptanalyst uses blackmail, threats, torture, extortion, bribery, etc. This method's main advantage is the decryption time's fundamental independence from the volume of secret information, the length of the key, and the cipher's mathematical strength.

The method can reduce the time to guess a password, for example, for AES, to an acceptable level; however, it requires special authorization from the relevant regulatory authorities. Therefore, it is outside the scope of this course and is not considered in its practical part.

NEW QUESTION 200

- (Exam Topic 1)

Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

- A. Macro virus
- B. Stealth/Tunneling virus
- C. Cavity virus
- D. Polymorphic virus

Answer: B

NEW QUESTION 205

- (Exam Topic 1)

Peter is surfing the internet looking for information about DX Company. Which hacking process is Peter doing?

- A. Scanning
- B. Footprinting
- C. Enumeration
- D. System Hacking

Answer: B

NEW QUESTION 207

- (Exam Topic 1)

What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

- A. Residual risk
- B. Impact risk
- C. Deferred risk
- D. Inherent risk

Answer: A

Explanation:

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

The residual risk is the risk or danger of an action or an event, a method or a (technical) process that, although being abreast with science, still conceives these dangers, even if all theoretically possible safety measures would be applied (scientifically conceivable measures); in other words, the amount of risk left over after natural or inherent risks have been reduced by risk controls.

· Residual risk = (Inherent risk) – (impact of risk controls)

NEW QUESTION 210

- (Exam Topic 1)

Which of the following is the BEST way to defend against network sniffing?

- A. Using encryption protocols to secure network communications
- B. Register all machines MAC Address in a Centralized Database
- C. Use Static IP Address
- D. Restrict Physical Access to Server Rooms hosting Critical Servers

Answer: A

Explanation:

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

To prevent networks from sniffing attacks, organizations and individual users should keep away from applications using insecure protocols, like basic HTTP authentication, File Transfer Protocol (FTP), and Telnet. Instead, secure protocols such as HTTPS, Secure File Transfer Protocol (SFTP), and Secure Shell (SSH) should be preferred. In case there is a necessity for using any insecure protocol in any application, all the data transmission should be encrypted. If required, VPN (Virtual Private Networks) can be used to provide secure access to users.

NOTE: I want to note that the wording "best option" is valid only for the EC-Council's exam since the other options will not help against sniffing or will only help from some specific attack vectors.

The sniffing attack surface is huge. To protect against it, you will need to implement a complex of measures at all levels of abstraction and apply controls at the physical, administrative, and technical levels. However, encryption is indeed the best option of all, even if your data is intercepted - an attacker cannot understand it.

NEW QUESTION 213

- (Exam 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 216

- (Exam 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 218

- (Exam Topic 1)

Which of the following incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an organization?

- A. Preparation phase
- B. Containment phase
- C. Identification phase
- D. Recovery phase

Answer: A

NEW QUESTION 222

- (Exam 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 226

- (Exam 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 228

- (Exam Topic 1)

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

However, he is unable to capture any logons though he knows that other users are logging in. What do you think is the most likely reason behind this?

- A. There is a NIDS present on that segment.
- B. Kerberos is preventing it.
- C. Windows logons cannot be sniffed.
- D. L0phtcrack only sniffs logons to web servers.

Answer: B

NEW QUESTION 230

- (Exam Topic 1)

Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform SNMP enquires over the network.

Which of these tools would do the SNMP enumeration he is looking for? Select the best answers.

- A. SNMPUtil
- B. SNScan
- C. SNMPScan
- D. Solarwinds IP Network Browser
- E. NMap

Answer: ABD

NEW QUESTION 233

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 234

- (Exam 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 236

- (Exam Topic 1)

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

When users accessed any page, the applet ran and exploited many machines. Which one of the following tools the hacker probably used to inject HTML code?

- A. Wireshark
- B. Ettercap
- C. Aircrack-ng
- D. Tcpdump

Answer: B

NEW QUESTION 238

- (Exam Topic 1)

When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's Computer to update the router configuration. What type of an alert is this?

- A. False negative
- B. True negative
- C. True positive
- D. False positive

Answer: D

Explanation:

True Positive - IDS referring a behavior as an attack, in real life it is

True Negative - IDS referring a behavior not an attack and in real life it is not False Positive - IDS referring a behavior as an attack, in real life it is not

False Negative - IDS referring a behavior not an attack, but in real life is an attack. False Negative - is the most serious and dangerous state of all !!!!

NEW QUESTION 239

- (Exam Topic 1)

You have the SOA presented below in your Zone.

Your secondary servers have not been able to contact your primary server to synchronize information. How long will the secondary servers attempt to contact the primary server before it considers that zone is dead and stops responding to queries?

collegae.edu.SOA, cikkye.edu ipad.college.edu. (200302028 3600 3600 604800 3600)

- A. One day
- B. One hour
- C. One week
- D. One month

Answer: C

NEW QUESTION 243

- (Exam Topic 1)

To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used to randomly generate invalid input in an attempt to crash the program.

What term is commonly used when referring to this type of testing?

- A. Randomizing
- B. Bounding
- C. Mutating
- D. Fuzzing

Answer: D

NEW QUESTION 244

- (Exam Topic 1)

Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?

- A. har.txt
- B. SAM file
- C. wwwroot
- D. Repair file

Answer: B

NEW QUESTION 247

- (Exam 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 249

- (Exam Topic 1)

The "Gray-box testing" methodology enforces what kind of restriction?

- A. Only the external operation of a system is accessible to the tester.
- B. The internal operation of a system is only partly accessible to the tester.
- C. Only the internal operation of a system is known to the tester.
- D. The internal operation of a system is completely known to the tester.

Answer: D**Explanation:**

White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of software testing that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing, an internal perspective of the system, as well as programming skills, are used to design test cases. The tester chooses inputs to exercise paths through the code and determine the expected outputs. This is analogous to testing nodes in a circuit, e.g. in-circuit testing (ICT). White-box testing can be applied at the unit, integration and system levels of the software testing process. Although traditional testers tended to think of white-box testing as being done at the unit level, it is used for integration and system testing more frequently today. It can test paths within a unit, paths between units during integration, and between subsystems during a system-level test. Though this method of test design can uncover many errors or problems, it has the potential to miss unimplemented parts of the specification or missing requirements. Where white-box testing is design-driven,[1] that is, driven exclusively by agreed specifications of how each component of the software is required to behave (as in DO-178C and ISO 26262 processes) then white-box test techniques can accomplish assessment for unimplemented or missing requirements.

White-box test design techniques include the following code coverage criteria:

- Control flow testing
- Data flow testing
- Branch testing
- Statement coverage
- Decision coverage
- Modified condition/decision coverage
- Prime path testing
- Path testing

NEW QUESTION 250

- (Exam 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 252**

- (Exam 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 254**

- (Exam Topic 1)

The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2014-0160. This bug affects the OpenSSL implementation of the Transport Layer Security (TLS) protocols defined in RFC6520.

What type of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?

- A. Public
- B. Private
- C. Shared
- D. Root

Answer: B**NEW QUESTION 258**

.....

