312-50V12^Q&As^

Certified Ethical Hacker Exam (CEHv12)

Pass EC-COUNCIL 312-50V12 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/312-50v12.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

During the process of encryption and decryption, what keys are shared?

A. Private keys

B. User passwords

C. Public keys

D. Public and private keys

Correct Answer: C

https://en.wikipedia.org/wiki/Public-key_cryptography Public-key cryptography, or asymmetric cryptography, is a cryptographic system that uses pairs of keys: public keys (which may be known to others), and private keys (which may never be known by any except the owner). The generation of such key pairs depends on cryptographic algorithms which are based on mathematical problems termed one-way functions. Effective security requires keeping the private key private; the public key can be openly distributed without compromising security. In such a system, any person can encrypt a message using the intended receiver\\'s public key, but that encrypted message can only be decrypted with the receiver\\'s private key. This allows, for instance, a server program to generate a cryptographic key intended for a suitable symmetric-key cryptography, then to use a client\\'s openly-shared public key to encrypt that newly generated symmetric key. The server can then send this encrypted symmetric key over an insecure channel to the client; only the client can decrypt it using the client\\'s private key (which pairs with the public key used by the server to encrypt the message). With the client and server both having the same symmetric key, they can safely use symmetric key encryption (likely much faster) to communicate over otherwise-insecure channels. This scheme has the advantage of not having to manually pre-share symmetric keys (a fundamentally difficult problem) while gaining the higher data throughput advantage of symmetric-key cryptography. With public-key cryptography, robust authentication is also possible. A sender can combine a message with a private key to create a short digital signature on the message. Anyone with the sender\\'s corresponding public key can combine that message with a claimed digital signature; if the signature matches the message, the origin of the message is verified (i.e., it must have been made by the owner of the corresponding private key). Public key algorithms are fundamental security primitives in modern cryptosystems, including applications and protocols which offer assurance of the confidentiality, authenticity and non-repudiability of electronic communications and data storage. They underpin numerous Internet standards, such as Transport Layer Security (TLS), S/MIME, PGP, and GPG. Some public key algorithms provide key distribution and secrecy (e.g., Diffie?ellman key exchange), some provide digital signatures (e.g., Digital Signature Algorithm), and some provide both (e.g., RSA). Compared to symmetric encryption, asymmetric encryption is rather slower than good symmetric encryption, too slow for many purposes. Today\\'s cryptosystems (such as TLS, Secure Shell) use both symmetric encryption and asymmetric encryption.

QUESTION 2

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

A. Advanced persistent

B. threat Diversion theft

C. Spear-phishing sites

D. insider threat

Correct Answer: A

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

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

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

an APT assault needs additional resources than a regular internet application attack. The perpetrators square measure typically groups of intimate cybercriminals having substantial resource. Some APT attacks square measure government-

funded and used as cyber warfare weapons.

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

They\\'re considerably additional advanced.

They\\'re not hit and run attacks--once a network is infiltrated, the culprit remains so as to realize the maximum amount info as potential. They\\'re manually dead (not automated) against a selected mark and indiscriminately launched against an

outsized pool of targets. They typically aim to infiltrate a complete network, as opposition one specific half. More common attacks, like remote file inclusion (RFI), SQL injection and cross-site scripting (XSS), square measure oftentimes

employed by perpetrators to ascertain a footing in a very targeted network. Next, Trojans and backdoor shells square measure typically wont to expand that foothold and make a persistent presence inside the targeted perimeter.

QUESTION 3

What is the following command used for?

net use \targetipc$ "" /u:"" A. Grabbing the etc/passwd file

B. Grabbing the SAM

C. Connecting to a Linux computer through Samba.

D. This command is used to connect as a null session

E. Enumeration of Cisco routers

Correct Answer: D

QUESTION 4

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

Correct Answer: A

QUESTION 5

What is correct about digital signatures?

A. A digital signature cannot be moved from one signed document to another because it is the hash of the original document encrypted with the private key of the signing party.

B. Digital signatures may be used in different documents of the same type.

C. A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.

D. Digital signatures are issued once for each user and can be used everywhere until they expire.

Correct Answer: A

QUESTION 6

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

Correct Answer: C

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)

QUESTION 7

During a black-box pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded. What type of firewall is inspecting outbound traffic?

A. Circuit

B. Stateful

C. Application

D. Packet Filtering

Correct Answer: C

https://en.wikipedia.org/wiki/Internet_Relay_Chat Internet Relay Chat (IRC) is an application layer protocol that facilitates communication in text. The chat process works on a client/server networking model. IRC clients are computer programs that users can install on their system or web-based applications running either locally in the browser or on a third-party server. These clients communicate with chat servers to transfer messages to other clients. IRC is a plaintext protocol that is officially assigned port 194, according to IANA. However, running the service on this port requires running it with root-level permissions, which is inadvisable. As a result, the well-known port for IRC is 6667, a high-number port that does not require elevated privileges. However, an IRC server can also be configured to run on other ports as well. You can\\'t tell if an IRC server is designed to be malicious solely based on port number. Still, if you see an IRC server running on port a WKP such as 80, 8080, 53, 443, it\\'s almost always going to be malicious; the only real reason for IRCD to be running on port 80 is to try to evade firewalls. https://en.wikipedia.org/wiki/Application_firewall An application firewall is a form of firewall that controls input/output or system calls of an application or service. It operates by monitoring and blocking communications based on a configured policy, generally with predefined rule sets to choose from. The application firewall can control communications up to the OSI model\\'s application layer, which is the highest operating layer, and where it gets its name. The two primary categories of application firewalls are network-based and host-based. Application layer filtering operates at a higher level than traditional security appliances. This allows packet decisions to be made based on more than just source/ destination IP Addresses or ports. It can also use information spanning across multiple connections for any given host.

Network-based application firewalls Network-based application firewalls operate at the application layer of a TCP/IP stack. They can understand certain applications and protocols such as File Transfer Protocol (FTP), Domain Name System (DNS), or Hypertext Transfer Protocol (HTTP). This allows it to identify unwanted applications or services using a non-standard port or detect if an allowed protocol is being abused.

Host-based application firewalls A host-based application firewall monitors application system calls or other general system communication. This gives more granularity and control but is limited to only protecting the host it is running on. Control is applied by filtering on a per-process basis. Generally, prompts are used to define rules for processes that have not yet received a connection. Further filtering can be done by examining the process ID of the owner of the data packets. Many host-based application firewalls are combined or used in conjunction with a packet filter.

QUESTION 8

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

Correct Answer: C

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.

QUESTION 9

Which DNS resource record can indicate how long any "DNS poisoning" could last?

A. MX

B. SOA

C. NS

D. TIMEOUT

Correct Answer: B

QUESTION 10

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

A. Man-in-the-disk attack

B. aLTEr attack

C. SIM card attack

D. Spearphone attack

Correct Answer: D

QUESTION 11

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

```
# nmap -sX host.domain.com
```

A. This is SYN scan. SYN flag is set.

B. This is Xmas scan. URG, PUSH and FIN are set.

C. This is ACK scan. ACK flag is set.

D. This is Xmas scan. SYN and ACK flags are set.

Correct Answer: B

QUESTION 12

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:]

Correct Answer: C

Google hacking or Google dorking https://en.wikipedia.org/wiki/Google_hacking It is a hacker technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites are using. Google dorking could also be used for OSINT.

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

-[site:] - Search within a specific website

QUESTION 13

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

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

A. Serverless computing

B. Demilitarized zone

C. Container technology

D. Zero trust network

Correct Answer: D

QUESTION 14

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

A. Black-box

B. Announced

C. White-box

D. Grey-box

Correct Answer: D

QUESTION 15

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

A. msfpayload

B. msfcli

C. msfd

D. msfencode

Correct Answer: D

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