312-50V12$^{Q\&As}$

Certified Ethical Hacker Exam (CEHv12)

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

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

QUESTION 1

You have gained physical access to a Windows 2008 R2 server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your toolkit, you have an Ubuntu 9.10 Linux LiveCD. Which Linux-based tool can change any user\\'s password or activate disabled Windows accounts?

A. John the Ripper

B. SET

C. CHNTPW

D. Cain and Abel

Correct Answer: C

QUESTION 2

A Certified Ethical Hacker (CEH) is given the task to perform an LDAP enumeration on a target system. The system is secured and accepts connections only on secure LDAP. The CEH uses Python for the enumeration process. After successfully installing LDAP and establishing a connection with the target, he attempts to fetch details like the domain name and naming context but is unable to receive the expected response. Considering the circumstances, which of the following is the most plausible reason for this situation?

A. The Python version installed on the CEH\\'s machine is incompatible with the Idap3 library

B. The secure LDAP connection was not properly initialized due to a lack of \\'use_ssl = True\\' in the server object creation

C. The enumeration process was blocked by the target system\\'s intrusion detection system

D. The system failed to establish a connection due to an incorrect port number

Correct Answer: B

The most plausible reason for the situation is that the secure LDAP connection was not properly initialized due to a lack of `use_ssl = True\\' in the server object creation. To use secure LDAP (LDAPS), the CEH needs to specify the use_ssl parameter as True when creating the server object with the ldap3 library in Python. This parameter tells the library to use SSL/TLS encryption for the LDAP communication. If the parameter is omitted or set to False, the library will use plain LDAP, which may not be accepted by the target system that only allows secure LDAP connections. For example, the CEH can use the following code to create a secure LDAP server object: from ldap3 import Server, Connection, ALL server = Server(\\'ldaps://\\', use_ssl=True, get_info=ALL) connection = Connection(server, user=\\'\\', password=\\'\\') connection.bind() The other options are not as plausible as option B for the following reasons:

A. The Python version installed on the CEH\\'s machine is incompatible with the ldap3 library: This option is unlikely because the ldap3 library supports Python versions from 2.6 to 3.9, which covers most of the commonly used Python

versions3. Moreover, if the Python version was incompatible, the CEH would not be able to install the library or import it in the code, and would encounter errors before establishing the connection. C. The enumeration process was blocked by

the target system\\'s intrusion detection system: This option is possible but not very plausible because the CEH was able to establish a connection with the target, which means the intrusion detection system did not block the initial handshake.

Moreover, the enumeration process would not affect the response of the target system, but rather the visibility of the results. If the intrusion detection system detected and blocked the enumeration, the CEH would receive an error message or

a blank response, not an unexpected response.

D. The system failed to establish a connection due to an incorrect port number:

This option is incorrect because the CEH was able to establish a connection with the target, which means the port number was correct. If the port number was incorrect, the CEH would not be able to connect to the target system at all, and

would receive a connection refused error.

References:

1: ldap3 - LDAP library for Python

2: How to use LDAPS with Python - Stack Overflow

3: ldap3 2.9 documentation

QUESTION 3

Sophia is a shopping enthusiast who spends significant time searching for trendy outfits online. Clark, an attacker, noticed her activities several times and sent a fake email containing a deceptive page link to her social media page displaying all-new and trendy outfits. In excitement, Sophia clicked on the malicious link and logged in to that page using her valid credentials. Which of the following tools is employed by Clark to create the spoofed email?

A. PyLoris

B. Slowloris

C. Evilginx

D. PLCinject

Correct Answer: C

QUESTION 4

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. Click here to reset your password and unlock your account."

C. A banner appears to a user stating, "Your Amazon order has been delayed. Click here to find out your new delivery date."

D. A pop-up appears to a user stating, "Your computer may have been infected with spyware. Click here to install an anti-spyware tool to resolve this issue."

Correct Answer: D

QUESTION 5

What is the known plaintext attack used against DES which gives the result that encrypting plaintext with one DES key followed by encrypting it with a second DES key is no more secure than using a single key?

A. Man-in-the-middle attack

B. Meet-in-the-middle attack

C. Replay attack

D. Traffic analysis attack

Correct Answer: B

https://en.wikipedia.org/wiki/Meet-in-the-middle_attack The meet-in-the-middle attack (MITM), a known plaintext attack, is a generic space-time tradeoff cryptographic attack against encryption schemes that rely on performing multiple encryption operations in sequence. The MITM attack is the primary reason why Double DES is not used and why a Triple DES key (168-bit) can be bruteforced by an attacker with 256 space and 2112 operations. The intruder has to know some parts of plaintext and their ciphertexts. Using meet-in-the- middle attacks it is possible to break ciphers, which have two or more secret keys for multiple encryption using the same algorithm. For example, the 3DES cipher works in this way. Meet-in-the-middle attack was first presented by Diffie and Hellman for cryptanalysis of DES algorithm.

QUESTION 6

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

Correct Answer: A

QUESTION 7

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

A. Password key hashing

B. Password salting

C. Password hashing

D. Account lockout

Correct Answer: B

Passwords are usually delineated as "hashed and salted". salting is simply the addition of a unique, random string of characters renowned solely to the site to every parole before it\\'s hashed, typically this "salt" is placed in front of each password. The salt value needs to be hold on by the site, which means typically sites use the same salt for each parole. This makes it less effective than if individual salts are used. The use of unique salts means that common passwords shared by multiple users ?like "123456" or "password" ?aren\\'t revealed revealed when one such hashed password is known ?because despite the passwords being the same the immediately and hashed values are not. Large salts also protect against certain methods of attack on hashes, including rainbow tables or logs of hashed passwords previously broken. Both hashing and salting may be repeated more than once to increase the issue in breaking the security.

QUESTION 8

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

A. Phishing malware

B. Zero-day malware

C. File-less malware

D. Logic bomb malware

Correct Answer: C

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

QUESTION 9

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 10

An organization has been experiencing intrusion attempts despite deploying an Intrusion Detection System (IDS) and Firewalls. As a Certified Ethical Hacker, you are asked to reinforce the intrusion detection process and recommend a better rule-based approach. The IDS uses Snort rules and the new recommended tool should be able to complement it. You suggest using YARA rules with an additional tool for rule generation. Which of the following tools would be the best choice for this purpose and why?

A. AutoYara - Because it automates the generation of YARA rules from a set of malicious and benign files

B. yarGen - Because it generates YARA rules from strings identified in malware files while removing strings that also appear in goodware files

C. YaraRET - Because it helps in reverse engineering Trojans to generate YARA rules

D. koodous - Because it combines social networking with antivirus signatures and YARA rules to detect malware

Correct Answer: B

YARA rules are a powerful way to detect and classify malware based on patterns, signatures, and behaviors. They can be used to complement Snort rules, which are mainly focused on network traffic analysis. However, writing YARA rules manually can be time-consuming and error-prone, especially when dealing with large and diverse malware samples. Therefore, using a tool that can automate or assist the generation of YARA rules can be very helpful for ethical hackers. Among the four options, yarGen is the best choice for this purpose, because it generates YARA rules from strings identified in malware files while removing strings that also appear in goodware files. This way, yarGen can reduce the false positives and increase the accuracy of the YARA rules. yarGen also supports various features, such as whitelisting, scoring, wildcards, and regular expressions, to improve the quality and efficiency of the YARA rules. The other options are not as suitable as yarGen for this purpose. AutoYara is a tool that automates the generation of YARA rules from a set of malicious and benign files, but it does not perform any filtering or optimization of the strings, which may result in noisy and ineffective YARA rules. YaraRET is a tool that helps in reverse engineering Trojans to generate YARA rules, but it is limited to a specific type of malware and requires manual intervention and analysis. koodous is a platform that combines social networking with antivirus signatures and YARA rules to detect malware, but it is not a tool for generating YARA rules, rather it is a tool for sharing and collaborating on YARA rules. References: yarGen - A Tool to Generate YARA Rules YARA Rules: The Basics Why master YARA: from routine to extreme threat hunting cases

QUESTION 11

In this attack, a victim receives an e-mail claiming from PayPal stating that their account has been disabled and confirmation is required before activation. The attackers then scam to collect not one but two credit card numbers, ATM PIN

number and other personal details. Ignorant users usually fall prey to this scam.

Which of the following statement is incorrect related to this attack?

A. Do not reply to email messages or popup ads asking for personal or financial information

B. Do not trust telephone numbers in e-mails or popup ads

C. Review credit card and bank account statements regularly

D. Antivirus, anti-spyware, and firewall software can very easily detect these type of attacks

E. Do not send credit card numbers, and personal or financial information via e-mail

Correct Answer: D

QUESTION 12

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

A. AOL

B. ARIN

C. DuckDuckGo

D. Baidu

Correct Answer: B

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

QUESTION 13

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

A. hping2 host.domain.com

B. hping2 --set-ICMP host.domain.com

C. hping2 -i host.domain.com

D. hping2 -1 host.domain.com

Correct Answer: D

http://www.carnal0wnage.com/papers/LSO-Hping2-Basics.pdf Most ping programs use ICMP echo requests and wait for echo replies to come back to test connectivity. Hping2 allows us to do the same testing using any IP packet, including ICMP, UDP, and TCP. This can be helpful since nowadays most firewalls or routers block ICMP. Hping2, by default, will use TCP, but, if you still want to send an ICMP scan, you can. We send ICMP scans using the -1 (one) mode. Basically the syntax will be hping2 -1 IPADDRESS [root@localhost hping2-rc3]# hping2 -1 192.168.0.100 HPING 192.168.0.100 (eth0 192.168.0.100): icmp mode set, 28 headers + 0 data bytes len=46 ip=192.168.0.100 ttl=128 id=27118 icmp_seq=0 rtt=14.9 ms len=46 ip=192.168.0.100 ttl=128 id=27119 icmp_seq=1 rtt=0.5 ms len=46 ip=192.168.0.100 ttl=128 id=27120 icmp_seq=2 rtt=0.5 ms len=46 ip=192.168.0.100 ttl=128 id=27121 icmp_seq=3 rtt=1.5 ms len=46 ip=192.168.0.100 ttl=128 id=27122 icmp_seq=4 rtt=0.9 ms -- 192.168.0.100 hping statistic -- 5 packets tramitted, 5 packets received, 0% packet loss round-trip min/avg/max = 0.5/3.7/14.9 ms [root@localhost hping2-rc3]#

QUESTION 14

Hackers often raise the trust level of a phishing message by modeling the email to look similar to the internal email used by the target company. This includes using logos, formatting, and names of the target company. The phishing message will often use the name of the company CEO, President, or Managers. The time a hacker spends performing research to locate this information about a company is known as?

A. Exploration

B. Investigation

C. Reconnaissance

D. Enumeration

Correct Answer: C

QUESTION 15

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

A. wash

B. ntptrace

C. macof

D. net View

Correct Answer: A