Exam Report: 8.1.15 Practice Questions

Date: 5/4/2020 6:13:57 pm
Time Spent: 32:53

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 82%

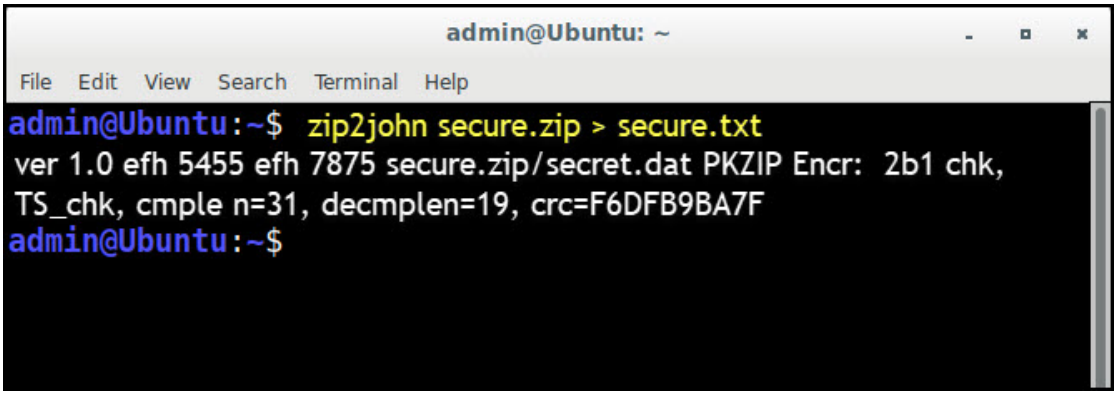
Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

You have just run the John the Ripper command shown in the image. Which of the following was this command used for?



- ~~To extract the password and save it in the secure.txt file.~~
- To extract the password and save it in a rainbow table named secure.txt.
- To extract the password hashes and save them in the secure.txt file.
- To extract the password from a rainbow hash and save it in the secure.txt file.

Explanation

The **zip2john** command is used to extract the password hashes from a zip file. Using the > output redirect operator saves the output to the specified file which is secure.txt in this case. After the hashes have been saved, you could run **john --format=pkzip secure.txt** to crack the password.

References

TestOut Ethical Hacker Pro - 8.1 System Hacking
[e_intro_hacking_eh1.exam.xml Q_INTRO_HACKING_JOHN_RIPPER_CRACK_EH1]

Question 2: Correct

Carl received a phone call from a woman who states that she is calling from his bank. She tells him that someone has tried to access his checking account and she needs him to confirm his account number and password to discuss further details. He gives her his account number and password. Which of the following types of non-technical password attack has occured?

- Password guessing
- Shoulder surfing
- Social engineering

- Dumpster diving

Explanation

Social engineering relies on human error. It works by feigning trustworthiness to convince someone to share information.

Shoulder surfing is watching and recording a password, pin, or access code that is being entered by someone nearby.

Dumpster diving relies on finding sensitive information that has been discarded in garbage cans, dumpsters, or other unsecure places that create access for attackers.

Password guessing happens when someone is able to easily guess a password, typically because it is very common, like a pet's name or a hobby.

References

TestOut Ethical Hacker Pro - 8.1 System Hacking
[e_intro_hacking_eh1.exam.xml Q_INTRO_HACKING_NONTECH_PASS_ATTACK_01_EH1]

Question 3: Correct

You are cleaning your desk at work. You toss several stacks of paper in the trash, including a sticky note with your password written on it. Which of the following types of non-technical password attacks have you enabled?

- Social engineering
- Dumpster diving
- Password guessing
- Shoulder surfing

Explanation

Dumpster diving relies on finding sensitive information that has been discarded in garbage cans, dumpsters, or other unsecure places that create access for attackers.

Shoulder surfing is watching and recording a password, pin, or access code that is being entered by someone nearby.

Social engineering relies on human error. It works by feigning trustworthiness to convince someone to give the attacker access.

Password guessing happens when someone is able to easily guess a password, typically because it is very common, like a pet's name or a hobby.

References

TestOut Ethical Hacker Pro - 8.1 System Hacking
[e_intro_hacking_eh1.exam.xml Q_INTRO_HACKING_NONTECH_PASS_ATTACK_02_EH1]

Question 4: Correct

Which of the following best describes shoulder surfing?

- Guessing someone's password because it is so common or simple.
- Someone nearby watches you enter your password on your computer and records it.
- Finding someone's password in the trash can and using it to access their account.
- Giving someone you trust your username and account password.

Explanation

Shoulder surfing is watching and recording a password, pin, or access code that is being entered by someone nearby.

Password guessing happens when someone is able to easily guess a password, typically because it is very

common, like "password", their pet's name, or their hobby.

Dumpster diving relies on finding sensitive information that has been discarded in garbage cans, dumpsters, or other unsecure places that create access for attackers.

Social engineering relies on human error. It works by convincing someone to give the attacker access because they trick them into trusting them.

References

TestOut Ethical Hacker Pro - 8.1 System Hacking
[e_intro_hacking_eh1.exam.xml Q_INTRO_HACKING_NONTECH_PASS_ATTACK_03_EH1]

Question 5: Correct

Which of the following techniques involves adding random bits of data to a password before it is stored as a hash?

- Keylogging
- Password sniffing
- Password salting
- Pass the hash

Explanation

Password salting is adding random bits of data to a password before it is stored as a hash, making password cracking much more difficult.

Password sniffing is a passive way for attackers to gain access to account. The sniffer collects data that is in transit in a LAN.

Pass the hash is a hacking technique where an attacker uses an underlying NTML or hash of a user's password to gain access to a server without ever using the actual plaintext password.

Keylogging is recording every stroke on the computer keyboard.

References

TestOut Ethical Hacker Pro - 8.1 System Hacking
[e_intro_hacking_eh1.exam.xml Q_INTRO_HACKING_PASS_CRACK_COUNTER_01_EH1]

Question 6: Correct

[!"#$%&'()*+,-./0123456789:;<=>?
@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~] are the possible values in which of the following hash types?

- Mix alpha-numeric
- Ascii-32-65-123-4
- Ascii-32-95
- Alpha-numeric-symbol32-space

Explanation

Ascii-32-95 characters can be any of the following: [!"#$%&'()*+,-./0123456789:;<=>?
@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~]

Ascii-32-65-123-4 characters can be any of the following: [!"#$%&'()*+,-./0123456789:;<=>?
@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`{|}~]

Alpha-numeric-symbol32-space characters can be any of the following:
[ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]

Mix alpha-numeric characters can be any of the following:
[abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]

References

TestOut Ethical Hacker Pro - 8.1 System Hacking
[e_intro_hacking_eh1.exam.xml Q_INTRO_HACKING_RAINBOWCRACK_01_EH1]

Question 7: Correct

Which of the following includes all possible characters or values for plaintext?

- Chain_len
- Chain_num
- Table_index
- Charset

Explanation

The charset includes all possible characters for the plaintext. For example, loweralpha-numeric is defined in charset.txt as [abcdefghijklmnopqrstuvwxyz0123456789].

The table_index parameter selects the reduction function. Rainbow tables with different table_index parameters use different reduction function.

Chain_num is the number of rainbow chains to generate. Rainbow table is simply an array of rainbow chains. The size of each rainbow chain is 16 bytes.

Chain_len is the rainbow chain length. A longer rainbow chain stores more plaintexts and requires more time to generate.

References

TestOut Ethical Hacker Pro - 8.1 System Hacking
[e_intro_hacking_eh1.exam.xml Q_INTRO_HACKING_RAINBOWCRACK_02_EH1]

Question 8: Incorrect

Jack is tasked with testing the password strength for the users of an organization. He has limited time and storage space. Which of the following would be the best password attack for him to choose?

- Brute force attack
- Keylogger attack
- ~~Dictionary attack~~
- Rainbow attack

Explanation

Rainbow attacks are like dictionary attacks, but instead of endlessly testing dictionary lists, they use tables that are precomputed with word lists and their hashes. This is much quicker than a dictionary attack or a brute-force attack and has much lower storage requirements.

In a dictionary attack, word lists often taken straight from dictionaries are tested against password databases. Beside all the standard words you find in a dictionary, these lists usually include variations on words that are common for passwords, like using the word "pa$$word". Lists can also include simple keyboard finger rolls, like q-w-e-r-t1234. The downside to this attack is this process can take a very long time.

In a brute force attack, every possible keystroke is tested for each single key in a password until the correct one is found. The disadvantages of this type of attack are that it takes a huge amount of processing power to execute and it is very time consuming.

Keyloggers record every stroke on the computer keyboard, but must either be installed manually on each computer with the hardware option, or every user will have to open an email attachment to install the software option. Both processes are very time consuming.

References

TestOut Ethical Hacker Pro - 8.1 System Hacking

[e_intro_hacking_eh1.exam.xml Q_INTRO_HACKING_RAINBOWCRACK_03_EH1]

Question 9: Correct

You have created and sorted an md5 rainbow crack table. You want to crack the password. Which of the following commands would you use to crack a single hash?

- **rcrack . -h 202cb962ac59075b964b07152d234b70**
- **rtgen md5 ascii-32-95 1 20 0 1000 1000 0**
- **rtgen sha1 ascii-32-95 1 20 0 1000 1000 0**
- **rcrack . -l /root/hashes.txt**

Explanation

The **rcrack . -h 202cb962ac59075b964b07152d234b70** command will crack the password contained in the **202cb962ac59075b964b07152d234b70** hash.

The **rcrack . -l /root/hashes.txt command** will crack all of the hashes contained in the hash file named hashes.txt.

The **rtgen sha1 ascii-32-95 1 20 0 1000 1000 0** command is used to create a sha1 rainbow crack table.

The **rtgen md5 ascii-32-95 1 20 0 1000 1000 0** command is used to create a md5 rainbow crack table.

References

TestOut Ethical Hacker Pro - 8.1 System Hacking
[e_intro_hacking_eh1.exam.xml Q_INTRO_HACKING_RAINBOWCRACK_04_EH1]

Question 10: Correct

You are using a password attack that tests every possible keystroke for each single key in a password until the correct one is found. Which of the following technical password attacks are you using?

- Pass the hash
- Password sniffing
- Brute force
- Keylogger

Explanation

In a brute force attack, every password will eventually be found because its technique is to test every possible keystroke for each single key in a password until the correct one is found.

Keyloggers log or record every keystroke on the computer keyboard to obtain passwords and other important data.

Pass the hash is a hacking technique where an attacker uses an underlying NTLM or hash of a user's password to gain access to a server without ever using the actual plaintext password.

Password sniffing is a passive way for attackers to gain access to an account. The sniffer collects data that is in transit in a LAN. If access is gained on one system in a LAN, then data can be gathered from data being sent from any other system in the network. The sniffer runs in the background, making it undetectable.

References

TestOut Ethical Hacker Pro - 8.1 System Hacking
[e_intro_hacking_eh1.exam.xml Q_INTRO_HACKING_TECH_PASS_ATTACK_01_EH1]

Question 11: Correct

Sam has used malware to access Sally's computer on the network. He has found information that will allow him to use the underlying NTLM to escalate his privileges without needing the plaintext password. Which of the following types of attacks did he use?

- Rainbow attack
- Password sniffing
- Pass the hash
- Dictionary attack

Explanation

Pass the hash is a hacking technique where an attacker uses an underlying NTLM or hash of a user's password to gain access to a server without ever using the actual plaintext password.

In a dictionary attack, word lists often taken straight from dictionaries are tested against password databases.

Password sniffing is a passive way for attackers to gain access to account. The sniffer collects data that is in transit in a LAN. If access is gained on one system in a LAN, the attacker can gather information being sent from any other system in the network.

Rainbow attacks are similar to dictionary attacks. Instead of endlessly testing dictionary lists, this method uses tables that are precomputed with word lists and their hashes.

References

TestOut Ethical Hacker Pro - 8.1 System Hacking
[e_intro_hacking_eh1.exam.xml Q_INTRO_HACKING_TECH_PASS_ATTACK_02_EH1]