COMP6224 Foundations of Cyber Security 2023/24

Coursework on Cyber Attack Analysis and Password Cracking

Student ID: *35424613*

Part 1 – Cyber-Attack Analysis

Task 1.1 – Kill Chain-based Analysis

The attack takes place in three steps.

First Step

Reconnaissance Phase

The first step of this 2-step attack is to find suitable employees to target and send the emails to in the router manufacturing company. This is an easier way to launch an attack since an insider is never suspected compared to an outsider/intruder and it is one of the easier ways in which an attacker gains accesses to internal systems without any misconception.

Weaponization Phase

The attacker sent an email with a malicious PDF in it, which upon clicking/opening installs malicious code in the employee's system. The PDF is the weapon used.

Delivery Phase

The PDF document was delivered to the employee's system via an email. This email contains the malicious PDF document which upon downloading infects the employee's system. This in turn results in the attackers taking control of the manufacturing companies' servers.

Exploitation Phase

The weapons here were mainly activated by means of User deception which is tricking the employee of the company to against the employer, which will benefit the attacker in one way or the other. Here in this case, the attacker makes the employee an insider, who will fetch the resources for the attacker. The employee must have opened the malicious PDF document which led the attacker to gain access of the employee's system.

Installation Phase

The attacker used the malicious PDF opened by an employee to install dangerous code/software in the employee's system.

Command and Control Phase

It is likely that the attackers gained access inside the employee's system by remotely executing using the malicious PDF opened by the employee. The server was then accessed for stolen credentials by remotely executing the code from the infected employee's system.

Second Step

Reconnaissance Phase

The server credentials of the router manufacturing company is being targeted by the attacker.

Weaponization Phase

Since this step was only to get the credentials of the server, no other weapons are being used.

Delivery Phase

The attackers have enough information to hack into the server and don't necessarily need any malware to be delivered.

Exploitation Phase

The attacker exploited the credentials by obtaining the confidential documents from the server which includes the detailed designs and technical specifications of the devices(routers) they produce.

Installation Phase

This phase was not specified in the document. But the attackers might have used malware(worms/trojans/botnets) to infect the server and obtain the designs and details of the routers the company designed.

Command and Control Phase

If botnets were used then the attacker might have had the advantage of infecting the server in no time and log all the activities, gather passwords etc. If worms were used, then the malware will be self-replicated into a lot of systems and the attacker can establish dominance. Else if Trojans are used, the attacker might have crucial information about the system or about the network.

Third Step

Reconnaissance Phase

The attackers, through their intelligence, gathered that the infected routers that are being used in the campaign of the political party's election. The zero-day vulnerability of the routers were exploited.

Weaponization Phase

The weapon used in this step was a type of malware called botnets. Botnets have the capability to spread on the internet in a large scale leading to immediate shutdown of the systems.

Delivery Phase

The attack was launched via the botnets by infecting the home internet routers.

Exploitation Phase

The attackers exploited the zero-day vulnerability of the routers to launch a Distributed Denial of Service and made the systems unavailable for many hours to gain complete control.

Installation Phase

The attacker might have installed a spyware (a kind of malware) to gather information about the computer and would have forwarded it to the third party.

Command and Control Phase

The launch of Distributed Denial of Service has made the home routers send many requests to the servers and these requests made the attackers gain access or complete dominance over the network.

Actions on Objective Phase

The result is not mentioned in the cyber-attack. The attackers might have been successful in their mission or not. Since there was a motive behind the attacker's actions, there must have been some ransom demand. But the cyber-attack mentions that there was no ransom demand from the political party's leader.

Task 1.2 – Cyber Actor Analysis

[*Up to 3 cyber actor profiles (or combinations of cyber actor profiles)*]

Cyber Actor Profile #1:.Cybercriminal

Attack Strategy

The cybercriminals use high end technology to compromise the network or information they want to attack. This attack can take many forms like Phishing, Hacking, DDos etc. In the above cyber-attack, the attacker used all three methods to bombard the network.

Motivations

The motivation here can be two types.
1.personal vengeance with the employee of the company. This motivates the attacker to bring bad name to him and his/her employer and demand a huge ransom from them to make it right in the market again.
2.Sometime attackers are hired by a third party for their own benefit. This may or may not benefit the cybercriminals. In this case they may be hired by the opponent political party to understand the political ideologies of the attacked party.

Cyber Actor Profile #2: Nation State

Attack Strategy

Nation state cyber threat actors are sophisticated and are often government backed. Since they have the license to hack, they sabotage and conduct espionage for the nation's benefits. They will be assigned to steal firm secrets, intercept critical discussions etc. In the given cyber-attack, they used well-crafted social engineering technique to target an employee inside the router manufacturing firm and sent him a phishing email. They might have also spread misinformation regarding the political parties' ideologies to the public.

Motivations

Nation state actors are purely motivated by nationalism. They do not want to be traced back and hence go to any lengths to achieve the attack. In this cyber-attack, with the information given, it seems that the main aim was not the ransom but to take down the political party by any means.

Cyber Actor Profile #3: Insider

Attack Strategy

The Insider in this case can be of two types.

1.Unintentional- The employee must have opened or clicked the phishing email and opened the document attached. This may lead to a malware installation in their computer.

2.Intentional- This happens when the insider wants to harm the organisation or a particular group people for personal benefits.

The given cyber-attack doesn't delve deep into this actor's role, but it can be either.

Motivations

The aftermath or the motivation behind this was that the illicit practise of intelligence gathering where they obtain other government's political ideas to use against them. This could have been done for political or financial advantage in this case.

Part 2 – Password Cracking

Task 2.1 - Dictionary-based cracking of passwords

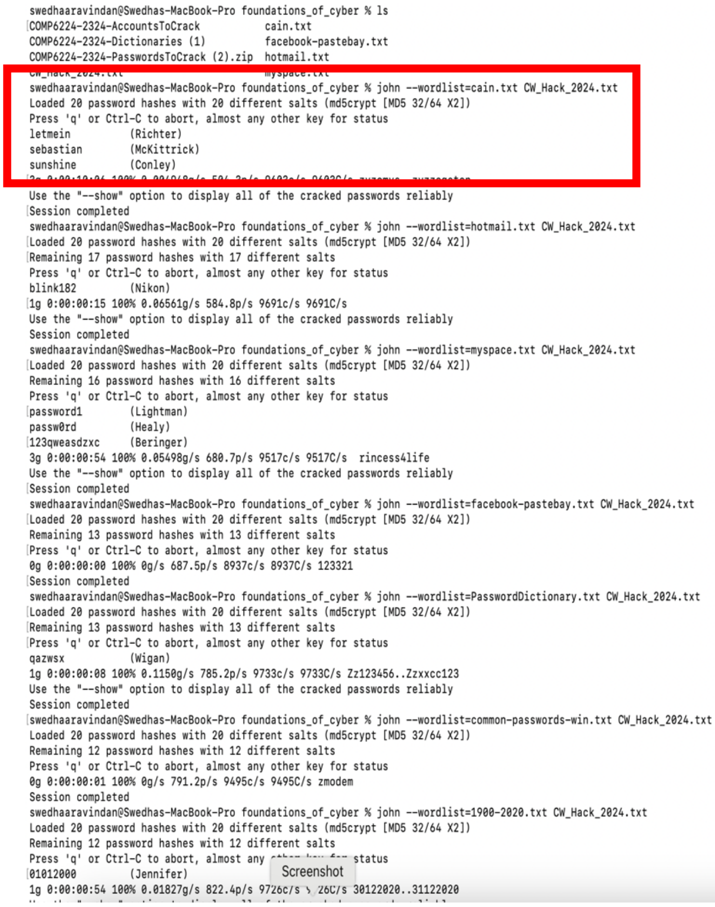
[*Up to 3 dictionaries, up to 20 passwords overall; you will need to add further hash/password entries*]

Dictionary #1

Name of the file: cain.txt

File source: Coursework Dictionary

Command (<u>also</u> include a screenshot): john --wordlist=cain.txt CW_Hack_2024.txt



```
swedhaaravindan@Swedhas-MacBook-Pro foundations_of_cyber % ls
COMP6224-2324-AccountsToCrack           cain.txt
COMP6224-2324-Dictionaries (1)          facebook-pastebay.txt
COMP6224-2324-PasswordsToCrack (2).zip  hotmail.txt
CW_Hack_2024.txt                        myspace.txt
swedhaaravindan@Swedhas-MacBook-Pro foundations_of_cyber % john --wordlist=cain.txt CW_Hack_2024.txt
Loaded 20 password hashes with 20 different salts (md5crypt [MD5 32/64 X2])
Press 'q' or Ctrl-C to abort, almost any other key for status
letmein          (Richter)
sebastian        (McKittrick)
sunshine         (Conley)
3g 0:00:10:04 100% [illegible]
Use the "--show" option to display all of the cracked passwords reliably
Session completed
swedhaaravindan@Swedhas-MacBook-Pro foundations_of_cyber % john --wordlist=hotmail.txt CW_Hack_2024.txt
Loaded 20 password hashes with 20 different salts (md5crypt [MD5 32/64 X2])
Remaining 17 password hashes with 17 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
blink182         (Nikon)
1g 0:00:00:15 100% 0.06561g/s 584.8p/s 9691c/s 9691C/s
Use the "--show" option to display all of the cracked passwords reliably
Session completed
swedhaaravindan@Swedhas-MacBook-Pro foundations_of_cyber % john --wordlist=myspace.txt CW_Hack_2024.txt
Loaded 20 password hashes with 20 different salts (md5crypt [MD5 32/64 X2])
Remaining 16 password hashes with 16 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
password1        (Lightman)
passw0rd         (Healy)
123qweasdzxc     (Beringer)
3g 0:00:00:54 100% 0.05498g/s 680.7p/s 9517c/s 9517C/s  rincess4life
Use the "--show" option to display all of the cracked passwords reliably
Session completed
swedhaaravindan@Swedhas-MacBook-Pro foundations_of_cyber % john --wordlist=facebook-pastebay.txt CW_Hack_2024.txt
Loaded 20 password hashes with 20 different salts (md5crypt [MD5 32/64 X2])
Remaining 13 password hashes with 13 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 100% 0g/s 687.5p/s 8937c/s 8937C/s 123321
Session completed
swedhaaravindan@Swedhas-MacBook-Pro foundations_of_cyber % john --wordlist=PasswordDictionary.txt CW_Hack_2024.txt
Loaded 20 password hashes with 20 different salts (md5crypt [MD5 32/64 X2])
Remaining 13 password hashes with 13 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
qazwsx           (Wigan)
1g 0:00:00:08 100% 0.1150g/s 785.2p/s 9733c/s 9733C/s Zz123456..Zzxxcc123
Use the "--show" option to display all of the cracked passwords reliably
Session completed
swedhaaravindan@Swedhas-MacBook-Pro foundations_of_cyber % john --wordlist=common-passwords-win.txt CW_Hack_2024.txt
Loaded 20 password hashes with 20 different salts (md5crypt [MD5 32/64 X2])
Remaining 12 password hashes with 12 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 100% 0g/s 791.2p/s 9495c/s 9495C/s zmodem
Session completed
swedhaaravindan@Swedhas-MacBook-Pro foundations_of_cyber % john --wordlist=1900-2020.txt CW_Hack_2024.txt
Loaded 20 password hashes with 20 different salts (md5crypt [MD5 32/64 X2])
Remaining 12 password hashes with 12 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
01012000         (Jennifer)
1g 0:00:00:54 100% 0.01827g/s 822.4p/s 9726c/s 9726C/s 30122020..31122020
Use the "--show" option to display all of the cracked passwords reliably
```

Cracked passwords

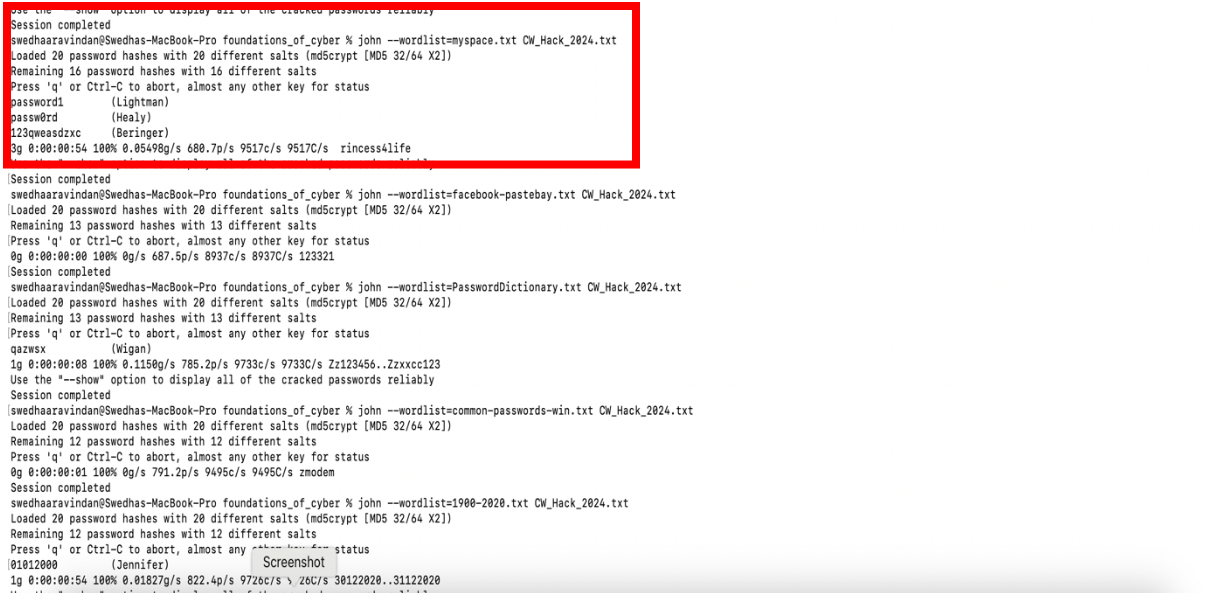
- password #1-letmein
- password #2-sebastian
- password #3-sunshine

Dictionary #2

Name of the file: myspace.txt

File source: Coursework Dictionary

Command (also include a screenshot): john --wordlist=myspace.txt CW_Hack_2024.txt



```
Use the "--show" option to display all of the cracked passwords reliably
Session completed
swedhaaravindan@Swedhas-MacBook-Pro foundations_of_cyber % john --wordlist=myspace.txt CW_Hack_2024.txt
Loaded 20 password hashes with 20 different salts (md5crypt [MD5 32/64 X2])
Remaining 16 password hashes with 16 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
password1        (Lightman)
passw0rd         (Healy)
123qweasdzxc     (Beringer)
3g 0:00:00:54 100% 0.05498g/s 680.7p/s 9517c/s 9517C/s  rincess4life
Use the "--show" option to display all of the cracked passwords reliably
Session completed
swedhaaravindan@Swedhas-MacBook-Pro foundations_of_cyber % john --wordlist=facebook-pastebay.txt CW_Hack_2024.txt
Loaded 20 password hashes with 20 different salts (md5crypt [MD5 32/64 X2])
Remaining 13 password hashes with 13 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 100% 0g/s 687.5p/s 8937c/s 8937C/s 123321
Session completed
swedhaaravindan@Swedhas-MacBook-Pro foundations_of_cyber % john --wordlist=PasswordDictionary.txt CW_Hack_2024.txt
Loaded 20 password hashes with 20 different salts (md5crypt [MD5 32/64 X2])
Remaining 13 password hashes with 13 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
qazwsx           (Wigan)
1g 0:00:00:08 100% 0.1150g/s 785.2p/s 9733c/s 9733C/s Zz123456..Zzxxcc123
Use the "--show" option to display all of the cracked passwords reliably
Session completed
swedhaaravindan@Swedhas-MacBook-Pro foundations_of_cyber % john --wordlist=common-passwords-win.txt CW_Hack_2024.txt
Loaded 20 password hashes with 20 different salts (md5crypt [MD5 32/64 X2])
Remaining 12 password hashes with 12 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 100% 0g/s 791.2p/s 9495c/s 9495C/s zmodem
Session completed
swedhaaravindan@Swedhas-MacBook-Pro foundations_of_cyber % john --wordlist=1900-2020.txt CW_Hack_2024.txt
Loaded 20 password hashes with 20 different salts (md5crypt [MD5 32/64 X2])
Remaining 12 password hashes with 12 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
01012000         (Jennifer)
1g 0:00:00:54 100% 0.01827g/s 822.4p/s 9726c/s 9726C/s 30122020..31122020
Use the "--show" option to display all of the cracked passwords reliably
```

Cracked passwords

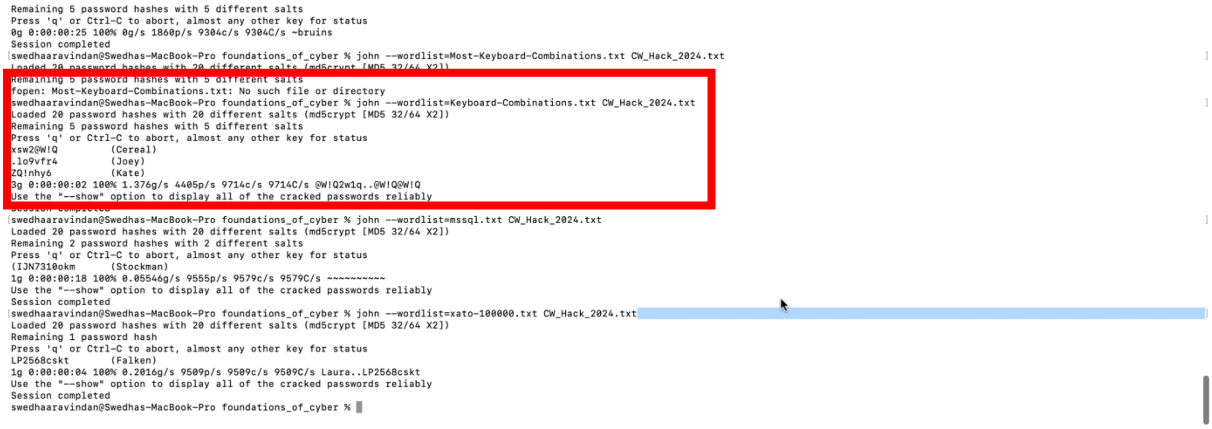
- password #1-password1
- password #2-passw0rd
- password #3-123qweasdzxc

Dictionary #3

Name of the file: Keyboard-Combinations.txt

File source: https://github.com/danielmiessler/SecLists/blob/master/Passwords/Keyboard-Combinations.txt

Command (also include a screenshot): john --wordlist=Keyboard-Combinations.txt CW_Hack_2024.txt



```
Remaining 5 password hashes with 5 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:25 100% 0g/s 1860p/s 9304c/s 9304C/s ~bruins
Session completed
swedhaaravindan@Swedhas-MacBook-Pro foundations_of_cyber % john --wordlist=Most-Keyboard-Combinations.txt CW_Hack_2024.txt
Loaded 20 password hashes with 20 different salts (md5crypt [MD5 32/64 X2])
Remaining 5 password hashes with 5 different salts
fopen: Most-Keyboard-Combinations.txt: No such file or directory
swedhaaravindan@Swedhas-MacBook-Pro foundations_of_cyber % john --wordlist=Keyboard-Combinations.txt CW_Hack_2024.txt
Loaded 20 password hashes with 20 different salts (md5crypt [MD5 32/64 X2])
Remaining 5 password hashes with 5 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
xsw2@W!Q         (Cereal)
.lo9vfr4         (Joey)
ZQ!nhy6          (Kate)
3g 0:00:00:02 100% 1.376g/s 4405p/s 9714c/s 9714C/s @W!Q2w1q..@W!Q@W!Q
Use the "--show" option to display all of the cracked passwords reliably
Session completed
swedhaaravindan@Swedhas-MacBook-Pro foundations_of_cyber % john --wordlist=mssql.txt CW_Hack_2024.txt
Loaded 20 password hashes with 20 different salts (md5crypt [MD5 32/64 X2])
Remaining 2 password hashes with 2 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
(IJN7310okm      (Stockman)
1g 0:00:00:18 100% 0.05546g/s 9555p/s 9579c/s 9579C/s ~~~~~~~~~~
Use the "--show" option to display all of the cracked passwords reliably
Session completed
swedhaaravindan@Swedhas-MacBook-Pro foundations_of_cyber % john --wordlist=xato-100000.txt CW_Hack_2024.txt
Loaded 20 password hashes with 20 different salts (md5crypt [MD5 32/64 X2])
Remaining 1 password hash
Press 'q' or Ctrl-C to abort, almost any other key for status
LP2568cskt       (Falken)
1g 0:00:00:04 100% 0.2016g/s 9509p/s 9509c/s 9509C/s Laura..LP2568cskt
Use the "--show" option to display all of the cracked passwords reliably
Session completed
swedhaaravindan@Swedhas-MacBook-Pro foundations_of_cyber %
```

Cracked passwords

- password #1-xsw2@W!Q
- password #2-.lo9vfr4

- password #3-ZQ!nhy6

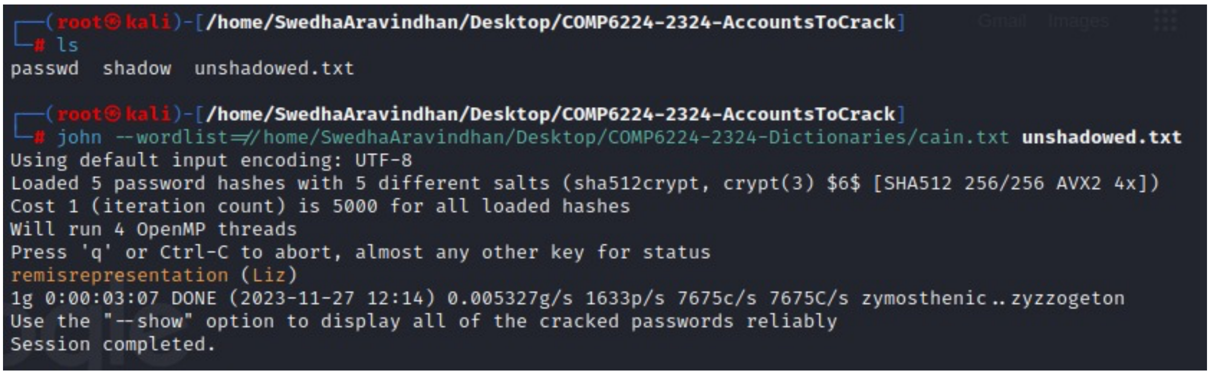
Task 2.2 - Password cracking of Linux accounts

Brute force

Brute force password cracking is essentially time consuming and resource intensive. Since passwords used in the dictionary are complex, it becomes more and more difficult for us to crack the passwords in brute forcing.

Dictionary

Command : john --wordlist=//home/SwedhaAravindhan/Desktop/COMP6224-2324-Dictionaries/myspace.txt unshadowed.txt



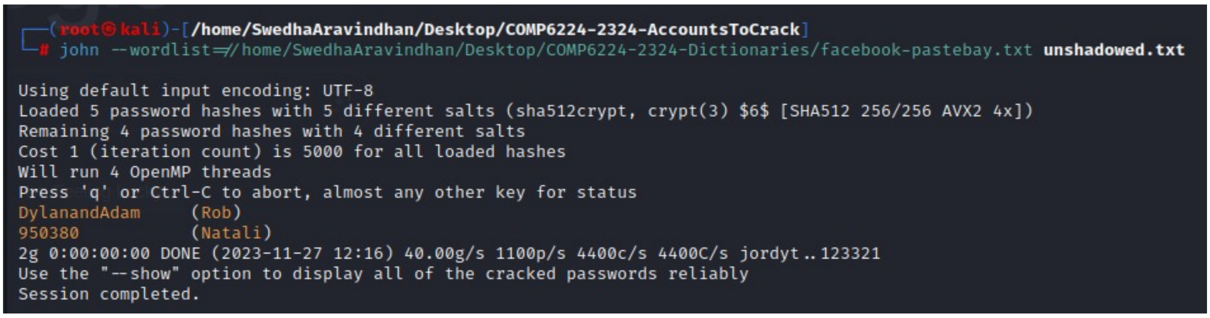
```
┌──(root㉿kali)-[/home/SwedhaAravindhan/Desktop/COMP6224-2324-AccountsToCrack]
└─# ls
passwd  shadow  unshadowed.txt

┌──(root㉿kali)-[/home/SwedhaAravindhan/Desktop/COMP6224-2324-AccountsToCrack]
└─# john --wordlist=//home/SwedhaAravindhan/Desktop/COMP6224-2324-Dictionaries/cain.txt unshadowed.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
remisrepresentation (Liz)
1g 0:00:03:07 DONE (2023-11-27 12:14) 0.005327g/s 1633p/s 7675c/s 7675C/s zymosthenic..zyzzogeton
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Cracked passwords

- username #1- Liz
- password #1 - remisrepresentation

Command: john --wordlist=//home/SwedhaAravindhan/Desktop/COMP6224-2324-Dictionaries/facebook-pastebay.txt unshadowed.txt



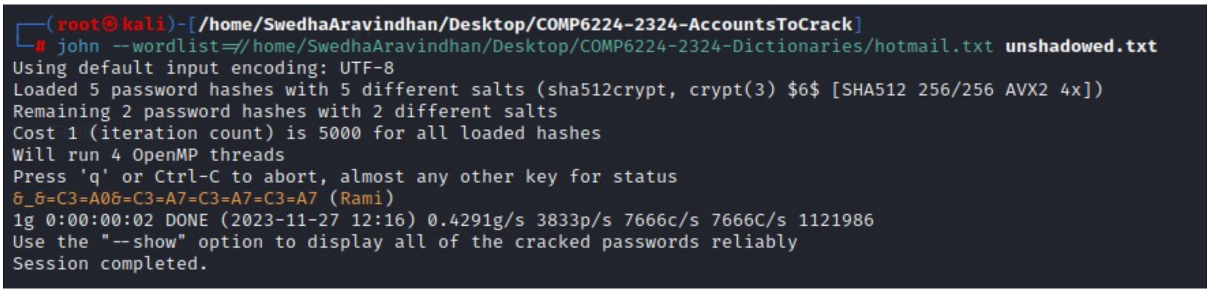
```
┌──(root㉿kali)-[/home/SwedhaAravindhan/Desktop/COMP6224-2324-AccountsToCrack]
└─# john --wordlist=//home/SwedhaAravindhan/Desktop/COMP6224-2324-Dictionaries/facebook-pastebay.txt unshadowed.txt

Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Remaining 4 password hashes with 4 different salts
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
DylanandAdam     (Rob)
950380           (Natali)
2g 0:00:00:00 DONE (2023-11-27 12:16) 40.00g/s 1100p/s 4400c/s 4400C/s jordyt..123321
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Cracked passwords

- username #1- Rob
- password #1- DylanandAdam
- username #2-Natali
- password #2-950380

Command: john --wordlist=//home/SwedhaAravindhan/Desktop/COMP6224-2324-Dictionaries/hotmail.txt unshadowed.txt

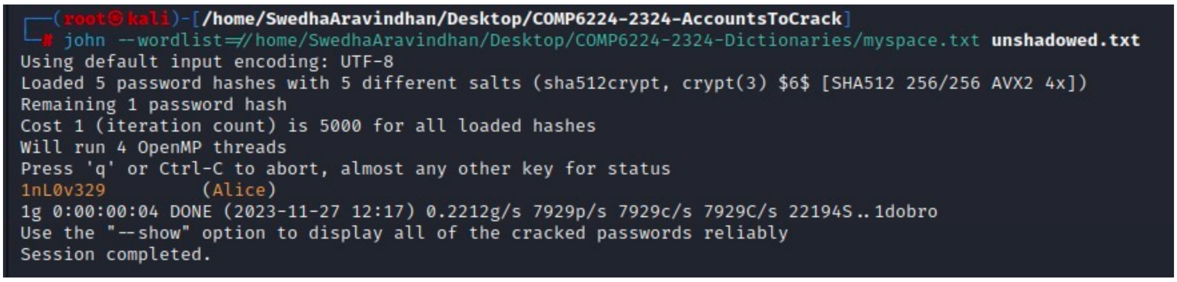


```
┌──(root㉿kali)-[/home/SwedhaAravindhan/Desktop/COMP6224-2324-AccountsToCrack]
└─# john --wordlist=//home/SwedhaAravindhan/Desktop/COMP6224-2324-Dictionaries/hotmail.txt unshadowed.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Remaining 2 password hashes with 2 different salts
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
&_&=C3=A0&=C3=A7=C3=A7=C3=A7 (Rami)
1g 0:00:00:02 DONE (2023-11-27 12:16) 0.4291g/s 3833p/s 7666c/s 7666C/s 1121986
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Cracked passwords

- username #1-Rami
- password #1- &_&=C3=A0&=C3=A7=C3=A7=C3=A7

Command: john --wordlist=//home/SwedhaAravindhan/Desktop/COMP6224-2324-Dictionaries/myspace.txt unshadowed.txt



```
┌──(root㉿kali)-[/home/SwedhaAravindhan/Desktop/COMP6224-2324-AccountsToCrack]
└─# john --wordlist=//home/SwedhaAravindhan/Desktop/COMP6224-2324-Dictionaries/myspace.txt unshadowed.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Remaining 1 password hash
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
1nL0v329         (Alice)
1g 0:00:00:04 DONE (2023-11-27 12:17) 0.2212g/s 7929p/s 7929c/s 7929C/s 22194S..1dobro
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Cracked passwords

- username #1-Alice
- password #1-1nL0v329

Result Comparison [max 200 words]

Dictionary based password cracking is far better method to crack passwords than brute force because of the following reasons:

-Brute force method is time consuming and resource intensive since they try every combination and permutation of the given pattern. Whereas Dictionary based is a targeted approach focusing on a limited set of passwords

-Brute force is less effective whereas Dictionary based attack is efficient where it involves targeting a specific set of pre-defined passwords in a dictionary which makes it easier.

-Brute force is done for every combination of a set of word whereas dictionary based attack targets common passwords and phrases first in order to get them cracked. This makes Dictionary based attack more successful.

Task 2.3 - Password analysis

Password #1

Password: letmein

Weaknesses

- weakness #1 – It could Possibly be a word associated with the individual.
- weakness #2 – It is a Common password and easily guessable
- weakness #3 - Short in length
- weakness #4 – No character variety, no numbers and symbols

Password #2

Password: sebastian

Weaknesses

- weakness #1 – It could Possibly be a word which is a name of the individual (personal information)
- weakness #2 – It is a moderately Common password
- weakness #3 - Short in length
- weakness #4 – No character variety, no numbers and symbols

Password #3

Password: sunshine

Weaknesses

- weakness #1 – It is a word from dictionary
- weakness #2 – It is a significantly Common password
- weakness #3 - Short in length
- weakness #4 – No character variety, no numbers and symbols

Password #4

Password: blink182

Weaknesses

- weakness #1 – It is a word and a number which is
- weakness #2 – It is a Common password
- weakness #3 - Short in length
- weakness #4 – No symbols

Password #5

Password: password1

Weaknesses

- weakness #1– It is a very Common password
- weakness #2 - Short in length
- weakness #3– No character variety, no symbols

Password #6

Password: passw0rd1

Weaknesses

- weakness #1 – It has a character that resembles a numerical which is easily identified.
- weakness #2 – It is a Common password
- weakness #3 - Short in length
- weakness #4 – No character variety, no numbers and symbols

Password #7

Password: 123qweasdzxc

Weaknesses

- weakness #1 – Easily guessable using a qwerty keyboard
- weakness #2 – It is a Common password
- weakness #3 – No character variety, no symbols
-

Password #8

Password: qazwsx

Weaknesses

- weakness #1 – Easily guessable using a qwerty keyboard
- weakness #2 – It is a Common password

- weakness #3 – No character variety, no symbols and numbers
- weakness #4- Short in length

Password #9

Password: 01012000

Weaknesses

- weakness #1 – Might be a personal information. ex: date or phone number
- weakness #2 – It is a Common password
- weakness #3- Short in length
- weakness #4 – No character variety, no alphabets and symbols

Password #10

Password: clotilde

Weaknesses

- weakness #1 – Might be a personal data ex: name or it can be a word from dictionary
- weakness #2 – short in length
- weakness #3– No character variety, no symbols and numbers

Password #11

Password: 1100101

Weaknesses

- weakness #1 – Might be a personal information. ex: date or phone number
- weakness #2 – Short in length
- weakness #3– No character variety , no symbols

Password #12

Password: dieumerci

Weaknesses

- weakness #1 – Might be a personal data ex: name or it can be a word from dictionary
- weakness #2 – short in length
- weakness #3– No character variety , no symbols and numbers
- weakness #4- Common French password. This word means “Thank God” which is common.
-

Password #13

Password: mamanjetaime

Weaknesses

- weakness #1 – Might be a personal data ex: name or it can be a word from dictionary.
- weakness #2 – short in length
- weakness #3– No character variety , no symbols and numbers
- weakness #4- Common French password. This word means “Mom, I love You’ which is common.
-

Password #14

Password: 12368878794

Weaknesses

- weakness #1 – Might be a personal information. ex: date or phone number
- weakness #2– No character variety , no symbols and alphabets

Password #15

Password: 34250003024812

Weaknesses

- weakness #1 – Might be a personal information. ex: date or phone number
- weakness #2– No character variety , no symbols and alphabets

Password #16

Password: xsw2@W!Q

Weaknesses

- weakness #1 – Short in length

Password #17

Password: .lo9vfr4

Weaknesses

- weakness #1 – Short in length
- weakness #2– No character variety

Password #18

Password: ZQ!nhy6

Weaknesses

- weakness #1 – Short in length

Password #19

Password: LP2568cskt

Weaknesses

- weakness #1 – Short in length
- weakness #2– No symbol is used

Password #20

Password: (IJN7310okm

Weaknesses

- No weakness

Password #21

Password: remisrepresentation

Weaknesses

- weakness #1 – No symbols and numbers are used
- weakness #2 – It can be personal data . For ex. This can be a name of a person
- weakness #3 – This is a word commonly found in dictionaries, so easy to crack.
- weakness #4

Password #22

Password: DylanandAdam

Weaknesses

- weakness #1 – No character variety is displayed. No number and symbols
- weakness #2 -Easily predictable is the attacker is aware of the individuals personal life.
- weakness #3 – Short in length

Password #23

Password: 950380

Weaknesses

- weakness #1 If the attacker has knowledge on individuals' personal life, then they can guess this password easily. It can be the birth date or phone number of that person.
- weakness #2 Short in Length
- weakness #3 No character variety-no alphabets and symbols
- weakness #4 Character set is narrowed since only numbers are used.

Password #24

Password: &_&=C3=A0&=C3=A7=C3=A7=C3=A7

Weaknesses

- weakness #1 It can be an encoding of the URL
- weakness #2 If the attacker understood that this password has URL encoded value, this limits the set used for cracking and hence easily identified.

Password #25

Password: 1nL0v329

Weaknesses

- weakness #1 Short in length
- weakness #2 No character variety-no symbols are being used
- weakness #3 Easily cracked if the attacker is aware of individuals personal life.
- Weakness #4 Common password – IN LOVE is phrased as the above password which could be an easy guess for the attacker.