

Coursework on Cyber Attack Analysis and Password Cracking

Student ID: 31990401

Part 1 – Cyber-Attack Analysis

Task 1.1 – Kill Chain-based Analysis

Reconnaissance Phase – 1st step of the attack

The reconnaissance phase is related to the attempt of the adversary to collect as much as possible information related to the target before the initial attack takes place. In our case (attack of the 1st step of the kill chain) we have to deal with an attack to the router's manufacture database. In the reconnaissance phase in this attack, hackers tried to collect the employee's emails in order to forward them the malicious PDF document.

Weaponization Phase – 1st step of the attack

The weaponization phase is about the preparation of cyber weapons that are going to be used in the attack. In this case, the hackers used a malicious PDF file. Malicious PDF files (most of the time embedded with payloads) it is always a very simple way of infecting the target's machines because this type of documents is very popular, and it is used almost by everyone. In this phase, the attackers could also prepare the mechanism to be used in the command-and-control phase.

Delivery Phase – 1st step of the attack

This phase is about the cyber weapon is delivered to the target. In this case, the malicious PDF document was delivered through an email. To be precise, hackers attached the malicious PDF inside an email and send it to an employee. The employee opened the email and therefore the malicious PDF document without having knowledge of the consequences. As a result, he/she gave hackers remote access to his/her computer.

Exploitation Phase – 1st step of the attack

This phase is related to the payload execution. In our case, the payload was executed through a PDF file. In more detail, PDF documents are object-oriented format documents so the data inside them (images, font types, etc.) are called objects. Each object acts in its own way while the file is opened. So, hackers added one more object in this PDF. This object was a piece of code (malicious) that is executed every time the file is opened.

Installation Phase – 1st step of the attack

In this phase, we examine the way the payload remained persistent. In this attack hackers wanted the victim to open the PDF document, then the payload is executed, and finally, this payload activated every time automatically. Hackers achieved this maybe by giving the payload the ability to be executed automatically every time the victim's computer was rebooted. The folder may be added to the list of the programs that are run automatically on start-up. They may also have created the payload in such a way that it is not detectable by any firewall or antivirus software.

Command and Control Phase – 1st step of the attack

The command and control phase is about establishing communication between the attacker and the victim. Hackers succeed to gain access to the victim's computer through a PDF payload. There are many PDF payloads. One of them is the payload that can give remote access to the attacker. Now, after the payload installed and executed, a connection was opened between the attacker's computer and the victim's computer. This payload gave the attacker the opportunity to use the victim's computer maybe with a terminal. As a result, the attackers were sending commands and the payload was answering with the server's information.

Reconnaissance Phase – 2nd step of the attack

This is the reconnaissance phase of the second step of the attack. In this case, hackers had already crucial technical information about the routers. The next step was to map the router's functionality and search for possible vulnerabilities (like the zero-day they found). So, they have maybe searched for any open ports in order to exploit it. They could have also searched for important router information (last update of the OS, new features, version). Finally, hackers could have searched and collected information about any possible firewall in order to overpass it.

Weaponization Phase – 2nd step of the attack

This phase of armaments involves settling the cyber cannons used by hackers to attack DDoS. According to the attack description, the DDoS attack was accomplished using a botnet. As a result, the cyber-weapon of the main hacker was the botnet that was installed on the router and then launched the DDoS attack. In this phase, the attackers could also prepare the mechanism to be used in the command-and-control phase.

Delivery Phase – 2nd step of the attack

In this phase, the cyber weapon (which is the botnet) delivered to the target (router) through a zero-day vulnerability. Hackers used this vulnerability in order to install the Bonet in the routers. This vulnerability could have been an open port like port 21 (FTP). As a result, hackers forwarded the botnet through FTP in the routers and then they installed it. The installation process could have been achieved because another port like 22 (SSH) could have been also open. Thus, hackers could also have access to a terminal, from which they were able to execute commands.

Exploitation Phase – 2nd step of the attack

The exploitation phase concerns how the botnet is executed by the router. In this case, each time the router was activated and connected to the network, the botnet was also activated and began sending multiple requests to the election website. The botnet could also be activated and send requests after the hackers give the appropriate commands.

Installation Phase – 2nd step of the attack

This phase related to the way the botnet remains installed and activated in the router. The botnet should be automatically activated after a reboot. Hackers may have been flag it as an important process so when the router is activated then the botnet is activated too. Hackers also had to think about a possible reboot or a format. For this reason, every time a new router is activated and connected to the network, another activated router sends the botnet to the new router. As a result, the botnet is always installed and ready to run in every router.

Command and Control Phase – 2nd step of the attack

This phase describes the way the botnet was communicating with the server in which the election system was stored. The attackers were aiming for the routers in order to spread their botnet and launch the DDoS attack. At this phase, after the attackers gained access to the routers, they may have used a terminal from which they sent commands to each of them individually to begin sending multiple requests to the site.

Actions on Objective Phase

From the first attack hackers achieved to gain some very important and crucial technical information about the routers. Next, by using this information they exploit a zero-day vulnerability and took the control of the routers by installing in them the botnets. Their initial purpose was to make a DDoS attack by using the botnet. So, they did. Hackers finally achieved to do the DDoS attack and set the election system out of order which resulted in the freezing of the election process.

Task 1.2 – Cyber Actor Analysis

Cyber Actor Profile #1: *National State*

Attack Strategy

Two of the most popular Nation States attacks are data breaches and DDoS. The reason of the first attack (data breach) is the leak of crucial information that can be helpful while the reason of the second attack (DDoS) is the disruption of the target system. The same strategy was implemented here as well. At first a data breach attack to the servers of the router manufacturer resulted in leaking crucial information (detailed design and technical specification of produced devices). Finally, the manipulation of the election system was achieved by using this information and by performing a DDoS attack.

Motivations

National-State hackers do work under a government and their purpose is to disrupt or set in danger adversary governments, organizations, or individuals and even to cause national incidents. In our case, National-State hackers aim for the elections in order to disrupt and manipulate the whole process. Their motivation could be the facilitations which could be offered by a candidate in business activities of the attacking country (e.g., better commercial circumstances or cases related to national defence and security).

Cyber Actor Profile #3: *Hacktivists*

Attack Strategy

Hackivist's purpose is the disturbance of the whole election process in order to express the different ideology. Therefore, in our case Hackivist's strategy is to set the election system out of order and freeze the whole process. This is the reason they selected the DDoS attack. Nevertheless, in order to accomplish this attack, some other important data are required (detailed design and technical specification of produced devices). These data have successfully come to their hands by performing a data breach attack.

Motivations

Hackivist's activities are related to ideological beliefs. In this case, hacktivists have ideologically motivated. For instance, they could disagree with the political ideas of the current government and try to weaken it. Furthermore, there is a possibility that Hackivist's ideas could be closer to another candidate political group. Finally, this attack could be in order for the Hacktivists to express their arguments about the election process.

Cyber Actor Profile #2: *Cybercriminals*

Attack Strategy

Data breach attack and DDoS is also some of the Cybercriminal's most popular attacks. Holding crucial information by a data breach attack can offer money to the attacker by demanding a ransom. In the same way a DDoS attack can offer money to the attacker (by demanding ransom). However, in our case Cybercriminals strategy wasn't to earn money by the data breach attack. Instead, they strategy was to use the data from the first attack (data breach) in order to implement the second attack (DDoS) from which they could ask for ransom.

Motivations

Cybercriminals are professional hackers who act in groups or even individually and their aim is their financial growth. In our case, Cybercriminals aim the elections, and their motivation could be financial. More specifically they could aim to gain a ransom in order to allow the election processes to be proceeding normally and to avoid the absence of government for an extended time.

Part 2 – Password Cracking

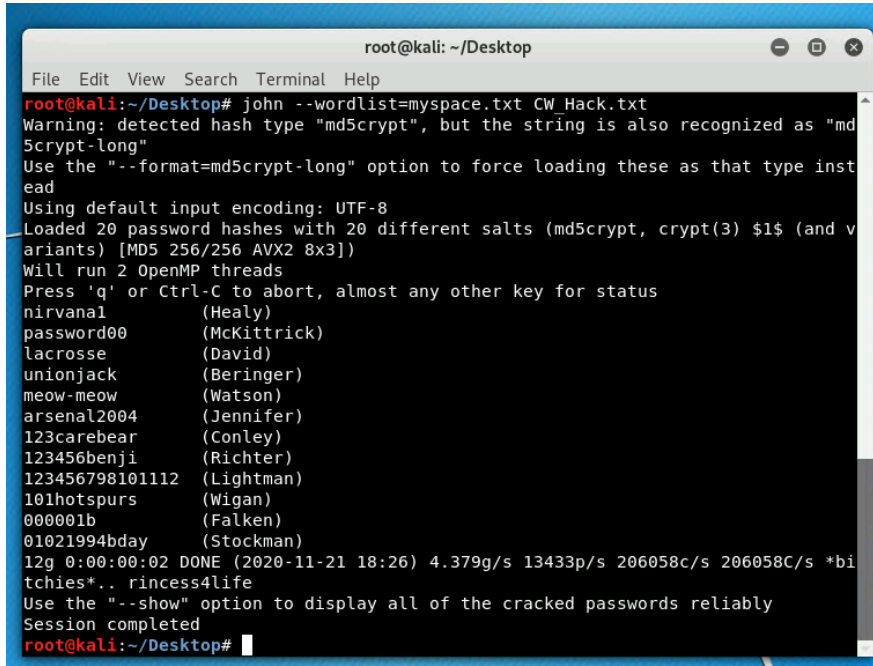
Task 2.1 - Dictionary-based cracking of passwords

Dictionary #1

Name of the file: myspace.txt

File source: From the coursework description PDF

Command: john - -wordlist=myspace.txt CW_Hack.txt



```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# john --wordlist=myspace.txt CW_Hack.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 20 password hashes with 20 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
nirvana1      (Healy)
password00    (McKittrick)
lacrosse      (David)
unionjack     (Beringer)
meow-meow     (Watson)
arsenal2004   (Jennifer)
123carebear   (Conley)
123456benji   (Richter)
123456789101112 (Lightman)
101hotspurs   (Wigan)
000001b       (Falken)
01021994bdy   (Stockman)
12g 0:00:00:02 DONE (2020-11-21 18:26) 4.379g/s 13433p/s 206058c/s 206058C/s *bi
tchies*.. rincess4life
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/Desktop#
```

Cracked passwords

- hash #1 - Healy:\$1\$dMG.Angc\$voUcF5OMOKVe8KRVPZDo0
- password #1 – nirvana1
- hash #2 - McKittrick:\$1\$gkxqsm6d\$EannM7a0wE0usozhaFtbZ0
- password #2 – password00
- hash #3 - David:\$1\$PYq9qbxG\$R1f0XANjTVUqY2jirDP2m0
- password #3 – lacrosse
- hash #4 - Beringer:\$1\$5CZTjuJz\$PdZgIxi04/VQfXau7yyOw/
- password #4 – unionjack
- hash #5 - Watson:\$1\$TXSDBii1\$M5W3gSEE1XEpJQMga2HwW/
- password #5 – meow-meow
- hash #6 - Jennifer:\$1\$29dLGi5L\$wq9cbXQk6qVqd9JP9k064/
- password #6 – arsenal2004
- hash #7 - Conley:\$1\$/QwXbILh\$I1LI3AMVBNomyGjVk.81q0
- password #7 – 123carebear
- hash #8 - Richter:\$1\$IqbHHqMW\$SUFNvBsVsOfRPLuRvv9vO/
- password #8 – 123456benji
- hash #9 - Lightman:\$1\$a.z3IJo7\$62zWdQ6.Yxcs3UXIBJ4Vt0
- password #9 – 123456789101112
- hash #10 - Wigan:\$1\$ixKfMrwa\$V6xH6lQlYH0rIRLksFVnt1
- password #10 – 101hotspurs
- hash #11 - Falken:\$1\$KTgPnjaP\$4qzISB6.eBXQnAav4UfmX/

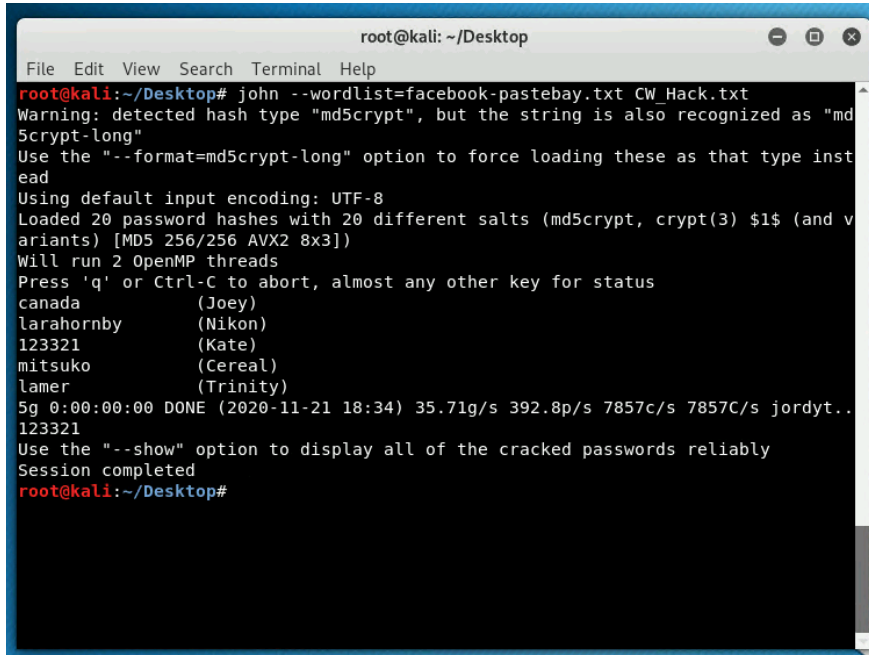
- password #11 – 000001b
- hash #12 - Stockman:\$1\$Su705PPY\$OIJPpxplJZ2QBinBNXyGN.
- Password #12 – 01021994bday

Dictionary #2

Name of the file: facebook-pastebay.txt

File source: From the coursework description PDF

Command: john --wordlist=facebook-pastebay.txt CW_Hack.txt



```

root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# john --wordlist=facebook-pastebay.txt CW_Hack.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 20 password hashes with 20 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
canada (Joey)
lara-hornby (Nikon)
123321 (Kate)
mitsuko (Cereal)
lamer (Trinity)
5g 0:00:00:00 DONE (2020-11-21 18:34) 35.71g/s 392.8p/s 7857c/s 7857C/s jordyt..
123321
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/Desktop#

```

Cracked passwords

- hash #1 - Joey:\$1\$A6uxrwMh\$scnihk/f7p7lwLeG0Uk2kx/
- password #1 - canada
- hash #2 - Nikon:\$1\$DM0bcOtQ\$Esuad9Ha8hJYfJb2Tgocu.
- password #2 – lara-hornby
- hash #3 - Kate:\$1\$GBji2U4L\$6XW.cfaqF0UwtI1/ZZ3BG1
- password #3 – 123321
- hash #4 - Cereal:\$1\$SwEULC2V\$kBZQ8NAXcSJL5KrWIJZY./
- password #4 – Mitsuko
- hash #5 - Trinity:\$1\$puf4MBZ9\$UzrhWH83A4HtVVUVakwTp0
- password #5 – lamer

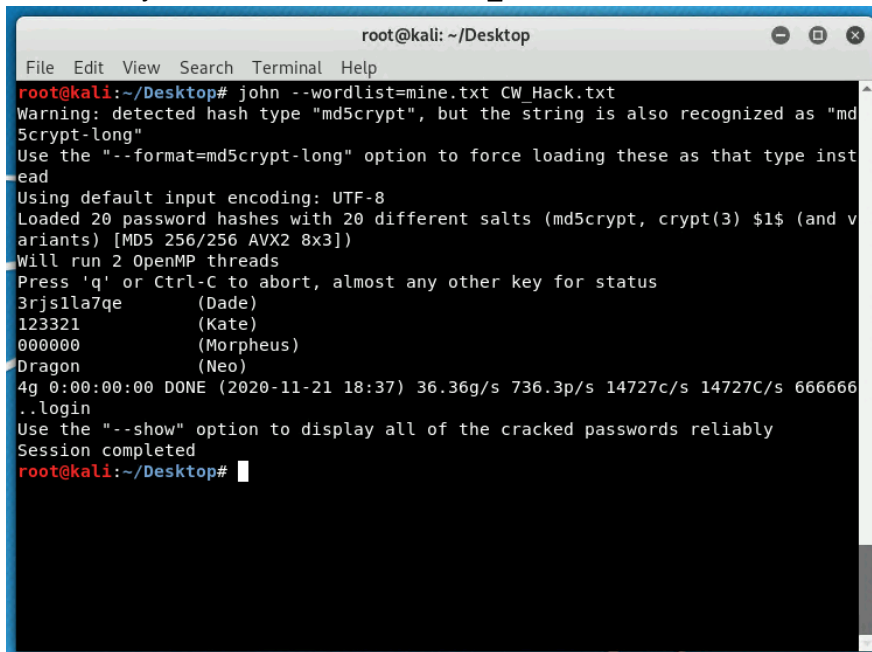
Dictionary #3

Name of the file: mine.txt

File source: From Wikipedia ("List of most common passwords":

https://en.wikipedia.org/wiki/List_of_the_most_common_passwords)

Command: john --wordlist=mine.txt CW_Hack.txt



```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# john --wordlist=mine.txt CW_Hack.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 20 password hashes with 20 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
3rjs1la7qe      (Dade)
123321          (Kate)
000000          (Morpheus)
Dragon          (Neo)
4g 0:00:00:00 DONE (2020-11-21 18:37) 36.36g/s 736.3p/s 14727c/s 14727C/s 666666
..login
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/Desktop#
```

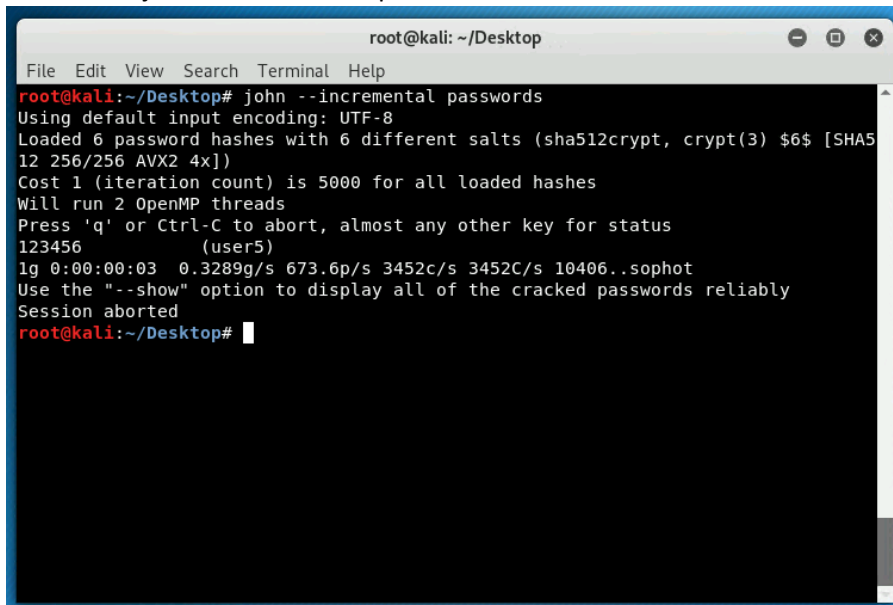
Cracked passwords

- hash #1 - Dade:\$1\$5JwpeptH\$HOsWr3z5s2DRkB9JtPZca0
- password #1 – 3rjs1la7qe
- hash #2 - Morpheus:\$1\$dyNX5WXS\$oR6LHqr1t6vJc0.F/rE.R1
- password #2 – 000000
- hash #3 - Neo:\$1\$y8HlgJLN\$BtRUhf5bxWYOH74seTZi2/
- password #3 - Dragon

Task 2.2 - Password cracking of Linux accounts

Brute force

Command: john --incremental passwords



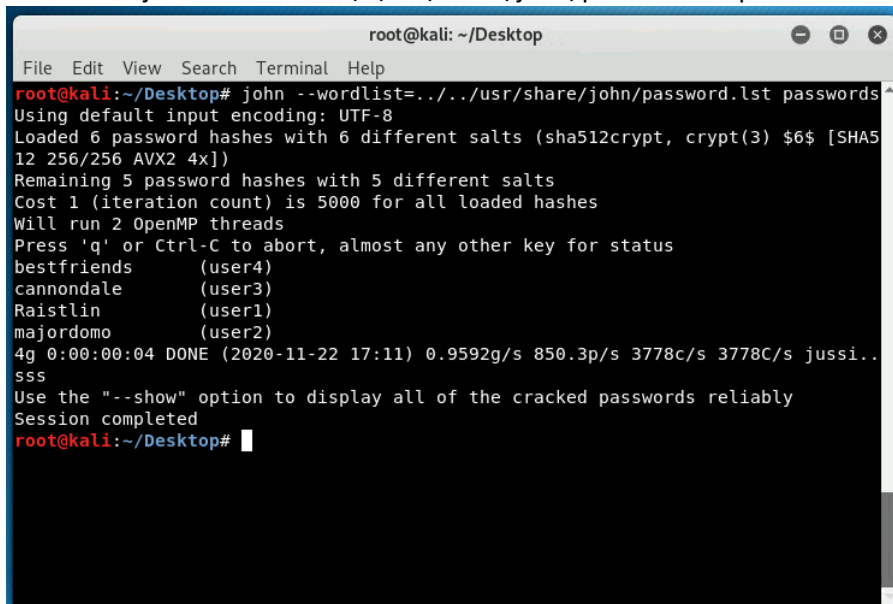
```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# john --incremental passwords
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) $6$ [SHA5
12 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456 (user5)
1g 0:00:00:03 0.3289g/s 673.6p/s 3452c/s 3452C/s 10406..sophot
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
root@kali:~/Desktop#
```

Cracked passwords

- username #1 – user5
- password #1 – 123456

Dictionary

Command: john --wordlist=../../usr/share/john/password.lst passwords



```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# john --wordlist=../../usr/share/john/password.lst passwords
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) $6$ [SHA5
12 256/256 AVX2 4x])
Remaining 5 password hashes with 5 different salts
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
bestfriends (user4)
cannondale (user3)
Raistlin (user1)
majordomo (user2)
4g 0:00:00:04 DONE (2020-11-22 17:11) 0.9592g/s 850.3p/s 3778c/s 3778C/s jussi..
sss
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/Desktop#
```

Cracked passwords

- username #1 – user4
- password #1 – bestfriends
- username #2 – user3
- password #2 – cannondale
- username #3 – user1
- password #3 – Raistlin

- username #4 – user2
- password #4 – majordomo

Result Comparison

The incremental mode supports 10 different entropy sources from which different combinations arise. (ASCII, LM_ASCII, Alnum, Alpha, LowerNum, UpperNum, LowerSpace, Lower, Upper, Digits). In our case, we haven't selected any source. As a result, the incremental mode will try to make combinations by using all the 10 sources. Thus, it will take a lot of time to find a suitable combination that matches the password we are searching for. On the other hand, when we use the dictionary the time needed is reduced significantly as the dictionary contains fewer combinations and as a result, the comparisons will be less. Next, we notice that in the brute force attack the password found is a simple password with only 6 different digits. Therefore, this password was found very fast as only the "Digits" entropy source needed. However, the dictionary attack gave us more complicated passwords. Brute force attack would take too long to find them because they would need many more combinations. Finally, the incremental mode will find the passwords in the end (because it will try all the possible combinations). However, the dictionary may not because the passwords may not be included in the dictionary we use.

Task 2.3 - Password analysis

Password #1

Password: nirvana1

Weaknesses

- weakness #1 – nirvana is a simple English word but is also a popular music band name. There are several dictionaries with music band names. Thus, this password could be included in such a dictionary which consists of band names and simple number combinations.
- weakness #2 – the password consists only of a word and one number. This is a very common password pattern most users prefer to use. Attackers know this kind of pattern so they will be able to recognize it and exploit the password.
- weakness #3 – the password length is very short. A common secure guideline is that passwords must have at least 10 characters. This password has only 8. This makes an attack easier because the fewer characters a password contains the fewer combinations that need to be done in order to be cracked.
- weakness #4 – this password does not have character variety. The password contains only numbers and letters, but it does not contain nor special characters nor capital letters. Thus, the complexity of the password is very weak.

Password #2

Password: password00

Weaknesses

- weakness #1 - the password consists only of a word and one number. This is a very common password pattern most users prefer to use. Attackers know this kind of pattern so they will be able to recognize it and exploit the password.
- weakness #2 - this password does not have character variety. The password contains only numbers and letters, but it does not contain nor special characters nor capital letters. Thus, the complexity of the password is very weak.

- weakness #3 – the word password is a very common word used by users in passwords. This word could be included in several dictionaries. Thus, there are a few possible combinations of this word with numbers that can finally exploit the password.
- weakness #4 - this password uses a repeated pattern (00). As a result, the password could be more predictable by an attacker.

Password #3

Password: lacrosse

Weaknesses

- weakness #1 - lacrosse is a simple possible English word. There are several dictionaries with simple English words. Thus, this password could be included in such a dictionary which consists of simple English words.
- weakness #2 - the password length is very short. A common secure guideline is that passwords must have at least 10 characters. This password has only 8. This makes an attack easier because the fewer characters a password contains the fewer combinations that need to be done in order to be cracked.
- weakness #3 - this password does not have character variety. The password contains only letters, but it does not contain nor special characters nor numbers nor capital letters. Thus, the complexity of the password is very weak.
- weakness #4 - this password is a very common password. To be precise it is one of the most 625 most common passwords users prefer to choose in order to secure their personal accounts.

Password #4

Password: unionjack

Weaknesses

- weakness #1 - unionjack is a simple possible English word. There are several dictionaries with simple English words. Thus, this password could be included in such a dictionary which consists of simple English words.
- weakness #2 - the password length is very short. A common secure guideline is that passwords must have at least 10 characters. This password has only 9. This makes an attack easier because the fewer characters a password contains the fewer combinations that need to be done in order to be cracked.
- weakness #3 - this password does not have character variety. The password contains only letters, but it does not contain nor special characters nor numbers nor capital letters. Thus, the complexity of the password is very weak.
- weakness #4 - the password consists only of a word. This is a very common password pattern most users prefer to use. Attackers know this kind of pattern so they will be able to recognize it and exploit the password.

Password #5

Password: meow-meow

Weaknesses

- weakness #1 - the password length is very short. A common secure guideline is that passwords must have at least 10 characters. This password has only 9. This makes an attack easier because the fewer characters a password contains the fewer combinations that need to be done in order to be cracked.
- weakness #2 - meow is a simple possible word. There are several dictionaries with simple words. Thus, this password could be included in such a dictionary which consists of simple words.
- weakness #3 – this password uses a repeated pattern (meow meow). As a result, the password could be more predictable by an attacker.
- weakness #4 - this password does not have character variety. The password contains only letters and a special character, but it does not contain nor numbers nor capital letters. Thus, the complexity of the password is very weak.

Password #6

Password: arsenal2004

Weaknesses

- weakness #1 - arsenal is a simple English word but is also a popular football team name. There are several dictionaries with football team names. Thus, this password could be included in such a dictionary which consists of football team names and simple numbers.
- weakness #2 - the password consists only of a word and three numbers. This is a very common password pattern most users prefer to use. Attackers know this kind of patterns so they will be able to recognise it and exploit the password.
- weakness #3 - this password does not have character variety. The password contains only numbers and letters, but it does not contain nor special characters nor capital letters. Thus, the complexity of the password is very weak.
- weakness #4 – the attacker can collect personal information about the victim (dates, favourite teams, etc.) and generate a dictionary with passwords related to his interests. Thus, if the favourite victim's team is arsenal and his birthday is in 2004 this combination may exist in the dictionary as a password.

Password #7

Password: 123carebear

Weaknesses

- weakness #1 - the password consists only of a word and three numbers. This is a very common password pattern most users prefer to use. Attackers know this kind of pattern so they will be able to recognize it and exploit the password.
- weakness #2 - this password does not have character variety. The password contains only numbers and letters, but it does not contain nor special characters nor capital letters. Thus, the complexity of the password is very weak.
- weakness #3 – this password includes three consecutive numbers (123). This is a common pattern and in combination with a simple word (carebear) this password is very vulnerable to dictionary attacks.

- weakness #4 – this password exists in one of the most popular dictionaries called “myspace”. This dictionary contains many combinations of passwords that consist of numbers and simple words.

Password #8

Password: 123456benji

Weaknesses

- weakness #1 - the password consists only of a word and five consecutive numbers. This is a very common password pattern most users prefer to use. Attackers know this kind of pattern so they will be able to recognize it and exploit the password.
- weakness #2 - this password does not have character variety. The password contains only numbers and letters, but it does not contain nor special characters nor capital letters. Thus, the complexity of the password is very weak.
- weakness #3 this password includes three consecutive numbers (123456). This is a common pattern and in combination with a simple word (benji) this password is very vulnerable to dictionary attacks.
- weakness #4 - this password exists in one of the most popular dictionaries called “myspace”. This dictionary contains many combinations of passwords that consist of numbers and simple words.

Password #9

Password: 1234567898101112

Weaknesses

- weakness #1 – the password consists only of numbers. This is a very common password pattern most users prefer to use. Attackers know this kind of pattern so they will be able to recognize it and exploit the password.
- weakness #2 - the digits included in this password may be mean something to the victim. Therefore, if the attacker knows some personal information about the victim, can generate a dictionary with possible passwords that consist of this information and exploit the password.
- weakness #3 - this password uses a consecutive (123456789...) pattern. As a result, the password could be more predictable by an attacker.
- weakness #4 - this password does not have character variety. The password contains only numbers, but it does not contain nor special characters nor letters nor capital letters. Thus, the complexity of the password is very weak.

Password #10

Password: 101hotspurs

Weaknesses

- weakness #1 - hotspurs is a nickname for the Tottenham football club. There are several dictionaries football club nicknames. Thus, this password could be included in such a dictionary which consists of football club nicknames.
- weakness #2 - this password does not have character variety. The password contains only letters and numbers, but it does not contain nor special characters nor capital letters. Thus, the complexity of the password is very weak.

- weakness #3 - the password consists only of a word and two numbers. This is a very common password pattern most users prefer to use. Attackers know this kind of pattern so they will be able to recognize it and exploit the password.
- weakness #4 - this password could be a possible address (according to Google maps). If the attacker knows the victim's address could use it as a possible password in a dictionary.

Password #11

Password: 000001b

Weaknesses

- weakness #1 - the password length is very short. A common secure guideline is that passwords must have at least 10 characters. This password has only 7. This makes an attack easier because the fewer characters a password contains the fewer combinations that need to be done in order to be cracked.
- weakness #2 - the password consists only of a word and two numbers. This is a very common password pattern most users prefer to use. Attackers know this kind of patterns so they will be able to recognise it and exploit the password.
- weakness #3 - this password does not have character variety. The password contains only letters and numbers, but it does not contain nor special characters nor capital letters. Thus, the complexity of the password is very weak.
- weakness #4 - this password uses a repeated pattern (00000). As a result, the password could be more predictable by an attacker.

Password #12

Password: 01021994bday

Weaknesses

- weakness #1 - this password is a possible telephone number or a date. There are several dictionaries with telephone numbers and dates. Thus, this password could be included in such a dictionary which consists of telephone numbers, or in a handmade dictionary made by using the victim's information.
- weakness #2 - this password does not have character variety. The password contains only letters and numbers, but it does not contain nor special characters nor capital letters. Thus, the complexity of the password is very weak.
- weakness #3 - the password consists only of a word and few numbers. This is a very common password pattern most users prefer to use. Attackers know this kind of pattern so they will be able to recognize it and exploit the password.
- weakness #4 - this password uses a repeated pattern (010...). As a result, the password could be more predictable by an attacker.

Password #13

Password: canada

Weaknesses

- weakness #1 - this password is a very common password. To be precise it is one of the most 310 most common passwords users prefer to choose in order to secure their personal accounts.

- weakness #2 - the password length is very short. A common secure guideline is that passwords must have at least 10 characters. This password has only 6. This makes an attack easier because the fewer characters a password contains the fewer combinations that need to be done in order to be cracked.
- weakness #3 - this password is a possible word. This word could be included in a dictionary as a simple word or name. If this word represents a person's name it might be easy to guess. If it is just a dictionary word it could be cracked very quickly.
- weakness #4 - this password does not have character variety. The password contains only letters, but it does not contain nor special characters nor numbers nor capital letters. Thus, the complexity of the password is very weak.

Password #14

Password: larahornby

Weaknesses

- weakness #1 - this password is a possible word. This word could be included in a dictionary as a simple word or name. If this word represents a person's name it might be easy to guess. If it is just a dictionary word it could be cracked very quickly.
- weakness #2 - this password does not have character variety. The password contains only letters, but it does not contain nor special characters nor numbers nor capital letters. Thus, the complexity of the password is very weak.
- weakness #3 - the password consists only of a word. This is a very common password pattern most users prefer to use. Attackers know this kind of pattern so they will be able to recognize it and exploit the password.
- weakness #4 - this password may represent a first name and the last name. If the real name of the victim is Lara Hornby, then the attacker could make different combinations with these two names. One of the easiest ones is "larahornby". Therefore, the password can be exploited because it consists of the real victim's name.

Password #15

Password: 123321

Weaknesses

- weakness #1 - the password length is very short. A common secure guideline is that passwords must have at least 10 characters. This password has only 6. This makes an attack easier because the fewer characters a password contains the fewer combinations that need to be done in order to be cracked.
- weakness #2 - this password does not have character variety. The password contains only numbers, but it does not contain nor special characters nor letters nor capital letters. Thus, the complexity of the password is very weak.
- weakness #3 - this password is consisting of three numbers (123) and then the same numbers reverted (321). This is a very common logic sequence, and this pattern is well known to hackers. Thus, the password is vulnerable if the attacker understands the sequence pattern.
- weakness #4 - this password is a very common password. To be precise it is one of the most 445 most common passwords users prefer to choose in order to secure their personal accounts.

Password #16

Password: mitsuko

Weaknesses

- weakness #1 - this password is a possible word. This word could be included in a dictionary as a simple word or name. If this word represents a person's name it might be easy to guess. If it is just a dictionary word it could be cracked very quickly.
- weakness #2 - the password length is very short. A common secure guideline is that passwords must have at least 10 characters. This password has only 7. This makes an attack easier because the fewer characters a password contains the fewer combinations that need to be done in order to be cracked.
- weakness #3 - this password does not have character variety. The password contains only letters, but it does not contain nor special characters nor numbers nor capital letters. Thus, the complexity of the password is very weak.
- weakness #4 - the password consists only of a word. This is a very common password pattern most users prefer to use. Attackers know this kind of pattern so they will be able to recognize it and exploit the password.

Password #17

Password: lamer

Weaknesses

- weakness #1 - this password is a very common password. To be precise it is one of the most 10 most common passwords users prefer to choose in order to secure their personal accounts.
- weakness #2 - the password length is very short. A common secure guideline is that passwords must have at least 10 characters. This password has only 5. This makes an attack easier because the fewer characters a password contains the fewer combinations that need to be done in order to be cracked.
- weakness #3 - this password is a possible word. This word could be included in a dictionary as a simple word or name. If this word represents a person's name it might be easy to guess. If it is just a dictionary word it could be cracked very quickly.
- weakness #4 - this password does not have character variety. The password contains only letters, but it does not contain nor special characters nor numbers nor capital letters. Thus, the complexity of the password is very weak.

Password #18

Password: 3rjs1la7qe

Weaknesses

- weakness #1 - this password does not have character variety. The password contains only numbers and letters, but it does not contain nor special characters nor capital letters. Thus, the complexity of the password is very weak.
- weakness #2 - the password consists only of letters and numbers. This is a very common password pattern most users prefer to use. Attackers know this kind of pattern so they will be able to recognize it and exploit the password.
- weakness #3 - this password could represent a possible word where some letters have been replaced by numbers. 3 is "e", 1 is "l" and 7 is "t". This technique is well known to hackers and the password can be exploited easily.

- weakness #4 – this password may be generated by a bot. Other similar passwords like this are “18atcskd2w” or “q0tsrbv488”. The attacker will understand that this password is generated by a bot and he will try to use dictionaries with bot passwords.

Password #19

Password: 000000

Weaknesses

- weakness #1 - this password does not have character variety. The password contains only numbers, but it does not contain nor special characters nor letters nor capital letters. Thus, the complexity of the password is very weak.
- weakness #2 - the password length is very short. A common secure guideline is that passwords must have at least 10 characters. This password has only 6. This makes an attack easier because the fewer characters a password contains the fewer combinations that need to be done in order to be cracked.
- weakness #3 - this password is a possible telephone number or a date. There are several dictionaries with telephone numbers and dates. Thus, this password could be included in such a dictionary which consists of telephone numbers, or in a handmade dictionary made by using the victim's information.
- weakness #4 - the password consists only of one number (0). This is a very common password pattern most users prefer to use. Attackers know this kind of pattern so they will be able to recognize it and exploit the password.

Password #20

Password: Dragon

Weaknesses

- weakness #1 - this password is a very common password. To be precise it is one of the most 10 most common passwords users prefer to choose in order to secure their personal accounts.
- weakness #2 - the password length is very short. A common secure guideline is that passwords must have at least 10 characters. This password has only 6. This makes an attack easier because the fewer characters a password contains the fewer combinations that need to be done in order to be cracked.
- weakness #3 - this password is a possible word. This word could be included in a dictionary as a simple word or name. If this word represents a person's name it might be easy to guess. If it is just a dictionary word it could be cracked very quickly.
- weakness #4 - this password does not have character variety. The password contains only letters, but it does not contain nor special characters nor numbers. Thus, the complexity of the password is very weak.

Password #21

Password: 123456

Weaknesses

- weakness #1 - this password is a possible telephone number or a date. There are several dictionaries with telephone numbers and dates. Thus, this password could be included in such a dictionary which consists of telephone numbers, or in a handmade dictionary made by using the victim's information.
- weakness #2 - this password is a very common password. To be precise it is one of the most 5 most common passwords users prefer to choose in order to secure their personal accounts.
- weakness #3 - the password length is very short. A common secure guideline is that passwords must have at least 10 characters. This password has only 6. This makes an attack easier because the fewer characters a password contains the fewer combinations that need to be done in order to be cracked.
- weakness #4 - this password does not have character variety. The password contains only numbers, but it does not contain nor special characters nor letters nor capital letters. Thus, the complexity of the password is very weak.

Password #22

Password: bestfriends

Weaknesses

- weakness #1 - this password is a possible word. This word could be included in a dictionary as a simple word or name. If this word represents a person's name it might be easy to guess. If it is just a dictionary word it could be cracked very quickly.
- weakness #2 - this password does not have character variety. The password contains only letters, but it does not contain nor special characters nor numbers nor capital letters. Thus, the complexity of the password is very weak.
- weakness #3 - the password consists only of a word. This is a very common password pattern most users prefer to use. Attackers know this kind of pattern so they will be able to recognize it and exploit the password.
- weakness #4 - this password exists in one of the most popular dictionaries called "passwords.lst". This dictionary contains many combinations of passwords that consist of numbers and simple words.

Password #23

Password: cannondale

Weaknesses

- weakness #1 - this password is a possible word. This word could be included in a dictionary as a simple word or name. If this word represents a person's name it might be easy to guess. If it is just a dictionary word it could be cracked very quickly.
- weakness #2 - this password does not have character variety. The password contains only letters, but it does not contain nor special characters nor numbers nor capital letters. Thus, the complexity of the password is very weak.
- weakness #3 - the password consists only of a word. This is a very common password pattern most users prefer to use. Attackers know this kind of pattern so they will be able to recognize it and exploit the password.

- weakness #4 – cannondale is a bicycle web app. The user may have used as a password the app's name. As a result, it very easy for a hacker to guess this password. Also, the hacker could use tools such as CeWL in order to generate a dictionary with words related to this web app.

Password #24

Password: Raistlin

Weaknesses

- weakness #1 - this password is a possible word. This word could be included in a dictionary as a simple word or name. I this his word represents a person's name it might be easy to guess. If it is just a dictionary word it could be cracked very quickly.
- weakness #2 - the password length is very short. A common secure guideline is that passwords must have at least 10 characters. This password has only 8. This makes an attack easier because the fewer characters a password contains the fewer combinations that need to be done in order to be cracked.
- weakness #3 - this password does not have character variety. The password contains only letters, but it does not contain nor special characters nor numbers. Thus, the complexity of the password is very weak.
- weakness #4 – this password is a very common password. To be precise it is one of the most 1615 most common passwords users prefer to choose in order to secure their personal accounts.

Password #25

Password: majordomo

Weaknesses

- weakness #1 – this password is a possible word. This word could be included in a dictionary as a simple word or name. I this his word represents a person's name it might be easy to guess. If it is just a dictionary word it could be cracked very quickly.
- weakness #2 - the password length is very short. A common secure guideline is that passwords must have at least 10 characters. This password has only 9. This makes an attack easier because the fewer characters a password contains the fewer combinations that need to be done in order to be cracked.
- weakness #3 - this password does not have character variety. The password contains only letters, but it does not contain nor special characters nor numbers nor capital letters. Thus, the complexity of the password is very weak.
- weakness #4 - the password consists only of a word. This is a very common password pattern most users prefer to use. Attackers know this kind of pattern so they will be able to recognize it and exploit the password.