Lab Report

CSE451, Computer and Networks Security

Name: Ahmed Khaled Saad Ali Mekheimer ID: 1809799

Lab No: (8) Experiment Title: Attacking Windows Servers, Part 3,

Cracking Windows Passwords with Cain and Abel

Date: 5 / 1 /2023

Questions & Discussion

1. Functionalities of Metasploit Software

Cain and Abel is a password recovery tool. Its scope is very broad, which means it uses several possible attacks to obtain system passwords, not just one. It is only available on Windows, not Linux or OSX. It is commonly used by attackers who want to gain unauthorized access to a system, but it can also be used by defenders to test their defenses or when attackers lock them out of their systems.

These are the features that we chose to talk about in the presentation. These are the features that Cain and Abel is typically used for:

- Finding and cracking stored passwords
- Cracking password hashes using bruteforce, dictionary, or rainbow table attacks
- Enumerating and sniffing the network
- Attacking via ARP Poisoning
- Dialup password cracker (Outdated)

1. Local Passwords:

LSA Secret:

- Stored in registry at HKEY_LOCAL_MACHINE/Security/Policy/Secrets
- This is used for managing a system's local security policy, auditing, authenticating, logging users on to the system, and storing private data.
- Default Password: passwords used to logon to Windows if auto-logon is enabled
- DPAPI: IE passwords are protected using DPAPI and login URL as entropy before saved in the registry

Wireless Password:

- Stored in registry for Windows XP; stored as local files(.xml) for Vista and above.
- The password is encrypted but Cain can decrypt the password and present in plain text format.

LM(Lan Manager hash) and NTLM:

- LM/NTLM are suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users.
- They are stored in c:\windows\system32\config\SAM. The file is encrypted and locked when Windows is running, but Cain can bypass the lock and decrypt the SAM file to get LM/NTLM hashes.
- LM/NTLM hashes are used for local logon.
- LTLM hash is introduced in 1993 with Windows NT 3.1 to replace LM hash.
- LM is based on DES but is broken due to its design flaws. First, LM hash only supports up to 14 characters. Second, passwords longer than 7 characters are divided and hashed separately. Third, the password is converted into all uppercase letters in the first process of LM hash. As a result, the key-space of LM hash is only 69^7; brute-force attack can crack the hash in few hours.
- NTLM is based on MD4 and does not have maximum length limitation. Therefore, NTLM is much secure than LM hashes. However, Windows does not utilize a technique called salting. As a result, NTLM hashes stored in Windows are vulnerable to rainbow table attacks.

2. Cracking with Cain

Brute Force:

- Bruteforce is a relatively simple attack which tries every single possible password combination based on password length as well as what the password may consist of.
- In Cain and Abel you are able to specify the minimum length of the password, the maximum length, and the character set that it may consist of (like alphanumeric, special symbols, etc)

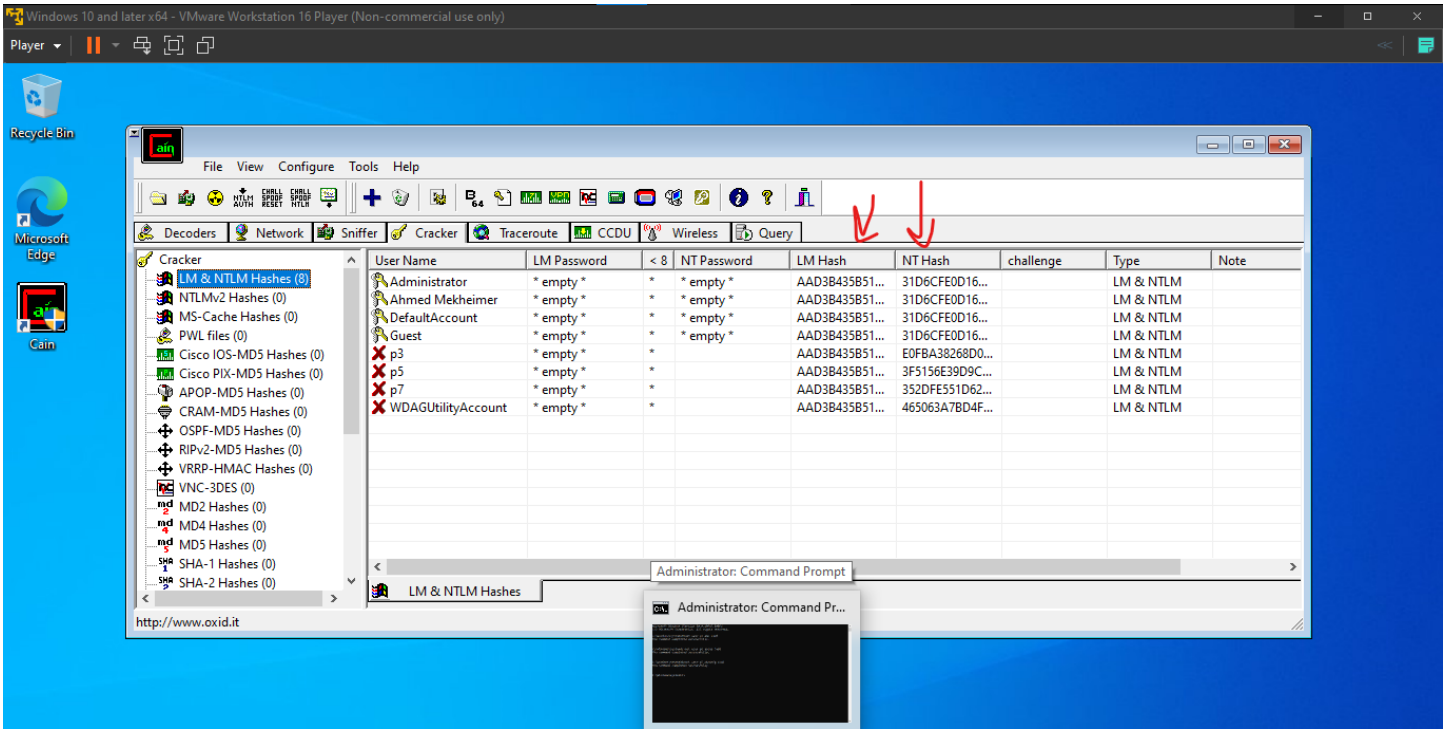
- The way bruteforcing works in Cain in Abel is as follows. First a hash that the user wants to crack is specified. Then once the attack is initiated, some permutation of the character set is hashed using the hash function through which the data we're trying to crack was hashed. Then the result of that is compared to our original hash. If it matches, that means we have found the plaintext password. Otherwise another permutation is tried.

Dictionary Attack:

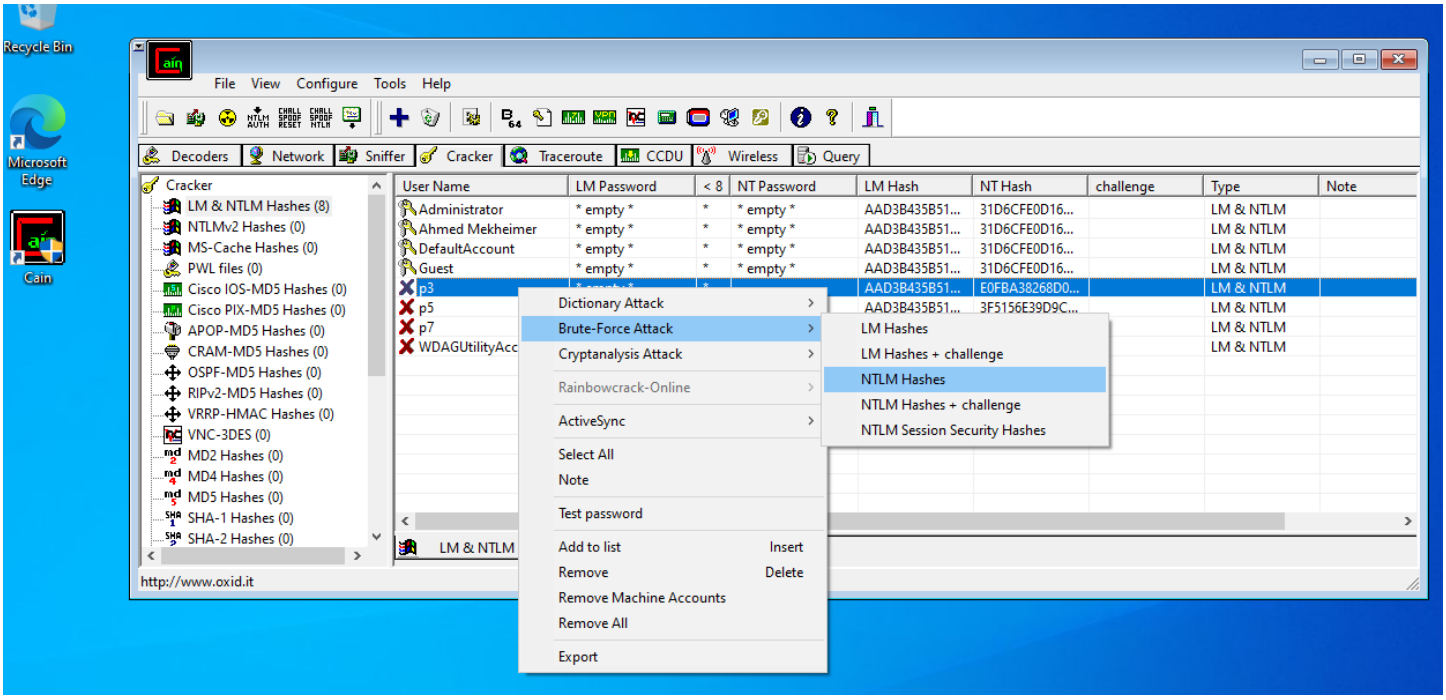
- Dictionary attacks are used when a bruteforce attack would take far too much time. It tries to gain access to a system by trying a list of pre-determined passwords, most of the time the most commonly used password. So it would try passwords like "password","letmein","p4ssw0rd", and so on. This list of passwords, typically stored as a text file, is called a dictionary.
- Cain and Abel does not come with a dictionary pre-installed, so you have to find one on your own. In our demonstrations we used a dictionary which contained the 10,000 most used passwords.
- The way it works is similar to bruteforcing. The password is hashed, and the hashes are compared.

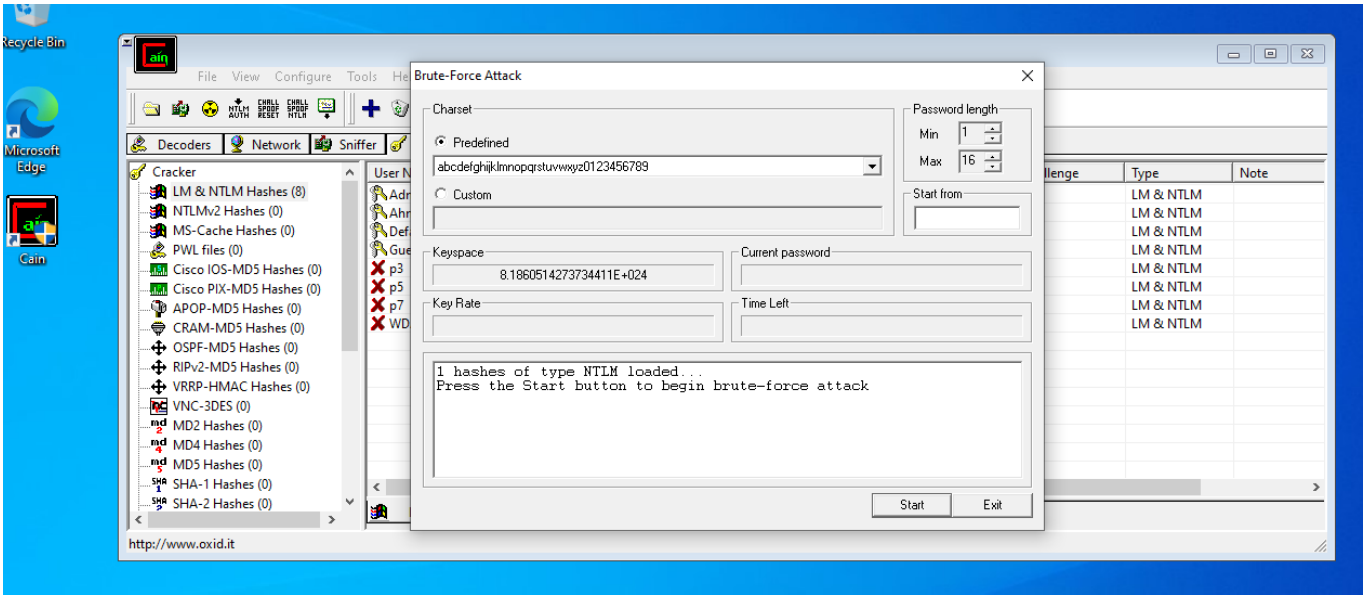
2. Screenshots

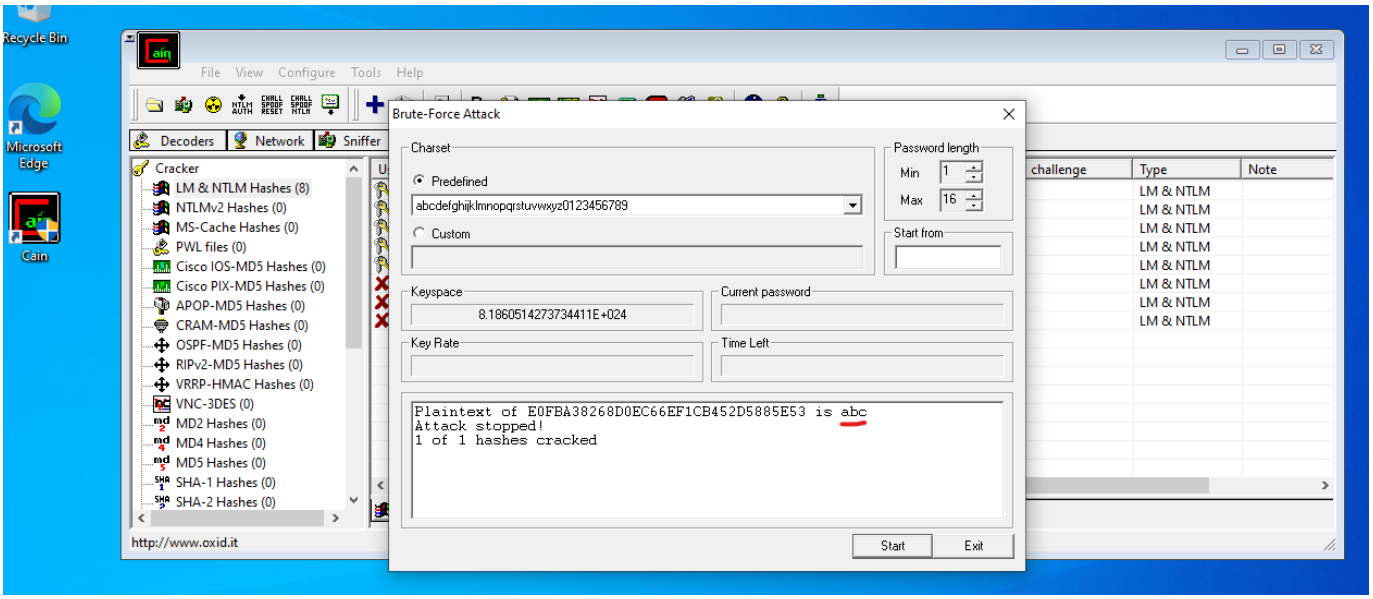
Displaying the Password Hashes

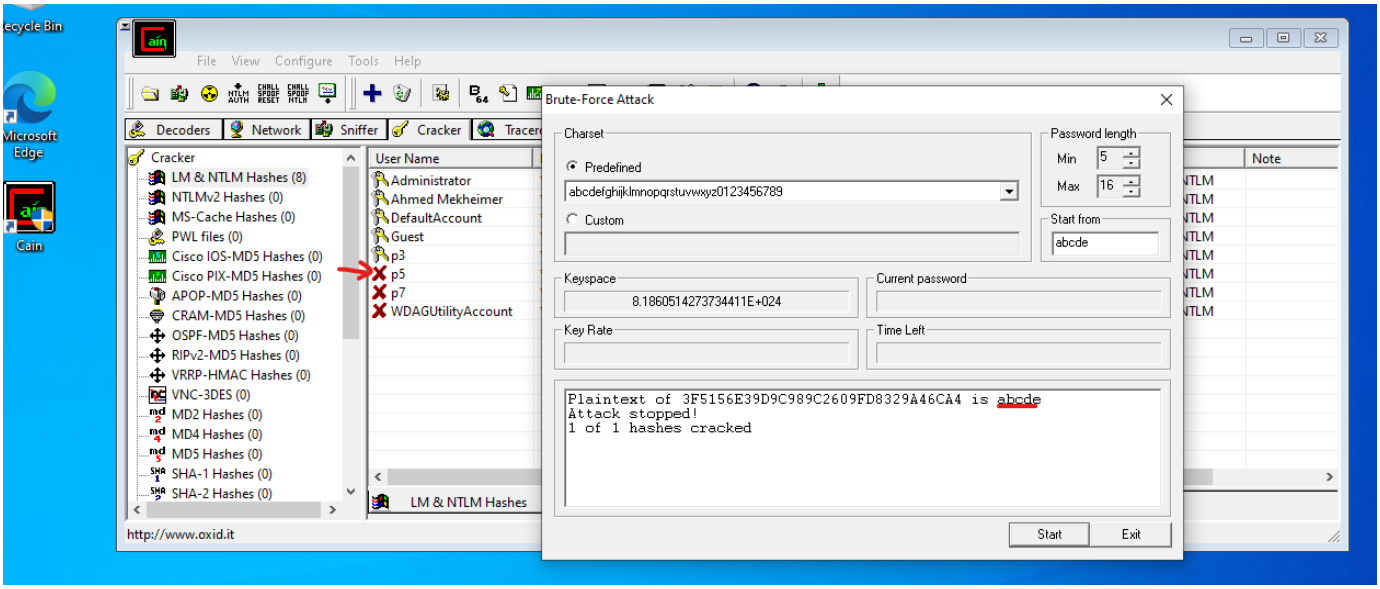


Cracking Passwords






Brute-Force Attack
Charset
Predefined
abcdefghijklmnopqrstuvwxyz0123456789
Custom
Password length
Min 1
Max 16
Start from
Keyspace
8.1860514273734411E+024
Current password
Key Rate
Time Left
Plaintext of E0FBA38268D0EC66EF1CB452D5885E53 is abc
Attack stopped!
1 of 1 hashes cracked
Start
Exit


Brute-Force Attack
Charset
Predefined
abcdefghijklmnopqrstuvwxyz0123456789
Custom
Password length
Min 5
Max 16
Start from
abcde
Keyspace
8.1860514273734411E+024
Current password
Key Rate
Time Left
Plaintext of 3F5156E39D9C989C2609FD8329A46CA4 is abcde
Attack stopped!
1 of 1 hashes cracked
Start
Exit

Two passwords found, abc and abcde, in the NT Password column of the Cain window