

Lab 8- Attacking Windows Servers, Part 3 Cracking Windows Passwords with Cain and Abel

Name: Hamza Abdellah Ahmed

ID: 18P7231

IP Configuration:-

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::1d8e:5076:19b8:733%12
    IPv4 Address. . . . . : 192.168.1.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Tunnel adapter isatap.{E926FE31-5AE0-421A-BC58-5D316170CFA7}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Local Area Connection* 3:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:0:2851:782c:1433:223d:3f57:fe8b
    Link-local IPv6 Address . . . . . : fe80::1433:223d:3f57:fe8b%8
    Default Gateway . . . . . : ::

C:\Users\Administrator>
```

Kali Configuration:-

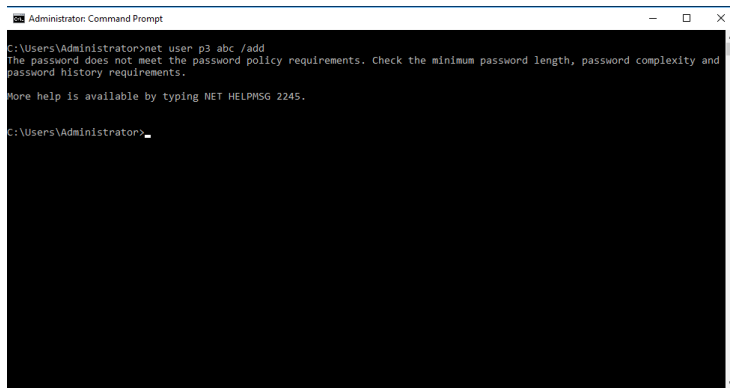
```
kali@kali: ~
File Actions Edit View Help

(kali@kali)~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.5 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::fc25:db25:aaff:975c prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:22:46:4f txqueuelen 1000 (Ethernet)
    RX packets 1585006 bytes 2269766702 (2.1 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 445843 bytes 58979557 (56.2 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 1717508 bytes 293720424 (280.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1717508 bytes 293720424 (280.1 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)~$
```

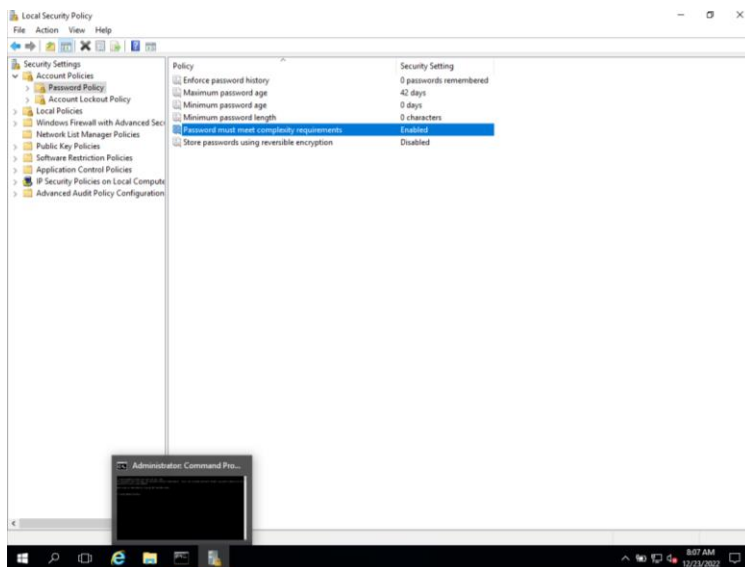
net user p3 abc /add

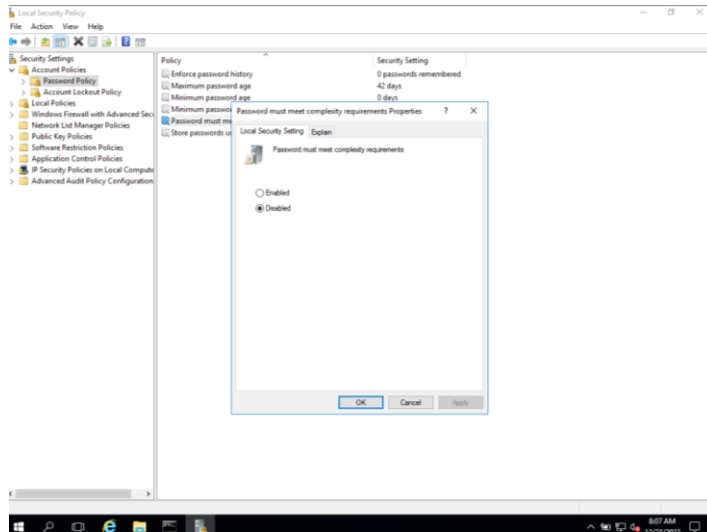


```
Administrator: Command Prompt
C:\Users\Administrator>net user p3 abc /add
The password does not meet the password policy requirements. Check the minimum password length, password complexity and password history requirements.
More help is available by typing NET HELPMSG 2245.

C:\Users\Administrator>
```

Displaying the Password Hashes





```
net user p3 abc /add
```

```
net user p5 abcde /add
```

```
net user p7 abcdefg /add
```

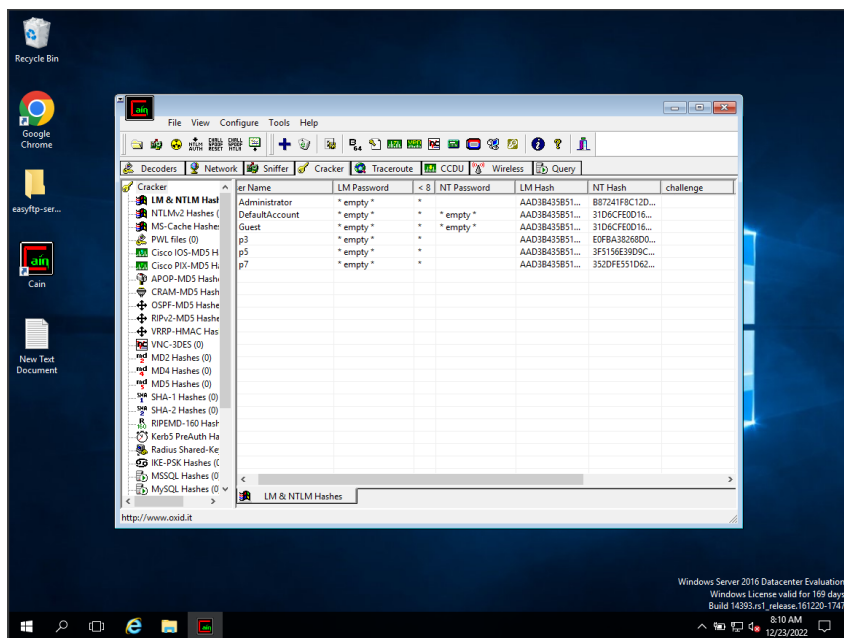
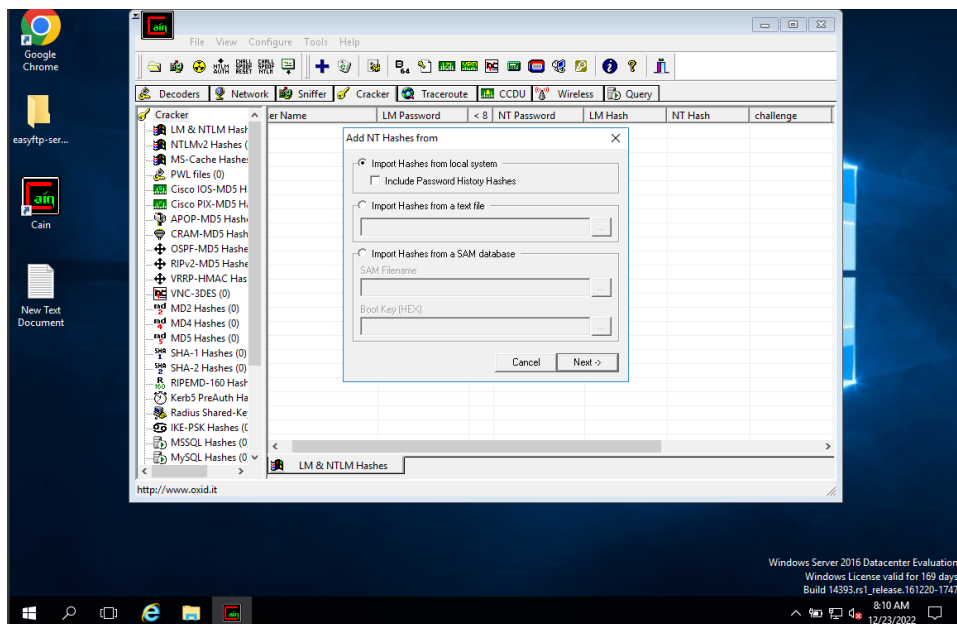
```
Administrator: Command Prompt

C:\Users\Administrator>net user p3 abc /add
The command completed successfully.

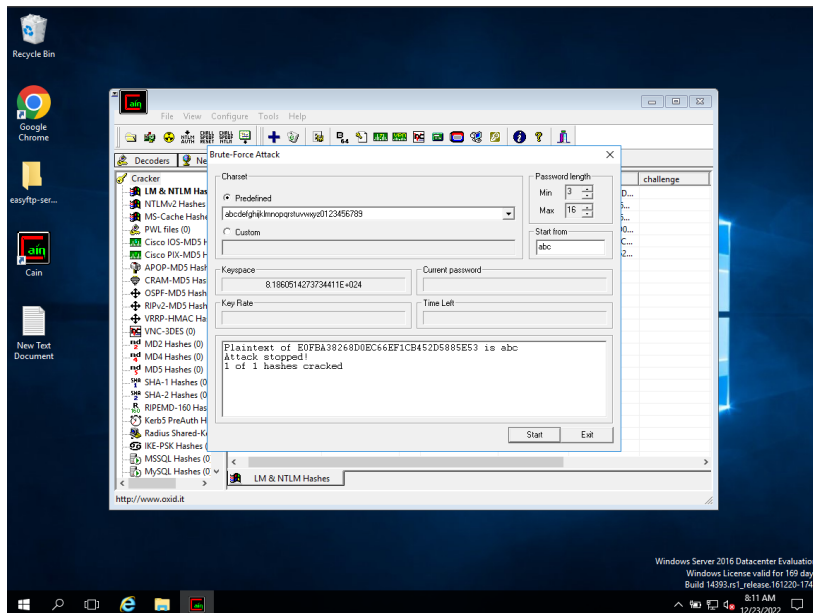
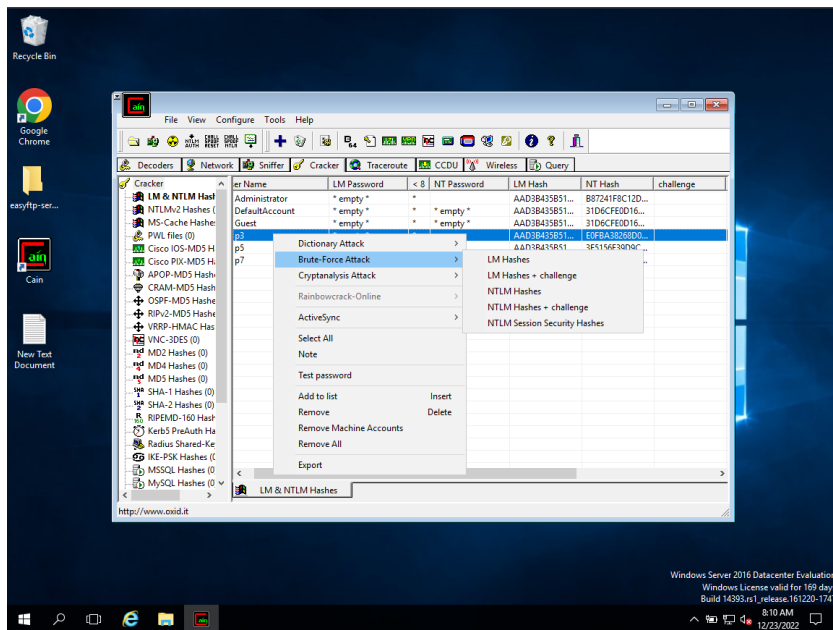
C:\Users\Administrator>net user p5 abcde /add
The command completed successfully.

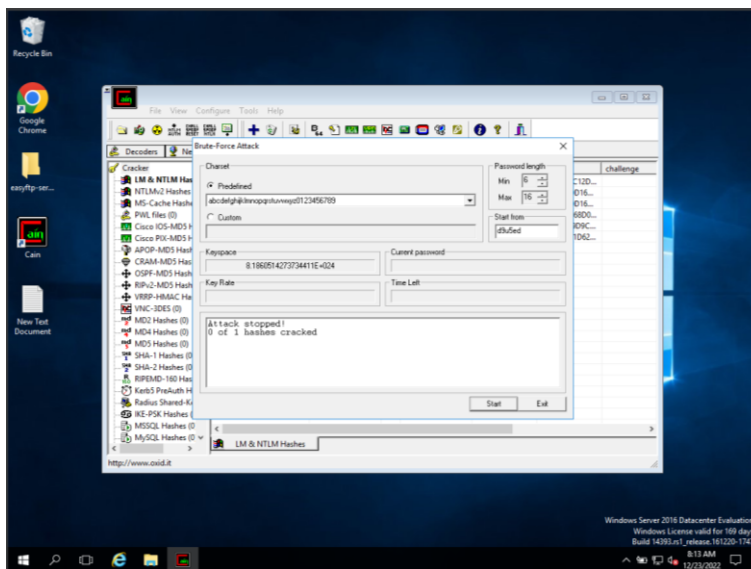
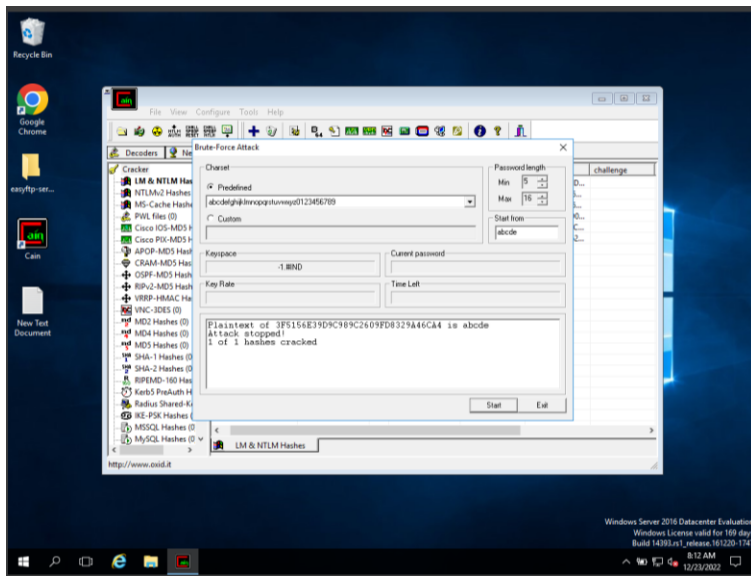
C:\Users\Administrator>net user p7 abcdefg /add
The command completed successfully.

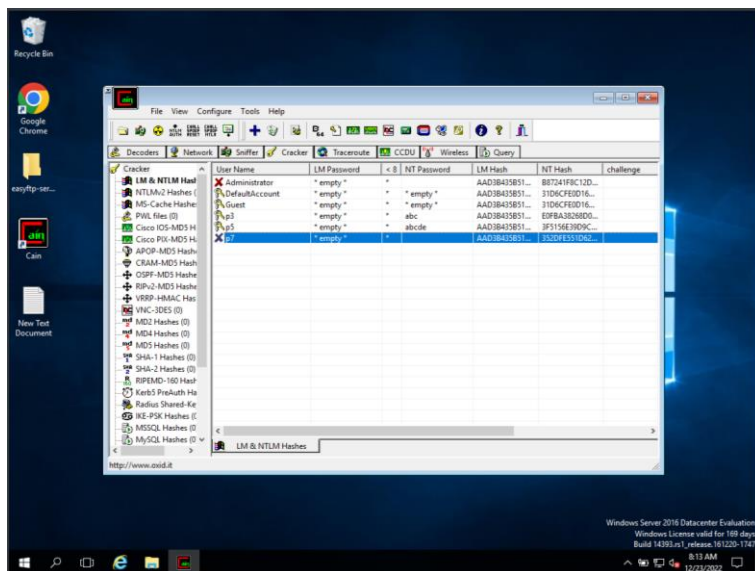
C:\Users\Administrator>
```



Cracking Passwords







Describe the functionality of the Cain & Abel Software

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kinds of passwords by sniffing the network, [cracking encrypted passwords](#) using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analyzing routing protocols.

The latest version is faster and contains a lot of new features like APR (ARP Poison Routing) which enables sniffing on switched LANs and Man-in-the-Middle attacks. The sniffer in this version can also analyze encrypted protocols such as SSH-1 and HTTPS and contains filters to capture credentials from a wide range of [authentication](#) mechanisms. The new version also ships routing protocols authentication monitors and routes extractors, dictionary and brute-force crackers for all common hashing algorithms and for several specific authentications, password/hash calculators, [cryptanalysis attacks](#), password decoders and some not so common utilities related to network and system security.