Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Presented by Powerpuff Girls
Sushmaa Lingaraj, Bernice Asamoah, Morayo Lawal, Sooji Lee

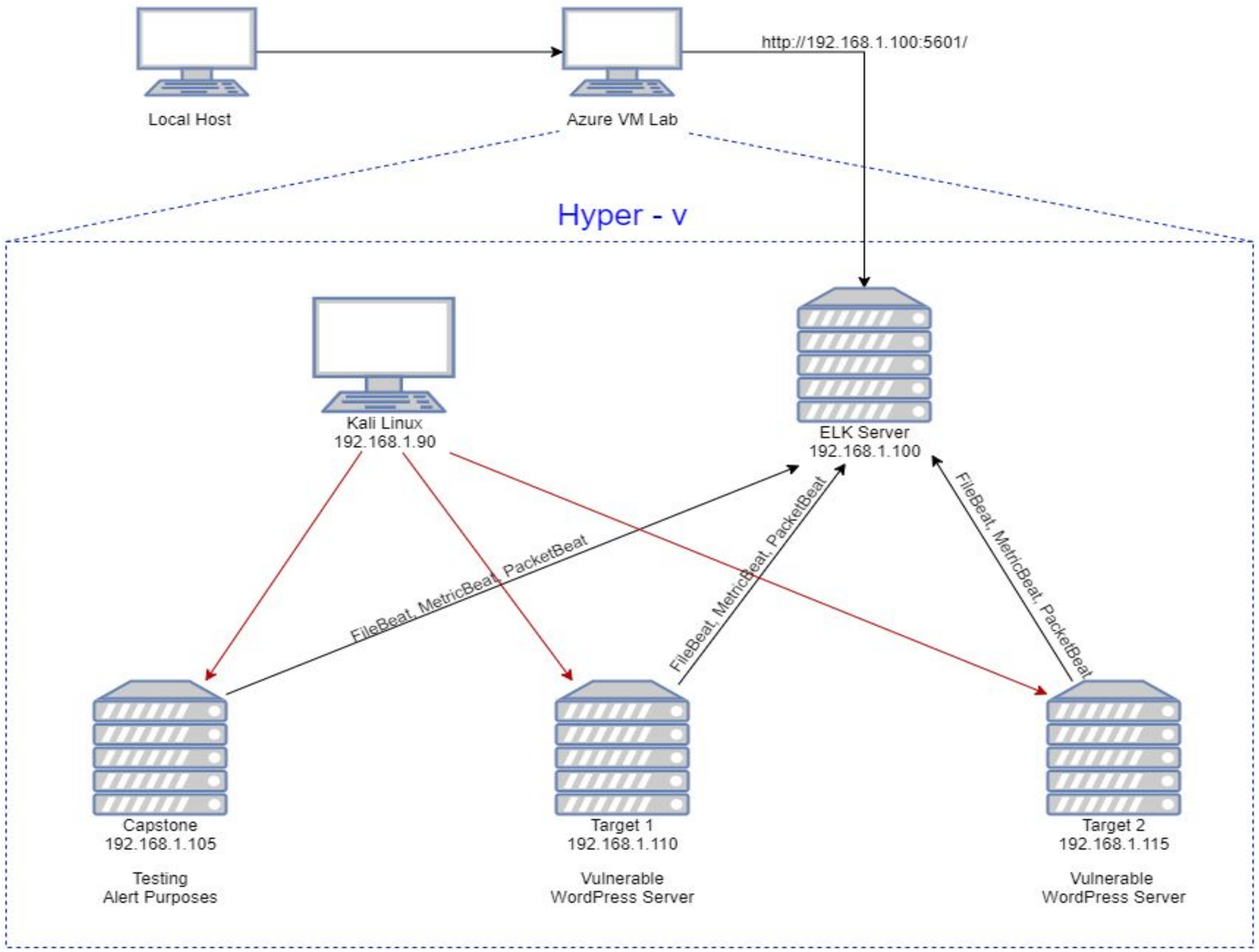
September 13, 2021

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

Network Topology



Network

Address Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines

IPv4: 192.168.1.90
OS: Linux 2.6.32
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.105
OS:Linux
Hostname: Capstone

IPv4: 192.168.1.110
OS: Linux
Hostname: Target 1

IPv4: 192.168.1.115
OS: Linux
Hostname: Target 2

Critical Vulnerabilities: Target 1 (From WPScan)

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

Vulnerability	Description	Impact
WordPress XMLRPC GHOST Vulnerability Scanner (CVE-2015-0235)	Used to determine if it is vulnerable to the GHOST using WordPress XMLRPC interface	If vulnerable, system will segfault (segmentation fault - where unauthorized is trying to get into memory system) and return a server error
WordPress XMLRPC DoS (CVE-2014-5266)	Vulnerable to XML based denial of service	Web Server can have an effect in availability (CIA Triad)
WordPress XML-RPC Username/Password Login Scanner (CVE-1999-0502)	Attempts to authenticate against Wordpress-site (via XMLRPC) using different combinations	Brute Force attack can be done to get the username & password of the web server for authentication
WordPress XML RPC Pingback API / Pingback Locator (CVE-2013-0235)	Allows attackers to send HTTP request to intranet servers for port-scanning attack.	One server can expose all the internal server composition

Critical Vulnerabilities: Target 1

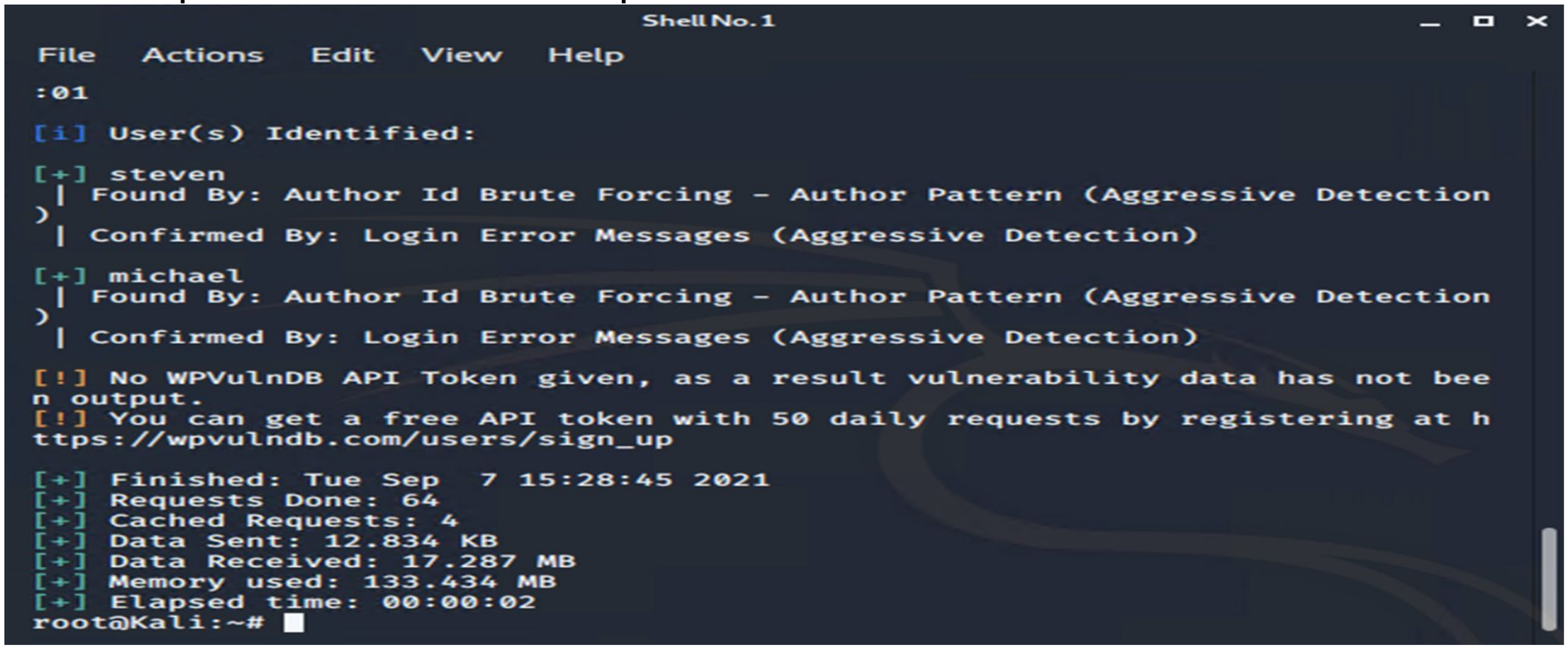
Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
Wordpress User Enumeration	WPScan detect the list of users with the specific options used (-u)	Unauthorized can get the username to target the specific account.
Open Port 22 SSH & Weak Password	Having Port 22 SSH open, anyone with the username and password can get into the system	Anyone can brute force attack the authentication for the system
Sensitive Data Exposure/ wp-config.php & SQL Database	SQL Database Configuration in Plaintext	Once the config file is seen, anyone can grab the Id & pw. Better protect it with encryption.
Python sudo privileges	User is given access to sudo privileges via Python	Attacker can escalate to root privileges easily gaining access to the system

Exploits Used

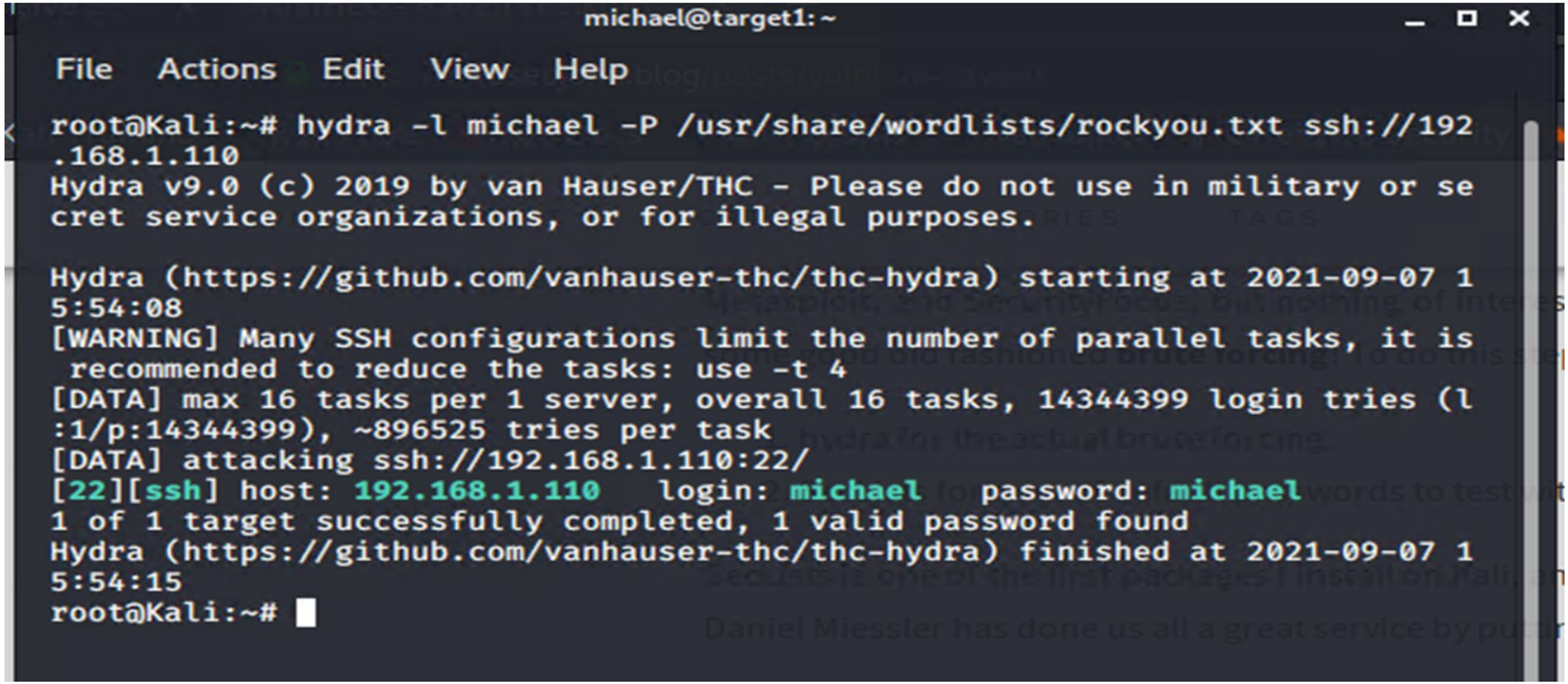
Exploitation: Wordpress User Enumeration

- WPScan was used to find the 2 users: Michael and Steven wpscan –-url http://192.168.1.110/wordpress -eu



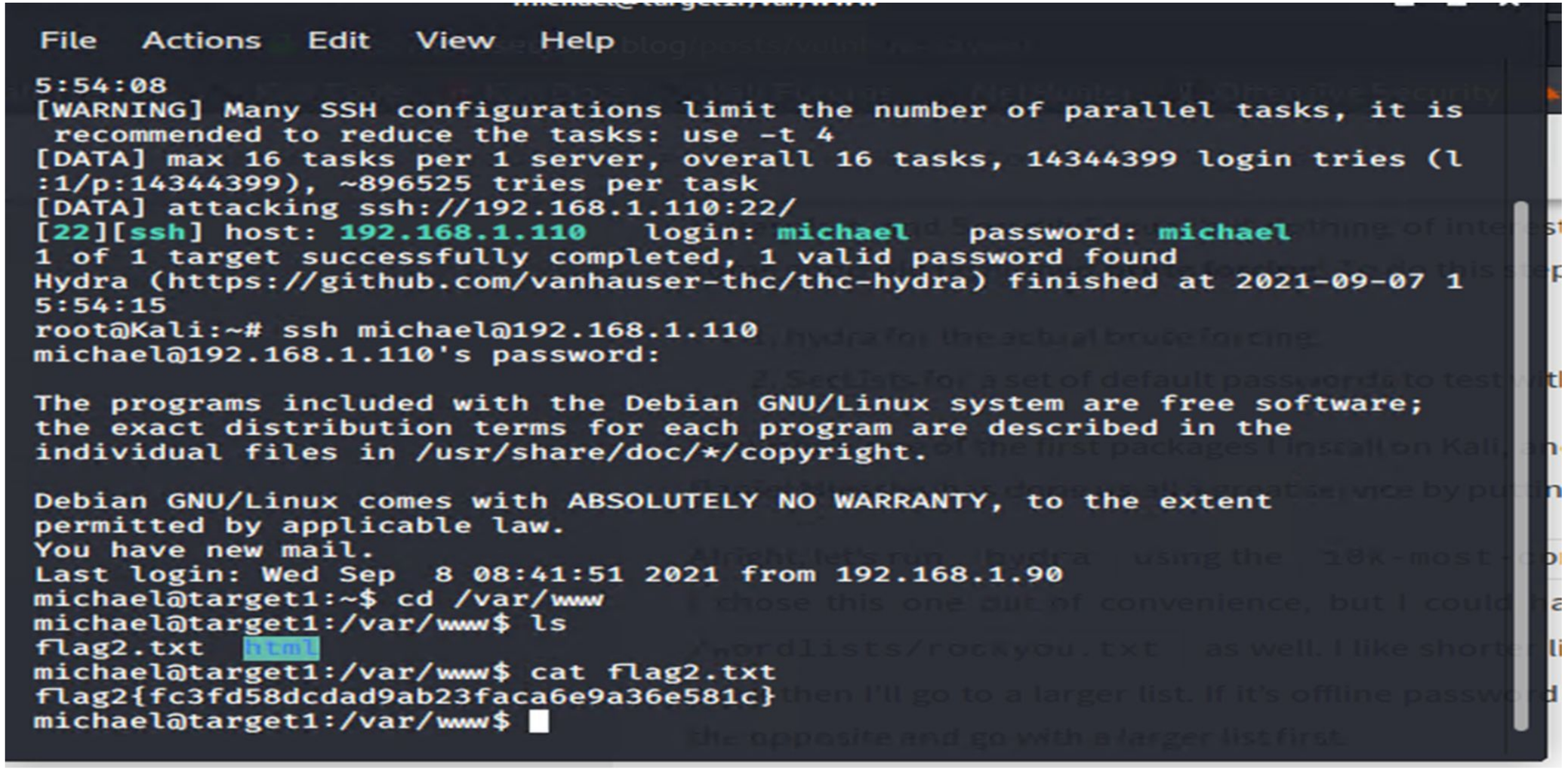
Exploitation: Open Port 22 SSH & Weak Password

- Hydra was used to get Michael's password



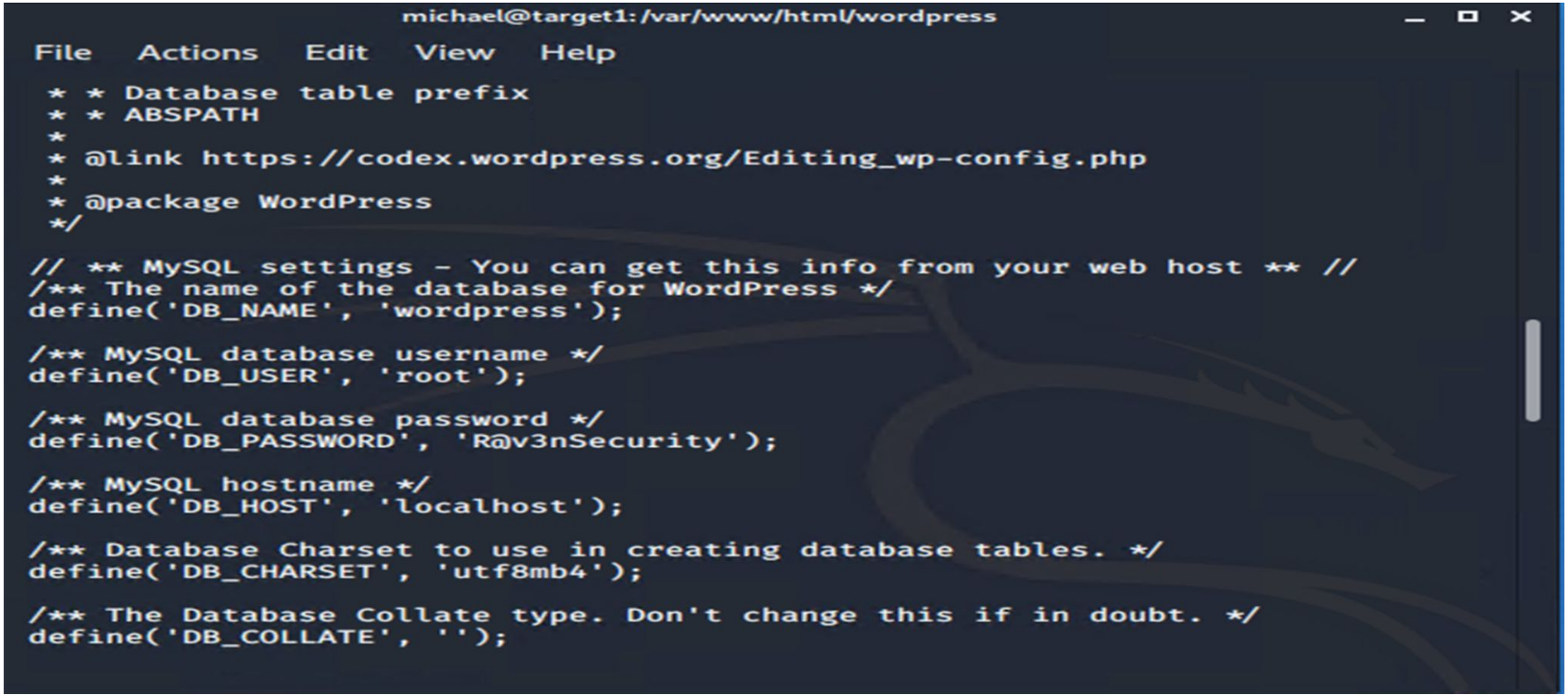
Exploitation: Open Port 22 SSH & Weak Password

- Use SSH to gain a user shell – Michael. Was able to access files through Michael's account.



Exploitation: Sensitive Data Exposure

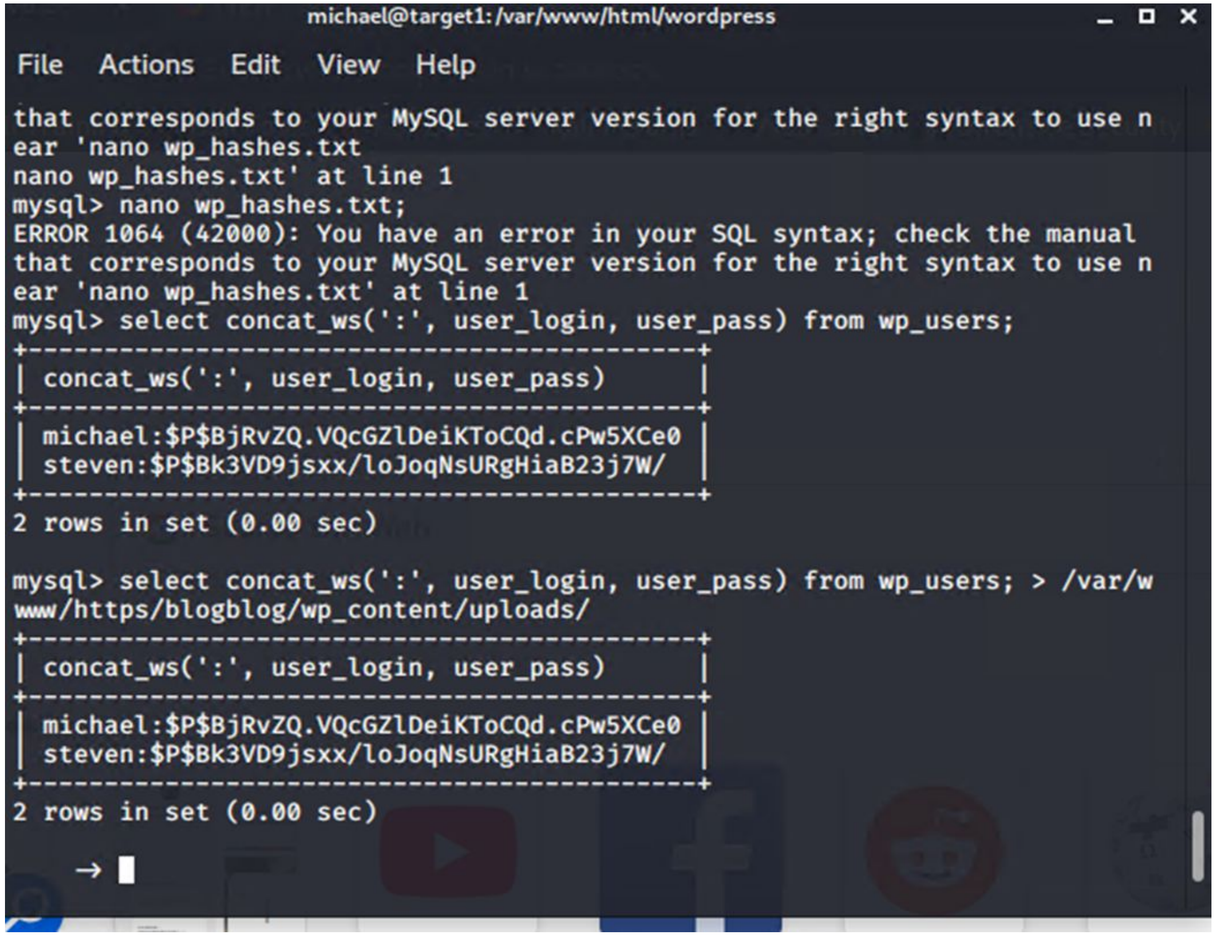
- Discovered the wordpress directory there is a wp-config.php file. Found the username is **root** and the password is **R@v3nSecurity**

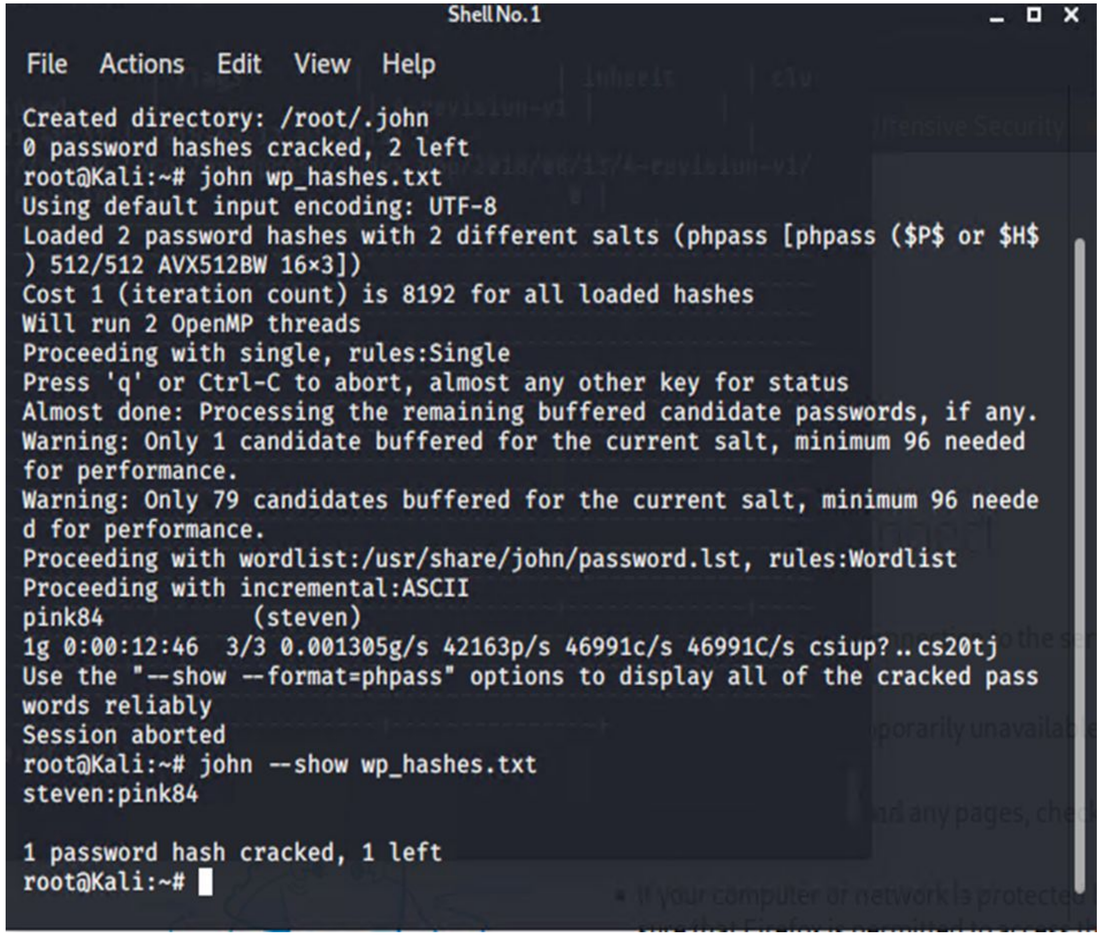


Exploitation: Sensitive Data Exposure

Password Hash With Insufficient Computational Effort

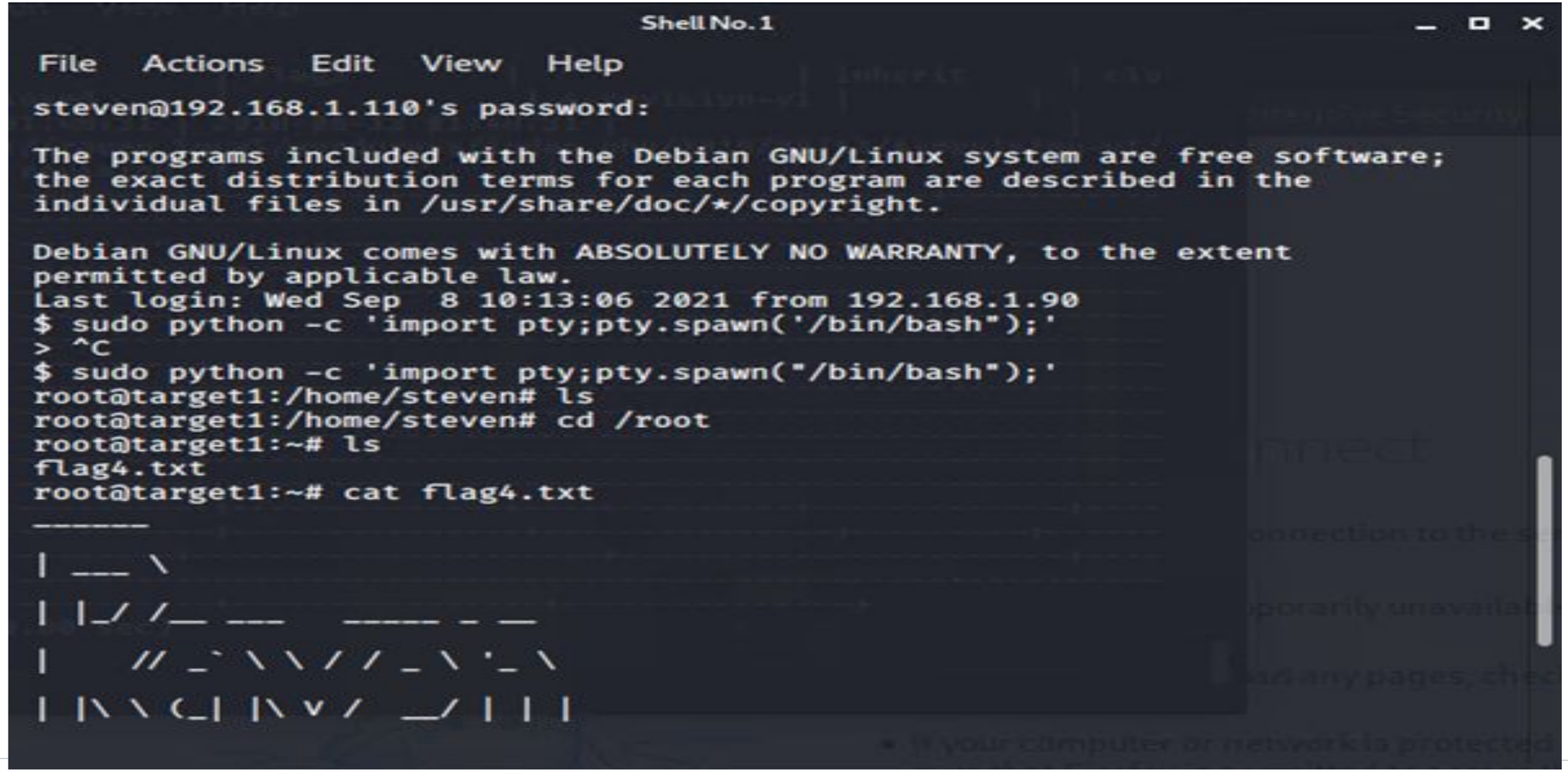
- From the wp_users, we can see both users Michael and Steven, and their corresponding hashes. John the ripper was used to crack the hashes





Exploitation: Python Sudo Privileges

- Once we got into Steven's password from John, we exploited Steven's account
- Exploited Steven's python sudo privileges through a spawn shell
- Achieved root access



Avoiding Detection

Stealth Exploitation of (Wordpress User Enumeration)

Monitoring Overview

- This alerts detection was used for this exploit:
  - **WHEN count () GROUPED OVER top 5 “http.response_status_code IS ABOVE 400 FOR THE LAST 5 minutes**
- **packetbeat-http.response_status_code** metrics was used
- **above 400 FOR THE LAST 5 MINUTES** threshold was fired at.

Mitigating Detection

- You can disable User Enumeration in Wordpress by using free plugin “WP Hardening”
  - Install and activate plugin > ‘Security Fixers’ tab > Stop user enumeration
- Underline factor is to educate the employees to use the stronger passwords for security purposes. (not using the same pw as id, like michael)
  - Company should also imply a policy for password change every 3-6 months.

Stealth Exploitation of [Open Ports 22 SSH]

Monitoring Overview

- SSH Login Alert would detect this exploit
- Monitor SSH Port for unauthorized access
- Triggers when user attempts to access system over Port 22

Mitigating Detection

- The best mitigation for this exploit would be closing the Port 22.
- However, there might be times when you would need Port 22 open.
  - If this is the case, we can create whitelisting of IPs so that only authorized can access the Port 22

Stealth Exploitation of (Sensitive Data Exposure)

Monitoring Overview

- Alert when SQL Database has gained access with unauthorized personnel.
- Triggers external/unauthorized IP connections that are made to the SQL database or any other sensitive files (like wp-config.php file)

Mitigating Detection

- Have all the sensitive data encrypted, not in plaintext
  - This will have the data not easily accessible
- Only whitelist the IPs that are being logged in for SQL database (ex. Administrators)

Stealth Exploitation of (Python Sudo Privileges)

Monitoring Overview

- Privilege Escalation Alert
- Monitor for unauthorized root access attempts, as well as “super-doer” activity
- Triggers when unauthorized sudo command usage or privileged directory access is attempted by unauthorized users.

Mitigating Detection

- Only authorize Sudo Privileges to the select few
  - (Ex. Administrators)
- For example, remove Python Sudo Privileges from Steven’s account.

References:

- Rapid7 (May, 2018) WordPress XMLRPC GHOST Vulnerability Scanner Retreived from https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
- Rapid7 (May, 2018) WordPress XMLRPC DoS Retreived from https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
- Rapid7 (May, 2018) WordPress XML-RPC Username/Password Login Scanner Retreived from https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
- National Vulnerability Database (Aug, 2013) CVE-2013-0235 Detail Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2013-0235
- cve.mitre.org (Sept, 2021) CVE-2016-10033 Retrieved from https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10033
- Vikas Kundu (Aug, 2021) How to Stop User Enumeration in WordPress? Retrieved from https://www.getastra.com/blog/cms/wordpress-security/stop-user-enumeration/


The End