# Red Team: Summary of Operations

## Table of Contents

- Exposed Services

- Critical Vulnerabilities

- Exploitation

### Exposed Services

Nmap scan results for each machine reveal the below services and OS details:

```bash

$ nmap ... # TODO: nmap -sV 192.168.1.110

```

This scan identifies the services below as potential points of entry:

- Target 1

- List of

- Exposed Services : ssh, http, rcpbind, netbios-ssn,

Fill out the list below. Include severity, and CVE numbers, if possible.\_

The following vulnerabilities were identified on each target:

- Target 1

- List of

- Critical

- Vulnerabilities:

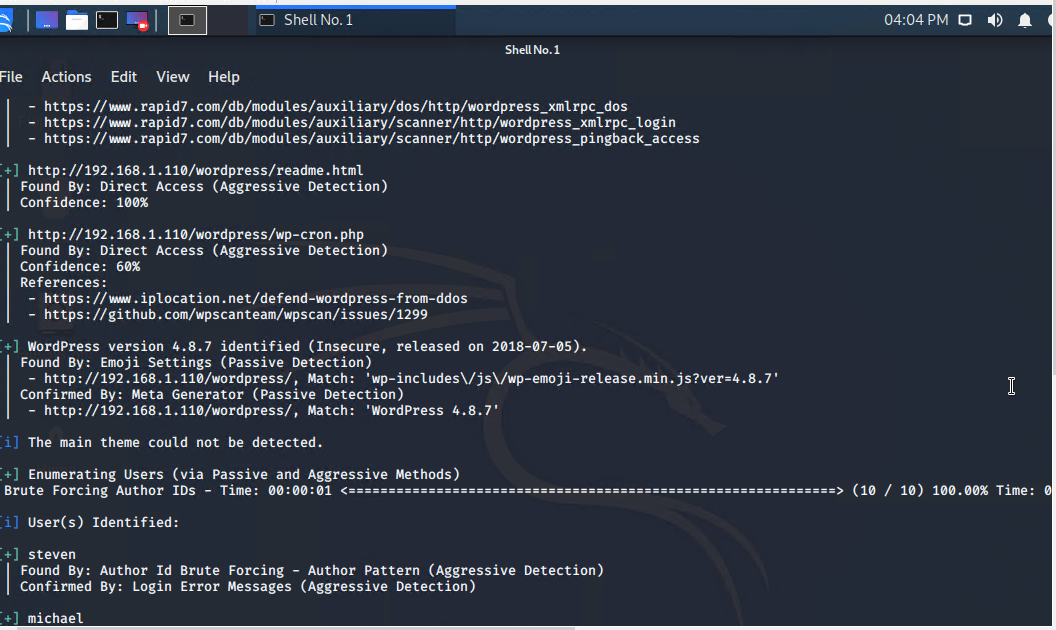
User Enumeration- CVE-2009-2335: Allowed for us to discover usernames. Severity of 5.0.

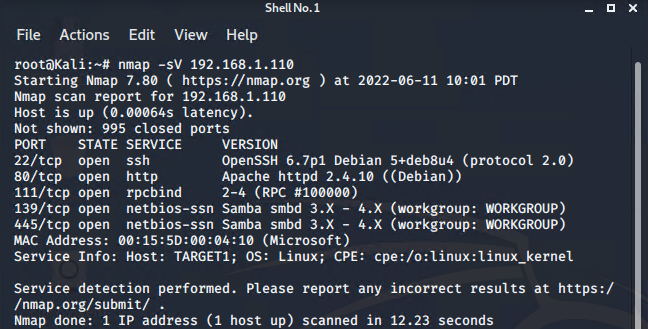
Weak Password Requirements- CWE-521- This allowed us to easily guess Michael's password. Severity of 8.1.

Wordpress Config File Exposed- CVE-2021-24692 – This allowed us to access the config file without any further authentication. Severity 6.5.

Privilege Escalation- CVE-2018-1000030- Using sudo -l showed us privilege that allowed us to run python command to escalate privileges. Severity 3.6.

Include vulnerability scan results to prove the identified vulnerabilities.\_





### Exploitation

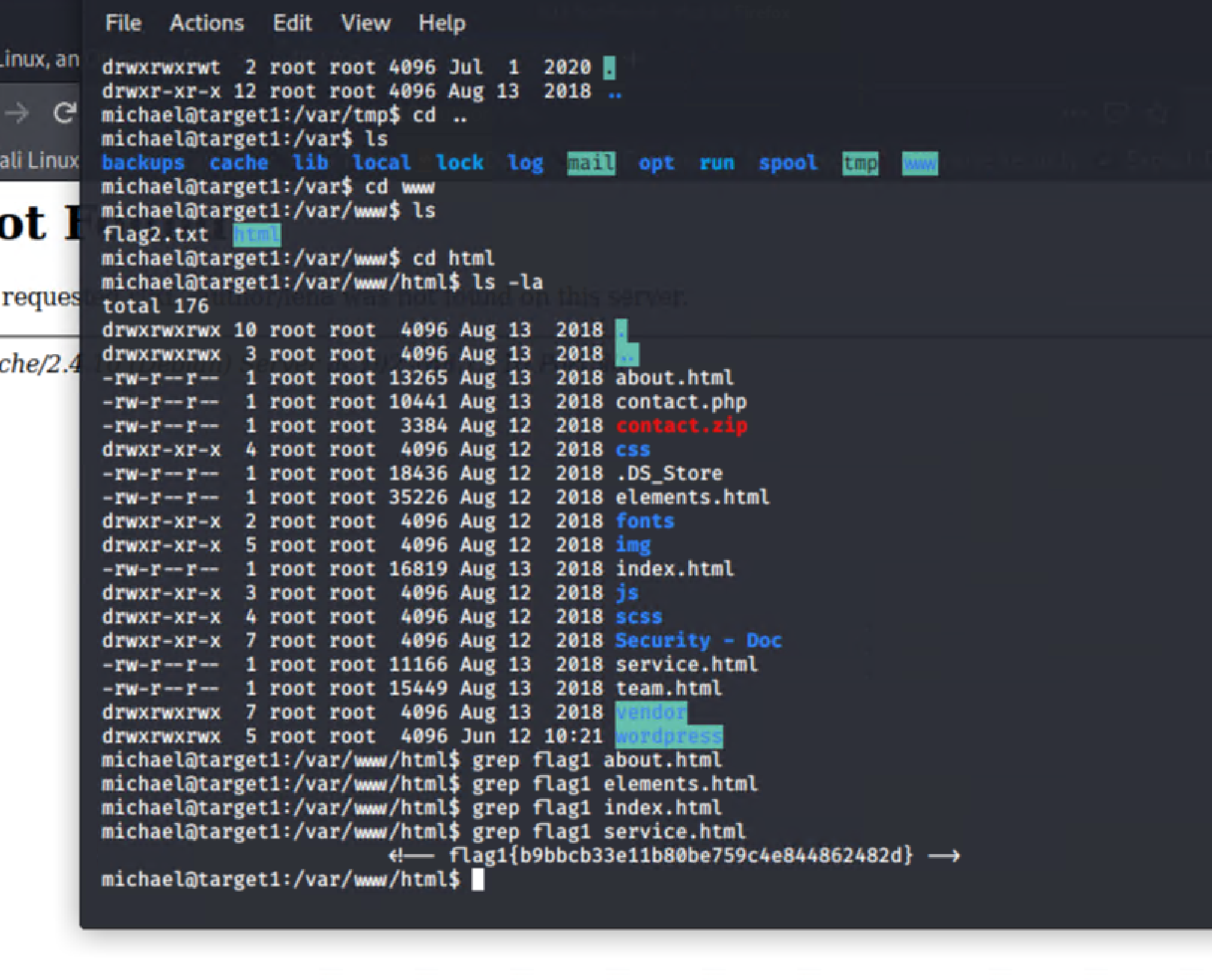
The Red Team was able to penetrate `Target 1` and retrieve the following confidential data:

- Target 1

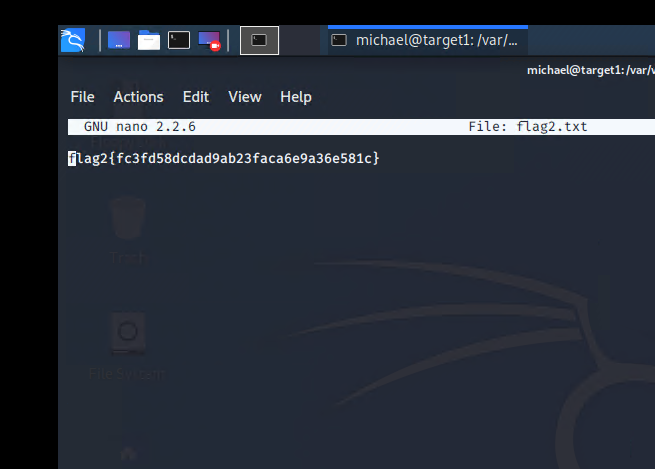
- `flag1.txt`:



- \*\*Exploit Used\*\*



- `flag2.txt`:



- \*\*Exploit Used\*\*

