# Red Team: Summary of Operations

## 

## Table of Contents

* Exposed Services
* Critical Vulnerabilities
* Exploitation

### Exposed Services

TODO: Fill out the information below.

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

$ nmap ... # TODO:



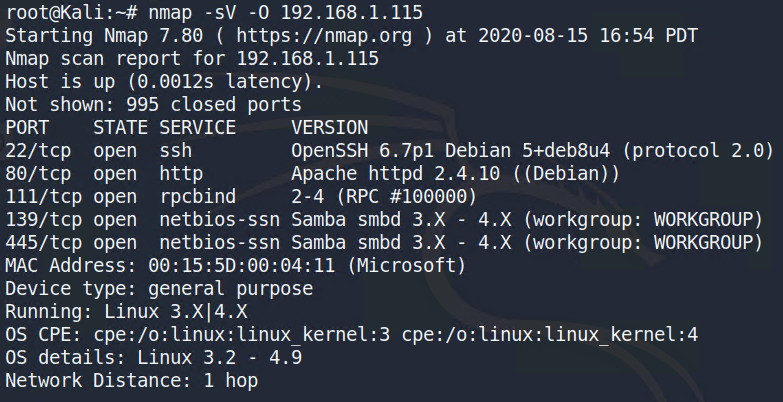
# TODO: Insert scan output



$ nmap ... # TODO: Add command to Scan Target 2



# TODO: Insert scan output



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

**Target 1**

1. ssh
2. http
3. netbios

**Target 2**

1. ssh
2. http
3. netbios

### Critical Vulnerabilities

TODO: Fill out the list below. Include severity and CVE numbers, if possible.

The following vulnerabilities were identified on each target:

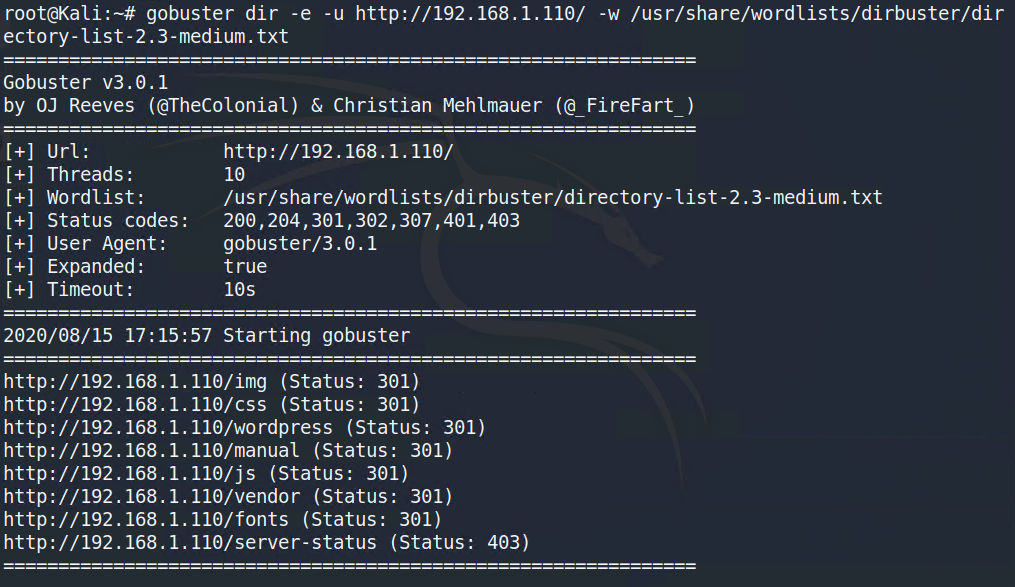
**Target 1**

1. CVE-2006-4028 - Wordpress Sites
2. [CVE-2017-7494](https://www.cvedetails.com/cve/CVE-2017-7494/) - Samba
3. CVE-2017-8779 - RPC bind

**Target 2**

1. CVE-2006-4028 - Wordpress Sites
2. [CVE-2017-7494](https://www.cvedetails.com/cve/CVE-2017-7494/) - Samba
3. CVE-2017-8779 - RPC bind

TODO: Include vulnerability scan results as proof of the identified vulnerabilities.



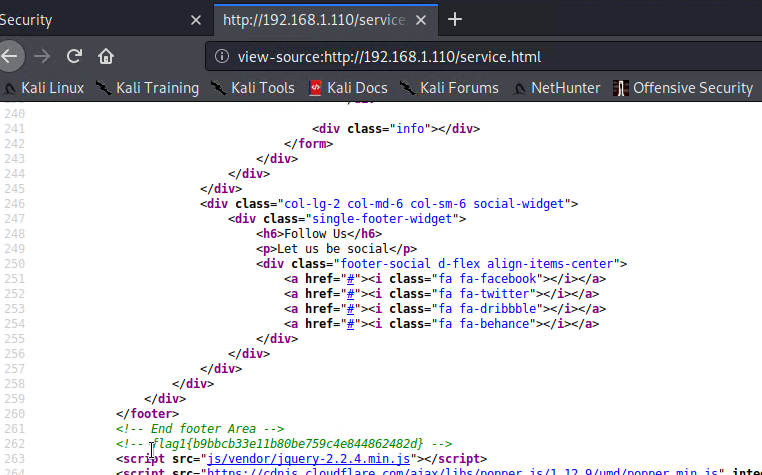
Exploitation

TODO: Fill out the details below. Include screenshots where possible.

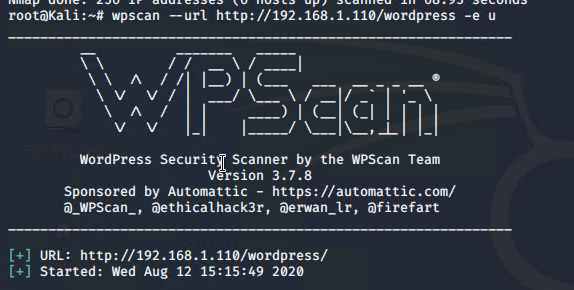
The Red Team was able to penetrate both Target 1 and Target 2 and retrieve the following confidential data:

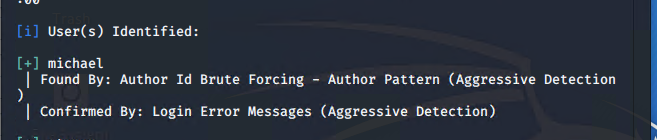
**Target 1**

* flag1.txt: TODO: Insert flag1.txt hash value.



* flag2.txt: TODO: Insert flag2.txt hash value.
* Exploit Used
  + TODO: wpscan
  + TODO: Include the command run.





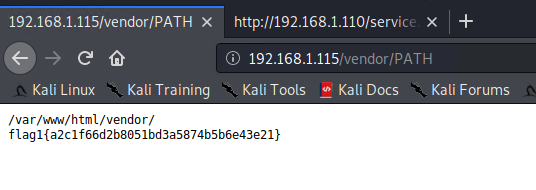


Password= Michael



**Target 2**

* flag1.txt: TODO: Insert flag1.txt hash value.
* Exploit Used



* flag2.txt: TODO: Insert flag2.txt hash value.
* Exploit Used
  + TODO: Identify the exploit used.
  + TODO: Include the command run.

