# **Red Team: Summary of Operations**

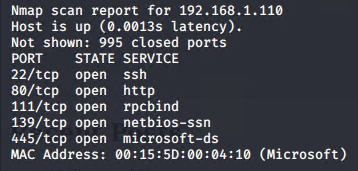
## **Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

### **Exposed Services**

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

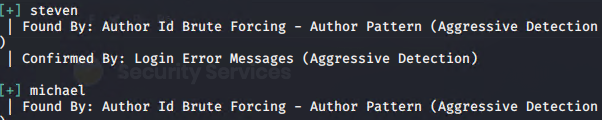
$ **nmap 192.168.1.0/24**



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

* Target 1
  + **Service ssh port 22**
  + **Service http port 80**

The following vulnerabilities were identified on each target:

* Target 1
  + 
  + 
  + 

### **Exploitation**

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

* Target 1
  + flag1.txt: 
  + **Exploit Used**
    - * ***ssh into Michael’s account and look in the/var/www files***
      * ***cd /var/www***
      * ***ls***
      * ***cd html***
      * ***ls***
      * ***cat service.html***
  + flag2.txt: **
    - **Exploit Used**
      * ***ssh into Michael’s account and look in the /var/www files***
      * ***cd /var/www***
      * ***ls***
      * ***cat flag2.txt***