# **Blue Team: Summary of Operations**

## **Table of Contents**

* Network Topology
* Description of Targets
* Monitoring the Targets
* Patterns of Traffic & Behavior
* Suggestions for Going Further

### **Network Topology**

The following machines were identified on the network:

* Target 1
  + **Operating System**: Linux
  + **Purpose**: Web Server
  + **IP Address**: 192.168.1.110
* Target 2
  + **Operating System**: Linux
  + **Purpose**: Web Server
  + **IP Address**: 192.168.1.115
* Capstone
  + **Operating System**: Linux
  + **Purpose**: Web Server
  + **IP Address**: 192.16.8.1.105
* ELK
  + **Operating System**: Linux
  + **Purpose**: SIEM
  + **IP Address**: 192.168.1.100
* Kali
  + **Operating System**: Linux
  + **Purpose**: Attack Machine
  + **IP Address**: 192.168.1.90
* ML-REFVM-684427
  + **Operating System**: Windows
  + **Purpose**: NATSwitch
  + **IP Address**: 192.168.1.1

### 

### **Description of Targets**

The target of this attack was: Target1 192.168.1.110

Target 1 is an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers. As such, the following alerts have been implemented:

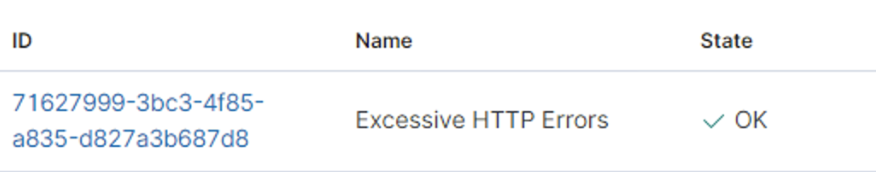
### **Monitoring the Targets**

Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:

#### **Excessive HTTP Errors**

[Excessive HTTP Errors] is implemented as follows:

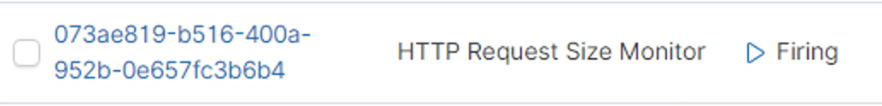
* **Metric**: http.response.status\_code
* **Threshold**: 400 for the last 5 minutes
* **Vulnerability Mitigated**: Brute Force Attacks
* **Reliability**: High reliability



#### **HTTP Request Size Monitor**

[HTTP Request Size Monitor] is implemented as follows:

* **Metric**: http.request.bytes
* **Threshold**: 3500 for the last 1 minute
* **Vulnerability Mitigated**: DOS Attacks
* **Reliability**: High reliability



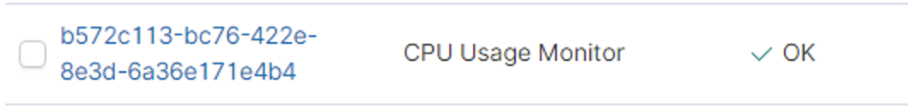
#### 

#### 

#### **CPU Usage Monitor**

Alert 3 is implemented as follows:

* **Metric**: system.process.cpu.total.pct
* **Threshold**: 0.5 for the last 5 minutes
* **Vulnerability Mitigated**: Excessive CPU Usage, Resource Usage Issues
* **Reliability**: Medium reliability

**

# **Red Team: Summary of Operations**

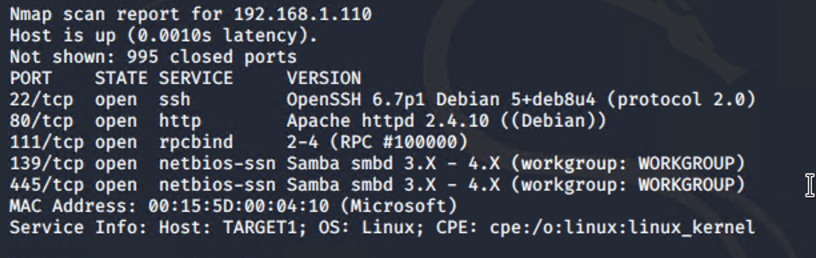
## **Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

### **Exposed Services**

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

$ nmap -sV 192.168.1.110



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

* Target 1

Port 22 / SSH

Port 80 / http

Port 111 / rpcbind

The following vulnerabilities were identified on each target:

* Target 1

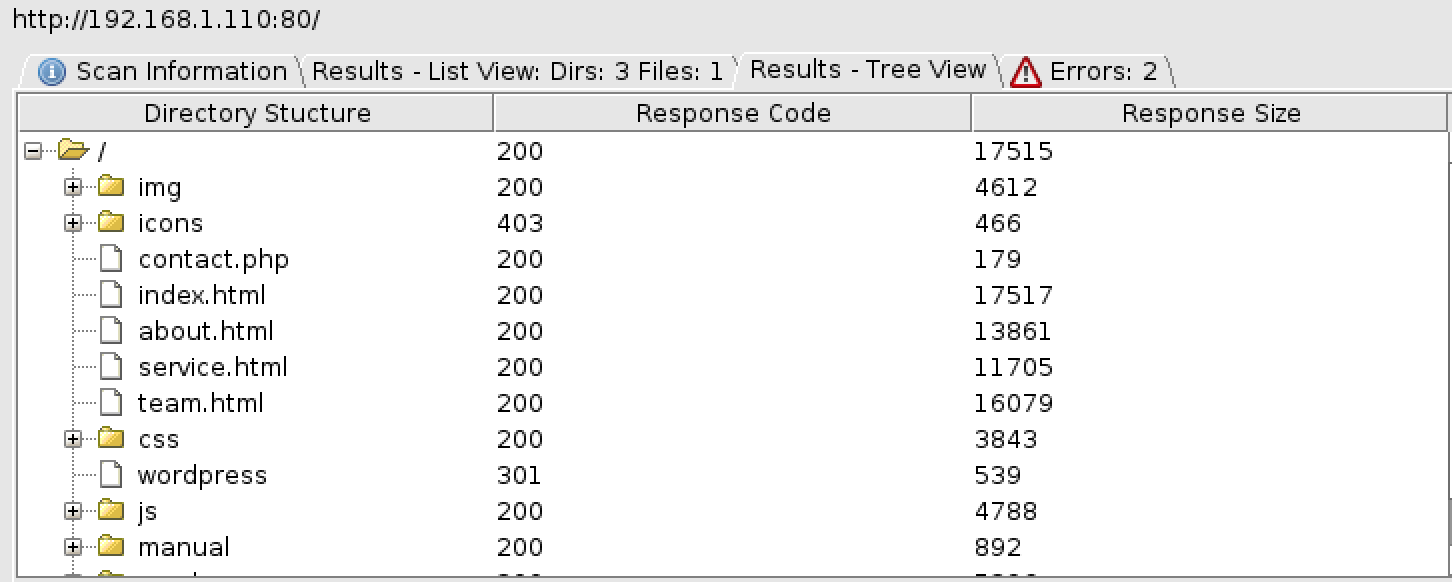
Port 22 is Open, this gives us the ability to ssh into the machine with discovered credentials.

Port 80 is Open, this gives us access to the web server via the web browser.

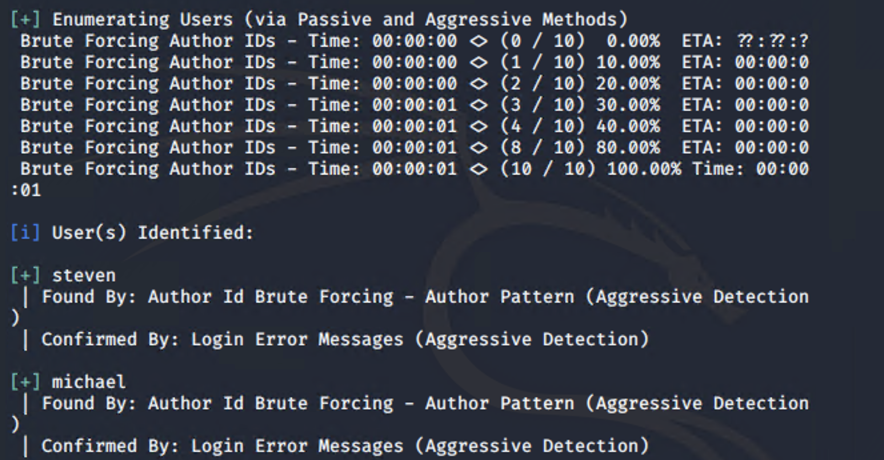
### **Exploitation**

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

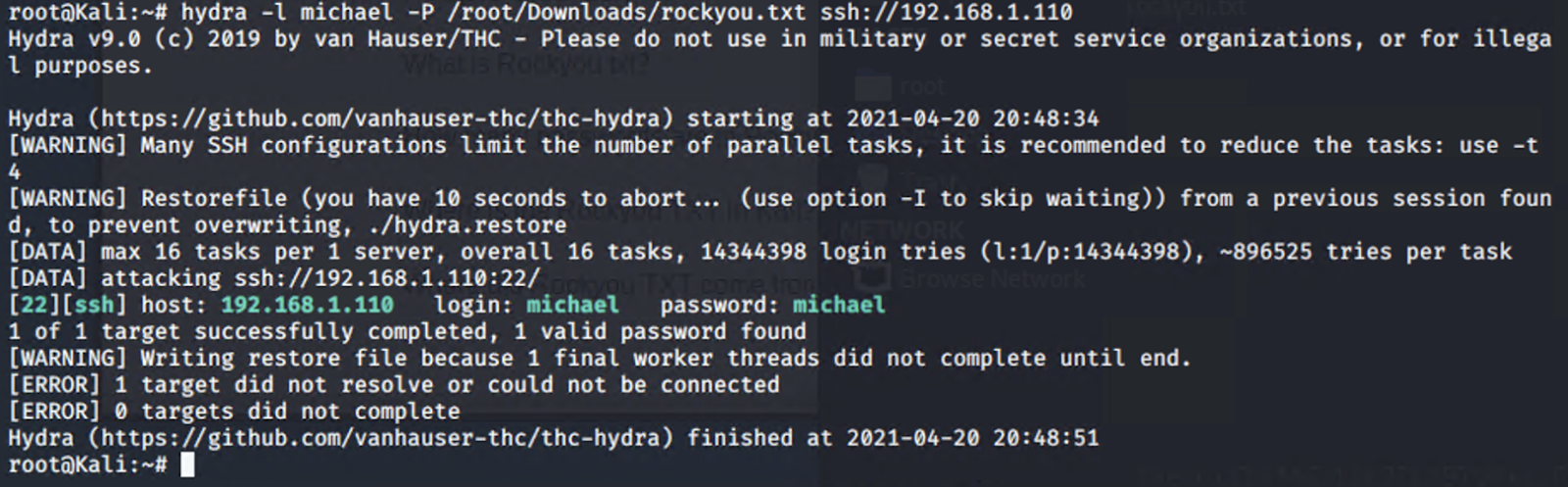
First, we ran an enumeration scan to uncover the users and hidden directories.

Dirbuster showed used the document containing flag1   


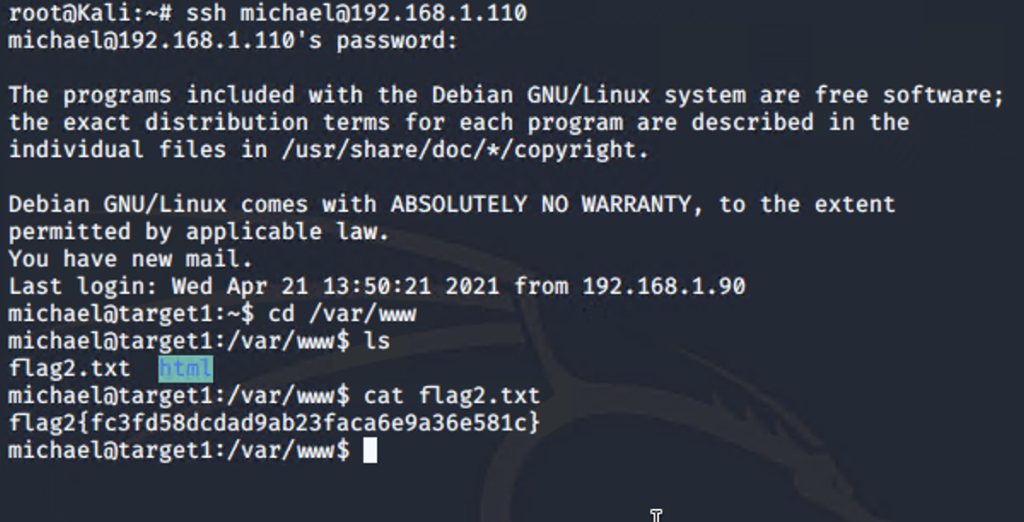
* Target1
  + flag1.txt:{b9bbcb33e11b80be759c4e844862482d}
    - **Exploit Used**
      * *Brute Force Directory discovery to identify service.html*
* **Exploit Used**
  + - *WordPress Security Scan*
    - wpscan --url <http://192.168.1.110/wordpress> --wp-content-dir -at -eu



* **Exploit Used**
  + - *Hydra (Brute Force Password Cracking)*
    - *hydra -l michael -P /root/Downloads/rockyou.txt ssh://192.168.1.110*

**

* + flag2.txt: *{fc3fd58dcdad9ab23faca6e9a36e581c}*
    - **Exploit Used**
      * *SSH*
      * *ssh michael@192.168.1.110*

**