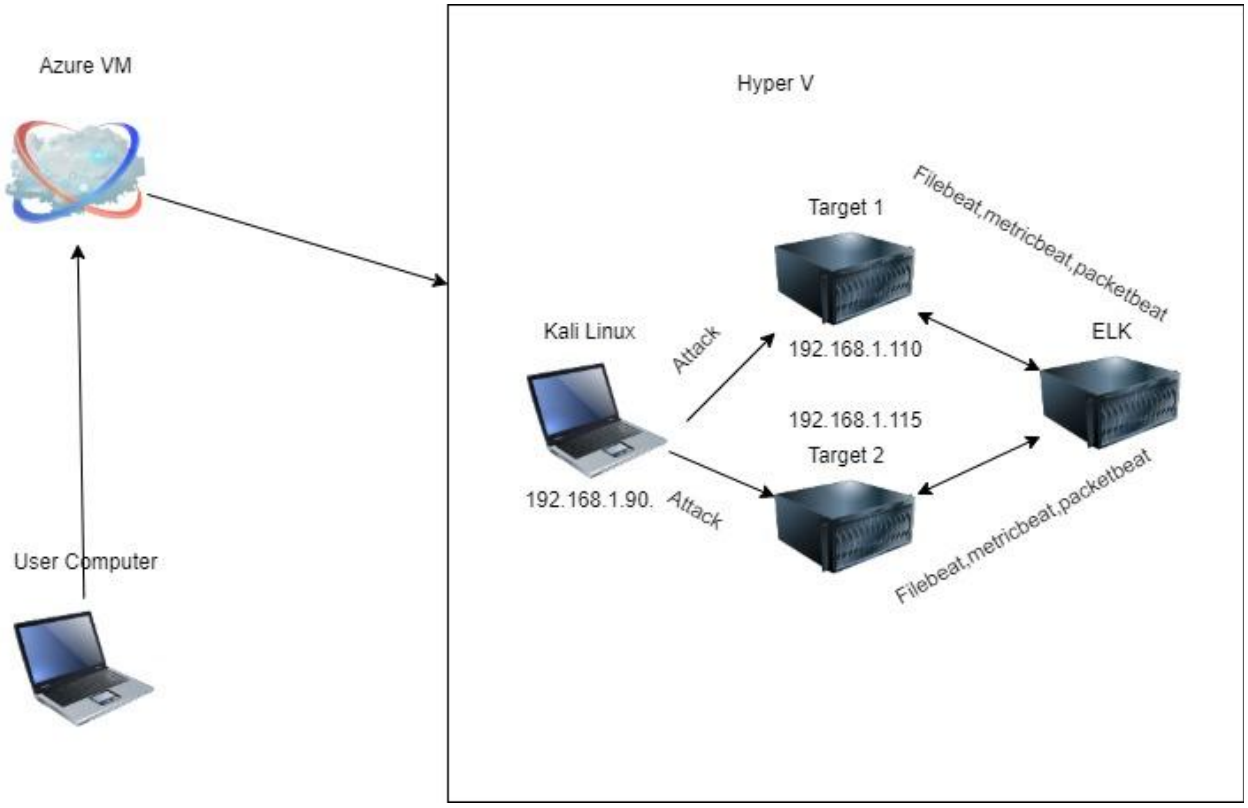
Blue Team: Summary of Operations

Table of Contents

Network Topology



The following machines were identified on the network:

- Network
  - **Address Range**: 192.168.1.0/24
  - **Netmask**: 255.255.255.0
  - **Gateway**: 10.0.0.1
- Machines

    - **Operating System**: Linux
    - **Purpose**: ELK
    - **IP Address**: 192.168.1.100
-
    - **Operating System**: Kali Linux
    - **Purpose**: Attacker
    - **IP Address**: 192.168.1.90
-
    - **Operating System**: Linux
    - **Purpose**: Target 1
    - **IP Address**: 192.168.1.110
-
    - **Operating System**: Linux
    - **Purpose**: Target 2
    - **IP Address**: 192.168.1.15

Description of Targets

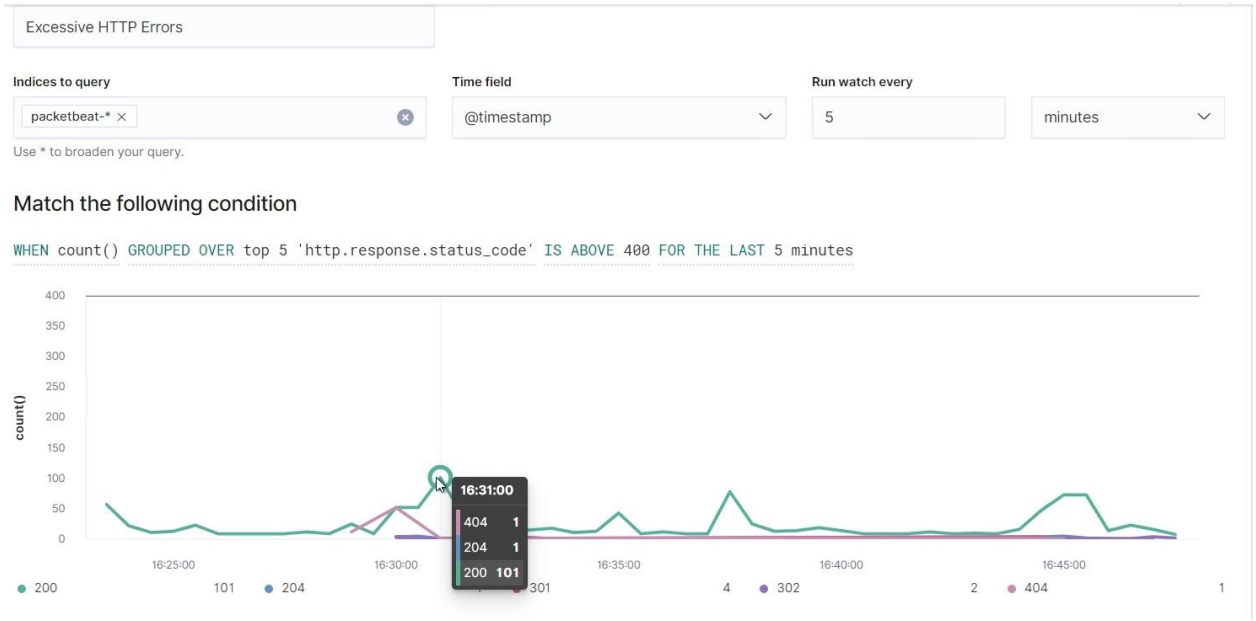
The target of this attack was: `Target 1` 192.168.1.110

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:

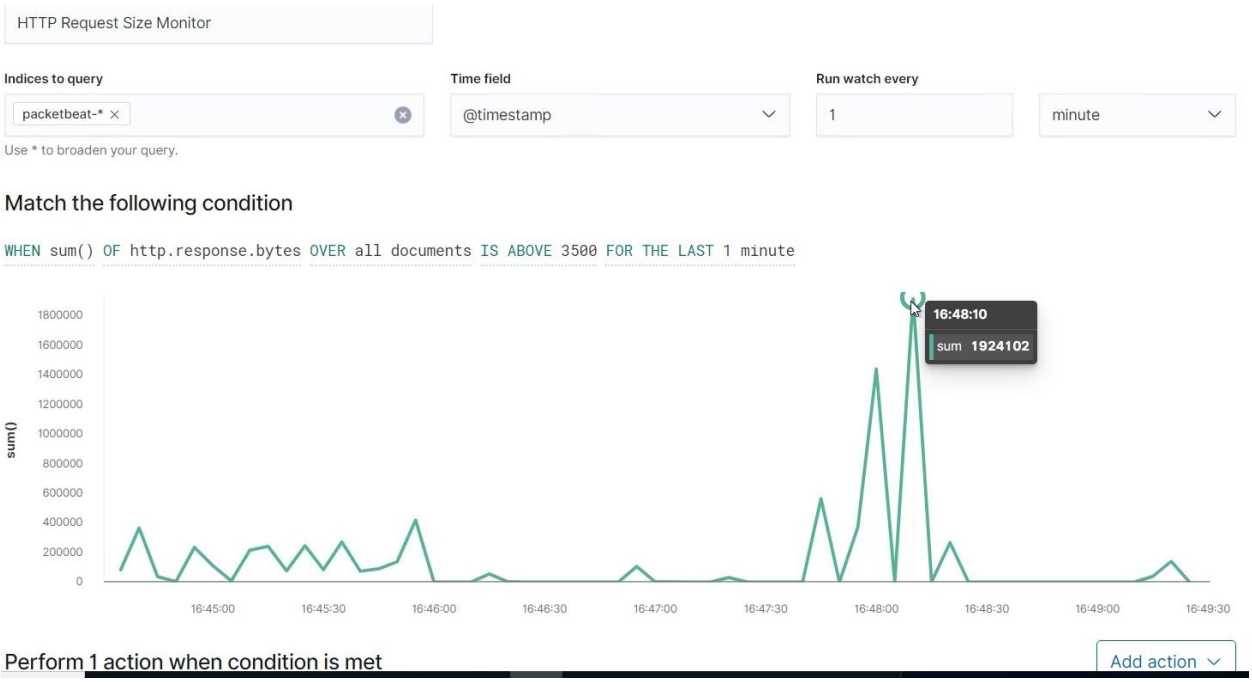
Excessive HTTP Errors



Alert 1 is implemented as follows:

- **Metric**: packetbeat*
- **Threshold**: WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
- **Vulnerability Mitigated**: Excessive HTTP Errors
- **Reliability**: low reliability creates false positives

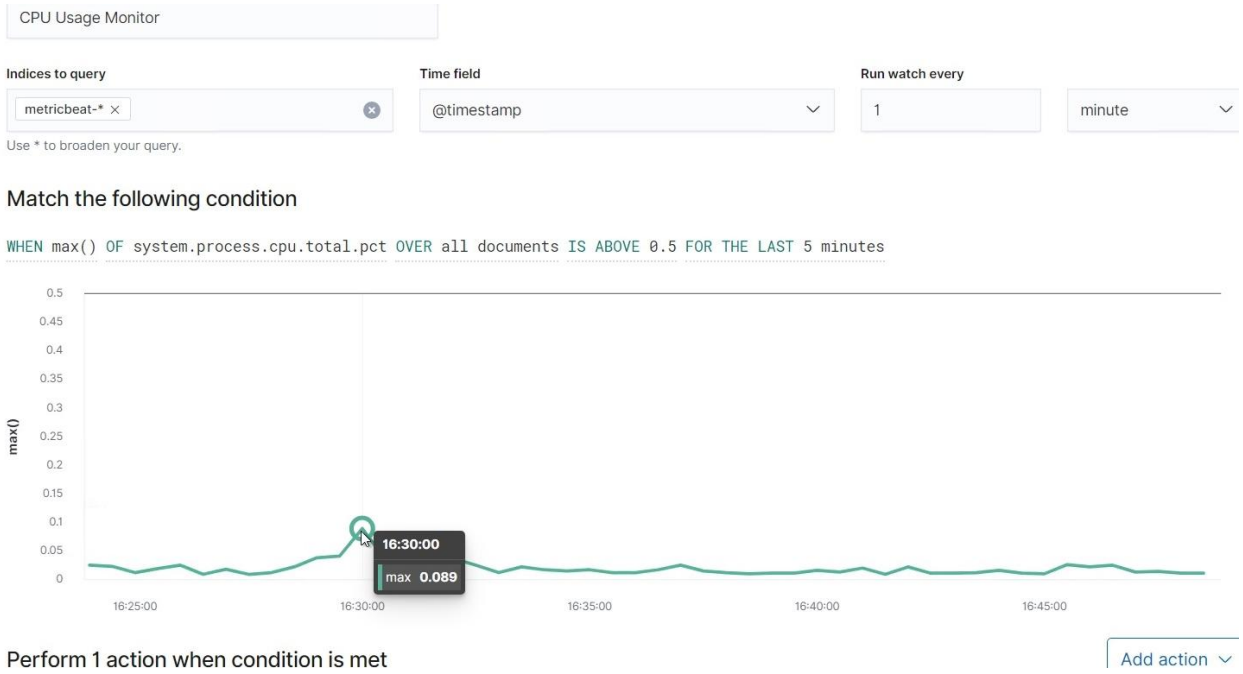
HTTP Requests Size Monitor



Alert 2 is implemented as follows:

- **Metric**: packetbeat*
- **Threshold**: WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
- **Vulnerability Mitigated**: HTTP Request Size Monitor
- **Reliability**: Medium Reliability, The amount of traffic per minute the alert spiked multiple times.

CPU Usage Monitor



Alert 3 is implemented as follows:

- **Metric**: metricbeat*
- **Threshold**: WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
- **Vulnerability Mitigated**: CPU Usage Monitor
- **Reliability**: Low reliability, The monitoring is stagnant.

Suggestions for Going Further (Optional)

- Each alert above pertains to a specific vulnerability/exploit. Recall that alerts only detect malicious behavior, but do not stop it. For each vulnerability/exploit identified by the alerts above, suggest a patch. E.g., implementing a blocklist is an effective tactic against brute-force attacks. It is not necessary to explain *how* to implement each patch.

The logs and alerts generated during the assessment suggest that this network is susceptible to several active threats, identified by the alerts above. In addition to watching for occurrences of such threats, the network should be hardened against them. The Blue Team suggests that IT implement the fixes below to protect the network:

- Vulnerability 1 Exposed WordPress Credentials
    - **Patch**: Update WordPress to the newest patch
    - **Why It Works**: Updated patch will disable the ability for attackers to gain access to user login credentials
- Vulnerability 2 CVE-2006-0151
    - **Patch**: Update to system to newest update
    - **Why It Works**: Updating system will disable the ability for attacks to do sudo command and use Python scripts to escalate privilege.
- Vulnerability 3 Weak passwords
    - **Patch**: Have 2 Multi factors, update password every three months, and must have 10 charter or more.
    - **Why It Works**: Making a password longer will make it harder for a bad actor to get in the account

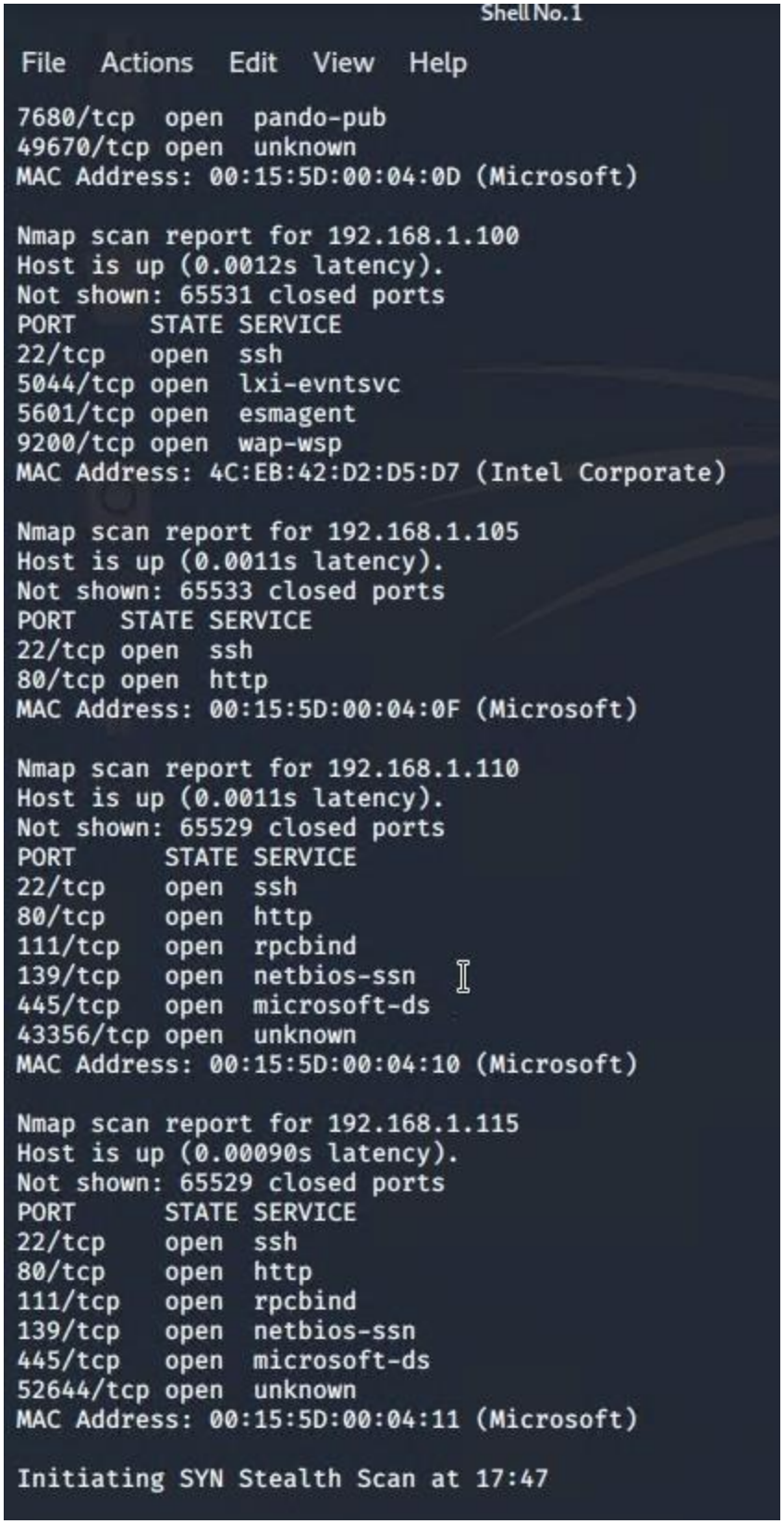
Red Team: Summary of Operations

Table of Contents

Exposed Services

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

```
$ nmap ... # nmap -sV 192.168.1.110/24 , nmap -T4 -v -p- 192.168.1.100
```



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

- Target 1
    - List of
    - Exposed Services

The following vulnerabilities were identified on each target:

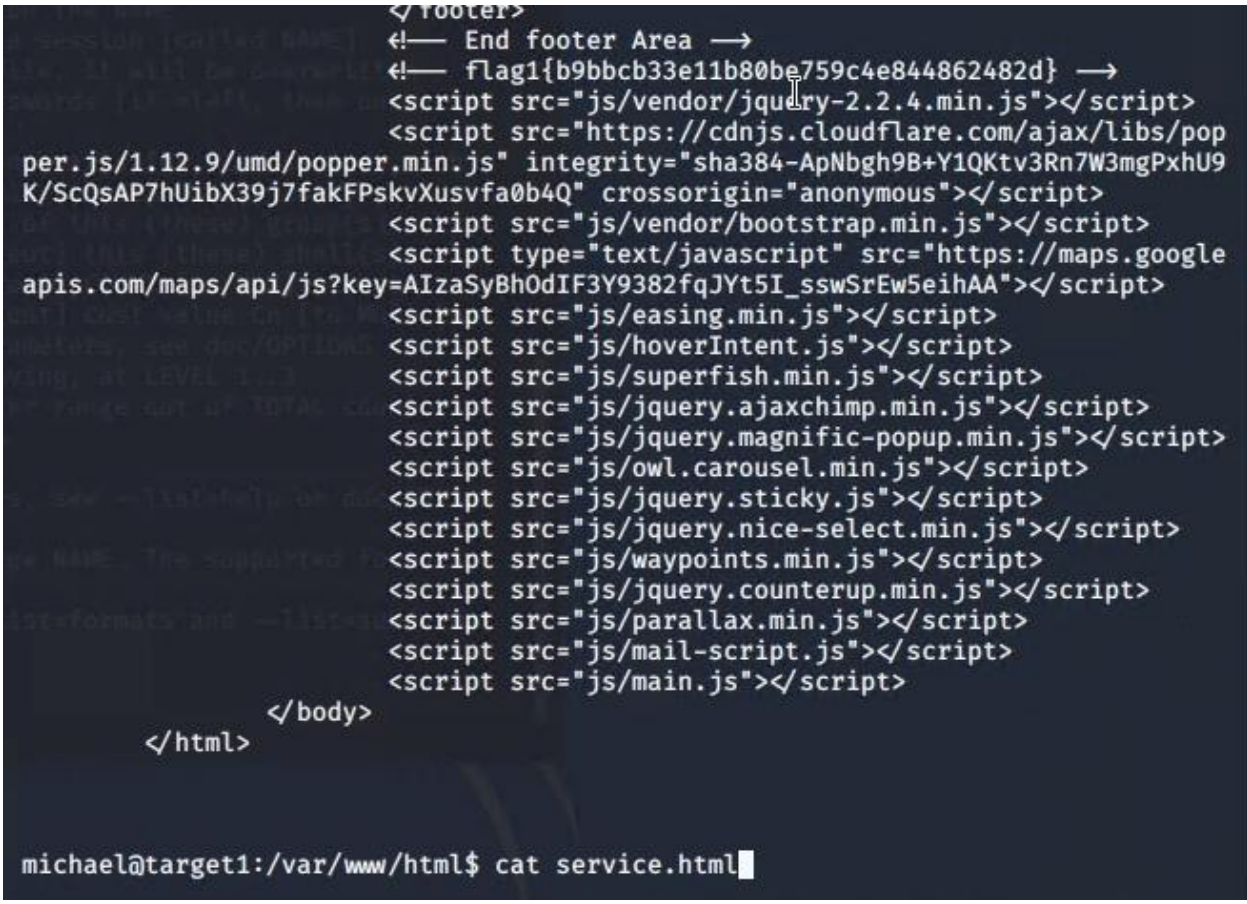
- Target 1
    - List of
    - Critical
    - Vulnerabilities

Exploitation

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

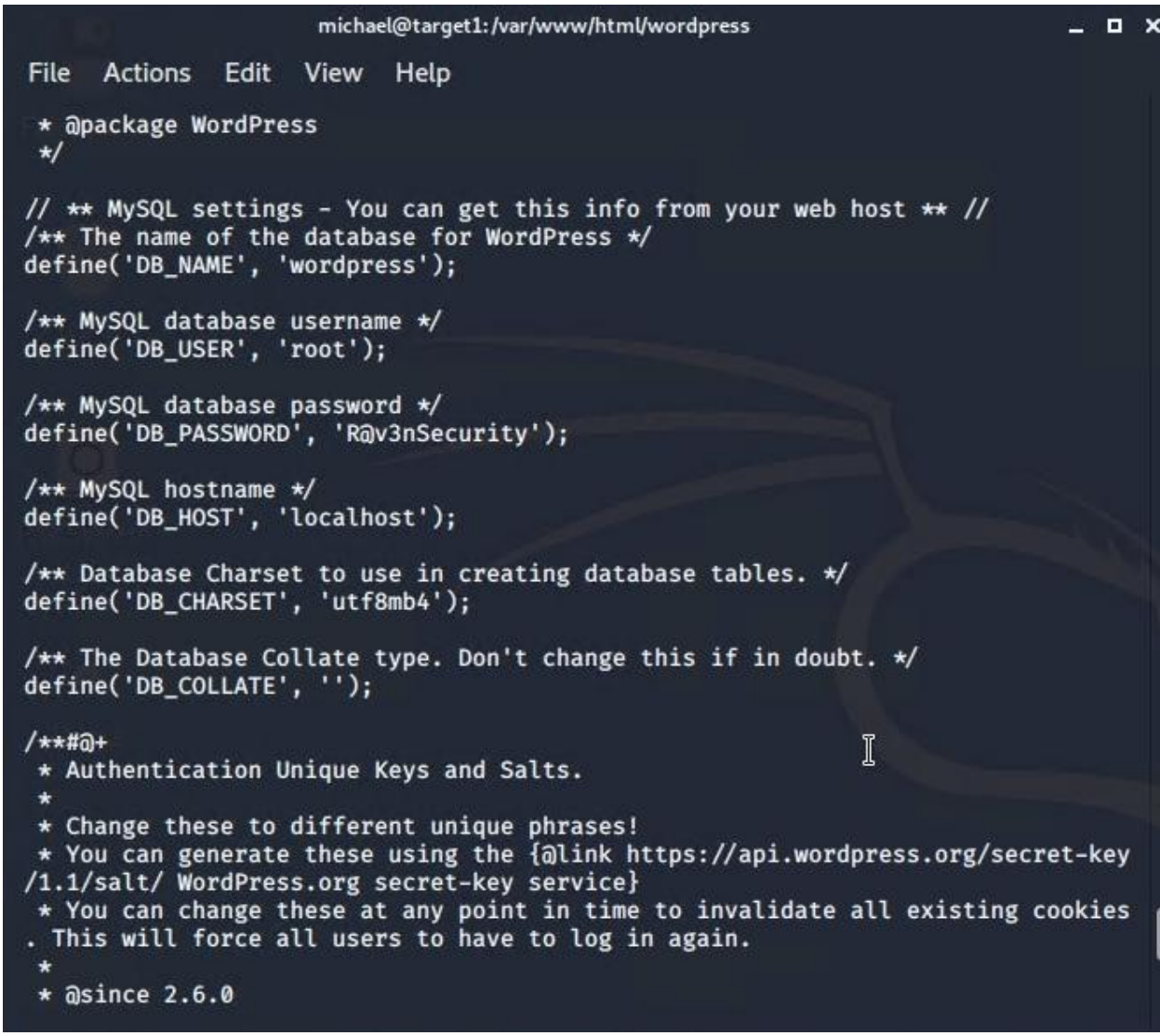
- Target 1

- `flag1.txt`: *TODO: Insert `flag1.txt`*



  - **Exploit Used**
    - *Weak password exploit michaels password was his name, so i was able to SSH into his account*
    - *SSH 192.168.1.110@michael password michael once in CD into /var/www/html and looked around and I CAT the service.html file and found flag1 hash*

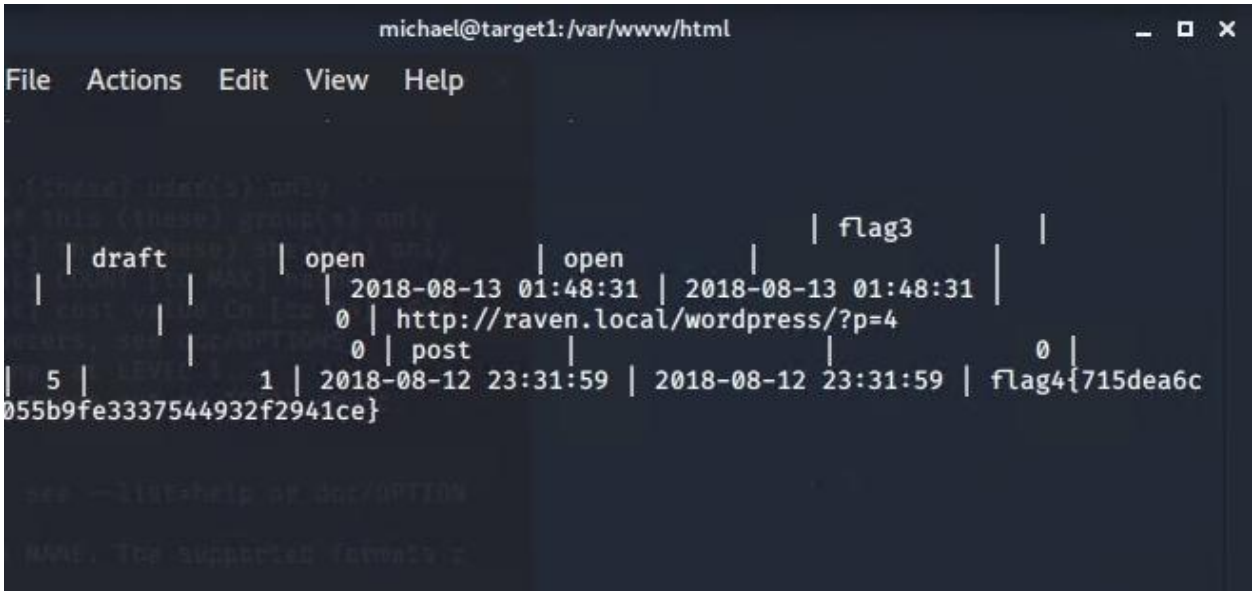
- `flag2.txt`:



  - **Exploit Used**
    - *Weak password exploit michaels password was his name, so i was able to SSH into his account*

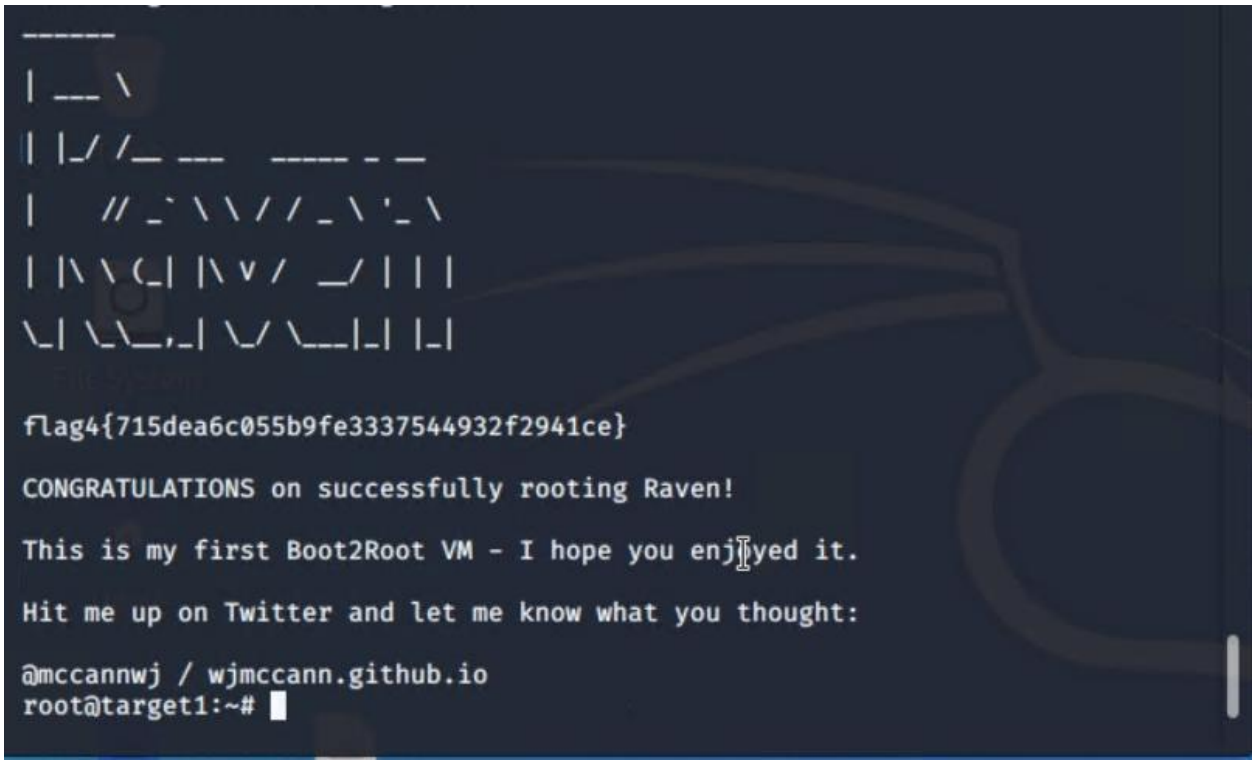
- *SSH 192.168.1.110@michael password michael once in CD into /var/www/ and looked around and LS the directory and found flag2 cat flag 2 and got the hash.*

`flag3.txt`:

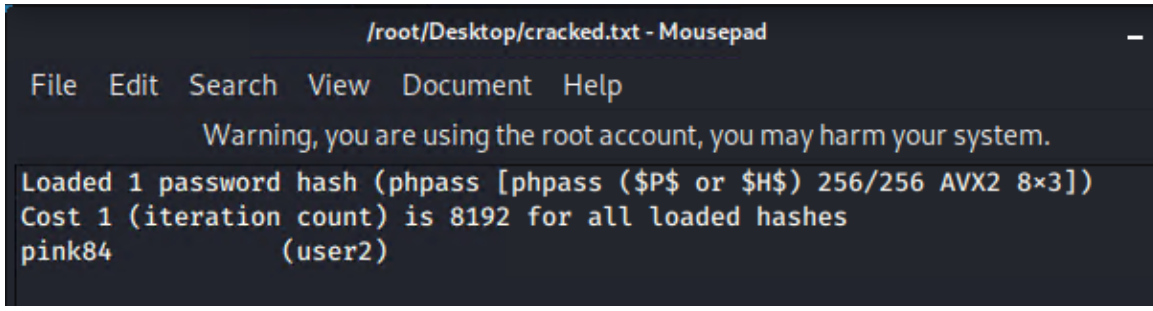


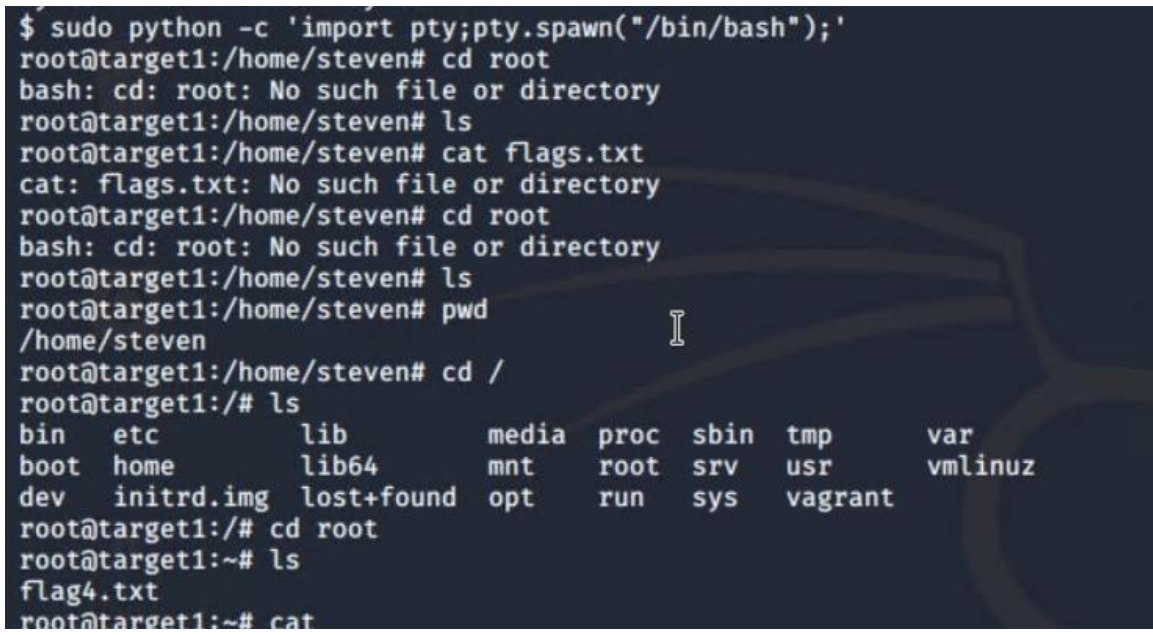
- **Exploit Used**
  - *Weak password exploit michaels password was his name, so i was able to SSH into his account*
  - *SSH 192.168.1.110@michael password michael once in CD into /var/www/html and looked around and LS the directory and found flag3 when I cat html.*

- `flag4.txt`:



  - **Exploit Used**
    - *We found the hashes to michaels and stevens with John the ripper. Once I gotstevens password pink84. I was able to SSH into stevens account once in stevens account I CD into root ls into root and found flag4 and cat flag4text it showed the final hash.*





Network Forensic Analysis Report

TODO Complete this report as you complete the Network Activity on Day 3 of class.

Time Thieves

You must inspect your traffic capture to answer the following questions:

1. What is the domain name of the users' custom site?

   frank-n-ted.com

2. What is the IP address of the Domain Controller (DC) of the AD network?

   10.6.12.12

3. What is the name of the malware downloaded to the 10.6.12.203 machine?

june11.d11

- Once you have found the file, export it to your Kali machine's desktop.

4. Upload the file to VirusTotal.com.
5. What kind of malware is this classified as?

   Trojan

Vulnerable Windows Machine

1. Find the following information about the infected Windows machine:

   - Host name: Rotterdam-pc
   - IP address: 172.16.4.205
   - MAC address: 00:59:07:b0:63:a4

2. What is the username of the Windows user whose computer is infected?

   mattijs.dervies

3. What are the IP addresses used in the actual infection traffic?

   185.243.115.84

4. As a bonus, retrieve the desktop background of the Windows host.

Illegal Downloads

1. Find the following information about the machine with IP address 10.0.0.201:

   - MAC address: 00:16::17:18:66:c8
   - Windows username: elmer.blanco
   - OS version: blanco-desktop