Blue Team: Summary of Operations

Table of Contents

Network Topology

The following machines were identified on the network:

- Kali
  - **Operating System**: Kali Linux
  - **Purpose**: Attacking machine
  - **IP Address**: 192.168.1.90
- ELK
  - **Operating System**: Ubuntu
  - **Purpose**: Monitors traffic during the attack
  - **IP Address**: 192.168.1.100
- Target 1
  - **Operating System**: Debian Linux
  - **Purpose**: Wordpress server being attacked
  - **IP Address:** 192.168.1.110
- Capstone
  - **Operating System**: Ubuntu
  - **Purpose**: Vulnerable Web Server
  - **IP Address**: 192.168.1.105

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:

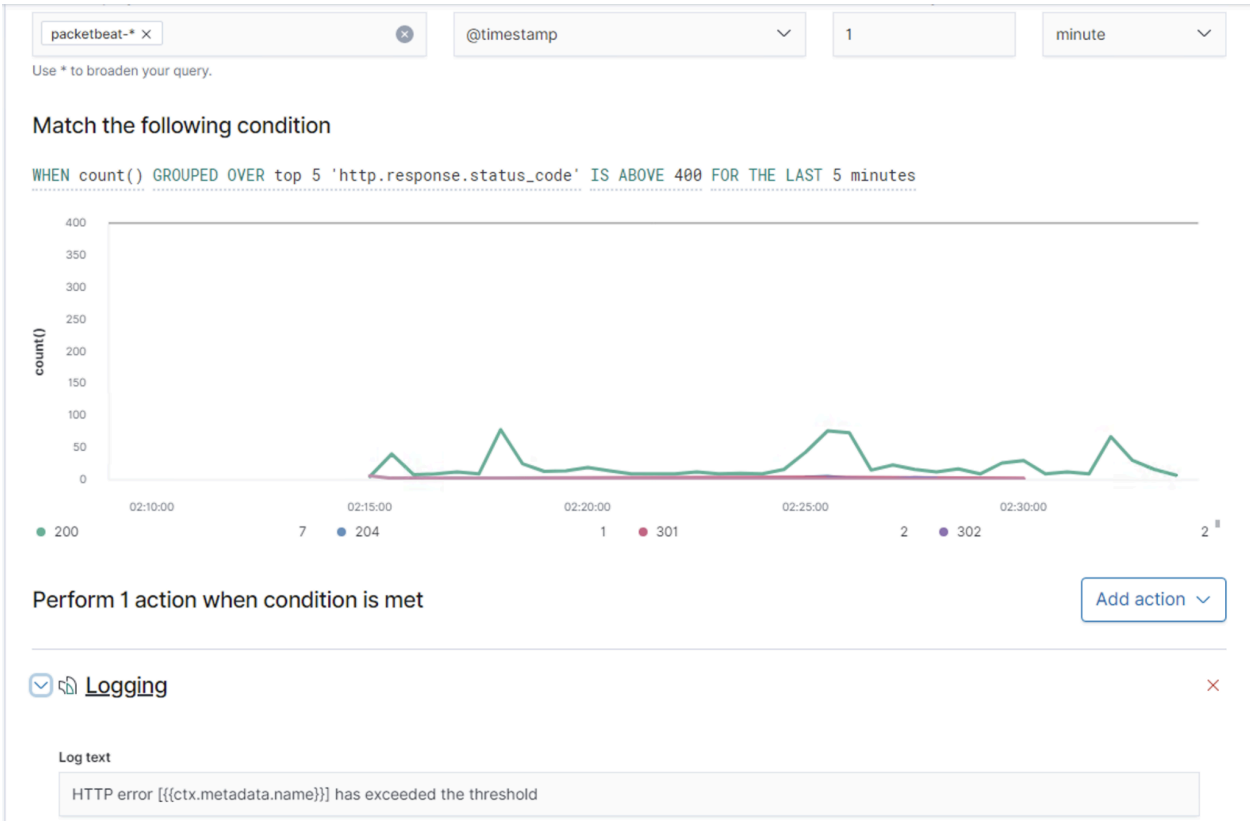
Monitoring the Targets

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:

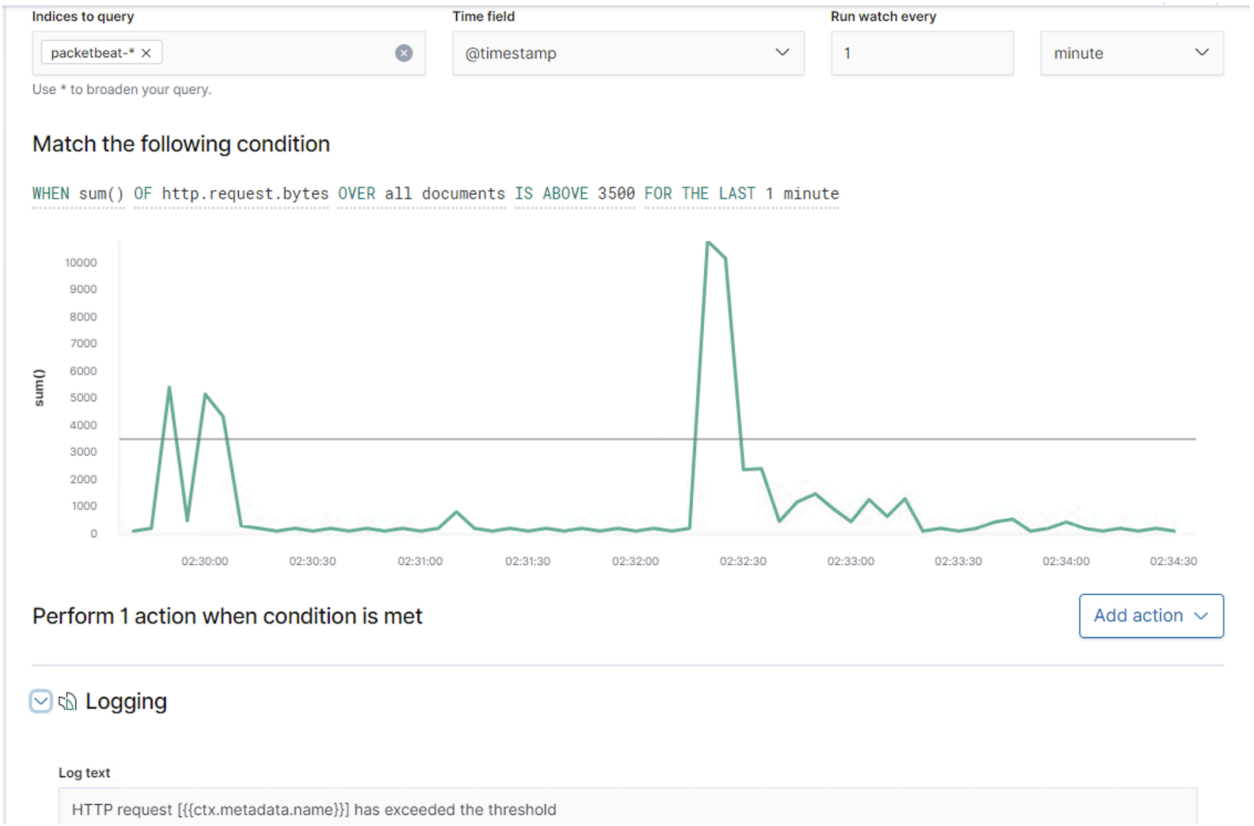
- **Metric**: WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
- **Threshold**: 400
- **Vulnerability Mitigated**: Bruteforce
- **Reliability**: This alert is highly reliable, this will filter out the successful or normal responses and allow us to see the errors that are a concern.



HTTP Request Size Monitor

Alert 2 is implemented as follows:

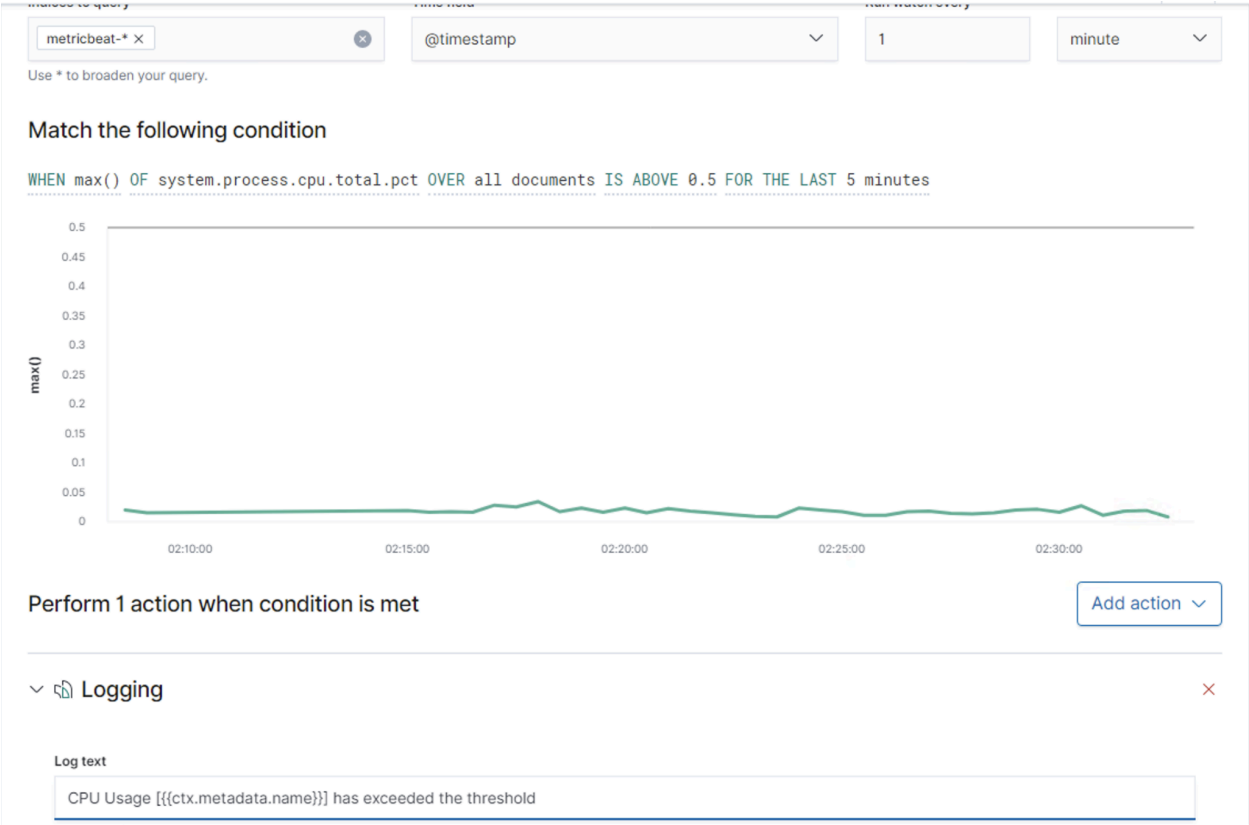
- **Metric**: WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
- **Threshold**: 3500
- **Vulnerability Mitigated**: DDOS
- **Reliability**: This alert could cause false positives and is considered a medium reliability, legitimate HTTP requests could set this alert off.



CPU Usage Monitor

Alert 3 is implemented as follows:

- **Metric**: WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
- **Threshold**: 0.5
- **Vulnerability Mitigated**: Malware
- **Reliability**: This alert is highly reliable, it will be obvious when a malicious software/program is running.



Red Team: Summary of Operations

Table of Contents

- Exposed Services
- Critical Vulnerabilities
- Exploitation

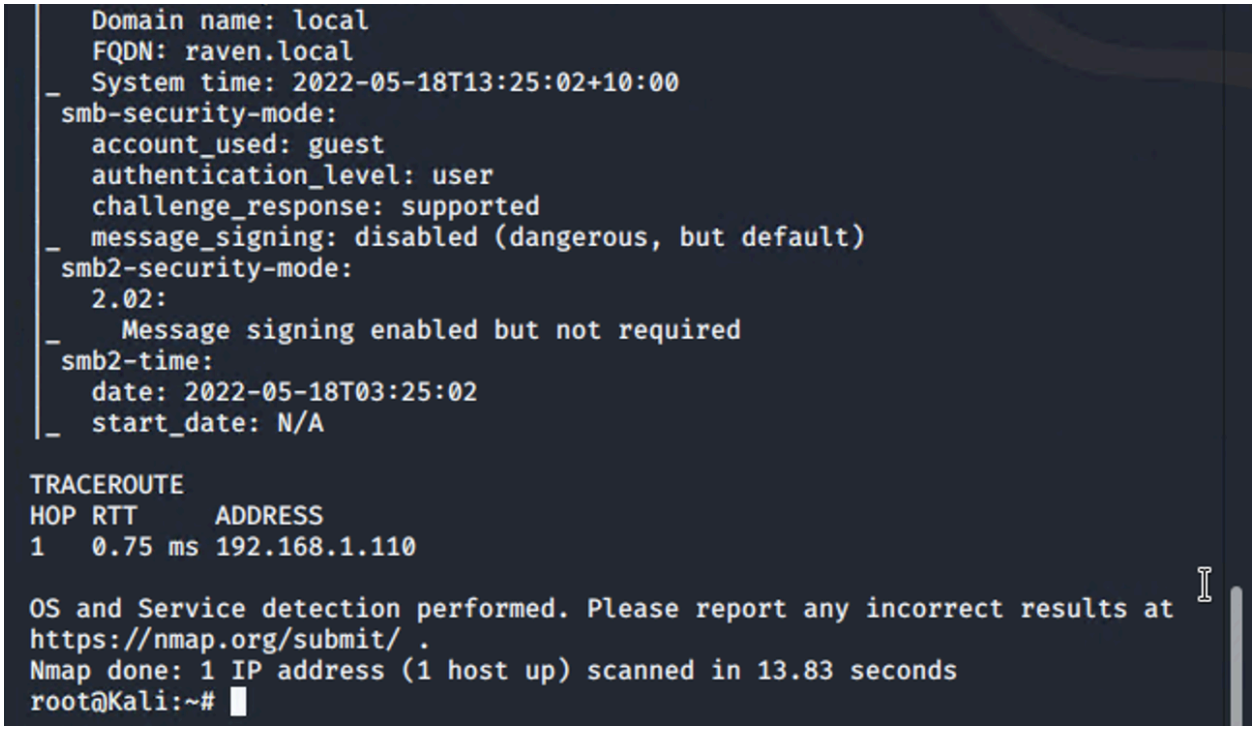
Exposed Services

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

$ nmap -sV 192.168.1.0/24

```
root@Kali:~# nmap -A 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-17 20:24 PDT
NSOCK ERROR [13.7510s] mksock_bind_addr(): Bind to 0.0.0.0:22 failed (IOD #
56): Address already in use (98)
Nmap scan report for 192.168.1.110
Host is up (0.00075s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 26:81:c1:f3:5e:01:ef:93:49:3d:91:1e:ae:8b:3c:fc (DSA)
|   2048 31:58:01:19:4d:a2:80:a6:b9:0d:40:98:1c:97:aa:53 (RSA)
|   256 1f:77:31:19:de:b0:e1:6d:ca:77:07:76:84:d3:a9:a0 (ECDSA)
|_  256 0e:85:71:a8:a2:c3:08:69:9c:91:c0:3f:84:18:df:ae (ED25519)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Raven Security
111/tcp open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          39868/udp   status
|   100024  1          47094/tcp6  status
|   100024  1          48077/udp6  status
|_  100024  1          60989/tcp   status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.2.14-Debian (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -3h19m59s, deviation: 5h46m24s, median: 0s
|_nbstat: NetBIOS name: TARGET1, NetBIOS user: <unknown>, NetBIOS MAC: <unk
nown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.2.14-Debian)
|   Computer name: raven
|   NetBIOS computer name: TARGET1\x00
|   Domain name: local
```



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

- Target 1
    - Ssh (Port 22)
    - HTTP (Port 80)

The following vulnerabilities were identified on each target:

- Target 1
    - Weak password enforcement (User “michael” had the password “michael”)
    - MySQL login credentials were located in “wp-config.php” in plaintext
    - User “Steven” was able to execute python code to escalate to root privileges

Exploitation

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

- Target 1
    - Ssh into user “Michael”’s account
        - **Exploit Used**
            - *User had the same username and password*
            - *Ssh michael@192.168.1.110*

```
root@Kali:~# ssh michael@192.168.1.110
michael@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
michael@target1:~$
```

- MySQL login credentials
  - **Exploit Used**
    - MySQL login credentials were in wp-config.php in plaintext
    - *Command to gain access: mysql -u -root -p*
      - *Password R@v3nSecurity*

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');
```

```
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 66
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 stateme
nt.

mysql>
```

Flag 3+4 were found in MySQL

Network Analysis

Time Thieves

At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range `10.6.12.0/24`.

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

   june11.dll

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

   Trojan

Vulnerable Windows Machines

The Security team received reports of an infected Windows host on the network. They know the following:

- Machines in the network live in the range `172.16.4.0/24`.
- The domain mind-hammer.net is associated with the infected computer.
- The DC for this network lives at `172.16.4.4` and is named Mind-Hammer-DC.
- The network has standard gateway and broadcast addresses.

Inspect your traffic to answer the following questions:

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?

   172.16.2.205 and 185.243.114.84

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

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:

- The machines using torrents live in the range `10.0.0.0/24` and are clients of an AD domain.
- The DC of this domain lives at `10.0.0.2` and is named DogOfTheYear-DC.
- The DC is associated with the domain dogoftheyear.net.

Your task is to isolate torrent traffic and answer the following questions:

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

2. Which torrent file did the user download?

Betty_Boop_Rythm_on_the_Reservation.avi.torrent