Input Correct Password の解説

工藤信一朗

2021 年 7 月 11 日

目次

1 Input Correct Password

これは、1~4 年生を対象にした問題でした。初心者向け CTF ではよくある問題として追加しました。

1.1 ソースコード

```c
#include <stdint.h>
#include <stdio.h>
#include <string.h>

int main(){
    char password[20] = "dmac_ps";
    char password0[20] = "asdf1234";
    char password1[20] = "true_pass";
    char password2[20] = "pass_kit";
    char password3[20] = "linux_mac_windows";
    char password4[20] = "print_pass";
    char password5[20] = "KitKitKitKitKitKit";
```

```
    char check_string[20];
    uint32_t buff;

    uint32_t check_result = 4;
    printf("password?:");
    memset(check_string, 0, sizeof(check_string));
    for (int i = 0; i < sizeof(check_string); i++) {
        buff = getchar();
        if (buff == EOF) break;
        if (buff == 0x0a) break;
        check_string[i] = buff;
    }

    check_result = strcmp(password, check_string);

    if (check_result == 0){
        printf("Succuss!!!\tflag is htp-ctf{users input} \n");
    } else {
        printf("error  \ncheck s*r*** command\n");
    }
    return 0;
}
```

1.2 解法

strings コマンドを利用することで平文となっている箇所を探し、確認します。

```
$ strings Input_correct_passwordcd
/lib64/ld-linux-x86-64.so.2
libc.so.6
puts
__stack_chk_fail
printf
memset
getchar
```

```
__cxa_finalize
strcmp
__libc_start_main
GLIBC_2.4
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u+UH
dmac_ps
asdf1234
true_pas
pass_kit
linux_maH
c_windowH
print_pa
KitKitKiH
tKitKitKH
[]A\A]A^A_
password?:
Succuss!!! flag is htp-ctf{users input}
error
check s*r*** command
:*3$"
GCC: (Ubuntu 9.3.0-17ubuntu1~20.04) 9.3.0
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.8060
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
what_password.c
__FRAME_END__
__init_array_end
_DYNAMIC
__init_array_start
```

```
__GNU_EH_FRAME_HDR
_GLOBAL_OFFSET_TABLE_
__libc_csu_fini
_ITM_deregisterTMCloneTable
puts@@GLIBC_2.2.5
_edata
__stack_chk_fail@@GLIBC_2.4
printf@@GLIBC_2.2.5
memset@@GLIBC_2.2.5
__libc_start_main@@GLIBC_2.2.5
__data_start
strcmp@@GLIBC_2.2.5
getchar@@GLIBC_2.2.5
__gmon_start__
__dso_handle
_IO_stdin_used
__libc_csu_init
__bss_start
main
__TMC_END__
_ITM_registerTMCloneTable
__cxa_finalize@@GLIBC_2.2.5
.symtab
.strtab
.shstrtab
.interp
.note.gnu.property
.note.gnu.build-id
.note.ABI-tag
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rela.dyn
.rela.plt
.init
```

```
.plt.got
.plt.sec
.text
.fini
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
.dynamic
.data
.bss
.comment
```

以下の点が文字列として定義されているのではないかと仮定しする。

```
dmac_ps
asdf1234
true_pas
pass_kit
linux_maH
c_windowH
print_pa
KitKitKiH
tKitKitKH
```

これを一つずつ入力し、確認するとフラグを確認することができます。

1.3 フラグ

htp-ctf{dmac_ps} 元ネタは Dennis Ritchie のパスワードである、dmac より。

Input Correct Password

問題の意図

バイナリファイルから平文で保存がされているパスワードの文字列を抜き出してもらう。

解法

stringsコマンドで文字列を抽出し、怪しい文字列をすべて確認する。

解説

プログラム内には複数(7個)のパスワードを配列として隠してあった、それを全部試すと成功する。