群聊精华 2021.7.27-2021.8.1

@haya问：密码喷洒的密码，感觉字典是个大问题，大家有不错的这种强弱口令字典吗?

@wywwzjj：

- https://github.com/r35tart/RW_Password

@L.N.:

- https://github.com/berzerk0/Probable-Wordlists
- https://github.com/kaonashi-passwords/Kaonashi

@haya：

- https://github.com/L-codes/pwcrack-framework

@山顶洞小霸王

- Windows下net accounts 命令可以查密码策略

@Astartes

- 密码喷洒可以被设备监控到吧，基本上不到最后一步不用这个，内网搜集搜集信息做个密码本加上姓名+符合规则的弱口令。剩下的看运气了。

@大海问：cs自带的portscan扫描一个C段，段的每个ip都开启了110,25,143端口，很明显不正常，各位前辈们有遇到过这种情况吗?

@Breezy：

- 25和110 我本机如果开了火绒就会扫出来
- 不是说 本机开了火绒我就监听到了25和110 是通过火绒出口 不管扫什么 都会有25和110端口

@Se7en问：师傅们，工作组环境在一个08r2上我smbexe登陆成功用的hash是8bxxx， lsass内存里抓出来administrator的hash是0a5cxxxx(找不到8bxxx)，而且这个机器抓到的有个用户的ntlm有三个，这是什么情况

@skrskrt：

- 缓存的有可能是历史密码，正常

@L.N.:

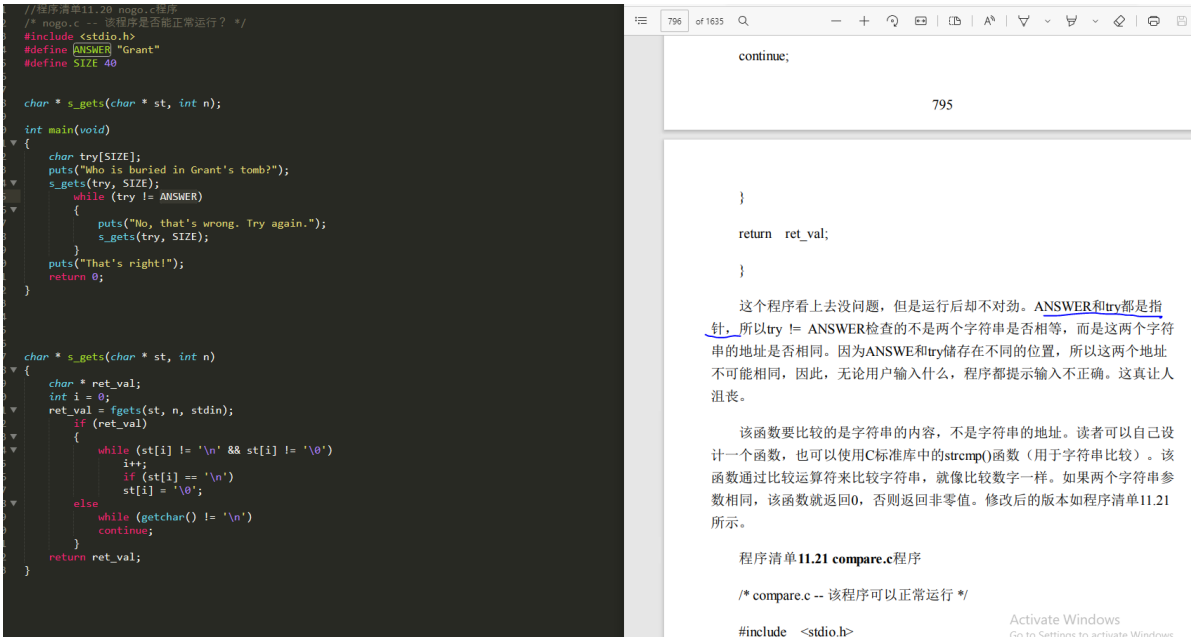
- 改密码了 一直没注销 关机过

@路人甲问：师傅们，请问有无linux下比较好用的后门，主要是要简单安全还有持续化。

@tomato答：

- pupy

@大海问：各位师傅你们好，晚辈请教一个概念问题，书中(c primer plus) 里说:ANSWER和try都是指针，我的疑问: ANSWER 不是常量吗？ try字符串吗？， 指针的申明不应该是 *吗？ 为什么说ANSWER和try都是指针



```c
//程序清单11.20 nogo.c程序
/* nogo.c -- 该程序是否能正常运行？ */
#include <stdio.h>
#define ANSWER "Grant"
#define SIZE 40

char * s_gets(char * st, int n);

int main(void)
{
    char try[SIZE];
    puts("Who is buried in Grant's tomb?");
    s_gets(try, SIZE);
        while (try != ANSWER)
        {
            puts("No, that's wrong. Try again.");
            s_gets(try, SIZE);
        }
    puts("That's right!");
    return 0;
}



char * s_gets(char * st, int n)
{
    char * ret_val;
    int i = 0;
    ret_val = fgets(st, n, stdin);
        if (ret_val)
        {
            while (st[i] != '\n' && st[i] != '\0')
                i++;
            if (st[i] == '\n')
            st[i] = '\0';
        else
            while (getchar() != '\n')
            continue;
        }
    return ret_val;
}
```

796 of 1635

continue;

795

}

return ret_val;

}

这个程序看上去没问题，但是运行后却不对劲。ANSWER和try都是指针，所以try != ANSWER检查的不是两个字符串是否相等，而是这两个字符串的地址是否相同。因为ANSWE和try储存在不同的位置，所以这两个地址不可能相同，因此，无论用户输入什么，程序都提示输入不正确。这真让人沮丧。

该函数要比较的是字符串的内容，不是字符串的地址。读者可以自己设计一个函数，也可以使用C标准库中的strcmp()函数（用于字符串比较）。该函数通过比较运算符来比较字符串，就像比较数字一样。如果两个字符串参数相同，该函数就返回0，否则返回非零值。修改后的版本如程序清单11.21所示。

程序清单**11.21 compare.c**程序

/* compare.c -- 该程序可以正常运行 */

#include <stdio.h>

@Astartes

- ANSWER 近似于 static const char* ANSWER = "Grant";
- 你进去调调就知道了，预处理的时候 define 定义的就都被替换了。

@skrtskrt

- #define ANSWER "Grant" 近似于 static const char* ANSWER = "Grant";

@L.N.

- 以前学c到指针的时候，老是搞不懂，后来学了内存相关知识，很多一下子就明白了，建议学指针之前可以看点内存相关知识，我看的是深入理解 c指针

@Hanamaki

- 1.用!=比较两个字符串是比较首地址 2.数组名大多数时候隐式转换成指向首元素的指针类型右值

@任我飞渡问：各位大佬，windows 有没有能跨用户session下键盘钩子的办法

L.N.答：

- CS是注入到指定用户的explorer.exe，然后开启键盘记录

@任我飞度：

- 搞定了，注入进程被杀，写个目标用户启动的计划任务。

@B1ngDa0

- 搞个system权限的就可以注入，system注入目标用户

@skrtskrt

- dll 也可以做键盘记录，用rundll 32 去启，而且不一定要用钩子。

@山顶小霸王

- dll还是exe，还有用什么去启跟键盘记录没啥必然的联系吧
  或者你想表达的是可信的进程去启动

@skrtskrt

- 对，https://blog.csdn.net/zhou191954/article/details/43309707

@Patrilic

- https://blog.csdn.net/sinat_24229853/article/details/47046581

@lengyi

- https://eyeofrablog.wordpress.com/2017/06/11/windows-keylogger-part-1-attack-on-user-land/
