UNIUNEA EUROPEANĂ

GUVERNUL ROMÂNIEI

Instrumente Structurale
2007-2013

Platformă de e-learning și curriculă e-content pentru învățământul superior tehnic

Sisteme de operare

35. Securitatea în Linux

chroot

- Modifică directorul rădăcină asociat procesului.
  - nu se poate accesa un director/fișier din afara ierarhiei impuse de noul director rădăcină
  - `chroot jail`
- Comanda chroot
- Apelul chroot
  - `chroot("/var/spool/postfix");`

Capabilities

- O cheie asociată unor acțiuni privilegiate sau unor drepturi de acces[4]
- Pot fi interschimbate între entități
  - nu este un lucru obișnuit în sistemele de operare actuale
- Capabilități POSIX (IEEE 1003.1e)
  - `CAP_NET_BIND_SERVICE`
  - `CAP_SYS_CHROOT`
  - `CAP_NET_RAW`
- `man 7 capabilities`

setuid/setgid

- Real user ID
- Effective user ID
- Bitul `setuid` (`chmod 4777`)
  - permite configurarea euid ca utilizatorul ce deține executabilul
- `setuid`
  - total privilege revocation (real user ID, effective user ID)
- `seteuid`
  - temporary privilege revocation (effective user ID)

main() în ping.c

```
int
main(int argc, char **argv) {
   struct hostent *hp;
   int ch, hold, packlen;
   int socket_errno;
   u_char *packet;
   char *target, hnamebuf[MAXHOSTNAMELEN];
   char rspace[3 + 4 * NROUTES + 1]; /* record route space */

   icmp_sock = socket(AF_INET, SOCK_RAW, IPPROTO_ICMP);
   socket_errno = errno;

   uid = getuid();
   if (setuid(uid)) {
         perror("ping: setuid");
         exit(-1);
   }
[...]
```

/etc/passwd + /etc/shadow

- /etc/passwd
  - user:password_hash:uid:gid:...
  - problemă
    - accesul utilizatorilor (nevoie de informații diferite de password_hash)
- /etc/shadow
  - user:password_hash:...
  - security enforcing
    - număr de zile între schimbat parola
    - număr de zile după care contul este dezactivat
    - ....

Password hash în Unix

- `man 3 crypt`
- Implicit DES
- `$id$salt$encrypted`
- `ID: 1 (MD5), 2a (Blowfish), 5 (SHA-256), 6 (SHA-512)`
- salt este folosit pentru a adăuga un nivel suplimentar de criptare a parolei
  - un salt pe 12 biți înseamnă 4096 de posibilități de criptare
  - un hash este bun dacă sunt greu de generat "coliziuni"
    - md5 nu mai este considerat chiar atat de sigur ..
    - http://www.crunchgear.com/2008/12/30/md5-collision-creates-rogue-certificate-authority/

Debian OpenSSL bug

- Apărut din 17 septembrie 2006[10]
- Cum?
  - test Valgrind peste OpenSSL
    - unitialized memory
  - Decizie
    - ștergerea a două linii de cod
    - o linie importantă pentru entropia de numere aleatoare (RNG)
- Testare cu ssh-vulnkey sau dowkd.pl

Debian Security Advisories

- [06 May 2011] DSA-2232 exim4 - format string vulnerability
- [06 May 2011] DSA-2231 otrs2 - cross-site scripting
- [01 May 2011] DSA-2230 qemu-kvm - several vulnerabilities
- [01 May 2011] DSA-2229 spip - programming error
- [01 May 2011] DSA-2228 iceweasel - several vulnerabilities
- [30 Apr 2011] DSA-2227 iceape - several vulnerabilities
- [26 Apr 2011] DSA-2226 libmodplug - buffer overflow
- [25 Apr 2011] DSA-2225 asterisk - several vulnerabilities
- [20 Apr 2011] DSA-2224 openjdk-6 - several vulnerabilities
- [20 Apr 2011] DSA-2223 doctrine - SQL injection
- [20 Apr 2011] DSA-2222 tinyproxy - incorrect ACL processing
- [19 Apr 2011] DSA-2221 libmojolicious-perl - directory traversal
- [19 Apr 2011] DSA-2220 request-tracker3.6, request-tracker3.8 - several vulnerabilities

PaX

- Patch pentru nucleul Linux[18]
- Principiul celui mai mic privilegiu pentru paginile de memorie
  - memoria de date marcată non-executabilă
  - memoria de cod marcată non-writable
- Prevenire execuție de cod arbitrară (shellcode)

ASLR

- Address space layout randomization[19]
- Rearanjare zone de cod/date
- Reducere probabilitatea „return-to-libc attack”
  - nu se suprascrie cod pe stivă
  - se apelează funcții existente (system(3))
- În Linux, integrat în PaX
- Windows Vista, Server 2008
- OpenBSD

W^X

- OpenBSD[20]
- Nici o pagină din spațiul de adresă al unui proces nu poate fi simultan scrisă sau executată
- Previne stack overflow
- Similar cu PaX și ExecShield
- Bitul NX (No eXecute) poate facilita implementarea[21]

Protejare la buffer overflow

- Stack Guard
- Stack Smashing Protection (ProPolice)[22]
- /GS la MS VS
- Se modifică organizarea unui stack frame
- Se folosește o “canary value”
  - plasată între buffer și control data (return address)
- Suprascrierea canary value = overflow

Stack Smashing Protection (GCC)

```
#include <stdio.h>
#include <string.h>

#define TEST_STRING "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa"

int main(void)
{
        char a[10];
        memcpy(a, TEST_STRING, strlen(TEST_STRING));
        return 0;
}

razvan@valhalla:~/code/stack_smash$ gcc -fstack-protector test.c
razvan@valhalla:~/code/stack_smash$ ./a.out
*** stack smashing detected ***: ./a.out terminated
======= Backtrace: =========
/lib/libc.so.6(__fortify_fail+0x37)[0x7f8a3021eaf7]
/lib/libc.so.6(__fortify_fail+0x0)[0x7f8a3021eac0]
[...]
```

Stack Smashing Protection (GCC) (2)

- Începând cu GCC 4.1

```
razvan@valhalla:~/code/stack_smash$ gcc -fstack-protector -S test.c
razvan@valhalla:~/code/stack_smash$ cat test.s
        [...]
        movq %fs:40, %rax
        movq %rax, -8(%rbp)
        [...]
        movq -8(%rbp), %rdx
        xorq %fs:40, %rdx
        je .L3
        call __stack_chk_fail
.L3:
        [...]
```

vmsplice bug

- Linux kernel 2.6.17-2.6.24.1
- 11 februarie 2008
- Combinație de integer overflow și buffer overflow în subsistemul de memory management al nucleului
- http://www.milw0rm.com/exploits/5092