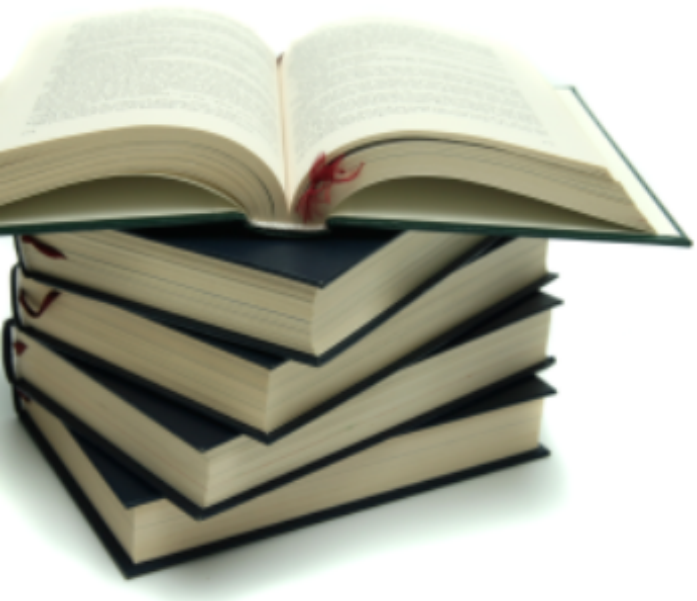
page crunch

Cursul 12



12

Securitatea sistemelor de operare

7 mai 2012 - 13 mai 2012

- OSC
  - Capitolul 14 Protection
  - Capitolul 15 Security
    - Secțiunile 15.1, 15.2, 15.5
- MOS
  - Capitolul 9 Security
    - Secțiunile 9.4, 9.6

Cuprins

- Principii de securitate [1]
- Cel mai mic privilegiu
- Drepturi pe fișiere
- Autentificarea utilizatorilor
- Vulnerabilitatea aplicațiilor
- Mecanisme de protecție

Non-cuprins

- Securitatea rețelei
- Atacuri de rețea: scanare, recunoaștere, DoS, man in the middle, sniffing
- Firewalls
- Criptare
- Politici de securitate
- Încredere (trust, chain of trust)
- Social engineering, honey pots

Principii de securitate

- Principiul celui mai mic privilegiu
- Cât mai puține caracteristici (feature creep)
- Controlul accesului
- Autentificare/autorizare
- Securizare (criptare)
- Defense in depth
- Risk management
- **Sistemul trebuie să rămână utilizabil**
  - Un sistem de securitate prea complicat va fi utilizat greșit => se obține efectul invers

Least privilege

- Accesarea doar a acelor resurse/date necesare
- Aplicat la utilizatori, procese
- Privilege escalation
- Privilege separation
- Privilege revocation
- Sandboxing

Kernel-mode

- Instrucțiunile privilegiate sunt executate în spațiul kernel
  - accesul la I/O
  - alocarea de resurse
  - handler-ele de întrerupere
  - gestiunea sistemului
- Suportul procesorului
  - niveluri de privilegiu (rings)[2]
  - x86: nivelul 0 (kernel), nivelul 3 (user)

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[3]
- 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[5]
  - 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);
        }
[...]
```

Drepturi pe fișiere

- Asocierea drepturilor de acces pentru utilizatori la fișiere[6]
- Citire, scriere, ștergere, execuție
- Creare fișier, listare, ștergere fișier, parcurgere

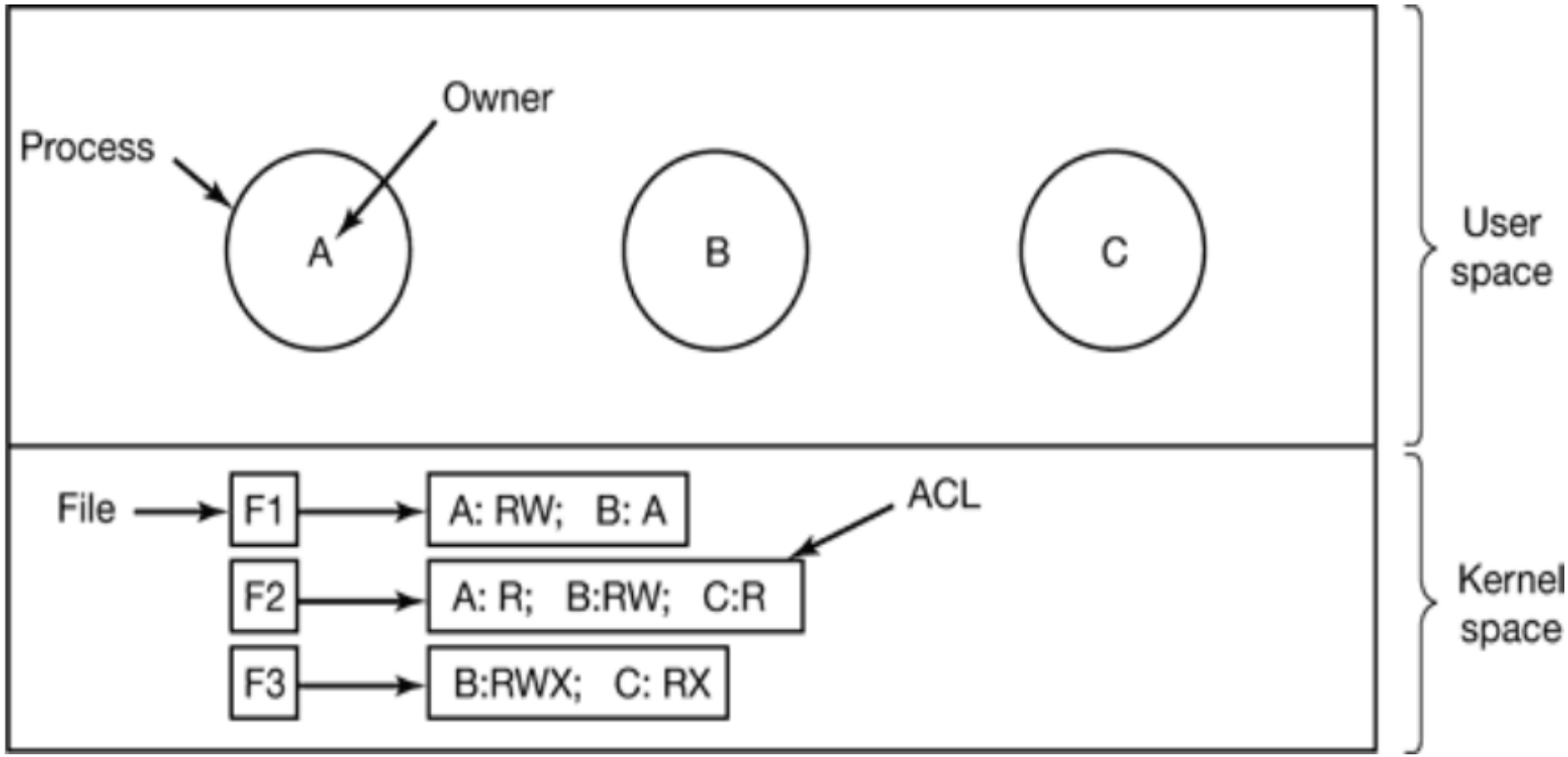
Matrice de acces

Domain	File1	File2	File3	File4	File5	File6	Printer1	Plotter2
1	Read	Read Write						
2			Read	Read Write Execute	Read Write		Write	
3						Read Write Execute	Write	Write

Drepturi pe fișiere în Unix

- Matrice de acces
- Domeniile sunt
  - utilizator (user) - deținătorul fișierului
  - grup (group) grupul deținător al fișierului
  - alții (others)
- Drepturi
  - read (r) citire, listare
  - write (w) scriere, creare fișier
  - execute (x) execuție, parcurgere

Liste de acces



Liste de acces (2)

- POSIX ACL[7]
  - implementate pe sisteme de fișiere Linux cu extended attributes
  - getfacl, setfacl
- Drepturi pe fișiere în Windows[8]
  - ACL pe NTFS
  - read, write, list, read and execute, modify, full control
- Role-based access control (RBAC)
  - sudo

Autentificarea utilizatorilor

- Accesul utilizatorilor în sistem
- Parolă
- Cheie publică
- Voice recognition, identificatori biometrici

/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[9]
- Implicit DES
- idsalt$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/

Autentificarea prin chei publice

- Cheie publică + cheie privată
- Cheia publică este pe sistem (server)
- Cheia privată este folosită pentru autentificare
- Legătură matematică
  - one way function
  - defapt este two-way, insa nu este computațional fezabil să se calculeze inversul funcției (încă..)
- RSA, DSA

Debian OpenSSL bug

- Apărut in 2006[10], descoperit prin 2008[10a]
- 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

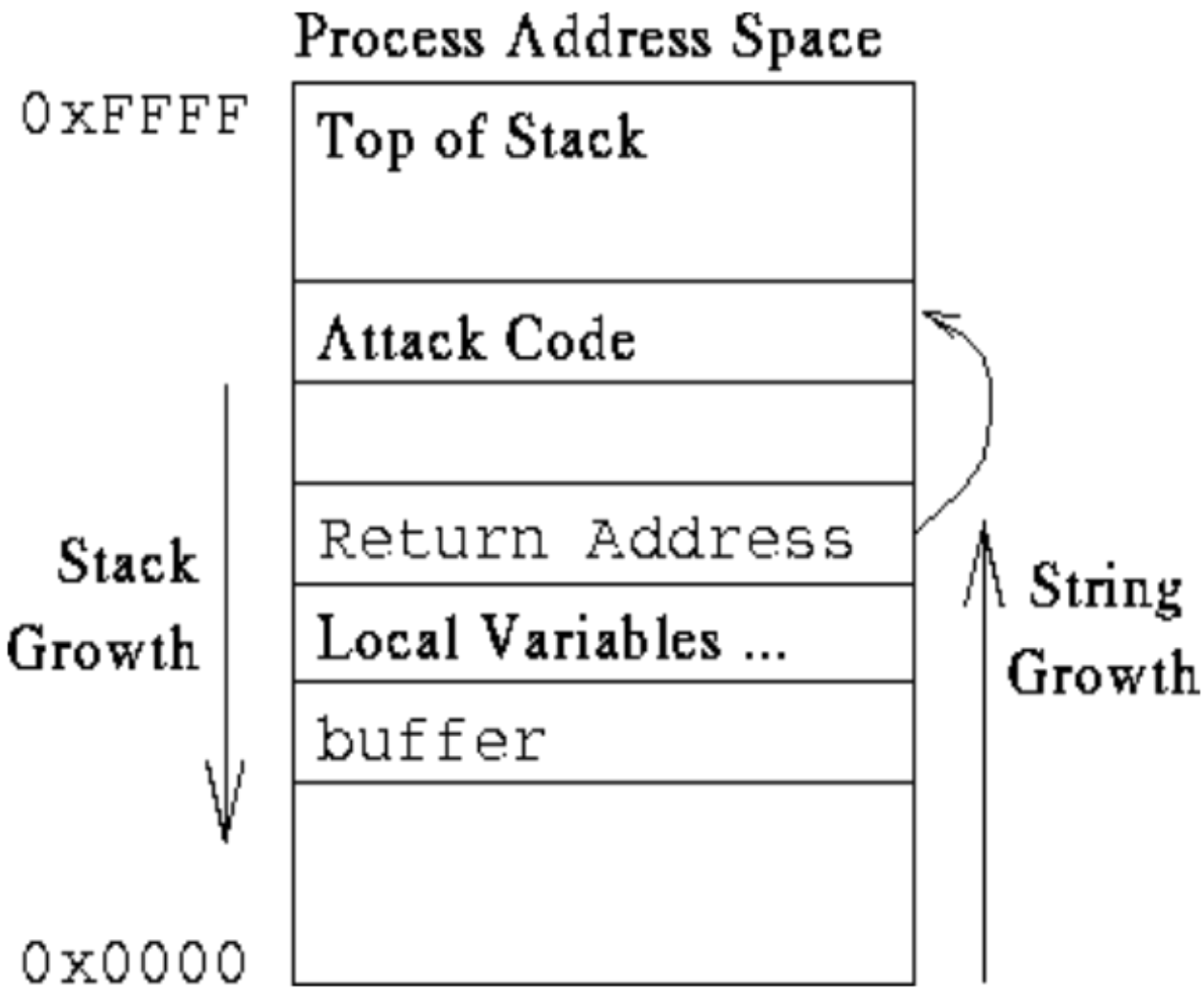
OTP

- One Time Password[11]
- Time-synchronized OTP
  - RSA SecurID
- Algoritm matematic
  - s initial seed
  - f one-way function
    - cryptographic hash function
      - it is easy to compute the hash value for any given message,
      - it is infeasible to find a message that has a given hash,
      - it is infeasible to modify a message without changing its hash,
      - it is infeasible to find two different messages with the same hash.
  - f(f(f(f(...f(s)...))), ..., f(s)

Debian Security Advisories

[04 May 2012] DSA-2459 quagga - several vulnerabilities
[03 May 2012] DSA-2462 imagemagick - several vulnerabilities
[02 May 2012] DSA-2464 icedove - several vulnerabilities
[02 May 2012] DSA-2463 samba - missing permission checks
[26 Apr 2012] DSA-2461 spip - several vulnerabilities
[25 Apr 2012] DSA-2460 asterisk - several vulnerabilities
[24 Apr 2012] DSA-2458 iceape - several vulnerabilities
[24 Apr 2012] DSA-2457 iceweasel - several vulnerabilities
[24 Apr 2012] DSA-2454 openssl - multiple vulnerabilities
[23 Apr 2012] DSA-2456 dropbear - use after free
[20 Apr 2012] DSA-2455 typo3-src - missing input sanitization

stack/buffer overflow



stack/buffer overflow (2)

- Un apel de funcție înseamnă crearea unui stack frame pe stivă
  - parametrii funcției
  - adresa de retur
  - registre salvate
- Se citește într-un buffer mai mult decât dimensiunea sa
- Organizarea stivei permite suprascrierea adresei de retur[12][13]
- Se rulează codul atacatorului

Shellcode

- Se face salt de obicei chiar în buffer[14]
- Buffer-ul este completat cu instrucțiuni de atac
- Shellcode
  - codul este folosit pentru deschiderea unui shell
  - codificat în limbaj de asamblare
  - de obicei se încearcă exploatarea unui program cu bitul setuid activat

Shellcode (2)

```
char shellcode[] =
                    // setuid(0);
    "\x31\xdb"        // xorl %ebx,%ebx
    "\x8d\x43\x17"    // leal 0x17(%ebx),%eax
    "\xcd\x80"        // int $0x80
                    // exec('/bin/sh');
    "\x31\xd2"        // xorl %edx,%edx
    "\x52"           // pushl %edx
    "\x68\x6e\x2f\x73\x68" // pushl $0x68732f6e
    "\x68\x2f\x2f\x62\x69" // pushl $0x69622f2f
    "\x89\xe3"        // movl %esp,%ebx
    "\x52"           // pushl %edx
    "\x53"           // pushl %ebx
    "\x89\xe1"        // movl %esp,%ecx
    "\xb0\x0b"        // movb $0xb,%al
    "\xcd\x80";       // int $0x80
```

Funcții de lucru pe șiruri

- EVIL :-)[15]
- gets
  - man pages: ‴Never use gets`
  - alternativa fgets
- strcpy, strcat
  - pot conduce la buffer overflow
  - trebuie știută dimensiunea șirului
- strtok, strsep
  - modifică șirul inițial
- din păcate, din cauza static linking-ului, aceste funcții trebuiesc păstrate pt. backwards compatibility

Funcții de lucru pe șiruri (2)

- Trebuie știută dimensiunea șirului
  - se poate folosi memcpy, memchr
- strncpy, strncat
  - ineficiente (dacă se cunoaște dimensiunea șirului)
  - nu se adaugă automat null terminatorul
- strcpy_s, strcat_s
  - se transmite dimensiunea șirului destinație
  - eșuează dacă șirul destinație nu este suficient de mare

Funcții de lucru pe șiruri (3)

- strlcat, strlcpy[16][17]
  - introduse în OpenBSD și NetBSD
  - neacceptate în glibc
  - versiuni îmbunătățite ale strncpy, strncat

```
if (strlcpy(dest, source, dest_len) >= dest_len)
        err(1, "String too long");
```

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:
        [...]
```

Integer overflow

- O operație aritmetică depășește spațiul alocat unui tip de date
  - 8 biți 255
  - 16 biți 65535
- Unexpected behavior
- Pentru întregi cu semn
  - poate lua valoare negativă (nu mai poate fi folosit ca index)
- Poate conduce la buffer overflow[23]

signed/unsigned comparison [24]

```
int a = -1;
unsigned int b = 20;
if (a < b) {
        /* expected behavior */
}
else {
        /* unexpected behavior */
}
```

Backdoor

- Security bypass
  - se trece de lanțul de securitate folosind o funcționalitate existentă a aplicației
- Benign backdoor easter eggs
- Mulți viruși/viermi instalează un backdoor pe sistem
- Symmetric backdoor
  - utilizabilă de oricine
- Asymmetric backdoor
  - utilizabilă doar de implementator

Backdoor (2)

- Ken Thompson Reflections on trusting trust[25]
- Modificarea codului programului login
  - utilizatorul ken primea acces privilegiat în sistem
- Modificarea codului compilatorului (folosit pentru a compila login)
- Modificarea compilatorului la compilare
- Se putea modifica și dezasamblorul
  - nu se putea detecta nici prin inspecția codului mașină

Rootkit

- Program destinat obținerii accesului privilegiat la sistem[26]
- Programul își ascunde prezența
- La nivel de nucleu module de kernel
- La nivel de bibliotecă hook-uri, înlocuire de apeluri de sistem
- Un sistem compromis de obicei va fi reinstalat (cost ridicat pentru ‴reparare`)

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

Resurse utile

- Organizații de securitate
  - http://secunia.com/
  - http://www.sans.org/
  - http://www.cert.org/
- Site-uri de vulnerabilități
  - http://www.metasploit.com
  - http://www.milw0rm.com/
  - http://osvdb.org/
- Site-uri cu articole de securitate
  - http://insecure.org/
  - http://www.phrack.com/

Cuvinte cheie

- least privilege
- kernel-mode/user-mode
- setuid
- matrice de acces
- ACL
- /etc/passwd, /etc/shadow
- buffer overflow
- shellcode
- PaX
- W^X
- stackGuard/ProPolice
- integer overflow
- backdoor
- rootkit

Exerciții

- Explicați cum se poate produce un atac de tipul stack overrun pe un sistem în care stiva crește în sus.[27]

- Cum se pot preveni atacuri return-to-libc folosind flag-ul NX?

- De ce următoarea funcție nu este recomandată pentru generarea de parole de tip one-time (OTP)?

```
unsigned long otp_fun(unsigned long x)
{
        return (x * x * x);
}
```

Întrebări