Bezpieczeństwo oprogramowania - lab 3

Zadanie 1

vim

Minimalne:

- execve
- brk
- arch_prctl
- access
- openat
- fstat
- stat
- mmap
- close
- read
- pread64
- mprotect
- munmap
- set_tid_address
- set_robust_list
- write
- select
- chdir

Zalecane:

- linux-vdso.so.1
- libm.so.6
- libtinfo.so.6
- libselinux.so.1
- libcanberra.so.0
- libacl.so.1
- libgpm.so.2
- libdl.so.2

- libpython3.8.so.1.0
- libpthread.so.0
- libc.so.6
- libpcre2-8.so.0
- libvorbisfile.so.3
- libtdb.so.1
- libltdl.so.7
- libexpat.so.1
- libz.so.1
- libutil.so.1
- libvorbis.so.0
- libogg.so.0

gcc

Minimalne:

- execve
- brk
- arch_prctl
- access
- openat
- fstat
- stat
- lstat
- readlink
- mmap
- close
- read
- write
- pread64
- mprotect
- ioctl
- rt_sigaction
- prlimit64

Zalecane:

- linux-vdso.so.1
- libc.so.6
- lib64/ld-linux-x86-64.so.2

passwd

Minimalne:

- execve
- brk
- arch_prctl
- access
- openat
- fstat
- mmap
- read
- pread64
- close
- mprotect
- arch_prctl
- set_tid_address
- set_robust_list
- rt_sigaction
- getuid
- socket
- connect
- lseek
- prlimit64

Zalecane:

- linux-vdso.so.1
- libpam.so.0
- libpam_misc.so.0
- libaudit.so.1
- libselinux.so.1
- libc.so.6
- libdl.so.2
- libcap-ng.so.0
- libpcre2-8.so.0
- lib64/ld-linux-x86-64.so.2
- libpthread.so.0

Ping

Minimalne:

- execve
- brk
- arch_prctl

- access
- openat
- fstat
- mmap
- close
- read
- pread64
- mprotect
- prctl
- getuid
- setuid
- write
- exit_group

Zalecane:

- linux-vdso.so.1
- libcap.so.2
- libgcrypt.so.20
- libresolv.so.2
- libc.so.6
- libgpg-error.so.0
- lib64/ld-linux-x86-64.so.2

Zadanie 2

Plik polityki AppArmor dla aplikacji `tcpdump`

```
#include <tunables/global>

/usr/sbin/tcpdump {
  #include <abstractions/base>
  #include <abstractions/nameservice>
  #include <abstractions/user-tmp>

  capability net_raw,
  capability setuid,
  capability setgid,
  capability dac_override,
  network raw,
  network packet,

  # for -D
  capability sys_module,
```

```
  @{PROC}/bus/usb/ r,
  @{PROC}/bus/usb/** r,

  # for -F and -w
  audit deny @{HOME}/.* mrwkl,
  audit deny @{HOME}/.*/ rw,
  audit deny @{HOME}/.*/** mrwkl,
  audit deny @{HOME}/bin/ rw,
  audit deny @{HOME}/bin/** mrwkl,
  @{HOME}/ r,
  @{HOME}/** rw,

  /usr/sbin/tcpdump r,
}
```

Zadanie 4

Plik polityki Grsecurity zabezpieczający przed nieuprzywilejowanym kontem sshd:

```
role sshd u
   subject /
      /  h
      /var/run/sshd r
      -CAP_ALL
      bind disabled
      connect disabled
```

Zadanie 5

	AppArmor	SELinux	Grsecurity
Możliwości	łatwy deployment, narzędzia GUI i CLI, szeroki wachlarz alertów	narzędzia GUI i CLI, jasna separacja polityk od wzmocnień, dobrze zdefiniowane interfejsy polityk, niezależne od języków politych, cache'owanie, dobra dokumentacja	system oparty na rolach, uniemożliwia uruchomienie samowolnego kodu na poziomie jądra, redukuje ryzyko wycieku przez błędy jądra, szeroki wachlarz alertów zawierających adres IP osoby wywołującej alert
Wydajność	wysoka	wysoka	
Łatwość konfiguracji	średnia	niska	wysoka