grsecurity

sicurezza in kernelspace

night@freaknet.org

Qualche info su di noi

- Freaknet Medialab: chi siamo?
- Chi sono?
- Perche’ questo seminario?

Approccio alla sicurezza

- Security cannot be solved in a single layer
- Additional security, if not user friendly, is useless
- You should be able to protect any third-party software you have installed, not only the software that is provided by your distribution
- Humans are often the weakest link in security

ref: (http://www.grsecurity.org/quickstart.pdf)

Versioning

- 2.1.8 per kernel 2.6.14.6
- 2.1.8 per kernel 2.4.32

Installazione

```
tar jxvf linux-x.x.x.tar.bz2
cd linux-x.x.x
patch -p0 < grsecurity-x.x.x
make menuconfig
```

Features

- PaX (http://pax.grsecurity.net)
- Chroot restrictions
- Auditing
- RBAC (Role Based Access Control)

PaX

- Obiettivo: evitare i bug che, modificando l'address space del processo, cambiano il flusso del programma
  - Esempio: [stack|heap] buffer overflow
  - Esempio: format string bug
- Modi di cambiare il flusso di esecuzione:
  - introduzione di codice arbitrario
  - esecuzione di codice esterno al programma

PaX: features

- Non-executable pages
  - cfr: W^X, ExecShield
  - Prevenzione di buffer overflow elementari
- mmap/mprotect restrictions
- ASLR (Address Space Layout Randomization)

PaX:no-exec

- Il kernel vieta che le pagine di memoria allocate a un task siano marcate anche come eseguibili
- Impossibilita’ di scrivere shellcode in queste pagine di memoria
- Alcuni programmi possono risentirne (es: XFree86)
  - soluzione: chpax

PaX:mmap/mprotect

- La possibilita’ di non eseguire codice in pagine di memoria non evita tutti gli exploit ma solo una minima parte
- E’ ancora possibile utilizzare tecniche come il return-into-libc e crearsi pagine di memoria eseguibili su cui inserire il codice malevolo
- Questa restrizione vieta che mmap crei pagine eseguibili

(http://pax.grsecurity.net/docs/mprotect.txt)

PaX:ASLR (userspace)

- Address Space Layout Randomization
- Questa feature permette di randomizzare gli indirizzi dello stack e dell'heap del programma
- Vengono anche randomizzati gli indirizzi delle librerie dinamiche mappate in memoria (cfr ExecShield)
- Esiste anche una ASLR in kernelspace

PaX:ulteriori features

- Non e’ possibile scrivere sul kernel tramite /dev/mem, /dev/kmem, /dev/port
- abilitazione della segmentation
- disabilitato raw I/O
- modifiche al /proc filesystem (maps | stat)

Auditing

- granularita’ di auditing
  - mount
  - segnali
  - chdir
  - exec
  - …
- E’ possiible definire un gruppo su cui fare auditing

Randomization

- PID
- Entropy pool
- TCP ports

RBAC

- Role Based Access Control
- Perche’ i tradizionali permessi UNIX non sono sufficienti?
- Utilizzo delle capability
- Learning mode: esempio di policy file

Domande?

- Contatto: night@freaknet.org
- Piazzavirtuale: piazzavirtuale@freaknet.org (necessita iscrizione)
- A voce