Veronika Dudová

PaX

Co je PaX?

- Bezpečnostní záplata linuxového jádra
- Ochrana přístupu k paměti
- Nabízí:
  - podporu nespustitelných stránek
  - randomizaci adresního prostoru (ASLR)

Význam a omezení

- Označuje:
  - datovou paměť jako nespustitelnou
  - programovou paměť jako nezapisovatelnou a náhodně ji uspořádává
- Tím efektivně zabraňuje mnoha bezpečnostním exploitům, jako jsou např. některé druhy přetečení zásobníku
- Činí útoky return-to-libc (ret2libc) těžko zneužitelné
- Nepředchází variables a pointers overwriting

Podpora nespustitelných stránek

- Označit paměťové stránky jako nespustitelné
  - metadata stránek rozšířit o bit X (RW > RWX)
- Pokud do takové stránky umístí útočník svůj kód a pokusí se jej vykonat, procesor mu to nedovolí
- No-eXecute bit (NX) je do procesorů implementován od roku 2004
- Kde není, PaX ho dokáže SW emulovat

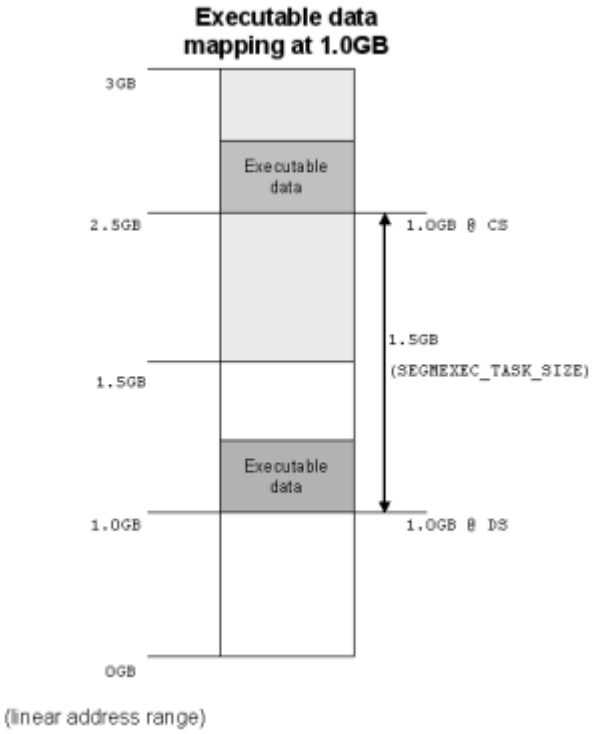
PAGEEXEC

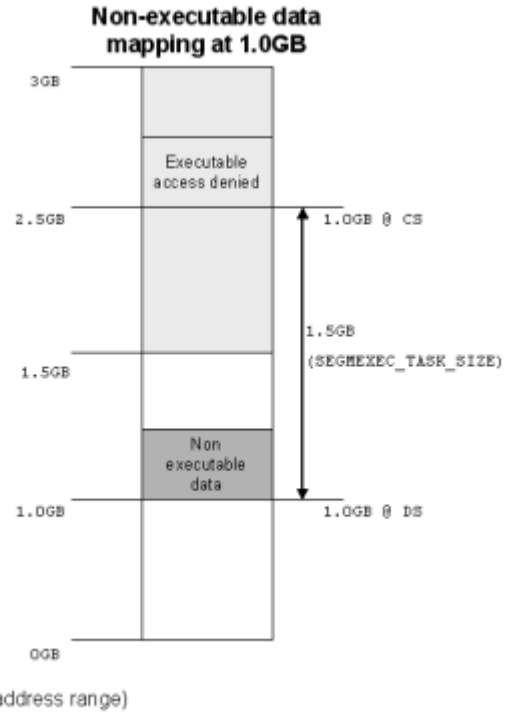
- Využívá nebo emuluje NX bit
- TLB jednotky - data (DTLB), instrukce (ITLB)
  - procesory Intel Pentium a výš, AMD Athlon/Duron
- Nastaví supervisor bit, při přístupu na stránku dojde k výpadku stránky
  - ITLB – ukončení procesu
  - DTLB – dočasné odstranění supervisor bitu, uložení hodnot do DTLB

SEGMEXEC (1)

- Segmentace: data segment, code segment
- Rozdělení adresního prostoru na polovinu, dolní pro data, horní pro code
- Zrcadlení virtuálního prostoru
  - duplikace každé spustitelné (executable) stránky v dolní polovině adresního prostoru do horní poloviny
- Instrukce chce přistoupit na adresy v datovém segmentu, které nemají žádný kód umístěný v jeho zrcadlené adrese → výpadek stránky, PaX ho obslouží a ukončí proces

SEGMEXEC (2)


Executable data mapping at 1.0GB
3GB
Executable data
2.5GB
1.0GB @ CS
1.5GB
(SEGMEXEC_TASK_SIZE)
1.5GB
Executable data
1.0GB
1.0GB @ DS
0GB
(linear address range)


Non-executable data mapping at 1.0GB
3GB
Executable access denied
2.5GB
1.0GB @ CS
1.5GB
(SEGMEXEC_TASK_SIZE)
1.5GB
Non executable data
1.0GB
1.0GB @ DS
0GB
(linear address range)

Omezení mprotec()

- Zabraňuje programům
  - změnit stav stránek paměti na spustitelné (executable), když tak nebyly vytvořeny
  - udělat ze spustitelných stránek určených jen ke čtení (read-only) zapisovatelné (writable)
  - vytvoření spustitelných stránek z anonymní paměti

Výhody a nevýhody

- PAGEEXEC
  - + velikost adresního prostoru aplikace nezměněna
  - - větší dopad na výkon (častější výpadky stránek)
- SEGMEXEC
  - + velmi nízký (téměř nulový) dopad na výkon
  - - omezení velikosti adresního prostoru aplikace
    - na 1,5 GB z původních 3 GB
- - nekompatibilita s některými aplikacemi
  - Java, wine

Randomizace adresního prostoru (ASLR)

- Proti útokům vyžadujícím znalost adresního prostoru (return-to-libc)
- Kód není na adresách, které předem známe
- Randomizace
  - Stack – 24 bits
  - Mmap – 16 bits
  - Executable – 16 bits
  - Heap – 12 bits (or 24 bits if executable is randomized also)
- PaX nabízí techniky RANDMMAP a RANDEXEC

ASLR - RANDMMAP

- Náhodný výběr 16 bitů adresy při hledání paměťového regionu pro systémové volání mmap()
- I randomizace základní adresy z programové hlavičky ELF binárního programu
- Velmi kvalitní ochrana ALE:
  - programy musí být kompilovány s dostatkem informací pro relokaci (ET_DYN)
  - většina programů je ET_EXEC, nutno znovu zkompilovat
- Distribuce Adamantix obsahuje ET_DYN programy standardně

ASLR - RANDEXEC

- Ochrana i pro ET_EXEC, ale není tak spolehlivá, může způsobit falešné poplachy
- Nahraje program na náhodnou adresu a zrcadlí na adresu původní
- Sleduje vazby mezi oběma částmi při pokusu o spuštění kódu – snaha detekovat netypické návratové adresy (normální vede do rand. části)
- Tento mechanismus není zapínán standardně
  - pomocí utility paxctl lze zapnout pro určené programy

Stav vývoje a podpora

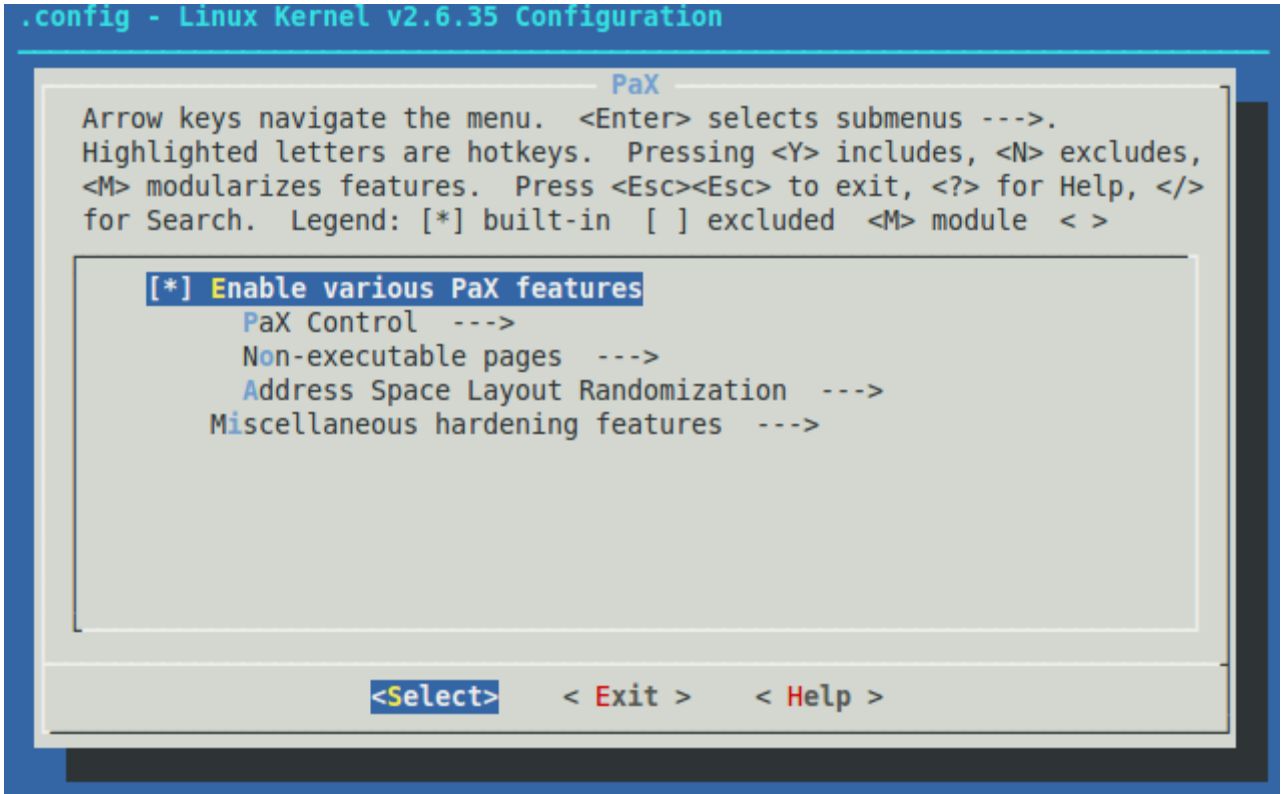
- Nejnovější verze
  - homepage: 2008, linux 2.6.27
  - grsecurity: 2010, linux 2.6.36
- PaX je součástí grsecurity
- V distribucích Adamantix (Trusted Debian), Hardened Gentoo
- V OpenBSD
- Kompatibilní s všemi distribucemi – nutný patch jádra

Patch jádra

- Stažení jádra a patche (pax.grsecurity.net)
- Aplikace patche
  - patch –p1 < pax-linux-2.6.36.patch
  - --dry-run
- **Konfigurace jádra (PaX)**
  - make menuconfig
- Kompilace jádra
- Instalace jádra

Konfigurace jádra

- Zajímá nás konfigurace PaX, nalezneme v Security Options → PaX



Konfigurace

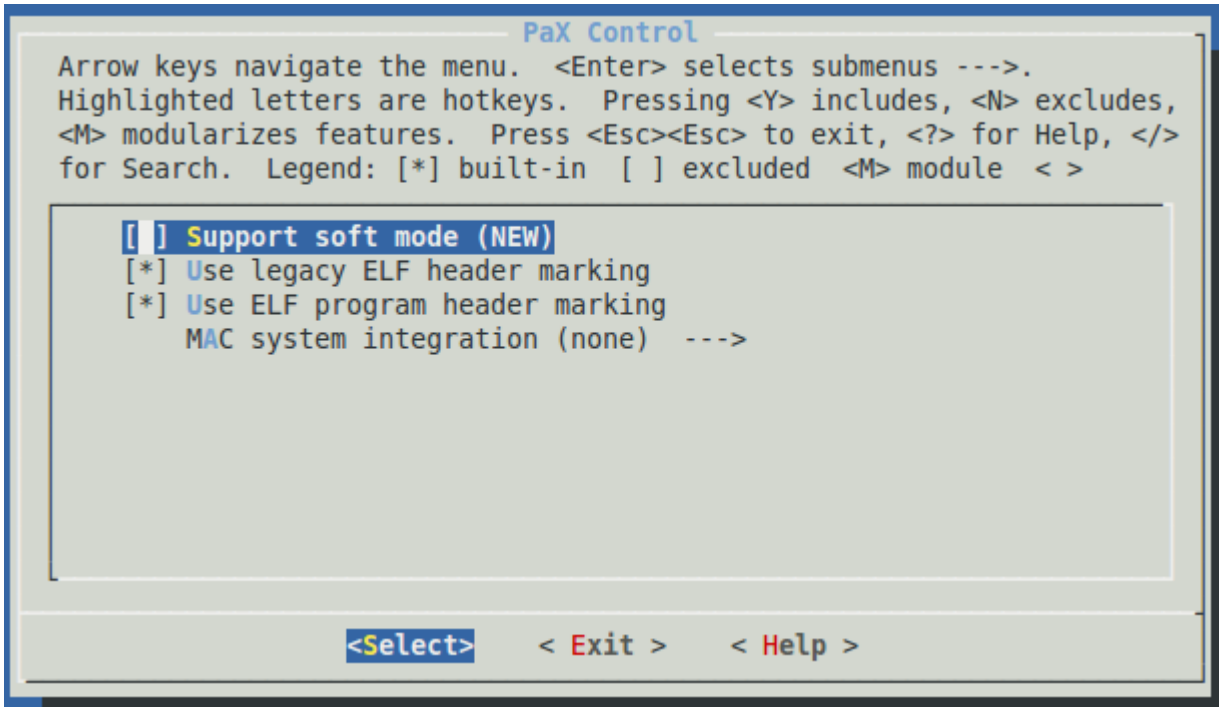
PaX Control

CONFIG_PAX_

SOFTMODE
- mechanismy nebudou defaultně používané
- musí se povolit PT_PAX_FLAGS

EI_PAX
- chpax
- deprecated

PT_PAX_FLAGS
- paxctl



Konfigurace

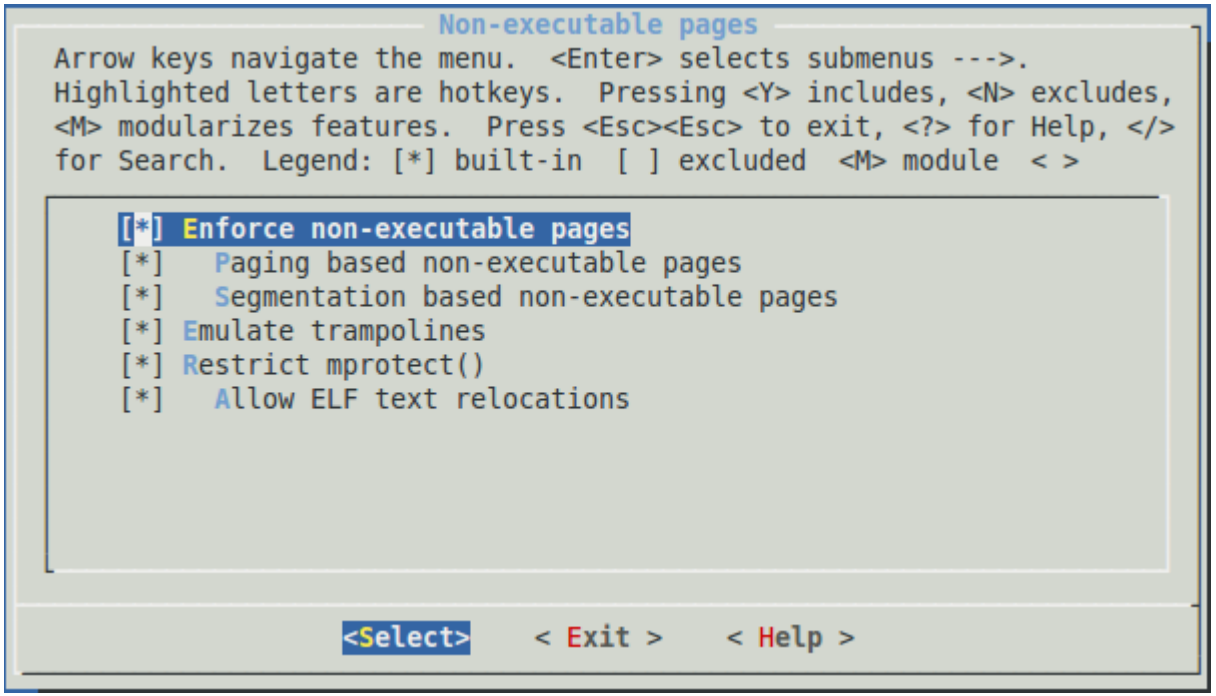
Non-executable pages

CONFIG_PAX_
NOEXEC
PAGEEXEC
SEGMEXEC

EMUTRAMP
- Y – paxctl, povolení trampolín u programů
- N – paxctl, vypnutí PAGEEXEC a SEGMEXEC

MPROTECT

ELFRELOCS
-N – když jen PIC ELF
- readelf –S (.rel.text)
- Allow x Disallow



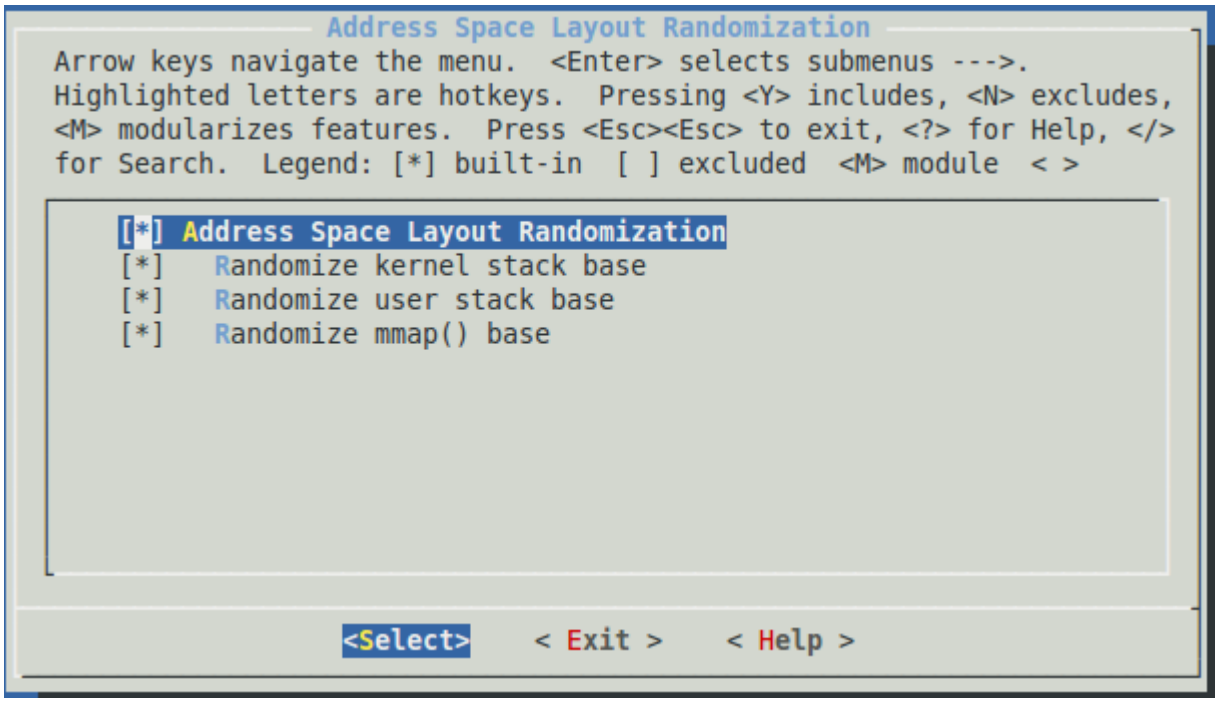
Konfigurace ASLR

CONFIG_PAX_

RANDKSTACK

RANDUSTACK
- ve 2 krocích
- druhý může udělat velký posun na vrcholu zásobníku → problém u programů které potřebují hodně paměti (víc jak 2.5GB nebo 1.25GB)
- paxctl

RANDMMAP



Konfigurace

MISCS

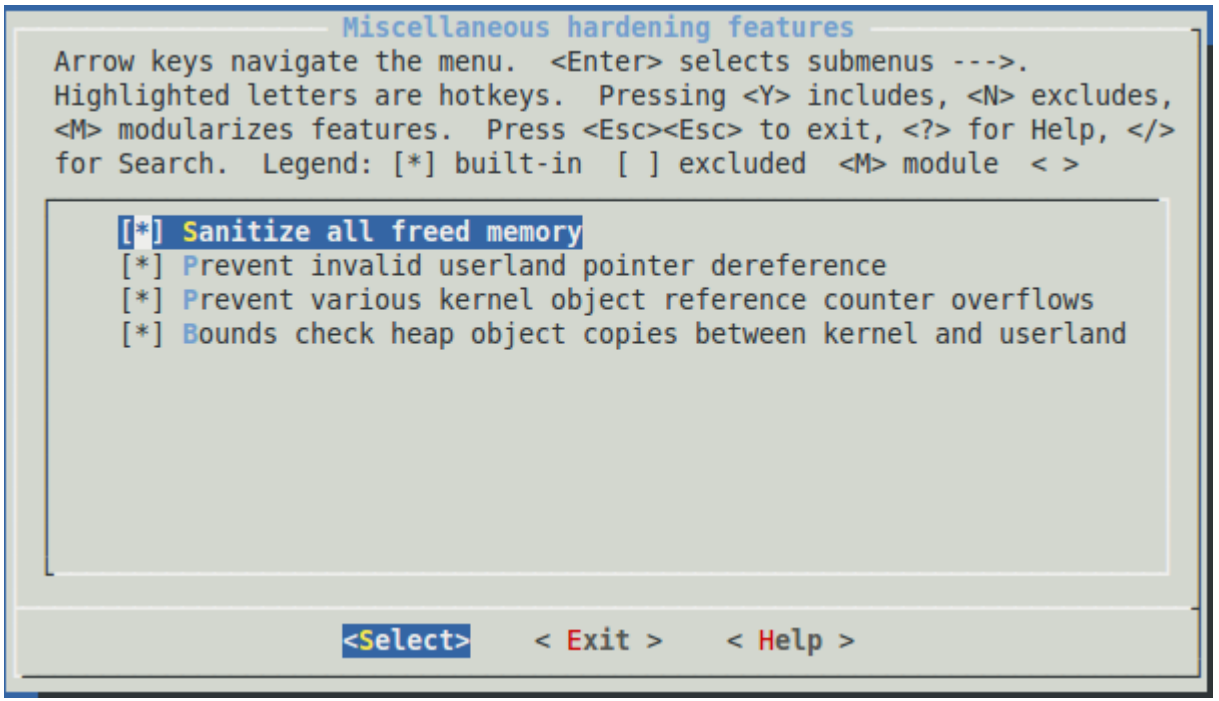
CONFIG_PAX_

MEMORY_SANITIZE
- vymazání stránek paměti jakmile jsou uvolněny
- dopad na výkon

MEMORY_UDEREF
- virtualizace - velké zpomalení

REFCOUNT
- memory leak

USERCOPY
- zanedbatelný dopad na výkon



Vlastní zkušenosti - Ubuntu

- Ubuntu 10.10 s jádrem 2.6.35
  - patch jádra – PaX
    - verze jádra a patche – 2.6.35.9, 2.6.36.1
      - previously applied patch detected: Assume –R?
    - konfigurace PaX (viz. předchozí)
    - kompilace OK, nabootování NE
  - patch jádra – grsecurity
    - jádro a patch 2.6.32
  - hotový balíček

Vlastní zkušenosti - Debian

- Debian 5.0 s jádrem 2.6.26
  - hotový balíček – obsahuje grsec 2.1.12
    - dep http://debian.cr0.org/repo/ kernel-security/
    - apt-get install linux-image-2.6.27.29-4-grsec
    - PaX – softmode, disable MPROTECT, pemRS
  - upravený balíček
    - linux-source-2.6.27.29-4-grsec
    - make menuconfig – upravit konfiguraci podle svého
    - kompilace, instalace

Utility (1)

- paxctl
  - disable/enable
    - PAGEEXEC (-p), EMUTRMAP (-e), MPROTECT (-m), RANDMMAP (-r), RANDEXEC (-x), SEGMEXEC (s)
  - view flags (-v)

```
debian:/home/veronika# paxctl -v test
PaX control v0.5
Copyright 2004,2005,2006,2007 PaX Team <pageexec@freemail.hu>

- PaX flags: -pS--mX--eR- [test]
        PAGEEXEC is disabled
        SEGMEXEC is enabled
        MPROTECT is disabled
        RANDEXEC is enabled
        EMUTRAMP is disabled
        RANDMMAP is enabled
```

  - File does not have a PT_PAX_FLAGS program header, try conversion (-c, -C)

Utility (2)

- pspax
  - součástí pax-utils
  - zobrazí ELF/PaX informace o běžících procesech

```
debian:/home/veronika# pspax
USER     PID    PAX    MAPS ETYPE      NAME            CAPS ATTR
root     1      pemRS  w^x  ET_EXEC    init            =ep cap_setpcap-e
root     965    pemRS  w^x  ET_EXEC    sh              =ep cap_setpcap-ep
root     967    pemRS  w^x  ET_EXEC    sh              =ep cap_setpcap-ep
root     1040   pemRS  w^x  ET_EXEC    file            =ep cap_setpcap-ep
root     1041   pemRS  w^x  ET_EXEC    pspax           =ep cap_setpcap-ep
```

- paxtest
  - otestování konfigurace PaX
  - pokus o spuštění kódu na zásobníku či datovém segmentu, pokus o simulaci return-to-libc útoku atd.

paxtest – Debian bez PaX

```
Mode: blackhat
Linux debian 2.6.26-2-686 #1 SMP Thu Nov 25 01:53:57 UTC 2010 i686 GNU/Linux

Executable anonymous mapping             : Vulnerable
Executable bss                           : Vulnerable
Executable data                          : Vulnerable
Executable heap                          : Vulnerable
Executable stack                         : Vulnerable
Executable anonymous mapping (mprotect)  : Vulnerable
Executable bss (mprotect)                : Vulnerable
Executable data (mprotect)               : Vulnerable
Executable heap (mprotect)               : Vulnerable
Executable shared library bss (mprotect) : Vulnerable
Executable shared library data (mprotect): Vulnerable
Executable stack (mprotect)              : Vulnerable
Anonymous mapping randomisation test     : 9 bits (guessed)
Heap randomisation test (ET_EXEC)        : 14 bits (guessed)
Heap randomisation test (ET_DYN)         : 16 bits (guessed)
Main executable randomisation (ET_EXEC)  : 10 bits (guessed)
Main executable randomisation (ET_DYN)   : 10 bits (guessed)
Shared library randomisation test        : 10 bits (guessed)
Stack randomisation test (SEGMEXEC)      : 19 bits (guessed)
Stack randomisation test (PAGEEXEC)      : 19 bits (guessed)
Return to function (strcpy)              : Vulnerable
Return to function (strcpy, RANDEXEC)    : Vulnerable
Return to function (memcpy)              : Vulnerable
Return to function (memcpy, RANDEXEC)    : Vulnerable
Executable shared library bss            : Vulnerable
Executable shared library data           : Killed
Writable text segments                   : Vulnerable
```

paxtest – Debian s PaX

```
Mode: blackhat
Linux debian 2.6.27.29-4-grsec #1 SMP Sun Aug 16 12:21:49 UTC 2009 i686 GNU/Linu
x

Executable anonymous mapping             : Killed
Executable bss                           : Killed
Executable data                          : Killed
Executable heap                          : Killed
Executable stack                         : Killed
Executable anonymous mapping (mprotect)  : Vulnerable
Executable bss (mprotect)                : Vulnerable
Executable data (mprotect)               : Vulnerable
Executable heap (mprotect)               : Vulnerable
Executable shared library bss (mprotect) : Vulnerable
Executable shared library data (mprotect): Vulnerable
Executable stack (mprotect)              : Vulnerable
Anonymous mapping randomisation test     : 17 bits (guessed)
Heap randomisation test (ET_EXEC)        : 13 bits (guessed)
Heap randomisation test (ET_DYN)         : 23 bits (guessed)
Main executable randomisation (ET_EXEC)  : 17 bits (guessed)
Main executable randomisation (ET_DYN)   : 17 bits (guessed)
Shared library randomisation test        : 17 bits (guessed)
Stack randomisation test (SEGMEXEC)      : 23 bits (guessed)
Stack randomisation test (PAGEEXEC)      : 23 bits (guessed)
Return to function (strcpy)              : Vulnerable
Return to function (strcpy, RANDEXEC)    : Vulnerable
Return to function (memcpy)              : Vulnerable
Return to function (memcpy, RANDEXEC)    : Vulnerable
Executable shared library bss            : Killed
Executable shared library data           : Killed
Writable text segments                   : Vulnerable
```

Shrnutí

- Kvalitní ochrana paměti proti různým bezpečnostním exploitům
- Použít grsecurity
- Patch jádra
- Utility – paxctl, paxtest

Odkazy

- http://pax.grsecurity.net/
- http://grsecurity.net
- http://en.wikipedia.org/wiki/PaX
- http://www.gentoo.org/proj/en/hardened/

Děkuji za pozornost