

## 6.3.1. Disable Mitigasi Linux Kernel

Pada beberapa teknik yang akan dilakukan diperlukan penonaktifan pada mitigasi linux kernel. Kita akan melakukan disable beberapa proteksi yang akan menghalangi keberhasilan proses eksploitasi. Untuk selanjutnya nanti secara bertahap kita akan aktifkan proteksi satu persatu pada bagian bypass mitigasi linux kernel.

Berikut ini mitigasi linux kernel yang perlu dinonaktifkan

### 1. Disable SMEP, SMAP, KPTI dan KSLR.

Untuk mendisable ketik :

```
sudo nano /etc/default/grub
```

pada bagian GRUB\_CMDLINE\_LINUX\_DEFAULT ubah jadi seperti ini :

```
GRUB_CMDLINE_LINUX_DEFAULT="kgdboc=ttyS0,115200 kgdbwait nokaslr nosmep nosmap  
pti=off ima_appraise=off ima_policy=tcb"
```

lalu :

```
sudo update-grub
```

### 2. Mengaktifkan `unprivileged_userfaultfd`

Untuk mengaktifkannya :

```
sudo nano /etc/sysctl.d/99-userfaultfd.conf
```

Tambahkan baris :

```
vm.unprivileged_userfaultfd = 1
```

lalu :

```
sudo sysctl -p /etc/sysctl.d/99-userfaultfd.conf
```

### 3. Melakukan disable pada beberapa mitigasi kernel lain :

1. CONFIG\_VMAP\_STACK
2. CONFIG\_STACKPROTECTOR
3. CONFIG\_SLAB\_FREELIST\_HARDENED
4. CONFIG\_SLAB\_FREELIST\_RANDOM

Untuk mendisable keempat mitigasi tersebut kita perlu melakukan compile ulang kernel.