# KEAMANAN JARINGAN KOMPUTER


**OLEH :**

LISA MARDALETA

09011181320032

**JURUSAN SISTEM KOMPUTER**

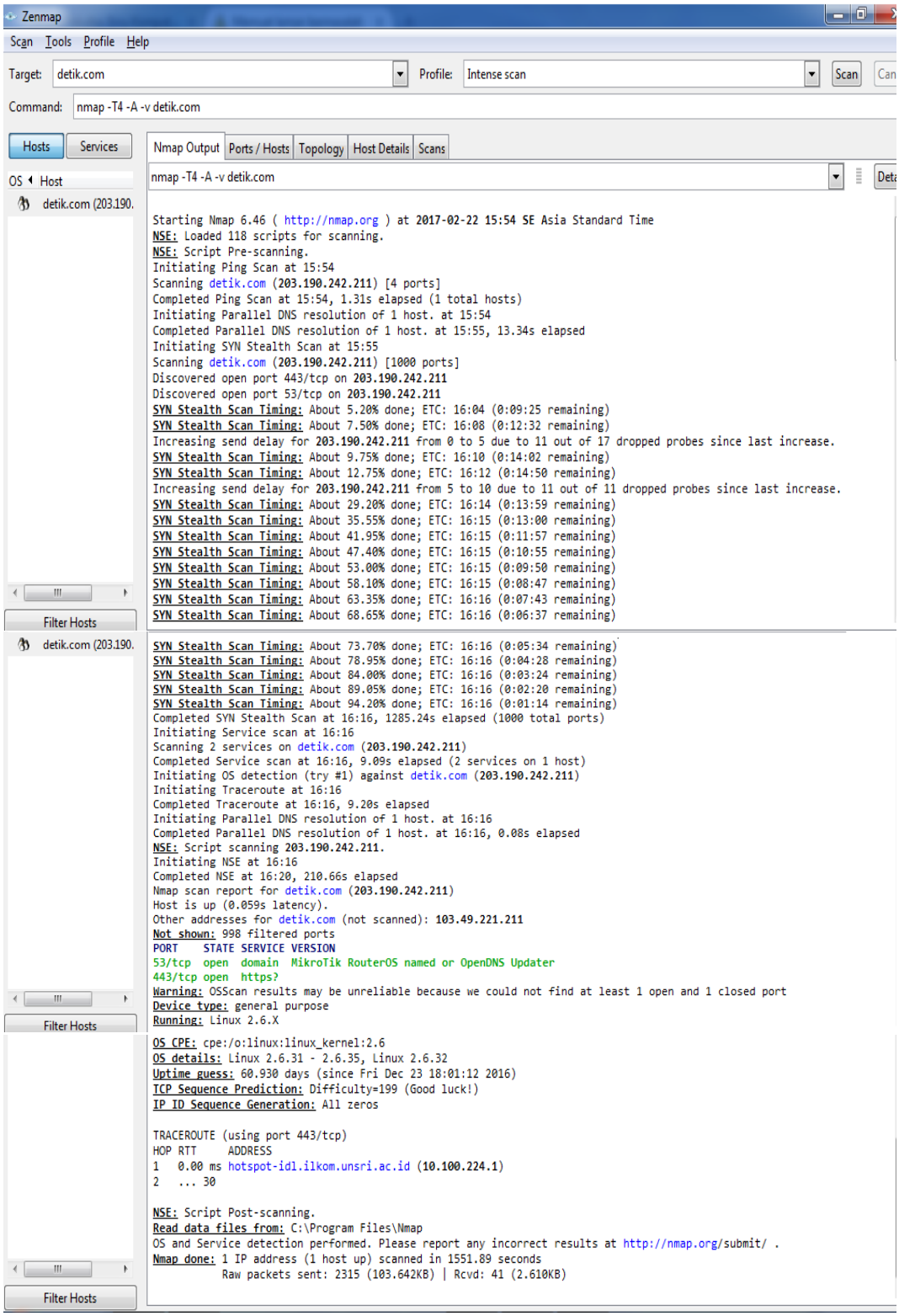
**FAKULTA ILMU KOMPUTER**

**UNIVERSITAS SRIWIJAYA**

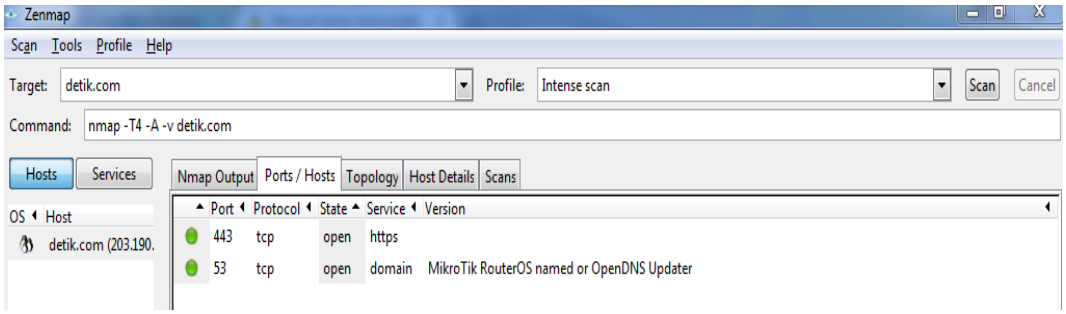
**2017**

## Scanning dengan domain “detik.com” menggunakan aplikasi Zenmap

- Berikut ini merupakan tampilan dari **Nmap Output** dengan domain detik.com.

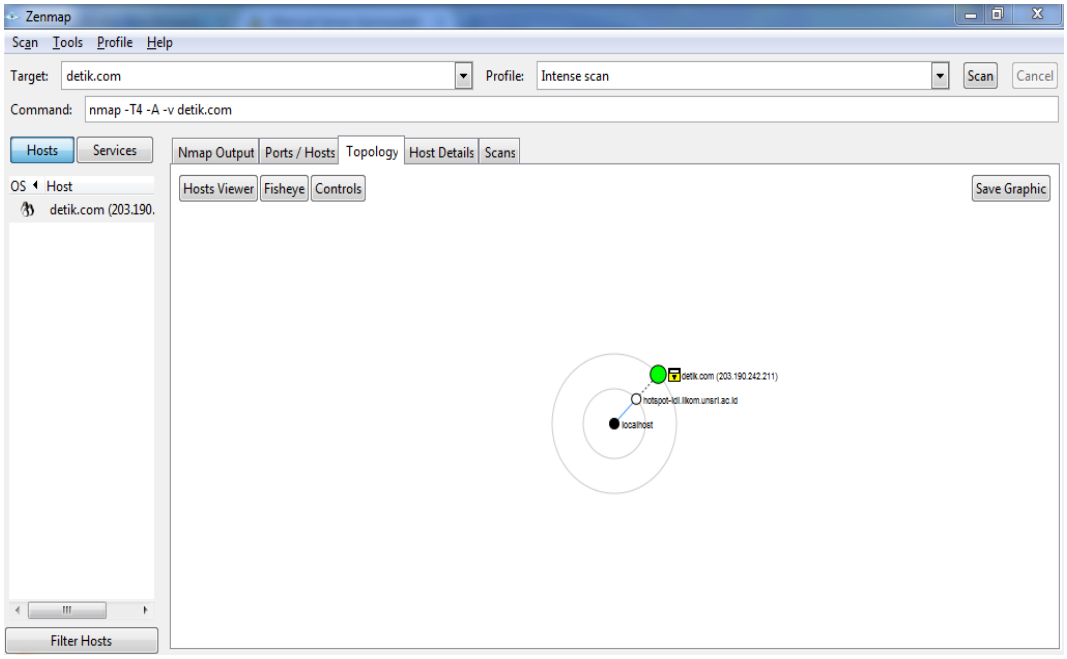


- Berikut ini merupakan tampilan dari **Ports / Hosts** dengan domain detik.com.



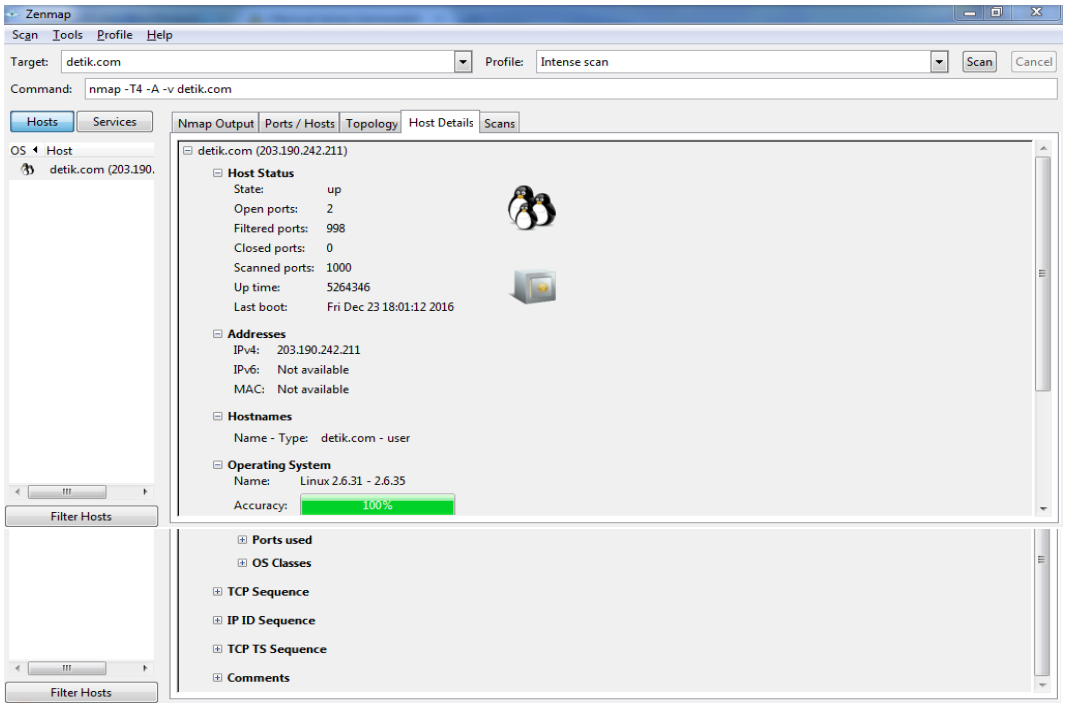

Gambar diatas manampilkan berupa 2 hasil layanan (service) dari domain "detik.com" yang berupa *port : 443, protokol : tcp, State : Open, Service : https* Dan *port : 53, Protocol : tcp, State : Open, Service : Domain, Version : Mikrotik RouterOS named or OpenDNS Updater.*

- Berikut ini merupakan tampilan dari **Topology** dengan domain detik.com.




Gambar diatas menampilkan detik.com (203.190.242.211), hotspot-idl.ilkom.unsri.ac.id, dan juga localhost, yang saling berkoneksi. Menjalankan domain detik.com dengan memakai localhost hotspot fasilkom unsri (hotspot-idl.ilkom.unsri.ac.id).

- Berikut ini merupakan tampilan dari **Host Details** dengan domain detik.com.




Host detail diatas menampilkan detik.com berupa IP 203.190.24.211, Host status berupa,

**State** : up, open ports : 2, Filtered Ports : 998, Closed Ports : 0, Scanned Ports : 1000, Up Time : 5264346, Last Boot : Fri dec 23 18:01:12 2016.

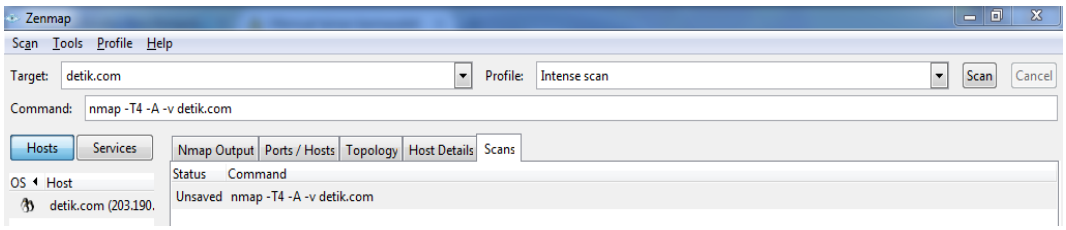
**Address :** IPv4 203.190.24.211, IPv6 Not Available, MAC Not Available.

**Hostnames :** Name- Type Detik.com-user.

**Operatyng System :** Name : Linux 2.6.31 – 2.6.35, Accuracy 100%.

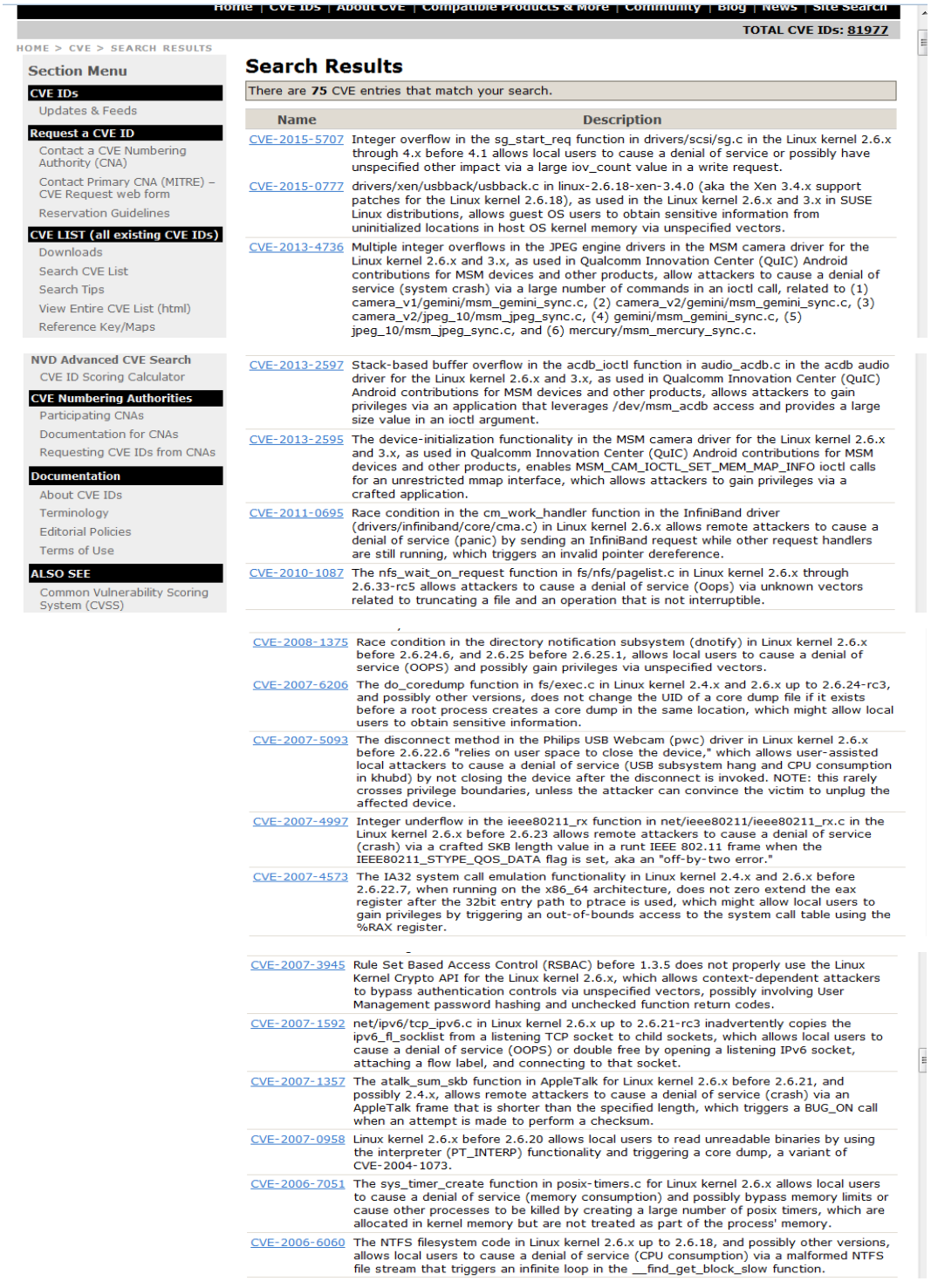
Sedangkan tampilan yang berikutnya tidak menampilkan apa-apa.

- Berikut ini merupakan tampilan dari **Scans** dengan domain detik.com.




Bagian **Scans** diatas menampilkan Status Command Unsaved nmap-t4 –A –v detik.com.

**Mencari CVE menggunakan Running : Linux 2.6.X , CVE nya ada 75, dan berikut tampilan dari sebagian CVE nya :**



Home | CVE IDs | About CVE | Compatible Products & More | Community | Blog | News | Site Search

TOTAL CVE IDs: 81977

HOME > CVE > SEARCH RESULTS

Section Menu

CVE IDs
Updates & Feeds

Request a CVE ID
Contact a CVE Numbering Authority (CNA)
Contact Primary CNA (MITRE) – CVE Request web form
Reservation Guidelines

CVE LIST (all existing CVE IDs)
Downloads
Search CVE List
Search Tips
View Entire CVE List (html)
Reference Key/Maps

NVD Advanced CVE Search
CVE ID Scoring Calculator

CVE Numbering Authorities
Participating CNAs
Documentation for CNAs
Requesting CVE IDs from CNAs

Documentation
About CVE IDs
Terminology
Editorial Policies
Terms of Use

ALSO SEE
Common Vulnerability Scoring System (CVSS)

## Search Results

There are **75** CVE entries that match your search.

| Name | Description |
|---|---|
| CVE-2015-5707 | Integer overflow in the sg_start_req function in drivers/scsi/sg.c in the Linux kernel 2.6.x through 4.x before 4.1 allows local users to cause a denial of service or possibly have unspecified other impact via a large iov_count value in a write request. |
| CVE-2015-0777 | drivers/xen/usbback/usbback.c in linux-2.6.18-xen-3.4.0 (aka the Xen 3.4.x support patches for the Linux kernel 2.6.18), as used in the Linux kernel 2.6.x and 3.x in SUSE Linux distributions, allows guest OS users to obtain sensitive information from uninitialized locations in host OS kernel memory via unspecified vectors. |
| CVE-2013-4736 | Multiple integer overflows in the JPEG engine drivers in the MSM camera driver for the Linux kernel 2.6.x and 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allow attackers to cause a denial of service (system crash) via a large number of commands in an ioctl call, related to (1) camera_v1/gemini/msm_gemini_sync.c, (2) camera_v2/gemini/msm_gemini_sync.c, (3) camera_v2/jpeg_10/msm_jpeg_sync.c, (4) gemini/msm_gemini_sync.c, (5) jpeg_10/msm_jpeg_sync.c, and (6) mercury/msm_mercury_sync.c. |
| CVE-2013-2597 | Stack-based buffer overflow in the acdb_ioctl function in audio_acdb.c in the acdb audio driver for the Linux kernel 2.6.x and 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to gain privileges via an application that leverages /dev/msm_acdb access and provides a large size value in an ioctl argument. |
| CVE-2013-2595 | The device-initialization functionality in the MSM camera driver for the Linux kernel 2.6.x and 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, enables MSM_CAM_IOCTL_SET_MEM_MAP_INFO ioctl calls for an unrestricted mmap interface, which allows attackers to gain privileges via a crafted application. |
| CVE-2011-0695 | Race condition in the cm_work_handler function in the InfiniBand driver (drivers/infiniband/core/cma.c) in Linux kernel 2.6.x allows remote attackers to cause a denial of service (panic) by sending an InfiniBand request while other request handlers are still running, which triggers an invalid pointer dereference. |
| CVE-2010-1087 | The nfs_wait_on_request function in fs/nfs/pagelist.c in Linux kernel 2.6.x through 2.6.33-rc5 allows attackers to cause a denial of service (Oops) via unknown vectors related to truncating a file and an operation that is not interruptible. |
| CVE-2008-1375 | Race condition in the directory notification subsystem (dnotify) in Linux kernel 2.6.x before 2.6.24.6, and 2.6.25 before 2.6.25.1, allows local users to cause a denial of service (OOPS) and possibly gain privileges via unspecified vectors. |
| CVE-2007-6206 | The do_coredump function in fs/exec.c in Linux kernel 2.4.x and 2.6.x up to 2.6.24-rc3, and possibly other versions, does not change the UID of a core dump file if it exists before a root process creates a core dump in the same location, which might allow local users to obtain sensitive information. |
| CVE-2007-5093 | The disconnect method in the Philips USB Webcam (pwc) driver in Linux kernel 2.6.x before 2.6.22.6 "relies on user space to close the device," which allows user-assisted local attackers to cause a denial of service (USB subsystem hang and CPU consumption in khubd) by not closing the device after the disconnect is invoked. NOTE: this rarely crosses privilege boundaries, unless the attacker can convince the victim to unplug the affected device. |
| CVE-2007-4997 | Integer underflow in the ieee80211_rx function in net/ieee80211/ieee80211_rx.c in the Linux kernel 2.6.x before 2.6.23 allows remote attackers to cause a denial of service (crash) via a crafted SKB length value in a runt IEEE 802.11 frame when the IEEE80211_STYPE_QOS_DATA flag is set, aka an "off-by-two error." |
| CVE-2007-4573 | The IA32 system call emulation functionality in Linux kernel 2.4.x and 2.6.x before 2.6.22.7, when running on the x86_64 architecture, does not zero extend the eax register after the 32bit entry path to ptrace is used, which might allow local users to gain privileges by triggering an out-of-bounds access to the system call table using the %RAX register. |
| CVE-2007-3945 | Rule Set Based Access Control (RSBAC) before 1.3.5 does not properly use the Linux Kernel Crypto API for the Linux kernel 2.6.x, which allows context-dependent attackers to bypass authentication controls via unspecified vectors, possibly involving User Management password hashing and unchecked function return codes. |
| CVE-2007-1592 | net/ipv6/tcp_ipv6.c in Linux kernel 2.6.x up to 2.6.21-rc3 inadvertently copies the ipv6_fl_socklist from a listening TCP socket to child sockets, which allows local users to cause a denial of service (OOPS) or double free by opening a listening IPv6 socket, attaching a flow label, and connecting to that socket. |
| CVE-2007-1357 | The atalk_sum_skb function in AppleTalk for Linux kernel 2.6.x before 2.6.21, and possibly 2.4.x, allows remote attackers to cause a denial of service (crash) via an AppleTalk frame that is shorter than the specified length, which triggers a BUG_ON call when an attempt is made to perform a checksum. |
| CVE-2007-0958 | Linux kernel 2.6.x before 2.6.20 allows local users to read unreadable binaries by using the interpreter (PT_INTERP) functionality and triggering a core dump, a variant of CVE-2004-1073. |
| CVE-2006-7051 | The sys_timer_create function in posix-timers.c for Linux kernel 2.6.x allows local users to cause a denial of service (memory consumption) and possibly bypass memory limits or cause other processes to be killed by creating a large number of posix timers, which are allocated in kernel memory but are not treated as part of the process' memory. |
| CVE-2006-6060 | The NTFS filesystem code in Linux kernel 2.6.x up to 2.6.18, and possibly other versions, allows local users to cause a denial of service (CPU consumption) via a malformed NTFS file stream that triggers an infinite loop in the __find_get_block_slow function. |

Pada tampilan CVE nya ada 75, namun diatas hanya sebagian saja yang ditampilkan (di screen), CVE tersebut menampilkan nama CVE berupa deskripsi mengenai CVE tersebut pada masing-masing CVE yang berbeda-beda.