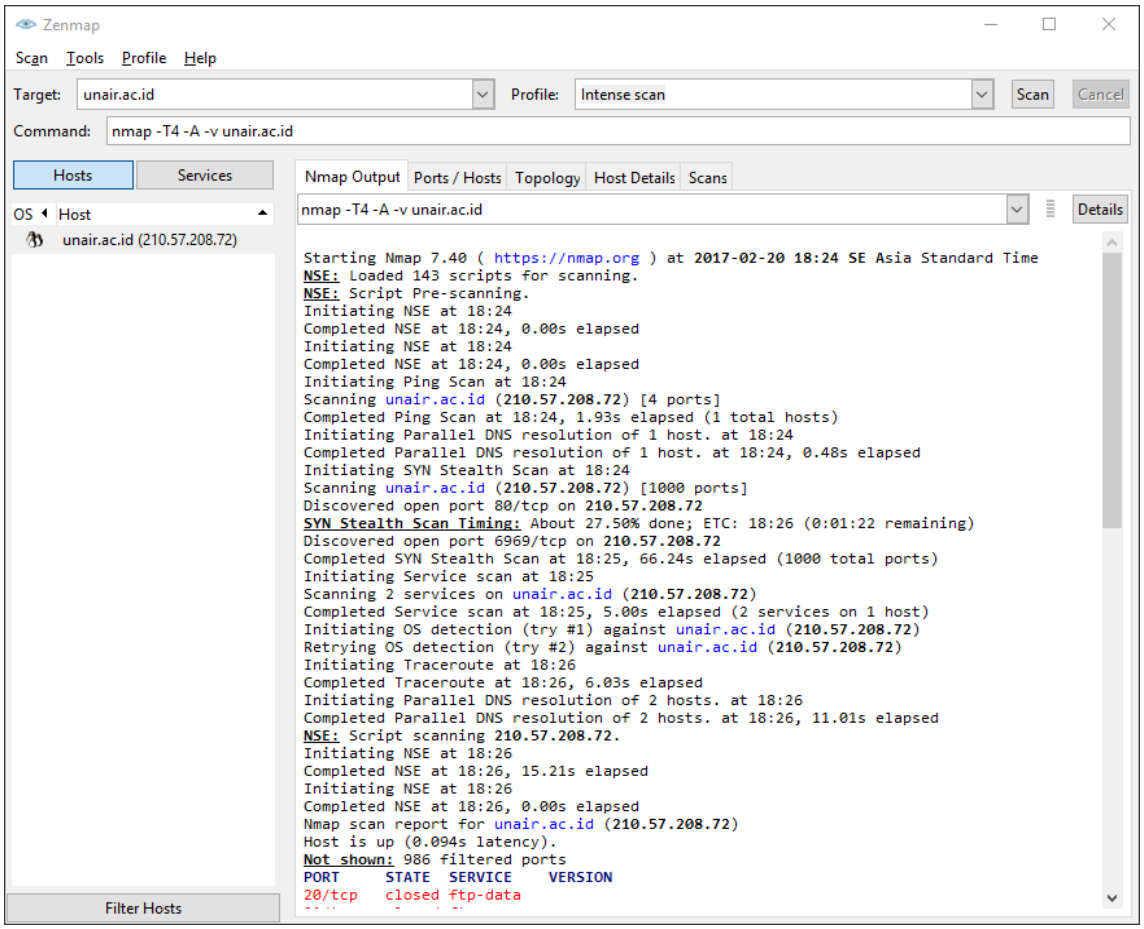
SCANNING unair.ac.id

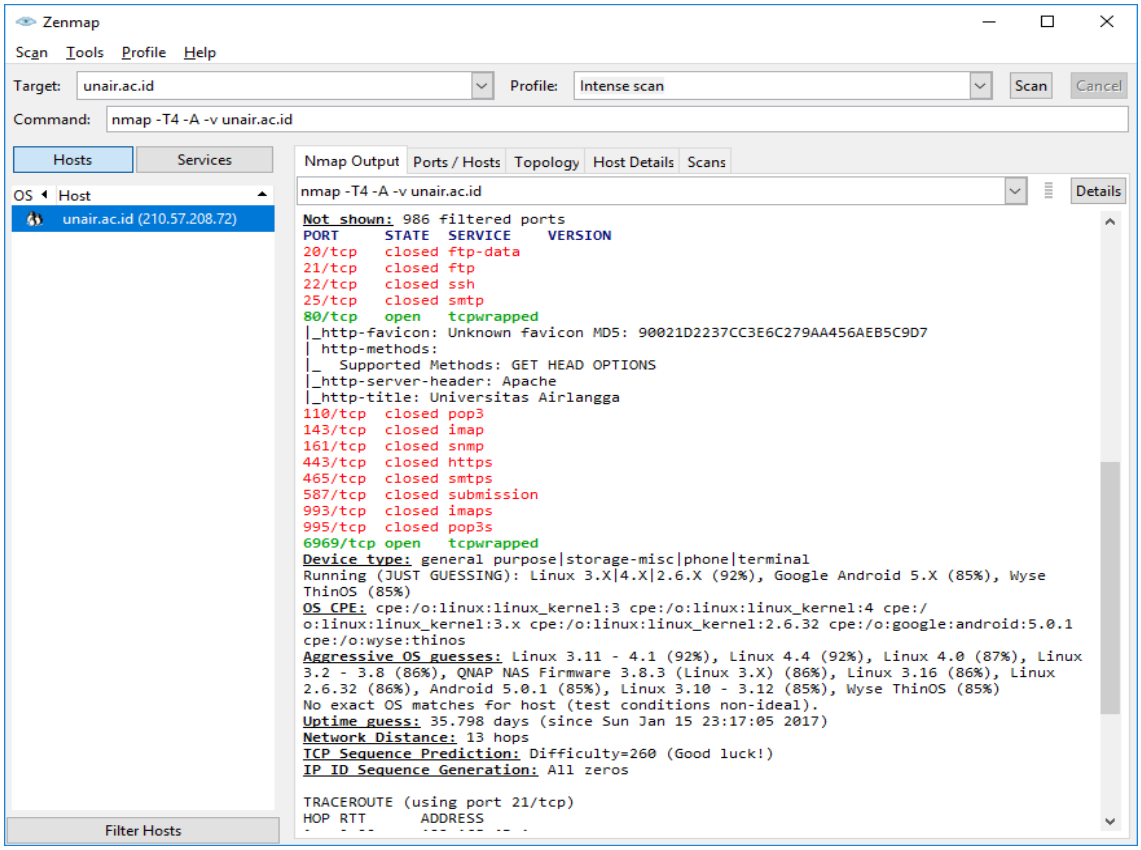
Scanning merupakan tanda dari dimulainya sebuah serangan oleh peretas (*pre-attack*). Pada tahap ini, peretas akan mencari berbagai kemungkinan yang dapat digunakan untuk mengambil alih komputer atau sistem dari target. Tahapan ini dapat dilakukan jika informasi yang didapat pada tahap *reconnaissance* mencukupi sehingga peretas bisa mencari "jalan masuk" untuk menguasai sistem. Berbagai peralatan (*tools*) dapat membantu seorang peretas untuk melalui tahapan ini.

Dalam melakukan *scanning* pada target unair.ac.id dengan ip *address* 210.57.208.72, *tools* yang digunakan yaitu: aplikasi Nmap-Zenmap GUI versi 7.40 yang di install pada sistem operasi Windows 10 dan *Command Prompt* (CMD) pada sistem operasi Linux Mint 18 Sarah.

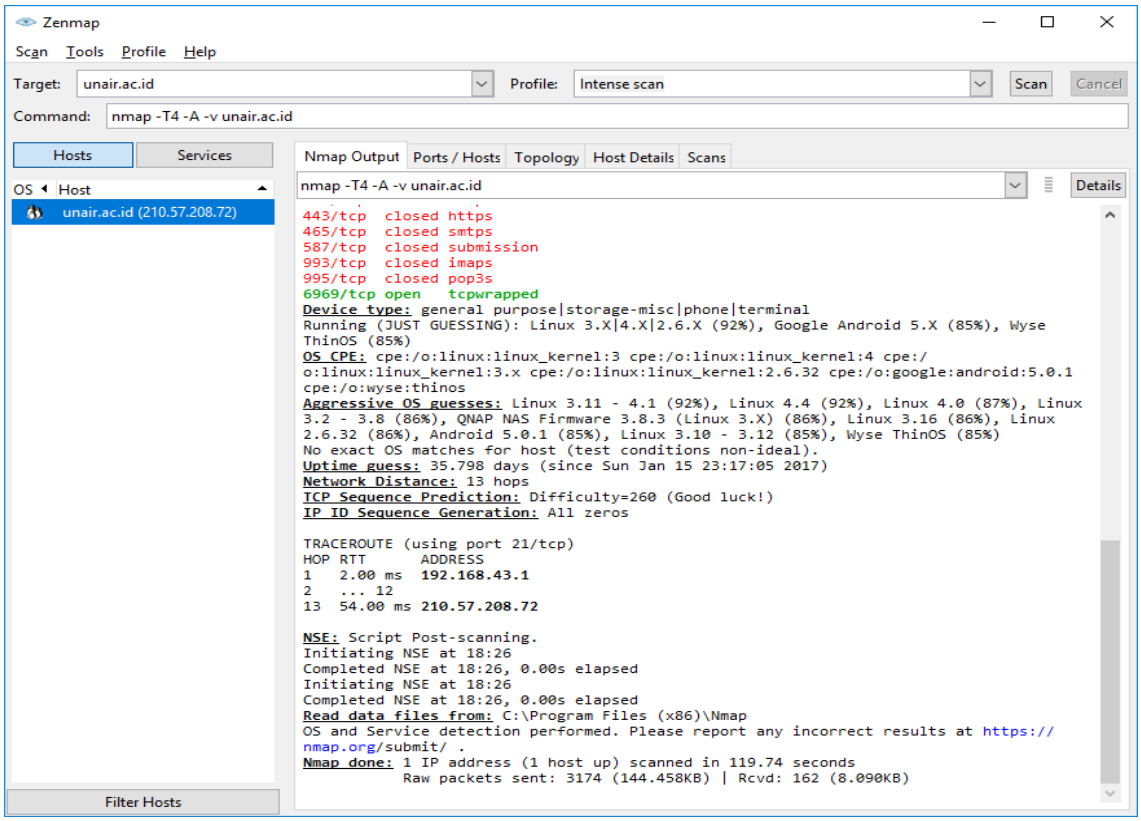
Berikut informasi yang didapat, misalnya port yang terbuka, system operasi yang *running* pada target unair.ac.id :



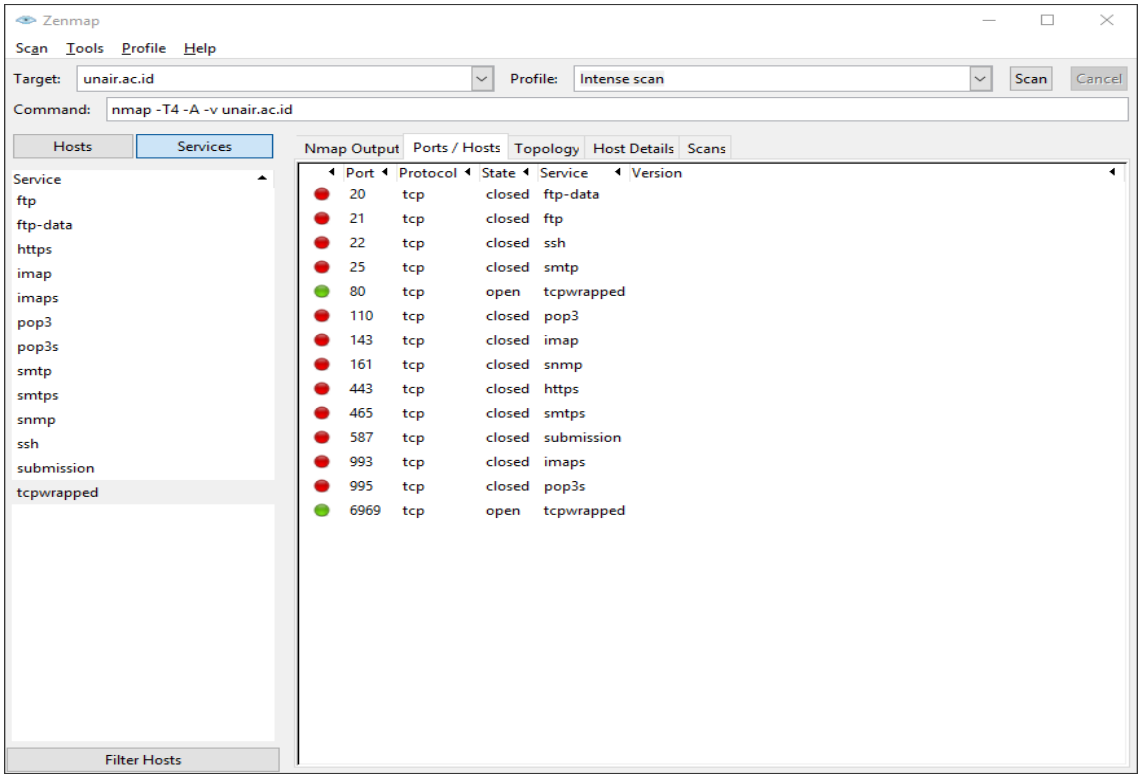
Gambar 1: proses *scanning* menggunakan *tools* zenmap



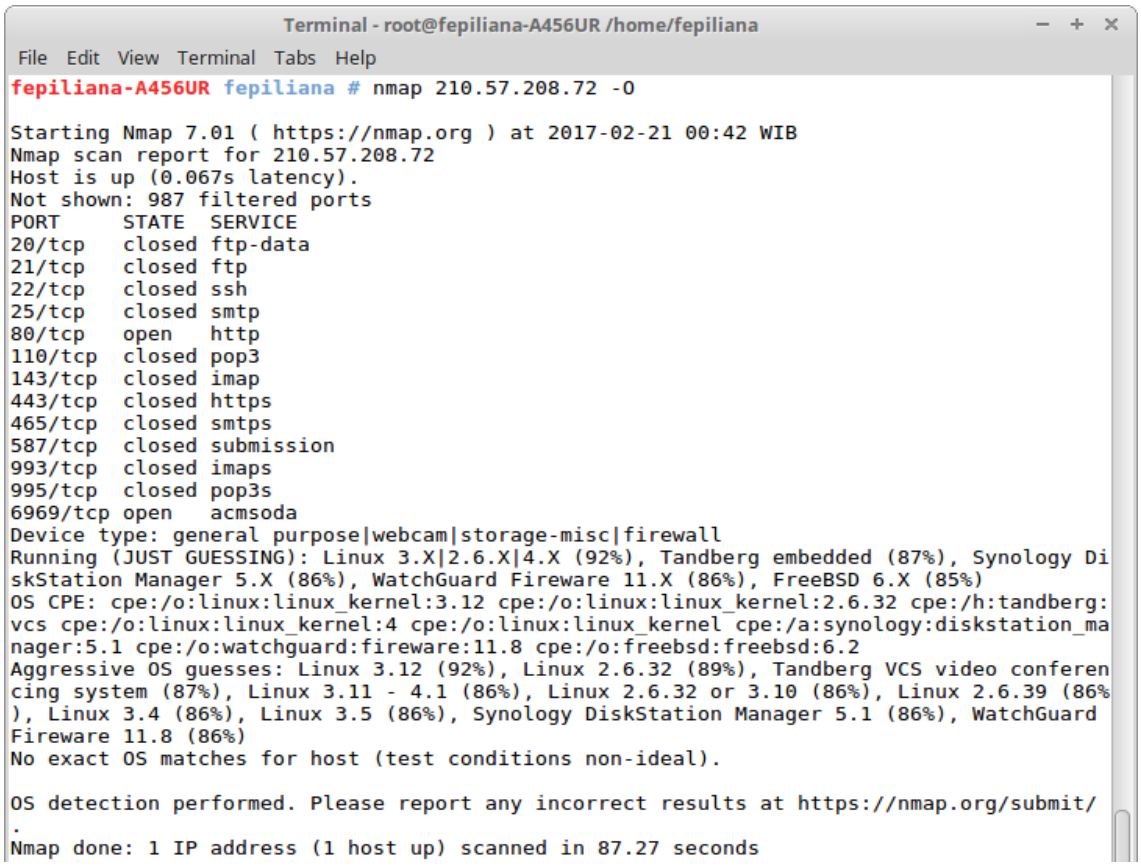
Gambar 2: proses *scanning* menggunakan *tools* zenmap (lanjutan)



Gambar 3: proses *scanning* menggunakan *tools* zenmap (lanjutan)



Gambar 4: Detail Port yang terdapat pada target menggunakan *tools* zenmap

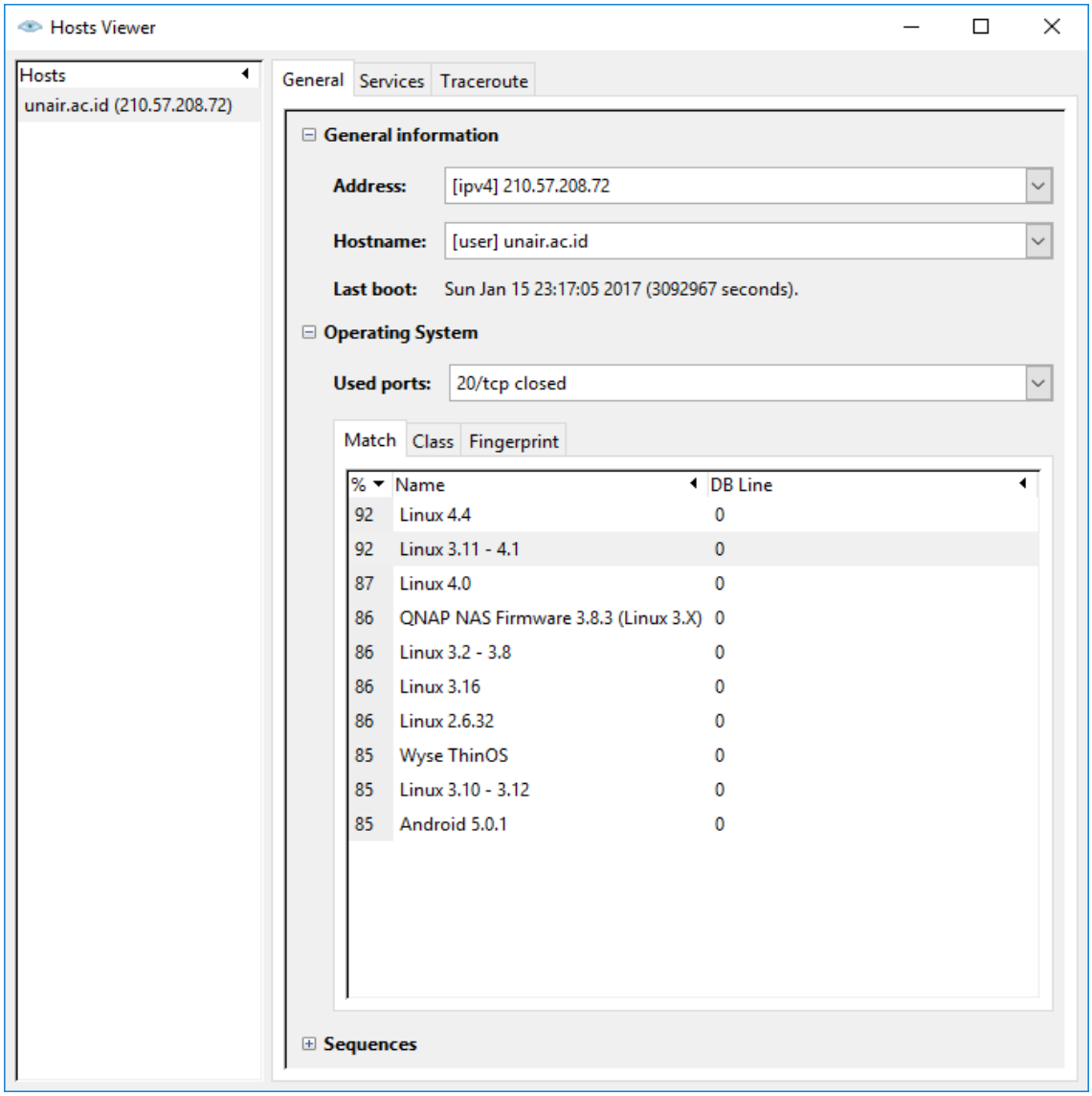


Gambar 5: proses *scanning* menggunakan nmap pada CMD Linux

Berdasarkan gambar 1, 2, 3, dan 4 terdeteksi ada 14 port yang *running* pada target. Di 14 port untuk berbagai macam service yang dilayani target, ada 2 port dengan status *open* yaitu layanan tcpwrapped dan 12 port status *closed* yaitu ftp-data, ftp, ssh, smtp, pop3, imap, snmp, https, smtps, submission, imaps, dan pop3s. Seluruh port yang *running* menggunakan protocol TCP. Sedangkan pada saat melakukan *scanning* menggunakan CMD Linux (lihat gambar 5) terdeteksi 13 port dengan *service* berbeda-beda yang *running* pada target. Pada hasil gambar 5, kita dapat mengetahui port yang *open* adalah *service* http dan acmsoda, lalu port yang *closed* adalah service ftp-data, ftp, ssh, smtp, pop3, imap, snmp, https, smtps, submission, imaps, dan pop3s. *Command* `nmap [ip_target] -O` maksudnya yaitu *command* yang digunakan untuk mengaktifkan deteksi sistem operasi pada target.

Maksud dari *open* dan *closed* yaitu :

- *Open yaitu* sebuah aplikasi secara aktif menerima koneksi paket TCP atau UDP pada port ini. Menemukan port terbuka ini seringkali merupakan tujuan utama scanning port. Orang dengan pikiran keamanan *(security-minded)* tahu bahwa setiap port terbuka merupakan celah untuk serangan. Penyerang dan pentesters ingin mengeksploitasi port terbuka, namun administrator berusaha menutup atau melindungi mereka dengan firewall tanpa mengganggu user yang berhak. Port terbuka juga menarik bagi *scan* bukan keamanan karena mereka memberitahu layanan yang dapat digunakan pada jaringan.
- *Closed* yaitu port tertutup dapat diakses (ia menerima dan menanggapi paket probe Nmap), namun tidak ada aplikasi yang mendengarkan padanya. Mereka bermanfaat dengan menunjukkan bahwa host up pada alamat IP tersebut (*host discovery*, atau ping *scanning*), dan sebagai bagian deteksi sistem operasi. Oleh karena port tertutup dapat dijangkau, bermanfaat untuk mencoba scan di waktu yang lain jikalau port tersebut terbuka. Administrator mungkin perlu mempertimbangkan untuk memblok port tersebut dengan *firewall*..



Gambar 6: detail sistem operasi yang *running* pada target menggunakan zenmap *tools*

Pada gambar 6 dapat kita lihat informasi tentang versi-versi sistem operasi yang terdapat pada target. Untuk mengetahui kelemahan dari sistem operasi yang *running* pada target, kita perlu menggunakan CVE. CVE (*Common Vulnerabilities and Exposures*) adalah *Standard for Information Security Vulnerability Names* yang dikelola oleh MITRE. CVE menyediakan referensi mengenai vulnerability yang ada pada satu produk. CVE menyediakan referensi mengenai vulnerability yang ada pada satu produk. CVE bisa dikatakan sebuah database mengenai setiap vulnerability yang di publish.

Berikut adalah detail inspeksi *scanning* berdasarkan CVE pada setiap sistem operas target:

- **Linux 4.4**

Prediksi sistem operasi Linux 4.4 yang digunakan pada target adalah 92%.

Nama	Deskripsi
CVE-2016-3070	Pelaksanaan trace_writeback_dirty_page di antara / jejak / peristiwa / writeback.h di kernel Linux sebelum 4.4 tidak benar berinteraksi dengan mm / migrate.c, yang memungkinkan pengguna lokal untuk menyebabkan penolakan layanan (NULL pointer dereference dan sistem crash) atau mungkin memiliki tidak ditentukan dampak lain dengan memicu halaman langkah tertentu.
CVE-2015-8966	arch / arm / kernel / sys_oabi-compat.c di kernel Linux sebelum 4.4 memungkinkan pengguna lokal untuk mendapatkan hak melalui crafted (1) F_OFD_GETLK, (2) F_OFD_SETLK, atau (3) perintah F_OFD_SETLKW dalam panggilan fcntl64 sistem.
CVE-2015-8963	Kondisi balapan di kernel / peristiwa / core.c di kernel Linux sebelum 4.4 memungkinkan pengguna lokal untuk mendapatkan hak atau menyebabkan penolakan layanan (penggunaan-setelah-bebas) dengan memanfaatkan salah penanganan struktur data swevent selama operasi CPU cabut.
CVE-2015-8962	Ganda kerentanan bebas dalam fungsi sg_common_write di driver / scsi / sg.c di kernel Linux sebelum 4.4 memungkinkan pengguna lokal untuk mendapatkan hak atau menyebabkan penolakan layanan (korupsi memori dan sistem crash) dengan memisahkan perangkat saat panggilan SG_IO ioctl.
CVE-2015-8787	Fungsi nf_nat_redirect_ipv4 di net / Netfilter / nf_nat_redirect.c di kernel Linux sebelum 4.4 memungkinkan penyerang remote untuk menyebabkan penolakan layanan (NULL pointer dereference dan sistem crash) atau mungkin memiliki dampak lain yang tidak ditentukan dengan mengirimkan paket IPv4 tertentu untuk sebuah antarmuka tidak lengkap dikonfigurasi , isu terkait dengan CVE-2003-1604.
CVE-2015-8785	fuse_fill_write_pages berfungsi dalam fs / sekering / file.c di kernel Linux sebelum 4.4 memungkinkan pengguna lokal untuk menyebabkan penolakan layanan (infinite loop) melalui sistem writev panggilan yang memicu panjang nol untuk segmen pertama dari IOV.
CVE-2015-8539	KUNCI subsistem dalam kernel Linux sebelum 4.4 memungkinkan pengguna lokal untuk mendapatkan hak atau menyebabkan penolakan layanan (BUG) melalui perintah keyctl dibuat yang negatif instantiate kunci, terkait dengan keamanan / kunci / dienkripsi-kunci / encrypted.c, keamanan / kunci / trusted.c, dan keamanan / kunci / user_defined.c.
CVE-2015-7515	Fungsi aiptek_probe di driver / input / tablet / aiptek.c di kernel Linux sebelum 4.4 memungkinkan penyerang proksimat fisik menyebabkan penolakan layanan (NULL pointer dereference dan sistem crash) melalui perangkat USB dibuat yang tidak memiliki titik akhir.

Nama	Deskripsi
CVE-2015-7513	arch / x86 / KVM / x86.c di kernel Linux sebelum 4.4 tidak mengatur ulang nilai-nilai PIT kontra selama restorasi negara, yang memungkinkan pengguna OS tamu untuk menyebabkan penolakan layanan (divide-by-nol kesalahan dan tuan OS crash) melalui nilai nol, terkait dengan kvm_vm_ioctl_set_pit dan kvm_vm_ioctl_set_pit2 fungsi.
CVE-2015-2124	kerentanan yang tidak ditentukan di Easy Setup Wizard di HP ThinPro Linux 4.1 melalui 5.1 dan Smart Nol Inti 4.3 dan 4.4 memungkinkan pengguna lokal untuk memotong dimaksudkan pembatasan akses dan hak istimewa gain melalui vektor diketahui.
CVE-2015-1339	Memori kebocoran di fungsi cuse_channel_release di fs / sekering / cuse.c di kernel Linux sebelum 4.4 memungkinkan pengguna lokal untuk menyebabkan penolakan layanan (konsumsi memori) atau mungkin memiliki ditentukan dampak lain dengan membuka / dev / cuse berkali-kali.
CVE-2013-6770	CyanogenMod / ClockWorkMod / Koush Superuser paket 1.0.2.1 untuk Android 4.3 dan 4.4 tidak benar membatasi set pengguna yang dapat menjalankan / system / xbin / su dengan opsi --daemon, yang memungkinkan penyerang untuk mendapatkan hak dengan memanfaatkan shell ADB akses dan Linux UID tertentu, dan kemudian membuat script Trojan horse.
CVE-2007-0773	Linux kernel sebelum 2.6.9-42.0.8 di Red Hat 4.4 memungkinkan pengguna lokal untuk menyebabkan penolakan layanan (kernel OOPS dari dereference null) melalui fput dalam ioctl 32-bit pada sistem x86 64-bit, memperbaiki memperbaiki CVE-2005-3.044,1 yang tidak lengkap.

- **Linux 3.11 - 4.1**

Berdasarkan gambar 6, prediksi target menggunakan sistem operasi linux 3.11 – 4.1 yaitu 92 %. Hanya ada 1 CVE tentang Linux 3.11 – 4.1

Nama	Deskripsi
CVE-2001-0775	CVE-2001-0775 Buffer overflow di xloadimage 4.1 (alias xli 1,16 dan 1,17) di Linux memungkinkan penyerang remote untuk mengeksekusi kode arbitrary melalui FACES format gambar yang berisi panjang (1) Nama depan atau (2) bidang Nama belakang.

- **Linux 4.0**

87% target menggunakan sistem operasi linux 4.0

Nama	Deskripsi
CVE-2016-6787	kernel / peristiwa / core.c dalam subsistem kinerja dalam kernel Linux sebelum 4.0 mismanages kunci selama migrasi tertentu, yang memungkinkan pengguna lokal untuk mendapatkan hak melalui aplikasi dibuat, alias Android internal yang bug 31.095.224.

Nama	Deskripsi
CVE-2016-6786	kernel / peristiwa / core.c dalam subsistem kinerja dalam kernel Linux sebelum 4.0 mismanages kunci selama migrasi tertentu, yang memungkinkan pengguna lokal untuk mendapatkan hak melalui aplikasi dibuat, alias Android internal yang bug 30.955.111.
CVE-2015-8967	arch / arm64 / kernel / sys.c di kernel Linux sebelum 4.0 memungkinkan pengguna lokal untuk melewati "izin halaman ketat" mekanisme perlindungan dan memodifikasi tabel sistem panggilan, dan akibatnya mendapatkan hak, dengan memanfaatkan akses tulis
CVE-2015-8830	integer overflow dalam fungsi aio_setup_single_vector di fs / aio.c di kernel Linux 4.0 memungkinkan pengguna lokal untuk menyebabkan penolakan layanan atau mungkin memiliki dampak lain yang tidak ditentukan melalui iovec AIO besar. CATATAN: kerentanan ini ada karena regresi CVE-2012-6701.
CVE-2015-8215	net / ipv6 / addrconf.c dalam tumpukan IPv6 di kernel Linux sebelum 4.0 tidak memvalidasi perubahan berusaha untuk nilai MTU, yang memungkinkan penyerang tergantung pada konteks untuk menyebabkan penolakan layanan (packet loss) melalui nilai yang (1) lebih kecil dari nilai compliant minimum atau (2) lebih besar dari MTU dari interface, seperti yang ditunjukkan oleh Router Advertisement (RA) pesan yang tidak divalidasi oleh daemon, kerentanan yang berbeda dari CVE-2015-0272. CATATAN: lingkup CVE-2015-0272 adalah terbatas pada produk NetworkManager.
CVE-2015-4036	Array kesalahan indeks dalam fungsi tcm_vhost_make_tpg di driver / vhost / scsi.c di kernel Linux sebelum 4.0 mungkin memungkinkan pengguna OS tamu untuk menyebabkan penolakan layanan (memori korupsi) atau mungkin memiliki dampak lain yang tidak ditentukan melalui panggilan VHOST_SCSI_SET_ENDPOINT ioctl dibuat. CATATAN: fungsi terpengaruh berganti nama menjadi vhost_scsi_make_tpg sebelum kerentanan diumumkan.
CVE-2015-2666	Berbasis Stack buffer overflow dalam fungsi get_matching_model_microcode di arch / x86 / kernel / cpu / microcode / intel_early.c di kernel Linux sebelum 4.0 memungkinkan penyerang tergantung pada konteks untuk mendapatkan hak dengan membangun sebuah header microcode dibuat dan memanfaatkan akses root untuk akses tulis ke initrd.
CVE-2015-0761	Cisco AnyConnect Aman Mobility Klien sebelum 3.1 (8009) dan 4.x sebelum 4.0 (2052) di Linux tidak benar menerapkan fungsi internal yang tidak ditentukan, yang memungkinkan pengguna lokal untuk mendapatkan hak akses root melalui pilihan vpnagent dibuat, alias Bug ID CSCus86790.
CVE-2014-0042	OpenStack Panas Template (heat-template), seperti yang digunakan dalam Red Hat Enterprise Linux OpenStack Landasan 4.0, set gpgcheck ke 0 untuk template tertentu, yang menonaktifkan GPG tanda tangan memeriksa paket download dan memungkinkan man-in-the-middle penyerang untuk menginstal paket sewenang-wenang melalui vektor ditentukan.

Nama	Deskripsi
CVE-2014-0041	OpenStack Panas Template (heat-template), seperti yang digunakan dalam Red Hat Enterprise Linux OpenStack Landasan 4.0, set sslverify ke false untuk repositori Yum tertentu, yang menonaktifkan perlindungan SSL dan memungkinkan man-in-the-middle penyerang untuk mencegah update melalui vektor yang tidak ditentukan.
CVE-2014-0040	OpenStack Panas Template (heat-template), seperti yang digunakan dalam Red Hat Enterprise Linux OpenStack Landasan 4.0, menggunakan koneksi HTTP untuk men-download (1) paket dan (2) kunci penandatanganan dari repositori Yum, yang memungkinkan man-in-the-middle penyerang untuk mencegah pembaruan melalui vektor yang tidak ditentukan.
CVE-2013-6470	Konfigurasi default dalam kontroler mandiri quickstack terwujud dalam OpenStack-mandor-installer, seperti yang digunakan dalam Red Hat Enterprise Linux OpenStack Landasan 4.0, menonaktifkan otentikasi untuk Qpid, yang memungkinkan penyerang untuk mengakses dengan menghubungkan ke Qpid.
CVE-2013-4669	FortiClient sebelum 4.3.5.472 pada Windows, sebelum 4.0.3.134 di Mac OS X, dan sebelum 4.0 pada Android; FortiClient Lite sebelum 4.3.4.461 pada Windows; FortiClient Lite 2.0 melalui 2.0.0223 di Android; dan FortiClient SSL VPN sebelum 4.0.2258 di Linux melanjutkan dengan sesi SSL setelah menentukan bahwa sertifikat X.509 server tidak valid, yang memungkinkan man-in-the-middle penyerang untuk mendapatkan informasi sensitif dengan memanfaatkan transmisi password yang terjadi sebelum peringatan pengguna tentang masalah sertifikat.
CVE-2011-2162	Beberapa kerentanan yang tidak ditentukan di FFmpeg 0.4.x melalui 0.6.x, seperti yang digunakan dalam MPlayer 1.0 dan produk lainnya, di Mandriva Linux 2.009,0, 2.010,0, dan 2.010,1; Perusahaan Server 4.0 (alias CS4.0); dan Mandriva Enterprise Server 5 (alias MES5) memiliki diketahui dampak dan serangan vektor, terkait dengan isu-isu "awalnya ditemukan oleh pengembang Google Chrome."
CVE-2010-2070	arch / ia64 / xen / faults.c di Xen 3.4 dan 4.0 di Linux kernel 2.6.18, dan versi kernel mungkin lain, ketika berjalan di IA-64 arsitektur, memungkinkan pengguna lokal untuk menyebabkan penolakan layanan dan "menghidupkan BE oleh memodifikasi topeng pengguna dari PSR, "seperti yang ditunjukkan melalui eksploitasi CVE-2006-0742.
CVE-2009-0032	CUPS pada Mandriva Linux 2008.0, 2008.1, 2009,0, Corporate Server (CS) 3.0 dan 4.0, dan Multi Jaringan Firewall (MNF) 2,0 memungkinkan pengguna lokal untuk menimpa file sewenang-wenang melalui serangan symlink pada file sementara /tmp/pdf.log.
CVE-2008-5161	Kesalahan penanganan dalam protokol SSH di (1) SSH Tectia Client dan Server dan Connector 4.0 melalui 4.4.11, 5.0 melalui 5.2.4, dan 5.3 melalui 5.3.8; Client dan Server dan ConnectSecure 6.0 melalui 6.0.4; Server untuk Linux pada IBM System z 6.0.4; Server untuk IBM z / OS 5.5.1 dan sebelumnya, 6.0.0, dan 6.0.1
CVE-2006-3287	Cisco Control System Wireless (WCS) untuk Linux dan Windows 4.0 (1) dan sebelumnya menggunakan default administrator username "root" dan password "publik", yang memungkinkan penyerang remote untuk mendapatkan akses (alias bug CSCse21391).

Nama	Deskripsi
CVE-2005-2720	Stack berbasis buffer overflow di perpustakaan ACE arsip dekompresi (vrAZace.dll) di HAURI produk Anti-Virus termasuk ViRobot Expert 4.0, Advanced Server, Linux Server 2.0, dan LiveCall, ketika file terkompresi scanning diaktifkan, memungkinkan penyerang remote untuk mengeksekusi sewenang-wenang kode melalui sebuah arsip ACE yang berisi file dengan nama file yang panjang.
CVE-2005-2670	Directory traversal kerentanan di HAURI produk Anti-Virus termasuk ViRobot Expert 4.0, Advanced Server, Linux Server 2.0, dan LiveCall memungkinkan penyerang remote untuk menimpa file sewenang-wenang melalui ".." urutan dalam nama file yang terkandung dalam (1) ACE, (2) ARJ, (3) CAB, (4) LZH, (5) RAR, (6) TAR dan (7) file ZIP.
CVE-2004-0217	Kemampuan LiveUpdate (liveupdate.sh) di Symantec AntiVirus Scan Engine 4.0 dan 4.3 untuk Red Hat Linux memungkinkan pengguna lokal untuk membuat atau menambahkan ke file sewenang-wenang melalui serangan symlink di /tmp/LiveUpdate.log.
CVE-2003-0658	Docview sebelum 1,1-18 di Caldera OpenLinux 3.1.1, SCO Linux 4.0, OpenServer 5.0.7, mengkonfigurasi web server Apache dengan cara yang memungkinkan penyerang remote untuk membaca sewenang-wenang file yang dapat dibaca publik melalui URL tertentu, kemungkinan berhubungan dengan menulis ulang aturan.
CVE-2003-0631	VMware GSX Server 2.5.1 build 4968 dan sebelumnya, dan Workstation 4.0 dan sebelumnya, memungkinkan pengguna lokal untuk mendapatkan hak root melalui variabel enivronment tertentu yang digunakan ketika meluncurkan sesi mesin virtual.
CVE-2003-0480	VMware Workstation 4.0 untuk Linux memungkinkan pengguna lokal untuk menimpa file sewenang-wenang dan hak gain melalui "manipulasi symlink."
CVE-2000-0573	Fungsi lreply di wu-ftpd 2.6.0 dan sebelumnya tidak benar membersihkan sebuah format string tidak dipercaya, yang memungkinkan penyerang remote untuk menjalankan perintah sewenang-wenang melalui perintah SITE EXEC.
CVE-1999-1387	Windows NT 4.0 SP2 memungkinkan penyerang remote untuk menyebabkan penolakan layanan (kecelakaan), mungkin melalui input cacat atau paket, seperti yang dihasilkan oleh Linux smbmount perintah yang disusun pada Linux 2.0.29 kernel tapi dijalankan pada Linux 2.0.25 .
CVE-1999-1335	Server snmpd di CMU-snmp SNMP paket sebelum 3,3-1 di Red Hat Linux 4.0 dikonfigurasi untuk memungkinkan penyerang remote untuk membaca dan menulis informasi sensitif.
CVE-1999-1299	rcp pada berbagai sistem Linux termasuk Red Hat 4.0 memungkinkan "tidak ada" user atau pengguna lain dengan UID dari 65.535 menimpa file sewenang-wenang, karena 65535 ditafsirkan sebagai -1 oleh chown dan panggilan sistem lainnya, yang menyebabkan panggilan gagal untuk memodifikasi kepemilikan file.
CVE-1999-0832	Buffer overflow di NFS server di Linux memungkinkan penyerang untuk menjalankan perintah melalui pathname lama.
CVE-1999-0831	Denial of service di Linux syslogd melalui sejumlah besar koneksi.

- **Linux 3.X (QNAP NAS Firmware 3.8.3)**

Berdasarkan gambar 6, prediksi target menggunakan sistem operasi linux 3.X adalah 86 %

Nama	Deskripsi
CVE-2013-0143	cgi-bin / pingping.cgi pada perangkat QNAP VioStor NVR dengan firmware 4.0.3, dan dalam komponen Surveillance Station Pro di QNAP NAS, memungkinkan jarak jauh dikonfirmasi pengguna untuk menjalankan perintah sewenang-wenang dengan memanfaatkan akses tamu dan menempatkan metakarakter shell dalam string.
CVE-2013-0142	perangkat QNAP VioStor NVR dengan firmware 4.0.3, dan komponen Surveillance Station Pro di QNAP NAS, memiliki akun tamu hardcoded, yang memungkinkan penyerang remote untuk mendapatkan web-server akses login melalui vektor ditentukan.

- **Linux 3.2 – 3.8**

Berdasarkan gambar 6, prediksi target menggunakan sistem operasi linux 3.2 – 3.8 yaitu 86 %

Nama	Deskripsi
CVE-2013-2548	Fungsi crypto_report_one di kripto / crypto_user.c di API laporan di kripto konfigurasi pengguna API dalam kernel Linux melalui 3.8.2 menggunakan nilai panjang yang salah selama operasi copy, yang memungkinkan pengguna lokal untuk mendapatkan informasi sensitif dari memori kernel dengan memanfaatkan kemampuan CAP_NET_ADMIN.
CVE-2013-2547	Fungsi crypto_report_one di kripto / crypto_user.c di API laporan di kripto konfigurasi pengguna API dalam kernel Linux melalui 3.8.2 tidak menginisialisasi anggota struktur tertentu, yang memungkinkan pengguna lokal untuk mendapatkan informasi sensitif dari memori kernel tumpukan dengan memanfaatkan CAP_NET_ADMIN yang kemampuan.
CVE-2013-2546	Laporan API di kripto konfigurasi pengguna API dalam kernel Linux melalui 3.8.2 menggunakan fungsi library C yang salah untuk menyalin string, yang memungkinkan pengguna lokal untuk mendapatkan informasi sensitif dari kernel stack memori dengan memanfaatkan kemampuan CAP_NET_ADMIN.

Nama	Deskripsi
CVE-2013-1763	Array kesalahan indeks dalam fungsi __sock_diag_rcv_msg di net / core / sock_diag.c di kernel Linux sebelum 3.7.10 memungkinkan pengguna lokal untuk mendapatkan hak melalui nilai keluarga besar dalam pesan Netlink.
CVE-2013-0231	Fungsi pciback_enable_msi pada driver PCI backend (driver / xen / pciback / conf_space_capability_msi.c) di Xen untuk kernel Linux 2.6.18 dan 3,8 memungkinkan pengguna OS tamu dengan akses perangkat PCI untuk menyebabkan penolakan layanan melalui sejumlah besar kernel log pesan. CATATAN: beberapa rincian ini diperoleh dari informasi pihak ketiga..

- **Linux 3.16**

Berdasarkan gambar 6, prediksi target menggunakan sistem operasi linux 3.16 yaitu 86 %

Nama	Deskripsi
CVE-2015-2830	arch / x86 / kernel / entry_64.S di kernel Linux sebelum 3.19.2 tidak mencegah bendera TS_COMPAT mencapai tugas user-mode, yang akan memungkinkan pengguna lokal untuk memotong seccomp atau audit mekanisme perlindungan melalui aplikasi dibuat yang menggunakan (1) garpu atau (2) dekat system call, seperti yang ditunjukkan oleh serangan terhadap seccomp sebelum 3.16.
CVE-2015-1805	(1) pipe_read dan (2) implementasi pipe_write di fs / pipe.c di kernel Linux sebelum 3.16 tidak benar mempertimbangkan efek samping dari panggilan __copy_to_user_inatomic dan __copy_from_user_inatomic gagal, yang memungkinkan pengguna lokal untuk menyebabkan penolakan layanan (sistem crash) atau mungkin mendapatkan hak melalui aplikasi dibuat, alias "I / O vektor berbagai overrun."
CVE-2014-7822	Pelaksanaan operasi file splice_write tertentu dalam kernel Linux sebelum 3.16 tidak menegakkan pembatasan pada ukuran maksimum file tunggal, yang memungkinkan pengguna lokal untuk menyebabkan penolakan layanan (system crash) atau mungkin memiliki dampak lain yang tidak ditentukan melalui dibuat sambatan system call, seperti yang ditunjukkan oleh penggunaan file descriptor terkait dengan filesystem ext4.

- **Linux 2.6.32**

Berdasarkan gambar 6, prediksi target menggunakan sistem operasi linux 2.6.32 yaitu 86 %

Name	Description
CVE-2013-2239	vzkernel sebelum 042stab080.2 dalam modifikasi OpenVZ untuk kernel Linux 2.6.32 tidak menginisialisasi variabel panjang tertentu, yang memungkinkan pengguna lokal untuk mendapatkan informasi sensitif dari kernel stack memori melalui (1) panggilan pengemudi ploop ioctl dibuat, terkait dengan ploop_getdevice_ioc yang fungsi dalam driver / blok / ploop / dev.c, atau (2) dibuat system call quotactl, terkait dengan fungsi compat_quotactl di fs / kuota / quota.c.
CVE-2013-2224	Sebuah Red Hat Patch tertentu untuk kernel Linux 2.6.32 pada Red Hat Enterprise Linux (RHEL) 6 memungkinkan pengguna lokal untuk menyebabkan penolakan layanan (operasi bebas yang tidak valid dan sistem crash) atau mungkin mendapatkan hak melalui panggilan sistem sendmsg dengan IP_RETOPTS pilihan, seperti yang ditunjukkan oleh hemlock.c. CATATAN: kerentanan ini ada karena memperbaiki yang salah untuk CVE-2012-3552.
CVE-2011-3593	Sebuah Red Hat Patch tertentu untuk fungsi vlan_hwaccel_do_receive di net / 8021q / vlan_core.c di kernel Linux 2.6.32 pada Red Hat Enterprise Linux (RHEL) 6 memungkinkan penyerang remote untuk menyebabkan penolakan layanan (sistem crash) melalui prioritas-tag VLAN frame.
CVE-2011-2189	net / core / net_namespace.c di kernel Linux 2.6.32 dan sebelumnya tidak benar menangani tingkat tinggi penciptaan dan pembersihan dari ruang nama jaringan, yang membuatnya lebih mudah bagi penyerang remote untuk menyebabkan penolakan layanan (konsumsi memori) melalui permintaan untuk daemon yang membutuhkan namespace terpisah per sambungan, seperti yang ditunjukkan oleh vsftpd.
CVE-2011-1576	Generic Menerima offload (GRO) pelaksanaan di kernel Linux 2.6.18 pada Red Hat Enterprise Linux 5 dan 2.6.32 pada Red Hat Enterprise Linux 6, seperti yang digunakan dalam Red Hat Enterprise Virtualization (RHEV) Hypervisor dan produk lainnya, memungkinkan penyerang jarak jauh menyebabkan penolakan layanan melalui paket VLAN dibuat yang diproses oleh fungsi napi_reuse_skb, yang mengarah ke (1) kebocoran memori atau (2) korupsi memori, kerentanan yang berbeda dari CVE-2011-1478.

Name	Description
CVE-2011-1020	Pelaksanaan proc filesystem di kernel Linux 2.6.37 dan sebelumnya tidak membatasi akses ke / proc direktori pohon proses setelah proses ini melakukan suatu exec dari program setuid, yang memungkinkan pengguna lokal untuk mendapatkan informasi sensitif atau menyebabkan penolakan layanan via terbuka, lseek, membaca, dan menulis panggilan sistem.
CVE-2011-0714	Gunakan-setelah-bebas kerentanan dalam Red Hat Patch tertentu untuk RPC soket server yang fungsi dalam kernel Linux 2.6.32 pada Red Hat Enterprise Linux (RHEL) 6 mungkin memungkinkan penyerang remote untuk menyebabkan penolakan layanan (crash) melalui data yang cacat dalam paket, yang berkaitan dengan lockd dan fungsi svc_xprt_received.
CVE-2010-1636	Fungsi btrfs_ioctl_clone di fs / btrfs / ioctl.c dalam fungsi btrfs di kernel Linux 2.6.29 melalui 2.6.32, dan mungkin versi lain, tidak menjamin bahwa file descriptor kloning telah dibuka untuk membaca, yang memungkinkan pengguna lokal untuk membaca informasi sensitif dari file descriptor write-only.
CVE-2010-1083	Fungsi processcompl_compat di driver / usb / inti / devio.c di kernel 2.6.x Linux melalui 2.6.32, dan versi kemungkinan lain, tidak jelas transfer penyangga sebelum kembali ke userspace ketika perintah USB gagal, yang mungkin membuatnya lebih mudah untuk fisik penyerang proksimat untuk mendapatkan informasi sensitif (memori kernel).
CVE-2009-4308	Fungsi ext4_decode_error di fs / ext4 / super.c di filesystem ext4 di kernel Linux sebelum 2.6.32 memungkinkan dibantu pengguna penyerang remote untuk menyebabkan penolakan layanan (NULL pointer dereference), dan mungkin memiliki dampak lain yang tidak ditentukan, melalui dibuat hanya-baca filesystem yang tidak memiliki jurnal.
CVE-2009-4020	berdasarkan tumpukan-buffer overflow dalam subsistem HFS di kernel Linux 2.6.32 memungkinkan penyerang remote untuk memiliki dampak yang tidak ditentukan melalui dibuat hirarkis File System (HFS) filesystem, terkait dengan fungsi hfs_readdir di fs / HFS / dir.c.
CVE-2009-1298	Fungsi ip_frag_reasm di net / ipv4 / ip_fragment.c di Linux kernel 2.6.32-RC8, dan 2.6.29 dan versi sebelumnya 2.6.32, panggilan IP_INC_STATS_BH dengan argumen yang salah, yang memungkinkan penyerang remote untuk menyebabkan penolakan layanan (NULL pointer dereference dan menggantung) melalui paket IP yang lama, kemungkinan berhubungan dengan fungsi ip_defrag.

- **Wyse ThinOS**

Berdasarkan gambar 6, prediksi target menggunakan sistem operasi Wyse ThinOS yaitu 85 %

Name	Description
CVE-2010-3031	Buffer overflow in Wyse ThinOS HF 4.4.079i, and possibly other versions before ThinOS 6.5, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long string to the LPD service.

- **Linux 3.10 - 3.12**

Berdasarkan gambar 6, prediksi target menggunakan sistem operasi Linux 3.10 - 3.12 yaitu 85 %

Name	Description
CVE-2014-5332	Race condition in NVMap in NVIDIA Tegra Linux Kernel 3.10 allows local users to gain privileges via a crafted NVMAP_IOC_CREATE IOCTL call, which triggers a use-after-free error, as demonstrated by using a race condition to escape the Chrome sandbox.
CVE-2013-2164	The mmc_ioctl_cdrom_read_data function in drivers/cdrom/cdrom.c in the Linux kernel through 3.10 allows local users to obtain sensitive information from kernel memory via a read operation on a malfunctioning CD-ROM drive.

- **Android 5.0.1**

Berdasarkan hasil entri dari CVE untuk system operasi Android 5.0.1 terdapat 3011 CVE entri. Pada tugas ini, penulis hanya menyajikan beberapa entri CVE untuk OS Android 5.01.

Name	Description
CVE-2017-5606	Pelaksanaan yang tidak benar "XEP-0280: Message Karbon" di beberapa klien XMPP memungkinkan penyerang remote untuk meniru setiap pengguna, termasuk kontak, pada layar aplikasi rentan ini. Hal ini memungkinkan untuk berbagai jenis serangan rekayasa sosial. CVE ini adalah untuk Xabber (hanya jika diaktifkan secara manual: 1.0.30, 1.0.30 VIP, beta 1.0.3 - 1.0.74; Android).

Name	Description
CVE-2017-5589	Pelaksanaan yang tidak benar "XEP-0280: Message Karbon" di beberapa klien XMPP memungkinkan penyerang remote untuk meniru setiap pengguna, termasuk kontak, pada layar aplikasi rentan ini. Hal ini memungkinkan untuk berbagai jenis serangan rekayasa sosial. CVE ini adalah untuk yaxim dan Bruno (0.8.6 - 0.8.8; Android).
CVE-2017-5027	Blink di Google Chrome sebelum 56.0.2924.76 untuk Linux, Windows dan Mac, dan 56.0.2924.87 untuk Android, gagal untuk menegakkan aman-inline kebijakan keamanan konten, yang memungkinkan penyerang remote untuk memotong kebijakan keamanan konten melalui halaman HTML dibuat.
CVE-2017-5023	Ketik kebingungan dalam Histogram di Google Chrome sebelum 56.0.2924.76 untuk Linux, Windows dan Mac, dan 56.0.2924.87 untuk Android, memungkinkan penyerang remote untuk berpotensi mengeksploitasi dekat nol dereference melalui halaman HTML dibuat.
CVE-2017-5022	Blink di Google Chrome sebelum 56.0.2924.76 untuk Linux, Windows dan Mac, dan 56.0.2924.87 untuk Android, gagal untuk menegakkan aman-inline kebijakan keamanan konten, yang memungkinkan penyerang remote untuk memotong kebijakan keamanan konten melalui halaman HTML dibuat.
CVE-2017-5021	Sebuah digunakan setelah bebas di Google Chrome sebelum 56.0.2924.76 untuk Linux, Windows dan Mac, dan 56.0.2924.87 untuk Android, memungkinkan penyerang remote untuk melakukan keluar dari memori batas dibaca melalui halaman HTML dibuat.
CVE-2017-5020	Google Chrome sebelum 56.0.2924.76 untuk Linux, Windows dan Mac, dan 56.0.2924.87 untuk Android, gagal membutuhkan sikap pengguna untuk operasi download yang kuat, yang memungkinkan penyerang remote yang meyakinkan pengguna untuk menginstal ekstensi berbahaya untuk mengeksekusi kode arbitrary melalui halaman HTML dibuat.
CVE-2017-5019	Sebuah digunakan setelah bebas di Google Chrome sebelum 56.0.2924.76 untuk Linux, Windows dan Mac, dan 56.0.2924.87 untuk Android, memungkinkan penyerang remote untuk berpotensi mengeksploitasi korupsi tumpukan melalui halaman HTML dibuat.
CVE-2017-5018	Google Chrome sebelum 56.0.2924.76 untuk Linux, Windows dan Mac, dan 56.0.2924.87 untuk Android, memiliki kebijakan keamanan konten kurang ketat pada halaman peluncur aplikasi Chrome, yang memungkinkan penyerang remote untuk menyuntikkan script atau HTML ke dalam halaman istimewa melalui halaman HTML dibuat.

Name	Description
CVE-2017-5016	Blink di Google Chrome sebelum 56.0.2924.76 untuk Linux, Windows dan Mac, dan 56.0.2924.87 untuk Android, gagal mencegah elemen UI tertentu dari yang ditampilkan oleh halaman non-terlihat, yang memungkinkan penyerang remote untuk menunjukkan elemen UI tertentu pada halaman mereka tidak mengontrol melalui halaman HTML dibuat.
CVE-2017-5015	Google Chrome sebelum 56.0.2924.76 untuk Linux, Windows dan Mac, dan 56.0.2924.87 untuk Android, salah ditangani mesin terbang Unicode, yang memungkinkan penyerang remote untuk melakukan domain spoofing melalui homographs IDN dalam nama domain dibuat.
CVE-2017-5014	Tumpukan buffer overflow selama pemrosesan gambar di Skia di Google Chrome sebelum 56.0.2924.76 untuk Linux, Windows dan Mac, dan 56.0.2924.87 untuk Android, memungkinkan penyerang remote untuk melakukan keluar dari memori batas dibaca melalui halaman HTML dibuat.
CVE-2017-5012	Sebuah meluap tumpukan buffer di V8 di Google Chrome sebelum 56.0.2924.76 untuk Linux, Windows dan Mac, dan 56.0.2924.87 untuk Android, memungkinkan penyerang remote untuk berpotensi mengeksploitasi korupsi tumpukan melalui halaman HTML dibuat.