Vulnerability Mapping pada Jaringan Komputer di Universitas X

Devi Christiani Angir[1], Agustinus Noertjahyana[2], Justinus Andjarwirawan [3]
Program Studi Teknik Informatika, Fakultas Teknologi Industri, Universitas Kristen Petra
Jl. Siwalankerto 121-131, Surabaya 60236
Telp (031) – 2983455, Fax. (031) - 8417658
devichristianii@gmail.com[1], agust@petra.ac.id[2], justin@petra.ac.id [3]

ABSTRAK

Universitas X saat ini bertumbuh semakin besar dan memiliki berbagai macam sistem informasi dalam menjalankan kegiatan operasionalnya. Salah satu *server* yang paling penting di Universitas X adalah www.xyz.ac.id. *URL* tersebut adalah salah satu *URL* yang sering dikunjungi oleh masyarakat luar untuk mengenal Universitas X lebih dekat secara umum. Keamanan *web server* biasanya merupakan masalah dari seorang *administrator*. Seringkali masalah keamanan sistem aplikasi maupun *web server* terabaikan dan pentingnya pengamanan baru disadari setelah terjadi bencana. Tanpa pengamanan sistem aplikasi yang baik, penerapan teknologi sehebat apapun akan sangat membahayakan institusi atau organisasi itu sendiri. Oleh karena itu, dibutuhkan evaluasi keamanan *server* dan melakukan *mapping vulnerability* untuk lebih mewaspadai keamanan *server*.

Berdasarkan latar belakang permasalahan itu, maka dibutuhkan evaluasi dengan menggunakan metode *penetration testing*. Selain itu, penelitian ini juga menggunakan pedoman dari modul *CEH (Certified Ethical Hacker)* dan *web* resmi acunetix. Pengujian skripsi ini adalah bertujuan untuk menemukan kelemahan *server* pada Universitas X yang ada. Beberapa masalah yang ditemukan setelah pengujian, antara lain: kelemahan yang ditemukan cukup banyak dimana setiap kelemahan yang ada mempunyai penanganan yang berbeda, *port* yang seharusnya tidak terbuka malah terbuka, dan *IP public* yang kurang penting sebaiknya tidak terbuka.

Solusi yang diberikan untuk mengatasi permasalahan tersebut antara lain*:* penggunaan standar acunetix ini dapat dipertahankan dan dilanjutkan, pengujian akan lebih baik dilakukan lebih dari 1 kali, melakukan *upgrade web server* ke versi yang lebih baru secara berkala, melakukan *filter port* yang ada, meningkatkan tingkat keamanan *web server*, *maintenance* secara berkala, dan melakukan pengujian keamanan secara rutin dan berkala, baik dengan berkonsultasi kepada bidang terkait maupun menggunakan suatu panduan (seperti acunetix, CEH, OWASP).

Kata Kunci: *Vulnerability, Penetration testing, Vulnerability Scanning, Certified Etchical Hacker,* Acunetix

ABSTRACT

X University is now growing increasingly large and has a wide variety of information systems to run its operations. One of the most important servers in X University is www.xyz.ac.id. That URL is one of the URLs that are frequented by the public outside to get to know closer about X University in general. Security of web server is usually a matter of an administrator. Sometimes, security issues or server application system and the importance of securing web server neglected only realized after the disaster. Without a good security application systems, the application of technology would be very dangerous as good as any institution or organization itself. Therefore, it takes a server security evaluation and conduct vulnerability mapping to be wary of the security server.

Based on the background of the problem, it is necessary to evaluate by using penetration testing. In addition, this study also uses the guidelines of the module CEH (Certified Ethical Hacker) and the official web Acunetix. Testing of this thesis is aimed to find the weaknesses of existing servers. Some problems were found after testing, among others: the weaknesses found pretty much where any weaknesses have different handling, ports should not be open even open, and less important public IP should not be open.

The solution provided to overcome these problems include: the use of Acunetix standards can be maintained and continued, testing will be done more than one time, to upgrade web server to a newer version periodically, to filter the existing port, increasing the level of web security server, periodic maintenance, and security testing regularly and periodically, either by consulting the relevant field or using a guide (like Acunetix, CEH, OWASP).

***Keywords**: Vulnerability, Penetration testing, Vulnerability Scanning, Certified Etchical Hacker, Acunetix*

1. PENDAHULUAN

Suatu organisasi yang menjalankan kegiatan operasional yang berbasis teknologi informasi pasti akan menggunakan jaringan komputer. Organisasi yang ada pada jaman ini sudah banyak yang menggunakan *server*. Maka, sebuah organisasi perlu memperhatikan faktor keamanan dalam jaringan yang dimiliki. Organisasi melakukan investasi pada sistem keamanan jaringan untuk melindungi aset terhadap ancaman yang ada dari para *hacker*. Keamanan jaringan komunikasi mutlak diperlukan untuk mampu memberikan layanan terus menerus bagi para penggunanya.

Untuk dapat mengurangi kerugian yang diakibatkan oleh para *hacker* yang merugikan, maka langkah awal yang harus dikembangkan adalah melakukan pengamatan dan evaluasi terhadap keamanan *server*.

World wide web merupakan bagian dari internet telah menjadi bagian dari kehidupan manusia, dimana sebuah *web* menjadi sumber informasi yang sangat dibutuhkan dikarenakan dapat menyajikan informasi yang diinginkan secara mudah, cepat, dan murah.

Pada perkembangannya, *web* telah meluas fungsinya. Di era sebelumnya penyajian informasi bersifat statis, setelah berkembangnya teknologi aplikasi berbasis *web* penyajian informasi menjadi bersifat lebih dinamis. Ketika informasi yang dimiliki relatif kecil, proses pencarian informasi dapat berjalan relatif mudah, akan tetapi ketika jumlah informasi yang disajikan semakin banyak, maka proses pencarian dan penampilan informasi tersebut ke dalam halaman *web* juga akan menjadi kendala tersendiri dan aplikasi harus dapat merespon akan hal ini.

Teknologi ini membawa perubahan yang signifikan dalam proses pembangunan sistem penyedia layanan dalam jaringan internet. Teknologi ini memampukan penyedia layanan untuk memberikan layanan yang lebih inovatif. Namun dibalik keuntungan itu semua, teknologi ini memiliki permasalahan dari segi keamanan.

Selain itu, dengan berkembangnya *www* dan Internet, menyebabkan pergerakan sistem informasi untuk menggunakannya sebagai basis. Banyak sistem yang tidak terhubung ke Internet tetapi tetap menggunakan basis *web* sebagai basis untuk sistem informasinya yang dipasang di jaringan Intranet. Untuk itu, keamanan sistem informasi yang berbasis *web* dan teknologi Internet bergantung kepada keamanan sistem *web* tersebut.

Keamanan *web server* biasanya merupakan masalah dari seorang *administrator*. Dengan memasang *web server* di sistem, maka membuka akses kepada orang luar. Apabila *server* terhubung ke Internet dan memang *web server* disiapkan untuk publik, maka harus lebih berhati-hati sebab membuka pintu akses ke seluruh dunia.

Seringkali masalah keamanan sistem aplikasi terabaikan dan pentingnya pengamanan baru disadari setelah terjadi bencana. Tanpa pengamanan sistem aplikasi yang baik, penerapan teknologi sehebat apapun akan sangat membahayakan institusi atau organisasi itu sendiri.

Vulnerability adalah suatu kelemahan yang mengancam nilai *integrity*, *confidentiality*, dan *availability* dari suatu aset. *Penetration testing* atau yang lebih dikenal dengan sebutan *pentest* adalah salah satu metode yang dapat digunakan untuk melakukan evaluasi terhadap suatu jaringan komputer. Selain itu, *mapping* terhadap *vulnerability* juga perlu dilakukan.

Universitas X saat ini bertumbuh semakin besar dan memiliki berbagai macam sistem informasi dalam menjalankan kegiatan operasionalnya[7]. Salah satu *server* yang paling penting di Universitas X adalah www.xyz.ac.id. *Web* tersebut adalah salah satu *web* yang sering dikunjungi oleh masyarakat luar untuk mengenal Universitas X lebih dekat secara umum.

Oleh karena itu, dengan melakukan *mapping vulnerabilities*, maka administrator Universitas X dapat lebih waspada terhadap kelemahan yang ada. Selanjutnya, administrator dapat melakukan maintenance untuk mencegah hal serupa terjadi kembali.

2. LANDASAN TEORI

2.1 Keamanan Jaringan

Satu hal yang perlu diingat bahwa tidak ada jaringan yang anti sadap atau tidak ada jaringan komputer yang benar-benar aman. Sifat dari jaringan adalah melakukan sebuah komunikasi. Setiap komunikasi dapat jatuh ke tangan orang lain dan dapat disalahgunakan. Sistem keamanan membantu mengamankan jaringan tanpa menghalangi penggunaannya dan menempatkan antisipasi ketika jaringan berhasil ditembus.

Keamanan jaringan ini dapat bertujuan untuk agar pemilik sistem informasi dapat menjaga sistem informasinya tidak ditembus atau disusupi oleh orang lain yang pada akhirnya dapat merusak sistem. Adapun tipe dari penyusup ini dapat berupa: *the curious*, *the malicious*, *the high-profile intruder*, dan *the competition.* [9]
Jenis-jenis segi keamanan jaringan yang ada antara lain: *confidentiality*, *integrity*, *availability*, *non-repudiation*, *authentication*, dan *accountability*. *Digital Signature* adalah salah satu teknologi yang digunakan untuk meningkatkan keamanan jaringan dan berfungsi untuk memastikan bahwa tidak ada data yang berubah. Cara kerja *digital signature* dilihat telah memenuhi salah satu syarat keamanan jaringan, yaitu *Non-repudiation*. [6]

2.2 Hacking

Hacking adalah paduan antara seni dan ilmu, untuk orang-orang yang mencoba masuk ke jaringan yang dilindungi ataupun tidak dilindungi. Hal ini dapat dikatakan sebagai seni namun bila dilakukan dengan tidak etis, umumnya cenderung untuk mencuri informasi pribadi, mengubah data keuangan perusahaan, menelusuri kode keamanan untuk mendapatkan akses jaringan yang tidak sah.
Ada dua jenis orang-orang yang menikmati *hacking* komputer, yaitu orang-orang yang mengembangkan minat dalam *hacking* komputer dari keingintahuan secara intelektual sederhana, dan lainnya dengan motif yang kurang mulia. Tapi sifat-sifat umum di antara semua *hacker* adalah memiliki kecerdasan teknologi, berani mengambil risiko, dan memiliki semangat tentang berbagai bahasa pemrograman.

Hacking komputer selalu melibatkan beberapa tingkat pelanggaran atas privasi orang lain dan melanggar keamanan jaringan. Hal ini karena para *hacker* menyebabkan kerusakan pada *file* rahasia dan halaman *website* atau perangkat lunak. Dampak yang dihasilkan dari kegiatan tersebut bervariasi dari yang sekadar ingin tahu sampai pada kegiatan ilegal. Namun, banyak perusahaan besar seringkali menyewa sebuah tim *hacker* untuk menyelidiki celah keamanan jaringan yang dimiliki.

Pada dasarnya ada tiga jenis *hacker* tergantung pada *domain* dari pekerjaan seseorang. Adapun beberapa *hacker* itu antara lain:

1. *White hat hacker*, merupakan orang yang menulusuri atau memecah sistem keamanan komputer untuk tujuan yang tidak berbahaya. Tujuan-tujuan ini berkisar pada pengujian sistem keamanan untuk menemukan celah besar dalam jaringan. Orang-orang seperti biasanya mengikuti cara yang sah dan bekerja dalam wilayah hukum *cyber*.
2. *Black hat hacker*. *Black hat hacker* umumnya menumbangkan keamanan komputer tanpa otorisasi dengan bantuan berbagai *virus* dan *hacking tools* lainnya. *Hacker* ini menggunakan teknologi untuk penipuan vandalisme, kartu kredit, atau pencurian identitas.
3. *Grey hat hacker*. *Grey hat hacker* merupakan bagian pertengahan jalan antara *black hat hacker* dan *white hat hacker*.

2.3 Penetration Testing (Pentest)

Penetration Testing adalah salah satu komponen penting dari *Security Audit* di mana merupakan metode untuk mengevaluasi keamanan sistem komputer atau jaringan dengan mensimulasikan serangan dari sumber yang berbahaya. Hal ini dapat diberikan

contoh seperti serangan yang dilakukan oleh *black hat hacker*, c*racker*, *defacer*, dan sebagainya.

Proses ini melibatkan analisis aktif terhadap sistem untuk setiap kerentanan potensial yang diakibatkan oleh sistem yang lemah atau konfigurasi sistem yang tidak benar atau kelemahan operasional dalam proses teknis. Masalah keamanan yang ditemukan akan disampaikan kepada pemilik sistem bersama dengan penilaian dampak dan mitigasi (solusi teknis) dari setiap kerentanan yang ditemukan.

Tipe untuk melakukan suatu *penetration testing* ada 2 macam [4]. Kedua macam itu antara lain:

1. *External Testing. External Testing* adalah *testing* dengan melakukan analisa terhadap informasi *public* yang tersedia, *network enumeration phase*, dan analisa keamanan *devices* yang digunakan.
2. *Internal Testing. Internal Testing* adalah *testing* yang akan menampilkan jumlah *network access points* yang mewakili beberapa *logical* dan *physical segment.*

Ada beberapa metode untuk melakukan *Penetration Testing* yang bisa digunakan, antara lain: *passive penetration testing, active penetration testing*, dan aggressive *penetration testing.*

Pada *penetration testing* di Universitas X ini, metode yang dilakukan adalah metode *passive penetration testing* dimana melakukan pengujian terhadap jaringan *server* Universitas X. (*domain*: www.xyz.ac.id) dengan melakukan *scanning range IP Address*.

Pada Gambar 1 dapat dilihat *penetration testing phases*. Fase dalam *penetration testing* ini melakukan mulai dari pengumpulan data sampai melakukan laporan, dimana bertujuan untuk mencari kelemahan dalam suatu sistem sebuah organisasi yang di evaluasi atau di *testing*.

Table 18-13
Penetration Testing Phases

Phase	Activities
1. Discovery	Acquire and evaluate information relevant to the organization and systems to be tested.
2. Enumeration	Acquire IDs, versions of software installed, and information concerning the network to be tested.
3. Vulnerability mapping	Characterize the information system environment and identify its vulnerabilities.
4. Exploitation	Try to exploit the system vulnerabilities and gain access privileges to the target system. Care is taken not to cause harm to the system or its information.
5. Report generation	Produce an executive overview report for management that profiles the network security posture and results of remediation activities, and generate an IT technical report for IT staff that details threats to the network, corresponding vulnerabilities discovered during testing, and remediation recommendations.

Gambar 1 *Penetration Testing Phases* [5]

2.4 Web Vulnerability Scanner

2.1.1 *Web*

Web adalah alamat atau lokasi di dalam *internet* suatu halaman *web*, umumnya membuat dokumen *HTML* dan dapat berisi sejumlah foto atau gambar grafis, musik, teks bahkan gambar yang bergerak dan dapat diakses selama 24 jam.

2.1.2 Database

Database adalah representasi kumpulan fakta yang saling berhubungan disimpulkan secara bersama sedemikan rupa dan tanpa pengulangan (redudansi) yang tidak perlu, untuk memenuhi berbagai kebutuhan. Data disimpan di dalam basis data dan perlu diorganisasikan sedemikan rupa supaya informasi yang dihasilkan berkualitas. Organisasi basis data yang baik juga berguna untuk efisiensi kapasitas penyimpanannya. Basis data tersusun atas bagian yang disebut *field* dan *record* yang tersimpan dalam sebuah *file*.

2.1.3 Vulnerability Scanner

Vulnerability scanner adalah sebuah program komputer yang di desain untuk mencari dan memetakan sistem untuk kelemahan pada aplikasi, komputer atau jaringan. Meningkatnya penggunaan internet membuat semakin banyaknya *website* yang bermunculan. Namun sangat disayangkan kejahatan internet terus meningkat seiring bermunculannya ragam artikel yang membahas masalah *hacking*.

2.1.4 Vulnerability research and tools

Vulnerability research merupakan salah satu cara untuk mengasah dan mengikuti perkembangan dalam dunia kegiatan *hacking*. *Vulnerability research* merupakan proses menemukan dan mencari kelemahan yang memungkinkan suatu sistem di-*hack*.

2.5 CEH (Certified Ethical Hacker)

CEH merupakan salah satu sertifikasi *IT Security*, dimana seseorang yang memegang sertifikat tersebut bertanggung jawab seumur hidup terhadap ilmu yang sudah dia miliki. Setiap pemegang sertifikat mempunyai *unique number* yang sudah terdaftar atas namanya. Seorang *CEH certified* biasanya dipercaya untuk mengelola jaringan atau sistem komputer menggunakan metode yang sama dengan metode seorang *hacker*. [8]

Seiring dengan semakin pentingnya keamanan komputer, kebutuhan akan profesional dibidang keamanan komputer semakin dibutuhkan. *CEH* adalah sertifikat profesional di bidang keamanan komputer yang dikeluarkan oleh Council of E-Commerce Consultants (EC-Council) yang diakui secara internasional.

Tujuan dari serifikasi ini adalah menciptakan orang-orang yang paham dan mengerti cara kerja serta memiliki kemampuan yang sama dengan hacker.

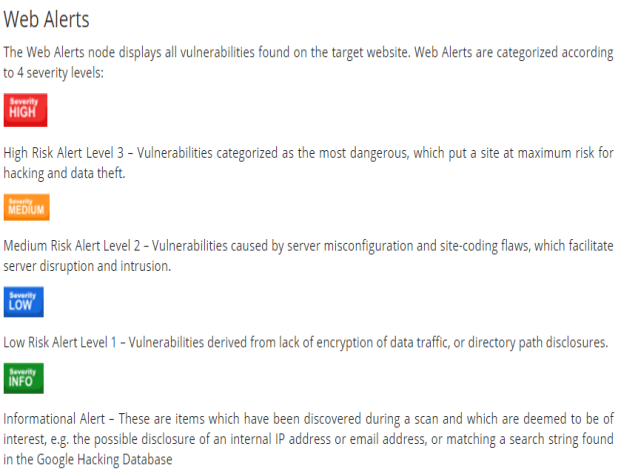
Sebuah etika *hacker* biasanya digunakan oleh sebuah organisasi yang percaya dia untuk mencoba menembus jaringan dan/atau sistem komputer, dengan menggunakan metode yang sama seperti seorang *hacker*, untuk tujuan menemukan dan memperbaiki kerentanan keamanan komputer. [10]

2.6 Acunetix (http://www.acunetix.com/)

Keamanan *website* mungkin aspek yang paling diabaikan saat ini. Padahal mengamankan perusahaan harus menjadi prioritas utama dalam setiap organisasi. *Hacker* berkonsentrasi mengusahakan upaya mereka pada aplikasi berbasis *web* (seperti *shopping cart*, *forms*, *login page*). *Web applications* dapat diakses 24 jam sehari, 7 hari seminggu dan bertugas untuk mengontrol data berharga karena *web applications* mempunyai akses langsung, seperti *database* pelanggan. *Web application* sering dibuat namun kurang dilakukan pengujian sehingga lebih mungkin mempunyai kerentanan yang kurang diperhatikan. Acunetix Web Vulnerability Scanner otomatis memeriksa *web application* terhadap *SQL Injection , XSS*, dan kerentanan *web* lainnya. [14]

Tool Acunetix Web Vulnerability Scanner 9.5 yang digunakan pada skripsi ini juga dapat menampilkan level dari hasil *scanning*.

Pada Gambar 2 dapat dilihat *severity levels* dari acunetix yang akan menjelaskan tingkat keamanan dari *URL* atau *IP address* yang di-*scanning*.



Gambar 2 Level *tool* Acunetix [13]

2.7 Range IP Address

Range IP Address adalah suatu jarak jangkauan sebuah *IP Address*. *Range IP Address* ini dapat dicari dengan cara menghitung *broadcast address* dan *network address* dari *IP Address* yang dimiliki.

2.8 MAC (Media Access Control) Layer

MAC layer adalah sebuah *subset* dari *link layer*, yang merupakan *physical layer* pada jaringan berbasis *IP*. *Layer 1* pada jaringan 802.11 menampilkan 3 fungsi essensial, antara lain:

- *Servers* sebagai *interface* antara *MAC layer* pada 2 atau lebih *geographic locations*. *Geographic locations* secara umum hanya beberapa ratus meter.
- Melakukan *actual sensing* untuk CSMA/CA *(Carrier Sense Multiple Access/Collision Avoidance) events*, yang terjadi pada *MAC layer*.
- Melakukan modulasi dan demodulasi *signal* antara 2 *geographic points* dimana 802.11 *equipment* berada.

2.9 TTL (Time to Live)

TTL adalah nilai waktu termasuk dalam paket yang dikirim melalui *TCP/IP* berbasis jaringan yang memberitahu penerima berapa lama waktu untuk terus atau menggunakan paket atau data yang dimasukkan sebelum waktunya habis dan membuang paket atau data.

Time-to-Live (TTL) telah diubah namanya pada *IP* versi 6. Dalam hal ini disebut *hop limit* dan memiliki fungsi yang sama seperti pada *TTL* di *IPv4*. Nilai dari *TTL* akan muncul pada beberapa utilitas jaringan seperti *Ping, traceroute*, dan utilitas jaringan *Path Ping* untuk mencoba untuk mencapai komputer *host* yang diberikan atau untuk melacak rute ke *host* tersebut. [11]

2.10 Hostname

Hostname adalah nama komputer. Pemberian nama ini spesifik, untuk satu komputer tertentu saja dalam suatu jaringan. Jika terjadi penamaan yang sama, maka sistem akan memberitahukan bahwa telah terjadi duplikasi nama. Tapi jika komputer tidak saling terkoneksi ke jaringan memberikan nama komputer yang sama tidak masalah.

Sebuah *hostname* adalah label yang diberikan ke perangkat yang terhubung ke jaringan komputer dan yang digunakan untuk mengidentifikasi perangkat dalam berbagai bentuk komunikasi elektronik seperti *World Wide Web*, *e-mail* atau *Usenet*. *Hostname* mungkin nama sederhana yang terdiri dari sebuah kata atau frase tunggal, atau mereka mungkin telah ditambahkan nama domain, yang merupakan nama dalam *Domain Name System (DNS)*, dipisahkan dari label tertentu *host* dengan titik (dot).

2.11 Port

Menciptakan sebuah jaringan komputer yang handal tentunya diperlukan kemampuan menganalisa dan memahami setiap karakteristik dan topologi jaringan komputer yang akan dibuat. Salah satu yang sangat berperan penting disini adalah penomoran *port* dan fungsinya pada jaringan komputer. [12]

Dalam jaringan komputer, *port* adalah sebuah titik spesifik dalam komunikasi antar *host* pada jaringan komputer. Sebuah *port* berhubungan langsung dengan alamat *IP* dari *host* serta jenis protokol yang digunakan dalam komunikasi jaringan.

Secara gampangnya, *port* ini bisa disebutkan sebagai jalur tujuan tertentu dari setiap jenis protokol yang berjalan pada jaringan.

Dalam praktiknya, *port* ini terbagi atas tiga kategori, antara lain:

- *Well-known port*, dimulai dari 0 sampai 255, namun diperlebar mendukung 0-1023
- *Registered Port*, dimulai dari 1024 sampai 49151
- *Dynamically Port*, terbentang antara 49152 sampai 65535.

3. ANALISA dan DESAIN SISTEM

3.1 Analisa Permasalahan

Scanning domain untuk *server* www.xyz.ac.id ini memang diperlukan. Hal ini dikarenakan *domain* tersebut merupakan salah satu *domain* yang penting di mana memberikan informasi gambaran secara umum mengenai Universitas X.

Scanning ini dilakukan dengan tujuan untuk mengetahui *vulnerability* yang ada. Dari *range IP address* yang di-*scanning*, nantinya akan diketahui *IP address* yang mempunyai *hostname* dan yang tidak mempunyai *hostname*. Setelah itu di-*scanning* lagi dengan *tools* berbeda untuk melihat kelemahan yang dimiliki. Hasil dari *scanning* ini nantinya dapat memberikan evaluasi kepada pengelola jaringan *server* Universitas X untuk lebih waspada lagi terhadap kelemahan yang ada.

3.2 Analisis Kebutuhan

Alasan dilakukan *penetration testing* pada skripsi ini adalah untuk menemukan titik kelemahan dan *vulnerabilities system* sebelum titik kelemahan tersebut dieksploitasi oleh *hacker* yang akan memberikan dampak buruk bagi keamanan *server* Universitas X (*domain*: www.xyz.ac.id). Selain itu, *penetration testing* ini dilakukan untuk memberikan gambaran bahwa manajemen terhadap sistem keamanan komputer merupakan sebuah hal penting yang harus dilakukan, menguji coba terhadap mekanisme alur keamanan sistem, dan melakukan evaluasi apakah sistem yang digunakan sudah memenuhi standar keamanan sistem komputer.

3.3 Analisa Sistem (*Software*)

Dalam skripsi ini, program aplikasi yang digunakan adalah program yang sesuai dengan metode dalam setiap *step penetration testing*. Pada Tabel 1 dapat dilihat sistem (*software*) yang digunakan untuk penetration testing dalam pengerjaan skripsi ini.

Tabel 1 Tabel sistem yang digunakan untuk skripsi

NO.	*STEP* (METODE)	*TOOLS*
1	***Footprinting***	Angry IP Scanner
2	***Scanning Fingerprinting***	Acunetix Web Vulnerability Scanner 9.5
3	***Enumeration***	Softperfect network scannner

3.4 Komponen Pengerjaan Skripsi

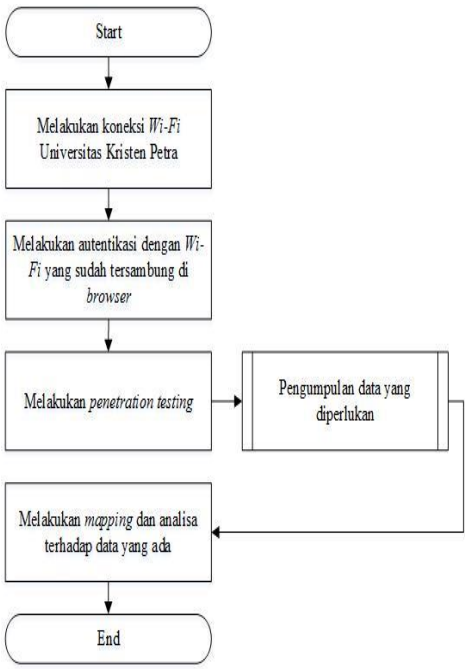
Berikut beberapa komponen yang dibutuhkan untuk penyelesaian skripsi ini. Beberapa komponen tersebut antara lain:

1. Organisasi
   Organisasi yang dianalisa dalam skripsi ini adalah Universitas X Surabaya.
2. *Wi-Fi*
   Wi-Fi terletak di Gedung P lantai 2 Universitas X..
3. Target analisa
   Target yang di-*penetration testing* dan dianalisa dalam skripsi ini adalah *server* Universitas X, dengan *domain* xyz.ac.id.
4. *Range IP Address*
   Pengerjaan pengumpulan data (*penetration testing*) menggunakan *range IP address*. *Range IP Address* tersebut adalah 203.189.xxx.0-203.189.xxx.255.

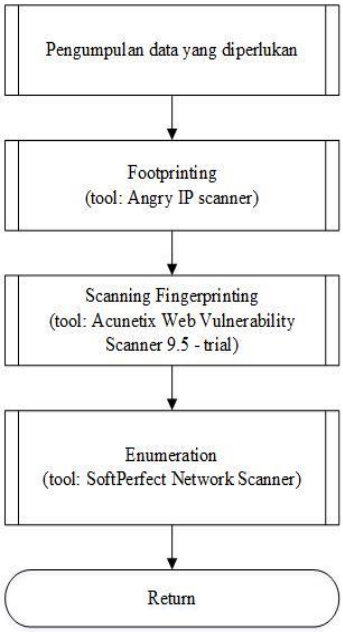
3.5 Penetration Testing

Pada Gambar 4 dapat dilihat hal-hal apa saja yang dilakukan saat melakukan skripsi ini menggunakan metode *penetration testing*. Pengerjaan skripsi ini dimulai dari melakukan koneksi dengan internet sampai melakukan *mapping* kelemahan.

Selanjutnya hal-hal apa saja yang dilakukan saat *penetration testing* dapat dilihat pada Gambar 5.



Gambar 4 Langkah-langkah pengerjaan skripsi



Gambar 5 Langkah-langkah pengerjaan *penetration testing*

3.5.1 *Footprinting*

Merupakan suatu proses yang ingin mengungkap dan mengumpulkan informasi sebanyak mungkin mengenai target jaringan. Tujuan dari melakukan *footprinting* antara lain mengumpulkan informasi mengenai *network* target, sistem informasi target, dan informasi suatu organisasi. [1]
Pada teknik ini, *tool* yang digunakan adalah Angry IP Address.

3.5.2 Scanning Fingerprinting

Scanning fingerprinting adalah salah satu prosedur untuk mengidentifikasi *host*, *port*, dan *services* dalam suatu jaringan. Selain itu, *scanning fingerprinting* merupakan tanda dimulainya sebuah serangan *hacker* (*pre-attack*). Melalui *scanning fingerprinting* ini, *hacker* akan mencari berbagai kemungkinan yang bisa digunakan untuk mengambil alih komputer korban. [2]
Pada skripsi ini, dari jenis *scanning* yang ada, *vulnerability scanning* adalah jenis yang akan digunakan untuk mengevaluasi keamanan dari jaringan server.

3.5.3 Enumeration

Enumeration merupakan suatu proses penggalian untuk mendapatkan *usernames*, nama mesin, *resources*, *shares*, dan *services* dari sebuah sistem. [3]

3.5.3.1 SNMP

SNMP (Simple Network Management Protocol) merupakan salah satu salah satu metode yang digunakan pada langkah *enumeration*. Pada teknik ini, *tool* yang digunakan adalah SoftPerfect network scanner.

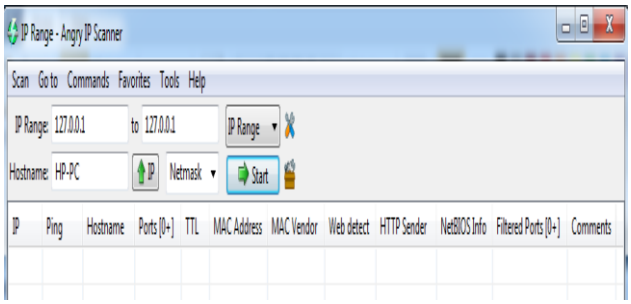
4. PENGUJIAN SISTEM

4.1 Software Penetration Testing

4.1.1 Footprinting

Langkah *footprinting* ini akan menggunakan *tool* Angry IP Scanner di mana tool ini dapat menampilkan detail dari suatu *range IP Address*. Sebagai *system administrator*, *tool* ini sangat membantu dalam menghemat waktu dan pikiran ketika mengawasi jaringan dari tangan jahil yang terhubung ke jaringan. Ketika ada alat (laptop/*workstation*) yang mencurigakan yang terhubung dengan jaringan, dapat langsung mengetahuinya sesegera mungkin.

Pada Gambar 6 dapat dilihat tampilan *tool* Angry IP address.

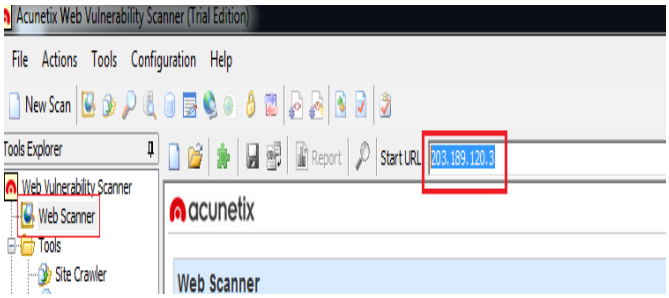


Gambar 6 Tampilan *tool* Angry IP Address

4.1.2 Scanning Fingerprinting

Langkah *scanning fingerprinting* ini akan menggunakan *tool* Acunetix Web Vulnerability Scanner 9.5 di mana *tool* ini dapat menampilkan detail dari suatu *range IP Address*. Sebagai *system administrator*, *tool* ini akan membantu dalam menemukan vulnerability dalam jaringan (*IP address* atau *hostname*). Selain menampilkan kelemahan atau celah dari suatu *source*, *tool* ini akan menampilkan level tingkat kelemahan dari *alerts* (*vulnerability*) yang ditemukan.

Pada Gambar 7 dapat dilihat tampilan *tool vulnerability scanner* (Acunetix Web Vulnerability Scanner 9.5).

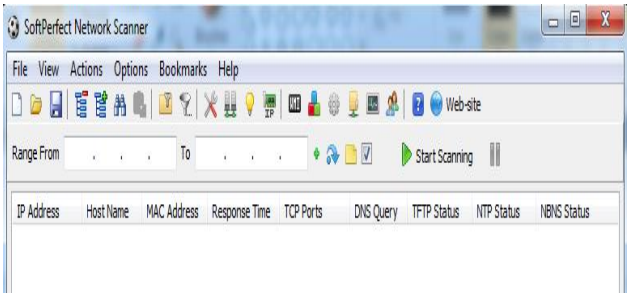


Gambar 7 Tampilan *tool vulnerability scanner* (Acunetix Web Vulnerability Scanner 9.5)

4.1.3 Enumeration

Langkah *enumeration* ini akan menggunakan *tool* SoftPerfect network scanner di mana *tool* ini dapat menampilkan detail dari suatu *range IP Address*, seperti *port* apa saja yang terbuka dari suatu *IP Address*. Jadi, sebagai seorang *tester*, akan dapat melihat dan mengevaluasi *port* yang terbuka apakah *port* tersebut cocok dengan *IP address* yang terkait.

Pada Gambar 8 dapat dilihat tampilan *tool* SoftPerfect network Scanner.



Gambar 8 Tampilan *tool* SoftPerfect network Scanner

4.2 Laporan Hasil Pengujian

Setelah pengumpulan data selesai dari melakukan tahap *penetration testing* (*footprinting*, *scanning fingerprinting*, dan *enumeration*) maka akan direkap untuk dievaluasi dan melakukan *mapping vulnerability* dan mencari solusi agar tidak menimbulkan dampak yang lebih merugikan.

Pada Tabel 2 dapat dilihat hasil pengujian dengan menggunakan *tool* Angry IP Scanner. Hasil ini merupakan hasil setelah direkap yang hanya mempunyai *hostname* saja.

Tabel 2 Hasil *scanning footprinting*

No.	*IP*	*Hostname*
1	203.189.xxx.3	UNITX
2	203.189.xxx.4	peter.xyz.ac.id
3	203.189.xxx.7	jacob.xyz.ac.id
4	203.189.xxx.23	source.xyz.ac.id
5	203.189.xxx.24	john.xyz.ac.id
6	203.189.xxx.35	electrical.xyz.ac.id
7	203.189.xxx.47	mail.xyz.ac.id
8	203.189.xxx.48	debianx.xyz.ac.id
9	203.189.xxx.58	REKNET
10	203.189.xxx.131	sim.xyz.ac.id
11	203.189.xxx.135	PMK-ONLINE
12	203.189.xxx.143	KASPERSKY
13	203.189.xxx.144	WIN2012NFS
14	203.189.xxx.150	opensource.xyz.ac.id
15	203.189.xxx.152	CCIS-REPO
16	203.189.xxx.179	phk.xyz.ac.id
17	203.189.xxx.205	dewey.xyz.ac.id
18	203.189.xxx.141	TUKKDVR02
19	203.189.xxx.8	VCENTER55
20	203.189.xxx.15	NEWLABPUSKOM
21	203.189.xxx.16	CCTVPUSKOM
22	203.189.xxx.17	PERBEKALAN

Tabel 2 Hasil *scanning footprinting* (lanjutan)

No.	*IP*	*Hostname*
23	203.189.xxx.28	FPORTFOLIO
24	203.189.xxx.41	POLIKLINIK
25	203.189.xxx.46	KONSELING

4.3 Summary Vulnerability

Berikut adalah hasil summary dari semua kelemahan yang ditemukan setelah melakukan pengujian:

- Dari semua kelemahan yang ada, kelemahan yang sering disebutkan pada description adalah *XSS*, *SQL injection*, dan kurangnya *CSRF protection*. Pada Tabel 3 dapat dilihat *summary vulnerability* untuk *description* yang paling sering ditemui.

Tabel 3 *Summary vulnerability* kategori *description*

Description				
No.	**Keterangan**	***Vulnerability***	**Total *alerts***	**Tingkat**
1	*Cross Site Scripting (XSS)*	Cross site scripting (verified)	12	*High*
		jQuery cross site scripting	8	*High*
2	*SQL Injection*	Blind SQL Injection	7	*High*
3	*CSRF (Cross Site Request Forgery) protection*	HTML form without CSRF protection	18	*Medium*

- Banyaknya kelemahan yang berdampak pada *denial of service*, dimana serangan ini dapat membuat *server overload*.
- Banyaknya rekomendasi untuk melakukan *upgrade*.

5. KESIMPULAN

Berdasarkan hasil pengujian dapat disimpulkan beberapa hal berikut:

1. *Research* kelemahan dengan menggunakan acunetix dijelaskan dengan detail. Selain itu juga dibagi berdasarkan tingkat level kelemahannya. Berikut level kelemahan yang terbagi pada acunetix beserta kelemahan yang paling banyak terjadi pada pengujian yang telah dilakukan, antara lain:
   - *High* : *Cross site scripting* sebanyak 12
   - *Medium* : *Directory listing* sebanyak 344
   - *Low* : *Session token in URL* sebanyak 53
   - *Informatioal* : *Broken links* sebanyak 85
2. Beberapa *vulnerability* hasil pengujian, diminta untuk melakukan *upgrade* (seperti contoh melakukan *upgrade* Apache maupun *web server* lainnya).
3. Adanya komputer yang menggunakan IP public dan membuka beberapa port yang tidak sesuai dengan fungsinya. Hal ini dapat menyebabkan adanya celah yang dapat dimanffatkan untuk diserang.
4. *Security* yang terdapat pada *domain* xyz.ac.id ditemukan banyak *vulnerability* setelah di-*scanning* dengan *vulnerability scanner*. Ada *hostname* yang mempunyai *vulnerability* cukup banyak, lebih dari 300.
5. *Domain* xyz.ac.id (termasuk *IP address*-nya) tidak dilakukan *update* secara berkala.

6. DAFTAR PUSTAKA

[1] Certified Ethical Hacker v7. 2012. Module 02 – Footprinting and Reconnaissance. *CEH_V7_Module_01.pdf.*

[2] Certified Ethical Hacker v7. 2012. Module 03 – Scanning Networks. *CEH_V7_Module_03.pdf.*.

[3] Certified Ethical Hacker v7. 2012. Module 04 – Enumeration. *CEH_V7_Module_04.pdf.*

[4] Certified Ethical Hacker v7. 2012. Module 19 – Penetration Tetsing. *CEH_V7_Module_19.pdf.*

[5] Dr. Eric Cole, Dr. Ronald Krutz, and James W. Conley. 2009. *Network Security Bible.* USA: Wiley Publishing Inc.

[6] Rafiuddin, R. 2010. *Manajemen Website dan WWW server*. Jakarta: Andi Publisher.

[7] Rusli, H. 2014. *Analysis and Implementation of Operational Security Management on Computer Center, Petra Christian University*. Surabaya: Universitas Kristen Petra.

[8] S'to. 2010. *CEH Certified Ethical Hacker 100% Illegal*. Jakarta: Jasakom.

[9] Sadikin, R. 2012. *Kriptografi Untuk Keamanan Jaringan*. Jakarta: Andi Publisher.

[10] "Certified Ethical Hacker". Retrieved March 12, 2015 from http://it.proxsisgroup.com/2015/01/mengenal-certified-ethical-hacking-ceh/.

[11] "Pengertian TTL". Retrieved March 2, 2015 from http://rizkyagung.com/apa-itu-time-to-live-ttl-pengertian-dan-penjelasan-ttl/.

[12] "Penjelasan Port". Retrieved March 2, 2015 from http://jamboaufa.net/port-nomor-dan-fungsinya-pada-jaringan-komputer/.

[13] "Vulnerability Level Acunetix". Retrieved January 5, 2015 from http://www.acunetix.com/support/docs/wvs/analyzing-scan-results/.

[14] "Vulnerability Scanning". Retrieved March 2, 2015 from http://www.acunetix.com/vulnerabilities/severity.