STMIK Amik Riau

SATIN – Sains dan Teknologi Informasi

journal homepage : http://jurnal.stmik-amik-riau.ac.id

Uji Web Server Universitas Lancang Kuning

Nurliana Nasution
Program Studi Teknik Informatika,
Universitas Lancang Kuning
nurliananst@unilak.ac.id

Mhd. Arief Hasan
Program Studi Teknik Informatika,
Universitas Lancang Kuning
m.arif@unilak.ac.id

Abstrak

Perkembangan Internet yang semakin hari semakin meningkat baik teknologi dan penggunaannya, membawa banyak dampak baik positif maupun negatif. Tentunya untuk yang bersifat positif. Saat ini website merupakan salah satu layanan informasi yang banyak diakses oleh pengguna internet di dunia. Sebagai salah satu layanan informasi maka perlu dibangun website yang mampu menangani permintaan (request) dari banyak pengguna dengan baik. Sifat heterogen dari perangkat lunak dan penyebaran yang terdistribusi memperkenalkan kompleksitas di dalam perangkt lunak yang harus ditangani selama pengujian. Di Universitas Lancang Kuning memiliki website resmi https://unilak.ac.id/, ketika suatu website dapat diakses oleh seluruh pengguna internet meskipun hanya secara terbatas, maka server website pun telah terhubung ke Internet. Oleh sebab itu administrator web dituntut untuk lebih berhati-hati, karena sangat memungkinkan bahwa layanan website tersebut akan disalah gunakan oleh hacker. Hacker sering melakukan aksinya dengan memanfaatkan dan menjadikan layanan website sebagai perantara untuk mendapatkan akses menuju server melalui celah keamanan yang terdapat pada layanan website.

Kata Kunci : Jaringan, Keamanan, Pengujian, Server, Web

1. Pendahuluan

Perkembangan Internet yang semakin hari semakin meningkat baik teknologi dan penggunaannya, membawa banyak dampak baik positif maupun negatif. Tentunya untuk yang bersifat positif, semua harus mensyukurinya karena banyak manfaat dan kemudahan yang didapat dari teknologi ini, misalnya dapat melakukan transaksi perbankan kapan saja dengan e-banking, *E-Commerce* juga membuat lebih mudah melakukan pembelianmaupun penjualan suatu barang tanpa mengenal tempat.

Saat ini website merupakan salah satu layanan informasi yang banyak diakses oleh pengguna internet di dunia. Sebagai salah satu layanan informasi maka perlu dibangun website yang mampu menangani permintaan (*request*) dari banyak pengguna dengan baik.

Aplikasi perangkat lunak web bersifat heterogen membuat tidak dapat terpisahkan secara alami. Keheterogenan ini memperkenalkan komplekssitas di dalam pengintegrasian yang sulit untuk model dan evaluasi. Sifat heterogen dari perangkat lunak dan penyebaran yang terdistribusi memperkenalkan kompleksitas di dalam perangkt lunak yang harus ditangani selama pengujian.

Pengujian untuk salah satu instrumen yang paling penting dalam pengembangan aplikasi web untuk mencapai produk-produk berkualitas tinggi yang memenuhi harapan pengguna. Metode dan pengujian sistematis dari aplikasi Web adalah tindakan penting

yang diberikan penekanan khusus dalam jaminan kualitas. Ini adalah upaya yang bertujuan untuk menemukan kesalahan dan kekurangan dalam perangkat lunak yang diuji, mengamati ekonomi, temporal, dan teknis kendala.

Pengujian dilibatkan dalam setiap tahap siklus pengembangan perangkat lunak dan kegiatan pengujian terkait erat dengan aktivitas pengembangan perangkat lunak. Karena itu, perkembangannya berbeda fase membutuhkan pendekatan yang berbeda pengujian(Vignjevic, Vucicevic, Djukic, & Radin, 2015). Selain itu, *human behavior* dari mahasiswa maupun karyawan ini sendiri juga perlu dilihat mengingat bahwa pelaku *hacking* ini adalah manusia sendiri. Terkadang, *human behavior* yang kurang baik ini dapat membawa dampak buruk baik secara langsung maupun tidak langsung (Pangalila, Noertjahyana, & Andjarwirawan, 2015).

Universitas Lancang Kuning memiliki *website* resmi https://unilak.ac.id/ dan beberapa *website* lainnya, ketika suatu *website* dapat diakses oleh seluruh pengguna internet meskipun hanya secara terbatas, maka *server website* pun telah terhubung ke internet. Oleh sebab itu administrator web dituntut untuk lebih berhati-hati, karena sangat memungkinkan bahwa layanan *website* tersebut akan disalah gunakan oleh *hacker*. *Hacker* sering melakukan aksinya dengan memanfaatkan dan menjadikan layanan *website* sebagai perantara untuk mendapatkan akses menuju *server* melalui celah keamanan yang terdapat pada layanan *website*.

Semakin berkembangnya teknologi Informasi maka untuk aplikasi komputasi dan jaringan menjadi bagian integral bagi lingkungan di perguruan tinggi. Universitas saat ini berada di garis depan kemajuan teknologi. Akses teknologi yang lebih besar menghasilkan lingkungan belajar yang berharga, di sisi lain juga dapat menghasilkan lingkungan komputasi yang rentan dengan ancaman keamanan yang lebih banyak. Kampus universitas membuktikan diri sebagai beberapa tempat paling berteknologi maju di dunia dengan menyediakan fasilitas seperti dukungan *Wi-Fi* yang luas, pembelajaran online dengan menggunakan perangkat lunak perkuliahan, perpustakaan digital, virtualisasi kelas, konferensi web, dll (Joshi & Singh, 2017).

2. Perencanaan dan Penetrasi

Proyek kami ini akan menggunakan perangkat lunak NMAP, menunjukkan bagaimana berbagai fitur NMAP dapat membantu kami mengumpulkan informasi, terutama port terbuka, deteksi sistem operasi dan kami juga akan melakukan pemindaian jaringan di mana kami akan menemukan semua komputer yang tersedia di jaringan. NMAP dapat membantu kita untuk mendeteksi detil komputer di jaringan yang IP kita tidak sadari. Begitu kita mengetahui alamat IP dari sistem target, kita bisa menggunakan NMAP untuk mendeteksi sistem operasi, Open Ports, Service/ Application Scanning. Setelah kita mengetahui alamat IP dari sistem remote, kita akan melakukan pemindaian kerentanan dengan menggunakan Nessus Vulnerability Scanner, setelah mengetahui kerentanan yang terkait dengan mesin target, kita akan mengetahui pemanfaatan yang sesuai untuk kerentanan tersebut dan akan melakukan pengujian penetrasi menggunakan Meta-split. . Pengujian penetrasi ini didasarkan pada pengujian kotak hitam dimana kita hanya diberi alamat IP komputer, kita bahkan akan melihat skenario dimana walaupun tidak mengetahui Alamat IP dari komputer target, kita dapat melakukan pemindaian jaringan dan beberapa Trik social engineering bisa kita tahu alamat ip mana yang menjadi milik komputer mana(Dawod, 2016).

3. Tinjauan Pustaka

3.1. Keamanan Komputer

Tujuan dari keamanan komputer untuk melindungi informasi komputer yang berada di dalamnya (Harjowinoto, Noertjahyana, & Andjarwirawan, 2016). Keamanan komputer sendiri meliputi beberapa aspek seperti yang tercantum di modul *Ethical Hacking and Countermeasures*, antara lain :

a. *Privacy*, adalah sesuatu yang bersifat rahasia (*private*) dimana ada pembatasan hak akses oleh orang tertentu saja.
b. *Confidentiality*, adalah pemberian data ke pihak lain tetapi tetap dijaga penyebarannya.
c. *Integrity*, adalah informasi yang tidak boleh diubah kecuali oleh pemilik informasi.
d. *Authentication*, adalah verifikasi pengguna melalui tampilan login dengan menggunakan nama user dan kata sandinya, jika cocok diterima dan sebaliknya.
e. *Availability*, adalah kesediaan data saat dibutuhkan.

Adapun beberapa langkah untuk mengamankan komputer seperti yang terlampir dalam modul *Ethical Hacking and Countermeasures*, yakni:

a. Aset, Perlindungan aset merupakan hal yg penting dan merupakan langkah awal dari berbagai implementasi keamanan komputer.
b. Analisa Resiko, identifikasi terhadap resiko yang mungkin terjadi, seperti sebuah *event* yang berpotensial untuk mengakibatkan kerugian terhadap sistem.
c. Keamanan jaringan, semua perangkat yang tersambung pada jaringan perlu diperhatikan keamanannya.
d. *Tools*, *tool* yang digunakan pada PC memiliki peran penting dalam hal keamanan karena *tool* yang digunakan harus benar - benar aman.
e. Prioritas, perlindungan PC secara menyeluruh.

3.2. Keamanan *Server*

Tidak ada *server* komputer yang benar-benar aman. Sebuah *server* membutuhkan sistem jaringan untuk berkomunikasi. Setiap komunikasi dapat jatuh ke tangan orang lain dan dapat disalahgunakan. Sistem keamanan membantu mengamankan *server* dan jaringannya tanpa menghalangi penggunaannya dan menempatkan antisipasi ketika jaringan berhasil ditembus. Selain itu, pastikan bahwa user dalam jaringan memiliki pengetahuan yang cukup mengenai keamanan dan pastikan bahwa mereka menerima dan memahami rencana keamanan yang dibuat. Jika tidak memahami hal tersebut, maka harus menciptakan suatu lubang (*hole*) keamanan pada jaringan yang ada (Harjowinoto, Noertjahyana, & Andjarwirawan, 2016). Keamanan komputer, dalam hal ini server meliputi beberapa aspek antara lain [3]:

a. *Confidentiality*.
   Confidentiality attack adalah pencegahan dalam menjaga informasi dari orang yang tidak berhak dan tidak berkepentingan untuk mengakses.
b. *Integrity*.
   Integrity adalah upaya pencegahan terhadap informasi yang tidak boleh diubah dan dihapus tanpa seijin pemilik informasi.
c. *Availability*.
   Availability adalah upaya pencegahan ditahannya informasi atau sumber daya terkait oleh mereka yang tidak berhak dimana berhubungan dengan ketersediaan informasi ketika dibutuhkan.
d. *Non-repudiation*.
   Non-repudiation merupakan hal yang yang bersangkutan dengan pengirim yang melakukan transaksi dan penerima. Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi.
e. *Authentication*.
   Authentication adalah suatu langkah untuk menentukan atau mengonfirmasi bahwa pengirim suatu informasi yang ada dapat diidentifikasi dengan benar dan ada jaminan bahwa identitas yang didapat tidak palsu. Melakukan *autentikasi* terhadap sebuah objek adalah melakukan konfirmasi terhadap kebenarannya, sedangkan melakukan autentikasi terhadap seseorang biasanya adalah untuk memverifikasi identitasnya, dengan kata lain informasi tersebut benar-benar dari orang yang dikehendaki.

3.3. *Hacker*

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

a. *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*.
b. *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.
c. *Grey hat hacker*, merupakan bagian pertengahan jalan antara *black hat hacker* dan *white hat hacke.*

3.4. *Vulnerability Testing*

Vulnerability Testing 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*, *cracker, defacer*, dan sebagainya.

Tujuan *vulnerability testing* adalah untuk menentukan dan mengetahui serangan-serangan yang bisa terjadi terhadap kerentanan yang ada pada sistem, mengetahui dampak bisnis yang diakibatkan dari hasil ekpoitasi yang dilakukan oleh penyerang.(Newson, 2005).

Tipe untuk melakukan suatu vulnerability testing ada 2 macam . Kedua macam itu antara lain :

a. *External Testing.*
   External Testing adalah *testing* dengan melakukan analisa terhadap informasi *public* yang tersedia, *network enumeration phase*, dan analisa keamanan *devices* yang digunakan.
b. *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 *Vulnerability testing* yang bisa digunakan , antara lain:

a. *Passive Vulnerability testing*. Dalam hal ini yang dilakukan adalah melakukan pemetaan dan pengujian terhadap kontrol yang ada didalam *web application*, *login*, dan konfigurasinya, sehingga dapat memetakan target sistem.
b. *Active Vulnerability testing. Active Vulnerability testing* merupakan melakukan kegiatan aktif dalam pengujian terhadap keamanan sistem dengan melakukan manipulasi input, pengambilan hak akses, dan melakukan

pengujian terhadap *vulnerability* yang sudah ada.

c. *Aggressive Vulnerability testing.*
Aggressive Vulnerability testing adalah melakukan eksploitasi terhadap *vulnerability*, melakukan reverse enginering terhadap *software* dan *system*, menanamkan *backdoor*, mengunduh *code*, dan mencoba mengambil alih finansial dan informasi yang ada di *server*.

3.5. Keamanan Jaringan

Satu hal yang perlu diingat bahwa tidak ada jaringan yang anti sadap atau tidak ada jaringan komputer yang benar-benar aman (Angir, Noertjahyana, & Andjarwirawan, 2015). 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*. 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*.

4. Metodologi

4.1. Analisa Permasalahan

Vulnerability testing server sistem administrasi Web UNILAK ini memang diperlukan. Hal ini dikarenakan *server* sistem administrasi tersebut memegang peranan yang sangat penting di Web UNILAK.

Vulnerability testing server ini dilakukan dengan tujuan untuk mengetahui *vulnerability* yang ada. Dari *range IP address* yang di-s*canning*, nantinya akan diketahui *IP address* yang mempunyai *NMap* dan yang tidak mempunyai *NMap info*. Setelah itu, dari *NMap info* yang ada, dapat diketahui *IP address* server Universitas Lancan. Selanjutnya, *IP address* tersebut akan di- *scanning* lagi dengan *tools* berbeda untuk melihat kelemahan yang dimiliki. Hasil dari *scanning* ini akan ditembus. Laporan ini nantinya dapat memberikan evaluasi kepada pengelola jaringan komputer Web UNILAK untuk lebih waspada lagi terhadap kelemahan yang ada.

4.2. Analisa Sistem

Penelitian ini, program aplikasi (*tool*) yang digunakan adalah program yang sesuai dengan langkah *penetration testing*. *Tool* yang digunakan ada yang didapatkan melalui cara *download* dari *internet*) sendiri. Pada Tabel 1 dapat dilihat sistem (*tool*) yang digunakan untuk *penetration testing* dalam pengerjaan penelitian.

Tabel 1. Tabel *tool* yang digunakan untuk penelitian

No	*Step*	*Tools*
1	*Footprinting* [4]	Angry IP Scanner
2	*Enumeration and Scanning Networks* [5] [6]	NMAP
3	*Pengujian Cloud*	

4.3. Metodologi *Vulnerability Testing*

Pada penelitian ini digunakan beberapa metodologi *vulnerability testing* . Adapun beberapa metodologi yang digunakan dalam penelitian ini adalah sebagai berikut:

a. *Information Gathering. Information gathering* merupakan salah satu dari langkah utama dalam melakukan *vulnerability testing.* Metodologi ini merupakan fase pertama dalam melakukan *vulnerability testing* dan dilakukan dengan menggunakan berbagai macam *tools, scanners, online resource,* mengirim *http* sederhana, dan lain-lain.

b. *Vulnerability Analysis. Vulnerability Analysis* merupakan metode untuk mengidentifikasi *vulnerability* dalam suatu *network*. Metodologi ini menyediakan ringkasan dari beberapa celah atau *flaw* dari sistem atau *network.*

c. *External Vulnerability/Penetration Testing. External vulnerability* testing dijalankan untuk mengetahui apakah *external network* tersebut aman atau tidak. Di dalam *external.*

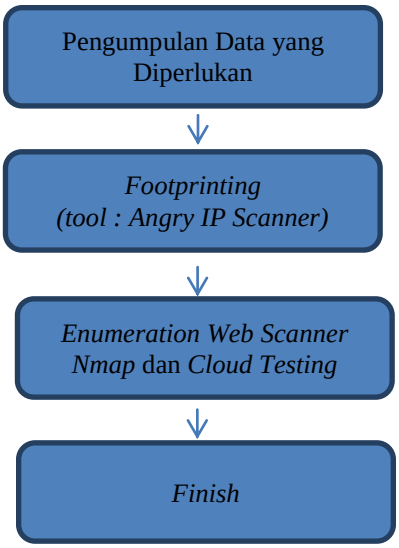
d. *vulnerability testing, hacking* dilakukan dengan cara yang sama dengan seseorang yang melakukan *attack* tetapi sama sekali tidak membahayakan *network.*

e. *Social Engineering. Social Engineering* adalah sebuah metode serangan yang digunakan oleh penyerang untuk mendapatkan informasi krusial dari sebuah perusahaan, biasanya dengan

kontak langsung dengan target, secara verbal, maupun informasi mengenai target yang ditemukan dimanapun.

4.4. Alur Pengujian

Pada Gambar 1 dapat dilihat *flowchart* pengerjaan jurnal. Pertama, *user* harus melakukan koneksi dengan *WiFi* dan melakukan autentikasi. Selanjutnya *user* dapat melakukan *vulnerability testing* untuk melakukan pengumpulan data.



Gambar 1. Langkah-langkah pengerjaan *vulnerability testing*

5. Hasil Dan Pembahasan

5.1. *Foot Printing*

a. *Physical (Environmental) Security*

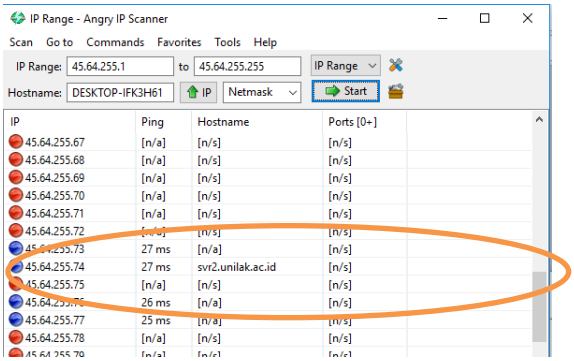
Setiap vulnerability diberikan solusi sebagai berikut

1) Pintu ruang *server* yang selalu terbuka. Pintu di ruang *server* harus ditutup dengan tujuan agar hanya orang yang berkepentingan yang dapat keluar masuk ruang *server*.
2) Terdapat barang-barang selain server sistem administrasi *Website* UNILAK. Barang-barang yang tidak berhubungan dengan *server* sistem administrasi diletakkan di tempat sesuai dengan fungsinya.
3) Air *conditioner* yang mengalami kebocoran. Dilakukan *maintenance* terhadap Air *conditioner* sesuai dengan periode tertentu yang ditentukan oleh pihak PUSKOM.

Hanya terdapat *smoke detector*, namun tidak ada alat pemadam api. Seharusnya di sebuah ruangan *server* diberi fasilitas pemadam api, seperti *water sprinkler*, atau penyemprot karbondioksida supaya api dapat sesegera mungkin terdeteksi dan dapat dipadamkan secara cepat sehingga server tidak mengalami kerusakan.

b. *Angry Ip Scanner*

Setelah melakukan autentikasi langsung ke website unilak.ac.id dengan menggunakan *IP static* dan mengetahui *topologi network public domain*, langkah selanjutnya yang dilakukan yaitu melakukan *scan IP address* yang memiliki *range* dengan menggunakan *Angry ip Scanner* untuk mengetahui detail siapa saja yang terkoneksi dalam jaringan sesuai dengan *topologi network Website* UNILAK. Berikut hasil dari scan dengan *Angry IP Scanner*.

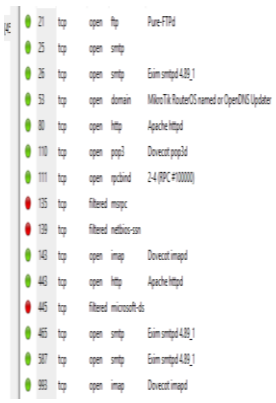


Gambar 2. *IP Public* Unilak.ac.id

5.2. *Vulnerability Testing dengan Nmap dan Cloud Testing*

a. Port Checking(Nmap)

Kelemahan-kelemahan yang telah ditemukan pada langkah sebelumnya, yaitu *enumeration* and *scanning networks*, akan digunakan untuk masuk ke dalam *server* dan dibahas kelemahan-kelemahan yang ditemukan. Kelamahan-kelemahan tersebut ditemukan karena adanya *port-port* yang terbuka seperti yang ditampilkan pada Gambar 3 berikut.

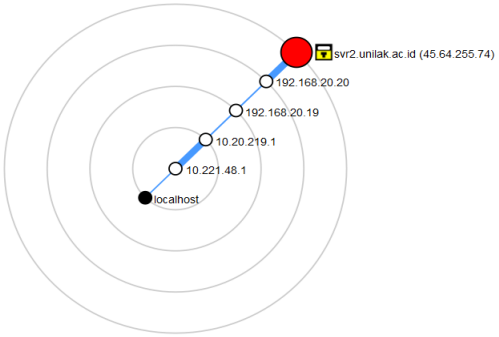


Gambar 3. *IP Port Cheking* (Daftar *Port* Terbuka/Tertutup)

Dari gambar 3 diatas dijelaskan dengan warna hijau merupakan daftar port yang terbuka dan warna merah merupakan port yang tertutup.

b. *Topologi* Jaringan

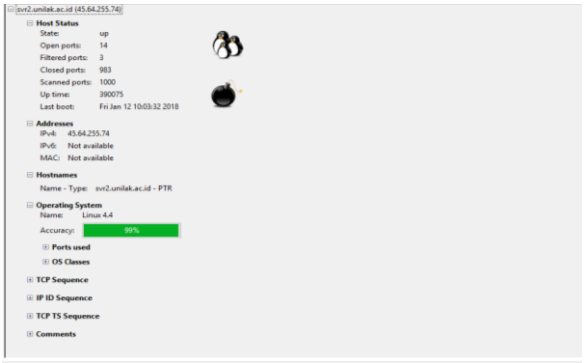
Kemudian scan dilanjutkan untuk mengetahui mapping dari jaringan dan server di Universitas Lancang Kuning. Dari hasil pengujian didapatkan topology jaringan pada gambar 4 berikut.



Gambar 4. *Topologi* Jaringan dari *Server* UNILAK

c. *Host Status* dan *Operating System(Nmap)*

Pengujian juga dilakukan untuk mengetahui *Host* Status dan Sistem Operasi yang digunakan. Dari pengecekan yang ada didapatkan *Server* UNILAK menggunakan Sistem Operasi Linux versi 4.4 pada gambar 5 berikut ini.



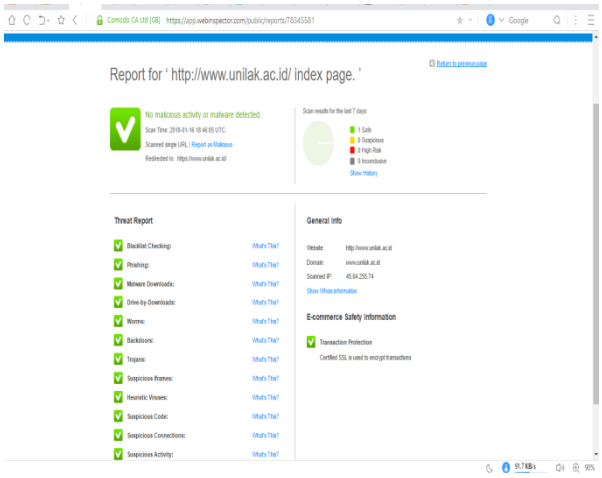
Gambar 5. *Status Host* dan *Sistem* Operasi yang digunakan

d. Pengujian *Cloud*

Pengujian akhir dari *server* UNILAK Peneliti menggunakan fasiltas pengujian web yang sudah disediakan oleh beberapa web ternama yang bersifat *cloud computing*. Dari hasil pengujian didapatkan hasil penilaian yang baik pada Web *Server* Universitas Lancang Kuning.

1) Pengujian pada Web *Inspector*

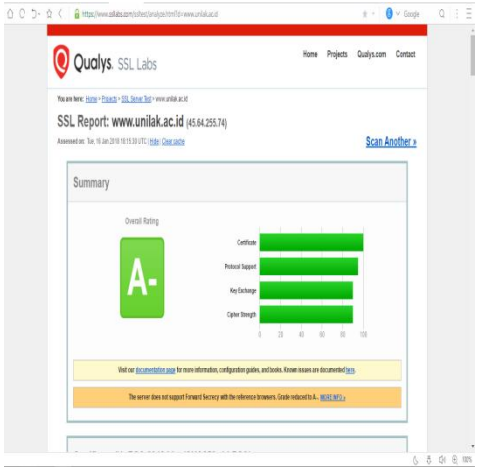
Pada pengujian web *inspector* tidak ditemukan masalah yang menimbulkan hal yang berbahaya di *Server* UNILAK. Seperti halnya *malware, phising, worm, trojan, blacklist checking*, dan lain sebagainya yang berkaitan dengan semua hal yang dapat mengganggu pada keamanan sebuah server pada gambar 6 berikut.



Gambar 6. Pengujian Pada *Web Inspector*

2) Pengujian *Grade Pada Qualis SSL* Lab

Pada pengujian peringkat keamanan yang dimiliki *Server* UNILAK didapatkan nilai A-. Minus ini dikarenakan *Server* UNILAK belum mempunyai *Forward Secrecy* pada beberapa *browser* utama pada gambar 7 berikut.



Gambar 7. Pengujian Pada Web Pada *Qualis Inspector*

6. Simpulan

Berdasarkan dari semua yang telah dilakukan selama pengerjaan penelitian, dapat disimpulkan beberapa hal, antara lain:

a. Kelemahan *physical security* yang ditemukan tidak direkomendasikan untuk sebuah ruangan *server* karena rentan terhadap orang luar yang masuk ke dalam ruang server dan mengambil perangkat keras yang ada, serta

b. Rentan terhadap rentan terhadap *disaster* seperti kebakaran dan terkena air.
c. Terbukanya beberapa *port* yang tidak sesuai dengan fungsinya. Hal ini dapat menyebabkan adanya celah yang dapat dimanfatkan untuk diserang.
d. Pada Pengujian *Cloud Web* UNILAK dikatagorikan dalam kondisi baik.

7. Ucapan Terima Kasih

Ucapan terima kasih kami sampaikan kepada LPPM UNILAK yang telah melaksanakan penelitian ini dan kepada PIHAK PUSKOM UNILAK yang sudah membantu dalam penyelesaian data penelitian ini.

8. Referensi

Angir, D. C., Noertjahyana, A., & Andjarwirawan, J. (2015). Vulnerability Mapping pada Jaringan Komputer di Universitas X. *Jurnal Infra*, *3*(2), pp.44-p.50. Retrieved from http://publication.petra.ac.id/index.php/teknik-informatika/article/view/3089/2781

Dawod, A. Y. (2016). Penetration Testing Methodology of Scanning Network using NMAP. *International Journal of Enhanced Research in Science Technology & Engineering*, *5*(12), 2319–7463. Retrieved from http://www.erpublications.com/uploaded_files/download/download_05_01_2017_11_36_35.pdf

Harjowinoto, D., Noertjahyana, A., & Andjarwirawan, J. (2016). Vulnerability Testing pada Sistem Administrasi Rumah Sakit X. *Jurnal Infra*, *4*(1), pp.227-p.232. Retrieved from http://publication.petra.ac.id/index.php/teknik-informatika/article/view/4074

Joshi, C., & Singh, U. K. (2017). Information security risks management framework – A step towards mitigating security risks in university network. *Journal of Information Security and Applications*, *35*, 128–137. https://doi.org/10.1016/j.jisa.2017.06.006

Newson, A. (2005). Network threats and vulnerability scanners. *Network Security*, *2005*(12), 13–15. https://doi.org/10.1016/S1353-4858(05)70314-7

Pangalila, R., Noertjahyana, A., & Andjarwirawan, J. (2015). Penetration Testing Server Sistem Informasi Manajemen dan Website Universitas Kristen Petra. *Jurnal Infra*, *3*(2), pp.271-p.276. Retrieved from http://publication.petra.ac.id/index.php/teknik-informatika/article/view/3145

Vignjevic, M. D., Vucicevic, M., Djukic, M., & Radin, B. (2015). Efficient adaptation and high reusability of test suites in a black box testing environment. In *2015 23rd Telecommunications Forum Telfor (TELFOR)* (pp. 1002–1004). IEEE. https://doi.org/10.1109/TELFOR.2015.7377634

e.