ANALISA IMPLEMENTASI TEKNIK *RECONNAISSANCE* PADA WEBSERVER (STUDI KASUS: UPT PUSKOM UNIVERSITAS DEHASEN)

Marsoni, Toibah Umi Kalsum, Adhadi Kurniawan

Program Studi Teknik Komputer Fakultas Ilmu Komputer Universitas Dehasen Bengkulu
Jl. Meranti Raya No. 32 Kota Bengkulu 38228 Telp. (0736) 22027, 26957 Fax. (0736) 341139

ABSTRACT

Information on the website is a matter that must be considered. The issue is important because if the information on a website accessible to people who are not responsible for the accuracy of such information would undoubtedly could even be misleading information. Activities to gather information on the web server needed a longer time to the system. This study did reconnaissance to obtain important information on the website, accunetix tool, nmap, nslookup, tcptraceroute can find information about the weaknesses of the website. From these results obtained some important information from the website using the tool. In order to know the complete information on the wireless network in the form of a simulation such as online.

Keywords: Reconaissance, webserver, accunetix

INTISARI

Informasi tentang website merupakan suatu hal yang wajib diperhatikan. Masalah tersebut penting karena jika informasi pada website diakses oleh orang yang tidak bertanggung jawab maka keakuratan informasi tersebut akan diragukan bahkan bisa menjadi informasi yang menyesatkan. Kegiatan untuk mengumpulkan informasi terhadap web server di butuhkan waktu yang lebih lama terhadap sistem. penelitian ini melakukan reconnaissance untuk mendapatkan informasi penting tentang website, tool accunetix, nmap, nslookup, tcptraceroute dapat mencari informasi tentang kelemahan dari website. Dari hasil penelitian ini didapatkan beberapa informasi penting dari website dengan menggunakan tool. Agar informasi lengkap di ketahui pada jaringan wireless dalam bentuk simulasi seperti online.

Kata Kunci: *Reconaissance, webserver, accunetix*

I. PENDAHULUAN

Internet merupakan sarana yang dapat digunakan untuk menyebarkan informasi secara cepat sampai tanpa ada batasan wilayahnya. Informasi yang dissebarkan melalui media internet salah satunya ditampilkan melalui halaman web sebuah website. Website biasanya ditempatkan pada server web yang dapat diakses melalui jaringan seperti internet.

Keamanan informasi pada website merupakan suatu hal yang wajib diperhatikan. Masalah tersebut penting karena jika informasipada website diakses oleh orang yang tidak bertanggung jawab maka keakuratan informasi tersebut akan diragukan bahkan bisa menjadi informasi yang menyesatkan.

Reconnaissance merupakan sebuah fase persiapan sebelum (attacker) melakukan pencurian informasi pada web server, dimana kegiatan ini adalah untuk mengumpulkan informasi sebanyak mungkin mengenai sasaran web server. Teknik reconnaissance menyertakan network scanning melalui jariangan internal dan eksternal yang dilakukakan tanpa memiliki izin dari pemilik server.

Banyak langkah bagi seorang hacker untuk mempelajari jaringan tanpa sepengetahuan pemilik server. Dengan menggunakan software atau pun tool secara online hacker dapat mengumpulkan informasi jaringan yang dibutuhkan untuk melakukan penyerangan. Informasi yang dikumpulkan merupakan pencarian kelemahan dari sistem yang digunakan. Kegiatan untuk mengumpulkan informasi terhadap web server di butuhkan waktu yang lebih lama terhadap sistem.

II. TINJAUAN PUSTAKA

A) Reconnaissance

Reconnaissance adalah istilah militer yang digunakan untuk menyebut metodologi yang digunakan untuk mengurangi ketidakjelasan tentang musuh, lingkungan, dan daerah untuk semua tipe (Thomas, 2010). Dalam arti lain adalah merupakan sebuah fase persiapan sebelum (attacker) melakukan penyerangan dimana kegiatan ini adalah untuk mengumpulkan informasi sebanyak mungkin mengenai sasaran. Teknik *reconnaissance* menyertakan network scanning melalui jariangan internal dan eksternal yang dilakukakan tanpa memiliki izin dari pemilik server.

Reconnaissance dibagi menjadi 2, yaitu Active Reconnaissance dan Passive Reconnaissance.

1) *Active Reconnaissance* adalah pengumpulan data dengan cara bertatap muka langsung atau berhubungan langsung dengan target/sasaran,

2) *Passive Reconnaissance* adalah menggunakan media informasi seperti berita, internet, dll.

Pada proses ini ada beberapa langkah yang dilakukan, yaitu :

1) Menentukan ruang lingkup aktifitas.

Pada proses ini kita akan mendapatkan sebanyak mungkin informasi yang berkaitan dengan lokasi, perusahaan, berita, alamat, email address, kebijakan, dll.

2) Network Enumeration

Network enumeration dilakukan untuk melihat domain yang digunakan oleh sebuah organisasi. Dengan menggunakan tools "whois" kita dapat melakukan kegiatan ini.

3) Mengetahui DNS record

Setelah kita mengetahui domain yang berkaitan dengan organisasi sasaran, selanjutnya kita perlu mencek hubungan alamat IP (IP address) & domain / hostname yang digunakan. Cara ini dapat dilakukan dengan menggunakan tools "See DNS Record" yang terdapat pada who.is.

4) Mengintai Jaringan

Setelah mengetahui daftar alamat IP (IP address) dari berbagai host yang ada di target anda. Langkah selanjutnya adalah memetakan topologi jaringan, baik yang menuju ke target sasaran maupun konfigurasi internal jaringan target. Biasanya kita mengunakan software seperti traceroute (Linux / UNIX), tracert (Windows), atau menggunakan tools yang sudah di sediakan oleh who.is untuk melakukan pemetaan jaringan.

B) Jaringan Komputer

Menurut Jufriadif (2008), Jaringan komputer adalah perpindahan data (Komunikasi Data) dari suatu komputer sumber (transmiter) ke komputer tujuan (receiver) yang melawati suatu media penghantar dalam bentuk bit-bit. Salah satu contoh dari jaringan komputer adalah video conference pada komputer, dimana suara dan video yang dihantar harus terlebih dahulu dirobah dalam bentuk kumpulan bitbit sebelum memasuki media penghantaran untuk di komunikasikan.

C) OSI (Open System Interconection)

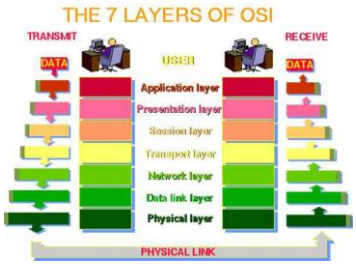
Menurut Sovana (2011:105), Pengertian dan Fungsi Layer pada OSI referensi OSI Model, OSI merupakan singkatan dari *Open System Interconnection* adalah standar komunikasi yang diterapkan di dalam jaringan komputer. Standar itulah yang menyebabkan seluruh alat komunikasi dapat saling berkomunikasi melalui jaringan. Dahulu ketika OSI belum digunakan, perangkat komunikasi yang berasal dari vendor berbeda tidak dapat saling berkomunikasi. Alat komunikasi yang diciptakan oleh IBM tidak dapat berkomunikasi dengan vendor lain. Sehingga dibentuklah standard OSI. tujuan utama dalam penggunaan model OSI adalah untuk membantu designer jaringan memahami fungsi dari tiap layer yang berhubungan dengan aliran komunikasi data. Termasuk jenis-jenis protocol jaringan dan metode transmisi.

Model referensi OSI secara konseptual terbagi ke dalam 7 lapisan dimana masing-masing lapisan memiliki fungsi jaringan yang *spesifik*. Model ini diciptakan berdasarkan sebuah proposal yang dibuat oleh *The International Standards Organization* (ISO) sebagai langkah awal menuju standarisasi protokol *Internasional* yang digunakan pada berbagai *Layer* .

Model OSI memiliki tujuh *Layer*. Prinsip-prinsip yang digunakan bagi ketujuh *Layer* tersebut adalah :

1) Sebuah *Layer* harus dibuat bila diperlukan tingkat abstraksi yang berbeda.
2) Setiap *Layer* harus memiliki fungsi-fungsi tertentu.
3) Fungsi setiap *Layer* harus dipilih dengan teliti sesuai dengan ketentuan standar *protocol internasional*.
4) Batas-batas *Layer* diusahakan agar meminimalkan aliran informasi yang melewati *interface*.
5) Jumlah *Layer* harus cukup banyak, sehingga fungsi-fungsi yang berbeda tidak perlu disatukan dalam satu *Layer* diluar keperluannya. Akan tetapi jumlah *Layer* juga harus diusahakan sesedikit mungkin sehingga arsitektur jaringan tidak menjadi sulit dipakai.

Model referensi OSI secara konseptual terbagi ke dalam 7 lapisan dimana masing-masing lapisan memiliki fungsi jaringan yang spesifik, seperti yang dijelaskan pada Gambar 1.



Gambar 1. Layer dalam OSI

1) Physical Layer

Physical Layer berfungsi dalam pengiriman raw bit ke channel komunikasi. Masalah desain yang harus diperhatikan disini adalah memastikan bahwa bila satu sisi mengirim data 1 bit, data tersebut harus

diterima oleh sisi lainnya sebagai 1 bit juga, dan bukan 0 bit. Secara umum masalah-masalah desain yang ditemukan di sini berhubungan secara mekanik, elektrik dan interface prosedural, dan media fisik yang berada di bawah lapisan fisik.

2) Data link Layer

Tugas utama *data link Layer* adalah sebagai fasilitas transmisi raw data dan mentransformasi data tersebut ke saluran yang bebas dari kesalahan transmisi. Sebelum diteruskan ke *Network Layer*, *data link Layer* melaksanakan tugas ini dengan memungkinkan pengirim memecag-mecah data input menjadi sejumlah data frame (biasanya berjumlah ratusan atau ribuan byte). Kemudian *data link Layer* mentransmisikan frame tersebut secara berurutan, dan memproses acknowledgement frame yang dikirim kembali oleh penerima. Masalah-masalah lainnya yang timbul pada *data link Layer* (dan juga sebagian besar *Layer-Layer* di atasnya) adalah mengusahakan kelancaran proses pengiriman data dari pengirim yang cepat ke penerima yang lambat. Mekanisme pengaturan lalu-lintas data harus memungkinkan pengirim mengetahui jumlah ruang buffer yang dimiliki penerima pada suatu saat tertentu.

3) Network Layer

Network Layer berfungsi untuk pengendalian operasi subnet. Masalah desain yang penting adalah bagaimana caranya menentukan route pengiriman paket dari sumber ke tujuannya. Bila pada saat yang sama dalam sebuah subnet terdapat terlalu banyak paket, maka ada kemungkinan paket-paket tersebut tiba pada saat yang bersamaan. Hal ini dapat menyebabkan terjadinya bottleneck. Pengendalian kemacetan seperti itu juga merupakan tugas *Network Layer*. memungkinkan jaringan-jaringan yang berbeda seperti protocol yang berbeda, pengalamatan dan Arsitektur jaringan yang ber beda untuk saling terinterkoneksi.

4) Transport Layer

Fungsi dasar transport *Layer* adalah menerima data dari session *Layer*, memecah data menjadi bagian-bagian yang lebih kecil bila perlu, meneruskan data ke *Network Layer*, dan menjamin bahwa semua potongan data tersebut bisa tiba di sisi lainnya dengan benar. Selain itu, semua hal tersebut harus dilaksanakan secara efisien, dan bertujuan dapat melindungi *Layer-Layer* bagian atas dari perubahan teknologi hardware yang tidak dapat dihindari.

5) Session Layer

Session *Layer* mengijinkan para pengguna untuk menetapkan session dengan pengguna lainnya. Sebuah session selain memungkinkan transport data biasa, seperti yang dilakukan oleh transport *Layer*, juga menyediakan layanan yang istimewa untuk aplikasi-aplikasi tertentu. Sebuah session digunakan untuk memungkinkan seseorang pengguna log ke remote timesharing system atau untuk memindahkan file dari satu mesin kemesin lainnya.

6) Presentation Layer

Pressentation *Layer* melakukan fungsi-fungsi tertentu yang diminta untuk menjamin penemuan sebuah penyelesaian umum bagi masalah tertentu. Pressentation *Layer* tidak mengijinkan pengguna untuk menyelesaikan sendiri suatu masalah. presentation *Layer* memperhatikan syntax dan semantik informasi yang dikirimkan contoh layanan pressentation adalah encoding data.

7) Application Layer

Application Layer memiliki fungsi untuk menentukan terminal virtual jaringan abstrak, serhingga editor dan program-program lainnya dapat ditulis agar saling bersesuaian. Untuk menangani setiap jenis terminal, satu bagian software harus ditulis untuk memetakan fungsi terminal virtual jaringan ke terminal sebenarnya. Fungsi *Application Layer* lainnya adalah pemindahan file. Sistem file yang satu dengan yang lainnya memiliki konvensi penamaan yang berbeda, cara menyatakan baris-baris teks yang berbeda, dan sebagainya. Perpindahan file dari sebuah sistem ke sistem lainnya yang berbeda memerlukan penanganan untuk mengatasi adanya ketidak-kompatibelan ini. Tugas *appication Layer*, seperti pada surat elektronik, remote job entry, *directory lookup*, dan berbagai fasilitas bertujuan umum dan fasilitas bertujuan khusus lainnya.

D) IP Address

(Kustanto&Saputro:2008:42) Sederetan angka biner 32 bit yang terbagi menjadi 4 kelompok. Alamat ditandai untuk memungkinkan pengalokasian variabel bit-bit untuk menentukan jaringan dan host. Pengkodean ini menampilkan fleksibilitas dalam menetapkan alamat-alamat ke host serta memungkinkan penggabungan ukuran-ukuran jaringan di dalam internet. Alamat IP biasanya ditulis dengan deret angka yang disebut *notasi desimal bertitik*, dengan angka desimal yang menampilkan setiap octet alamat-alamat 32 bit. Sebagai contoh, alamat IP 11000000 11100100 0001 00111001 ditulis 192.228.17.57.

Setiap bagian dapat menampung 255 kemungkin angka, jadi total alamat IP yang tersedia 255 x 255 x 255 x 255 = 4.228.250.625. akan tetapi dalam kenyataan dalam pengalokasiannya ada batasan-

batasan serta kelas tertentu, jadi tidak sembarang salah satu dari 4 milyar kemungkinanalamat IP tersebut dapat dipergunakan begitu saja.

Fasilitas Windows 2003 yang signifikan adalah kemampuan untuk berhubungan ke Internet dan sistem-sistem yang tidak serupa. Windows 2003 menyediakan fasilitas-fasilitas keamanan tingkat tinggi yang dapat diimplementasikan ketika berhubungan ke suatu sistem pada sebuah jaringan. Untuk mendukung semua fasilitas tersebut, Windows 2003 TCP/IP memiliki kapabilitas yang baru dan canggih. Kapabilitas yang dimaksud adalah:

1) IP Security.

IP Security (IPSec) adalah suatu teknologi yang dipakai untuk meng-encrypt lalu lintas jaringan TCP/IP. IPSec memungkinkan transfer data yang aman di antara client-client yang jauh dan server perusahaan secara pribadi melalui virtual private network (VPN).

Layer Two Tunneling Protocol. Layer Two Tunneling Protocol (L2TP) merupakan suatu kombinasi PPTP dan Layer Two Forwarding (L2F). L2F adalah suatu protocol transmisi yang memungkinkan server akses dial-up membingkai lalu lintas dial-up di dalam Point to Point Protocol (PPP) dan mentransmisikannya pada hubungan WAN ke server L2F (routetiap segment yang diterima dengan sukses.

2) Kelas Alamat IP

Untuk mempermudah pendistribusiannya, alamat IP dibagi kelas-kelas tertentu. Pada dasarnya ada kelas 5 alamat IP yaitu kelas A, kelas B, kelas C, kelas D, dan kelas E. Kelas A,B,C didistribusikan untuk umum, sedangkan kelas D dan E digunakan untuk *muticast* dan *eksperimen.* Setiap alamat IP memiliki *network* ID dan *host* ID. *Nework* ID adalah identias jaringan sedangkan host ID adalah identitas node. Pada dasarnya pembagian kelas alamat IP didasarkan atas pembagian *network* ID dan *host* ID tersebut. Adapun kelas-kelas yang dimaksud dilihat pada Tabel 1.

Tabel 1. Kelas IP Address

Kelas	Batas
A	0.0.0.0 - 127.225.225.225
B	128.0.0.0-191.225.225.225
C	192.0.0.0-223.255.255255
D	224.0.0.0-239.255.255.255
E	240.0.0.0 -247.255.255.255.1

Alamat IP berdasarkan identitas jaringan dan identitas hostnya dibagi menjadi tiga kelas sebagai berikut :

a) Kelas A

Ciri kelas ini adalah bahwa oktet pertama dari lamat IP-nya ada dalam rentang nilai 0 s.d 127. Oktet pertma menunjukan identitas jaringan sedangkan oktet ke-2, ke-3 dan ke-4 menunjukan identitas hostnya. Misalnya pada alamat IP 120.45.3..201, identitas jaringannya adalah 120 dan identitas hostnya adalah 45.3.201

b) Kelas B

Ciri kelas ini adalah bahwa oktet pertama dari alamat IP-nya ada dalam rentang nilai 128. S.d 191. Oktet pertama dan ke-2 menunjukkan identitas jaringan sedangkan oktet ke-3 dan ke-4 menunjukkan identitas host. Misalnya pada alamat IP 145.45.3.201, identitas jaringannya adalah 145.45 dan identitas hostnya adalah 3.201

c) Kelas C

Ciri kelas ini adalah bahwa oktet pertama dari alamat IP-nya ada dalam rentang nilai 192. S.d 223. Oktet pertama, ke-2 dan ke-3 menunjukkan identitas jaringan, sedangkan oktet ke-4 menunjukkan identitas host. Misalnya pada alamat IP 217.45.3.201, identitasnjaringannya adalah 217.45.3 dan identitas hostnya adalah 201.

Jadi bila kita mengetahui alamat IP suatu situs, kita dapat menentukan tergolong dalamkelas apakah situs tersebut dan apakah identitas jaringan dan identitas host dari situs tersebut. Alamat IP dalam rentang oktet pertama 224 s.d 247 dogolongkan dalam kelas D dan digunakan untuk keperluan IP *multicasting*. Alamat IP dalam rentang oktet pertama 248 s.d 255 dogolongkan dalam kelas E dan hanya digunakan untuk keperluan eksperimental. (Yani:2007).

III. METODOLOGI PENELITIAN

A) Metode Penelitian

Penelitian ini dilakukan dengan menggunakan penelitian eksperimen. Penelitian ini untuk menemukan, mengembangkan, dan mengkaji kebenaran suatu pengetahuan yang menggunakan metode ilmiah. Dalam penelitian ini lebih terarah kepada beberapa teknik reconnaissance terhadap web server. Dilakukan dengan menggunakan beberapa aplikasi dan tool untuk mendapatkan informasi yang dibutuhkan terhadap suatu web server.

Metode penelitian yang digunakan dalam penlitian ini adalah melalui Analisis, penulis menganalisis informasi-informasi yang berkaitan dengan reconnaissance yang didapat setelah

dilakukan pengujian koneksi terhadap simulasi jaringan.

Mengidentifikasi hasil informasi yang didapat dari beberapa teknik reconnaissance. Hasil analisis akan digunakan sebagai masukan bagi admin UPT Puskom terhadap keamanan jaringan pada infrastruktur jaringan komputer universitas dehasen.

B) Perangkat keras dan perangkat lunak

Dalam implementasi yang akan dilakukan pada penelitian ini analisis perbandingan ini dengan spesifikasi perangkat keras yang digunakan antara lain :

1) Netbook dengan CPU intel Atom N550 (1,5Ghz)
2) *Wireless* Intel *Wi-fi* Link 1000 BGN
3) Memory 1GB DDR3
4) Storage 120GB HDD
5) Battery 6-cell Li-on

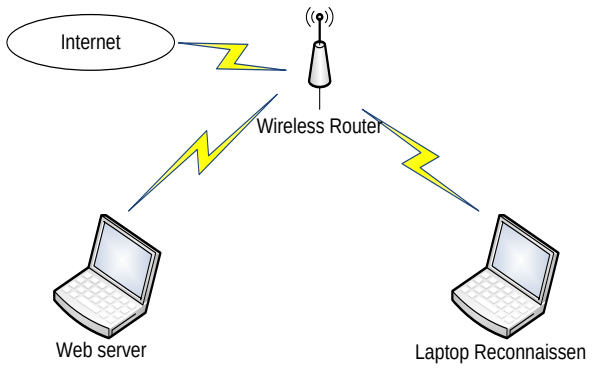
Software yang akan digunakan untuk melakukan analisa terhadap penelitian ini adalah :

1) Sistem Operasi yang digunakan Windows 7
2) Perangkat Acunnetik
3) Virtualbox / vmware.
4) Kali Linux

C) Metode Perancangan Sistem

1) Blok Diagram Global

Percobaan yang akan dilakukan dalam penelitian ini terlihat pada blok diagram global gambar 3.3. dibawah ini :



Gambar 2. Blok Diagram Global

Dalam mendapatkan hasil analisis perbandingan tahap reconnaissance adalah dengan membangun jaringan seperti gambar 2. Kedua perangkat terhubung pada wireless dan terkoneksi ke internet.

Webserver yang dibangun diimplementasikan pada laptop menggunakan software webserver yaitu xampp. Dan pada webserver diinstallkan satu aplikasi open source wordpress. Dan melalui internet percobaan pada web server secara online.

Laptop reconnaissance digunakan untuk mencari informasi yang terdapat pada laptop webserver. Informasi yang dicari sesuai fungsi reconnaissance seperti nama host, ip ranges, sistem operasi, port yang digunakan dll. Pada computer ini diinstallkan kali linux pada sistem virtual yaitu aplikasi virtualbox. Mesin linux ini dijadikan pencari informasi dengan menggunakan tool-tool yang sudah tersedia.

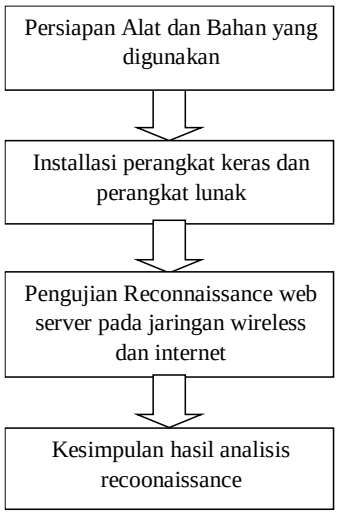
2) Prinsip Kerja

Tahapan dalam mengumpulkan informasi semua data sebanyak-banyaknya. Reconnaissenance aktif akan melakukan aktifitas seperti mengumpulkan keberadaan internet antara lain nama domain, alamat ip khusus, layanan-layanan yang telah ditemukan, prokol jaringan.

Beberapa teknik untuk mendapatkan informasi tersebut dilakukan beberapa cara. Antara lain dengan menggunakan tool dan aplikasi yang bisa melakukan scanning untuk mengumpulkan informasi yang dibutuhkan pada suatu webserver.

3) Rencana Kerja

Rencana kerja yang akan dilakukan untuk melakukan analisis dalam mengumpulkan informasi terhadap suatu webserver ini seperti Gambar 10.



Gambar 3. Kerangka Kerja Penelitian

D) Rancangan Pengujian

Pengujian yang dilakukan adalah dengan menggunakan beberapa aplikasi untuk reconnaissance. Aplikasi yang sangat popule adalah seperti accunetix.

Bukan hanya aplikasi accunetix saja yang digunakan juga dibadingkan dengan tool-tool yang tersedia pada sistem kali linux. Beberapa pengujian untuk perbandingan ini adalah mencari tahu lebih detil infromasi yang terkandung pada sistem server.

IV. PEMBAHASAN

A) Hasil

Reconnaissance adalah berasal dari bahasa militer yang artinya adalah secara aktif mencari dan mengumpulkan semua informasi yang berkaitan dengan musuh. Sedangkan dalam dunia ethical hacking proses reconnaissance mengamati sasaran dan mengumpulkan informasi "how, when, where the doing". Dengan mengidentifikasi kebiasaan, tindakan, orang orangnya maka akan nampak kelemahan dari target.

Pada penelitian ini metode yang digunakan metode simulasi, Menurut Law dan Kelton (1991), simulasi didefinisikan sebagai sekumpulan metode dan aplikasi untuk menirukan atau merepresentasikan perilaku dari suatu sistem nyata, yang biasanya dilakukan pada komputer dengan menggunakan perangkat lunak tertentu. Perangkat

Dalam penelian ini menggunakan 2 laptop yang mana satu di fungsikan sebagai server dengan menginstallkan aplikasi web server xampp. Laptop ke dua digunakan sebagai laptop penguji sebagai reconnaissance yang terkoneksi dengan jaringan wireless ke server.

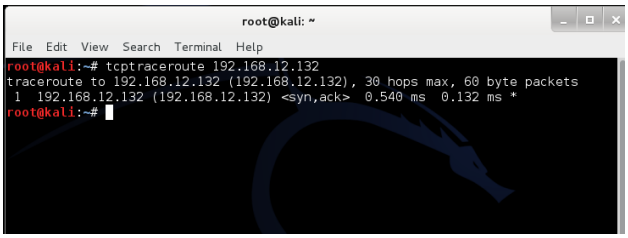
Untuk mendapatkan informasi yang dibutuh beberapa pengujian dilakukan terhadap computer server tersebut. Berikut hasil pengujian terhadap server dengan tool dan aplikasi accunetic.

1) Hasil Reconaissance Pada Jaringan Wireless

Beberapa informasi yang didapatkan dari hasil reconnaissance terhadap web server dengan koneksi wireless.

a) Tcptraceroute

Tool ini digunakan untuk melihat informasi tentang status service yang aktif pada computer. Berikut informasi dari server dengan ip 192.168.12.132

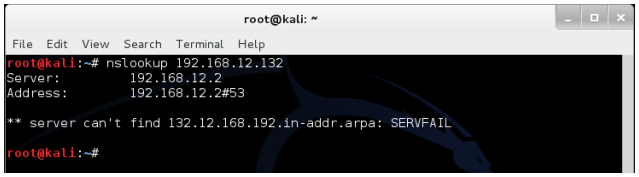


Gambar 4.Tool tcptraceroute

Ip address 192.168.12.132 telah mengirim syn (syncrhonisation) yang diterima dari ip server tersebut, dan computer server menjawab permintaan tersebut dengan mengirimkan ack (ack, syn) flag dengan waktu 0.540 ms 0.132 ms.

b) Nslookup

Nslookup merupakan suatu tool untuk melihat query DNS server yang digunakan dan juga melihat IP Address suatu domain maupun sebaliknya.

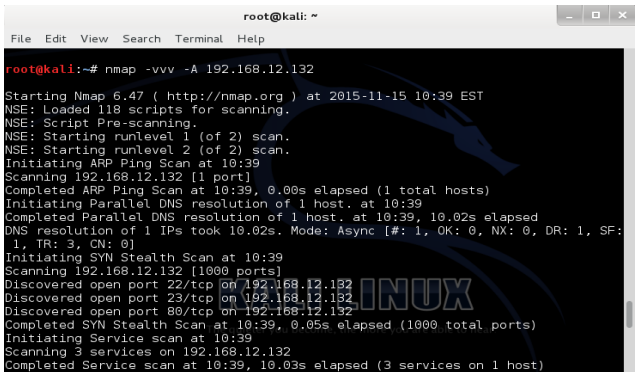


Gambar 5. Tool nslookup

Bahwa dns komputer klien yang digunakan adalah 192.168.12.2 dan server 132.12.168.192 tidak dapat memberikan alamat server ip tersebut.

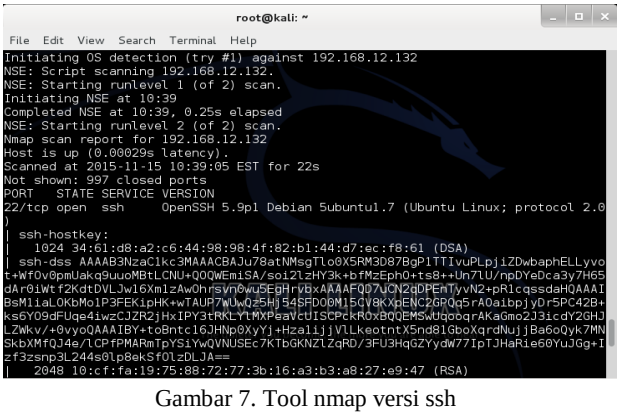
c) Nmap

Nmap merupakan tool untuk memeriksa jaringan secara cepat, meskipun dapat pula bekerja terhadap host tunggal. Nmap menggunakan paket ip raw dalam cara yang canggih untuk menentukan host mana saja yang tersedia pada jaringan, layanan (nama aplikasi dan versi) apa yang diberikan, sistem operasi (dan versinya) apa yang digunakan, apa jenis firewall/filter paket yang digunakan, dan sejumlah karakteristik lainnya.



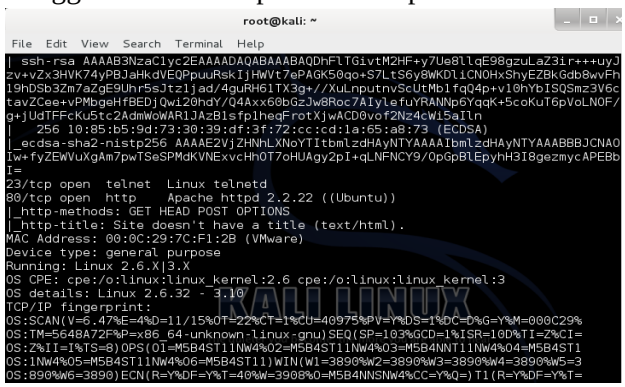
Gambar 6.Tool nmap

Dari gambar 6, informasi yang dihasilkan dari perintah nmap –vvv –A, terdapat 3 yaitu port 22, 23 dan 80 open. Artinya server tersebut mengizinkan telnet, ssh dan http dapat diakses.



Gambar 7. Tool nmap versi ssh

Pada gambar 7 terlihat bahwa ssh port 22 menggunakan versi Open SSH 5.9 pada linux ubuntu.



Gambar 8.Tool nmap telnet dan http

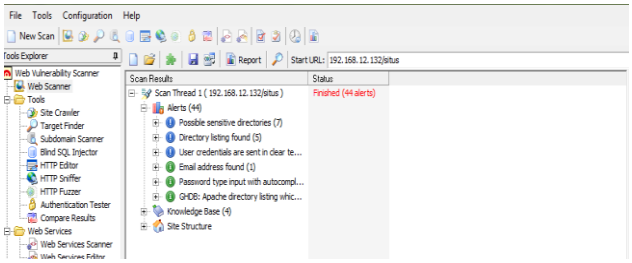
Gambar 8 juga menampilkan informasi telnet dan http yang open denggan versi kedua protocol tersebut.

d) Aplikasi Accunetic

Reconnaissance pada webserver digunakan aplikasi accunetix vulnarebility scanner, beberapa informasi yang didapatkan dari server web yaitu :

1) Alert (peringatan)

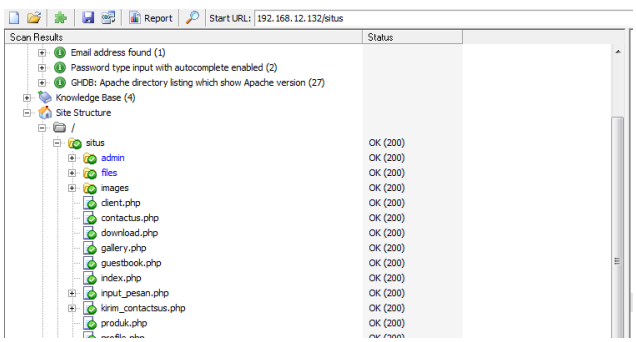
Terdapat 44 informasi peringatan ancaman keamanan pada webserver yang ditampilkan pada Gambar 9.



Gambar 9. Hasil scanning dengan aplikasi accunetix

2) Webserver

Pada server web yang bernama situs setelah scanning informasi yang dihasilkan adalah informasi struktur situs di web server. Dengan informasi sangat memberikan kemudahan bagi yang membutuhkan informasi website.



Gambar 10. Informasi struktur web site

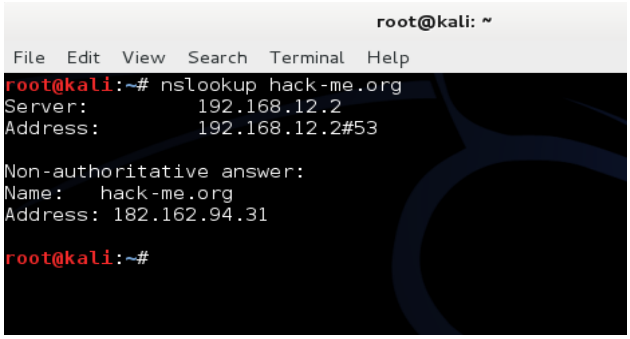
2) Hasil Reconaissance online

Informasi yang didapatkan dari hasil reconnaissance terhadap web server dengan terkoneksi pada jaringan internet. Dilakukan dengan beberapa

Menggunakan nslookup untuk mengetahui informasi ip address website hack-me.org.

a) Hasil nslookup

Hasil nslookup terhadap situs hack-me.org, didapat beberapa informasi.



Gambar 11. Hasil nslook pada website hack-me.org

Informasi dari situs nslookup bahwa didapat dari situs hack-me dengan ip dari domain tersebut adalah 182.162.94.31.

b) Hasil Whois

Whois merupakan sebuah protokol query/response yang digunakan untuk melakukan query terhadap database yang bertujuan untuk mendapatkan pemilik dari sebuah nama domain dan alamat IP pada Internet. Hasil whois terhadap ip address 182.162.94.31 digunakan dengan mengakses situs whois.domaintools.com.

IP Information for 182.162.94.31
Quick Stats
inetnum: 182.162.0.0 - 182.162.255.255
netname: KIDC
descr: LG TELECOM KIDC
descr: KIDC, 261-1 Nonhyun-dong, Kangnam-gu, Seoul
descr: **********
descr: Allocated to KRNIC Member.
descr: If you would like to find assignment
descr: information in detail please refer to
descr: the KRNIC Whois Database at:
descr: http://whois.nic.or.kr/english/index.htm
descr: **********
country: KR
admin-c: JA366-AP
tech-c: JA366-AP
status: ALLOCATED PORTABLE
remarks: www.kidc.net
mnt-by: MNT-KRNIC-AP
mnt-lower: MNT-KRNIC-AP

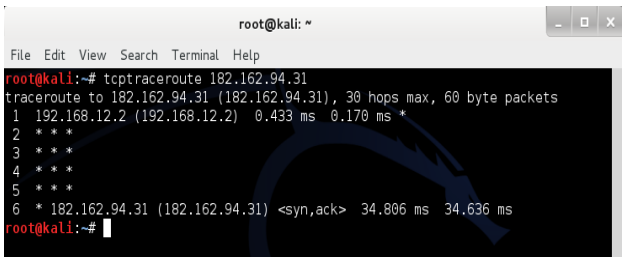
changed: hostmaster@nic.or.kr 20100406
source: APNIC

person: Jinhoon Ahn
nic-hdl: JA366-AP
e-mail: ip@kidc.net
address: 261-1 Nonhyun-dong, Kangnam-gu, Seoul
phone: +82-2-2086-2926
fax-no: +82-2-2086-2939
country: KR
changed: hostmast@nic.or.kr 20100401
mnt-by: MNT-KRNIC-AP
source: APNIC

inetnum: 182.162.0.0 - 182.162.255.255
netname: KIDC-KR
descr: LG DACOM KIDC
country: KR
admin-c: IA115-KR
tech-c: IM115-KR
status: ALLOCATED PORTABLE
mnt-by: MNT-KRNIC-AP
mnt-irt: IRT-KRNIC-KR
remarks:
This information has been partially mirrored by APNIC fr
om
remarks:
KRNIC. To obtain more specific information, please use t
he
remarks: KRNIC whois server at whois.krnic.net.
changed: hostmaster@nic.or.kr
source: KRNIC

c) Hasil Tcptraceroute

Tcptraceroute yang dilakukan terhadap ip 182.162.94.31 terdapat informasi seperti pada Gambar 12.

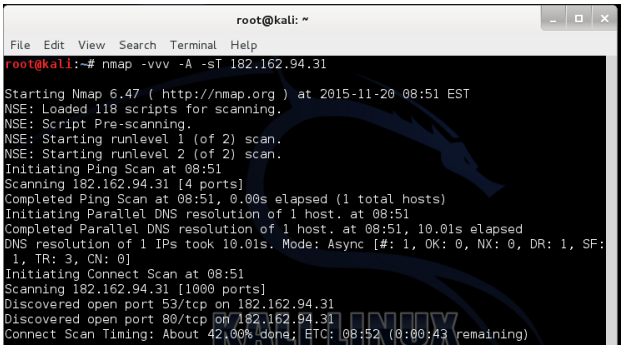


Gambar 12. Hasil pengujian tcptraceroute

d) Hasil nmap

Ada dua kali traceroute dari computer klien ke server hack-me.com yaitu
TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 0.24 ms 192.168.12.2
2 ... 21
22 196.85 ms 182.162.94.31

Begitu juga dengan port yang terbuka pada server tersebut adalah 53 dan 80.



Gambar 13. Hasil nmap pada ip address 182.162.94.31

Port 53 merupakan protocol MikroTik RouterOS named or OpenDNS Updater.

B) Pembahasan

Sesuai dengan rencana kerja yang dipaparkan pada bab III, bahwa penelitian ini dilakukan beberapa tahap untuk mendapatkan hasil yang diinginkan.

1) Tahapan persiapan

Persiapan ini terdiri dari hardware dan software yang dibutuhkan antara lain. Hardware yang digunakan dalam penelitian ini adalah dua perangkat computer. Dimana 1 di fungsikan sebagai server dan yang satunya digunakan sebagai klien. Sebagai computer server software yang di installkan adalah vmware sebagai mesin virtual dan linux ubuntu server.

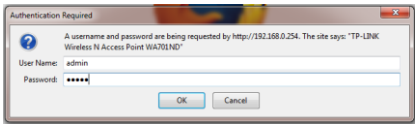
Kedua computer dikoneksikan dengan perangkat access point, untuk terkoneksi ke jaringan internet dari perangkat akses point terkoneksi dengan modem.

2) Tahapan installasi

Cara konfigurasi Wireless sebagai acess point dengan nama ssid (service set Identifier) adalah Hotspot Puskom langkahnya sebagai berikut:

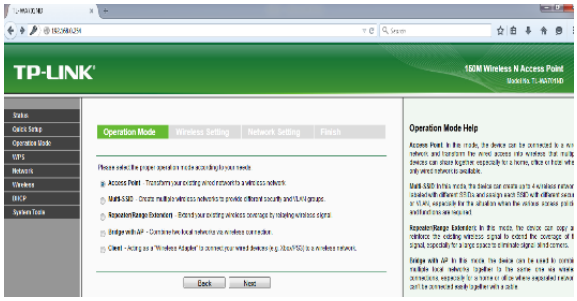
a) Terlebih dahulu gunakan kabel utp untuk menghubungkan perangkat Acess point dengan laptop untuk mengkonfigurasi perangkat.
b) Setting ip address laptop berada pada network address perangkat access point. Yang peneliti lakukan dengan alamat ip 192.168.0.123.
c) Jalankan aplikasi Browser pada laptop, karna panel acess point tampilan berbasis web. Kemudian masukan ip address acess point dan tekan Enter. Ip address default acess point yaitu 192.168.0.254.
d) Kemudian akan muncul pop-up untuk memasukkan username dan password panel.

Secara default, usernamenya adalah admin sedangkan passwordnya juga sama admin.



Gambar 14. Autentikasi username dan password masuk ke panel acess point

e. Tampilan panel setelah terbuka.



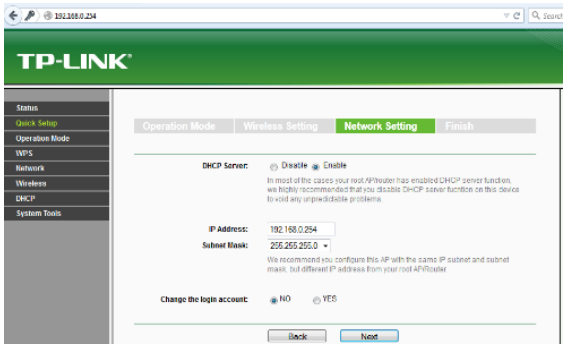
Gambar 15. Tampilan panel acess point tp-link

Pilihan yang dikonfigurasi pada perangkat acess point yaitu dijadikan sebagai perangkat *Acess Point.* Perangkat inilah yang berfungsi sebagai penghubung beberapa laptop siswa dan guru.

f. Memberikan nama SSID untuk perangkat acess point.

SSID (Service set Identification) merupakan nama service untuk koneksi pada jaringan wireless. Nama SSID yang penulis konfigurasi adalah Hotspot Puskom.

Berikutnya klik tombol next untuk melakukan sebagai media koneksi pada jaringan wireless smp pgri mengakatifkan network dengan sistem DHCP. Konfigurasi host dinamik DHCP yaitu untuk memudahkan pengalokasian alamat ip address.



Gambar 16. Mengaktifkan DHCP pada Perangkat Acess Point

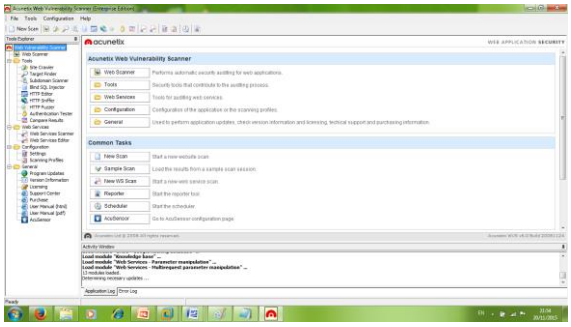
Subnetmask yang digunakan adalah subnetmask pada jaringan kelas C subnetmasknya adalah 255.255.255.0. kemudian klik next dan Finish.

3) Proses Reconaissance dengan Accunetik vulnarebility

Keamanan web memang sangat penting untuk menjamin kelangsungan website agar tetap online dan banyak di kunjungi oleh orang lain.

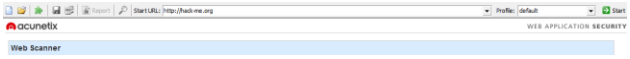
Banyak cara yang dapat dilakukan untuk audit website jika kita memang tidak punya basic ke ilmuan untuk mengamankan secara manual. salah satunya dapat dilakukan menggunakan software yaitu menggunakan acunetix Web Vulnerability Scanner. Software ini dapat offline maupun online.

Pertama jalankan software acunetix ini kemudian klik File ==>> New.



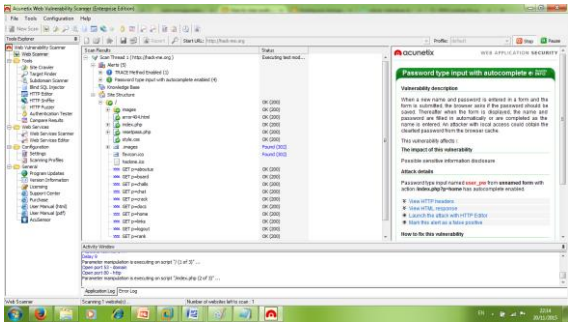
Gambar 17. Menjalankan acunetix Web Vulnerability Scanner

Kemudian klik web scanner, untuk memasukan alamat web dalam mendapatkan reconnaissance.



Gambar 18. Scanner hack-me.org

Hasil Reconaissence terhadap ip 182.162.94.31 terdapat beberapa informasi struktur dari website hack-me.org. dan informasi ancaman terhadap keamanan website tersebut ditampilkan dalam alert. Seperti pada gambar 27.



Gambar 19. Struktur website ditampilkan

C) Hasil Pengujian

1) Pengujian Pada Jaringan Wireless

Pada pengujian ini dilakukan dari komputer klien dan computer server yang sama terkoneksi dengan hotspot puskom. Klien melakukan reconnaissance terhadap server yang situs. Hasil dari pengujian tersebut pada Tabel 2.

Tabel 2. Analisa pada Jaringan Wireless

No	Analisa	Hasil	Kesimpulan
1	Name Hosting	192.168.12.132/situs	Informasi dari softaware accunetix
2	Sistem Operasi	Sistem Operasi server adalah linux ubuntu 12.01	Tool nmap dari kali linux untuk mendapatkan informasi so.
3	Port dan Protocol	Pada server port yang discovered adalah port 22,23 dan 80	Port 22 protocol ssh, 23 protocol telnet dan 80 protocol http
4	Ip Address	192.168.12.132/24	Whois pada kali linux untuk mendapatkan informasi ip

2) Pengujian pada jaringan internet

Pengujian pada jaringan internet dilakukan terhadap ip address 182.162.94.31. hasil yang didapatkan dari pengujian ini terlihat dari Tabel 3.

Tabel 3. Pengujian Akses Remote Server

No	Analisa	Hasil	Kesimpulan
1	Hosting	- Hack-me.org - Nslookup :182.162.94.31 - Lokasi ip address: Korea, Republic of Seoul Lg Telecom Kidc - Webserver: apache - Webserver ada vulnarebility	Website hackme berlokasikan di korea setalah discaning dengan software accunetix. Untuk informasi webserver memiliki vulnarebility dengan tool nmap pada kali linux
2	Sistem Operasi	Windows 7	Tool nmap menemukan informasi sistem operasi hack-me.org. dengan memberikan perintah –vvv –A
3	Port dan Protocol	- Port 23 dan 80 discovered open - Protocol Miktotik dan http	Port 23 untuk mikrotik dicoba diakses dari klien tidak berhasil. Dan port 80 merupakan layanan service dari http
4	Ip Address	182.162.0.0 - 182.162.255.255	Tool whois menemukan informasi terhadap server.

V. PENUTUP

A) Kesimpulan

Beberapa hal yang dapat disimpulkan dari hasil penelitian ini, antara lain:

1) Proses reconnaissance dapat dilakukan dengan beberapa aplikasi pada linux kali dan accunetix nulnarebility scanning.
2) Pengujian dilakukan dua tahapan, yaitu local dan internet dan hasil yang didapat dari local tidak banyak informasi yang didapatkan.
3) Informasi yang didapatkan dari hasil reconnaissance ini sangat membantu administrator dalam mengelola keamanan terhadap website.
4) Pada website hack-me.org tidak dapat merequest permintaan dari klien karna website dilindungi oleh firewall

B) Saran

Berdasarkan penelitian yang telah dilakukan beberapa saran yang dapat penulis berikan :

1) Pengujian local sebaiknya ada domain name sistem yang terkoneksi dengan jaringan wireless.
2) Tidak adanya infrastruktur yang baik pada jaringan wireless banyak informasi yang diharapkan tidak dapat diketahui.

DAFTAR PUSTAKA

Ahmad Yani, 2007, *Panduan Membangun Jaringan Komputer*: Bandung, 107 Hal.

Jufriadif, 2007, Komunikasi Data dan Jaringan Komputer teori dan praktek, Padang, UPI-YPTK:161

Kustanto & Daniel T Saputro, 2008, *Membangun Server Internet dengan Mikrotik OS*, Yogyakarta, Gava Media: 189.

Sovana Iwan, 2011, *Teori dan Modul Praktikum Jaringan Komputer*, Bandung, Modula: 362.

Tom Thomas, 2010, *Network Security First-step*, Yogyakarta, Andi Offset: 511 Hal