ANALISA PENGUJIAN KERENTANAN TERHADAP WEB SERVER SIMAK (Studi Kasus : STMIK Kharisma Karawang)

Wahyudi
Sistem Informasi, STMIK Kharisma Karawang.
Jl. Pangkal Perjuangan KM.1 Karawang
Wahyudi008@gmail.com

Abstrak

Pengujian penetrasi jaringan adalah salah satu metode yang dapat digunakan untuk mengidentifikasi dan mengeksploitasi kerentanan keamanan pada sistem komputer. Ini membantu untuk mengevaluasi efektivitas dan ketidakefektifan setiap tindakan keamanan yang telah dilakukan. STMIK Kharisma Karawang sebagai salah satu perguruan tinggi yang memiliki jurusan teknologi informasi tentunya sangat berkepentingan untuk mengamankan seluruh data/asset yang ada. Tujuan dari penulisan penelitian ini adalah untuk memberikan gambaran umum, manfaat, strategi dan metodologi yang digunakan dalam pengujian penetrasi jaringan serta mengidentifikasi tren masa depan dan arah penelitian lebih lanjut dalam pengujian penetrasi dan keamanan jaringan. Metodologi pengujian penetrasi mencakup tiga fase: persiapan pengujian, pengujian dan analisis pengujian. Tahap pengujian melibatkan langkah-langkah berikut: pengumpulan informasi, analisis kerentanan, dan eksploitasi kerentanan. Pengujian penetrasi tidak hanya dapat dilakukan pada komputer tapi juga dapat berfungsi di berbagai macam jaringan: jaringan internet (IP), SS7, nirkabel, dan konvergensi.

Kata kunci: pengujian penetrasi, analisis kerentanan, kejahatan dunia maya, jaringan komputer

Abstract

Network penetration testing is one method that can be used to identify and exploit security vulnerabilities in computer systems. This helps to evaluate the effectiveness and ineffectiveness of any security measures that have been taken. STMIK Kharisma Karawang as one of the universities that has information technology majors is certainly very interested in securing all existing data / assets. The purpose of writing this study is to provide an overview, benefits, strategies and methodologies used in network penetration testing and identify future trends and further research directions in penetration testing and network security. The penetration testing methodology includes three phases: preparation for testing, testing and analysis of testing. The testing phase involves the following steps: information gathering, vulnerability analysis, and vulnerability exploitation. Penetration testing can not only be done on computers but also can function on various networks: internet (IP), SS7, wireless, and convergence.
Keywords: penetration testing, vulnerability analysis, cyberspace crime, computer networks

PENDAHULUAN

STMIK Kharisma Karawang sebagai salah satu perguruan tinggi yang berada di bawah KOPERTIS Wilayah IV Jawa Barat, sebagai perguruan tinggi teknologi informasi yang dalam kegiatan proses belajar mengajar banyak menggunakan komputer. Seiring dengan perkembangan teknologi, tentunya diperlukan suatu media penyimpanan yang digunakan untuk menyimpan seluruh kegiatan kampus maupun data mahasiswa untuk kelancaran proses belajarnya yang semua itu tentunya memerlukan sebuah perangkat untuk mengolah dan menyimpan data tersebut atau yang lebih kita kenal dengan sebutan server. Seiring dengan perkembangan teknologi tersebut, keamanan

terhadap asset/data perlu menjadi perhatian oleh semua pihak. Mengingat banyaknya serangan yang dilakukan penyerang belakangan ini yang bertujuan mengambil data-data yang sensitif.

Untuk menghindari kerugian yang diakibatkan oleh serangan penyerang, maka perlu dilakukan langkah awal yang harus dilakukan adalah dengan melakukan semacam evaluasi terhadap keamanan server yang ada. Tujuan dari evaluasi keamanan ini adalah untuk mengurangi kemungkinan-kemungkinan yang dapat terjadi akibat penyalahgunaan terhadap asset/data yang ada di STMIK Kharisma Karawang.

Untuk melindungi asset / data yang ada, keamanan menjadi salah satu isu utama dalam sistem informasi. Konektivitas komputer tumbuh melalui internet, yang diperluas dengan peningkatan sistem dan pertumbuhan yang begitu cepat dari kompleksitas sistem. Perkembangan dunia komputasi yang begitu pesat telah membuka masalah keamanan perangkat lunak yang lebih besar daripada di masa sebelumnya. Selain itu, pentingnya melindungi informasi dengan mengikuti pendekatan yang baik dan terstruktur untuk memberikan perlindungan terhadap risiko yang mungkin terjadi.

Dalam upaya untuk memecahkan masalah keamanan dan mematuhi aturan keamanan maka berbagai metode jaminan keamanan dilakukan termasuk desain yang baik dari perangkat lunak yang digunakan dalam pengujian penetrasi.

Pengujian penetrasi merupakan salah satu metode komprehensif untuk menguji kelengkapan, keterpaduan, operasional dan dasar dunia komputer yang terdiri dari perangkat keras, perangkat lunak dan manusia. Dalam proses dan penanggulangannya melibatkan analisa sistem aktif untuk setiap potensi kerentanan, termasuk kekurangan atau konfigurasi sistem yang tidak benar, kelemahan *hardware* maupun *software*.

TUJUAN

Penetration Test (*Pentest*) atau pengujian kerentanan adalah sebuah metode untuk melakukan evaluasi terhadap keamanan dari sebuah sistem dan jaringan komputer. Evaluasi dilakukan dengan cara melakukan sebuah simulasi serangan (*attack*). Hasil dari *pentest* ini sangat penting sebagai masukan bagi pengelola sistem informasi untuk memperbaiki tingkat keamanan dari sistem komputernya. Laporan hasil *Pentest* akan memberikan masukan terhadap kondisi kerentanan terhadap sebuah sistem sehingga memudahkan dalam melakukan evaluasi dari sistem keamanan komputer yang sedang berjalan.

Vulnerability Assessment and Penetration Testing Technique [12]

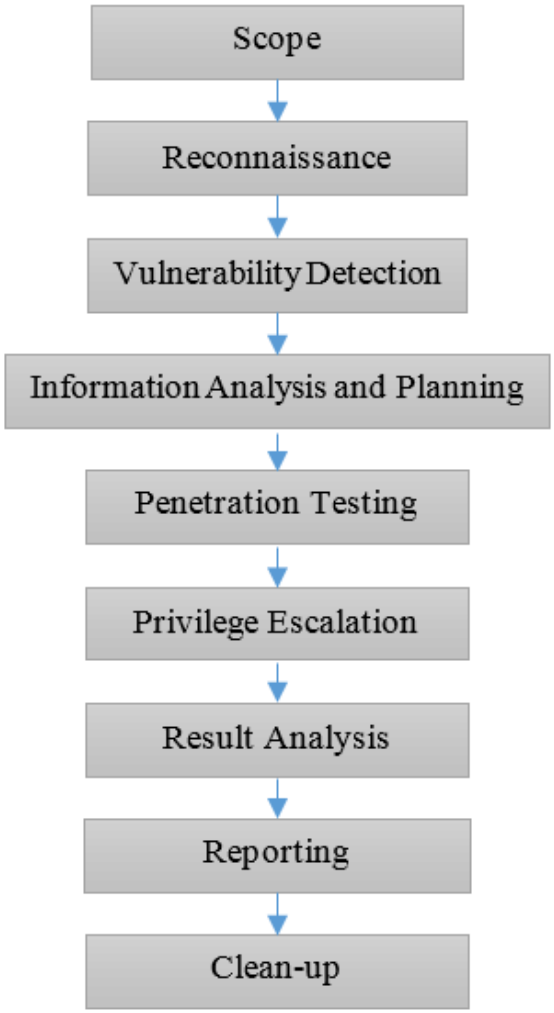
Vulnerability Assessment Technique

1. Analisa Statis – pada teknik ini tidak melakukan exploitasi terhadap sistem melainkan hanya menganalisis struktur kode dan konten dari sebuah sistem. Pada teknik ini hanya mencari tahu tentang semua jenis kerentanan. Kelemahan dari teknik ini adalah sangat lambat dan membutuhkan waktu yang lama untuk melakukannya.
2. Pengujian Manual – dalam pengujian ini tidak memerlukan alat atau perangkat lunak apa pun untuk mengetahui kerentanan yang terdapat dalam sebuah sistem, yang digunakan dalam pengujian ini adalah pengetahuan dan pengalaman. Keuntungan dari teknik ini adalah biaya yang murah dibandingkan dengan teknik yang lainnya.
3. Pengujian Otomatis – pengujian ini menggunakan alat penguji kerentanan otomatis untuk mengetahui kerentanan dalam sistem. Keuntungan dari pengujian ini adalah pengerjaan penetrasi yang lebih cepat dan mudah.
4. Pengujian *fuzz* – juga dikenal sebagai *fuzzing*, pengujian ini dilakukan dengan cara memasukan data yang tidak valid atau acak ke dalam sistem dan kemudian mencari *crash*-nya.

Penetration Testing Technique

Pada teknik ini terdapat beberapa teknik dan metode untuk melakukan *Pentest,* diantaranya adalah apa yang disebut dengan *black box, white box* dan *grey box. Black box testing* adalah metode *Pentest* dimana diasumsikan penguji tidak mengetahui sama sekali infrastruktur dari target *pentest* [9]. Dengan demikian pada *black box test* ini, penguji harus mencoba untuk menggali dari awal semua informasi yang diperlukan kemudian melakukan analisis serta menentukan jenis *attack/*serangan

yang akan dilakukan. Pada *White box testing* terjadi sebaliknya, penguji telah mengetahui semua informasi yang diperlukan untuk melakukan *pentest* [9]. Sementara *gray box* atau kombinasi dari kondisi *black box* dan *white box* [9]. Pengertian lain dari *white box* adalah *" full disclosure"*, *grey box* adalah *" partial disclosure"* dan *black box* adalah *" blind disclosure"* .

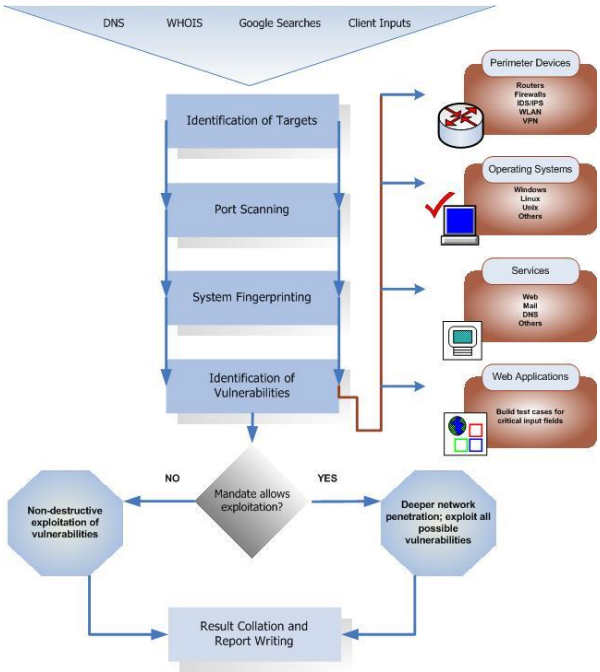


Gambar 1. *Vulnerability Assessment and Penetration Testing Life cycle*

Dalam *Vulnerability Assessment* and Penetration testing terdapat 9 langkah [7 dan 12], seperti diperlihatkan pada Gambar 1. Langkah pertama adalah ruang lingkup pengetesan dapat menggunakan teknik *black box*, *grey box* dan *white box*. Langkah berikut nya adalah menganalisa informasi yang diperoleh dari langkah pertama seperti sistem operasi yang digunakan, jaringan dan alamat IP yang digunakan. Langkah berikutnya yaitu *vulnerability detection* dimana pada langkah ini adalah mendeteksi kelemahan yang terdapat dari informasi yang diperoleh di langkah kedua. Setelah pengujian ini langkah berikutnya adalah *information analysis and planning* dengan cara menganalisis setiap informasi yang diperoleh dari langkah kedua untuk mengetahui kerentanannya dan membuat rencana untuk *penetration testing,* yang akan dilakukan pada langkah ini adalah melakukan pengetesan untuk mengetahui kerentanan sebuah sistem. Setelah berhasil menembus sistem dengan memperoleh privilege pada sistem. Langkah selanjutnya adalah melakukan *result analysis* berupa menganalisis seluruh kerentanan yang diperoleh dari sebuah sistem dan menyusun rekomendasi untuk mengatasi kerentanan tersebut.

Semua kegiatan ini didokumentasikan dan diinformasikan ke pihak yang berwenang untuk diambil tindakan yang sesuai. Setelah semua langkah ini dilakukan, sistem yang memiliki kerentanan harus segera diperbaiki atau ditutup seluruh kelemahannya.

Gambaran lebih detail dari standard pelaksanaan pentest [1] adalah sebagaimana terdapat dalam Gambar 2 dibawah ini :



Gambar 2. Standard pelaksanaan *Penetration Testing*

Ini merupakan langkah-langkah standar pelaksanaan pentest yang saat ini banyak digunakan.

Informasi terkait tentang kejahatan dan keamanan komputer dalam beberapa tahun terakhir ini perlu disadari bahwa tindakan pencegahan harus dilakukan sedini mungkin, untuk melindungi seluruh informasi data sebelum serangan tersebut benar-benar terjadi. Perkembangan keamanan yang sangat cepat pada sebuah sistem yang semula merupakan sesuatu yang tidak diperhitungkan sekarang menjadi sesuatu yang harus ada dan menjadi perhatian khusus. [2][6]. Manajemen mulai menyadari bahwa keamanan merupakan bagian penting dari setiap sistem dan mengabaikannya dapat menyebabkan masalah besar. Namun, salah satu isu yang telah berkembang adalah pertanyaan mengenai apakah tindakan pencegahan yang dilakukan oleh sebuah organisasi cukup atau tidak. Bagaimana manajemen dapat memastikan bahwa sistem dan keamanan jaringan mereka aman, sehat dan terutama kerentanan tidak diabaikan [2][6]. *Audit* berkala dan pengujian penetrasi yang dilakukan sangat luar biasa dengan menggunakan metode yang handal dan biaya yang besar untuk meyakinkan bahwa data/*asset* yang dimiliki dalam kondisi aman - setidaknya untuk sementara waktu. Jenis penilaian ini hanya menyediakan "*snapshot in time*" dari kondisi keamanan sistem atau jaringan [2][14]. Salah satu metode yang digunakan untuk mengikuti terhadap perubahan keamanan internal guna melindungi terhadap data/*asset* adalah dengan melakukan pengecekan terhadap kerentanan dengan cara melakukan pengecekan secara berkala dengan menggunakan alat pemindaian otomatis. Salah satu alat tersebut adalah *NESSUS*, utilitas *freeware* yang dirancang untuk mengidentifikasi titik-titik kerentanan suatu sistem dan memberikan informasi tentang cara memperbaikinya. Tujuan dari makalah ini adalah untuk mengilustrasikan manfaat penerapan *NESSUS* sebagai pemindai kerentanan berbiaya rendah sebagai pelengkap model keamanan yang ada. Materi ini akan membahas mengenai pemindaian kerentanan secara umum, apa arti *NESSUS*, bagaimana cara memindai jaringan sendiri, dan akhirnya mengapa pemindai kerentanan adalah komponen penting dari model keamanan yang efektif.

PENETRATION TEST

Dahulu untuk melindungi komputer dari pengguna yang tidak sah dengan cara memberi *password* pada sistem komputer, dan anda bisa yakin bahwa data yang terdapat dalam sistem komputer kita aman terhadap pengguna yang tidak sah untuk mengakses komputer tersebut. Dengan kerentanan baru seperti *buffer overflows* dan serangan *denial of service*, keamanan telah menjadi perhatian lebih dari sekedar memperbaiki *bug* dari kerusakan pada sistem komputer. *Server Web Microsoft IIS* telah menjadi target oleh peretas dengan cara mengeksploitasi kelemahan sistem. Metode peretasan ini bukan dengan cara mengambil alih sistem dengan cara merentas password *admin* tapi melakukan manipulasi layanan untuk menyediakan hak akses (*command prompt*) kepada orang yang tidak sah. *Administrator* harus menjadi orang yang pertama yang mengetahui kelemahan tersebut dan melakukan perbaikan, yaitu dengan cara memperbaiki lubang ini, biasanya untuk menutupi atau memperbaikinya perlu dilakukan *update patch* atau menonaktifkan layanan yang tidak diinginkan.

Salah satu pusat perhatian terhadap keamanan adalah dengan begitu cepatnya perkembangan internet yang menjadikan seluruh server terhubung satu dengan yang lainnya. Menjaga keamanan menjadi hal yang menakutkan ketika melihat begitu banyak peralatan perentas yang dapat digunakan untuk melancarkan serangan ke server secara automatis.

Meskipun proses peretasan tersebut berhasil dilakukan, dalam waktu yang singkat pula perangkat lunak baru bermunculan guna mengatasi serangan tersebut. Melakukan pencegahan secara aktif terhadap kerentanan dapat membantu mengidentifikasi layanan atau kerentanan yang tidak diinginkan secara dini sebelum dapat membahayakan sistem yang ada. Tidak sedikit untuk mengamankan data/asset yang dimiliki perusahaan merekrut para ahli keamanan yang lebih baik dikarenakan sumber daya yang ada belum dapat menanganinya.

Dasar yang kuat untuk keamanan yang baik adalah mengembangkan keahlian internal dalam pengujian kerentanan yang dilakukan oleh

administrator sistem dan untuk mengembangkan metode pelaksanaan pengujian yang efektif [9]. Selanjutnya, dengan memahami atau mengetahui bagaimana seorang penyusup mencoba merusak sistem yang dimiliki diharapkan *administrator* dapat melindungi sistemnya secara maksimal, ini adalah asumsi bahwa semakin profesional seorang tahu tentang alat yang digunakan untuk melawan perentas, maka semakin baik [2][9]. Dengan melakukan pemindaian kerentanan internal, dengan menggunakan utilitas seperti *NESSUS*, maka pekerjaan terkait dengan keamanan akan dilakukan secara otomatis, teratur dan untuk memastikan menggunakan sistem keamanan yang tepat [2][14]).

MENGAPA PERLU PENETRATION TEST ?

Tujuan utama dari pengujian penetrasi adalah mengidentifikasi sistem komputer, jaringan atau aplikasi web untuk menemukan kerentanan keamanan yang dapat dieksploitasi penyerang. Pengujian penetrasi dapat diotomatisasi dengan aplikasi perangkat lunak atau dilakukan secara manual. Sistem komputer yang profesional akan menggunakan pengujian penetrasi untuk mengatasi masalah kerentanan dan menitik beratkan pada kerentanan tingkat tinggi.

KEUNTUNGAN DARI *PENETRATION TEST*

Dari perspektif bisnis, pengujian penetrasi membantu melindungi organisasi dari kerugian melalui pencegahan kehilangan asset., pembuktian uji kelayakan dan kepatuhan kepada regulator industri, pelanggan, pemegang saham; menjaga citra perusahaan; dan merasionalisasi investasi keamanan informasi [2][4].

Rata-rata Perusahaan menghabiskan biaya 11,7 Juta USD untuk masalah keamanan cyber; penambahan biaya keamanan mencapai 22,7% per tahun; rata-rata peningkatan pelanggaran keamanan sebanyak 130 kasus per tahun; pertumbuhan kejahatan komputer yang mencapai 27,4% per tahun [11].

Proses pemulihan dari pelanggaran keamanan dapat merugikan bisnis sampai ribuan atau bahkan jutaan dolar termasuk pengeluaran untuk program perlindungan pelanggan, denda peraturan, dan hilangnya pengoperasian bisnis. Sebuah studi baru-baru ini oleh *IBM Security* menemukan bahwa biaya rata-rata dari pelanggaran data secara global pada tahun 2018 adalah $ 3,86 juta, yang 6,4% lebih tinggi dibandingkan dengan hasil tahun lalu [12].

Pengujian penetrasi dapat mengidentifikasi dan mengatasi risiko sebelum pelanggaran keamanan terjadi, sehingga pencegahan dapat dilakukan untuk mengurangi kerugian finansial yang disebabkan oleh pelanggaran keamanan. Dunia Industri telah membuat peraturan mengenai persyaratan sistem komputasi. Ketidakpatuhan pada persyaratan dapat mengakibatkan perusahaan menerima sanksi berat, pemenjaraan, atau *valid* [2][4].

Pengujian penetrasi, sebagai layanan proaktif, memberikan informasi yang tidak dapat dibantah yang dapat membantu perusahaan untuk memenuhi aspek audit atau kepatuhan peraturan. Satu insiden yang menyebabkan data klien yang disusupi hilang atau rusak dapat menghilangkan kepercayaan konsumen dan menghilangkan seluruh reputasi bisnis yang dapat membahayakan seluruh organisasi. Pengujian penetrasi menciptakan kesadaran untuk meningkat tentang pentingnya keamanan di semua tingkat organisasi. Ini membantu organisasi menghindari insiden keamanan yang mengancam citra, risiko hilangnya reputasi dan berdampak pada kesetiaan pelanggan. Pengujian penetrasi mengevaluasi efektivitas produk keamanan yang ada dan menyediakan data pendukung untuk investasi masa depan atau peningkatan teknologi keamanan. Ini dapat dijadikan sebagai "Bukti Permasalahan yang ada pada Keamanan" dan kasus yang nyata untuk proposal investasi kepada manajemen senior [2][14].

METODE PENELITIAN

Metode pengembangan sistem yang digunakan dalam penelitian ini adalah dengan menggunakan teknik *grey box* untuk melakukan pengujian penetrasi terhadap server yang akan di cek kelemahan dengan menggunakan aplikasi *Software NESSUS* Tahapan untuk proses penelitian ini adalah dengan melakukan beberapa tahapan seperti :

1. Identifikasi target, ini merupakan proses awal yaitu dengan menentukan target server yang akan dilakukan *assessment*.

2. *Port Scanning*, proses dimana aplikasi akan melakukan *scanning* terhadap target yang akan di *assessment*.
3. *System Fingerprint* adalah proses untuk mengetahui informasi yang terdapat pada sistem/server yang di-*scan*.
4. Mengidentifikasi kelemahan pada sistem, adalah proses identifikasi kelemahan yang terdapat dalam sebuah sistem, informasi ini diperoleh dari proses *scanning*. Kategori Informasi kelemahan sistem yang diperoleh dapat berupa kategori *high risk, medium risk, low risk* dan *info* .

JENIS DATA

Jenis data yang digunakan dalam peneliti ada dua jenis yaitu :

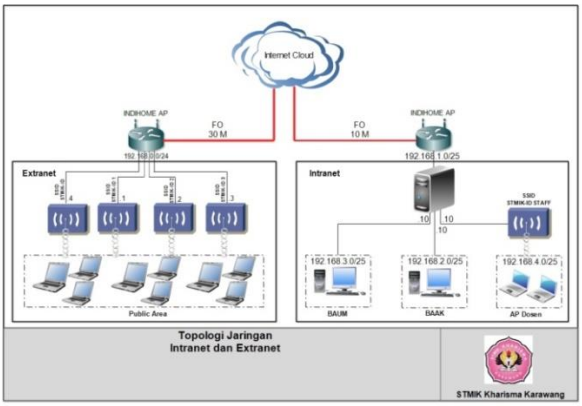
1. Data Primer yaitu data-data yang diperoleh peneliti secara langsung dengan melakukan proses *assessment* pada server yang terdapat di STMIK Kharisma dan berdasarkan pengalaman peneliti saat melakukan *network assessment* di beberapa perusahaan di Jakarta.
2. Data Sekunder, yaitu data-data yang diperoleh peneliti dari literatur, buku referensi, ataupun dari *browsing internet*.

METODE PENGUMPULAN DATA

Metode pengumpulan data yang dilakukan dalam penelitian ini adalah :

1. Observasi : dengan melakukan pengujian penetrasi terhadap server yang bersangkutan
2. Wawancara : mengumpulkan informasi terkait spesifikasi server, topologi jaringan dan segmentasi IP yang terdapat dalam jaringan yang ada.
3. Studi Pustaka : mengumpulkan literatur, buku referensi ataupun dari *browsing* di internet.

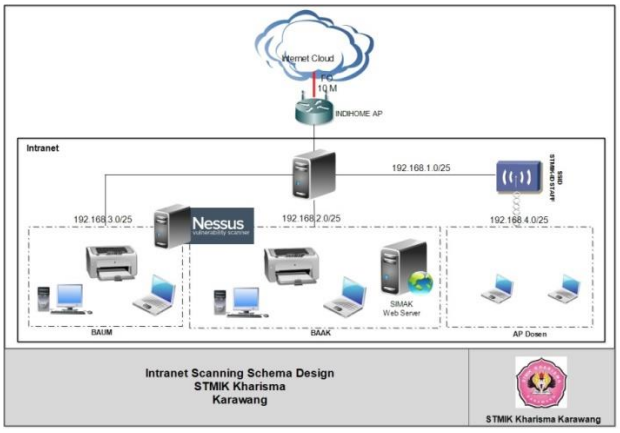
HASIL PENELITIAN DAN PEMBAHASAN



Gambar 3. Topologi Jaringan Intranet dan Extranet

Gambar di atas merupakan topologi *existing* dari jaringan yang akan di *assessment* di mana jaringan dibagi menjadi dua bagian yaitu *public area* di mana area ini dialokasikan untuk mahasiswa yang memilik besaran bandwidth sebesar 30M sedangkan area kedua adalah *private area* di mana komputer yang terhubung di area ini adalah staf dosen dan karyawan STMIK Kharisma dengan besaran bandwidth sebesar 10M. Untuk Server sendiri terletak di jaringan intranet atau *private area*.

INTRANET SCANNING SCHEMA DESIGN

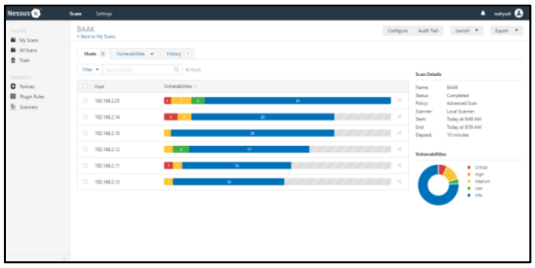


Gambar. 4 *Intranet Scanning Schema Design*

Gambar di atas merupakan rancangan untuk proses *assessment* jaringan di mana perangkat/aplikasi *NESSUS* ditempatkan di segment yang sama dengan Server yang akan di *scanning* (SIMAK Web Server). Proses *scanning* dapat dilakukan dengan cara men-*scanning* seluruh segment IP yang berada dalam satu

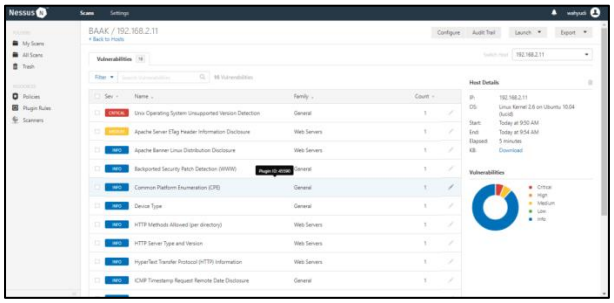
segment yang sama dengan server atau langsung ke server target. Dalam kasus ini scanning dilakukan secara langsung karena IP dari server tersebut sudah diketahui dalam hal ini segment IP yang akan di *scanning* adalah 192.168.2.0/24

HASIL SCANNING DAN ANALISIS



Gambar 5. Hasil *Scanning*

Dari hasil Gambar 5 diatas bahwa dari segment IP 192.168.2.0/24 hanya terdapat 6 komputer yang aktif atau online . Untuk SIMAK Web Server sendiri memiliki IP 192.168.2.11, berdasarkan gambar diatas terlihat bahwa pada IP tersebut terdapat 1 kelemahan/lubang yang berstatus *critical* dengan tanda warna merah, 1 kelemahan/lubang yang berstatus mediun dengan tanda warna kuning dan 14 yang berstatus *info* dengan tanda warna biru. Langkah selanjutnya adalah dengan melihat kelemahan-kelemahan apa saja yang terdapat pada IP 192.168.2.11 dengan cara melakukan *scanning* terhadap IP tersebut. seperti diperlihatkan pada gambar 6 dibawah ini.



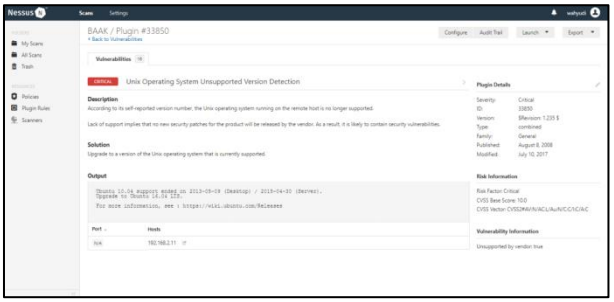
Gambar 6. Hasil *Scanning* SIMAK Web Server

Dari hasil *scanning* terhadap SIMAK Web Server (192.168.2.11) terdapat satu *critical* yaitu *Unix Operating System Unsupported Version Detection*, ini menginformasikan bahwa Sistem Operasi LINUX yang digunakan pada SIMAK Web Server menggunakan sistem operasi LINUX yang sudah tidak di dukung lagi oleh LINUX, hal tersebut dapat terjadi jika Sistem Operasi yang digunakan menggunakan versi yang sudah lawas.

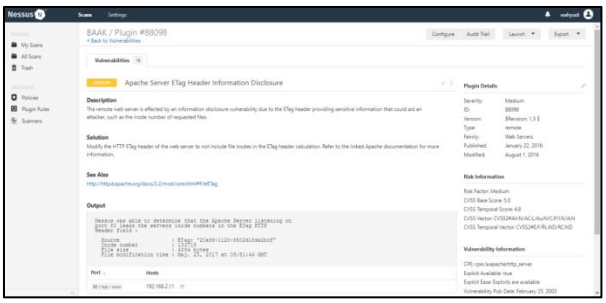
Kelemahan kedua yaitu *Apache Server ETag Header Information Disclosure* dengan status kerentanannya sedang. Pesan kerentanan ini menjelaskan bahwa terdapat informasi yang terbuka pada *Header ETag Apache Server* dan kelemahan ke tiga adalah berstatus informasi saja, ini tidak berdampak pada keamanan server itu sendiri.

DESKRIPSI dan SOLUSI

Penjelasan terkait dengan kelemahan dan pemecahan masalahnya, juga tersedia pada sistem *NESSUS* ini, untuk kelemahan yang berstatus *critical* dan *medium* dapat dilihat pada Gambar 7 dan Gambar 8 dibawah ini :



Gambar 7. *Description, Solution Critical Status*



Gambar 8. *Description, Solution Medium Status*

KESIMPULAN DAN SARAN

Kesimpulan : Pengetesan yang dilakukan untuk mengetahui kerentanan yang terdapat pada Web Server SIMAK yang terdapat di STMIK Kharisma Karawang adalah sebagai berikut :

1. *NESSUS* adalah salah satu aplikasi yang banyak digunakan untuk mengetahui kerentanan yang terdapat pada sebuah sistem komputer, selain dapat digunakan untuk pengujian penetrasi, juga terdapat *feature* lainnya berupa solusi untuk memecahkan setiap permasalahan yang ditemukan.
2. Hasil dari *assessment* pada *web server* SIMAK STMIK Kharisma dengan IP

192.168.2.11 ditemukan dua kelemahan yaitu *Unix Operating System Unsupported Version Detection* yang berstatus critical atau high risk dan *Apache Server ETag Header Information Disclosure* dengan status medium atau middle risk.

SARAN :

1. Perlu dilakukan *update/upgrade* terhadap sistem operasi yang terdapat pada Web Server SIMAK
2. Memodifikasi setiap informasi yang terdapat pada *ETag Header Apache Server*
3. Dilakukan pengecekan secara berkala guna menghindari serangan yang berasal dari luar dengan memanfaatkan kelemahan yang ada pada sistem.

DAFTAR PUSTAKA

[1]. Anonymous., "Penetration Test.", 2013., URL : https://www.niiconsulting.com

[2]. Bacudio, Aileen G.et.el., "An Overview of Penetration Testing" Nov 2011., URL : https://www.researchgate.net/publication/274174058_An_Overview_of_Penetration_Testing (diakses Dec 2018).

[3]. De Beaupré, Adrien. "Know Yourself: Vulnerability Assessments". June 21st, 2001. Sans Institute Information Security Reading Room. URL: http://rr.sans.org/audit/know.php (April 4th, 2002) .

[4]. Heiser, Jay. "Counterpoint: Beware the Red Herring". August 2000. Information Security Magazine. URL: http://www.infosecuritymag.com/articles/august00/features3.shtml (April 5th, 2002).

[5]. Https://catatanforensikadigital.wordpress.com/2013/11/14/penetration-test-pentest-2/ (diakses Sabtu, 17/12/2018)

[6]. Kurtz, George and Prosise, Chris. "Penetration Testing Exposed: Audits, Assessments & Tests (Oh, My) Part 3". September 2000. Information Security Magazine. URL: http://www.infosecuritymag.com/articles/september00/features3.shtml (April 5th, 2002).

[7]. Narayan Goel, Jai., "Vulnerability Assessment & Penetration Testing as a Cyber Defence Technologi". 3rd International Confference on Recent Trends in Computing 2015 (ICRTC-2015).

[8]. Nist, usaid mission site vulnerability assessment and remediation. 2015. URL: http://www.nist.gov. Last Accessed: JAN 2015

[9]. Payne, Patricia. "A Model for Peer Vulnerability Assessment". December 17th, 2001. Sans Institute Information Security Reading Room. URL: http://rr.sans.org/penetration/model.php (April 4th, 2002).

[10]. Prole, Ken., "White Box, Black Box, and Gray Box Vulnerbility Testing : What's the Different and Why Does It Matter ?". Jan, 2018. URL : https://codedx.com/2018/01/black-white-and-gray-box-vulnerability-testing-code-dx-blog/

[11]. Richard, Kevin. , "COST OF CYBER CRIME STUDY" Accenture Security 2017 URL : https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

[12]. Tripwire Guest., "5 Reasons Why Your Business Needs Penetration Testing.", Nov 2018., URL : https://www.tripwire.com/state-of-security/security-data-protection/5-reasons-business-needs-penetration-testing/

[13]. Vulnerability assessment and penetration testing (vapt). 2015. URL: http://memorize.com/vulnerability-assessment-and-penetration-te Last Accessed: JAN 2015.

[14]. Winkler, Ira. "Audits, Assessments & Tests (Oh, My) Part 1". July 2000. Information Security Magazine. URL: http://www.infosecuritymag.com/articles/july00/features4.shtml (April 5th, 2002).