IMPLEMENTASI METODE ONLINE SCANNER UNTUK MENCARI KERENTANAN KEAMANAN (VULNERABILITY) SERVER (Studi Kasus: Website www.unsika.ac.id)

Purwantoro

Program Studi Teknik Informatika
Universitas Singaperbangsa Karawang (UNSIKA)
Jl. Ronggowaluyo Teluk Jambe Timur - Karawang 41361 Jawa Barat
http://www.unsika.ac.id
purwantoro.masbro@staff.unsika.ac.id

Naskah diterima 21 Maret 2017

ABSTRACT

Computer Network Security system absolutly as important thing in managing server content proccess for user's necessity. The vulnerability of Computer security is the main priority for network access. online scanner for securities' vulnerability are provided by server developper.Internet network's. testing can be done through locally (LAN) or throught internet line. each online scanner server provide different result to client web browser depend on the avalilabilities'service of developper vulnerability scanner server provider

Keyword*: online,scanner, vulnerability, server, network,computer, testing.*

ABSTRAK

Sistem keamanan jaringan sangat penting dalam kegiatan pengelolaan sebuah server yang menyediakan content kebutuhan pengguna, kerentanan keamanan (vulnerability) menjadi fokus dan prioritas utama dalam sistem jaringan komputer untuk menjaga kelangsungan hidup jaringan sistem tersebut, scanner secara online banyak disediakan oleh pengelola situs dengan server yang semakin canggih. testing vunerability bisa dilakukan secara internal melalui jaringan LAN ataupun secara External, setiap Server Scanner akan memberikan informasi yang berbeda tergantung layanan yang disediakan.

Kata Kunci*: online,scanner, kerentanan, server, jaringan,komputer, test.*

I. PENDAHULUAN

Jaringan komputer atau *Computer network* adalah hubungan antar dua komputer atau lebih dengan perangkatnya yang saling berinteraksi sehingga mempunyai fungsi dan kegunaan tertentu dalam membantu kemudahan kegiatan manusia.

Dalam menjaga keberlangsungan jaringan, maka perlu diperhatikan hal-hal yang mengarah pada terjadinya kesalahan (*error*) yang disebabkan oleh perangkat keras (*hardware*), perangkat lunak (s*oftware*) ataupun kesalahan manusia yang mengoperasikan komputer dalam jaringan tersebut (*Human error*). Dalam komunikasi menggunakan jaringan pada komputer selalu berpotensi pada keamanan itu sendiri, yang lebih banyak adalah ancaman dari manusia pengguna jaringan komputer (*Network*). Website merupakan sarana yang memanfaatkan teknologi jaringan komputer, menyajikan antar muka (*user interface*) untuk komunikasi. Dalam pengelolaan data dan informasi, setiap website menggunakan komputer server untuk melayani kebutuhan informasi, data, email ataupun file, sehingga keberlangsungan hidup server mutlak diperlukan, setiap pengelola server harus selalu waspada dan selalu memelihara trafik paket data yang masuk ataupun yang keluar pada jaringan tersebut. Semakin baik sebuah website akan semakin banyak pengunjung yang memanfaatkan *content* website tersebut dan juga berbanding lurus dengan ancaman pada sistem jaringan tersebut,.

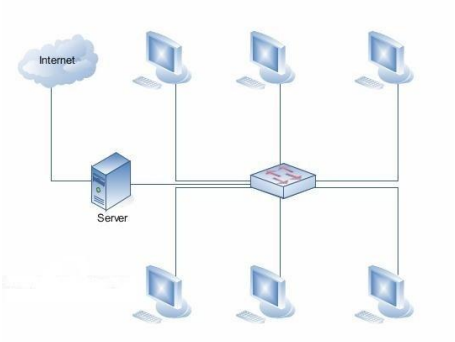
Kerentanan pada masalah keamanan (*vulnarebility*) sebuah server sangat berpotensi sebagi celah untuk menerobos keamanan jaringan tersebut dan sangat berbahaya pada proses pengelolaan data dan informasi, khususnya data dan informasi yang sangat berharga.

II. TINJAUAN PUSTAKA

2.1. Jaringan komputer

a. LAN(local Area Network)

LAN adalah jaringan komputer yang scoopnya kecil , seperti jaringan komputer yang ada di kantor,rumah, dan suatu tempat yang hanya digunakan untuk komunikasi pada lingkup kecil

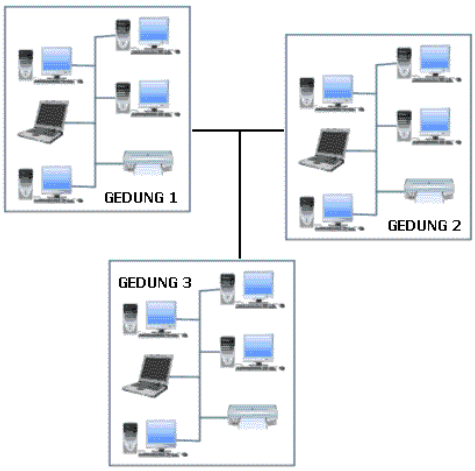


Gambar 1. arsitektur jaringan LAN

Jaringan LAN sering digunakan pada laboratorium sebuah lembaga pendidikan seperti sekolahan, lembaga kursus, internal perusahaan ataupun kampus-kampus.

b.MAN

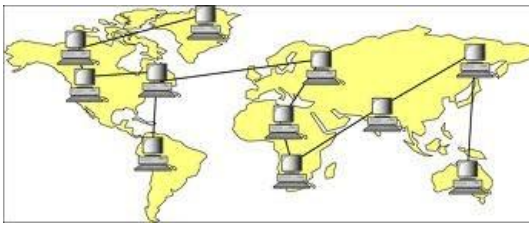
Metropolitan Area Network (MAN) adalah jaringan komputer yang wilayahnya mencakup dalam kota, jangkauan koneksi sampai 50 km. Jaringan ini adalah gabungan beberapa LAN yang lebih besar yang saling berinteraksi antar jaringan LAN internal ke jaringan internal LAN lainnya. Pada konsepnya MAN mempunyai daerah yang cakupannya lebih luas dari LAN. Jaringan ini digunakan untuk mempermudah keperluan pengelolaan data yang berikat pada wilayah tertentu.



Gambar 2. arsitektur jaringan MAN

c.WAN

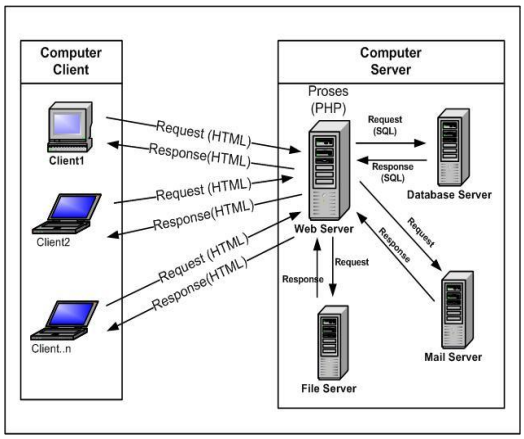
Wide Area Network adalah merupakan jaringan komputer yang mencakup area yang besar sebagai contoh yaitu jaringan komputer antar wilayah, kota atau bahkan negara, atau dapat didefinisikan juga sebagai jaringan komputer yang membutuhkan router dan saluran komunikasi publik



Gambar 3. arsitektur jaringan MAN

2.2.Komunikasi Client server

Komunikasi yang dilakukan pada pemanfaatan jaringan komputer adalah dengan menggunakan konsep *Client server* dimana server sebagai pelayan utama dalam pengelolaan data dan informasi. *Client* akan mengirimkan permintaan(*request*) pada web server, kemudian web server akan mengecek permintaan tersebut, bila permintaan berhubungan dengan *database*, maka web server akan berkomunikasi dengan *database* server dan kemudian akan menjawab dan menyampaikan permintaan client (*response*). Bila permintaan ada maka akan diberikan data atau informasi ke client, dan jika tidak ada maka web server akan menjawab dengan pesan permintaan yang diinginkan tidak ada. Dan bila permintaan client berhubungan dengan masalah email, maka web server akan meneruskan permintaan tersebut kepada mail server dan hasilnya akan disampaikan kepada client, dan jika permintaan client berkaitan dengan masalah file (*upload*dan *download*) maka web server akan berkomunikasi dengan file server untuk keperluan masalah tersebut.



Gambar 4. client server

2.3.Sistem keamanan jaringan komputer

Sistem keamanan jaringan komputer adalah cabang dari teknologi yang dikenal sebagai informasi keamanan yang diterapkan pada komputer dan jaringan. Tujuan keamanan komputer meliputi perlindungan informasi dari pihak yang tidak berkepentingan dengan tetap memudahkan akses dan penggunaan oleh para pengguna. Keamanan sistem komputer merupakan mekanisme dan proses kolektif terhadap informasi sensitif

dan berharga dan juga layanan yang dilindungi dari publik, ancaman kegiatan yang tidak sah atau individu yang tidak dapat dipercaya dan kejadian-kejadian yang tidak direncanakan adalah faktor yang harus selalu diwaspadai, pada sistem jaringan komputer terdapat beberapa konsep yang selalu menyertainya,yaitu:

- **resiko / tingkat bahaya**: menunjukkan seberapa besar kemungkinan keberhasilan para intruder dalam mengakses data dan informasi penting dalam sebuah jaringan melalui read aaccess, write access dan denial of service yang meutup utilitas jaringan normal dengan cara menghabiskan bandwidth, CPU dan Resources memory
- **ancaman**:usaha terhadap akses ilegal yang seolah-olah para intruder memiliki akses penuh dalam penguasaan jaringan tersebut
- **kerapuhan sistem *(vulnerability):*** seberapa kuat proteksi penjagaan dan penutupan celah keamanan sehingga para intruder tidak bisa memiliki otoritas akses pada jaringan komputer.

2.4 Jenis serangan vulnerability jaringan

Banyak cara dalam proses melakukan serangan pada sebuah jaringan komputer

a. Port scanning

Merupakan suatu proses untuk mencari dan membuka port pada suatu jaringan komputer. Dari hasil *scanning* akan didapat letak kelemahan sistem
tersebut. Pada dasarnya sistem *port scanning* udah untuk dideteksi, tetapi penyerang akan menggunakan beberapa cara metode untuk menyembunyikan

b. Teardrop

Teknik penyerangan yang dilakukan dengan mengeksploitasi proses *disassembly-reassembly* paket data. Dalam jaringan internet sering kali data harus dipotong menjadi paket yang lebih kecil untuk menjamin reliabilitas dan proses *multiple* akses jaringan. Pada proses pemotongan data paket yang normal, setiap potongan diberi informasi *offset* data yang berbunyi "Potongan *byte* ini merupakan potongan 600 *byte* dari total 800 *byte* paket yang dikirimkan". Program *teardrop* melakukan manipulasi potongan data sehingga terjadi *overlapping* antara paket yang diterima di bagian penerima setelah potongan-potongan paket disusun kembali

c. IP Spoofing

Teknik ini bekerja dengan mengganti alamat IP pengguna yang lain yang bukan penyerang sebenarnya. Hal ini terjadi karena salah rancang (*design flaw*)bagian urutan nomor (*sequence number*) dari paket TCP/IP. Dalam beberapa kasus, penyerang menggunakan satu alamat IP sumber yang spesifik pada semua paket IP yang keluar untuk membuat semua pengembalian paket IP dan pesan ICMP ke pemilik alamat tersebut.

d. ICMP Flood

Konsep ICMP Flood ini, Penyerang melakukan eksploitasi dengan tujuan untuk membuat target *host* menjadi terganggu, yang disebabkan oleh pengiriman sejumlah paket yang besar ke arah target *host* (membanjiri target). Eksploitasi sistem ini dilakukan dengan mengirimkan suatu perintah "ping" dengan tujuan *broadcast* atau *multicast* dimana pengirim dibuat seolah-olah adalah

target *host*. Semua balasan dikembalikan ke target *host*. Hal inilah yang menyebabkan *host* target menjadi terganggu dan menurunkan kinerja jaringan bahkan dapat menyebabkan *denial of service*

e. UDP Flood

UDP flood mengaitkan dua sistem tanpa disadari. Dengan cara *spoofing,User Datagram Protocol* (UDP) flood attack akan menempel pada *servis* UDP*chargen* di salah satu mesin, yang untuk keperluan "percobaan" akan mengirimkan sekelompok karakter ke mesin lain, yang diprogram untuk meng*echo* setiap kiriman karakter yang diterima melalui servis *chargen*. Karena paket UDP tersebut di-*spoofing* diantara ke dua mesin tersebut maka yang terjadi adalah "banjir" tanpa henti paket kiriman karakter yang tidak berguna diantara diantara kedua mesin tersebut. Untuk menanggulangi UDP flood, *disable* semua *servis* UDP di semua mesin di jaringan, atau dengan menyaring semua servis UDP yang masuk pada *firewall*.

f. Packet Interception

Gangguan jenis ini dilakukan dengan membaca paket di saat paket tersebut sedang mengalami *packet sniffing*. *Packet interception* merupakan cara penyerang untuk mendapatkan informasi yang ada di dalam paket tersebut. Hal ini dapat dicegah dengan mengenkripsi terlebih dahulu, sehingga penyerang akan mengalami kesulitan untuk membuka paket tersebut.

g. Smoorf Attack

Gangguan jenis ini biasanya dilakukan dengan menggunakan *IP spoofing*,yaitu mengubah nomor IP dari datangnya *request*. Dengan menggunakan *IP spoofing*, respons dari *ping* tadi dialamatkan ke komputer yang IP-nya di-*spoof*.Akibatnya, komputer tersebut akan menerima banyak paket. Hal ini dapat mengakibatkan pemborosanpenggunaan *bandwidth* jaringan yang menghubungkan komputer tersebut.

2.5 Aspek Keamanan Jaringan Komputer

Menurut dari Simson Garfinkel *"PGP : Pretty Good Privacy"*, O'Reilly & Associ-ates, Inc, 1995 bahwa Aspek–aspek keamanan komputer dapat dibedakan menjadi, antara lain :

a. Privacy / Confidentiality

Privacy adalah menjaga informasi dari orang yang tidak berhak mengakses, yang dimana lebih ke arah data-data yang bersifat privat, contohnya : Email seorang pemakai (*user*) tidak boleh dibaca oleh administrator. Sedangkan Confidentiality berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut. Contohnya : data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, pin password dan informasi sebagainya) harus dapat diproteksi dalam penggunaan dan penyebarannya. Adapun bentuk serangan dalam bentuk usaha penyadapan (dengan program Sniffer), sedangkan usaha-usaha yang dapat dilakukan untuk meningkatkan *privacy* dan *confidentiality* adalah dengan menggunakan teknologi kriptografi.

b. Integrity

Informasi tidak boleh diubah tanpa seijin pemilik informasi. Contohnya : E-mail di *Intercept* ditengah jalan, diubah isinya, kemudian diteruskan kealamat yang dituju. Adapun bentuk serangan yang dilakukan adanya virus, trojan horse atau pemakai lain yang mengubah informasi tanpa ijin, "Man in the middle attack" dimana seseorang menempatkan diri ditengah pembicaraan dan menyamar sebagai orang lain.

c. Authentication

Metode untuk menyatakan bahwa informasi betul betul asli atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud. Dapat menggunakan dukungan tools yang membuktikan keaslian dokumen, dapat dilakukan dengan teknologi watermaking (untuk menjaga "*Intellectual Property*" yaitu dengan menandai dokumen atau hasil karya dengan "tanda tangan" pembuat) dan *digital signature*. Acces Control, yaitu berkaitan dengan pembatasan orang dapat mengakses informasi. *User* harus menggunakan password, biometric (ciri-ciri khas orang) dna sejenisnya.

d. Avaibility

Ketersediaan informasi ketika dibutuhkan. Adapun ancaman yang dapat terjadi meliputi : Denial Of Service Attack (DoS Attack) dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai down, hang, crash.

2.6 Tools pendeteksi vulnerability secara online

Teknologi internet menawarkan banyak sekali tools yang disediakan berbasis website (*online scanner*) dengan kemampuan kapasitas dan kecepatan server yang sangat canggih dan mumpuni dalam proses mendeteksi *vulnerability* jaringan komputer serta memberikan informasi detil terhadap sumberdatya hardware ataupun software, antara lain:

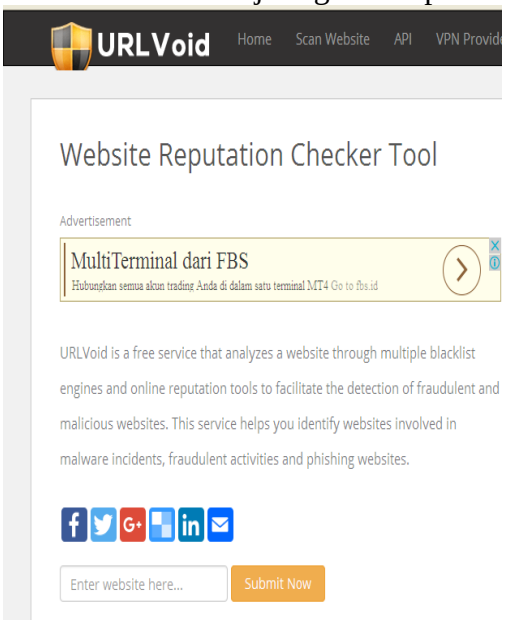
a. Virus Total

Virus total yang beralamat : https://www.virustotal.com mampu menscan utilitas yang ada pada sebuah server

Gambar 5. Virustotal

b. Urlvoid

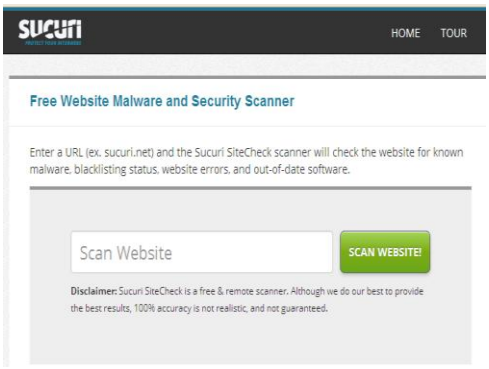
Urlvoid adalah online scanner server yang mempunyai alamat URl browser pada http://www.urlvoid.com mampu melakukan scanning pada software keamanan jaringan komputer



Gambar 6. Urlvoid

c. Sucuri

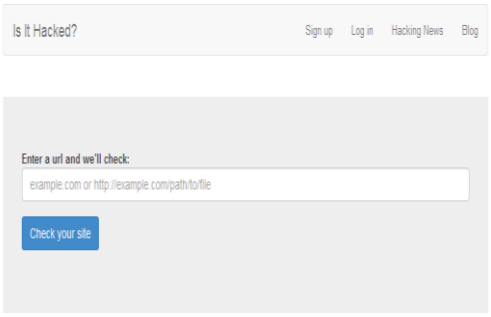
Alamat lengkap online scanner ini adalah https://sitecheck.sucuri.net/ adalah server penyedia jasa scanner online gratis yang bisa digunakan oleh umum untuk melakukan testing terhadap kerentanan keamanan jaringan komputer yang dibangun serta memberikan informasi yang akurat mengenai hal-hal yang berhubungan dengan jaringan tersebut baik secara hardware, software dan piranti keamanan yang digunakan.



Gambar 7. sucuri

d. Isithacked

Merupakan online scanner server yang mempunyai alamat URL lengkap *http://www.isithacked.com/*.

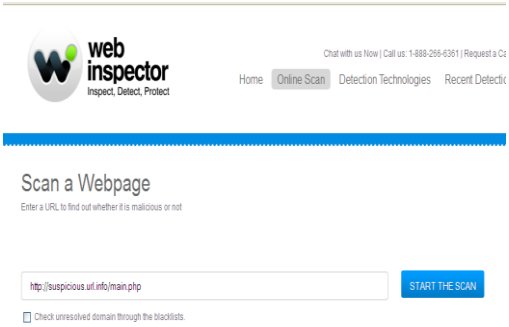


Gambar 8. itshacked

scanner ini mempunyai banayak feature pendeteksian vulnarebility meliputi checking for cloaking, status codes, spammy looking links, iframes dan blacklistchecks

e. Webinspector

Merupakan sebuah aplikasi scanner secara online, yang bisa diakses melalui url : https://app.webinspector.com/ yang mempunyai banyak feature yang berkaitan dengan malicious activity dan malware. informasi yang disajikan sangat lengkap dan scanner vulnerability ini juga merupakan layanan yang disediakan oleh pengembang secara gratis. User akan menerima informasi lebih lengkap lagi saat user melakukan proses login yang disediakan oleh webinspecor ini.



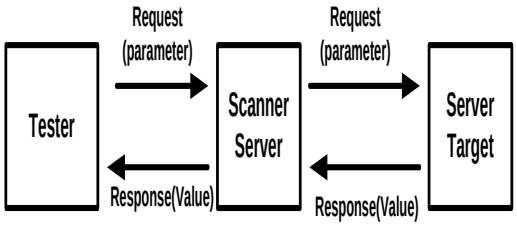
Gambar 9.webinspector

III. METODOLOGI PENELITIAN

3.1. Desain scanning vulnerability process

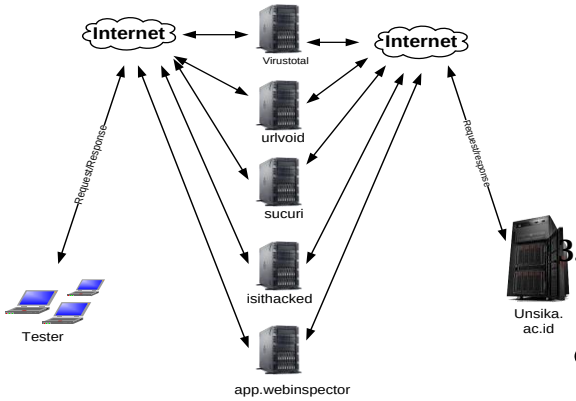
Skema yang dirancang menggunakan komunikasi *Client server* bertingkat, yang dalam hal ini untuk mencapai target melalui perantara, Tester akan mengirimkan *request* yang membawa parameter pada server perantara, kemudian server perantara meneruskan dari permintaan tester ke server target dengan membawa paramater yang ada dan secara otomatis server akan

mengolah parameter tersebut dan hasilnya server target akan meresponse dengan meberikan data dan informasi dari permintaan server perantara, kemudian server perantara meneruskan ke komputer Tester dengan memberikan informasi yang lengkap sesuai dengan parameter permintaan.



Gambar 10. skema proses scanning website

permintaan user akan diresponse dengan meberikan informasi dan data berupa value sesuai dengan parameter permintaan dari pengguna layanan vulnerability online scanner.

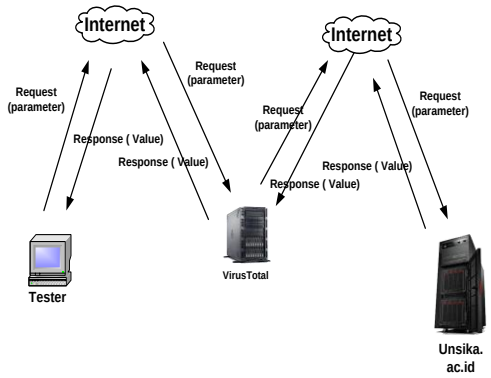


Gambar 11. skema proses scanning website

proses scanning pencarian kerentanan keamanan (vulnarebility) website target dalam hal ini http://www.unsika.ac.id/ dilakukan dengan menggunakan scanner server security online:

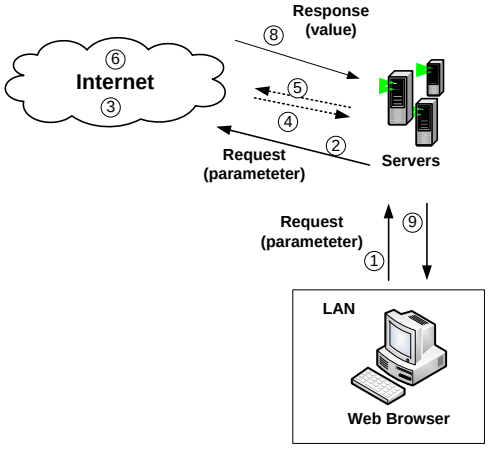
1. https://www.virustotal.com
2. http://www.urlvoid.com/
3. https://sitecheck.sucuri.net/
4. http://www.isithacked.com/
5. https://app.webinspector.com/

Proses yang dilakukan oleh tester dalam mengakses server target (unsika.ac.id) melalui server scanner virustotal dengan mencantumkan parameter. parameter tersebut nantinya akan diteruskan pada server tujuan dan saat server tujuan menerima parameter kemudian mengolahnya dan hasilnya akan dikembalikan(response) pada scanner server dengan membawa value yang seterusnya akan dikirim ke tester mengenai informasi hasil pengolahan parameter yang dikirim



Gambar 12. Scanning dengan website Virus Total

3.2 Scanning melalui jalur internal

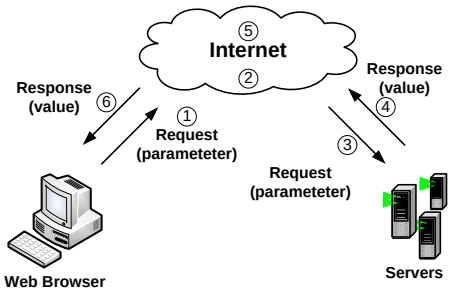


Gambar 13. skema proses scanning jalur internal

proses scanning dengan memanfaatkan jaringan LAN area internal yang langsung berkomunikasi dengan server, dari komputer web browser internal mengakses Server scanner di luar kampus kemudian mengecek server target dan hasilnya diumpan kembali ke server eksternal kemudian dikirim kembali dari server scanner ke komputer web browser Client melalui server yang ditest

3.3 Scanning Melalui Jalur External

Berbeda dengan penggunaan jalur komunikasi jaringan internal, state pada scanning melaui jalur external secara perhitungan proses lebih pendek.



Gambar 14. Skema Proses Scanning Jalur External

Proses yang dilakukan langsung dari komputer web browser yang berada di luar jaringan server Target, Komputer browser mengirim request disertai parameter testing ke server target melalui Scanner server dan hasilnya akan diumpan kembali sebagai response dengan membawa value yang diminta oleh browser tester.

IV. HASIL DAN PEMBAHASAN

Dari ujicoba proses scanning server unsika terdapat beberapa output, scanning dilakukan dengan menggunakan beberapa server menunjukkan hasil yang berbeda

4.1 Hasil Proses Scanning

a. Hasil Scanning virustotal.com

Tabel 1. hasil list virus total

No	URL Scanner	Result
1	ADMINUSLabs	Clean site
2	AegisLab WebGuard	Clean site
3	AlienVault	Clean site
4	Antiy-AVL	Clean site
5	Avira (no cloud)	Clean site
6	Baidu-International	Clean site
7	BitDefender	Clean site
8	Blueliv	Clean site
9	C-SIRT	Clean site
10	Certly	Clean site
11	CLEAN MX	Clean site
12	Comodo Site Inspector	Clean site
13	CyberCrime	Clean site
14	desenmascara.me	Clean site
15	Dr.Web	Clean site
16	Emsisoft	Clean site
17	ESET	Clean site
18	Fortinet	Clean site
19	FraudScore	Clean site
20	FraudSense	Clean site
21	G-Data	Clean site
22	Google Safebrowsing	Clean site
23	K7AntiVirus	Clean site
24	Kaspersky	Clean site
25	Malc0de Database	Clean site
26	Malekal	Clean site
27	Malware Domain Blocklist	Clean site
28	Malwarebytes hpHosts	Clean site
29	Malwared	Clean site
30	MalwareDomainList	Clean site
31	MalwarePatrol	Clean site
32	malwares.com URL checker	Clean site
33	Nucleon	Clean site
34	OpenPhish	Clean site
35	Opera	Clean site
36	ParetoLogic	Clean site
37	Phishtank	Clean site
38	Quttera	Clean site

39	Rising	Clean site
40	SCUMWARE.org	Clean site
41	SecureBrain	Clean site
42	securolytics	Clean site
43	Spam404	Clean site
44	Sucuri SiteCheck	Clean site
45	Tencent	Clean site
46	ThreatHive	Clean site
47	Trustwave	Clean site
48	VX Vault	Clean site
49	Web Security Guard	Clean site
50	Websense ThreatSeeker	Clean site
51	Webutation	Clean site
52	Yandex Safebrowsing	Clean site
53	ZCloudsec	Clean site
54	ZDB Zeus	Clean site
55	ZeroCERT	Clean site
56	Zerofox	Clean site
57	ZeusTracker	Clean site
58	zvelo	Clean site
59	AutoShun	Unrated site
60	Netcraft	Unrated site
61	PhishLabs	Unrated site
62	Sophos	Unrated site
63	StopBadware	Unrated site
64	URLQuery	Unrated site

b. Hasil urlvoid.com server

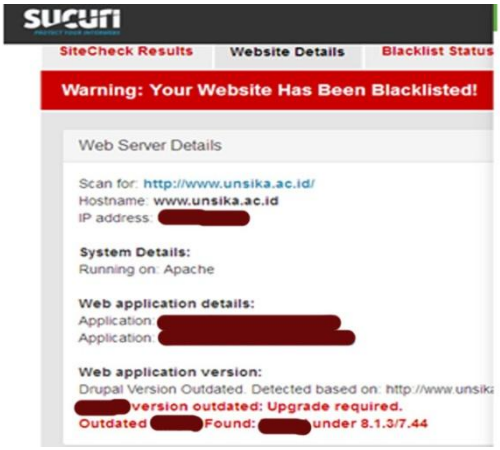
Hasil output proses scanning dengan urlvoid adalah sebagai berikut"

Tabel 2. hasil output scanning urlvoid

AVGThreatLabs	clean
Avira	clean
Bambenek Consulting	clean
BitDefender	clean
CyberCrime	clean
c_APT_ure	clean
Disconnect.me (Malw)	clean
DNS-BH	clean
DrWeb	clean
DShield	clean
Fortinet	clean
GoogleSafeBrowsing	clean
hpHosts	clean
Malc0de	clean
MalwareDomainList	clean
MalwarePatrol	clean
MyWOT	clean
OpenPhish	clean
PhishTank	clean
Quttera	clean
Ransomware Tracker	clean
SCUMWARE	clean
Spam404	clean
SURBL	clean
ThreatCrowd	clean
ThreatLog	clean
urlQuery	clean
URLVir	clean
VXVault	clean
WebSecurityGuard	clean
YandexSafeBrowsing	clean
ZeroCERT	clean
ZeuS Tracker	clean

c. Hasil sucuri.net server

Hasil Scanning dengan menggunakan vulnerability Scanner server sucri.net memberikan informasi yang detil dan jelas.



Gambar 15 hasil output sucuri

Tabel 3 informasi status website target

Website:	www.unsika.ac.id/
Status:	Site Potentially Harmful. Immediate Action is Required.
Web Trust:	Blacklisted (10 Blacklists Checked): Indicates that a major security company (such as Google, McAfee, Norton, etc) is blocking access to your website for security reasons. Please see our recommendation below to fix this issue and restore your traffic.

Tabel 4 vunarebilty information

Scan	Result	Severity	Recommendation
Website Blacklisting	**Detected**	**Critical**	Clean Up Clean Up & Remove Blacklisting
Site Likely Compromised	**Detected**	**Critical**	Clean Up Clean Up & Remove Blacklisting
Website Firewall	**Not Found**	**Medium Risk**	With Sucuri Firewall
Outdated Software	**Detected**	**Medium Risk**	With Sucuri Firewall

Tabel 5 Domain Black list

Domain blacklisted by SpamHaus DBL: unsika.ac.id
Domain clean by Google Safe Browsing: unsika.ac.id
Domain clean by Norton Safe Web: unsika.ac.id
Domain clean on Phish tank: unsika.ac.id
Domain clean on the Opera browser: unsika.ac.id
Domain clean by SiteAdvisor: unsika.ac.id
Domain clean by the Sucuri Malware Labs blacklist: unsika.ac.id
Domain clean on Yandex (via Sophos): unsika.ac.id
Domain clean by ESET: unsika.ac.id

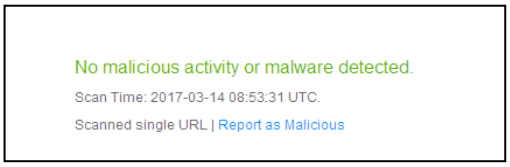
d. Hasil isithacked.com

Tabel 6 vunarebilty

no	Result
1	**Checking for cloaking** Looks cool.
2	**Status codes** These should normally all be the same. • GoogleBot returned code 200 • Google Chrome returned code 200

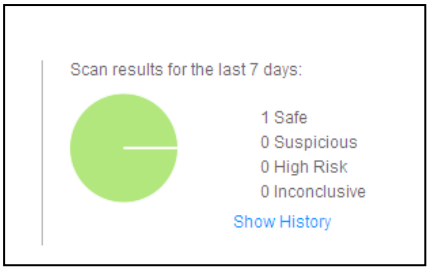
3	**Spammy looking links** Any links with funky anchor text? Nothing scary here!
4	**iframes** Any iframes? Nope!
5	**Blacklist Checks** Google Safe Browse reports not in malware database Phishtank reports URL not found

e.app.webinspector.com



\

mbar 16 hasil output webinspector



Gambar17 status prioritas

4.2 Pembahasan Uji Coba

Pada setiap proses server scanner memberikan hasil yang berbeda sesuai fitur yang disediakan

a. Vrus total memberikan informasi tentang virus dan malware yang detil dan disajikan dalam bentuk tabel lengkap dengan path dan result masing masing item
b. UrlVoid memberikan informasi yang berkaitan mirip dengan virus total, termasuk informasi link detil setiap item yang discan
c. sucuri.net: informasi yang diberikan paling lengkap diantara online scanner lainnya, meski gratis, layanan ini sangat baik dijadikan referensi dalam keamanan sistem jaringan komputer, sucuri juga memberikan informasi kerentanan dan informasi penanggulanan terhadap celah kemanan.
d. itshacked memberikan informasi tentang kegiatan yang berhubungan dengan proses hacking dan activitas pebetrasi lainnya
e. webinspector: meberikan informasi tentang malicious software atau malware dan informasi status prioritas kerentanan terhadap sistem keamanan jaringan komputer.

V. PENUTUP

Simpulan

Melakukan proses scanning dalam mendeteksi kerentanan keamanan sebuah sistem jaringan komputer banyak dilakukan, dari pembahasan diatas dapat disimpulkan:

- Online vulnerability scanner merupakan salah satu cara penggunaan tools yang menediakan layanan gratis yang memiliki fitur lengkap dan mudah dalam penggunaannya.
- proses scanning dapat dilakukan melalui jalur internal (LAN) dan jalur eksternal (web servise)
- diantara server scanner yang digunakan, sucuri.net memberi informasi yang lengkap termasuk sumberdaya hardware, software dan tools keamanan yang digunakan
- setiap penyedia scanning vulnerability secara online meberikan informasi yang berbeda sesuai dengan layanan

yang disediakan oleh penyedia tersebut

Saran

Dalam menanggapi isu keamanan sistem jaringan komputer, setiap kegiatan harus sering dilakukan:

- lakukan backup data berkala
- lakukan scanning terhadap vulnerability melalui online atau off line dan segera menambal path yang menjadi celah keamanan
- gunakan scanner online yang gartis dan yang versi berbayar setiap saat untuk mencegah dn menanggulangi kegiatan ilegal yang mengancam pada keberlangsungan proses server dalam penyediaan layanan
- update setiap software atau aplikasi yang digunakan pada server
- meski setiap Online vulnerability scanner meberikan informasi yang berbeda, penggunaan lebih banyak online scanner akan meberikan kelengkapan informasi dalam kegiatan menjaga dan memelihara keamanan sistem jaringan komputer.

UCAPAN TERIMA KASIH

Ucapan terima kasih disampaikan kepada seluruh civitas akademika Universitas Singaperbangsa Karawang

DAFTAR PUSTAKA

[1] Alfred Basta, W. H. (2008). *Computer Security and Penetration Testing*

[2] Amarudin, Widyawan, & Najib, W. (2014, Februari 8). *Analisis Keamanan Jaringan Single Sign On (SSO) Dengan Lightweight Directory Access Protocol (LDAP) Menggunakan Metode MITMA*. Seminar Nasional Teknologi Informasi dan Multimedia

[3] Ariyus,Doni M.Kom, (2007)*Sistem Penyusupan pada Jaringan Komputer*. Yogjakarta: Andi

[4] Bacudio, A. G. (2011). An Overview of Penetration Testing. *Journal of Network Security & Its Applications*.

[5] Digdo, G. P.(2012) *Analisis Serangan dan Keamanan pada Aplikasi Web*. Jakarta: Elex ,edia Komputindo

[6] Kim, I. M. (2012). *Penetration Testing For Web Aplication*

[7] Kompan, M. (2012, May). *Enterprise Web Application Security.* Masaryk University

[8] Naik, N. (2009). *Penetration Testing A Roadmap to Network*

[9] Ralph La Barge, T. M. (2012). *Cloud Penetration Testing.*

[10] Tom Thomas, 2010, *Network Security First-step*, Yogyakarta, Andi Offset

[11] Wilhelm, T. (2010). *Professional Penetration Testing Creating and Operating a Formal Hacking Lab*

[12] W3C. 2004. *Web service Architecture* .Tersedia pada http://www.w3.org/TR/ws arch, W3C Working Group. (diakses pada tanggal 12 Februari 2017).