Kajian *Vulnerability* Keamanan Jaringan Internet Menggunakan Nessus

Didi Juardi*

Fakultas Ilmu Komputer, Universitas Singaperbangsa Karawang, Jl. H.S. Ronggowaluyo, Karawang *41361*
*E-mail: didi.juardi@staff.unsika.ac.id

Abstrak. Keamanan jaringan komputer merupakan salah satu hal penting dan mendasar dalam pemanfaatan sebuah sistem. vulnerability dalam sebuah sistem jaringan komputer seringkali dikesampingkan, hingga apabila terjadi suatu ancaman /serangan logic maupun physic yang merusak pada sistem tersebut. Salah satu bentuk yang ditempuh diantaranya adalah melakukan sebuah analisis secara periodik, baik itu logic dan physic, sehingga nantinya diharapkan dari analisis tersebut menghasilkan suatu laporan audit yang berisi deteksi dari berbagai macam vulnerability yang ada, untuk kemudian diambil langkah-langkah proteksi yang tepat, yang diperlukan sebagai jaminan keamanan untuk keberlangsungan sistem tersebut. Nessus bekerja dengan memeriksa target yang anda telah anda tentukan, seperti Sekumpulan host atau bisa juga host dalam fokus tersendiri. Begitu aktivitas scan selesai, anda dapat melihat informasi hasilnya baik dalam bentuk grafikal atau baris, Interface (tampilan) grafikal Nessus dibangun dengan menggunakan Gimp Toolkit (gtk). Gtk adalah sebuah library gratis yang banyak digunakan untuk membangun interface grafikal dibawah X.

Kata kunci: *Keamanan, Vulnerability, Nessus, Host*

1 Pendahuluan

Perkembangan Teknologi Informasi di era global seperti sekarang ini, keamanan jaringan internet harus sangat diperhatikan, karena jaringan komputer Internet yang sifatnya publik dan global pada dasarnya tidak aman. Pada saat data terkirim dari suatu terminal asal menuju ke terminal tujuan dalam Internet, data itu akan melewati sejumlah terminal yang lain yang berarti akan memberi kesempatan pada user Internet yang lain untuk menyadap atau mengubah data tersebut.

Belakangan ini, pencurian identitas pribadi melalui media internet semakin marak. Utamanya, yang menjadi incaran adalah akun perbankan beserta *password* akun bank dan informasi-informasi penting lainnya. Berbagai cara bisa digunakan misalnya melalui *phishing*, *email scan* ataupun menggunakan piranti yang sanggup melacak gerak-gerik kebiasaan *user* ketika mengakses situs-situs web di internet. Kebocoran informasi ini tidak hanya terjadi secara personal tapi

Diterima 1 Mei 2017, Direvisi 19 September 2017, Diterima untuk publikasi 28 November 2017

juga dapat terjadi secara korporat. Yang mana tidak tertutup kemungkinan kebocoran itu datang dari orang dalam sendiri.

Sistem keamanan jaringan komputer yang terhubung ke Internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif, dan bagaimana untuk mengetahui *vulnerability* dari suatu jaringan, sehingga dengan mengetahui kelemahan yang terdapat pada jaringan maka lagkah-langkah untuk mengatasi kelemahan ini dapat dilakukan.

2 Landasan Teori

2.1 TCP/IP (Transmission Control Protokol/Internet Protocol)

Protokol adalah spesifikasi formal yang mendefinisikan prosedur-prosedur yang harus diikuti ketika mengirim dan menerima data (Werner, 1996). Protokol mendefinisikan jenis, waktu, urutan dan pengecekan kesalahan yang digunakan dalam jaringan. Transmission Control Protocol/Internet Protocol (TCP/IP) merupakan protokol untuk mengirim data antar komputer pada jaringan. Protokol ini merupakan protokol yang digunakan untuk akses Internet dan digunakan untuk komunikasi global. TCP/IP terdiri atas dua protokol yang terpisah. TCP/IP menggunakan pendekatan lapisan (layer) pada saat membangun protokol ini. Dengan adanya pendekatan berlapis ini memungkinkan dibangunnya beberapa layanan kecil untuk tugas-tugas khusus. TCP/IP terdiri dari lima layer, yaitu:

a. Layer Application, di dalam layer ini aplikasi seperti FTP, Telnet, SMTP, dan NFS dilaksanakan.
b. Layer Transport, di dalam layer ini TCP dan UDP menambahkan data transport ke paket dan melewatkannya ke layer Internet.
c. Layer Internet, layer ini mengambil paket dari layer transport dan menambahkan informasi alamat sebelum mengirimkannya ke layer network interface.
d. Layer Network Interface, di dalam layer ini data dikirim ke layer physical melalui device jaringan.
e. Layer Physical, layer ini merupakan sistem kabel yang digunakan untuk proses mengirim dan menerima data.

2.2 Pengertian Dasar Vulnerability

Sebuah vulnerability adalah suatu poin kelemahan dimana suatu sistem rentan terhadap serangan. Sebuah ancaman (*threats*) adalah suatu hal yang berbahaya bagi keberlangsungan system (Lehtinen,Russel & Gangemi Sr, 2006:12). Ada tiga kata kunci yang timbul dan saling berkaitan apabila kita mendiskusikan

mengenai isu-isu daripada kemanan komputer, yaitu: vulnerabilitas, ancaman (*threats*), dan tindakan pencegahan (*countermeasures*). Bahaya tersebut dapat berupa manusia (*a system cracker or a spy*), suatu peralatan yang rusak, atau sebuah kejadian seperti kebakaran dan banjir, yang mungkin dapat menge ksploitasi kerentanan suatu sistem.

Semakin banyak vulnerabilitas dan ancaman yang dapat terjadi di dalam suatu sistem, sudah seharusnya semakin tinggi pula kesadaran kita untuk dapat memproteksi sistem dan informasi yang berada di dalamnya. Sebuah teknik untuk melindungi suatu sistem dinamakan dengan tindakan pencegahan (*countermeasures*) (Lehtinen,Russel & Gangemi Sr, 2006:12).

2.3 Pengertian Dasar Vulnerability

Pada era global ini, keamanan sistem informasi berbasis Internet harus sangat diperhatikan, karena jaringan komputer Internet yang sifatnya publik dan global pada dasarnya tidak aman. Pada saat data terkirim dari suatu terminal asal menuju ke terminal tujuan dalam Internet, data itu akan melewati sejumlah terminal yang lain yang berarti akan memberi kesempatan pada user Internet yang lain untuk menyadap atau mengubah data tersebut.

Sistem keamanan jaringan komputer yang terhubung ke Internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif. Apabila ingin mengamankan suatu jaringan maka harus ditentukan terlebih dahulu tingkat ancaman (*threat*) yang harus diatasi, dan resiko yang harus diambil maupun yang harus dihindari. Berikut ini akan dibahas mengenai ancaman (*threat*), kelemahan, dan *Policy* keamanan (*security policy*) jaringan.

2.4 Insiden Keamanan Jaringan

Insiden keamanan jaringan adalah suatu aktivitas terhadap suatu jaringan komputer yang memberikan dampak terhadap keamanan sistem yang secara langsung atau tidak bertentangan dengan security policy sistem tersebut.Secara garis besar, insiden dapat diklasifikasikan menjadi: *probe, scan, account compromize, root compromize, packet sniffer, denial of service, exploitation of trust, malicious code,* dan *infrastructure attacks.* Berikut ini akan dibahas mengenai jenis- jenis insiden tersebut.

2.5 Nessus

Nessus adalah sebuah program yang berfungsi sebagai *security scanner* yang akan mengaudit jaringan yang dituju lalu menentukan kelemahan-kelemahan dari jaringan yang dituju. Berikut ini adalah fitur-fitur yang dimiliki oleh Nessus:

- *Plug-in architecture*
  Setiap *security test* ditulis sebagai *external plugin*. Dengan fitur seperti ini, kita dapat dengan mudah menambah tes yang kita inginkan tanpa harus membaca kode dari *nessusd engine.*

- *NASL (Nessus Attack Scrpiting Language)*
  NASL adalah sebuah bahasa yang didesain untuk menulis program *security test* dengan mudah dan cepat. Selain dengan NASL, bahasa C juga dapat digunakan untuk menulils program *security test*.

- *Up-to-date security vulnerability database*.
- *Client-sever architecture*
  Nessus *security scanner* terdiri dari dua bagian yaitu: sebuah server yang berfungsi sebagai pelaku serangan, dan sebuah client yang berfungsi sebagai *frontend*. Client dan server dapat berjalan pada sistem yang berbeda. Arti dari fitur ini adalah bahwa keseluruhan jaringan dapat diaudit melalui sebuah PC, dengan server yang melakukan serangan ke jaringan yang dituju. Dapat mengetes jumlah host yang banyak dalam waktu yang sama.

- *Smart service recognation*.
  Nessus tidak mempercayai host yang dituju menggunakan port standar yang ditentukan oleh IANA. Ini berarti Nessus dapat mengenali sebuah *Web server* yang berjalan pada port yang bukan merupakan port standar (contohnya pada port 8080), atau sebuah FTP server yang berjalan pada port 31337.

- *Multiple Services*
  Apabila ada dua buah *Web server* pada host yang dituju maka Nessus akan mengetes kedua *Web server* tersebut.

- *Complete reports.*
  Nessus tidak hanya memberi tahu kelemahan dari jaringan yang dituju tetapi juga memberikan cara yang dapat digunakan untuk mencegah *the bad guy* utnuk mengeksploitasi kelemahan dari jaringan dan juga memberikan level resiko dari setiap masalah yang ditemukan.

- *Exportable reports.*
  Unix client dapat mengekspor laporan sebagai Ascii text, HTML, LaTeX, dll.

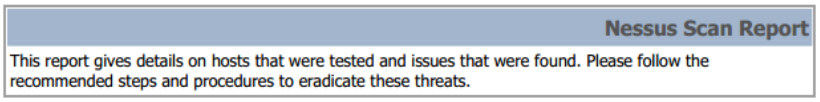
3 Hasil dan Pembahasan

3.1 Scanning Jaringan Menggunakan Nessus

Nessus adalah alat pemindaian keamanan jarak jauh, yang memindai komputer dan menimbulkan peringatan jika menemukan kerentanan yang dapat digunakan hacker berbahaya untuk mendapatkan akses ke komputer mana pun yang telah Anda kaitkan ke jaringan. Hal ini dilakukan dengan menjalankan lebih dari 1200 cek pada komputer tertentu, menguji untuk mengetahui apakah ada serangan ini yang dapat digunakan untuk masuk ke komputer atau membahayakannya. Scanning dilakukan untuk mengetahui suatu host dalam jaringan komputer terdapat vulnerability atau tidak tergantung dari keamanan dari masing-masing host. Berikut ini merupakan scanning pada host yang tidak terdapat vulneberality dan host yang terdapat vulnerability.

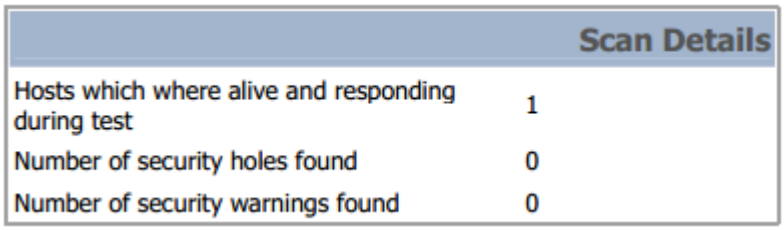
3.1.1 Host Tanpa Vulnerability

Hasil sanning jaringan komputer internet menggunakan Nessus yang tidak terdapat vulnerability pada host 152.102.20.5 sebagai berikut



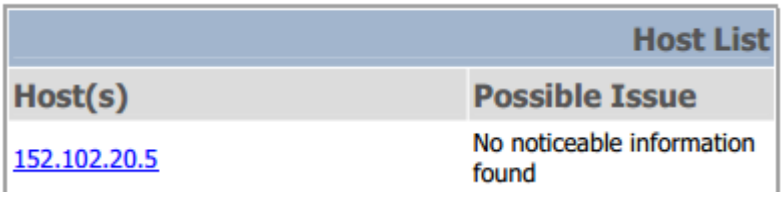
Nessus Scan Report

This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.



Scan Details

Hosts which where alive and responding during test	1
Number of security holes found	0
Number of security warnings found	0



Host List

Host(s)	Possible Issue
152.102.20.5	No noticeable information found

Analysis of Host		
Address of Host	**Port/Service**	**Issue regarding Port**
152.102.20.5	telnet (23/tcp)	No Information
152.102.20.5	h323hostcall (1720/tcp)	No Information

Security Issues and Fixes: 152.102.20.5		
Type	**Port**	**Issue and Fix**

Pada host tersebut pada gambar diatas menunjukkan bahwa host 152.102.20.5 tidak terdapat vulnerability berdasarkan *report scanning* tersebut.

Security Issues and Fixes: 152.102.20.184		
Type	**Port**	**Issue and Fix**
Vulnerability	http (80/tcp)	The remote host has FrontPage Server Extensions (FPSE) installed. There is a denial of service / buffer overflow condition in the program 'shtml.exe' which comes with it. However, no public detail has been given regarding this issue yet, so it's not possible to remotely determine if you are vulnerable to this flaw or not. If you are, an attacker may use it to crash your web server (FPSE 2000) or execute arbitrary code (FPSE 2002). Please see the Microsoft Security Bulletin MS02-053 to determine if you are vulnerable or not. *** Nessus did not actually check for this flaw, so this *** might be a false positive Solution : See http://www.microsoft.com/technet/security/bulletin/ms02-053.asp Risk factor : High CVE : CAN-2002-0692 BID : 5804 Nessus ID : 11311
Vulnerability	http (80/tcp)	The remote frontpage server may leak information on the anonymous user By knowing the name of the anonymous user, more sophisticated attacks may be launched Check the following data for any potential leaks:

method=open service:3.0.2.1105
<p>status=

status=917505
osstatus=0
msg=The user 'IUSR_TP1' is not authorized to execute the 'open service' method.
osmsg=

</body>
</html>
1

CVE : CAN-2000-0114
Nessus ID : 10077

Vulnerability http (80/tcp)

The IIS server appears to have the .HTR ISAPI filter mapped.

At least one remote vulnerability has been discovered for the .HTR filter. This is detailed in Microsoft Advisory MS02-018, and gives remote SYSTEM level access to the web server.

It is recommended that even if you have patched this vulnerability that you unmap the .HTR extension, and any other unused ISAPI extensions if they are not required for the operation of your site.

Solution :
To unmap the .HTR extension:
1.Open Internet Services Manager.
2.Right-click the Web server choose Properties from the context menu.
3.Master Properties
4.Select WWW Service -> Edit -> HomeDirectory -> Configuration and remove the reference to .htr from the list.

Risk factor : High
CVE : CVE-2002-0071
BID : 4474
Nessus ID : 10932

Vulnerability http (80/tcp)

The remote WebDAV server may be vulnerable to a buffer overflow when it receives a too long request.

An attacker may use this flaw to execute arbitrary code within the LocalSystem security context.

*** As safe checks are enabled, Nessus did not actually test for this
*** flaw, so this might be a false positive

Solution : See http://www.microsoft.com/technet/security/bulletin/ms03-007.asp
Risk Factor : High
CVE : CAN-2004-0109
BID : 7116
Nessus ID : 11412

Vulnerability http (80/tcp)

The IIS server appears to have the .SHTML ISAPI filter mapped.

At least one remote vulnerability has been discovered for the .SHTML filter. This is detailed in Microsoft Advisory MS02-018 and results in a denial of service access to the web server.

It is recommended that even if you have patched this vulnerability that
you unmap the .SHTML extension, and any other unused ISAPI extensions
if they are not required for the operation of your site.

An attacker may use this flaw to prevent the remote service
from working properly.

*** Nessus reports this vulnerability using only
*** information that was gatherered. Use caution
*** when testing without safe checks enabled

Solution: See
http://www.microsoft.com/technet/security/bulletin/ms02-018.asp
and/or unmap the shtml/shtm isapi filters.

To unmap the .shtml extension:
1.Open Internet Services Manager.
2.Right-click the Web server choose Properties from the context menu.
3.Master Properties
4.Select WWW Service -> Edit -> HomeDirectory -> Configuration
and remove the reference to .shtml/shtm and sht from the list.

Risk factor : Medium
CVE : CAN-1999-1376, CVE-2000-0226, CVE-2002-0072
BID : 4479
Nessus ID : 10937

Hasil scanning tersebut menjelaskan adanya vulnerability pada host 152.102.20.184 :

- Host dengan IP152.102.20.184 memiliki *Front Page Server Extension (FPS)* yang terinstal di dalamnya, yang dapat menyebabkan *denial of service (DOS)/buffer overflow* di dalam program shtml.exe
- *Frontpage server* pada host dengan IP 152.102.20.184 sangat mungkin untuk membocorkan informasi pada *anonymous user*, yang dapat menyebabkan serangan yang membahayakan host.
- *IIS server* pada host dengan IP 152.102.20.184 mempunyai HTR ISAPI *filter mapped*. Sedikitnya ada sebuah *vulnerability* yang disebabkan oleh HTR *filter*. Hal ini dapat diatasi dengan cara melakukan *unmap* pada *extension* pada .HTR.
  Server ini juga mungkin mempunyai .SHTML ISAPI *filter mapped*. Sama seperti HTR, sedikitnya ada sebuah *vulnerability* yang disebabkan oleh SHTML *filter*.
- WebDAV *server* mungkin mempunyai *vulnerability* ketika menerima *request* yang terlalu panjang.

4 Kesimpulan

- Jaringan komputer internet yang sifatnya publik dan global pada dasarnya kurang aman dan untuk meningkatkan keamanan jaringan

internet dapat menggunakan beberapa metode,contohnya metode authentikasi, penggunaan metode enkripsi-dekripsi, dan menggunakan Firewall.

- Kelemahan suatu sistem jaringan dapat dilihat dengan menggunakan tool-tool seperti scanner, TCP/IP assembler, Network Protocol Analyzer, dan lain-lain.
- Nessus adalah sebuah program yang berfungsi sebagai security scanner yang akan mengaudit jaringan yang dituju lalu menentukan kelemahan-kelemahan dari jaringan yang dituju. Nessus juga dapat menghasilkan informasi berupa deskripsi target, kondisi target, serta solusi dari kelemahan/ permasalahan yang dialamai komputer target.

5 Referensi

[1] Anonim.: *Sistem Jaringan Komputer untuk Pemula,* Yogyakarta , Andi, Madcoms, 2010.

[2] Brenton, Hunt. :*Network Security*., Jakarta : PT Elex Media Komputindo, 2005**.**

[3] http://www.nessus.org diakses dari tanggal 9 Maret 2017 sampai dengan 30 April 2017

[4] Lehtinen, Russell, Gangemi.: *Computer Security Basics*. Inc. United Stated of America, O'Reilly Media, 2006.

[5] Mancill, T *: A Primer for Network Administrator*, 2nd ed., *Linux Routers* , Prentice Hall, 2002.

[6] Pereira, M., *Encyclopedia of Internet Technologies and Applications*, Information Science Publishing, 2007.

[7] Setiawan, Thomas. *Analisis Keamanan Jaringan Internet Menggunakan Hping, Nmap, Nessus, dan Ethereal*, Bandung, Departemen Teknik Elektro Fakultas Teknologi Industri Institut Teknologi Bandung, 2004.

[8] W. Purbo, Onno: TCP/IP, Jakarta : PT. Gramedia. 2002

[9] Wiharjito, Tony : Keamanan Jaringan Internet. Jakarta : PT. Gramedia, 2002.

[10] Wijaya, Hendra :Cisco Router. Jakarta : PT. Gramedia, 2002.