YAYASAN AKRAB PEKANBARU
Jurnal AKRAB JUARA
Volume 5 Nomor 3 Edisi Agustus 2020 (240-246)

19

VULNERABILITY ASSESSMENT PADA SITUS WWW.HATSEHAT.COM MENGGUNAKAN OPENVAS

Dewi Laksmiati
Universitas Bina Sarana Informatika
(Naskah diterima: 1 Juni 2020, disetujui: 28 Juli 2020)

Abstract

The evolving cyberspace not only creates positive things, but also negative. One of them is the Cyber Security problem which is currently a critical problem. An example of a cyber security problem is hacking by exploiting vulnerable systems. Vulnerability Assessment tools can help give user of these tools information about how to protect their infrastructure. Problems that arise, users have difficulties in identifying which tools are ideal for their assessment. This study aims to do functional test of Vulnerability Assessment tools OpenVAS. In this test we do vulnerability scan to www.hatsehat.com site. Our results show that there are vulnereabilities found that need to be remediated
Keywords: *Cyber Security, Vulnerability Assessment, Vulnerability Scan, OpenVAS*

Abstrak

Perkembangan dunia maya tidak hanya menghasilkan hal positif, namun juga negatif. Salah satunya adalah masalah Cyber Security yang saat ini menjadi salah satu masalah kritis. Contoh masalah cyber security adalah peretasan dengan cara mengeksploitasi sistem yang rentan. Tools/Alat Penilaian Kerentanan (*Vulnerability Assessment*) dapat membantu memberikan pengguna perangkat ini informasi tentang cara melindungi infrastruktur mereka. Masalah yang muncul, pengguna menghadapi kesulitan dalam mengidentifikasi alat mana yang ideal untuk penilaian mereka. Penelitian ini bertujuan untuk melakukan pengujian terhadap alat *Vulnerability Assessment*, OpenVAS. Dalam pengujian ini menerapkan pemindaian kerentanan (*vulnerability scanning*) pada server situs www.hatsehat.com. Hasil penelitian menunjukkan ada beberapa celah yang perlu diremediasi.
Kata Kunci: Keamanan Siber, Penilaian Kerentanan, Pemindaian Kerentanan, OpenVAS

I. PENDAHULUAN

Hampir semua perusahaan saat ini menjalankan operasionalnya dengan basis teknologi informasi. Sehingga kemanaan data menjadi sesuatu yang vital, dimana data rentan serangan dalam bentuk pembobolan, manipulasi, penghilangan para *hacker*. Sayangnya hal ini belum disadari

oleh sebagian besar orang, sehingga orang baru menyadari pentingnya keamanan data setelah terjadi serangan.

Penelitian dilakukan oleh "*Computer Security Institute*" menunjukkan 90% dari organisasi ikut serta dalam penelitian telah mengalami pelanggaran keamanan dalam 12 bulan terakhir saat riset dibuat. 8% dari organisasi ini menderita kerugian finansial yang besar setelah pelanggaran ini. Banyak dari organisasi ini yang tidak memiliki profesional keamanan bersertifikat, mereka juga tidak menyewa pihak luar untuk memeriksa keamanan jaringan mereka. Jaringan dan sistem mereka sangat rentan, hal ini bisa menjadi alasan utama keberhasilan serangan.

Hal ini tentunya harus ditindaklanjuti, langkah awal yang perlu dilakukan untuk meminimalisir potensi ancaman keamanan dan penyalahgunaan data tersebut, perlu dilakukan evaluasi secara proaktif terhadap keamanan server yang ada sehingga ancaman dapat dihilangkan dan celah diblokir sebelum kerusakan dapat dilakukan pada sistem.

Vulnerability Assessment mencakup proses analisa teknologi yang digunakan dalam organisasi, mencari kelemahan apa pun yang dapat dieksploitasi oleh penyerang, dan memberikan rekomendasi tentang bagaimana organisai dapat meningkatkan keamanan data anda.

Pada fase pertama, fokus ditempatkan pada sistem keamanan agar lebih memahami jenis perangkat lunak dan perangkat yang digunakan oleh bisnis serta penggunaannya setiap hari. Fase kedua melibatkan memeriksa sistem infrastruktur saat ini. Pada langkah ini, setiap kelemahan dalam sistem keamanan diidentifikasi dan diperbaiki. Pada fase terakhir *Vulnerability Assessment*, perbaikan diuji untuk memastikan bahwa semuanya ada di tempat yang tepat. Jika ada kebutuhan untuk perbaikan, proses dimulai kembali dari fase dua dan setelah penilaian selesai, pemilik sistem akan diberikan penjelasan terperinci tentang apa yang diubah dan mengapa itu diubah.

Dalam penulisan ini akan dibahas penggunaan tools *vulnerability assessment* sebagai bagian dari fase kedua.

II. KAJIAN TEORI

Vulnerability Assessment

Vulnerability Assessment adalah proses mendefinisikan, mengidentifikasi, mengklasifikasikan, dan memprioritaskan kerentanan dalam sistem komputer, aplikasi, dan infrastruktur jaringan dan memberikan organisasi melakukan penilaian dengan pengetahuan, kesadaran, dan latar belakang risiko yang

diperlukan untuk memahami ancaman terhadap lingkungannya dan bereaksi dengan tepat.

Proses *vulnerability assessment* yang dimaksudkan untuk mengidentifikasi ancaman dan risiko yang ditimbulkannya biasanya melibatkan penggunaan alat pengujian otomatis, seperti pemindai keamanan jaringan, yang hasilnya terdaftar dalam laporan *vulnerability assessment*.

Gambar 1 Alur *Vulnerability Asessment*

Jenis *Vulnerability Assessment*

Vulnerability assessment tergantung pada penemuan berbagai jenis kerentanan sistem atau jaringan, yang berarti proses penilaian mencakup penggunaan berbagai alat, pemindai, dan metodologi untuk mengidentifikasi kerentanan, ancaman, dan risiko. Beberapa jenis *Vulnerability Assessment* yaitu:

- Pemindaian berbasis jaringan
- Pemindaian berbasis host
- Pemindaian jaringan nirkabel
- Pemindaian aplikasi

Dibawah ini penjelasan untuk masing-masing

- **Pemindaian berbasis jaringan**

  Digunakan untuk mengidentifikasi kemungkinan serangan keamanan jaringan. Jenis pemindaian ini juga dapat mendeteksi sistem yang rentan pada jaringan kabel atau nirkabel.

- **Pemindaian berbasis host**

  Digunakan untuk menemukan dan mengidentifikasi kerentanan di *server, workstation* atau *host* jaringan lainnya. Jenis pemindaian ini biasanya memeriksa *port* dan layanan yang mungkin juga terlihat oleh pemindaian berbasis jaringan, tetapi ini menawarkan visibilitas yang lebih besar ke pengaturan konfigurasi dan menambal sejarah sistem yang dipindai.

- **Pemindaian jaringan nirkabel**

  Pemindaian jaringan Wi-Fi suatu organisasi biasanya fokus pada titik-titik serangan dalam infrastruktur jaringan nirkabel. Selain mengidentifikasi titik akses jahat, pemindaian jaringan nirkabel juga dapat memvalidasi bahwa jaringan perusahaan dikonfigurasikan dengan aman.

- **Pemindaian aplikas**

  Digunakan untuk menguji situs web untuk mendeteksi kerentanan perangkat lunak yang diketahui dan konfigurasi yang salah dalam aplikasi jaringan atau web.

- **Pemindaian basis dat**

Digunakan untuk mengidentifikasi titik-titik lemah dalam basis data untuk mencegah serangan jahat, seperti serangan injeksi SQL.

OpenVAS

Open Vulnerability Assessment System (OpenVAS) adalah v*ulnerability scanner* yang dikelola dan didistribusikan oleh *Greenbone Networks*. Ini dimaksudkan untuk menjadi pemindai kerentanan lengkap dengan berbagai tes bawaan dan antarmuka Web yang dirancang untuk membuat pengaturan dan menjalankan pemindaian kerentanan dengan cepat dan mudah sambil memberikan tingkat konfigurasi pengguna yang tinggi.

III. METODE PENELITIAN

3.1 Metode Observasi

Melakukan pengumpulan data-data dengan cara mengamati serta mencatat secara sistematis tentang perangkat dan aplikasi yang digunakan dalam konfigurasi dalam prak-tek langsung.

3.2 Metode Studi Pustaka

Yaitu menggunakan literatur baik dalam bentuk media online, artikel atau buku bacaan yang berkaitan dengan penyusunan artikel ini.

3.3 Metode Pengembangan Jaringan

1. Analisa Kebutuhan

Analisa akan dilakukan melalui beberapa tahapan, yaitu:

a. Observasi langsung
b. Memahami semua kondisi kebutuhan di lapangan terkait kebutuhan penilaian kerentanan (*vulnerability assessment*)
c. Analisia hasil observasi.

2. Desain

Perancangan dilakukan melalui beberapa tahapan, yaitu:

a. Pemilihan server web untuk pengujian.
b. Pemilihan alat untuk pemindaian kerentanan *(vulnerability scan*)

3. Testing

Melakukan pemindaian menggunakan tools penilaian kerentanan

4. Implementasi

Untuk menjalankan OpenVAS diperlukan langkah berikut.

a. Instalasi dan konfigurasi Linux

Instalasi Kali Linux dilakukan pada mesin virtual (VM) pada sistem lokal. Kali Linux dipilih karena merupakan salah satu distro Linux paling populer di dunia keamanan siber. *Server* diinstall dengan spesifikasi :

Processor : 4 core
RAM : 16 GB
Hard Disk : 100GB

b. Instalasi OpenVAS

Setelah Kali Linux diinstall, langkah selanjutnya adalah melakukan instalasi Open VAS yang tersedia pada repository Kali Linux. Setelah selesai menginstall, *service* OpenVAS harus diinisiasi secara manual dengan mengeksekusi perintah melalui terminal

IV. HASIL PENELITIAN

Pada bab ini akan dijelaskan mengenai hasil pengujian dan analisa hasil pemindaian kerentanan pada www.hatsehat.com

4.1. Ikhtisar Hasil Pemindaian

Pada sub bab ini akan dipaparkan mengenai hasil pengujian dan analisa hasil pemindaian kerentanan (*Vulnerability Scan*) secara umum.

Tabel 1 Tabel Ikhtisar Hasil Pemindaian

Host	High	Medium	Low	Log	False Positive
174.136.57.146 www.hatsehat.com	15	48	6	164	0
Total: 1	15	48	6	164	0

Tabel 2 Hasil Pemindaian Medium dan High

Service (Port)	Threat Level
53/tcp	High
6543/tcp	High
80/tcp	Medium
2082/tcp	Medium
53/tcp	Medium
2079/tcp	Medium
465/tcp	Medium
2095/tcp	Medium
2083/tcp	Medium
993/tcp	Medium
21/tcp	Medium
995/tcp	Medium
143/tcp	Medium
2096/tcp	Medium
2086/tcp	Medium
6543/tcp	Medium
443/tcp	Medium
110/tcp	Medium
2077/tcp	Medium
2087/tcp	Medium
587/tcp	Medium

Dari tabel di atas didapatkan hasil pemindaian berikut:

- 16 kerentanan pada level *High* (tersebar pada 3 port)
- 48 kerentanan pada level *Medium* (tersebar pada 19 port)

4.2. Kerentanan Level *High* dan Solusinya

Pada penulisan ini akan difokuskan pada temuan yang lebih kritis tingkatannya (Level *High*). Hasil temuannya seperti berikut:

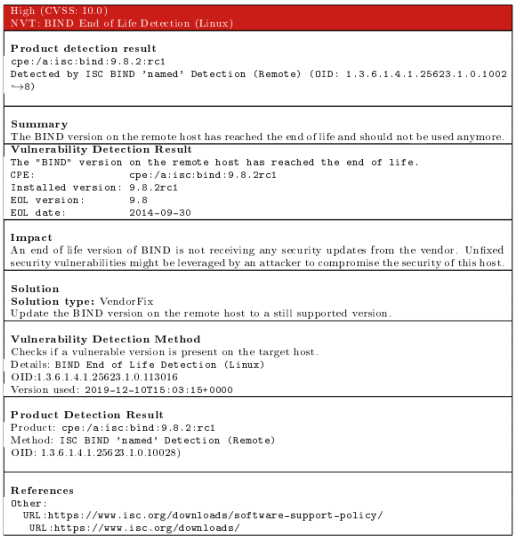
Tabel 3 Temuan Level *High*

Problem	Total Issues	Port
BIND outdated	9	53
OpenSSH	6	6543

Dari hasil temuan di atas didapatkan 15 kerentanan yang secara umum disebabkan dua hal yaitu tidak *update*-nya BIND dan Open

SSH pada server. Hal ini mengakibatkan server beresiko dapat ditembus oleh peretas. Sehingga berakibat kehilangan dan pencurian data.

Tabel 3 Contoh Kerentanan Pada BIND



High (CVSS: 10.0)
NVT: BIND End of Life Detection (Linux)

Product detection result
cpe:/a:isc:bind:9.8.2:rc1
Detected by ISC BIND 'named' Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.1002
↪8)

Summary
The BIND version on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result
The "BIND" version on the remote host has reached the end of life.
CPE: cpe:/a:isc:bind:9.8.2rc1
Installed version: 9.8.2rc1
EOL version: 9.8
EOL date: 2014-09-30

Impact
An end of life version of BIND is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

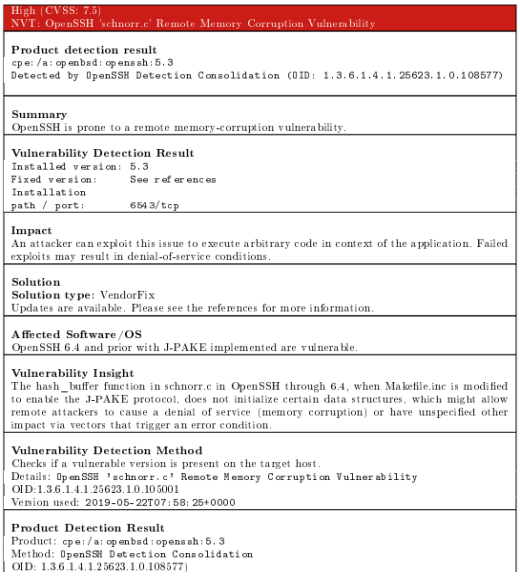
Solution
Solution type: VendorFix
Update the BIND version on the remote host to a still supported version.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: BIND End of Life Detection (Linux)
OID:1.3.6.1.4.1.25623.1.0.113016
Version used: 2019-12-10T15:03:15+0000

Product Detection Result
Product: cpe:/a:isc:bind:9.8.2:rc1
Method: ISC BIND 'named' Detection (Remote)
OID: 1.3.6.1.4.1.25623.1.0.10028)

References
Other:
URL:https://www.isc.org/downloads/software-support-policy/
URL:https://www.isc.org/downloads/

Tabel 4 Hasil Pengujian Kecepatan Akses Situs Setelah Diterapkan Cloudflare



High (CVSS: 7.5)
NVT: OpenSSH 'schnorr.c' Remote Memory Corruption Vulnerability

Product detection result
cpe:/a:openbsd:openssh:5.3
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)

Summary
OpenSSH is prone to a remote memory-corruption vulnerability.

Vulnerability Detection Result
Installed version: 5.3
Fixed version: See references
Installation
path / port: 6543/tcp

Impact
An attacker can exploit this issue to execute arbitrary code in context of the application. Failed exploits may result in denial-of-service conditions.

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

Affected Software/OS
OpenSSH 6.4 and prior with J-PAKE implemented are vulnerable.

Vulnerability Insight
The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: OpenSSH 'schnorr.c' Remote Memory Corruption Vulnerability
OID:1.3.6.1.4.1.25623.1.0.105001
Version used: 2019-05-22T07:58:25+0000

Product Detection Result
Product: cpe:/a:openbsd:openssh:5.3
Method: OpenSSH Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.108577)

Dalam laporan didapatkan juga solusi yang disarankan yaitu pembaruan BIND ke versi 9.11.0rc3 dan pembaruan Open SSH ke versi 7.3 ke atas. sehingga memperkecil resiko kehilangan atau perubahan data oleh peretas dikemudian hari.

V. KESIMPULAN

Dari perancangan dan implementasi serta pengujian OpenVAS diperoleh kesimpulan sebagai berikut:

1. Proses Vulnerability Assessment terhadap website www.hatsehat.com berjalan dengan baik dan menghasilkan temuan kelemahan atau kerentanan.
2. Temuan yang perlu segera ditindak lanjuti adalah temuan terkait dengan tidak updatenya BIND dan OpenSSH yang menyebabkan OpenVAS menemukan 15 issue (9 issue BIND, 6 issue OpenVAS.
3. BIND perlu diperbarui ke versi 9.11.0rc3 ke atas
4. OpenSSH perlu diperbarui ke versi 7.3 ke atas

DAFTAR PUSTAKA

Shakeel, Irfan. December 2015. “The Art of Network Vulnerability Assessment” Infosec Institute

Morris, Monica. January 2016 " Importance of Security Assessments" SDTek.net. https://www.sdtek.net/importance-security-assessments/ (diakses pada 21 Mei 2020 15:24 WIB)

Anonim. April 2018 "Vulnerability Assessment (Vulnerability Analysis)" Search SecurityTechTargethttps://searchsecurity.techtarget.com/definition/vulnerability-assessment-vulnerability-analysis (diakses pada 17 Mei 2020 14:33 WIB)

Anonim. December 2019 “Vulnerability Assessment"SilentBreachhttps://silentbreach.com/vulnerability-assessment.php (diakses pada 17 Mei 2020 14:33 WIB)

Anonim. October 2018 “A Brief Introduction to the OpenVAS Vulnerability Scanner" InfoSechttps://resources.infosecinstitute.com/a-brief-introduction-to-the-openvas-vulnerability-scanner/ (diakses pada 1 Juni 2020 19:29 WIB)

Scarfone, Karen; Murugiah Souppaya; Amanda Cody; Angela Orebaugh; September 2008 “Technical Guide to Information Security Testing and Assessment,” NIST Special Publication 800-115, National Institute of Standards and Technology,https://csrc.nist.gov/publications/detail/sp/800-115/final

Anonim. 2017 "Security Vulnerabiliy Assessment" ISACA

El Idrissi, S, N. Berbiche, F. Guerouate, and M. Sbihi. 2017 “Performance Evaluation of Web Application Security Scanners for Prevention and Protection against Vulnerabilities.” International Journal of Applied Engineering Research 12 (21): 11068-11076.