TUGAS KEAMANAN SISTEM INFORMASI

"VULNERABILITY SCANNING"

DOSEN PENGAMPU:

Gede Arna Jude Saskara, S.T.,M.T

Oleh:

I Gede Riyan Ardi Darmawan

(1815091037)

Sistem Informasi Kelas 4A

PROGRAM STUDI SISTEM INFORMASI

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNIK DAN KEJURUAN

UNIVERSITAS PENDIDIKAN GANESHA

TAHUN AKADEMIK 2019/2020

TUGAS 9 - KEAMANAN SISTEM INFORMASI

Mata Kuliah : Keamanan Sistem Informasi

Kode Mata Kuliah : SIF1433-AmanSI

SKS : 3 SKS

Dosen Pengempu : Gede Arna Jude Saskara, S.T.,M.T

Instruksi :

Carilah materi terkait Vulnerability Scan

Jawab :

Vulnerability Scanning

Definisi Vulnerability

Vulnerability atau celah keamanan adalah suatu cacat pada system/infrastruktur yang memungkinkan terjadinya akses tanpa izin dengan melakukan exploit terhadap kecacatan sistem tersebut. Cacat sistem ini dapat terjadi oleh karena kesalahan dalam merancang, membuat, atau mengimplementasikan sistem. Vulnerability atau celah keamanan digunakan oleh hacker sebagai dasar dalam pembuatan exploit sebagai jalan untuk masuk kedalam sistem secara ilegal. Hacker biasanya akan membuat exploit sesuai dengan vulnerability yang ditemukan.

Setiap sistem pasti memiliki celah keamanan atau vulnerability (No System Is Safe), namun yang menyebabkan sistem tersebut belum teretas adalah celah keamanan tersebut belum ditemukan, lambat laun vulnerability dari sistem tersebut pasti akan ditemukan oleh hacker. Tidak semua hacker menggunakan vulnerability ini untuk tindakan kejahatan dan memperkaya diri sendiri, jika celah ini ditemukan oleh kelompok hacker Black Hat maka kemungkinan celah tersebut akan digunakan untuk mengexploit sistem untuk digunakan sendiri atau mengexploit untuk dijual atau dilelang di deep web. Sementara jika ditemukan oleh kelompok hacker white hat, biasanya dia akan melaporkan celah keamanan tersebut kepada developer aplikasi agar celah tersebut dapat ditambal atau diperbaiki. Biasanya developer akan memberi imbalan bagi yang menemukan bug atau celah keamanan tersebut.

Dimana Vulnerability Mungkin Terjadi?

Vulerability yang sering diexploitasi pada umumnya ada pada level software dan exploitasi ini dapat dilakukan dari jarak yang jauh. Vulnerability kemungkinan terjadi pada Firmware (hardcoded software), Operation System, Software, Brainware,

Website. Firmware adalah software/mini operation system yang tertanam langsung (hardcore) kedalam chip pada perangkat tertentu, seperti Router, kamera, scanner, dll dengan tujuan untuk memudahkan upgrade kompability perangkat atau penambahan fitur. Vulnerability pada tingkat firmware sangat berbahaya jika terjadi pada perangkat seperti router, sehingga vendor-vendor tipa perangkat akan selalu mengediakan pembaharuan/upgrade untuk menambal atau mengatasi vulnerability ini.

Pada Operation System, jika dilihat sebuah sistem operasi jenis apapun (Linux, Mac, Windows, dll) pasti memiliki celah keamanan yang tinggi dan menunggu waktu untuk ditemukan. Oleh karena itu, sangat perlu adanya untuk selalu melakukan upgrade system dari operation system kita agar celah-celah keamanan ini dapat tertutupi. Selain Operation System, vulnerability juga dapat ditemukan pada sebuah Software, software yang diinstal bisa menjadi jalan masuk bagi hacker terutama aplikasi yang terhubung langsung ke internet, seperti software browser, document reader, dll. Oleh karena itu perlu adanya menggunakan software asli dan bukan bajakan dan tetap mengupgrade software tersebut ke versi yang lebih terbaru agar terhindar dari exploitasi yang memanfaatkan vulnerability pada software yang terinstall.

Disisi operator, ketidaktahuan atau kepolosan dari seorang operator bisa menjadi salah satu celah keamanan bagi seorang hacker, hacker dapat melakukan social enginering pada operator tersebut sehingga secara tidak sengaja operator tersebut menyerahkan akun atau informasi penting ke hacker tanpa disadari. Secanggih apapun sistem saat ini, pasti saja sebuah sistem memiliki kelemahan disisi ini. Vulnerability juga sering terjadi pada sebuah website, website memiliki beragam komponen didalamnya sehingga website memiliki banyak sisi untuk diserang. Selain itu, faktor keamanan penyedia jasa hosting juga menjadi salah satu faktor yang bisa menjadi vulnerability pada sebuah website. Oleh karena itu, sebaiknya pastikan website yang dihosting sudah memiliki fitur keamanan terbaru serta penyedia jasa hosting yang digunakan memberikan jaminan keamanan bagi usernya.

Zero Day Vulnerability, Exploit, dan Attack

Zero Day Vulnerability adalah sebuah vulnerability yang ditemukan oleh hacker sedangkan pihak developer tidak mengetahuinya, dan hacker mengambil keuntungan dari vulnerability tersebut untuk menyebarkan malware atau masuk kesistem secara ilegal. Sedangkan Zero Day Exploit adalah exploit yang dilakukan dan dibuat oleh

hacker berdasarkan Zero Day Vulnerability yang ditemukannya untuk mengexploitasi sistem yang rentan terhadap vulnerability yang ditemukannya. Zero Day Attack terjadi ketika software/hardware dengan vulnerability diexploitasi dan hacker berhasil membuat malware dan menginjeksikannya kedalam vulnerability tersebut sebelum pihak developer diberikan kesempatan untuk menemukan dan memberbaiki vulnerability pada hardware/software yang dikembangkannya. Secara umum berikut merupakan kronologi terjadinya Zero Day Attack:

a. Pihak developer dari suatu perusahaan membuat software/hardware ,tetapi mereka tidak tau bahwa software/hardware yang dibuatnya mempunyai celah keamanan (vulnerability)

b. Hacker menemukan celah keamanan tersebut sebelum pihak developer menemukan dan memperbaikinya

c. Hacker membuat exploit berdasarkan vulnerability yang ditemukan

d. Setelah exploit dilepaskan ke public, maka exploit tersebut akan menyerang sistem yang rentan untuk mencuri data/masuk ke sistem

e. Setelah jatuh korban, biasanya korban akan melaporkan masalah tersebut ke developer, dan pihak developer melakukan analisa terhadap masalah tersebut

f. Pihak developer mengetahui vulnerability dari sistem yang mereka kembangkan, dan pihak developer juga mengetahui kelemahan dari malware tersebut, sehingga pihak developer membuat patch untuk menambal/memperbaiki vulnerability tersebut.

Jenis Exploit

Exploit merupakan sebuah senjata yang dibuat khusus oleh hacker untuk menyerang kelemahan (vulnerability) secara spesifik dari suatu sistem guna mendapatkan akses ke sistem atau jaringan secara paksa. Ada dua jenis exploit, yakni Local Exploit dan Remote Exploit.

a. Local Exploit

Exploit ini hanya bisa mengexploitasi sebuah vulnerability secara local/ dikomputer itu sendiri, biasanya digunakan untuk membangkitkan rootkit, sehingga aplikasi dengan user biasa memiliki hak akses administrator. Pada local exploit, biasanya attacker akan memasukkan payload kedalam file sesuai format aplikasi yang umum digunakan, dan ketika file tersebut dibuka, maka secara otomatis program payload yang berisi shellcode atau perintah untuk mendownload dan mengeksekusi payload dari remote server tersebut akan

dieksekusi dan akhirnya attacker telah berhasil menguasai komputer korban. Local Exploit ini hanya bisa berjalan di komputer yang terinstall software tertentu yang memiliki vulnerability didalamnya.

b. Remote Exploit

Pada remote exploit, attacker akan mengexploitasi sistem melalui service port yang terbuka di komputer/server korban, dengan menggunakan exploit yang dibuat khusus, attacker akan mengirimkan payload yang berisi shellcode malware(biasanya backdoor/trojan). Exploitasi ini dilakukan dengan jarak jauh menggunakan jaringan internet atau jaringan local (bisa target dalam 1 jaringan dengan attacker).Exploitasi jenis ini memanfaatkan celah (vulnerability) service port yang terbuka di komputer client /server ,misalnya mengexploitasi port 443 (SSL heart bleed vuln),SMB port 445 ,ssh port 22 dll,tergantung port yang terbuka oleh service didalam system.

Pada exploitasi aplikasi berbasis web /website attacker biasnaya menyerang kelemahan fitur yang ada,seperti vitur upload file,melakukan penetrasi dengan memasukan query lewat URL dan melihat error yang dihasilkan, tampilah error disini bisa dipakai oleh attacker untuk menganalisa struktur dari database /sistem yang sedang di serang. melalui tampilan error inilah si attacker bisa mendapat informasi seperti versi database,module yang digunakan,plugin yang aktif,struktur database,library yang digunakan dll.

Vulnerability Scanning

Vulnerability Scanner adalah aplikasi yang mengidentifikasi dan membuat inventaris semua sistem (termasuk server, desktop, laptop, mesin virtual, wadah, firewall, sakelar, dan printer) yang terhubung ke jaringan. Untuk setiap perangkat yang dikenali juga berusaha mengidentifikasi sistem operasi yang dijalankannya dan perangkat lunak yang diinstal di dalamnya, bersama dengan atribut lain seperti port terbuka dan akun pengguna.

Sebagian besar Vulnerability Scanner juga akan mencoba masuk ke sistem menggunakan standar atau kredensial lain untuk membangun gambaran sistem yang lebih terperinci. Setelah membangun *inventory*, Vulnerability Scanner memeriksa setiap item dalam *inventory* terhadap satu atau lebih basis data kerentanan yang diketahui untuk melihat apakah ada item yang rentan terhadap kerentanan ini. Hasil Vurnerability Scanner adalah daftar semua sistem yang ditemukan dan diidentifikasi

pada jaringan, yang menyoroti kerentanan yang diketahui yang mungkin perlu diperhatikan.

Vulnerability Scanning vs Penetration Testing

Vulnerability Scanning dan Peneration Testing merupakan kedua istilah yang seringkali membingungkan, tetapi pada kenyataannya kedua prosedur keamanan tersebut sangat berbeda dan digunakan untuk tujuan yang berbeda pula. Pada tingkat paling dasar, Vulnerability Scanning bertujuan untuk mengidentifikasi sistem apa pun yang memiliki kerentanan yang diketahui, sementara Penetration Testing bertujuan untuk mengidentifikasi kelemahan dalam konfigurasi sistem spesifik dan proses dan praktik organisasi yang dapat dieksploitasi untuk membahayakan keamanan. Sebagai ilustrasi perbedaan Vulnerability Scanning dengan Penetration Testing, pada Penetration Testing mungkin melibatkan hal-hal berikut:

a. Menggunakan Social Engineering seperti menyamar sebagai manajer dan meminta kata sandi karyawan untuk mendapatkan akses ke database atau sistem lain
b. Mencegat dan menggunakan kata sandi tidak terenkripsi yang dikirim melalui jaringan
c. Mengirim email phising kepada pengguna untuk mendapatkan akses ke akun

Cara Kerja Vulnerability Scanning

Vulnerability Scanning menemukan sistem dan perangkat lunak yang telah diketahui kerentanan keamanannya, tetapi informasi ini hanya berguna bagi tim keamanan TI ketika digunakan sebagai bagian pertama dari empat proses yang ada pada Vulnerability Management Process. Keempat proses yang ada pada Vulnerability Management Process yakni:

a. Identifikasi Vulnerability

Cara utama untuk mengidentifikasi Vulnerability adalah melalui Vulnerability Scanning, dan kemanjuran pemindai bergantung pada dua hal:

- Kemampuan pemindai untuk menemukan dan mengidentifikasi perangkat, perangkat lunak dan port terbuka, dan mengumpulkan informasi sistem lainnya
- kemampuan untuk menghubungkan informasi ini dengan informasi kerentanan yang diketahui dari satu atau lebih database kerentanan

Vulnerability Scanning dapat dikonfigurasi agar dapat lebih atau kurang agresif , ini penting karena ada kemungkinan bahwa proses pemindaian dapat mempengaruhi kinerja atau stabilitas sistem yang sedang periksa. Ini juga dapat menyebabkan masalah bandwidth pada beberapa jaringan di sistem tersebut. Solusi untuk hal ini adalah dengan menjadwalkan pemindaian kerentanan di luar jam kerja, tetapi ini mengarah pada kemungkinan bahwa karyawan yang menghubungkan laptop ke jaringan mungkin tidak terhubung saat pemindaian berlangsung. Salah satu cara untuk mengatasi masalah kedua ini adalah melalui penggunaan agen endpoint yang berjalan pada laptop dan perangkat lain, yang memungkinkan sistem manajemen kerentanan untuk mendapatkan data inventaris yang didorong oleh agen ketika terhubung ke jaringan daripada ditarik selama pemindaian terjadwal dari jaringan organisasi. Pendekatan lain adalah dengan menggunakan teknik yang disebut Adaptive Vulnerability Scanning, yang mendeteksi perubahan pada jaringan, seperti koneksi laptop baru atau perangkat lain untuk pertama kalinya. Ketika ini terjadi, Vulnerability Scanning diluncurkan secara otomatis dan memindai sistem baru sesegera mungkin, daripada menunggu pemindaian terjadwal berikutnya.

b. Evaluasi risiko yang ditimbulkan oleh Vulnerability yang teridentifikasi

Salah satu tantangan Vulnerability Scanning adalah bahwa ia dapat menghasilkan daftar panjang kerentanan yang telah diidentifikasi, dan jika daftar terlalu panjang dapat membanjiri sumber daya tim keamanan TI. Oleh karena itu, tahap evaluasi sangat penting, karena menentukan tingkat kerentanan dan memungkinkan staf keamanan TI untuk memutuskan:

- Seberapa kritis kerentanan itu dan apa dampaknya terhadap organisasi jika ingin dieksploitasi dengan sukses
- Seberapa praktis bagi seorang peretas untuk mengeksploitasi kerentanan (misalnya, dapatkah itu dieksploitasi dari internet atau apakah akses fisik diperlukan), dan seberapa mudah ini dapat dicapai (mungkin menggunakan kode eksploitasi yang tersedia untuk umum)
- Apakah kontrol keamanan yang ada dapat mengurangi risiko kerentanan dieksploitasi
- Jika kerentanan yang terdeteksi adalah "false positive", maka dapat diabaikan

Pada akhirnya, tujuan dari tahap evaluasi adalah untuk memungkinkan staf keamanan TI untuk memprioritaskan kerentanan yang memerlukan perhatian paling mendesak untuk mengurangi risiko keamanan secara keseluruhan secara efektif dan efisien.

c. Perawatan atau perbaikan terhadap Vulnerability yang teridentifikasi

Setiap kerentanan yang terdeteksi selama Vulnerability Scanning dan bukan positif palsu harus ditambal atau diperbaiki sehingga mereka tidak lagi menimbulkan risiko. Sayangnya, perbaikan atau tambalan sederhana tidak selalu segera tersedia, dan dalam keadaan ini staf keamanan TI dapat memilih untuk mengurangi risiko yang ditimbulkan dengan berhenti menggunakan sistem yang rentan, menambahkan kontrol keamanan lain untuk mencoba membuat kerentanan lebih sulit untuk mengeksploitasi, atau cara lain yang mengurangi kemungkinan kerentanan dieksploitasi atau mengurangi dampaknya dieksploitasi dengan sukses.

Sebagai alternatif, tindakan terbaik mungkin hanya dengan menerima bahwa kerentanan ada dan tidak mengambil tindakan lebih lanjut. Ini mungkin merupakan kasus di mana risiko yang ditimbulkan oleh kerentanan rendah, atau di mana dampak eksploitasinya relatif rendah terhadap biaya memperbaikinya.

d. Melaporkan Vulnerability dan cara penanganannya

Setelah Vulnerability berhasil ditangani, maka selanjutnya Vulnerability tersebut dapat dilaporkan dan juga hasil penangannya dapat di publikasikan ke sistem yang terdampat (melakukan update terhadap sistem).

Jenis Vulnerability Scanning

Tidak semua teknik Vulnerability Scanning sama, dan untuk memastikan kepatuhan terhadap peraturan tertentu (seperti yang ditetapkan oleh Dewan Standar Keamanan PCI), perlu untuk melakukan dua jenis pemindaian kerentanan yang berbeda: pemindaian kerentanan internal dan eksternal.

a. External Vulnerability Scanning

Seperti namanya, pemindaian kerentanan eksternal atau External Vulnerability Scanning dilakukan dari luar jaringan organisasi, dan tujuan

utamanya adalah untuk mendeteksi kerentanan dalam pertahanan perimeter seperti port terbuka di firewall jaringan atau firewall aplikasi web khusus. Pemindaian kerentanan eksternal dapat membantu organisasi memperbaiki masalah keamanan yang dapat memungkinkan peretas memperoleh akses ke jaringan organisasi.

b. Internal Vulnerability Scanning

Sebaliknya, pemindaian kerentanan internal atau Internal Vulnerability Scanning dilakukan dari dalam pertahanan perimeter organisasi. Tujuannya adalah untuk mendeteksi kerentanan yang dapat dieksploitasi oleh peretas yang berhasil menembus pertahanan perimeter, atau sama dengan "ancaman orang dalam" seperti kontraktor atau karyawan yang tidak puas yang memiliki akses sah ke bagian-bagian jaringan.

c. Unauthenticated dan Authenticated Vulnerability Scans

Variasi serupa dari pemindaian kerentanan internal dan eksternal yang identik adalah konsep pemindaian kerentanan yang tidak diautentikasi dan diautentikasi. Pindaian yang tidak terautentikasi, seperti pindaian eksternal, mencari kelemahan dalam batas jaringan, sementara pindaian yang diautentikasi memberikan pemindai kerentanan dengan berbagai kredensial istimewa, memungkinkan mereka untuk menyelidiki bagian dalam jaringan untuk kata sandi yang lemah, masalah konfigurasi, dan database atau aplikasi yang tidak terkonfigurasi.

Pertahanan Keamanan Tambahan

Seperti yang disebutkan sebelumnya, Penetration Testing berbeda dari Vulnerability Scanning baik dalam bagaimana hal itu dilakukan dan dalam tujuannya. Langkah-langkah keamanan lain yang juga melengkapi Vulnerabiliry Scanning dan Management Program meliputi:

a. Breach and attack simulation

Breach and attack simulation (BAS) tools digunakan untuk menjalankan serangan yang disimulasikan untuk mengukur efektivitas kemampuan pencegahan, deteksi dan mitigasi perusahaan. Sebagai contoh, perangkat lunak dapat mensimulasikan serangan phishing pada sistem email perusahaan, serangan cyber pada firewall aplikasi web perusahaan, upaya pengelupasan data, gerakan lateral dalam jaringan, atau serangan malware pada titik akhir. Tujuan BAS

adalah untuk menjawab pertanyaan penting tentang postur keamanan organisasi, seperti apakah peringatan dibuat untuk kondisi yang tepat, dan seberapa efektif dan cepat staf dapat menanggapi peringatan.

b. Threat Hunting

Cybercriminals menghabiskan rata-rata 191 hari di dalam jaringan perusahaan sebelum terdeteksi, menurut penelitian IBM, dan selama waktu itu mereka dapat berupaya untuk mengkompromikan peningkatan jumlah sistem dan mengeksfiltrasi sejumlah besar data. Perburuan ancaman bertujuan untuk mengatasi hal ini dengan secara aktif mencari jaringan malware di perusahaan yang mungkin telah ditempatkan di atasnya atau penyerang yang sedang melakukan kegiatan kriminal secara berkelanjutan. Untuk melakukan perburuan ancaman, diperlukan infrastruktur keamanan yang relatif canggih, termasuk Security Information and Event Management (SIEM) system, dan staf keamanan yang terlatih.

c. Application security testing

Application security testing tools dapat dianggap sebagai alat pengujian kerentanan khusus untuk aplikasi, dan mereka menawarkan cara menganalisis kode aplikasi yang lebih cepat dan biaya lebih rendah daripada tinjauan kode manual. Mereka bisa efektif untuk menemukan kelemahan dan kerentanan yang diketahui dalam kode, dan banyak arahan kepatuhan peraturan mengamanatkan penggunaan alat-alat ini untuk memeriksa kode secara teratur.

Vulnerability Scanning Tools

Ada banyak software yang dapat digunakan untuk Vulnerability Scanning, namun kebanyakan dari mereka berbayar, tetapi ada juga beberapa Vulnerability Scanning tools yang bersifat open source, yakni :

- OpenVAS
- Nexpose Community
- Nikto
- Retina
- Wireshark
- Aircrack-ng

Daftar Sumber :

Ordinary, Arie.(17 Juli 2019).*"Apa Itu Vulnerability (Celah Kemananan)?"*.Dimuat pada https://www.tembolok.id/pengertian-vulnerability-contoh-dan-pencegahan/. Diakses pada 3 Mei 2020.

Rubens, Paul.(5 April 2019).*"Vulnerability Scanning: What It Is and Hot To Do It Right"*.Dimuat pada https://www.esecurityplanet.com/network-security/vulnerability-scanning.html. Diakses pada 3 Mei 2020.