NAMA : Muhammad Rizallul Hakim

NIM : 09011381722085

MATA KULIAH : Administrasi dan Manajemen Jaringan

Resume dari Video di website BrightTalk.com dengan Materi yang berjudul "NNT Vulnerability Tracker™ Overview".

Lampiran Sertifikat:

Resume NNT Vulnerability Tracker™ Overview

Kerentanan baru atau *New Vulnerability* dapat ditemukan setiap hari. Setiap titik lemah atau *Weakspot* dalam sebuah sistem merupakan suatu ancaman, Seperti memungkinkan serangan cyber untuk mencuri data maupun melumpuhkan sebuah sistem bisnis. Bahkan kerentanan yang tampaknya kecil dapat digunakan sebagai pijakan untuk menginfiltrasi jaringan, lalu memasang serangan yang lebih merusak.

Meskipun ada upaya terbaik dari industri untuk mengembangkan produk yang aman, akan tetapi kelemahan dari security yang tidak diduga mungkin masih secara tidak sengaja ditemukan di salah satu produk.

Security researchers dan *"White Hat" Hacker* di seluruh dunia mencoba untuk membasmi *vulnerability* baru. Dan eksploitasi serta pelanggaran yang dapat terjadi sebelum kita tahu bahwa ada masalah keamanan yang lain. Misalnya, kerentanan itu tidak ditemukan selama bertahun-tahun, terlepas dari penggunaan produk OPENSSL di seluruh dunia yang mendunia.

Pada saat ini, lebih dari 112.000 kerentanan yang telah diidentifikasi (https://nvd.nist.gov) berpacu dengan waktu untuk menemukan kerentanan dan memperbaikinya sebelum seorang hacker dapat mengeksploitasinya.

NNT Vulnerability Tracer membuat *threat hunting* dengan cara membuat entri *Common Vulnerabilities and Exposures (*CVE*)* untuk vulnerability yang berhasil ditemukan, *NNT scanner* anda akan diperbarui melalui *live feed*.

CVE disertai dengan "*NNT vulnerability test*" yang relevan untuk mengidentifikasi keberadaan kerentanan di dalam sistem. Dan juga Menjalankan pemindaian sangat lah mudah.

Saat menjalankan pemindaian untuk pertama kali, Menentukan jaringan dan rentang IP dari Perangkat yang ingin dipindai.

NNT vulnerability tracker akan memberikan pilihan untuk menggunakan perpaduan kredensial dan non-kredensial, pengujian fleksibelitas untuk pemindaian pada program.

Pengujian dengan menggunakan non-kredensial akan memberikan hasil yang cepat dan bisa dibilang lebih nyata dalam simulasi sebuah serangan, semetara itu pengujian menggunakan kredensial akan meningkatkan akurasi dan mengurangi "false-positives".

Ketika sudah mendapatkan target untuk dipindai, Selanjutnya dapat memilih apa tipe pemindaian yang akan digunakan dan ketika ingin menjadwalkannya.

NNT Vulnerability Tracker menyediakan berbagai opsi sehingga dapat mengoptimalkan kecepatan pemindaian dan kedalaman pengujian-dari pemindaian *inventory* hingga pemindaian "*All Vulnerabilities*".

Pemindai Generasi Sebelumnya sangat rentan melaporkan *"false-positives". Quality of Detection (QoD)* Memungkinkan Anda untuk memilih keakuratan hasil.dengan hanya menyelidiki masalah real. Anda dapat menghemat waktu.

sebagai solusi kelas enterprise*, NNT Vulnerability Tarcker* dapat didistribusikan penuh dengan beberapa contoh pemindaian, yang memungkinkan anda untuk menggunakan pemindaian lokal untuk jaringan yang sedang di *test*.

Anda juga memiliki pilihan dalam rentang pengujian yang akan digunakan dengan 7 opsi bawaan, atau Anda dapat membuatnya sendiri. Anda bahkan dapat memilih intensitas, kecepatan, dan urutan tes yang akan digunakan untuk pemindaian.

Hasil pemindaian akan disajikan dengan jelas sesuai tingkat keparahan untuk setiap kerentanan yang ditemukan.

cara yang sangat berguna untuk mengurutkan hasil adalah dengan metode resolusi, yaitu dengan tiga opsi utama:

- *workaround (Deployment)*
- *Vendorfix (Patching)*
- *Mitigation (Configuration)*

Dalam konteks keamanan dan kepatuhan, CIS Controls (a.k.a SANS Top 20) Menjabarkan praktik keamanan utama terbaik untuk setiap organisasi

6 Kontrol pertama disebut "Basic" meskipun penting bisa menjadi deskripsi yang lebih akurat

pada kenyataannya Kontrol 1,2,3,5 dan 6 terkait erat dan Kontrol yang paling penting untuk Beroperasi terus menerus untuk pertahanan cyber yang aktif.

Inti dari siklus Kontrol keamanan ini adalah kebutuhan untuk menjaga integritas sistem, karena setiap pelanggaran dihasilkan dari perubahan, atau kebutuhan untuk perubahan.