Nama Anggota :
Abi Daffa A (17/410818/SV/12745) **Konsep Scanning Secara Umum**
Maida K.R (17/415522/SV/13387) **Penjelasan Teknik Scanning**
Andri Fritzent (17/415510/SV/13375) **Pengertian UDP Scanning**
Fathul Firdaus (15/386060/SV/09446)**Penjelasan Cara Kerja UDP Scanning**
Rizky Kurniawan (17/415529/SV/13394) **Tools Yang Digunakan**
Dear Nasyita (17/410830/SV/12757) **Countermeasures Yang Dapat Dilakukan**

Konsep Scanning Network Secara Umum :
Network Scanning adalah salah-satu komponen-komponen dari kecerdikan penyerang dalam pengumpulan informasi untuk membuat profil perusahaan.
Network Scanning mengacu pada sekumpulan prosedur untuk mengidentifikasi hosts, ports, dan layanan di dalam jaringan
Tujuan Network Scanning adalah

1. Menjelajahi hosts yang hidup,alamat IP, dan iport-port yang terbuka dari hosts yang hidup
2. Menjelajahi sistem operasi dan arsitektur sistem
3. Menjelajahi layanan-layanan yang berjalan pada hosts
4. Menjelajahi kerentanan sistem yang hidup

Cara kerja Scanning network secara umum :
Cracker atau hacker biasanya mencari titik kelemahan yang ada untuk mendapatkan akses ke host. Contohnya, apabila cracker sudah mengetahui host menjalankan proses SMTP server, ia dapat menggunakan kelemahan-kelemahan yang dimiliki oleh SMTP server untuk mendapatkan akses ke host.
Hacker akan mengumpulkan informasi dari hasil scanning yang dilakukan. Setelah ia mempunyai informasi yang dibutuhkan, hackers dapat menyiapkan serangan yang akan dilakukan.
Scanning dilakukan dengan men-scan port TCP/IP untuk mengetahui open port dari sebuah live host. Dari proses scanning ini, dapat diperoleh informasi mengenai port-port mana saja yang terbuka, layanan-layanannya, juga versi yang digunakan. Hacker dapat mencari tahu kelemahan-kelemahan yang bisa digunakannya untuk masuk ke dalam host dari informasi tersebut.

Penjelasan Teknik Scanning :
Beberapa contoh teknik scanning yang biasa digunakan dalam network scanning :
TCP Connect (Full-open Scan) – Jenis scan ini konek ke port sasaran dan menyelesaikan three-way handshake (SYN, SYN/ACK, dan ACK). Scan jenis ini mudah terdeteksi oleh sistem sasaran.
Stealth Scan (Half-open Scan) – Teknik ini dikenal sebagai half-opening scanning karena suatu koneksi penuh TCP tidak sampai terbentuk. Sebaliknya, suatu paket SYN dikirimkan ke port sasaran. Bila SYN/ACK diterima dari port sasaran, kita dapat mengambil kesimpulan bahwa port itu berada dalam status listening. Suatu RST/ACT akan dikirim oleh mesin yang melakukan scanning sehingga koneksi penuh tidak akan terbentuk. Teknik ini bersifat tersembunyi, dibandingkan TCP connect penuh, dan tidak akan tercatat pada log sistem sasaran.

TCP FIN scan (-sF) – Teknik ini mengirim suatu paket FIN ke port sasaran. Berdasarkan RFC 793, sistem sasaran akan mengirim balik suatu RST untuk setiap port yang tertutup. Teknik ini hanya dapat dipakai pada stack TCP/IP berbasis UNIX.
TCP Xmas Tree scan (-sX) – Teknik ini mengirimkan suatu paket FIN, URG, dan PUSH ke port sasaran. Berdasarkan RFC 793, sistem sasaran akan mengembalikan suatu RST untuk semua port yang tertutup.
TCP Null scan (-sN) – Teknik ini membuat off semua flag. Berdasarkan RFC 793, sistem sasaran akan mengirim balik suatu RST untuk semua port yang tertutup.

Pengertian UDP Scanning :
UDP Scanning adalah metode scan dengan memanfaatkan pengiriman UDP packet. Bila PORT sasaran memberikan respon berupa pesan “ICMP PORT unreachable” artinya PORT ini tertutup. Sebaliknya bila tidak menerima pesan di atas, kita dapat menyimpulkan bahwa PORT itu terbuka. UDP scanning merupakan proses yang amat lambat apabila anda mencoba melakukan scan terhadap suatu perangkat yang menjalankan packet filtering berbeban tinggi.

Penjelasan Cara Kerja UDP Scanning :
Cara kerja udp scanning :
Kita mengirimkan paket udp dan men
unggu respond an ketika mengirimkan ini ada 3 status:
- Jika kita menerima jawaban maka port yang diinginkan berarti terbuka
- Jika kita menerima ICMp unreachable paket berarti port yang diingikan tertutup
- Jika kita tidak menerima respon apa-apa maka port yang diinginkan terbuka, atau bisa juga pesan kita di filter oleh protocol karena alasan tertentu

Tools Yang Digunakan :
Daftar berikut berdasarkan tools populer yang sering digunakan untuk menggambarkan topologi jaringan yang digunakan attacker.
1. Nmap
2. Unicornscan
3. Angry IP Scan
4. Netcat

Countermeasures Yang Dapat Dilakukan :
1. Konfigurasikan firewall dan IDS untuk mendeteksi dan memblokir probe.
2. Gunakan aturan khusus untuk mengunci jaringan dan memblokir port yang tidak diinginkan.
3. Jalankan port Alat pemindaian untuk menentukan apakah firewall mendeteksi aktivitas pemindaian port dengan akurat.
4. Pakar Keamanan harus memastikan konfigurasi yang tepat dari aturan anti-pemindai dan anti-spoofing.
5. Pakar keamanan suatu organisasi juga harus memastikan bahwa IDS, router, dan firmware firewall diperbarui untuk rilis terbaru mereka.

Refrensi :
Andri Fritzent:
http://simbel.tedi.sv.ugm.ac.id/stage3.4/mod/page/view.php?id=3296
https://www.lautan-it.com/2018/08/pengertian-port-scanning-beserta.html
Rizky Kurniawan :
Tools yang digunakan https://securitytrails.com/blog/best-port-scanners
Abi Daffa A dan Maida:
https://www.google.com/amp/s/kuliahkuliah.wordpress.com/2016/03/19/laporan-pendahuluan-network-scanning-probing/amp/
Dear Nasyita :
https://www.w3schools.in/ethical-hacking/scanning-techniques/#Countermeasures_Against_Scanning
Fathul Firdaus :
https://kuliahkuliah.wordpress.com/2016/03/19/laporan-pendahuluan-network-scanning-probing/
nmap.org