LAPORAN AKHIR

Mata Praktikum	: SISTEM KEAMANAN KOMPUTER
Kelas	: 3IA11
Minggu ke-	: 5
Tanggal	: 31/10/2024
Materi	: FOOTPRINTING DAN SCANNING
NPM	: 51422161
Nama	: MUHAMMAD TARMIDZI BARIQ
Dosen Matakuliah	: ANDREAS HADIYONO
Jumlah Lembar	:

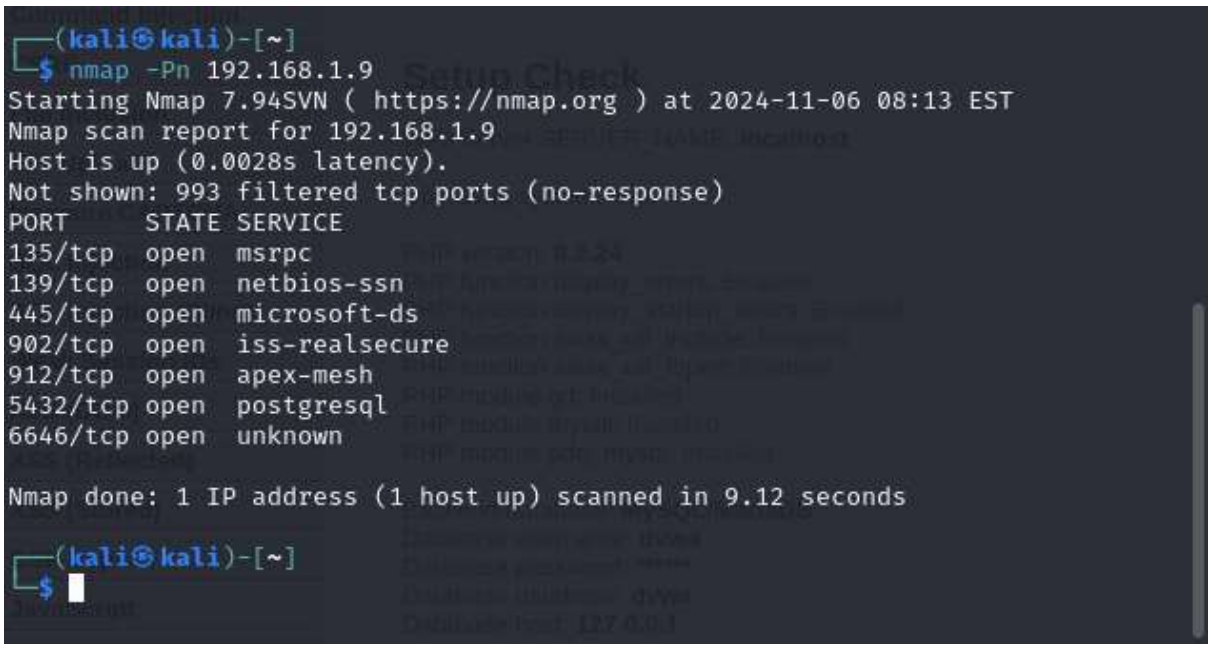
LABORATORIUM TEKNIK INFORMATIKA

UNIVERSITAS GUNADARMA

2024

Penggunaan Nmap

Scan IP Tunggal



Tujuan

Melakukan pemindaian pada IP 192.168.1.9 untuk mengidentifikasi port terbuka dan layanan yang berjalan.

Hasil

1. 135/tcp open msrpc:

   Port 135 digunakan untuk Microsoft RPC (Remote Procedure Call), sering kali digunakan oleh sistem Windows untuk komunikasi antar layanan di jaringan. Port ini bisa menjadi target serangan jika ada kerentanan di layanan RPC.
2. 139/tcp open netbios-ssn:

   Port ini digunakan oleh layanan NetBIOS Session Service, yang memungkinkan komunikasi di jaringan lokal dan sering dipakai untuk berbagi file dan printer di Windows. Port ini dapat dieksploitasi oleh penyerang untuk mendapatkan akses ke file yang dibagikan atau informasi jaringan.
3. 445/tcp open microsoft-ds:

   Port ini digunakan untuk SMB (Server Message Block) atau CIFS (Common Internet File System) di Windows. SMB sering digunakan untuk berbagi file dan sumber daya antar

perangkat di jaringan. Port ini sering menjadi target serangan ransomware dan eksploitasi SMB.

4. 902/tcp open iss-realsecure:

   Port ini digunakan oleh VMware Authentication Daemon, yang sering muncul pada server yang menjalankan VMware. Port ini memungkinkan klien untuk terhubung ke VM menggunakan VMware Workstation atau vSphere Client. Port ini memungkinkan koneksi ke VM melalui VMware Workstation atau vSphere Client, yang bisa menjadi titik serangan jika tidak diamankan.

5. 912/tcp open apex-mesh:

   Port ini biasanya dikaitkan dengan layanan Apex Mesh atau aplikasi khusus lain. Namun, port ini tidak umum dan bisa jadi dikonfigurasi untuk aplikasi atau layanan tertentu. Layanan pada port ini tidak umum dan bisa jadi telah dikonfigurasi untuk tujuan tertentu, yang harus diaudit keamanannya.

6. 5432/tcp open postgresql:

   Port ini adalah port default untuk PostgreSQL, sebuah sistem manajemen basis data relasional yang sering digunakan dalam aplikasi server. Pastikan PostgreSQL dikonfigurasi dengan kata sandi yang kuat dan tidak mudah diakses oleh pengguna yang tidak sah.

7. 6646/tcp open unknown:

   Port ini terdaftar sebagai unknown, artinya tidak ada informasi resmi mengenai layanan di port ini. Biasanya, ini mungkin dikonfigurasi oleh aplikasi atau layanan yang tidak standar. Port ini perlu diperiksa lebih lanjut untuk menentukan layanan yang berjalan dan potensi kerentanannya.

Kesimpulan

Server atau perangkat dengan IP 192.168.1.9 ini kemungkinan adalah server Windows dengan PostgreSQL dan mungkin layanan VMware, serta beberapa port terbuka yang menunjukkan adanya aplikasi khusus atau layanan yang dikustomisasi. Untuk mengamankan perangkat, perlu dilakukan audit keamanan pada port-port terbuka ini dan membatasi akses hanya pada jaringan yang terpercaya.