nmap

This uses the `nmap` tool to perform a detailed TCP port scan on the IP range `192.168.0.0/24`.

```
sudo nmap -sS -p- -PE -PP -PS80,443 -PA3389 -PU40125 -A -T4 -oA tcpscan-%D 192.168.0.0/24
```

- `sudo`: Runs the command with administrative privileges.
- `nmap`: The command-line tool used for network exploration and security auditing.
- `-sS`: Performs a TCP SYN scan, which is the default scan type for privileged users.
- `-p-`: Scans all 65,535 TCP ports.
- `-PE`: Sends ICMP echo requests (ping) to discover live hosts.
- `-PP`: Sends ICMP timestamp requests to discover live hosts.
- `-PS80,443`: Sends TCP SYN packets to ports 80 and 443 (default web server) to discover open ports.
- `-PA3389`: Sends TCP ACK packets to port 3389 (default RDP) to discover open ports.
- `-PU40125`: Sends UDP packets to port 40125 (unlikely to be in use) to discover open ports (some services such as the `chargen` protocol respond to empty UDP packets).
- `-A`: Enables aggressive scanning options, including OS detection, version detection, script scanning, and traceroute.
- `-T4`: Sets the timing template to "Aggressive" to speed up the scan (otherwise it can take quite a while, even on a /24 network).
- `-oA tcpscan-%D`: Specifies the output file name format. `%D` is a placeholder for the current date and time.
- `192.168.0.0/24`: Specifies the IP range to scan, in this case, all IP addresses from `192.168.0.0` to `192.168.0.255`.

For a simpler verbose scan,

```
sudo nmap -v -A -sS -p- -O target
```

- `sudo`: Runs the command with administrative privileges.
- `nmap`: The command-line tool used for network exploration and security auditing.
- `-v`: Enables **verbose output**, providing more detailed information during the scan.
- `-A`: Enables **aggressive scanning** options, including OS detection, version detection, script scanning, and traceroute.
- `-sS`: Performs a **TCP SYN** scan, which is the default scan type for privileged users.
- `-p-`: Scans **all 65,535 TCP ports**.
- `-O`: Enables **OS detection**, which attempts to determine the operating system running on the target.
- `target`: Specifies the target IP address, DNS name, or CIDR range to scan.

Revision #2
Created 28 May 2024 18:00:02 by Cesar Gzz
Updated 28 May 2024 19:56:54 by Cesar Gzz