Scanning with Rustscan

We'll explore RustScan, a fast and efficient port scanning tool that leverages the Rust programming language to achieve lightning-fast scanning speeds. It is an other alternative to nmap but it does integrates with nmap perfectly and thats what i love about it.

Key Features of RustScan

RustScan offers several key features that make it a valuable addition to your security toolkit:

- **Extremely fast scanning**: RustScan can scan a host for all 65,535 TCP ports in under 10 seconds.
- **Nmap integration**: RustScan can automatically run Nmap scans on the identified open ports, providing a comprehensive analysis.
- **Flexible output**: RustScan supports various output formats, including JSON and CSV, making it easy to integrate with other tools and scripts.
- **Customizable scanning**: RustScan provides options for specifying target IP addresses, port ranges, and scan rates.

Installation

- Go to the below URL

https://github.com/RustScan/RustScan/releases

- Download the deb file.
- Install it.

```
sudo dpkg -i rustscan_2.2.3_amd64.deb
```

Usage

Lets see some basis usage of using Rust scan.

To perform a all TCP port scan we will provide the -a flag.

```
rustscan -a IP
```

Lets integrate it with nmap.

```
rustscan -p 22,80,445 -a 192.168.29.141 -- -A

rustscan -a 192.168.29.141 -- -sV
```

By leveraging the speed of RustScan and the power of Nmap, you can conduct efficient and thorough port scans, saving time and resources in the process.
