Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

elddy / NimScan Public

Notifications Fork 38 Star 388

Code Issues 8 Pull requests Actions Projects Security Insights

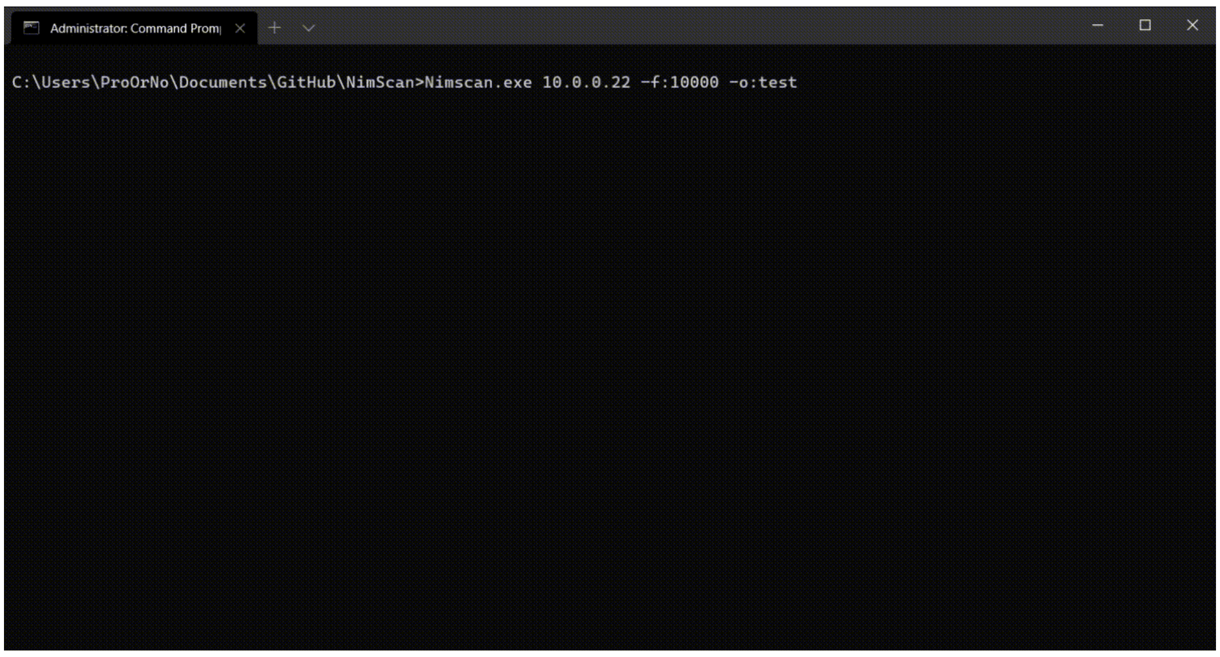
master Go to file Code

elddy Removed stdout.eraseLine() 6440f53 · 3 years ago 73 Commits

libForC	Check OSDiscovery module at compile ...	3 years ago
modules	Removed stdout.eraseLine()	3 years ago
.gitignore	Output to CSV and Verbose mode	4 years ago
LICENSE	Initial commit	5 years ago
NimScan.nim	OSDiscovery feature	4 years ago
NimScan.nim.cfg	optimization	4 years ago
README.md	Update README.md	4 years ago

👑 NimScan 👑

Really fast port scanner (With filtered option - Windows support only)



```
C:\Users\ProOrNo\Documents\GitHub\NimScan>Nimscan.exe 10.0.0.22 -f:10000 -o:test
```

Benchmarks

⚙️ Category	👁️ Nmap	🤖 RustScan	♨️ masscan	👑 NimScan
Filtered	~107 Seconds	❌	❌	~60 Seconds (Windows Only)
non-filtered	~25 Seconds	~3 Seconds (Linux)	~8 Seconds (Linux)	~7 Seconds (2 threads)
Dependencies	Npcap driver	Nmap	libpcap driver	No dependencies

About

🚀 Fast Port Scanner 🚀

c windows linux fast nim cpp scanner port pentesting port-scanner port-scanning security-tools filtered redteam port-scan

Readme
MIT license
Activity
388 stars
3 watching
38 forks
Report repository

Releases 4

🔥 New Banner & Features 🔥 Latest
on Mar 9, 2021

+ 3 releases

Packages

No packages published

Contributors 3

elddy
Hydra820
kevrool

Languages

- Nim 97.8%
- C 2.2%

Can be used as module/library	✗	✗	✗	✓

All bechmarks were performed inside LAN and on 65K ports.

Usage

```
Usage:
    NimScan <host | IPs> -p:<portX>-<portY> [--timeout=<time>] [--fi
    NimScan <host | IPs> -p:<port>
    NimScan <host | IPs> -p:<port1>,<port2>,<portN>
    NimScan (-h | --help)
Options:
    -h, --help            Show this screen.
    -p, --ports           Ports to scan. [default: 1-65,535]
    -a, --all             Use rawsockets to find filtered/closed/ope
    -t, --threads         Number of threads per scan.
    -f, --files=<limit>   File descriptors per thread limit.
    -i, --ignore          Ignore ping latency check.
    --timeout=<time>      Timeout to add to the latency [default: 15
```

Examples

Scan range between 1 to 5000 ports

```
NimScan 10.0.0.0/24 -p:1-5000
```

Scan specific ports

```
NimScan 10.0.0.1-10.0.0.10 -p:80,443,445
```

Show closed/filtered/open using rawsockets

```
NimScan.exe 10.0.0.69 -a
```

C/C++ Library 🧑‍💻

Guide

Exported functions

```
scan(char * host, int * ports, int size);
scanner(char * host, int * ports, int size, char * parameters);
```

Options

- host - IP/HOST to scan
- ports - Ports to scan
- size - Size of ports array
- parameters - Parameters to give for the scanner as mentiond above under Usage

Create

README   MIT license

```
int main(void)
{
    NimMain(); // A MUST!

    int ports[] = {1, 445, 8080, 3389, 135, 139};
    int size = sizeof ports / sizeof ports[0];

    scan(<IP/HOST>, ports, size); // Scan given ports with default c

    scanner(<IP/HOST>, NULL, 0, "<arguments>"); // Scanning all 65K
    return 0;
}
```

Compile

Make sure NimScanToC.a is in your program's folder.

```
gcc <file>.c -L. -l:NimScanToC.a -w -o NimScan.exe
```