









Sign in


 3CORESec / MAL-CL Public


 Notifications


 Fork 43


 Star 308


<> Code

 Issues

 Pull requests


 Actions



 Security


 Insights

MAL-CL / Descriptors / Other / Advanced Port Scanner / 





Name	Last commit message	Last commit date
 ..		
 README.md		

README.md 

Advanced Port Scanner

Table of Contents

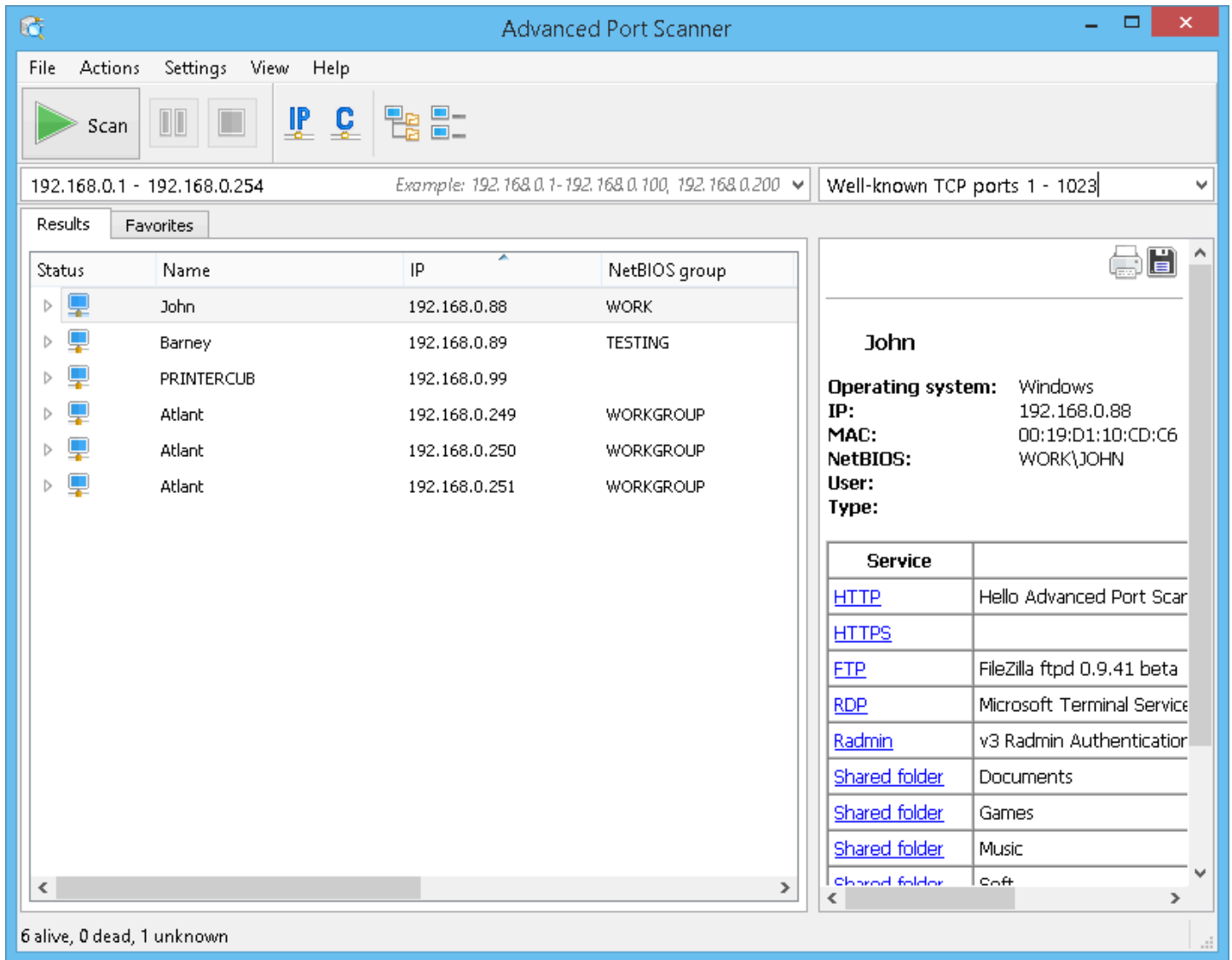
- [Advanced Port Scanner](#)
 - [Table of Contents](#)
 - [Acknowledgement\(s\)](#)
 - [Description](#)
 - [Versions History](#)
 - [File Metadata](#)
 - [Common CommandLine](#)
 - [Threat Actor Ops \(TAOps\)](#)
 - [Common Process Trees](#)

- [Default Install Location](#)
- [DFIR Artifacts](#)
- [Examples In The Wild](#)
- [Documentation](#)
- [Blogs / Reports References](#)
- [ATT&CK Techniques](#)
- [Telemetry](#)
- [Detection Validation](#)
- [Detection Rules](#)
- [LOLBAS / GTFOBins References](#)

Acknowledgement(s)

- 3CORESec - [@3CORESec](#)
- Nasreddine Bencherchali - [@nas_bench](#)

Description



Advanced Port Scanner is a free network scanner allowing you to quickly find open ports on network computers and retrieve versions of programs running on the detected ports —

[Advanced Port Scanner](#)

Versions History

- TBD

File Metadata

- TBD

Common CommandLine

```
advanced_port_scanner.exe /portable [PATH] /lng [Language]
```



```
advanced_port_scanner_console.exe /r:[IP RANGE]
```

```
advanced_port_scanner_console.exe /r:[IP RANGE] /p:[PORT RANGE]
```

```
advanced_port_scanner_console.exe /s:ip_ranges.txt /f:scan_results.txt
```

Threat Actor Ops (TAOps)

- TBD

Common Process Trees

- TBD

Default Install Location

```
C:\Program Files (x86)\Advanced Port Scanner\
```



```
C:\Users\Administrator\AppData\Local\Temp\2\Advanced Port Scanner 2\
```

```
C:\Users\[user]\AppData\Local\Programs\Advanced Port Scanner Portable\
```

DFIR Artifacts

- TBD

Examples In The Wild

- [ANY.RUN — pscan24.exe](#)

Documentation

- [Advanced Port Scanner \(GUI\) — Help](#)
- Advanced Port Scanner Help:

Usage:

`</r:<IP range> OR /s:<source_file>> [/p:<ports list>] [/f:<output_file>]`

Description:

`/r` - address or range of IP addresses to scan, ex 192.168.0.1-192.168.0.255
or

`/s` - path to the file with IP ranges with 1 IP/IP range per line format, ex
192.168.0.1-192.168.0.128
192.168.0.155
192.168.1.10

`/p` - list of ports to scan, ex
1-20
1,2,UDP:1-10

`/f` - path to the file where scan results will be written

Example:

```
advanced_port_scanner_console.exe /r:192.168.0.1-192.168.0.255  
advanced_port_scanner_console.exe /r:192.168.0.1-192.168.0.255 /p:1-10  
advanced_port_scanner_console.exe /s:ip_ranges.txt /f:scan_results.txt
```

Blogs / Reports References

- TBD

ATT&CK Techniques

- [T1046 — Network Service Scanning](#)
- [T1135 — Network Share Discovery](#)

Telemetry

- [Security Event ID 4688 — A new process has been created](#)
- [Sysmon Event ID 1 — Process creation](#)

- [PsSetCreateProcessNotifyRoutine/Ex](#)
- [ETW - Microsoft-Windows-Kernel-Process - Event ID 1 - ProcessStart](#)

Detection Validation

- TBD

Detection Rules

- TBD

LOLBAS / GTFOBins References

- None