Files

master

Go to file

- Descriptors
  - Antivirus
  - NirSoft Utilities
  - Other
    - AdFind
    - Advanced IP Scanner
    - Advanced Port Scanner
      - README.md
    - AnyDesk
    - CleanWipe
    - Defender Control
    - Defender Exclusion Tool (AKA ...
    - IntelliAdmin Network Administ...
    - LaZagne
    - NBTscan
    - PAExec
    - Radmin
    - Rclone
    - SoftPerfect Network Scanner
    - TPAR
    - Winrar
    - Sysinternals
    - Windows 2000 Resource Kit Tools
    - Windows
  - Images
  - Template
  - LICENSE
  - README.md

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

nasbench Add "File Metadata" Section 8c22267 · 3 years ago History

Name	Last commit message	Last commit date
..		
README.md	Add "File Metadata" Section	3 years ago

README.md

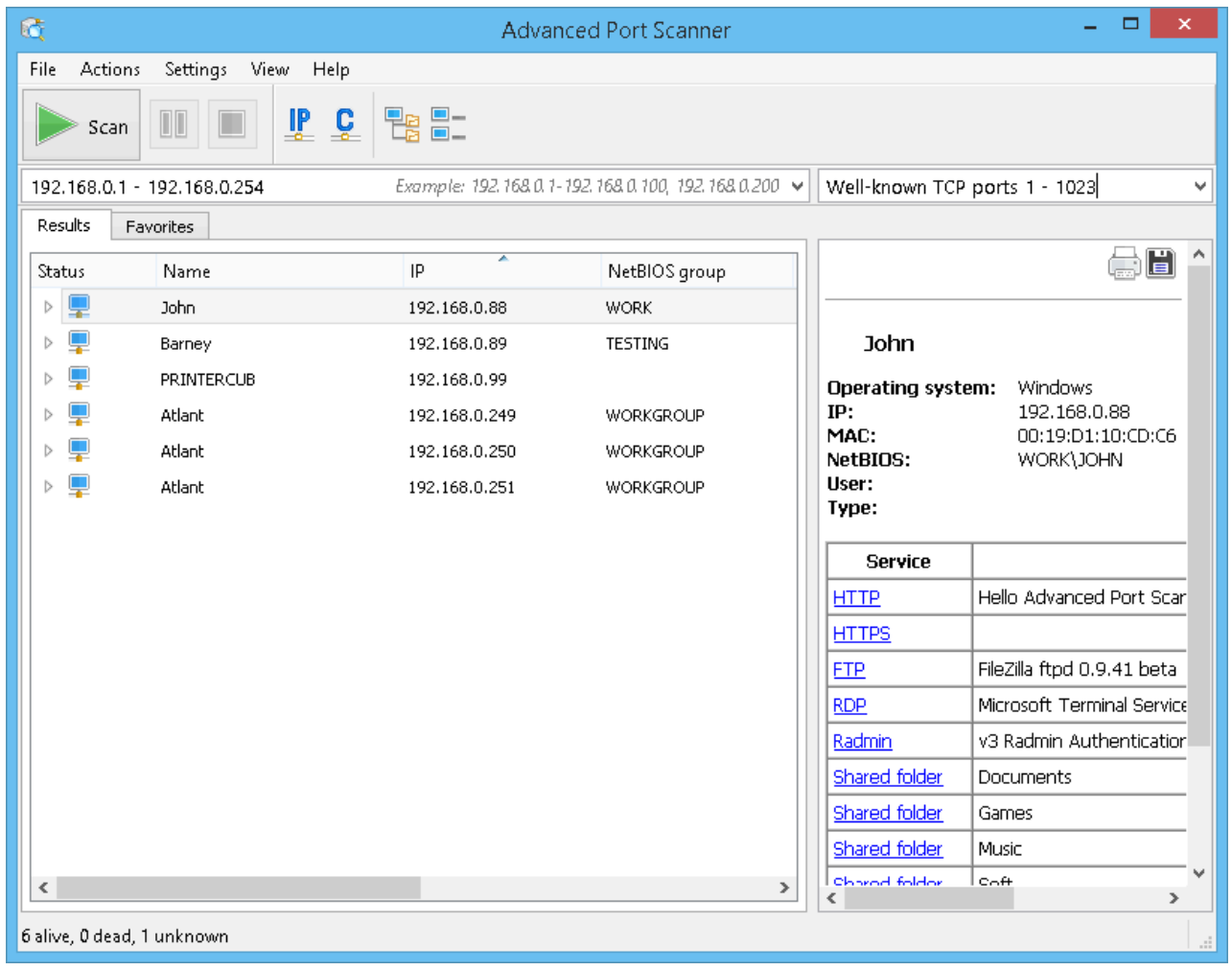
Advanced Port Scanner

Table of Contents

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.
or
/s - path to the file with IP ranges with 1 IP/IP range per line format,
     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