PortScanner Pro — Product & Documentation

PortScanner Pro — Product & Documentation

1. Product Overview
PortScanner Pro is a professional network reconnaissance tool built for security teams, system administrators, and network auditors. It performs fast, reliable port discovery and service fingerprinting across IPv4/IPv6 targets, with multi-protocol support, customizable scanning profiles, and detailed exportable reports suitable for vulnerability management workflows.

Key benefits:
- Rapid discovery of open services across large address spaces.
- Accurate service and version fingerprinting.
- Flexible scanning modes (TCP/UDP/SYN/ACK/Connect/Stealth).
- Integrations with SIEMs and ticketing systems via JSON/XML/CSV output.
- User-friendly GUI and full-featured CLI for automation.

2. Core Features
- Multi-protocol scanning: TCP (SYN/Connect), UDP, SCTP probe support.
- Service fingerprinting: Application-level probes to deduce service type and version.
- Parallelism & rate control: Tunable concurrency and adaptive throttling to avoid network overload.
- Scheduling & scans-as-a-service: Save, schedule, and run recurring scans.
- Agentless & agent-based options: Remote agent for segmented networks.
- Custom probe library: Add custom application probes and signatures.
- Credentialed scanning (optional): Use SSH/WinRM credentials to perform deeper checks.
- Export formats: JSON, CSV, XML, PDF-ready HTML reports.
- Integrations: Webhooks, REST API, SIEM connectors.
- Role-based access control & audit logs.
- Dark-mode GUI with map and topology visualizations.

3. Typical Use Cases
- Asset discovery for vulnerability management.
- Network inventory and service mapping.
- Validation of firewall/ACL configurations.
- Compliance scans (supporting scan scheduling and reports).
- Incident response reconnaissance.

4. Installation & Requirements
Supported platforms: Linux (preferred), macOS, Windows (limited features), Docker.

Minimum requirements (small deployments):
- CPU: 2 cores
- RAM: 4 GB
- Disk: 10 GB
- Network: Outbound raw-socket capability for SYN/stealth scans (Linux with CAP_NET_RAW or run as root)

Recommended (enterprise):
- CPU: 8+ cores

- RAM: 16+ GB
- Disk: 100 GB
- Dedicated scanning network interface

Installation (Linux, tarball):
1. Download portscanner-pro-<version>.tar.gz
2. Extract: tar -xzf portscanner-pro-<version>.tar.gz
3. Install dependencies (example Debian/Ubuntu): sudo apt update && sudo apt install -y libpcap-dev python3 python3-venv
4. Install and run: cd portscanner-pro-<version> && ./install.sh && sudo ./portscanner-pro

Docker:
- Pull image: docker pull company/portscanner-pro:latest
- Run (example): docker run --cap-add=NET_RAW -p 8080:8080 company/portscanner-pro

5. Quickstart (CLI)
Scan a single host for top 1000 ports:
  sudo portscanner-pro scan --target 192.0.2.10 --top-ports 1000

Scan a CIDR range with parallelism and output to JSON:
  sudo portscanner-pro scan --target 198.51.100.0/24 --concurrency 200 --output report.json

Run a scheduled scan:
  portscanner-pro schedule add --name "Weekly-Inventory" --cron "0 3 * * 1" --targets 10.0.0.0/16

Example: Credentialed deeper check (SSH)
  portscanner-pro credential-scan --target 10.0.0.5 --ssh-user ubuntu --ssh-key /path/id_rsa --checks service-version

6. GUI Quickstart
- Start server: sudo systemctl start portscanner-pro
- Open browser: http://<host>:8080
- Login with admin credentials created during install
- Add targets in "Targets" -> New scan -> Select profile -> Run now or schedule

7. Example Outputs (CLI JSON snippet)

```
{
  "target":"192.0.2.10",
  "ports":[
    {"port":22,"protocol":"tcp","state":"open","service":"ssh","version":"OpenSSH 8.2p1"},
    {"port":80,"protocol":"tcp","state":"open","service":"http","version":"Apache httpd 2.4.41"}
  ],
  "scan_time":"2025-10-15T10:12:03Z"
}
```


8. Best Practices
- Always obtain written authorization before scanning networks you do not own.
- Use scheduled scans and rate-limiting to reduce impact on production systems.
- Segment scanning traffic via a dedicated interface or VLAN.
- Keep probe libraries and signatures up to date.

- Validate results with follow-up credentialed scans where appropriate.

9. Security & Legal Notes
Port scanning may be considered intrusive; ensure you have permission from asset owners. Misuse of PortScanner Pro for unauthorized access or attacks is strictly prohibited. Logs and audit trails are kept for compliance; configure retention policies according to local regulations.

10. FAQ
Q: Is PortScanner Pro safe to run on production systems?
A: When configured with conservative rate limits and off-hours scheduling, it can be run safely. Start with small subsets and monitor.

Q: Does it support IPv6?
A: Yes, full IPv6 scanning is supported.

Q: Can I integrate with my SIEM?
A: Yes. There are webhooks, REST API, and direct connectors for major SIEMs.

11. Changelog (sample)
v1.4.0 — 2025-08-01
- Added UDP probe improvements and enhanced fingerprinting
- New REST API endpoints for scan orchestration

v1.3.0 — 2024-12-15
- GUI dark mode and topology visualization
- Improved scheduling engine

Contact & Support:
Email: support@portscannerpro.example
Docs: https://docs.portscannerpro.example