OFFSEC

www.offsec.ir

Introduction OWASP Nettacker

Automated Penetration Testing Framework

Ali Razmjoo Qalaei
ali@offsec.ir
ali.razmjoo@owasp.org

self.author

- Software Engineering Student
- OWASP Chapter and Project Leader
  - Iran Chapter Leader (link)
- OWASP ZSC Project Leader (link)
  - Founder/Creator (9 Contributors) (link)
  - Contributed OWASP ZSC API in GDB Peda (link)
  - Google Summer of Code (GSoC 2016) (link)
  - DEF CON Demo Lab (link)
  - Blackhat Arsenal 2016 (link)
  - Presented in OFFSECONF 2016 (link)
  - Top 10 Best Security Tools by ToolsWatch (link)
  - OWASP Code Sprint 2017 (link)
- Vira: Strategic Development of Security Arenas (PJS)
  - CEO/Founder (viraintel.com)
  - Full Stack Developer
- OWASP Nettacker Project Leader
  - Founder/Creator (5 Contributors) (link)
  - R&D Phase
- Programmer and Security Researcher
  - Researcher
  - Mentor
  - Penetration Tester
  - OFFSEC Leader (Iran) (link)

self.intro

OWASP Nettacker project is created to automate information gathering, vulnerability scanning and eventually generating a report for networks, including services, bugs, vulnerabilities, misconfigurations, and other information. This software will utilize TCP SYN, ACK, ICMP and many other protocols in order to detect and bypass Firewall/IDS/IPS devices. By leveraging a unique method in OWASP Nettacker for discovering protected services and devices such as SCADA. It would make a competitive edge compared to other scanner making it one of the bests.

OWASP
The Open Web Application Security Project

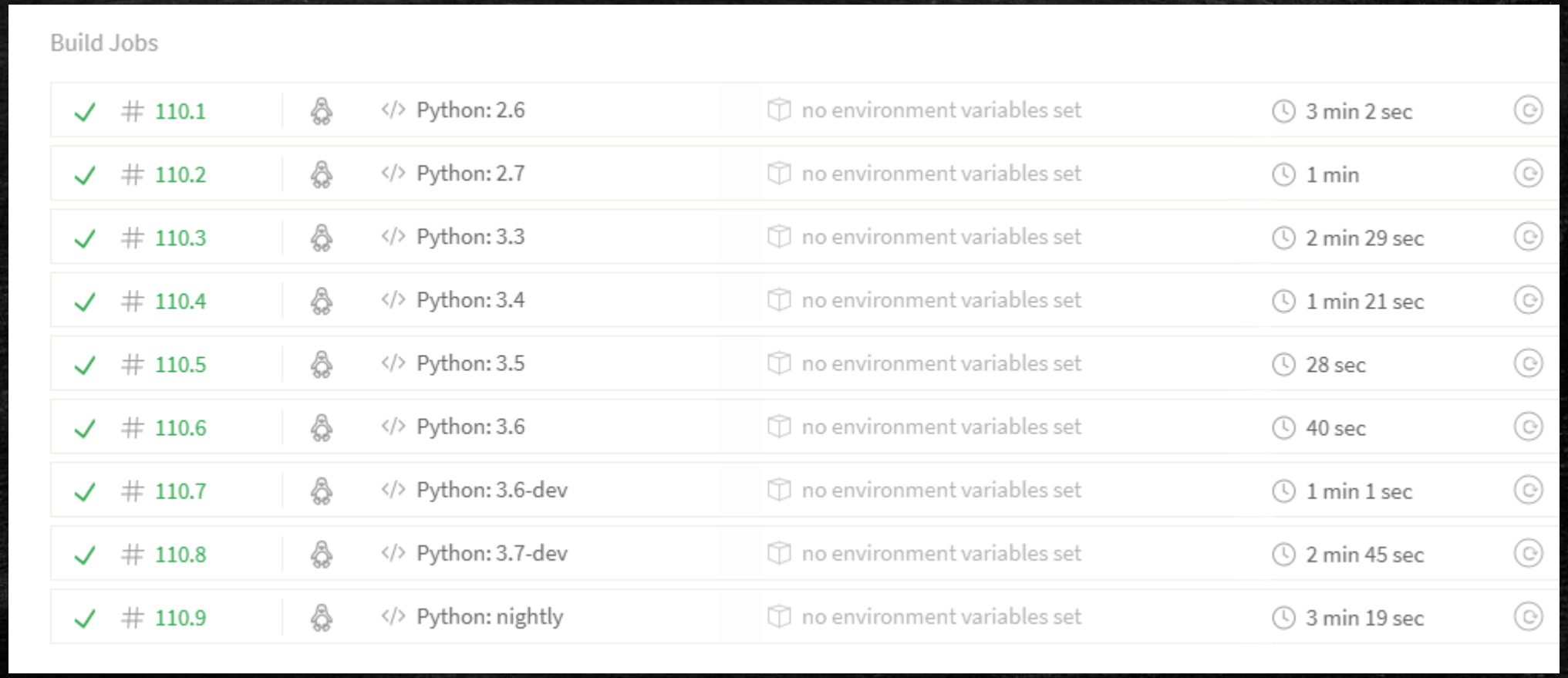
self.urls

- OWASP Page: https://www.owasp.org/index.php/OWASP_Nettacker
- Home: http://nettacker.z3r0d4y.com/
- Github: https://github.com/viraintel/OWASP-Nettacker
- Mailing List: https://groups.google.com/forum/#!forum/owasp-nettacker

OFFSEC
www.offsec.ir

self.why_owasp_nettacker

- Easy to run and use
  - Run everywhere with Python 2.x, 3.x https://travis-ci.org/viraintel/OWASP-Nettacker/



OFFSEC
www.offsec.ir

self.why_owasp_nettacker

- Easy to use
  - Enabled default options
  - Customizable Configuration
    - Profiles

OFFSEC
www.offsec.ir

self.why_owasp_nettacker

- High Speed
  - Highest speed with fewest hardware resources (CPU: Intel Core i7-3610QM 2.30 GHz)
- 10 threads
  - 0.9% of 1 core of CPU

python.exe	0.9%	13.6 MB	0 MB/s	0 Mbps

- 1000 threads
  - 6.4% of 1 core of CPU

python.exe	6.4%	27.6 MB	0 MB/s	0 Mbps

- Measure-Command {**python nettacker.py** -i 192.168.0.1 -t 1000 -T 0.5 -m tcp_connect_port_scan}
  - TotalSeconds : **2.8466034**

self.why_owasp_nettacker

- Multi Language Support
  - Supporting 20 language
  - Easy to contribute languages (JSON)

```
Engine:
  Engine input options

  -L LANGUAGE, --language LANGUAGE
                        select a language ['ru', 'fr', 'en', 'nl', 'el', 'vi',
                        'id', 'de', 'tr', 'ps', 'ur', 'fa', 'hy', 'hi', 'ko',
                        'it', 'zh-cn', 'ar', 'ja', 'es']
  -v VERBOSE_LEVEL, --verbose VERBOSE_LEVEL
                        verbose mode level (0-5) (default 0)
  -V, --version         show software version
```

OFFSEC
www.offsec.ir

self.why_owasp_nettacker

- Multi Language Support
  - Supporting 20 language
  - Easy to contribute languages (JSON)

OFFSEC
www.offsec.ir

self.why_owasp_nettacker

- Getting focus on IoT Security
  - Show an example? D-Link DWR 932C
    - By Ehsan Nezami and Ali Razmjoo Qalaei – ViraIntel Full Stack Developers

- Mobile Application
  - Telegram BruteForce Passcode with adb Android (link)
    - By Sepehr Keshavarz Haddad – ViraIntel Full Stack Developers

self.owasp_nettacker_categories

- Brute
  - ssh_brute
  - ftp_brute
  - smtp_brute
- Scan
  - dir_scan
  - tcp_connect_port_scan
  - viewdns_reverse_ip_lookup_scan
- Graph
  - d3_tree_v1_graph (closed) – D3 JS Lib
  - d3_tree_v2_graph (opened) – D3 JS Lib
  - jit_circle_v1_graph - JIT JS Lib

OFFSEC
www.offsec.ir

self.owasp_nettacker_categories

OWASP Nettacker Categories are not limited, we already working on WiFi Networks, Exploiting and Payloads, Fuzzers, AI and Machine Learning, and other categories. (Publish Soon)

- WiFi
  - disconnect_all_clients_wifi
  - wps_vulnerability_wifi
  - wpa2_attack_wifi
- Scan
  - device_scan
  - os_scan
  - router_scan
  - tcp_udp_signature_scan
- Fuzzer
  - web_application_fuzz
  - binary_argv_fuzz
- Exploit
  - heartbleed_exploit
  - eternal_blue_exploit
  - microsoft_office_hta_exploit
  - dlink_dir605L_dos_exploit
- Payload (OWASP ZSC)
  - windows_shellcode_x86_payload
  - windows_shellcode_x64_payload
  - osx_shellcode_x86_payload
  - osx_shellcode_x64_payload
  - linux_shellcode_x86_payload
  - linux_shellcode_x64_payload
  - windows_x86_egg_hunter_payload
  - linux_x86_egg_hunter_payload

OFFSEC
www.offsec.ir

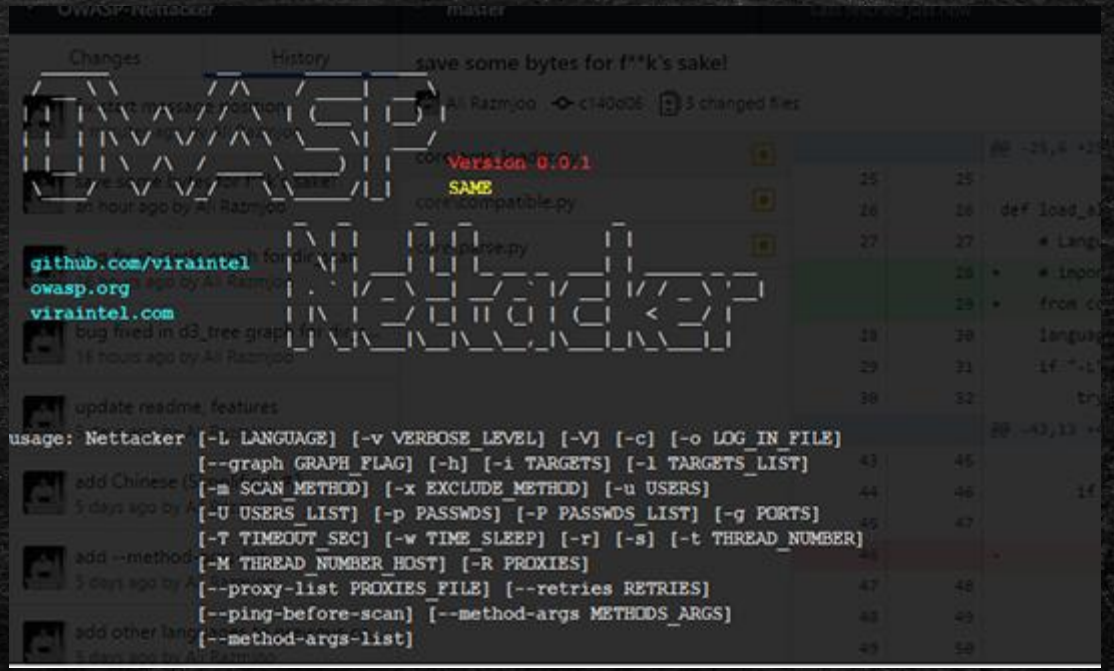
self.owasp_nettacker_features

- Smart and Automated
  - Won't ask any question while scanning
- HTML& TEXT Report
  - Graphs (Network Map)
  - Multi Language
- Attack IP Range
  - Use RIPE database
- Find Subdomains
  - Use sublister
- Customize attacks
  - Each module with different output (defaults are available)
  - Define timeout
  - Define thread number for a host
  - Define thread for scan hosts
  - Define retries
  - Define ping before scan
  - Define time to sleep (delay)
  - Define proxy
  - Define language
- Available Soon
  - Use tor
  - Local API
  - GUI, Web UI
  - Online API
  - Google Chrome and Mozilla Firefox plugin/addons
  - API Fuzzer
  - Documents with video tutorials

OFFSEC
www.offsec.ir

self.usage

Documents (Wiki Page): https://github.com/viraintel/OWASP-Nettacker/wiki



OFFSEC
www.offsec.ir

self.developers_status

OFFSEC
www.offsec.ir

self.how_to_develop

If anyone interested to contribute OWASP Nettacker Project, we gladly support and appreciate that!

Developers Wiki Page: https://github.com/viraintel/OWASP-Nettacker/wiki/Developers

OFFSEC
www.offsec.ir

QUESTION?

Contact

https://github.com/viraintel/OWASP-Nettacker/issues
ali.@offsec.ir
ali.Razmjoo@owasp.org

OFFSEC
www.offsec.ir

THE END – DROP THE MIC

OFFSEC

www.offsec.ir