Using OWASP Nettacker

For Recon and Vulnerability Scanning

Sam Stepanyan (@securestep9)

OWASP London Chapter Leader

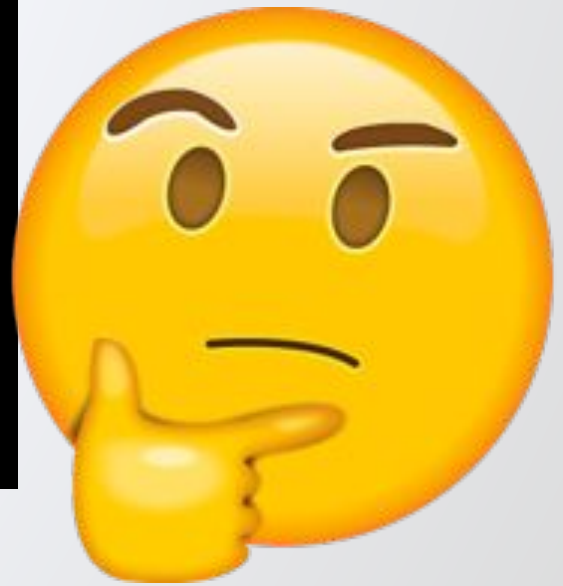
OWASP Nettacker Project Co-Leader

$ whoami - Sam Stepanyan

- OWASP London Chapter Leader
- Software development background
- **Application** Security Consultant, Financial Services, London
- I am a **Defender**
- Why am I presenting a talk about a tool
  which consists of words “**Net**work” and “At**tacker**”???

I FIRST TRIED NETTACKER IN 2017:

```
-m SCAN_METHOD, --method SCAN_METHOD
                    choose scan method ['ProFTPd_memory_leak_vuln',
                    'wordpress_dos_cve_2018_6389_vuln',
                    'XSS_protection_vuln', 'ProFTPd_cpu_consumption_vuln',
                    'x_powered_by_vuln', 'Bftpd_memory_leak_vuln',
                    'apache_struts_vuln', 'http_cors_vuln',
                    'Bftpd_remote_dos_vuln',
                    'ProFTPd_directory_traversal_vuln',
                    'Bftpd_parsecmd_overflow_vuln',
                    'ProFTPd_bypass_sqli_protection_vuln',
                    'ssl_certificate_expired_vuln',
                    'wp_xmlrpc_pingback_vuln', 'xdebug_rce_vuln',
                    'self_signed_certificate_vuln',
                    'weak_signature_algorithm_vuln',
                    'Bftpd_double_free_vuln',
                    'ProFTPd_exec_arbitary_vuln',
                    'options_method_enabled_vuln', 'server_version_vuln',
                    'ProFTPd_integer_overflow_vuln',
                    'ProFTPd_restriction_bypass_vuln',
                    'CCS_injection_vuln', 'wp_xmlrpc_bruteforce_vuln',
                    'ProFTPd_heap_overflow_vuln', 'heartbleed_vuln',
                    'content_type_options_vuln', 'clickjacking_vuln',
                    'content_security_policy_vuln', 'wappalyzer_scan',
                    'wp_user_enum_scan', 'port_scan', 'pma_scan',
                    'wp_timthumbs_scan', 'drupal_modules_scan',
                    'sender_policy_scan', 'wp_plugin_scan',
                    'viewdns_reverse_ip_lookup_scan', 'drupal_theme_scan',
                    'wordpress_version_scan', 'admin_scan',
```



black hat®
EUROPE 2018

Dr Greg Fragkos (@drgfragkos) and I were asked to demo OWASP Nettacker at BlackHat Europe2018 as Nettacker project leaders could not get to London in time.

We had to learn the tool overnight to be able to demo it at BlackHat Arsenal. Then this happened ==>

Crowds Watching OWASP Nettacker Demo at BlackHat Europe London, December 2018

Crowds Watching OWASP Nettacker Demo at BlackHat Europe London, December 2019

OWASP NETTACKER PROJECT

OWASP Nettacker is an open source software tool which assists with Penetration Testing by automating Information Gathering and Vulnerability Scanning tasks.
This software can be run on Windows/Linux/MacOS under Python

GOOGLE SUMMER OF CODE

Accepted as a Google Summer Of Code (**GSoC**) Project OWASP Nettacker was **Enhanced by GSoC Students**

- **Know a Student? Let them know about GSoC:**
- **Paid internship by Google**
- **Students apply to enhance/improve an Open Source project participating in GSoC**
- **Students work on an Open Source project during their summer break guided by mentors**
- **OWASP participates in GSoC every year**

“SWISS ARMY KNIFE”?

- a tool consisting of many tools
- not necessarily compatible with each other
- can they be all used together???

WHY OWASP NETTACKER?

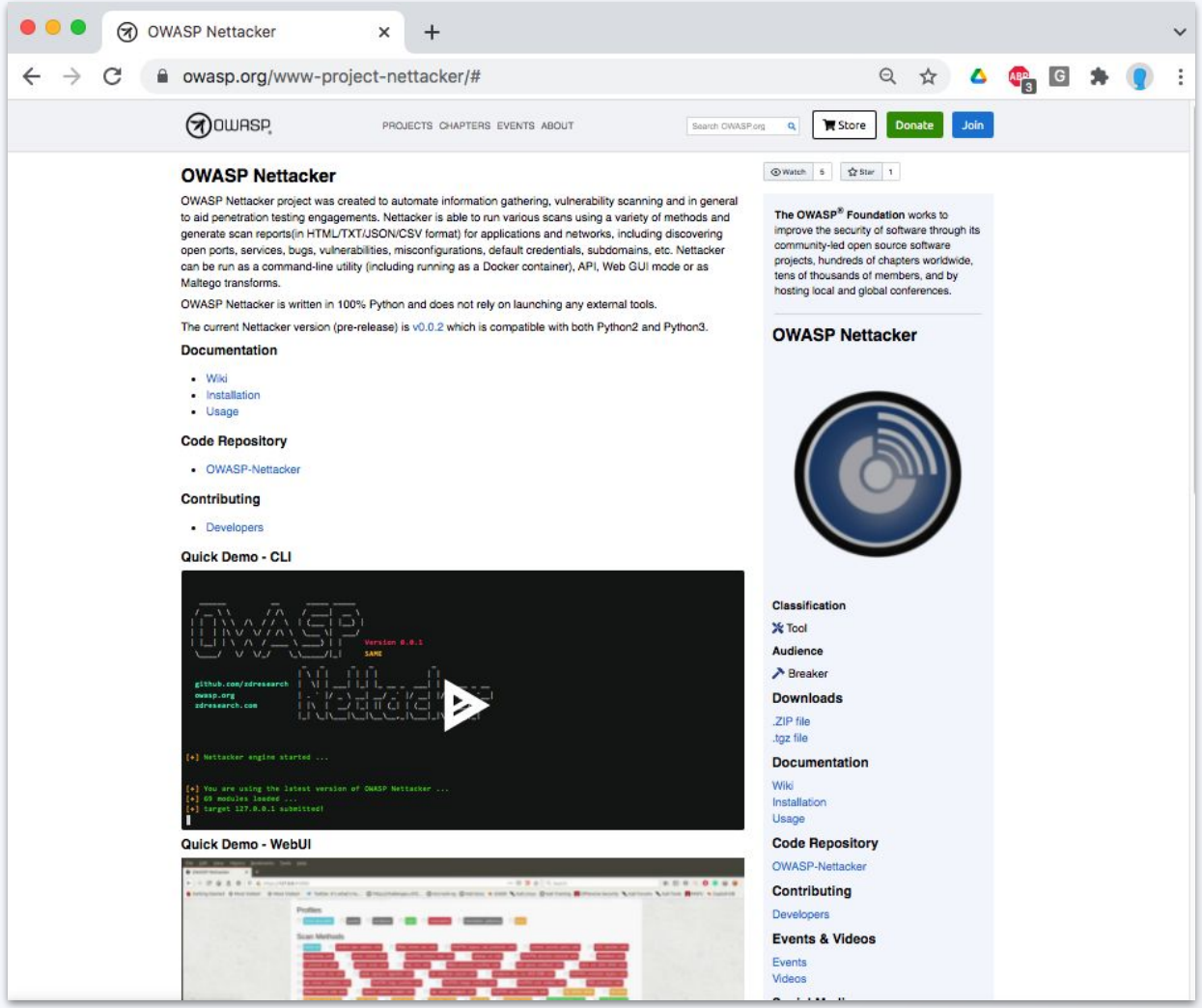
- a collection of tools
- modular structure
- easy to create own modules
- fast performance / multi-threading
- customizable profiles (bundle of modules focused on specific task)
- automate and run from command line

WHY OWASP NETTACKER?

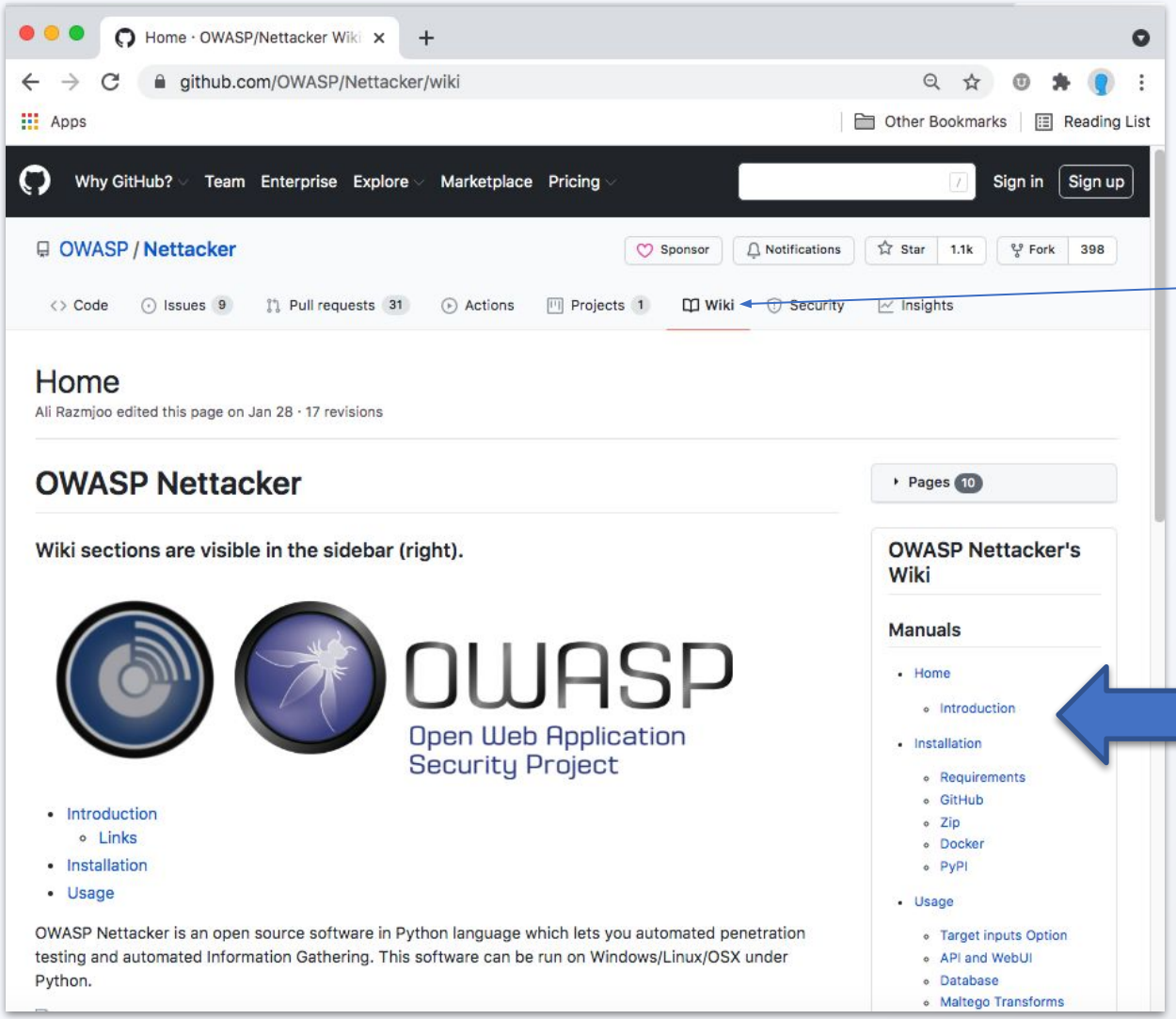
- it is not “officially released” yet
- not even in “beta” - v0.0.2/v0.0.3
- looking for more contributors

- …however it already has:
- CLI (command line interface)
- Web UI
- API
- Report generator
- Maltego transforms
- 70+ modules

https://owasp.org/www-project-nettacker



https://github.com/OWASP/Nettacker



Documentation Wiki

Installation Instructions

OTHER SCANNERS VS OWASP NETTACKER

BURP SUITE, OWASP ZAP	**Scan ONE website for MANY web app vulnerabilities (whatever the scanner is able to find). Crawl one website to discover all URLs, parameters…**
OWASP Nettacker	**Scans ONE or MANY (hundreds or thousands) IP addresses, networks or subdomains for OPEN PORTS and ONE or MORE SPECIFIC vulnerabilities, listed by the user (bundled in modules)**

INSTALLING OWASP NETTACKER

OWASP Nettacker is on GitHub

I will use **v0.0.2 today for my demo** as the latest v0.0.3 currently has a couple of issues (but it has **great new features** - we will cover this later!)

=> Install dependencies first! Read The Manual (Wiki)!

To install the latest version directly from GitHub using **git**, run these commands:

git clone https://github.com/OWASP/Nettacker

cd Nettacker

pip install -r requirements.txt

INSTALLING NETTACKER IN KALI LINUX

How To Install OWASP Nettacker on KALI Linux 2021.1

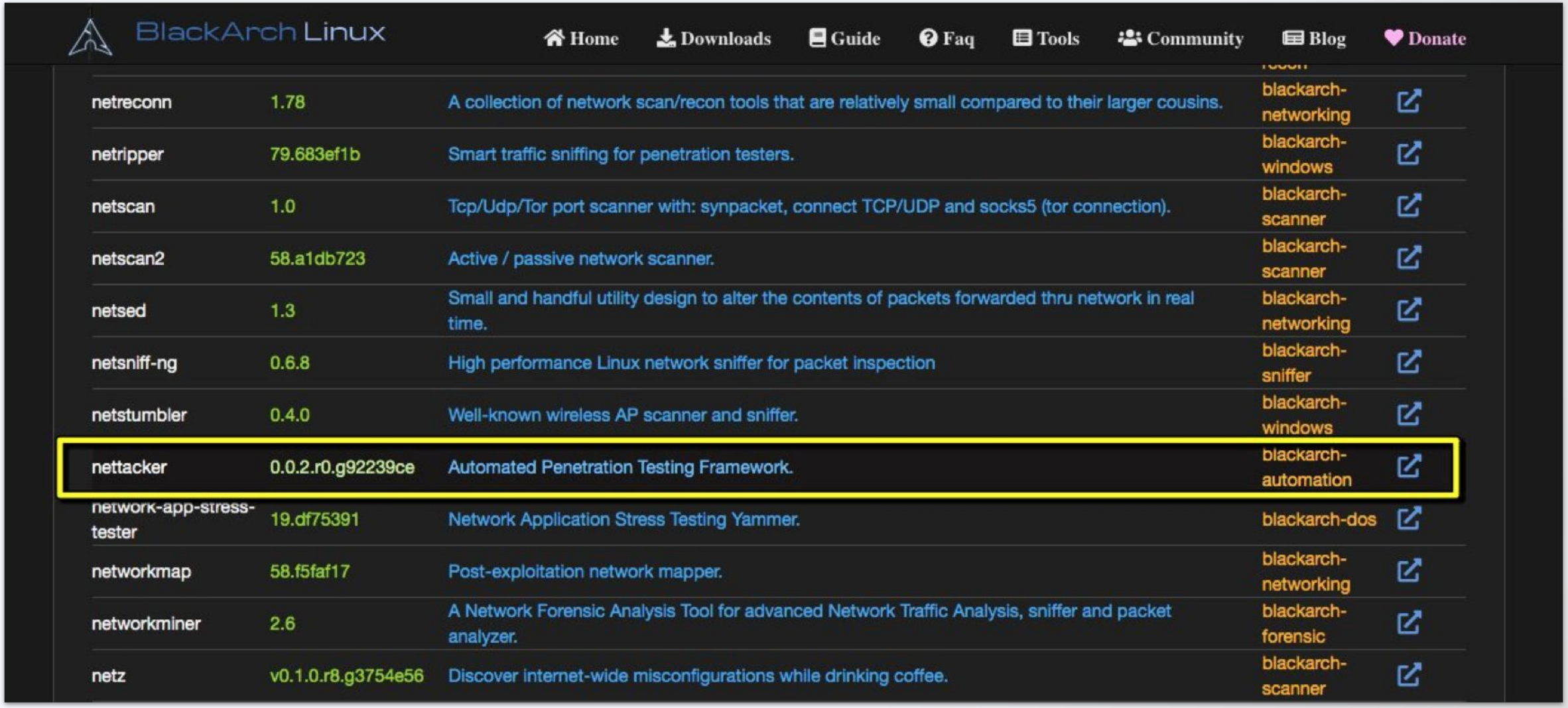
236 views • 3 months ago

securestep9

PIP for Python2 download command: wget https://bootstrap.pypa.io/pip/2.7/get-pip.py

NETTACKER INCLUDED IN BLACKARCH LINUX

NETTACKER INCLUDED IN BLACKARCH LINUX



BlackArch Linux | Home | Downloads | Guide | Faq | Tools | Community | Blog | Donate

netreconn	1.78	A collection of network scan/recon tools that are relatively small compared to their larger cousins.	blackarch-networking
netripper	79.683ef1b	Smart traffic sniffing for penetration testers.	blackarch-windows
netscan	1.0	Tcp/Udp/Tor port scanner with: synpacket, connect TCP/UDP and socks5 (tor connection).	blackarch-scanner
netscan2	58.a1db723	Active / passive network scanner.	blackarch-scanner
netsed	1.3	Small and handful utility design to alter the contents of packets forwarded thru network in real time.	blackarch-networking
netsniff-ng	0.6.8	High performance Linux network sniffer for packet inspection	blackarch-sniffer
netstumbler	0.4.0	Well-known wireless AP scanner and sniffer.	blackarch-windows
nettacker	0.0.2.r0.g92239ce	Automated Penetration Testing Framework.	blackarch-automation
network-app-stress-tester	19.df75391	Network Application Stress Testing Yammer.	blackarch-dos
networkmap	58.f5faf17	Post-exploitation network mapper.	blackarch-networking
networkminer	2.6	A Network Forensic Analysis Tool for advanced Network Traffic Analysis, sniffer and packet analyzer.	blackarch-forensic
netz	v0.1.0.r8.g3754e56	Discover internet-wide misconfigurations while drinking coffee.	blackarch-scanner

NETTACKER IN DOCKER

No Official OWASP image yet (coming soon!)

——— simply Compose your own =>

```
git clone https://github.com/OWASP/Nettacker
cd Nettacker
docker-compose up
```

RESPONSIBLE USE WARNING

You shall not misuse this tool nor any other security tool for unauthorized access

Performing security scans without permission from the owner of the computer system is illegal.

NETTACKER MODULE TYPES

- 'scan' - e.g. port_scan
- 'vuln' - e.g. apache_struts_vuln
- 'brute'- e.g. ssh_brute

NETTACKER SCAN MODULES

- `admin_scan'*
- `cms_detection_scan'*
- `dir_scan'*
- `drupal_version_scan'
- 'drupal_modules_scan'
- 'drupal_theme_scan'
- `icmp_scan' *
- `joomla_template_scan'
- 'joomla_user_enum_scan'
- 'joomla_version_scan'
- `pma_scan'*
- `port_scan' *
- 'sender_policy_scan'
- `subdomain_scan' *
- 'viewdns_reverse_ip_lookup_scan'
- `wappalyzer_scan'*
- `wordpress_version_scan' *
- 'wp_plugin_scan'
- 'wp_theme_scan'
- 'wp_timthumbs_scan'
- 'wp_user_enum_scan'

NETTACKER VULN MODULES

- 'apache_struts_vuln'
- 'Bftpd_double_free_vuln'
- 'Bftpd_memory_leak_vuln'
- 'Bftpd_parsecmd_overflow_vuln'
- 'Bftpd_remote_dos_vuln'
- 'CCS_injection_vuln'
- 'clickjacking_vuln'
- 'content_security_policy_vuln'
- 'content_type_options_vuln'
- 'citrix_cve_2019_19781_vuln'*
- 'heartbleed_vuln'
- 'http_cors_vuln'
- msexchange_cve_2021_26855_vuln *
- 'options_method_enabled_vuln'
- 'ProFTPd_bypass_sqli_protection_vuln'
- 'ProFTPd_cpu_consumption_vuln'
- 'ProFTPd_directory_traversal_vuln'
- 'ProFTPd_exec_arbitary_vuln'
- 'ProFTPd_heap_overflow_vuln'
- 'ProFTPd_integer_overflow_vuln'
- 'ProFTPd_memory_leak_vuln'
- 'ProFTPd_restriction_bypass_vuln'
- 'self_signed_certificate_vuln'
- 'server_version_vuln'*
- 'ssl_certificate_expired_vuln' *
- 'weak_signature_algorithm_vuln'
- 'wordpress_dos_cve_2018_6389_vuln'
- 'wp_xmlrpc_bruteforce_vuln'
- 'wp_xmlrpc_pingback_vuln'
- 'XSS_protection_vuln'
- 'x_powered_by_vuln' *
- 'xdebug_rce_vuln'

NETTACKER BRUTE MODULES

- 'ftp_brute'
- 'http_basic_auth_brute'
- 'http_form_brute'
- 'http_ntlm_brute'
- 'smtp_brute'
- 'ssh_brute'
- 'telnet_brute'
- 'wp_xmlrpc_brute'

IOT SCAN (@IOTSCAN)

- original name for Nettacker (and still its Twitter handle)
- scan your network for IoT devices
- scan IoT device for open ports
- brute force scan for default credentials (admin/admin)

NETTACKER PORT SCAN MODULE

- port scanner **(port_scan)**
- easier to use & faster (compared with ***nmap***)
- add **-t <threads> -M <threads/host>**
- uses Python multi-threading
- add **-g to list specific ports to scan**
  e.g. -g 80,443

RUNNING NETTACKER 101

```
nettacker -i <target> -m <module>

nettacker -i 192.168.1.149 -m port_scan

nettacker -i 192.168.1.0/24 -m port_scan
```

NETTACKER TARGETS

```
-i (ip|range|cidr/bits|domain|url)
```

- 192.168.1.1
- 192.168.1.1-192.168.255.255
- 192.168.1.0/24
- owasp.org
- http://owasp.org
- https://owasp.org

LIST OF TARGETS FROM FILE

```
nettacker -l <list_of_targets> -m <module>
```

<list_of_targets> - a text file containing the list of targets

CHAINING MODULES

```
nettacker -i <target> -m <method1>,<method2>…
nettacker -i 192.160.1.149 -m port_scan,pma_scan
nettacker -i owasp.org
-m port_scan, server_version_vuln -g 80,443
```

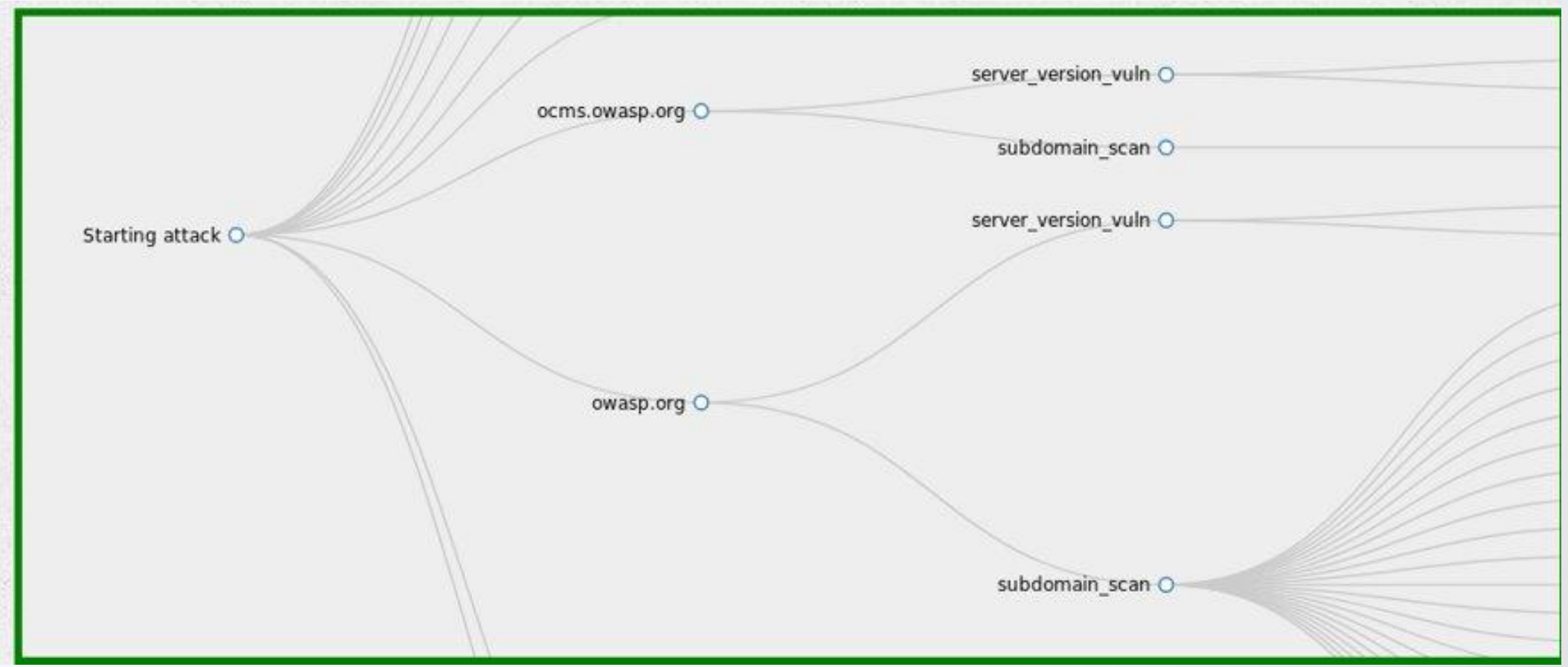
NETTACKER PROFILES

- ‘info’
- ‘scan’
- ‘brute’
- ‘vuln’
- ‘wp’
- ‘joomla’
- 'all'

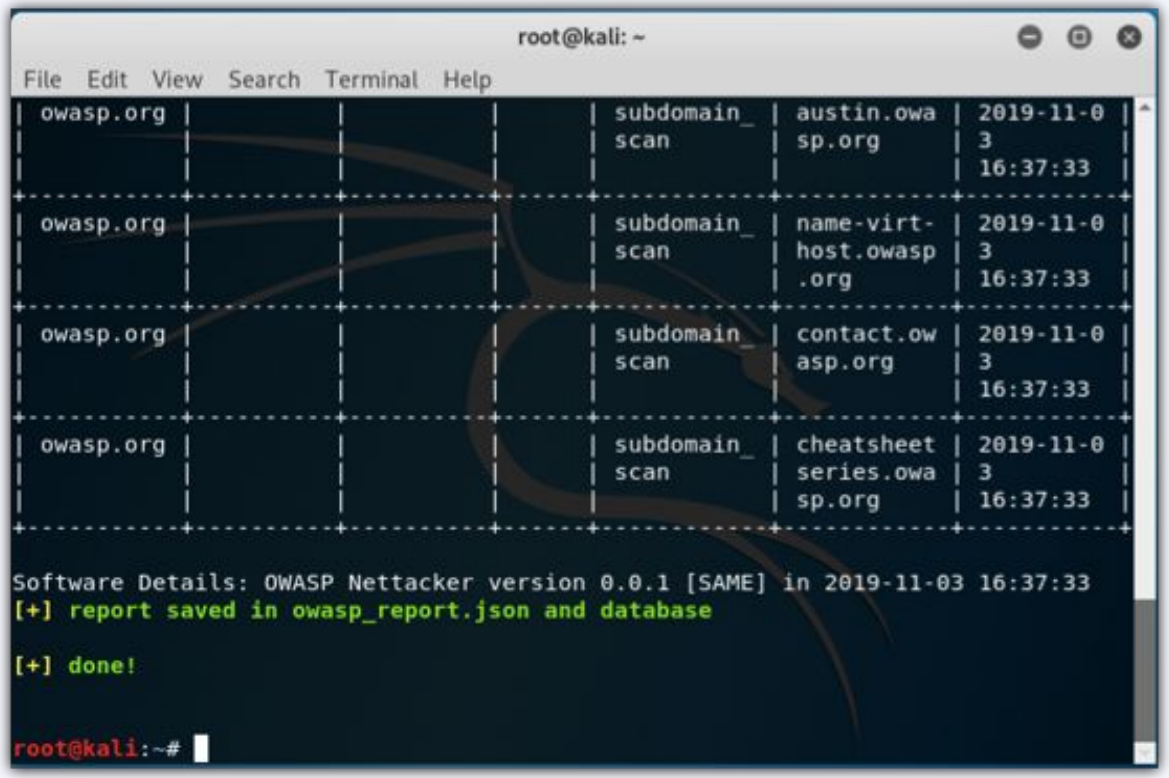
```
nettacker -i <target> —-profile info
```

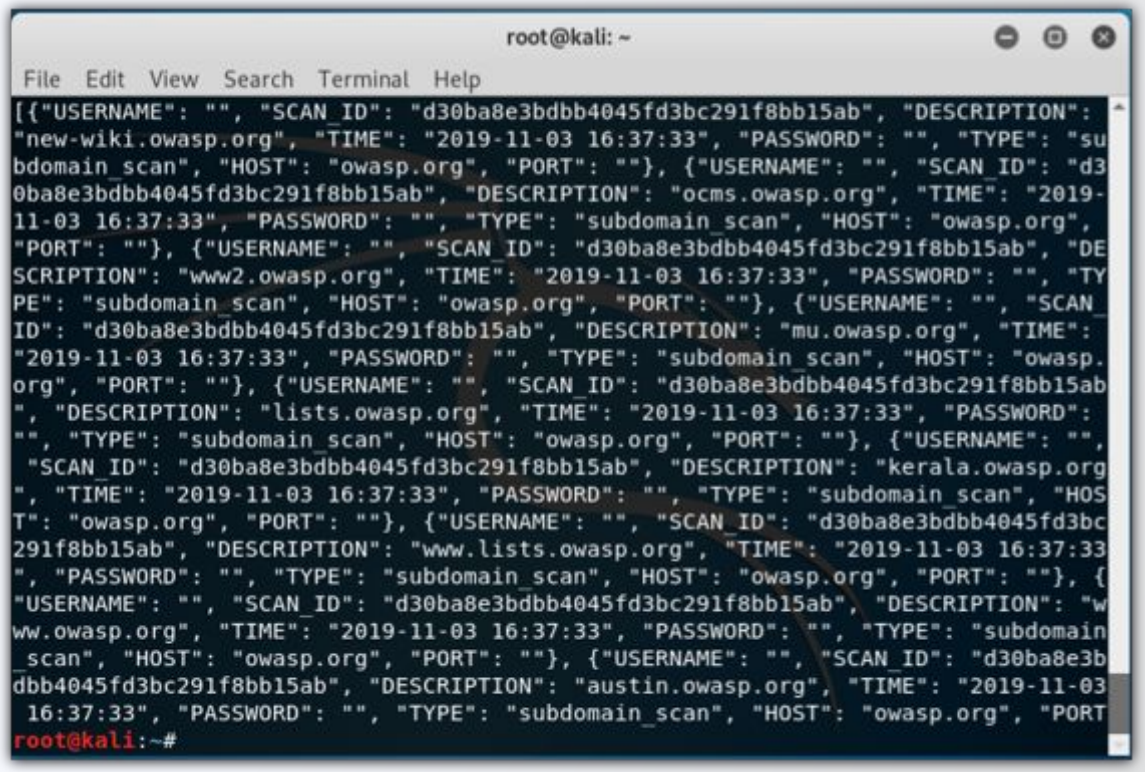
LIVE DEMO – IN KALI LINUX

NETTACKER GRAPHS

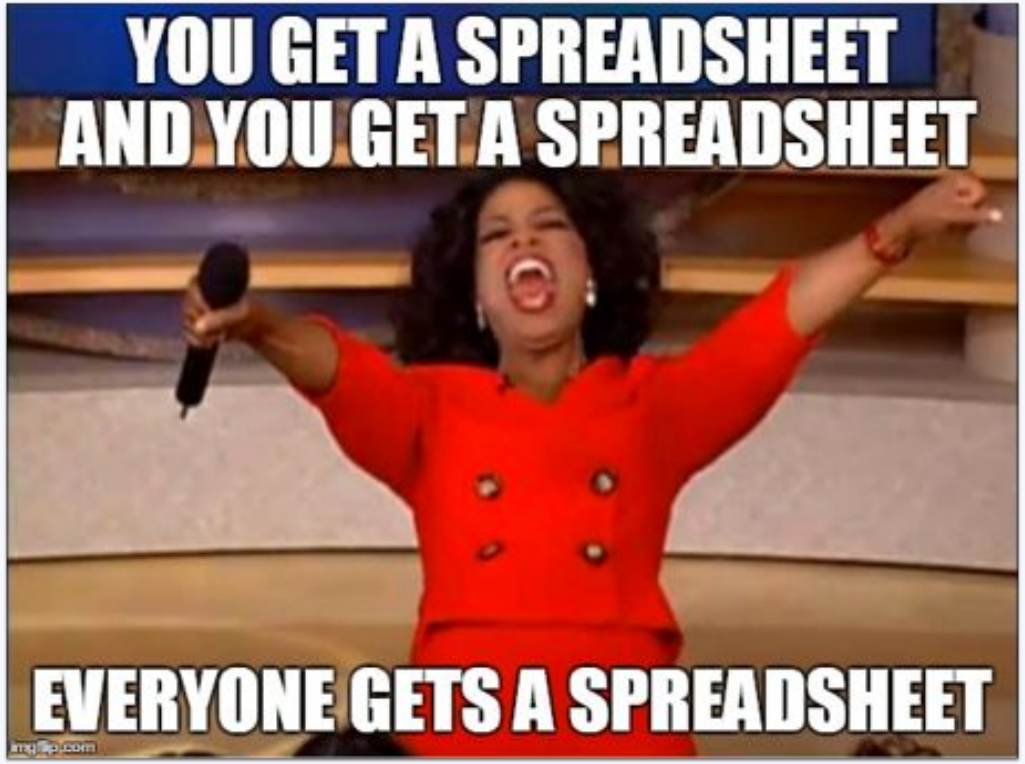


NETTACKER REPORTS IN HTML, JSON, CSV





REPORT IN A SPREADSHEET- A MANAGER'S DREAM!



Book1 - Microsoft Excel

Home | Insert | Page Layout | Formulas | Data | Review | View

From Access | From Web | From Text | From Other Sources | Existing Connections | Refresh All | Connections | Properties | Edit Links | Sort | Filter | Clear | Reapply | Advanced | Text to Columns | Remove Duplicates | Data Validation | Consolidate | What-If Analysis | Group | Ungroup | Subtotal

Get External Data | Connections | Sort & Filter | Data Tools | Outline

A2 | ocms.owasp.org

	A	B	C	D	E	F	G
1	HOST	TYPE	PORT	DESCRIPTION	USERNAM	PASSWOI	TIME
2	ocms.owasp.org	server_version_vuln	80	AtlassianProxy/1.15.8.1			##########
3	ocms.owasp.org	server_version_vuln	443	AtlassianProxy/1.15.8.1			##########
4	www2.owasp.org	server_version_vuln	443	cloudflare			##########
5	www2.owasp.org	server_version_vuln	80	cloudflare			##########
6	www.owasp.org	server_version_vuln	80	cloudflare			##########
7	www.owasp.org	server_version_vuln	443	cloudflare			##########
8	austin.owasp.org	server_version_vuln	443	cloudflare			##########
9	austin.owasp.org	server_version_vuln	80	cloudflare			##########
10	secureflag.owasp.org	server_version_vuln	443	nginx			##########
11	secureflag.owasp.org	server_version_vuln	80	nginx			##########
12	kerala.owasp.org	server_version_vuln	443	cloudflare			##########
13	kerala.owasp.org	server_version_vuln	80	cloudflare			##########
14	lists.owasp.org	server_version_vuln	443	cloudflare			##########
15	lists.owasp.org	server_version_vuln	80	cloudflare			##########
16	name-virt-host.owasp.org	server_version_vuln	80	cloudflare			##########
17	name-virt-host.owasp.org	server_version_vuln	443	cloudflare			##########
18	cheatsheetseries.owasp.org	server_version_vuln	443	cloudflare			##########

Sheet1 | Sheet2 | Sheet3

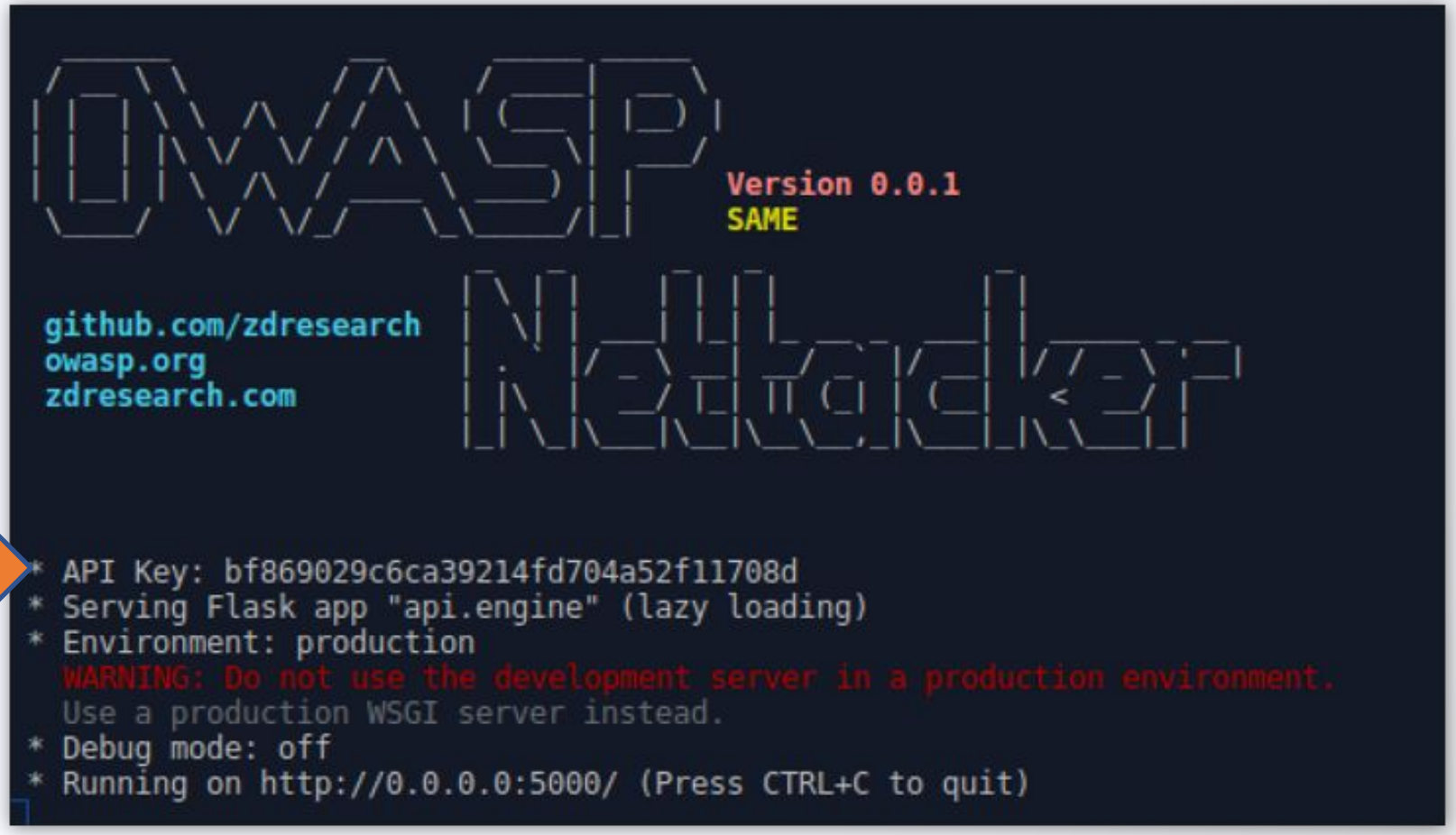
Ready | 100%

OWASP A0 - "ASSET INVENTORY"

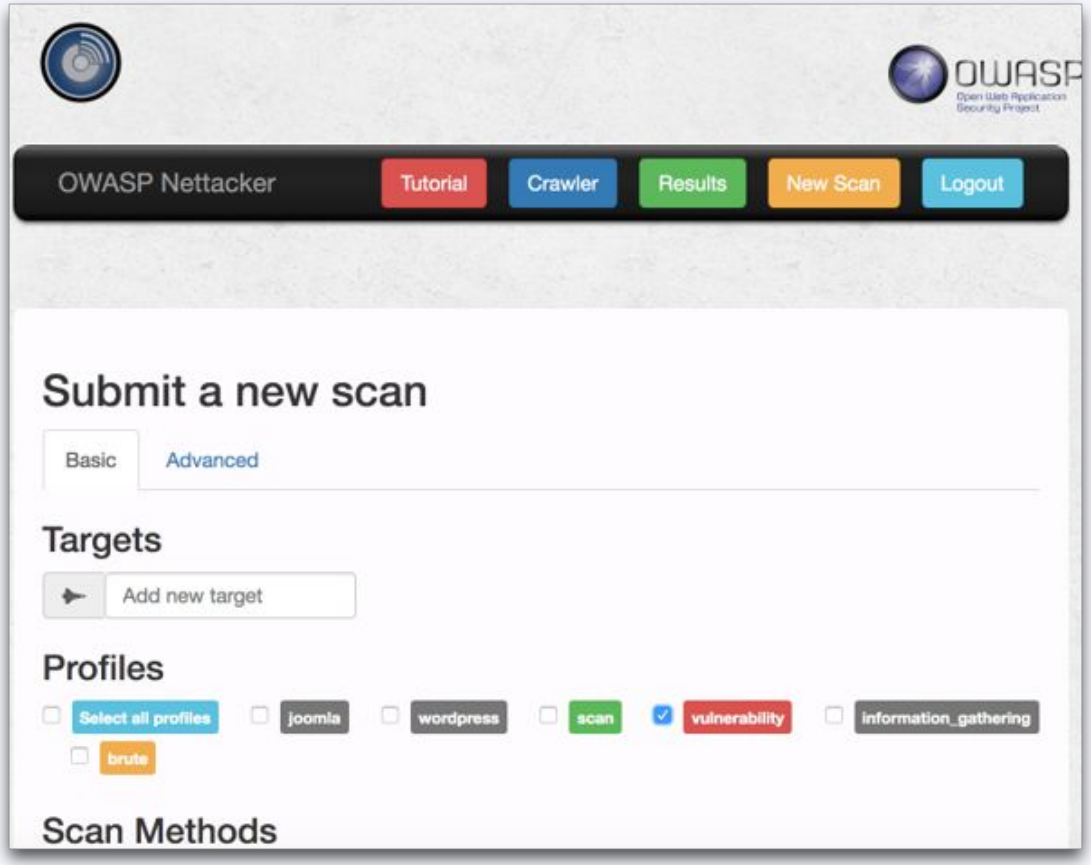
"if you don't know what you OWN you cannot possibly secure it"

OWASP NETTACKER API & WEB UI

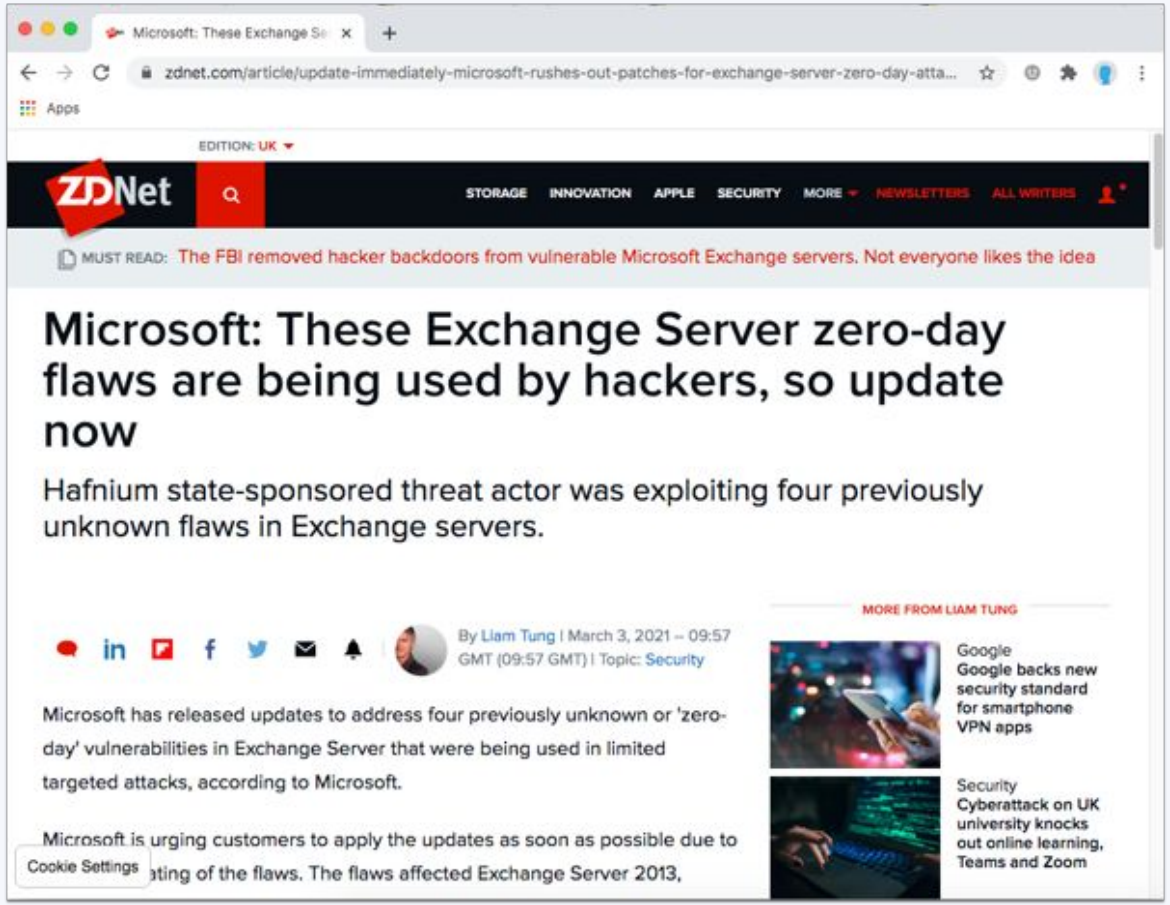
Copy the API KEY - You Need It To Login To WEB UI

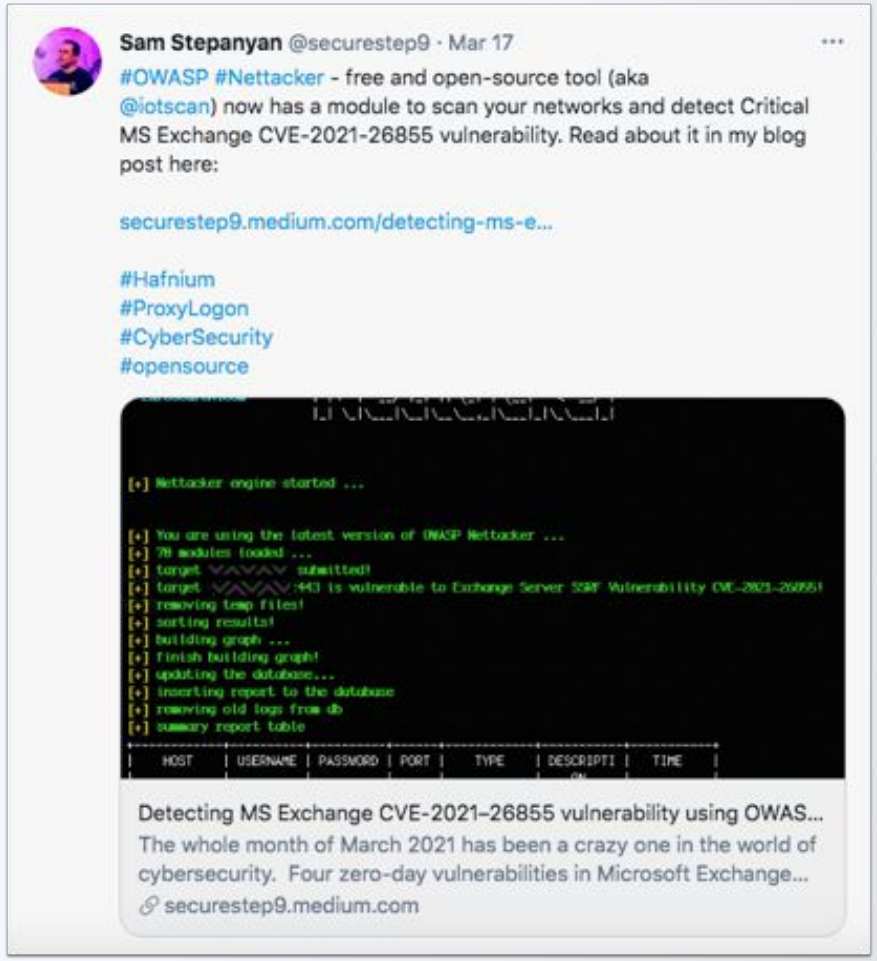


OWASP NETTACKER API & WEB UI



MS EXCHANGE SERVER CVE-2021-26855





SCANNING FOR CVE-2021-26855 VULNERABILITY


```
nettacker -i 192.168.1.1/24 –m
msexchange_cve_2021_26855_vuln
```

SOME NETTACKER USE CASES

- asset discovery
- scan network for open ports
- scan network for new hosts/web servers/ssh servers etc
- scan network for default credentials (admin/admin)?
- scan network for a specific vulnerability (e.g. MSExchange CVE)
- discover & scan subdomains & open ports on them
- discover expired SSL certs in your ip ranges
- find subdomains hosting vulnerable versions of WordPress, Drupal and Joomla
- search scanned assets & vulnerabilities in a built-in database
- download scan results as CSV (or JSON/XML)

TOP 10 MOST STARRED OWASP REPOS

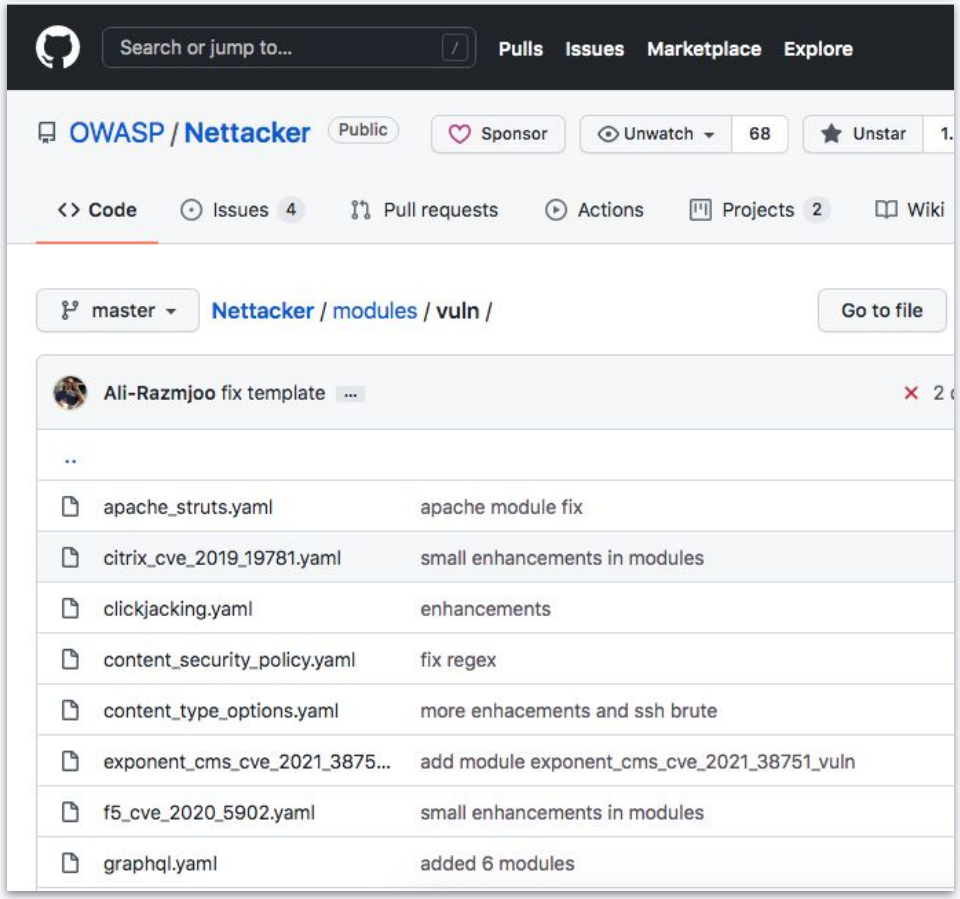
	Repo Name	GitHub Stars
1	CheatSheetSeries	20,162
2	OWASP-MSTG	8,745
3	Amass	6,746
4	Go-SCP	4,116
5	WSTG	4,116
6	Top10	2,765
7	DevGuide	1,885
8	**Nettacker**	**1,652**
9	ASVS	1,626
10	NodeGoat	1,552

https://github.com/OWASP?sort=stargazers

Users on the GitHub are able to "star" other people's repositories, thereby saving them in their list of Starred Repos. Some people use "stars" to indicate that they like a project, other people use them as bookmarks so they can follow what's going on with the repo later.

GitHub Stars are an easy metric to keep track of, and can be used to measure how popular an open source project is.

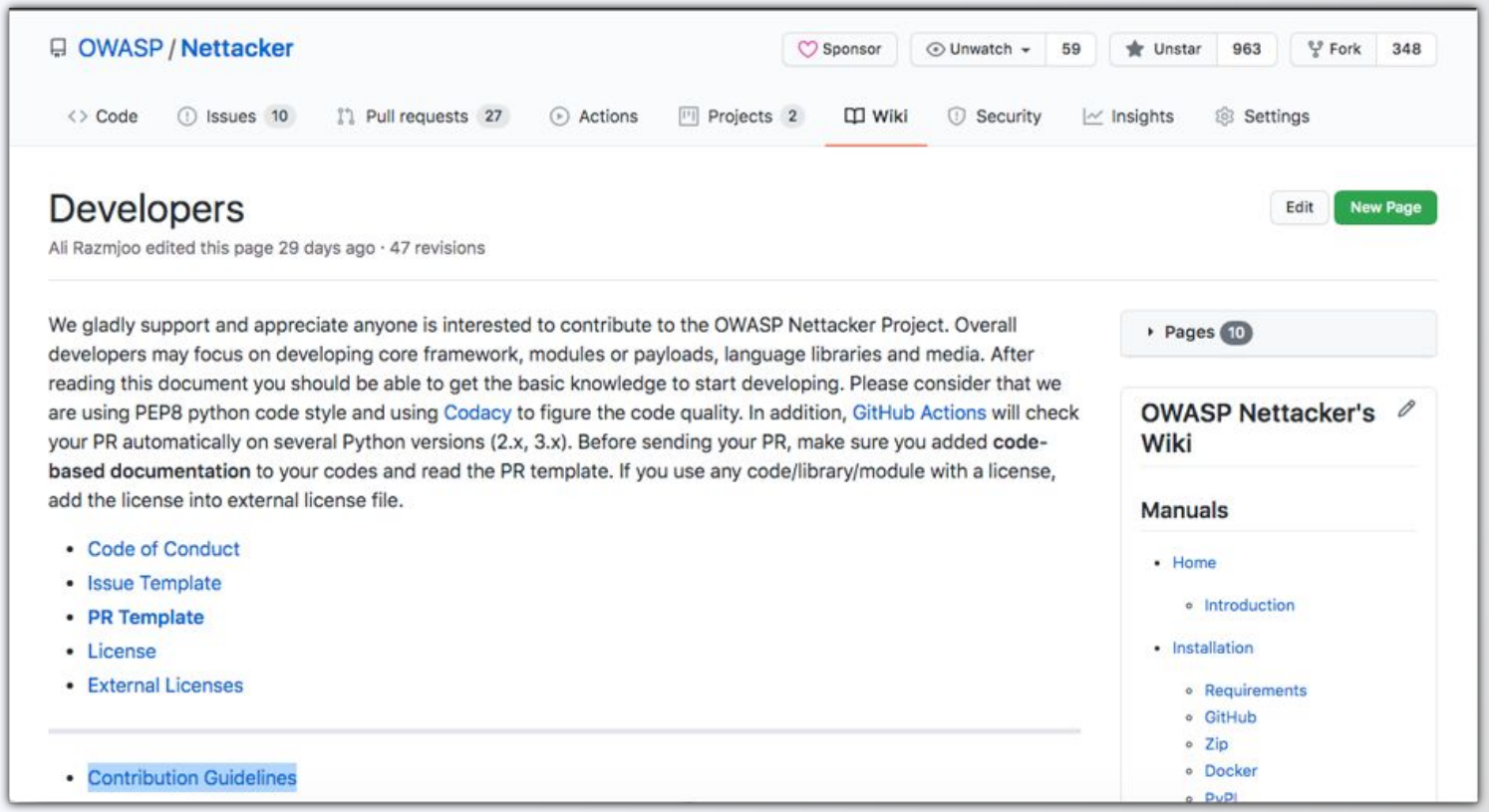
OWASP NETTACKER v0.0.3
YAML-BASED MODULES




```yaml
payloads:
  - library: http
    verify: false
    timeout: 10
    cert: ""
    stream: false
    proxies: ""
    steps:
      - method: get
        headers:
          User-Agent: "{user_agent}"
        url:
          nettacker_fuzzer:
            input_format: "{{schema}}://{target}:{{ports}}/{{paths}}"
            prefix: ""
            suffix: ""
            interceptors:
            data:
              paths:
                - "tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=/etc/passwd"
                - "tmui/login.jsp/..;/tmui/locallb/workspace/directoryList.jsp?directoryPath=/etc/"
                - "tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=id"
              schema:
                - "http"
                - "https"
              ports:
                - 80
                - 443
        response:
          condition_type: and
          conditions:
            status_code:
              regex: "200"
              reverse: false
            content:
              regex: root:.*:0:0:|/etc/passwd|/etc/shadow|uid\\=*.+gid
              reverse: false
```

HOW TO CONTRIBUTE

- Developer Wiki:
  https://github.com/OWASP/Nettacker/wiki/Developers
- **Read & follow the Contributor guidelines**
- **Help with translations, documentation**



Nettacker: Attack Your Network - Before The Real Attackers Do!

Thank You! Q&A ?

sam.stepanyan @ owasp.org

securestep9