Yuki Chan Tool

Information Security Inc.

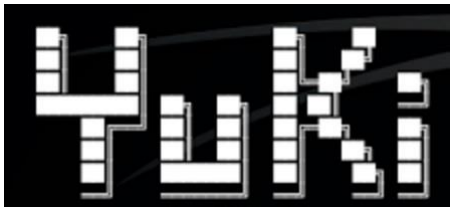
iSEC
information security inc.

Contents

- About Yuki chan
- Features
- Modules included
- Requirements
- Demo configuration
- Installing the tool
- Using the tool
- References

About Yuki chan

- Yuki Chan is an Automated Penetration Testing tool
- The tool will audit all standard security test methods



Features

- Automated
- Intel-Gathering
- Vulnerability Analysis
- Security Auditing
- OSINT
- Tracking
- System Enumeration
- Fuzzing
- CMS Auditing
- SSL Security Auditing

Modules included

- Whois domain analyzer
- Nslookup
- Nmap
- TheHarvester
- Metagoofil
- DNSRecon
- Sublist3r
- Wafw00f
- WAFNinja
- XSS Scanner
- WhatWeb
- Spaghetti
- WPscan

Modules included

- WPscanner
- WPSeku
- Droopescan (CMS Vulnerability Scanner Wordpress, Joomla, Silverstripe, Drupal, And Moodle)
- SSLScan
- SSLyze
- A2SV
- Dirsearch

Requirements

- sslyze
- wafw00f
- droopescan
- argparse
- netaddr
- dnspython
- requests
- beautifulsoup4
- prettytable
- progressbar
- configparser
- parse

Demo configuration

- Kali Linux 2017 64 bit (https://www.kali.org/downloads/)
- http://www.kitploit.com/2017/04/kali-linux-20171-release.html

Installing the tool

- Clone it

```
root@kali2017:~# git clone https://github.com/Yukinoshita47/Yuki-Chan-The-Auto-Pentest.git
Cloning into 'Yuki-Chan-The-Auto-Pentest'...
remote: Counting objects: 3100, done.
remote: Compressing objects: 100% (2659/2659), done.
remote: Total 3100 (delta 405), reused 3098 (delta 403), pack-reused 0
Receiving objects: 100% (3100/3100), 11.50 MiB | 3.67 MiB/s, done.
Resolving deltas: 100% (405/405), done.
```

- Change filemode

```
root@kali2017:~/Yuki-Chan-The-Auto-Pentest# pwd
/root/Yuki-Chan-The-Auto-Pentest
root@kali2017:~/Yuki-Chan-The-Auto-Pentest# chmod 775 wafninja joomscan install-perl-module.sh
root@kali2017:~/Yuki-Chan-The-Auto-Pentest# stat wafninja joomscan install-perl-module.sh
```

Installing the tool

- Install requirements

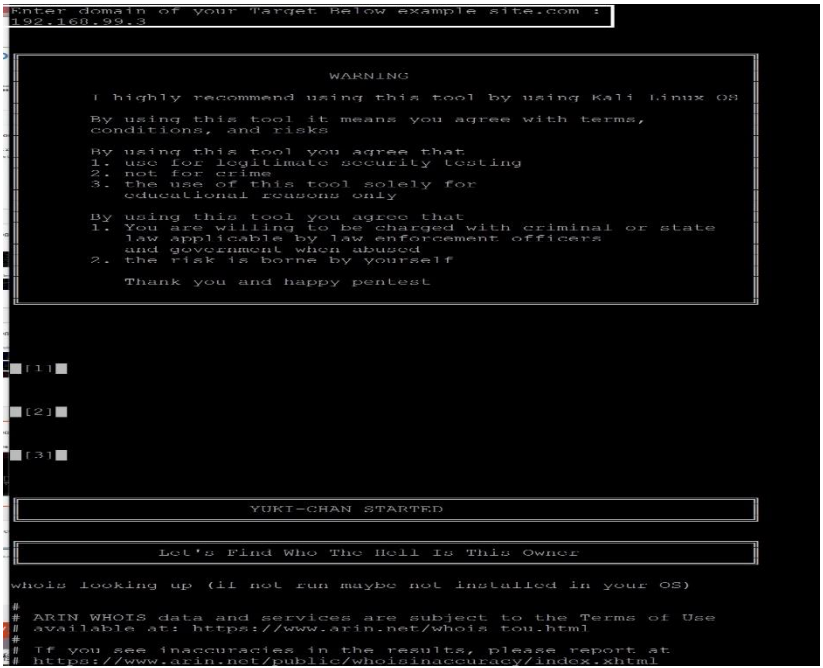
```
root@kali2017:~/Yuki-Chan-The-Auto-Pentest# apt-get install python-pip python-dev libffi-dev libssl-dev libxml2-dev libxslt1-dev  zlib1g-dev
Reading package lists... Done
root@kali2017:~/Yuki-Chan-The-Auto-Pentest# pip install -r requirements.txt
Collecting sslyze (from -r requirements.txt (line 1))
Requirement already satisfied: wafw00f in /usr/lib/python2.7/dist-packages (from -r requirements.txt (line 2))
root@kali2017:~/Yuki-Chan-The-Auto-Pentest# ./install-perl-module.sh
```

Installing the tool

- Starting the tool

Using the tool

- Whois lookup



Using the tool

- Running nmap

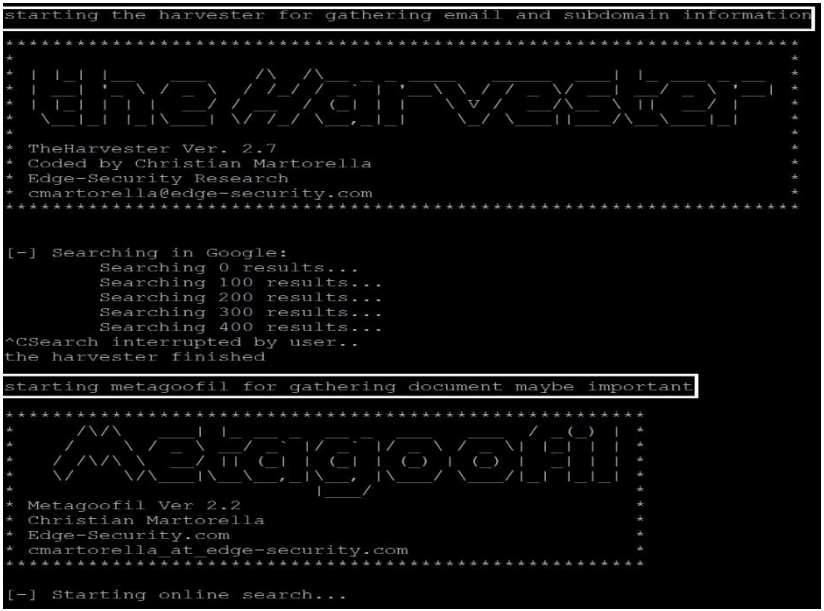
```
scanning with nmap (if not run maybe not installed in your OS)

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-19 05:02 EDT
Initiating Ping Scan at 05:02
Scanning 192.168.99.3 [4 ports]
Completed Ping Scan at 05:02, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:02
Completed Parallel DNS resolution of 1 host. at 05:02, 0.01s elapsed
Initiating SYN Stealth Scan at 05:02
Scanning 192.168.99.3 [1000 ports]
Completed SYN Stealth Scan at 05:02, 9.80s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.99.3
adjust_timeouts2: packet supposedly had rtt of -98368 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -98368 microseconds.  Ignoring time.
Retrying OS detection (try #2) against 192.168.99.3
Nmap scan report for 192.168.99.3
Host is up (0.0051s latency).
Not shown: 998 filtered ports
PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Cisco Aironet 1250 WAP (IOS 12.4) or IOS XE (94%), Cisco C7200 router (IOS 15) (94%), Cisco 827H ADSL router (IOS
12.2) (93%), Cisco 870 router or 2960 switch (IOS 12.2 - 12.4) (93%), Cisco 2960 switch (IOS 12.2) (91%), Cisco 1700-series router (91%),
 Cisco 2950 switch (IOS 12.1) (91%), Cisco Catalyst Express 500 switch (IOS 12.2) (91%), OpenBSD 3.8 - 4.6 (91%), OpenBSD 5.5 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
           Raw packets sent: 2042 (92.738KB) | Rcvd: 25 (2.266KB)
scanning with nmap finished
```

Using the tool

- Running TheHarvester and Metagoofil



References

- Kitploit
http://www.kitploit.com/2017/09/yuki-chan-automate-pentest-tool.html

- Kali Linux
https://www.kali.org/downloads/