Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

V3n0M Scanner

Nesa aula, vamos mostrar o programa V3n0M. Ele é um scanner de código aberto e livre. Desenvolvido a partir do scanner baltazar, foram adaptados diversos novos recursos que melhoram a funcionalidade e usabilidade. É principalmente um software experimental.

V3n0M Scanner

Este programa é para encontrar diversas vulnerabilidades. Ele limpa a web usando *dorks* e organiza as URLs encontradas.

V3n0M Scanner

Ele é muito útil para executar em:

- Cloudflare Resolver [Cloudbuster]
- LFI-> RCE e XSS Scanner [LFI-> RCE & XSS]
- SQL Injection Vuln Scanner [SQLi]
- Listas grandes de D0rk
- Crawler FTP
- DNS BruteForcer
- Python3.5 Scanner baseada em *async*

V3n0M Scanner

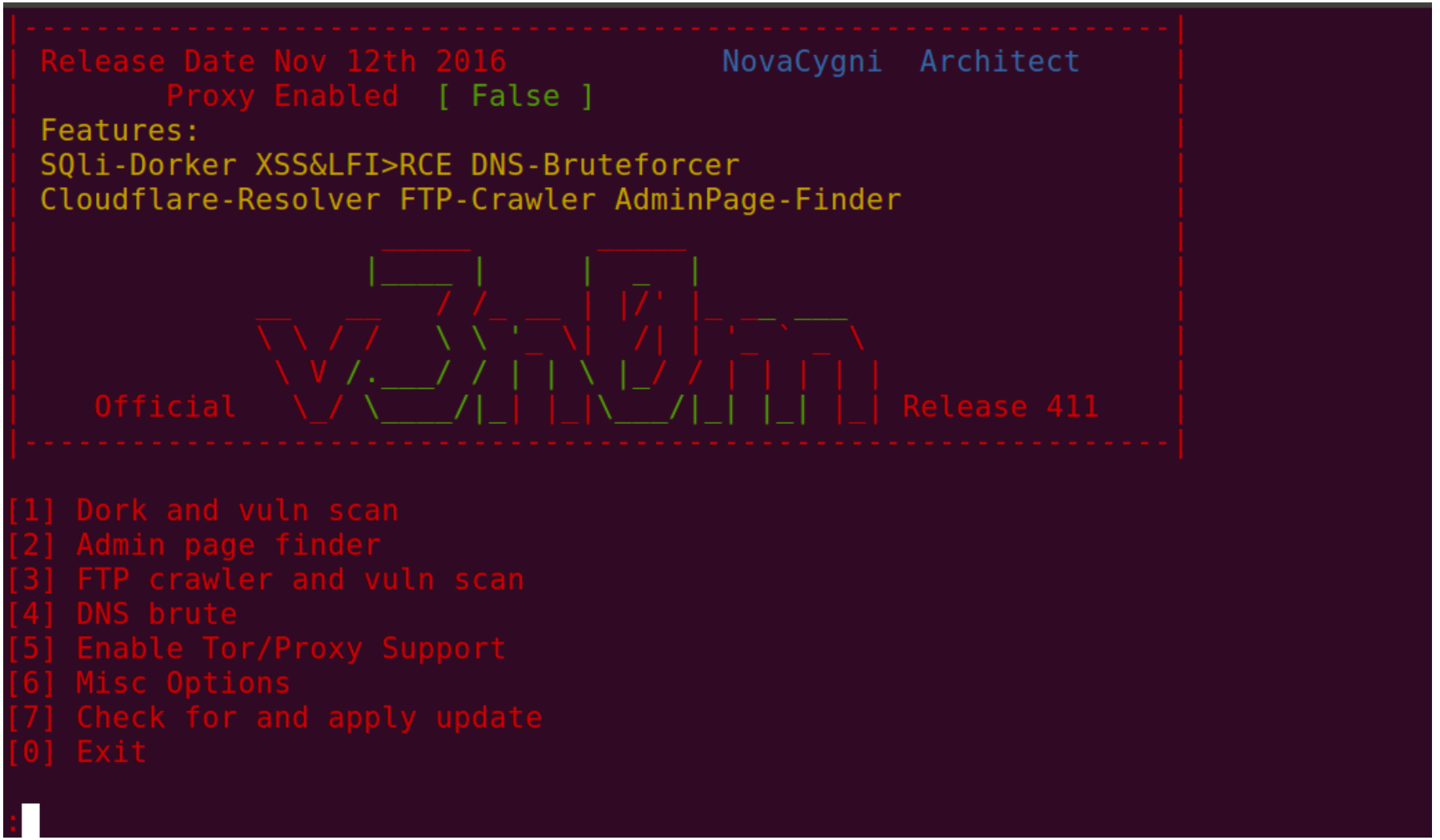
Para você fazer a instalação segue esses passos:

```
# apt-get install python3-pip

# pip3 install setuptools

# git clone https://github.com/v3n0m-Scanner/V3n0M-

Scanner.git

# cd V3n0M-Scanner/

# python3 setup.py install --user
```

Depois, é só executar o arquivo:

```
# cd src/

# python3 v3n0m.py
```

V3n0M Scanner



Agora, vamos achar sites reais na internet que estejam vulneravéis. Só que para isso, vamos criar o nosso próprio proxy.

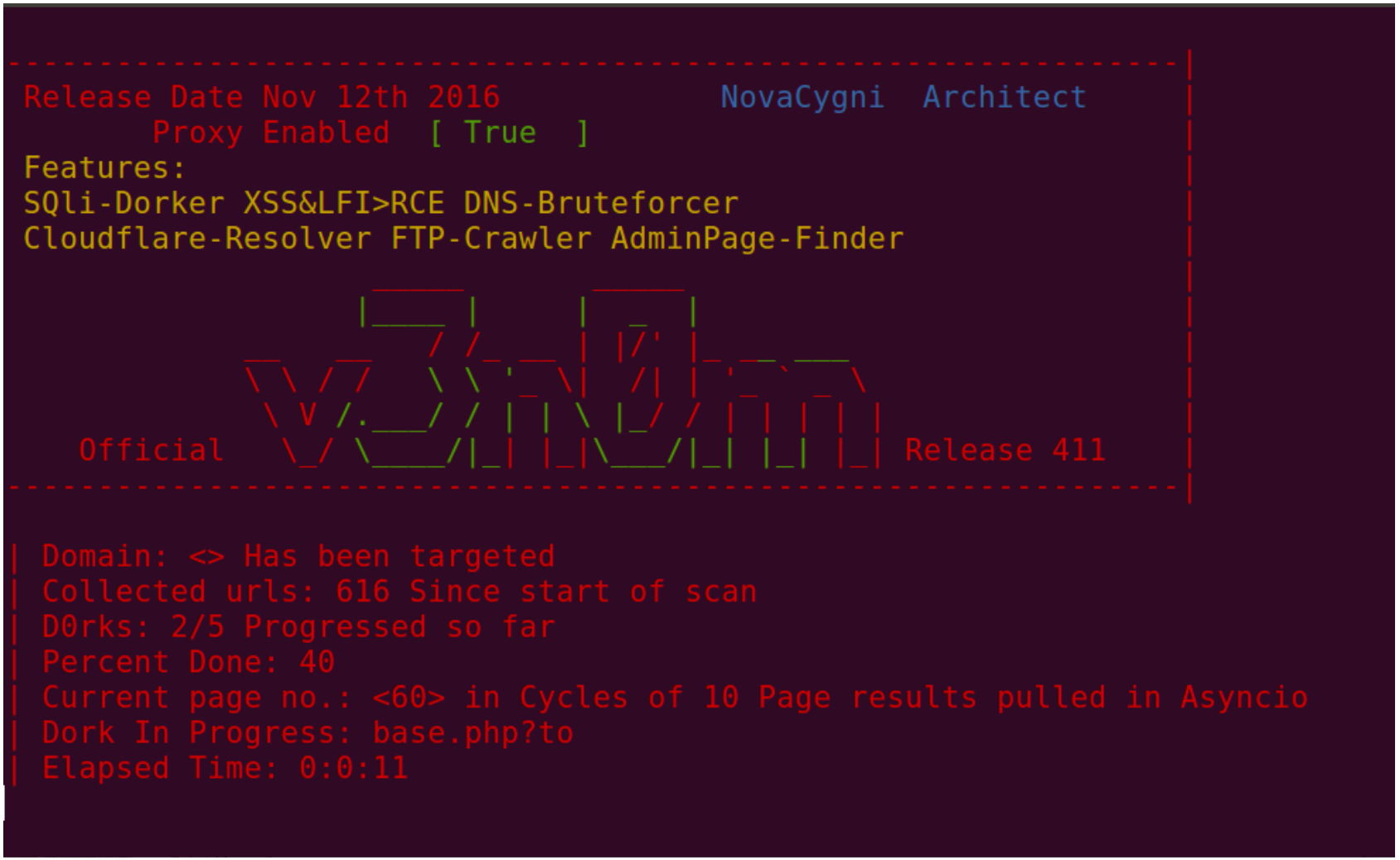
- [5] Enable Tor/Proxy Support > Enter
- Requires Username/Password? > False
- Please select Proxy Type > socks4
- Please enter Proxy IP address > 127.0.0.1
- Please enter Proxy Port > 9050
- Proxy Account Username e Proxy Account Password : <vazio>

V3n0M Scanner

Agora, vamos escanear os Dorks!

- [1] Dork and vuln scan
- Choose your target(domain) ie .com : <enter>
- Choose the number of random dorks : 5
- Enter no. of threads, Between 50 and 500: 500
- Between 20 and 100: 100

V3n0M Scanner



V3n0M Scanner

Depois de faze o escaneamento, ele posta os resultados e diz qual Dork ele encontrou.

```
 | Collected urls: 2429 Since start of scan
 | D0rks: 5/5 Progressed so far
 | Percent Done: 100
 | Current page no.: <100> in Cycles of 10 Page results pulled in Asyncio
 | Dork In Progress: displayArticleB.php?id=
 | Elapsed Time: 0:0:36


[+] URLS (unsorted) : Contains all the trash results still including duplicates:
  2429
[+] URLS (sorted)  : Trash, Duplicates, Dead-Links and other rubbish removed  25
8

[1] SQLi Testing, Will verify the Vuln links and print the Injectable URL to the
 screen
[2] SQLi Testing Auto Mode Will attempt to Verify vuln sites then Column count i
f MySQL detected
[3] LFI - RCE Testing [!] Broken, Please Wait for fix [!]
[4] XSS Testing
[5] Save valid Sorted and confirmed vuln urls to file
[6] Print all the UNSORTED urls
[7] Print all Sorted and Confirmed Vulns from last scan again
[8] Back to main menu
:
```

V3n0M Scanner

Escolha a primeira opção:

```
[6] Print all the UNSORTED urls
[7] Print all Sorted and Confirmed Vulns from last scan again
[8] Back to main menu
:1

[+] Preparing for SQLi scanning ...
[+] Can take a while and appear not to be doing anything...
[!] Please be patient if you can see this message, its Working ...

http://www.sedimental.com/catalog/index.php?ID=67 is vulnerable --> MySQL Classi
c
http://southbayballet.org/photo-gallery.php?id=38 is vulnerable --> MySQL Classi
c
http://www.p5n.net/mtl/news-full.php?id=14 is Vulnerable --> MiscError
http://www.eki-chem.com/index2.php?module=&amp;page=contact&amp;action=send is v
ulnerable --> MySQL Classic
http://www.odinshundar.se/memberinfo.php?id=15 is Vulnerable --> MiscError
http://www.readyicons.com/iconset-preview.php?id=11 is Vulnerable --> MiscError
http://www.bransonparksandrecreation.com/page.php?id=64 is vulnerable --> MySQL
Classic
http://www.tacc.co.il/story.php?id=9 is vulnerable --> MySQL Classic
http://www.valence-sports-orientation.fr/page.php?id=124 is Vulnerable --> MiscE
rror
http://www.thornbridgebrewery.com/shop.php?catid=2 is vulnerable --> MySQL Class
```