Cangibrina – Dashboard Finder

11 de setembro de 201516 de setembro de 2015 / Fnkoc

ATENÇÃO: Este post é atualizado toda vez que alguma função é inserida ou removida da ferramenta.

Hoje trarei uma ferramenta desenvolvida por mim mesmo – UAU – cujo desenvolvimento inicial teve como motivação a aprendizagem da linguagem de programação Python. Portanto, fui adicionando ao longo do tempo vários recursos que achava interessante.

A ferramenta se encontra no Github e está sob licença GPL v2

Irei fazer este post em diferentes etapas, sendo introdução a ferramenta, apresentação de recursos e informações, instalação e, por último, uso da mesma.

Introdução: Quais os objetivos e como funciona?

Cangibrina é uma ferramenta multiplataforma (Testada em Windows e Linux) que possui a simples tarefa de achar o painel de administração de um determinado site. Para isso, o Cangibrina utiliza diversas técnicas como brute-force baseado em wordlist, robots.txt, dorks de busca utilizando os motores Google e DuckDuckGo, filtro de extensão e também o Nmap.

Apresentação de Recursos e Informações

Threads

Com o objetivo de concluir a tarefa no menor tempo possível, tornei a ferramenta multi-processo, ou seja, ela cria vários processos independentes no sistema para poder concluir a tarefa em menor tempo.

$ cangibrina -u google.com -t 10

Wordlist

Você pode utilizar uma wordlist de sua preferência, através do argumento -w /caminho/wordlist, ou a wordlist padrão, que é selecionada automaticamente quando o argumento -w não é informado.
Dentro do diretório Wordlist eu incluí 4 wordlists diferentes: wl_default (5509 possibilidades) wl_small (126 possibilidades) wl_medium (481 possibilidades) e wl_medium2 (980 possibilidades). O que muda de uma para outra é o número de possibilidades que cada uma possui.

É recomendado utilizar um filtro de extensão para otimizar o scan

```
$ cangibrina -u google.com -w /opt/cangibrina/Wordlist/wl_medium --ext php
```

Dorks

Utiliza os motores de busca Google e DuckDuckGo. A dork utilizada é definida pelo usuário, utilizando -d <dork>, ou na ausência do argumento -d uma dork padrão.

$ cangibrina -u google.com -d 'inurl:login ext:php'

Nmap

Este recurso nada mais é do que a execução do comando sudo nmap -Pn -sC -sS -g 53 -D '127.0.0.1' target.com, que visa descobrir portas e serviços disponíveis no servidor, coletar informações dos serviços descobertos e ainda realizar um bypass caso exista um firewall para que o Nmap não seja barrado.

$ cangibrina -u google.com -n

User Agent

Traz a opção de alterar seu user-agent durante os testes para que, assim, se pareça com um usuário normal.

$ cangibrina -u google.com -a

Proxy HTTP

Traz a opção de mudar seu IP, para que, assim, você possa assumir uma nova identidade online e evitar ser bloqueado.
É utlizado HTTP proxy.

$ cangibrina -u google.com -p 187.25.2.485:8080

TOR

Utiliza a rede TOR para adiquirir um novo IP. É necessário ter o serviço instalado no sistema.

$ cangibrina -u google.com -T

Output

Permite que você configure o nome dos arquivos log gerados.

$ cangibrina -u google.com -s google

Continue lendo o texto para mais exemplos.

Instalação

Linux

Cangibrina pode ser encontrado no AUR e nos repositórios do BlackArch

$ pacman -S cangibrina

Para outras distribuições, baixe do GitHub.

Faça o download da ferramenta

##Baixe o código

$ git clone https://github.com/fnk0c/cangibrina.git

##Entre no diretório

$ cd cangibrina

##Execute o arquivo “setup.py”

$ python setup.py install

Este script irá instalar as dependências e criar um link simbólico para o cangibrina, fazendo-o ser reconhecido como um comando pelo terminal Linux.

Windows

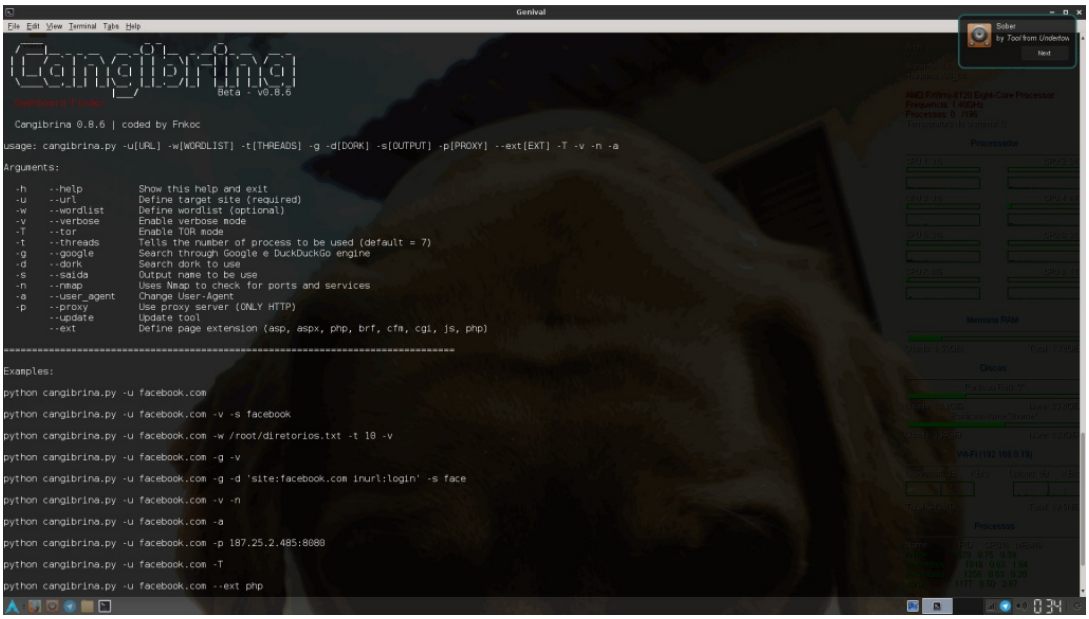
1. Faça o download da ferramenta utilizando seu navegador.
   https://github.com/fnk0c/cangibrina/archive/master.zip
2. Descompacte a ferramenta.
3. Abra o prompt de comando.
   INICIAR > pesquisar > prompt ou Tecla Windows + R

4. Vá até a pasta onde se encontra a ferramenta e rode o seguinte comando
   python setup.py install

Pronto, agora você já pode utilizar a ferramenta.

Utilização

Ao digitar “cangibrina” sem argumentos você verá a ajuda.



Para realizar o scan em um determinado site basta utilizar o comando:

$ cangibrina -u target.com

Porém, vamos incrementar mais.

Irei digitar os comandos e explicar (lembrando que a documentação está disponível em português e inglês).

cangibrina -u cienciahacker.com.br -t 6

-u > determina o site a ser utilizado

-t > número de threads – processos – a serem criados

Ao rodar este comando, tendo o Ciência Hacker como alvo, deve retornar o erro 403 (proibído)

Isso acontece porque o cloundflare bloqueia requisições automáticas. Para contornar isso podemos adicionar o argument “-a”, que irá modificar o user-agent.

$ cangibrina -u cienciahacker.com.br -v -a -t 6

-v > modo verbose (imprime na tela tudo que o programa faz)

-a > Modifica user-agent

Feito isso o programa consegue estabelecer conexão com o site. e como podem observar, o programa detectou um redirecionamento da URL, ficando para o usuário a decisão de seguir ou não o redirecionamento.

Ao final do scan você verá algo parecido com isso.

Realizando buscas utilizando o Google e o DuckDuckGo

cangibrina -u google.com -t 15 -g -d ‘site:google.com inurl:login’

-g > Ativa a busca por painéis desprotegidos utilizando a busca do Google DuckDuckGo
-d > Informa dork de busca personalizada
*DEVE SER ESCRITA ENTRE ASPAS SIMPLES

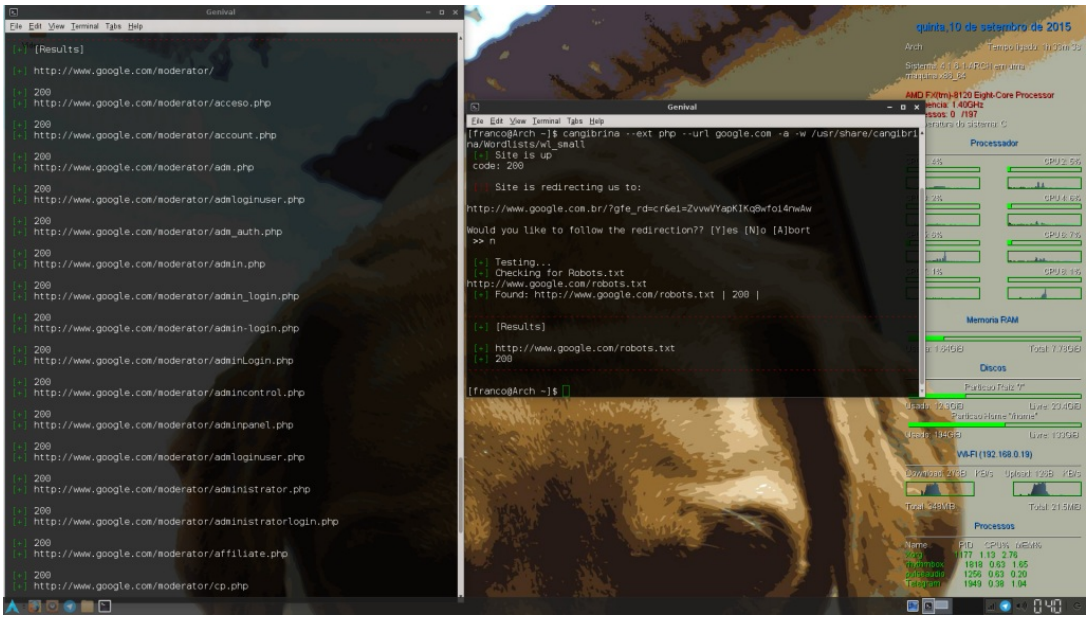
cangibrina -u cienciahacker.com.br -n -a

-n > Ativa scan utilizando Nmap

-a > Utiliza user-agent

cangibrina -u google.com -w /opt/cangibrina/Wordlist/wl_small

-w > Informa wordlist personalizada



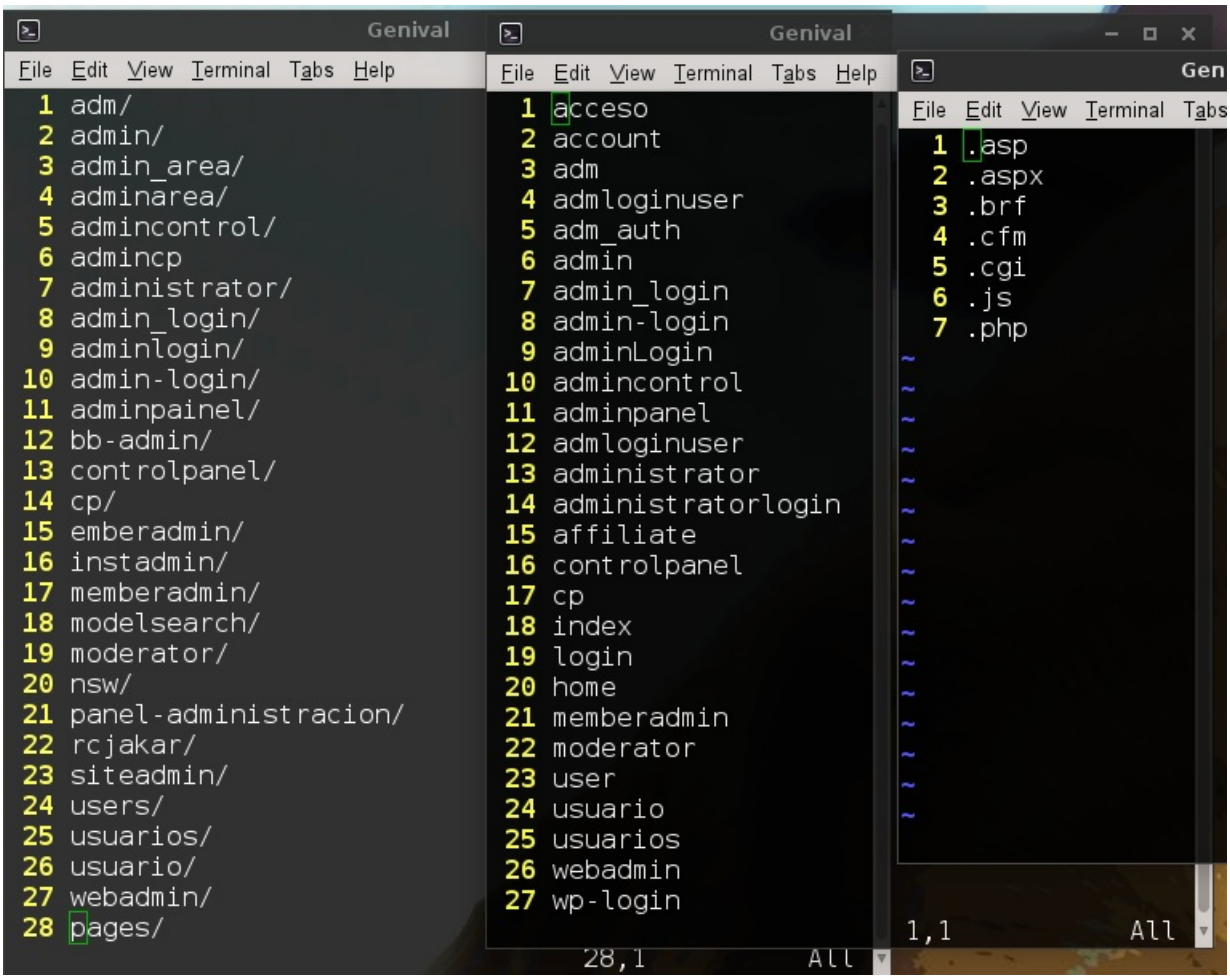
Reparem que a wordlist *wl_small* trouxe menos resultados, por isso a escolha da wordlist é sempre importante. Imagine que você tem como alvo um site russo, com certeza se você utilizar uma wordlist que contenha algumas palavras em russo você terá mais chances dependendo do tipo de site.

O cangibrina trás uma maneira fácil e simples para você criar sua própria wordlist. Trata-se do “wl-generator.py”

wlgenerator: Gerando wordlists

A ferramenta se encontra em /usr/share/cangibrina/Wordlists/wl\ generator/

Como podem reparar, existem 3 (três) arquivos TXT. Nestes arquivos, você adiciona páginas, diretórios e extensões que lhe sejam interessantes, para que assim tenha a wordlist mais acertiva possível.



Para gerar sua wordlist, basta executar:

python wlgenerator.py

E pronto, sua wordlist personalizada foi gerada.