****

**Visão**

Com a crescente demanda sobre Tecnologias, percebemos que muitas pessoas apesar de buscarem informações, não possuem fontes que queiram realmente passar o conhecimento da maneira como ela deve ser, livre e com embasamento técnico que permita ser aplicado e utilizado quando necessário, além de serem testados em sua criação, tornando esta informação útil e confiável.

**Missão**

O Laboratório foi criado com a intenção de buscar e disseminar o conhecimento de uma maneira clara e objetiva, de forma gratuita, auxiliando na evolução dos membros e da sociedade na qual estas informações são compartilhadas, buscando o crescimento de todos os envolvidos nesta criação de valores.



Caso você pense que com a leitura dos materiais da How2Security, você irá se tornar um Cracker capaz de invadir sistemas, se você espera encontrar aqui scripts infalíveis para invasão e, a partir deles, sair por aí invadindo computadores, essa não é a leitura indicada. Indicamos, sim a leitura do Código Penal (Lei 2.848/1940), principalmente a Lei Carolina Dickmann (Lei 12.737/2012), nos Artigos 154-A e 154-B.

*154-A Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:*

*Pena – Detenção, de 3 meses a 1 ano, e multa*

Este material é um conjunto de informações compiladas de documentos e ferramentas do Mundo Underground testadas em ambiente de laboratório na nossa intranet. Desta forma, todo conhecimento aqui condensado é tangível, assim como as orientações das contramedidas.

Dessa forma, esperamos ter sido bem claros que, em momento algum, estamos com a pretensão de ensinar a você como se tornar um invasor. Estaremos sim, mostrando muitas das técnicas utilizadas pelos crackers e, em alguns casos, pelos scripts kiddies, para que você, como administrador de redes, seja capaz de identificá-las em tempo hábil para se defender, antes que alguém com desejos menos nobres ô faça por você.

Assim sendo, todo o conteúdo dessa literatura tem apenas o objetivo didático de informar e preparar os administradores de redes dos novos tempos. Em momento algum nos responsabilizamos pelo mau uso desse conhecimento ou por danos causados em seu equipamento ou de terceiros, assim como também não somos responsáveis pelos códigos e ferramentas aqui citados.

Sandro Melo

Adaptado por Wellington Silva aka Well

**0 – Scanning – Enumerando o Alvo com o DIRB**

O Dirb faz a enumeração da estrutura do website. Ferramentas como o Dirb ajudam a automatizar o escaneamento da estrutura do website.

O Dirb envia requisições manuais para uma determinada página web e, de acordo com o código HTTP de resposta, verifica se um arquivo e/ou diretório existem. Por exemplo, supondo que seja necessário checar se os arquivos ***index.bkp***, ***upload.php***, diretório ***admin*** existem no endereço do alvo, para isso, ele utiliza uma wordlist para levantar os documentos existentes no servidor.

**1 – Utilizando o DIRB**

Primeiramente vamos ver sua sintaxe e opções:

**# dirb <url> <wordlist> <opções>**

Onde:

* **-a User-Agent** 🡪 Especificar um User-Agent;
* **-c cookie** 🡪 Define um Cookie;
* **-H** cabeçalho 🡪 Define um novo cabeçalho para as requisições HTTP;
* **-i** 🡪 Case-inentivive. Não há diferença entre letras maiúsculas e minúsculas;
* **-l** 🡪 exibe o cabeçalho “Location:”;
* **-N código** 🡪 Ignora respostas com determinado código HTTP;
* **-o saída** 🡪 Grava a saída em um arquivo;
* **-p proxy:porta** 🡪 Utiliza um proxy. Caso não seja especificado, é usado o valor padrão para a porta 1080;
* **-P usuário:senha** 🡪 Usuário e senha para proxy autenticado;
* **-r** 🡪 Não busca de forma recursiva;
* **-R** 🡪 Recursividade interativa. Pergunta se o usuário realmente quer fazer uma busca em cada diretório que o Dirb encontar
* **-S** 🡪 Modo silencioso. Não exibe cada teste feito;
* **-t** 🡪 Não força o uso de barra / no fim de cada URL;
* -u usuário:senha 🡪 Usuário e senha para autenticação HTTP;
* **-v** 🡪 Exibepáginas não encontradas (NOT FOUND);
* **-w** 🡪 O Dirb continua a execução mesmo que mensagens de aviso (warning) sejam enviadas ao usuário;
* **-X extensão** 🡪 Adiciona a extensão no final de cada busca. Exemplo: -X .html (adiciona html em cada nome de busca feito pelo Dirb);
* **-resume** 🡪 Retorna de onde parou a busca após ter pressionado a tecla **q**.

Caso você ainda não tenha uma wordlist, você poderá utilizar as que vem por padrão com o Dirp. Essas wordlist se encontram em /usr/share/dirp/wordlists.

Outro ponto é que podemos parar uma busca pressionado a tecla **q** e retoma de onde parou utilizando a opção **–resume**.

root@kali-wellx86:~# dirb http://192.168.0.105

-----------------

DIRB v2.22

By The Dark Raver

-----------------

START\_TIME: Tue Apr 17 01:13:20 2018

URL\_BASE: http://192.168.0.105/

WORDLIST\_FILES: **/usr/share/dirb/wordlists/common.txt**

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.105/ ----

+ http://192.168.0.105/.bash\_history (CODE:200|SIZE:189)

**==> DIRECTORY: http://192.168.0.105/~test/**

+ http://192.168.0.105/access (CODE:200|SIZE:187)

+ http://192.168.0.105/cgi-bin/ (CODE:403|SIZE:289)

+ http://192.168.0.105/index (CODE:200|SIZE:0)

+ http://192.168.0.105/info (CODE:200|SIZE:52216)

+ http://192.168.0.105/info.php (CODE:200|SIZE:52085)

**==> DIRECTORY: http://192.168.0.105/javascript/**

**==> DIRECTORY: http://192.168.0.105/phpmyadmin/**

+ http://192.168.0.105/server-status (CODE:403|SIZE:294)

**==> DIRECTORY: http://192.168.0.105/test/**

**==> DIRECTORY: http://192.168.0.105/webdav/**

---- Entering directory: http://192.168.0.105/~test/ ----

+ http://192.168.0.105/~test/index (CODE:200|SIZE:86)

+ http://192.168.0.105/~test/index.html (CODE:200|SIZE:86)

---- Entering directory: http://192.168.0.105/javascript/ ----

---- Entering directory: http://192.168.0.105/phpmyadmin/ ----

+ http://192.168.0.105/phpmyadmin/favicon.ico (CODE:200|SIZE:18902)

+ http://192.168.0.105/phpmyadmin/index.php (CODE:200|SIZE:8625)

**==> DIRECTORY: http://192.168.0.105/phpmyadmin/js/**

**==> DIRECTORY: http://192.168.0.105/phpmyadmin/lang/**

+ http://192.168.0.105/phpmyadmin/libraries (CODE:403|SIZE:301)

+ http://192.168.0.105/phpmyadmin/phpinfo.php (CODE:200|SIZE:0)

+ http://192.168.0.105/phpmyadmin/setup (CODE:401|SIZE:480)

**==> DIRECTORY: http://192.168.0.105/phpmyadmin/themes/**

---- Entering directory: http://192.168.0.105/test/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.

(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.0.105/webdav/ ----

+ http://192.168.0.105/webdav/index.html (CODE:200|SIZE:6)

---- Entering directory: http://192.168.0.105/phpmyadmin/js/ ----

---- Entering directory: http://192.168.0.105/phpmyadmin/lang/ ----

---- Entering directory: http://192.168.0.105/phpmyadmin/themes/ ----

**==> DIRECTORY: http://192.168.0.105/phpmyadmin/themes/original/**

---- Entering directory: http://192.168.0.105/phpmyadmin/themes/original/ ----

**==> DIRECTORY: http://192.168.0.105/phpmyadmin/themes/original/css/**

**==> DIRECTORY: http://192.168.0.105/phpmyadmin/themes/original/img/**

---- Entering directory: http://192.168.0.105/phpmyadmin/themes/original/css/ ----

---- Entering directory: http://192.168.0.105/phpmyadmin/themes/original/img/ ----

-----------------

END\_TIME: Tue Apr 17 01:14:11 2018

DOWNLOADED: 50732 - **FOUND: 15**

root@kali-wellx86:~#

Podermos executar utilizando um outro User-Agent.

root@kali-wellx86:~# dirb http://192.168.0.105 -a "Teste Well"

-----------------

DIRB v2.22

By The Dark Raver

-----------------

START\_TIME: Tue Apr 17 01:18:16 2018

URL\_BASE: http://192.168.0.105/

WORDLIST\_FILES: /usr/share/dirb/wordlists/common.txt

USER\_AGENT: Teste Well

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.105/ ----

+ http://192.168.0.105/.bash\_history (CODE:200|SIZE:189)

==> DIRECTORY: http://192.168.0.105/~test/

+ http://192.168.0.105/access (CODE:200|SIZE:187)

+ http://192.168.0.105/cgi-bin/ (CODE:403|SIZE:289)

+ http://192.168.0.105/index (CODE:200|SIZE:0)

+ http://192.168.0.105/info (CODE:200|SIZE:52096)

+ http://192.168.0.105/info.php (CODE:200|SIZE:51965)

==> DIRECTORY: http://192.168.0.105/javascript/

==> DIRECTORY: http://192.168.0.105/phpmyadmin/

+ http://192.168.0.105/server-status (CODE:403|SIZE:294)

==> DIRECTORY: http://192.168.0.105/test/

==> DIRECTORY: http://192.168.0.105/webdav/

---- Entering directory: http://192.168.0.105/~test/ ----

+ http://192.168.0.105/~test/index (CODE:200|SIZE:86)

+ http://192.168.0.105/~test/index.html (CODE:200|SIZE:86)

+ Dumping session state and Quitting.

-----------------

END\_TIME: Tue Apr 17 01:18:26 2018

DOWNLOADED: 8235 - FOUND: 9

root@kali-wellx86:~#

Vamos olhar os logs no servidor alvo.

root@kali-wellx86:~# root@ubuntu:/var/www# tail -f /var/log/apache2/access.log | grep -i test

192.168.0.101 - - [16/Apr/2018:20:22:39 -0700] "GET /~test/Music HTTP/1.1" 404 472 "-" **"Teste Well"**

192.168.0.101 - - [16/Apr/2018:20:22:39 -0700] "GET /~test/mx HTTP/1.1" 404 469 "-" **"Teste Well"**

192.168.0.101 - - [16/Apr/2018:20:22:39 -0700] "GET /~test/my HTTP/1.1" 404 469 "-" **"Teste Well"**

192.168.0.101 - - [16/Apr/2018:20:22:39 -0700] "GET /~test/myaccount HTTP/1.1" 404 476 "-" "Teste Well"

192.168.0.101 - - [16/Apr/2018:20:22:39 -0700] "GET /~test/my-account HTTP/1.1" 404 477 "-" **"Teste Well"**

Algumas vezes, arquivos e diretórios são exibidos apenas para usuários autenticados no sistema.

root@kali-wellx86:~# dirb http://192.168.0.105/h2s-lab/secret/

-----------------

DIRB v2.22

By The Dark Raver

-----------------

START\_TIME: Tue Apr 17 01:38:00 2018

URL\_BASE: http://192.168.0.105/h2s-lab/secret/

WORDLIST\_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4613

**---- Scanning URL: http://192.168.0.105/h2s-lab/secret/ ----**

**(!) WARNING: All responses for this directory seem to be CODE = 401.**

**(Use mode '-w' if you want to scan it anyway)**

-----------------

END\_TIME: Tue Apr 17 01:38:00 2018

DOWNLOADED: 101 - FOUND: 0

root@kali-wellx86:~#

Então podemos passar usuário e senha para fazer o crowling desse site.

root@kali-wellx86:~# dirb http://192.168.0.105/h2s-lab/secret/ -u admin:123456

-----------------

DIRB v2.22

By The Dark Raver

-----------------

START\_TIME: Tue Apr 17 01:38:12 2018

URL\_BASE: http://192.168.0.105/h2s-lab/secret/

WORDLIST\_FILES: /usr/share/dirb/wordlists/common.txt

**AUTHORIZATION: admin:123456**

-----------------

GENERATED WORDS: 4613

**---- Scanning URL: http://192.168.0.105/h2s-lab/secret/ ----**

**+ http://192.168.0.105/h2s-lab/secret/secret.php (CODE:200|SIZE:51)**

-----------------

END\_TIME: Tue Apr 17 01:38:19 2018

DOWNLOADED: 4613 - FOUND: 1

root@kali-wellx86:~#

**2 – Referências**

**Referências Bibliográficas**

**[1]** MELO, Sandro – Estudo de Técnicas para Exploração de Vulnerabilidades em Redes TCP/IP, 2º Ed, Rio de Janeiro, 2006, Editora Alta Books Ltda.

**[2]** Packetwatch Research. Disponível em <http://www.packetwatch.net/netcatfix.php>. Acessado em 28/03/2017.

**[3]** Fontes Netcat. Disponível em <http://download.insecure.org/stf/nc110.tgz>. Acessado em 28/03/2017.

**[4]** MORENO, Daniel – Penest em Aplicações Web – São Paulo – 2017, Novatec