****

**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 Dirbuster**

O Dirbuster é uma ferramenta de enumeração de arquivos e diretórios, similar ao Dirb.

**1 – Utilizando o Dirbuster**

O Dirbuster é uma ferramenta com interface gráfica (GUI) e tem as seguintes opções:

* **Target** 🡪 Especificar o alvo;
* **Work Method** 🡪 Método HTTP;
  + **Use Get request only** 🡪 Usa somente o método GET no envoi de requisições;
  + **Auto Switch (HEAD and GET)** 🡪 Alterna entre GET e HEAD.
* **Number of Threads** 🡪 Define o número de threads executadas ao mesmo tempo. Quanto mais threads são abertas no computador local, mais requisições são feitas ao mesmo tempo para o servidor e mais rápido será o processo de enumeração de arquivos e diretórios. A opção Go Faster aumenta consideravelmente a quantidade de threads locais que podem ser usadas;
* **Select scanning type** 🡪 Tipo de scanning;
  + **List based brute force** 🡪 Utiliza wordlist. Cada palavra da lista é adicionada o fim da URL e enviada ao servidor. De acordo com o código retornado pelo servidor o Dirbuster determina quais arquivos e diretórios existem no servidor web;
  + **Pure brute force** 🡪 Utiliza brute force.
* **Char set** 🡪 Habilitado somente em ataques de brute force (Select scanning type 🡪 Pure brute force). Há diversas opções de força bruta, como somente números, mesclagem entre números e caracteres minúsculos, etc.;
  + **Min Length** 🡪 Habilitado somente em ataques de brute force e estipula o tamanho mínimo dos caracteres/número;
  + **Max Length** 🡪 Habilitado somente em ataque de brute force e estipula o tamanho máximo dos caracteres/números.
* **Select start options** 🡪 Como o Dirbuster irá realizar a varedura;
  + **Standard start point** 🡪 Modo padrão;
    - **Brute force Dirs** 🡪 Hsbilitado quando se deseja descobrir quais são os diretórios do servidor web;
    - **Brute force files** 🡪 Habilitado quando se deseja descobrir quais são os arquivos do servidor web;
    - **Be recursive** 🡪 Ao descobrir um nome de diretório, o Dirbuster será recursivo, realizando a varredura dentro desse diretório descoberto;
    - **Use blank extension** 🡪 Busca por nomes sem extensões;
    - **Dir to start with** 🡪 Diretório base a ser iniciado a varredura
    - **File extension** 🡪 Extensões de arquivos que serão pesquisados (.php, .html, .docx, etc.).
* **URL Fuzz** 🡪 Fuzzing na URL. Essa opção é utilizada em situações em que se queira auditar algum parâmetro de URL.

Vamos fazer um teste utilizando as opções: Brute Force Dirs, Brute force file, Be recursive, Use blankextension e File extension (php,df).

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.

**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