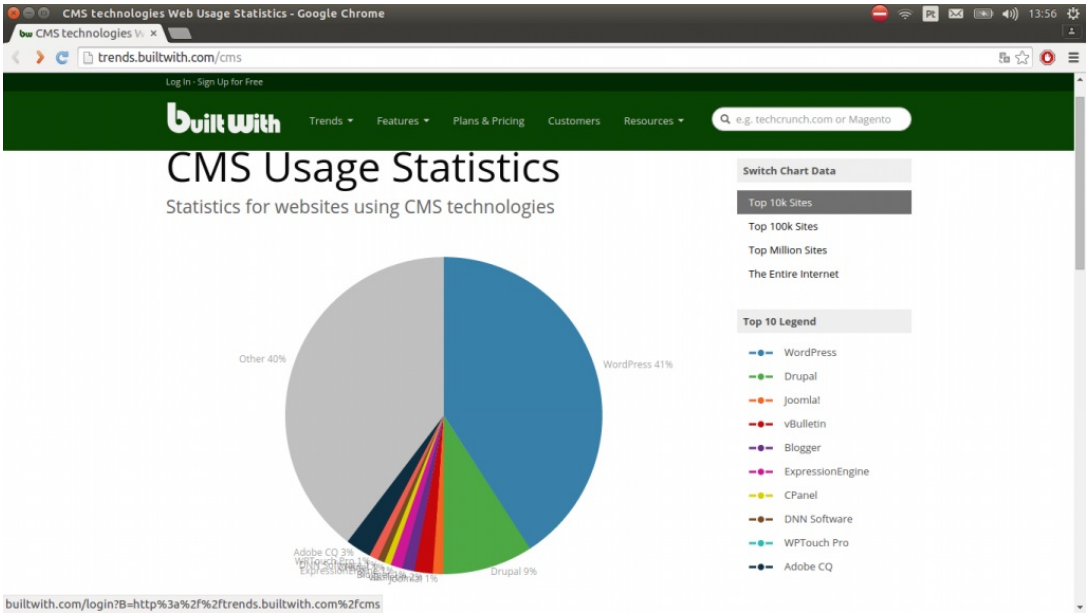
Explorando vulnerabilidades no WordPress com Wpscan

6 de setembro de 201523 de setembro de 2015 / s0ph0s

Muito utiliza-se CMS (como WordPress, Drupal e Joomla) atualmente, devido o fácil gerenciamento que ele permite fazer em websites, porém o que muitos não sabem é a quantidade de falhas contidas nesses serviços. Traremos hoje a ferramenta ***Wpscan*** que é utilizada para fazer varreduras em sites gerenciados por *WordPress,* buscando por falhas de segurança, nos outros artigos traremos ferramentas de scanners para outros tipos de CMS.

Para quem ainda se familiariza com o WordPress, ele é muito utilizado em sites de e-commerce, prestação de serviços e blogs, e considerado o CMS mais utilizado na web segundo uma pesquisa.



Conhecendo o Wpscan

O *Wpscan* é uma ferramenta feita em Ruby que traz informações do nosso alvo através de sua varredura, reportando possíveis falhas em plugins, temas, timthumbs, entre outras. Veja a lista abaixo das suas principais funções:

- Enumeração de Usuário
- Enumeração de Serviço
- Enumeração de Vulnerabilidade
- Enumeração de Plugin
- Enumeração de Plugin Vulnerável
- Quebra de Senha Fraca
- Outras Verificações (Nome do Tema, Listagem de Diretórios, ...)

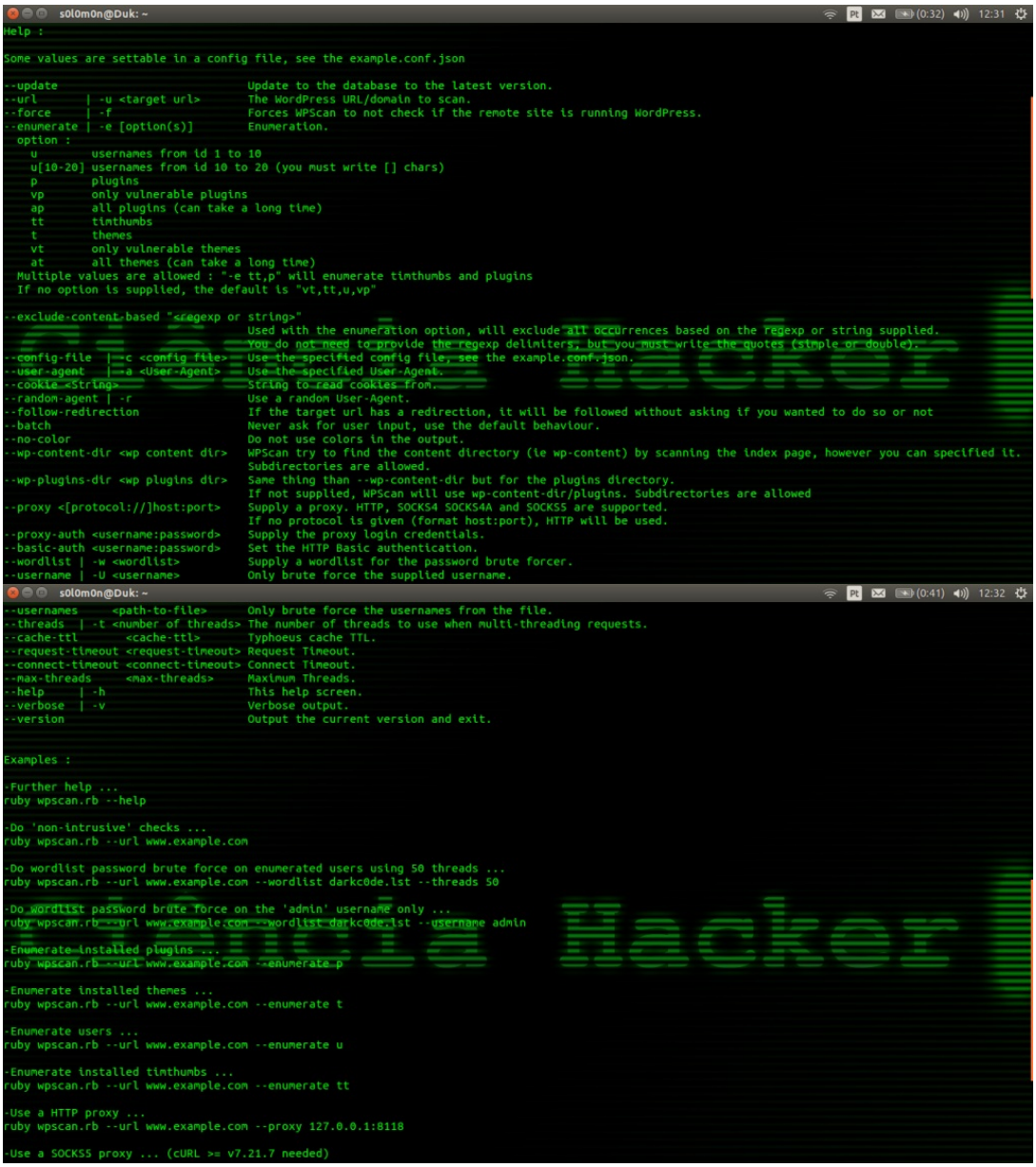
Instalando o Wpscan

Ele já vem por padrão na maioria das distribuições de PenTest, como o Kali Linux e Parrot Security. Mas caso queira baixar utilize nossa ferramenta *Organon* (clique aqui para ver como instala-la) para realizar o download e instalação automatica para você.

Realizando as configurações de ataque

Para verificar todas as opções da ferramenta de o comando *–help*

```
# wpscan --help
```



Veja que ela lista todos os detalhes, desde da sua utilização até exemplos de tipos de varreduras. Devido ela ser muito extensa em seus recursos, vamos usufruir dos principais dela:

- –url ***site_alvo*** – indica o site alvo.
- –enumerate ***PARÂMETRO*** – usado para determinar as opções de scan cujo algumas são as seguintes.
  - vp – faz busca somente por plugins vulneráveis.
  - vt – faz busca somente por temas vulneráveis.
  - p – faz busca por plugins.
  - t – faz busca por temas.
  - u – lista usuários do site (do ID 1 ao 10).
  - uid-id – especifica o range de IDs a serem verificados.
- –threads ***NÚMERO*** – executa o escaneamento usando N threads.
- –wordlist ***senhas.txt*** – utilizado num ataque de força bruta com uma *wordlist*.
- –username ***USUARIO*** – seleciona um usuário para fazer um ataque.
- –proxy ***<protocolo>://<host>:<porta>*** – seleciona um proxy para ser utilizado durante sua utilização. Ex:. *–proxy socks5://127.0.0.1:9000*

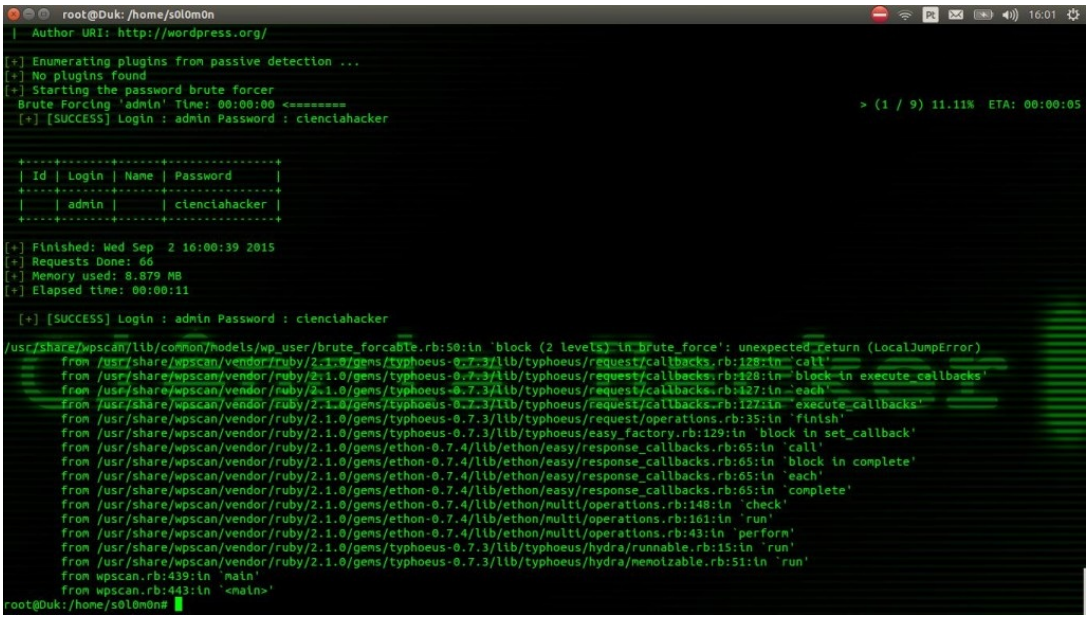
A seguir realizaremos alguns testes no nosso site, que serve como laboratório, lembrando que todos os comandos devem ser executados como superusuário (root).

O primeiro exemplo de comando é para enumerar os plugins e temas vulneráveis, a qual ele indica o tipo da falha e como explora-la.

wpscan –url http://laboratorio.pe.hu –enumerate vpt

Repare que com uma simples varredura trouxe diversas informações, como falhas relacionada a XSS, a versão do servidor e do tema. Muitas vezes ele não vai conseguir enumerar todos os serviços, devido algum mecanismo de segurança do site que falaremos mais no final.
Com o comando *–u* a seguir podemos enumerar os usuários cadastrados no site, o nosso usuário é "admin" no exemplo desse site. Então vamos tentar atacar ele através de uma wordlist nomeada *senhas.txt.* Uma vez que muitos servidores bloqueiam esse tipo de ataque, usaremos *thread*s para limitar o intervalo de requisições e não permitir que algum mecanismo de segurança nos bloqueie.

```
# wpscan --url http://laboratorio.pe.hu --wordlist /home/s0l0m0n/senhas.txt --username admin --threads 10
```



Caso queira usar um proxy, ou usar o TOR damos o seguinte comando:

```
#wpscan --url http://laboratorio.pe.hu --wordlist /home/s0l0m0n/senhas.txt --username admin --threads 10 --
proxy HTTP://127.0.0.1:8123
```

Se protegendo de falhas no WordPress

Para evitar falhas segurança no seu WordPress é necessário que mantenha os serviços dele atualizado, como deixar sempre a versão mais recente dos Plugins e Temas (lembrando que o próprio CMS avisa dessas atualizações nos ícones de notificações).

Outra forma também é baixar plugins de segurança para WordPress como o **Acunetix WP Security** que analisa se tem alguma falha de segurança e é usado também para proteção de ataques. Recomenda-se também o **Stop User Enumeration** que bloqueia a verificação de usuários listado no seu site, dificultando um possível ataque de força bruta (lembre-se também de configurar uma senha difícil para não ser facilmente quebrada).

, ,