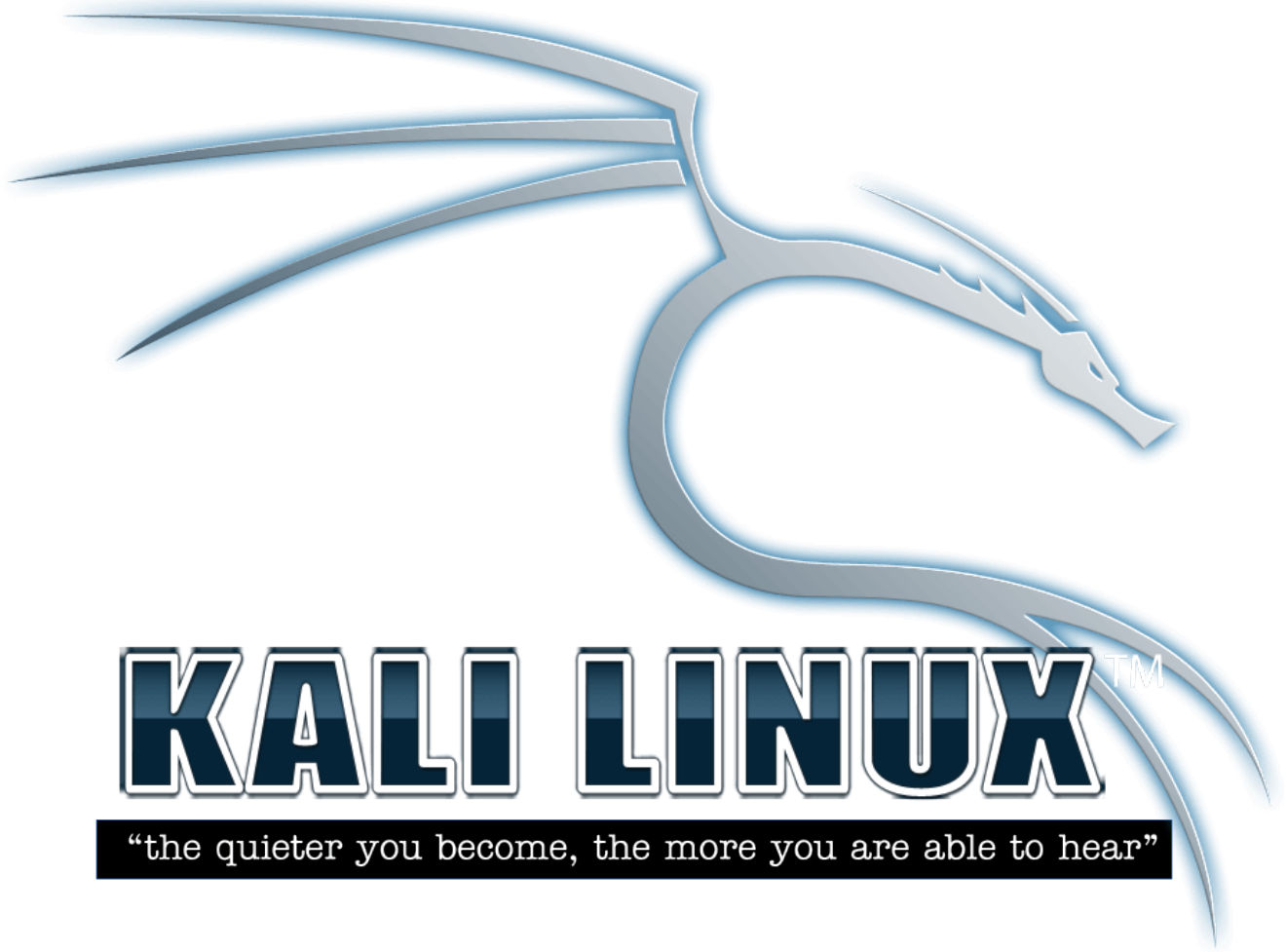
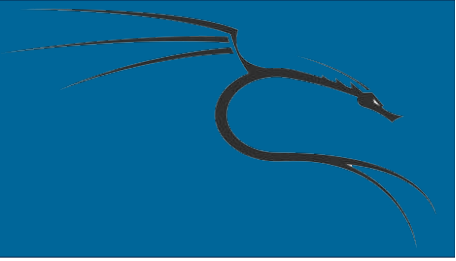
Pentest com Kali Linux





Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Criar um site de phishing

Na aula anterior, usamos o SET para duplicar um site e usar para coletar as senhas. Duplicar apenas a página de login não funcionará com usuários mais avançados. Eles podem ficar suspeitos quando digitam a senha correta e obter redirecionado para a página de login novamente ou tentará navegar para algum outro link na página e vamos perder como eles deixam nossa página e ir para o site original.

Criar um site de phishing

Vamos salvar a página para o nosso kali, e então fazer as modificações necessárias. Primeiro, vamos fazer o download da página do BodgeIt.

```
# wget -r -P bodgeit_offline/ http://192.168.1.163/bodgeit/
```

Em seguida, a página offline será armazenada no diretório bodgeit_offline.

Criar um site de phishing

O primeiro passo será copiar o site baixado para nossa pasta raiz do Apache no Kali. Dentro da pasta do bodgeit_offline copie todo o conteúdo para o Apache:

```
# cp -r bodgeit_offline/192.168.1.163/bodgeit/ /var/www/html/
# service apache2 start
```

Criar um site de phishing

Em seguida, precisamos atualizar nossa página de login para torná-lo redirecionado para o script que irá colher as senhas.

Abra o arquivo login.jsp dentro do diretório html (/var/www/html/bodgeit/) e procure o seguinte código:

```
<h3>Login</h3>

Please enter your credentials: <br/><br/>

<form method="POST">
```

Agora, no formulário tag adicione a ação para chamar post.php:

```
<form method="POST" action="post.php">
```

Criar um site de phishing

Precisamos criar esse arquivo no mesmo diretório onde está o

login.jsp é, criar post.php.

Como você pode ver, as senhas serão salvas em passwords_C00kb00k.txt; Precisamos criar esse arquivo e definir as permissões adequadas. Vá para /var/www/html/bodgeit/ no terminal raiz e emita os seguintes comandos:

```
# touch passwords_C00kb00k.txt

# chown www-data passwords_C00kb00k.txt
```

Criar um site de phishing

Lembre-se que o servidor web é executado sob o usuário de dados www, por isso precisamos fazer com que o usuário proprietário do arquivo, para que ele possa ser escrito pelo processo do servidor web Apache.

Criar um site de phishing

Agora, é hora do usuário vítima ir para esse site, suponha que façamos o usuário ir para http://192.168.1.145/bodgeit/login.jsp.

Abra um navegador da web e vá até lá.

Criar um site de phishing

Preencha o formulário de login com algumas informações de usuário e senha qualquer.

Depois que logar, ele vai dar a resposta da login e também vai fazer um redirect automático na página original.

Criar um site de phishing

Vamos verificar o arquivo de senhas; No terminal, digite

cat passwords_C00kb00k.txt

```
root@kali:/var/www/html/bodgeit# cat passwords_C00kb00k.txt
Array
(
    [username] => user@mail.com
    [password] => password
)
```