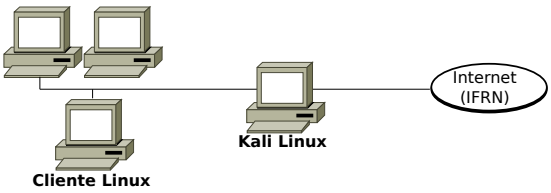
INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Professor: Macêdo Firmino
Disciplina: Segurança de Computadoores
Prática 10: Quebradores de Senha (Hydra e Medusa) e Captura de Senha com Site Falso (Setoolkit)

Olá turma, no teste de penetração deveremos fazer a exploração das vulnerabilidades. Umas destas vulnerabilidades é o acesso ao sistema. Para exploramos se faz necessário a utilização da engenharia social para conhecermos informações dos usuários para criarmos dicionários que serão utilizados para quebrar senhas. Na aula de hoje, iremos aprender algumas ferramentas (Hydra e Medusa) que quebram senhas com o auxilio de dicionários. Além disso, conheceremos uma ferramentaque possibilita criarmos sites falsos para capturamos credenciais (login e senha) de usuários. Além disso, iremos entender a importância de se utilizar boas senhas.

Configurando o Ambiente

Para estudarmos estes conceitos e ferramentas iremos utilizar duas máquinas virtuais. Uma será a máquina MetasploiTable (alvo) que iremos explorar as atividades e outra máquina com Kali Linux (atacante) para testarmos as vulnerabilidades. Crie as duas máquinas e suas respectivas configurações de rede (rede NAT).



As ferramentas Hydra, Medusa e setoolkit já vem instalado por padrão na distribuição Kali Linux. Na sequência iremos aprender a utiliza-las.

O openssh já vem instalado no MetasploiTable, podemos verificar o seu funcionamento tentando logar na máquina. Para isso, no seu Kali Linux digite o comando:

```
ssh -oHostKeyAlgorithms=+ssh-dss
 msfadmin@10.0.2.4
```

Onde msfadmin é o usuário que desejamos logar e 10.0.2.4 é o IP da máquina MetasploiTable.

THC Hydra

O Hydra é uma ferramenta para quebra de senhas em serviços online gratuita, tanto para Linux quanto para Windows com interface gráfica. Essencialmente THC Hydra é uma ferramenta rápida e estável *Network Login Hacker*, que usa um dicionário de força bruta para ataques e tentar várias combinações de senha e login contra uma página.

Dicionário é uma lista de palavras conhecidas e possíveis senhas que um software que irá testar cada uma delas para tentar descobrir a senha.

O Hydra suporta um vasto conjunto de protocolos incluindo Mail (POP3, IMAP, etc.), bancos de dados, LDAP, SMB, VNC e SSH. Na sequência iremos utiliza-lo para saber a qualidade da nossa senha em um servidor ssh local.

Os principais parâmetros são:

- -s Define a porta de destino
- -l Define o usuário de acesso
- -L Define o arquivo de wordlist de usuários
- -p Define a senha
- -P Define o arquivo de wordlist de senhas
- -M Define o arquivo de wordlist de alvos
- -t Define o número de conexões em paralelo, default 16
- -f Faz o hydra parar quando o primeiro user/password é encontrado
- -s Conecta via ssl
- -vV Define modo verbose

Exemplo do uso de Hydra para um ataque de Força Bruta para o usuário root no IP 12.18.1.14 no serviço ssh, com a utilização de dicionário:

01. Para fazer um teste básico no serviço de ssh execute:

```
hydra -l root -
P wordlist.txt 12.18.1.14 ssh
```

onde: "root" é o usuário que iremos tentar quebrar a senha; "wordlist.txt" é um dicionário utilizado para testar possíveis senhas; "12.18.1.14" IP do alvo; "ssh" é nome do módulo do respectivo serviço que será atacado.

Medusa

Medusa, assim com o Hydra, é uma ferramenta de brute-force para auditoria de segurança, visando mostrar a facilidade de quebrar senhas fracas visando mostrar como é fácil pessoas não autorizadas quebrarem senhas fracas. Ambos quebram senha remotas, dando suporte a SMB, HTTP, POP3, MS-SQL, SSHv2, e outros. Agora iremos conhecer a utilização da ferramenta.

Sintaxe:

```
Medusa [-h host|-H file] [-u username|-
U file]
[-p password|-P file] -M module [OPT]
```

onde:

- -h [TEXT]: Nome do computador ou IP alvo;
- -H [FILE]: Arquivo contendo nomes ou IPs alvos;
- -u [TEXT]: Nome do usuário para teste;
- -U [FILE]: Arquivo contendo nomes de usuários para teste;
- -p [TEXT]: senha para teste;
- -P [FILE]: Arquivo contendo senha para testes;
- -M [TEXT]: Nome do módulo para executar.

Exemplo do uso de Medusa para um ataque de Força Bruta com a utilização de dicionário:

01. Para fazer um teste básico no serviço de ssh execute:

```
medusa -h 192.168.1.108 -u root
  -P pass.txt -M ssh
```

onde: "129.168.1.108" é o computador alvo, "root" é o usuário, "pass.txt" contém um dicionário de possíveis senhas e "ssh" é o serviço que será utilizado para quebrar a senha.

Social Engineering Toolkit

A engenharia social corresponde ao ato de manipular uma pessoa para tomar qualquer ação que pode ou não ser do interesse do alvo, por exemplo, acessar um site falso. Uma das ferramentas mais comumente usadas em relação a ataques de engenharia social chama-se Social Engineering Toolkit (setoolkit). Ela é uma ferramenta de código aberto que contém opções de ataque. Ele foi e será utilizado apenas para fins de teste.

Com o setoolkit é possível clonar um site legítimo e induzir a vítima a visitar o link e inserir suas credenciais (login e senha). Desta forma, o invasor coletará suas credenciais e poderá redirecioná-lo para o site original para que ele não suspeite que algo estranho tenha acontecido.

A ferramenta setoolkit já vem instalada por padrão no Kali. Para inicia-lá, digite o comando:

```
sudo setoolkit
```

Ao inserir o comando nos é retornada a seguinte informação:

```
Select from the menu:

  1) Social-Engineering Attacks
  2) Penetration Testing (Fast-Track)
  3) Third Party Modules
  4) Update the Social-Engineer Toolkit
  5) Update SET configuration
  6) Help, Credits, and About

 99) Exit the Social-Engineer Toolkit
```

Agora selecione a opção 1) Social-Engineering Attacks. Para iniciarmos um ataque de engenharia social. Na sequência surgirá um novo menu questionando o tipo de ataque de engenharia social.

```
Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) Wireless Access Point Attack Vector
  8) QRCode Generator Attack Vector
  9) Powershell Attack Vectors
 10) Third Party Modules

 99) Return back to the main menu.
```

Na sequência, selecione a opção 2) Website Attack Vectors para iniciarmos os ataques WEB.

Feito isso ele nos perguntará qual tipo de ataque WEB estamos planejando. Selecione a opção 3) Credential Harvester Attack Method.

```
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu
```

Em seguida, ele irá mostrar três opções conforme mostrado abaixo, a primeira opção será "Web Template" que fornece alguns sites predefinidos que você usa para phishing. A segunda opção é "Clonador de site". Com esta opção você pode clonar a página de login de qualquer site da Web e a terceira opção que usaremos para este tutorial é "Importação personalizada". Com isso, você pode usar seu próprio modelo de página de login. Iremos utilizar a opção "Web Template".

```
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu
```

A ferramenta irá solicitar o endereço IP para colocar o site clonado. No nosso caso será a própria máquina kali Linux. Se você estiver executando o ataque na LAN, pode fornecer seu endereço IP interno e, se estiver executando o ataque na WAN, deverá fornecer seu endereço IP externo. Nesta aula, utilizaremos na LAN. Digite seu endereço IP e pressione Enter.

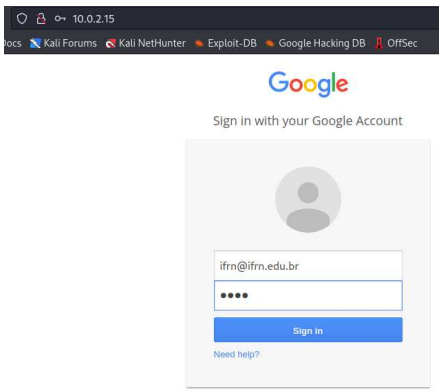
```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:
```

Entre os templates que esta versão disponibiliza está uma página java genérica, o login do Google e a tela de login do Twitter. Utilizaremos o template do Google. Para isso, selecione a opção 2.

```
1. Java Required
2. Google
3. Twitter
```

Possa ser que seja necessário, o setoolkit solicitará para parar o apache e iniciar o serviço do NGINX para hospedar a página. Realizada esta permissão, a página falsa estará rodando e esperando o acesso do cliente.

Nesta etapa é utilizado a engenharia social para enviar o link para o usuário e convencê-lo a entrar na página. Quando o usuário entrar, ele verá a tela de login do Google. Quando ele colocar as suas informações, o setoolkit irá capturar e mostrar o usuário e senha digitado.



Como podemos observar a senha digitada é mostrada no setoolkit.

```
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=ifrn@ifrn.edu.br
POSSIBLE PASSWORD FIELD FOUND: Passwd=ifrn
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
```

Contramedidas

Uma senha, ou *password*, serve para autenticar uma conta, ou seja, é usada no processo de verificação da sua identidade, assegurando que você é realmente quem diz ser e que possui o direito de acessar o recurso em questão. É um dos principais mecanismos de autenticação usados na Internet devido, principalmente, a sua simplicidade.

Algumas das formas como a sua senha pode ser descoberta são:

- Ao ser usada em computadores infectados. Muitos códigos maliciosos, armazenam as teclas digitadas, espionam você pela webcam e gravam a posição da tela onde o mouse foi clicado.
- Ao ser usada em sites falsos. Ao digitar a sua senha em um site falso, achando que está no site verdadeiro.
- Por meio de tentativas de adivinhação;
- Ao ser capturada enquanto trafega na rede, sem estar criptografada;
- Por meio do acesso ao arquivo onde a senha foi armazenada caso ela não tenha sido gravada de forma criptografada;
- Com o uso de técnicas de engenharia social, como forma a persuadi-lo a entregá-la voluntariamente;
- Pela observação da movimentação dos seus dedos no teclado ou dos cliques do mouse.

Cuidados a serem tomados ao usar suas contas e senhas:

- Certifique-se de não estar sendo observado ao digitar as suas senhas;
- Não forneça as suas senhas para outra pessoa;
- Certifique-se de fechar a sua sessão ao acessar sites que requeiram o uso de senhas.
- Elabore boas senhas;
- Altere as suas senhas sempre que julgar necessário;
- Não use a mesma senha para todos os serviços que acessa;
- Certifique-se de utilizar serviços criptografados quando o acesso a um site envolver o fornecimento de senha;
- Seja cuidadoso ao usar a sua senha em computadores potencialmente infectados ou comprometidos;
- Usar a mesma senha para acessar diferentes contas pode ser bastante arriscado, pois basta ao atacante conseguir a senha de uma conta para conseguir acessar as demais contas onde esta mesma senha foi usada.

Uma senha boa, bem elaborada, é aquela que é difícil de ser descoberta e fácil de ser lembrada. Não convém que você crie uma senha forte se, quando for usá-la, não conseguir recordá-la. Também não convém que você crie uma senha fácil de ser lembrada se ela puder ser facilmente descoberta por um atacante. Alguns elementos que você deve usar na elaboração de suas senhas são:

- Números aleatórios;
- Grande quantidade de caracteres: quanto mais longa for a senha mais difícil será descobri-la;
- Diferentes tipos de caracteres: procure misturar caracteres, como números, sinais de pontuação e letras maiúsculas e minúsculas;
- Selecione caracteres de uma frase: baseie-se em uma frase e selecione a primeira, a segunda ou a última letra de cada palavra.
- Faça substituições de caracteres: invente um padrão de substituição baseado, por exemplo, na semelhança visual (“w” e “vv”) ou de fonética (“ca” e “k”) entre os caracteres.

Atividade

01. Instale uma máquina virtual Ubuntu com Openssh-server. Crie um usuário “aluno” com a senha “12345678”. Crie um outro usuário, chamado de “professor”, com a respectiva senha “Q0sbnjdtq”.

02. Utilizando a máquina virtual com o Kali Linux, as ferramentas apresentadas e dicionários disponibilizados no Google Sala de Aula, realize um ataque de descoberta de senha no servidor SSH;

03. Foi possível quebrar as senhas dos usuários aluno e professor? Qual foi o comando, dicionário e tempo utilizados para quebrar a senha dos usuários via ssh?

04. Utilizando o setoolkit clone sites e observe se você consegue capturar as senhas digitadas nas páginas falsas.