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

Professor: Macêdo Firmino
Disciplina: Segurança de Computadoores
Prática 01: Testes de Senha com Quebrador Baseado em Dicionários

Olá turma, hoje conhecer a importância de se utilizar boas senhas. Para isso utilizaremos algumas ferramentas que quebram senhas com o auxilio de dicionários. Iremos fazer um teste com uma senha fraca e com senhas fortes.

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

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. Esta ferramenta suporta um vasto conjunto de protocolos incluindo Mail (POP3, IMAP, etc.), bancos de dados, LDAP, SMB, VNC e SSH.

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:

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

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

onde:

- wordlist.txt: é um dicionário utilizado para testar possíveis senhas;
- 12.18.1.14: IP do alvo;
- ssh: 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 melhor o Medusa.

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:

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 contem um dicionário de possíveis senhas e SSH é o serviço que será utilizado para quebrar a senha.

Dicas de Boas Senhas

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;
- 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, e aquela que e 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 dif??cil 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 os dicionários disponíveis no SUAP, realize um ataque de Força Bruta com o HYDRA, tendo como alvo o servidor SSH;

03. Utilizando os dicionários disponíveis no SUAP, faça um ataque de Força Bruta com o MEDUSA, tendo como alvo o servidor SSH.

04. Foi possível quebrar as senhas dos usuários