Resultado: Tarefa Realizada dia 01/04/16

Representando a atividade **Login - Força Bruta.**

Duração dos Testes:1 h

Duração total da atividade: 1h 20 min

**Objetivo**: Utilizar de forma automatizada uma ferramenta que simule

vários logins para descobrir se é possível acertar o login por chutes ou se site possui algum mecanismo que impeça que um login seja acertado ao acaso.

**Ferramenta:** Hydra é uma ferramenta automatizada para tentar realizar o procedimento de força bruta em uma página web. Bastando forncer uma lista de usuários ou senhas ela é configurável para fazer *“n”* tentativas por minuto onde n é um numero entre 1 e 16. Para funcionar o mais básico é fornece-la um login e um exemplo de senha com a URL do alvo que ela tentará.

**Resultados**

**Tentativa 1**

configurar a hydra e fazer ela realizar os testes

***Impedimento***: hydra não está reclamando de 3 parametros quando

o mapeamento indica claramente q o login só passa 2.

**Resultado**: indefinido

**Tentativa 2:**

Inserir um login válido e senha mais comuns num numero de

16 tentativas

*comando: hydra -l admin -P forcaBruta 192.168.0.58 http-post-form “vacina/login.php:login=^USER^:senha=^PASS^:logado=false”*

No comando acima:

1. -l significa o login utilizado no momento. Deve ser sempre admin pois é o unico usuário válido passado pela equipe de TI.
2. -P é o arquivo contendo as senhas que ele tentará utilizar.
3. 192.168.0.58 é o IP onde está hospedada a aplicação.
4. http-post-form é o método utilizado, no caso , POST do HTTP.
5. *“vacina/login.php:login=^USER^:senha=^PASS^:logado=false”* é a URL utilizada para fazer a requisição
   1. USER é onde ela deve inserir o login válido usada na requisição.
   2. PASS é onde a hydra deve inserir a senha válida usada na requisição

**Resultado:** Passou no Teste

**Tentativa 3:**

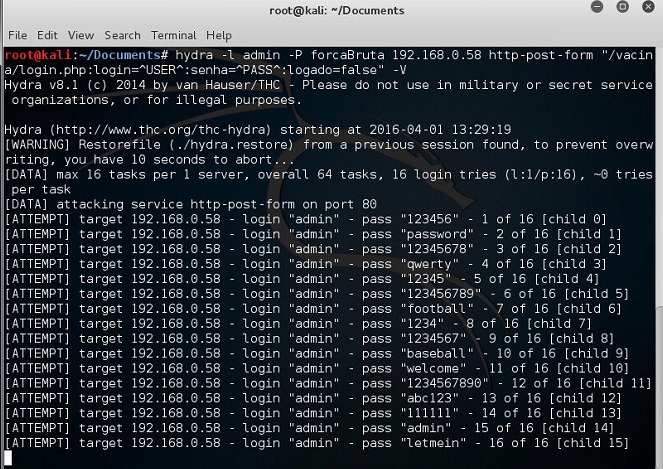
Consegui configurar a ferramenta e executar 16 testes por min fazendo tentativas com o login

admin (cedido pelo DGTI) e com um dicionário de senhas retiradas da lista de piores senhas de 2015 da SplashData.

*comando: hydra -l admin -P forcaBruta 192.168.0.58 http-post-form “vacina/login.php:login=^USER^:senha=^PASS^:logado=false” -V*

No comando acima:

1. -l significa o login utilizado no momento. Deve ser sempre admin pois é o único usuário válido passado pela equipe de TI.
2. -P é o arquivo contendo as senhas que ele tentará utilizar.
3. 192.168.0.58 é o IP onde está hospedada a aplicação.
4. http-post-form é o método utilizado, no caso , POST do HTTP.
5. *“vacina/login.php:login=^USER^:senha=^PASS^:logado=false”* é a URL utilizada para fazer a requisição
   1. USER é onde ela deve inserir o login válido usada na requisição.
   2. PASS é onde a hydra deve inserir a senha válida usada na requisição
6. -V é para exibir no console o resultado da operação.



Conforme mostra a imagem acima, houve várias tentativas que não deram sucesso de logar.Há uma vulnerabilidade nesse aspecto.

Referencia Externa:

[Piores Senhas 2015](https://www.teamsid.com/worst-passwords-2015/)