**ESQUEMA DE PLANO DE AULA PRÁTICA**

**TAREFA 8c** "Scanning para descobrir Rootkits"

Tópico no Moodle: “Descobrindo Rootkits ”

Data:

Tempo de Aula: 1 hora-aula

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

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

**ASSUNTO**

**Um rootkit é uma coleção de softwares maliciosos composto de (malware, backdoor, trojan, logclean) projetado como um programa para ocultar processos suspeitos da sua detecção e permitir, frequentemente, acesso remoto para um sistema de computador.**

**Rootkits podem ser instalados usando vários métodos, incluindo código executável oculto dentro de links de páginas web, softwares baixados da Internet ou sobre arquivos e documentos.**

**BIBLIOGRAFIA BÁSICA E INSTALAÇÕES**

Backtrack 5 Cookbook, Wllie Prittchett e David De Smet, PACKT Publishing, 2012, páginas 258-259.

**REQUISITOS**

No sentido de escanear para descobrir se existe um rootkit, você pode ou usar sua VM Backtrack, e fazer login para uma VM comprometida remotamente, ou montar o DVD do Backtrack 5 R3 sobre um sistema de computador para o qual você tenha acesso físico.

1. **VM Backtrack 5 ou Backtrack 5 R3 DVD num computador (CD Live do Backtrack que pode ser rodado sem ser instalado no HD);**
2. **Por exemplo, uma VM Metasploitable 2, uma VM comprometida remotamente.**

 **OBJETIVOS DA AULA**

Nesta experiência podemos utilizar **chkrootkit.**

**SELEÇÃO DE CONTEÚDO – A PRÁTICA**

Um conteúdo mínimo, consistindo de um roteiro de aula, com Backtrack 5 e Metasploit 2, visando o objetivo acima, pode ser colocada como:

**MOSTRE SEU EXPERIMENTO**

**Abra o Virtualbox.**

**Execute a VM Backtrack 5, Execute a VM Metasploitable 2.**

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

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

1. **Escolha Ver em Backtrack** 🡪 **Forensics** 🡪 **Anti-Virus Forensics Tools** 🡪 **chkrootkit**
2. **Abra um terminal em Backtrack e localize o arquivo de execução do chkrootkit:**

**root@bt:/pentest/forensics/chrootkit#./chkrootkit**

1. **chkrootkit começará a execução imediatamente e você será provido com uma saída de tela, a medida que os “checks” são processados. Visualize a tela.**

**OUTROS COMANDOS CHKROOTKIT**

Aqui está alguns comando CHKROOTKIT úteis:

-h : Mostra o arquivo de ajuda do chkrootkit (help)

-V : Mostra a versão corrente rodando

-l : Mostra uma lista de testes disponíveis (uma letra “L” minúscula)

**CONCLUSÃO**

**Nesta prática, usamos chkrootkit para encontrar malwares, trojans (cavalos de tróia), backdoors (códigos executando em portas em máquinas remotas em proveito do atacante), logcleans (apagadores de logs), em uma VM vulnerável como Metasploitable, ou mesmo nosso localhost. Chkrootkit é um scanner muito efetivo que pode ser usado para determinar se nosso sistema tem sido atacado, ou em alguma máquina que você pense estar infectada por rootkits (um kit de malware, trojan, backdoors, logclean).**