**ESQUEMA DE PLANO DE AULA PRÁTICA**

**TAREFA 8b** "Detecção de Intrusão e Visualização de Logs"

Tópico no Moodle: “Detecção de Intrusão”

Data:

Tempo de Aula: 1 hora-aula

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

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

**ASSUNTO**

**Detecção de intrusão (IDS) é um método usado para monitorar atividade maliciosa sobre uma rede de computadores ou um sistema (uma máquina). Ou seja um IDS pode monitorar um segmento de rede ou uma máquina. Existem alguns tipos de IDS, mas o que veremos é baseado num conjunto de predefinidos de regras. Essas regras ficam situadas numa base de dados e materializam os ataques já conhecidos em redes de computadores. Numa rede, um IDS é visto como o último nível de segurança, que equivale a um alarme dentro de uma casa ou prédio, que pode alarmar quando ocorrer alguma invasão (intrusão). Um IDS adiciona uma camada adicional de segurança para uma rede por analisar informação, a partir de vários pontos na rede, e determinar se um possível ataque tem ocorrido ou localizar se um possível ataque está presente.**

**Nesta experiência, exploraremos como usar Metasploit para monitorar uma rede (nossa rede virtual – 192.1681.0), ou uma parte desta (um range de IPs de algumas máquinas desta rede), ou mesmo uma só máquina, por exemplo, a Metasploitable VM, que é bastante vulnerável. Usaremos a ferramenta Snort como nosso IDS e análise de logs. Ataques são descobertos pela verificação desses logs obtidos pelo IDS. Snort foi desenvolvido por Sourcefire e é um open source, que tem a capacidade de agir como um IDS ou um IPS (Intrusion Prevention Detection). Uma da vantagens de Snort é permitir a análise do tráfego de rede em tempo real, e tomar respostas mais rápidas, antes que a invasão ocorra.**

**Executando Snort numa rede e o utilizando para detecção de intrusão, não para (stop) exploits de ocorrerem. Snort apenas nos dá a habilidade para vermos o que está acontecendo em nossa rede.**

**BIBLIOGRAFIA BÁSICA E INSTALAÇÕES**

Visite <http://snort.org/start/rules> e baixe a Sourcefire Vulnerability Research Team (VTR) Certified Rules. Uma conjunto de regras de ataques válido deve ser mantido, no sentido de Snort funcionar para detecção. Você precisará de uma conta e pode assinar Snort em <https://www.snort.org/signup> .

Para ver uma lista estendida de comandos Snort, visite Snort User Manual em [http://www.snort.org/assets/166/snort\_manual .pdf](http://www.snort.org/assets/166/snort_manual%20.pdf)

**REQUISITOS**

1. **VM Backtrack 5.**
2. **Metasploitable 2 VM**

 **OBJETIVOS DA AULA**

Conhecer como monitorar uma máquina na nossa rede virtual, como por exemplo, a VM Metasploitable 2.

**SELEÇÃO DE CONTEÚDO – A PRÁTICA**

Um conteúdo mínimo, consistindo de um roteiro de aula, com Backtrack e 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 gráfica do Backtrack.**

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

1. **Start o service Snort:**

**Escolha Ver em Backtrack** 🡪 **Services** 🡪 **Snort Service** 🡪 **Snort Start ou Snort Stop**

1. **Abra um terminal em Backtrack e localize o arquivo de configuração:**

**root@bt:~# locate snort.conf**

1. **Edite o arquivo de configuração usando o editor nano:**

**root@bt:~# nano /etc/snort/snort.conf**

**Altere o padrão para:**

 **var HOME\_NET 192.168.1.114**

**(exemplo monitorando Metasploitable)**

**Altere o padrão para: var HOME\_NET 192.168.1.0/24**

**(exemplo monitorando a rede interna, toda, com máscara 24, significando que a parte deste IP 192.168.1 endereça a rede e o último dígito identifica a máquina na rede (114 é uma maquina da rede).**

**Precisamos qual é a rede externa considerada. Para a maior parte dos propósitos, desejamos qualquer endereço IP, que não seja parte de nossa rede interna. Assim:**

**Descomente com “#”, var EXTERNAL any**

**Altere, comentando com “#”, var External\_NET !$HOME\_NET**

1. **Depois que o serviço Snort tenha sido iniciado, deve-se executar a aplicação a partir de uma janela de terminal no Backtrack. Poucas opções são aqui descritas e usadas:**
* **-q : Esta opção diz ao Snort para rodar no modo linha de comando.**
* **-v : Este comando permite-nos a ver uma saída na tela, de cabeçalhos (TCP-UDP)/IP. Este é o chamado de “modo sniffer”.**

**Sniffer significa que pacotes de rede IP, contendo mensagens TCP-UDP são “farejados”, quando chegam na placa de rede da máquina onde o Snort funciona, a qual é passada pelo módulo Sniffer do Snort (ou qualquer IDS baseado em regras de ataques), para o status de “prosmícuo”, significando que todos os pacote recebidos são “farejados” para descobrir se tem ataques no código binário das mensagens. Um IDS assim, verifica toda a extensão do pacote que é farejado, diferentemente de um firewall que só verifica os endereços e portas, fonte-destino nos pacotes de rede.**

* **-c : Esta opção permite-nos a selecionar nosso arquivo de configuração. Neste caso, é /etc/snort/snort.conf .**
* **-i : Esta opção permite-nos especificar a interface de rede (eth1, por exemplo), que está sendo onde o monitoramento do IDS Snort ocorre.**

 **Use estas opções para executar o seguinte comando:**

 **root@bt:~# snort –q –v –i eth1 –c /etc/snort/snort.conf**

**Veja a tela de saída, mostrando os logs em eth1 da máquina 114 ou de toda uma rede interna.**

**Para parar os logs , pressione Ctrl+C**

1. **Uma experiência seria provocar um ataque na VM Metasploitable, para ver como aparece nos logs.**
2. **Para parar o Snort, dê o comando:**

 **root@bt:~# exit**

**CONCLUSÃO**

**Nesta prática, customizamos o Snort. Usamos para monitorar uma a VM Metasploitable.**