Conectando la investigación y educación europea y latinoamericana

Curso: Tratamento de Incidentes de Segurança da Informação
Prática 02: Análise de LOGs

Este roteiro de atividades visa exercitar os princípios da análise de LOGs para investigação de incidentes de segurança

Parte 01: Configuração de Servidor de LOGs

Nesta atividade a turma será dividida em duplas e cada membro irá configurar a máquina como servidor de LOGs e também a configurará para enviar os LOGs para o servidor do colega.

1. Instale o servidor de LOGs

2. Configure para receber os LOGs na porta 10514/tcp

3. Separe as mensagens de autenticação das demais

4. Salve os arquivos dos LOGs remotos em:
   /var/syslog-ng/servidores/nome-servidor/{auth.log, syslog}

5. Configure rotacionamento dos arquivos de LOG conforme Marco Civil da Internet

6. Configure o host para enviar LOGs ao servidor do colega

   6.1. Teste o envio dos LOGs
   6.2. Que tal testar o envio criptografado? Uma possibilidade é usar o *stunnel* para isso.

Parte 02: Análise de LOGs de NAT

Considere que você recebeu uma notificação de incidente de segurança informando que um host da rede de sua instituição estava fazendo atividade maliciosa. Analise o arquivo *firewall-nat.log* (que contém informações das traduções NAT da sua rede) utilizando utilitários do GNU/Linux e esteja

ápito a discorrer sobre:

1. Como foi utilizado os comandos/scripts para agilizar a análise do arquivo de LOG

2. Recomendações para ações de erradicação

3. Recomendações para ações de contenção

4. Recomendações para recuperação do incidente

Incidente reportado:
- Origem: 203.0.113.91:65152
- Data/Hora: 2019-08-05, 12:51:30 (GMT-3)
- Máquina realizando tentativas de ataque web contra a máquina xx.xx.188.223:443

OBS: Para fins didáticos do curso criamos o arquivo nat.log pequeno, porém em um ambiente real os arquivos de LOGs são muitas vezes maiores, portanto a prática é focada em criar comandos do terminal GNU/Linux que possam agilizar a análise dos LOGs.

Boa prática! Em caso de dúvidas, não hesite em consultar os instrutores.