UFBA	**X WTR do PoP-BA/RNP** Ponto de Presença da RNP na Bahia Universidade Federal da Bahia Instrutores: Italo Valcy e Gildásio Júnior	PoP-BA Ponto de Presença da RNP na Bahia

BELLA
Building the Europe Link to Latin America

Conectando la investigación y educación europea y latinoamericana

Curso: Tratamento de Incidentes de Segurança da Informação

Prática 04: Dinâmica de Tratamento de Incidentes

Este roteiro de atividades visa exercitar os princípios da dinâmica de tratamento de incidentes de segurança, abordando principalmente a parte de investigação e correção

Parte 01: Investigação de Incidentes

Na máquina WebServer-MZ-SEG4 aconteceram alguns incidentes de segurança:

- Desfiguração de dois sites
- Malware para mineração de criptomoeda instalado

Sua missão é investigar e entender por completo como esses incidentes aconteceram.

Recomendação: Conforme for encontrando informações sobre o incidente organize-as (em um arquivo docx ou txt) para facilitar na escrita de um relatório sobre o incidente.

Concluiu e ainda tem tempo? Que tal algumas práticas extras? Veja na página seguinte! :-)

Extra 1: Correção por Hardening

Um dos incidentes que ocorreu no servidor foi causado por má prática de configuração do serviço. Nesse tipo de caso, correções para sanar a vulnerabilidade, tanto por melhorias na configuração como por outros meios (ex: firewall), podem ser aplicadas.

Faça correções para sanar a vulnerabilidade específica:

1. Configure filtro das rotas expostas pelo Tomcat

2. Configure o Tomcat para escutar apenas localhost e adicione regras do IPTables para barrar o tráfego externo

Extra 2: Contenção com Fail2Ban

Em um dos incidentes foi explorada um comportamento corredo do serviço, não se tratando de nenhuma vulnerabilidade de código, por exemplo. Em casos como esses podemos atuar aplicando medidas extras de segurança.

No nosso cenário pode ser feita a configuração de um software para bloquear hosts que estejam fazendo muitas requisições para login, para isso:

1. Instale e configure o fail2ban para barrar usuários que tentam fazer muitas tentativas de login

OBS: Discuta com seu colega do lado melhores práticas para montarem uma política que deve ser aplicada no fail2ban (por exemplo: bloquear após a 10ª tentativa de login falho).

Extra 3: Aplicação de VirtualPatching

Um dos incidentes de segurança ocorreu por haver uma vulnerabilidade de implementação do software que o site web foi construído. Em casos como esse o mais recomendado é aplicar o patch de correção desenvolvido pela equipe oficial da aplicação.

Considere um cenário que você não pode aplicar o patch de correção (seja pelo patch ainda ter vulnerabilidades, seja pela necessidade burocrática para um processo desses etc.) mas que ainda assim é necessário fazer a mitigação dessa vulnerabilidade.

Uma possibilidade para casos como esses é a aplicação de virtual patching. Vamos utilizar o ModSecurity para barrar explorações dessa vulnerabilidade:

1. Entenda como a vulnerabilidade ocorre e como ela é de fato explorada

2. Entenda como funciona a criação de regras no ModSecurity

3. Crie regras no ModSecurity que barre um ataque que explore essa vulnerabilidade em específica.

4. Faça testes a fim de testar se realmente a vulnerabilidade foi sanada.

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