LEI: Segurança Informática e nas Organizações 2019-2020

Projeto 4: Análise de Sistemas

Entrega: 3 de Janeiro 2020, 23:59

Objetivos

- Análise de registos de operação
- Utilização de mecanismos de confinamento
- Controlos do SO Linux
- Permissões de ficheiros

1 Descrição

Bom dia,

A nossa empresa recebeu um pedido de um cliente que parece estar em apuros. Aparentemente alguém invadiu um dos servidores (uma VM). A Firewall externa detetou uns downloads suspeitos e congelaram logo a VM, pelo que o atacante (se é que foi um ataque) não deve ter feito muito. Foi um aviso automático, pelo que não se descarta ser um falso alarme. Eles têm duas Firewalls: uma para a Internet e outra para a rede Interna.

Isto já é um cliente antigo, de uma loja chamada Express Motors. O programador não é o melhor (aliás, conheço poucos piores), pelo que a página possui bastantes problemas. Em tempos a nossa empresa fez uma auditoria ao software e pentest. Reportámos muitas coisas básicas, a maioria relacionada com a má utilização de PHP. Segundo me lembro era possível realizar SQL injection no login, nos campos dos produtos (type ou productid...), o PHP para downloads permitia obter ficheiros do sistema, etc... Não havia um único query bem construído. Até faziam um include diretamente de um GET (o lang=XX típico). Foi uma daquelas análises longas de fazer.

Recomendámos usarem confinamento, acederem à DB devidamente e validarem corretamente todas as entradas. Claramente não implementaram

alguma coisa e agora poderá ter acontecido algo mais grave.

O nosso trabalho vai ser de análise forense para verificar o que aconteceu e qual o impacto.

Prepara um relatório que descreva com detalhe:

- O que estava implementado a nível de confinamento das aplicações (tínhamos recomendado isto).
- Qual a sequência de ações que o atacante tomou?
- Que vulnerabilidades foram exploradas e como? Quais o atacante tentou explorar mas foram barradas?
- Que alterações foram realizadas e qual o propósito aparente?
- Foram realmente realizadas transferências? Se sim, como e qual o conteúdo?
- Porque é que a Firewall externa detetou transferências mas não detetou as restantes ações?

Para auxiliar este trabalho, podes encontrar 2 imagens do disco da VM. Uma possui a imagem de referência que a empresa utiliza. A outra possui a imagem da VM que suspeitam ter sido atacada.

Podes montar ambas as imagens (Read-only), numa VM que já tenhas e comparar os sistemas de ficheiros (find, diff, rdiff, etc...) Deverão existir registos em /var/log.

2 Notas

Considera-se que os trabalhos são realizados por 2 alunos e que o documento final submetido é de sua autoria. A utilização de recursos existentes na Internet ou partilhado com outros colegas leva à anulação imediata do trabalho.