Laboratório Avançado de Produção Pesquisa e Inovação em Software

Escopo dos Testes de Penetração (Pentesting scope)

Red Team @ LAPPIS

Brasília, aos 17 de Julho de 2024

1. Introdução

O presente documento consiste na definição de escopo dos testes de penetração que serão executados pelo time responsável pela segurança do projeto Brasil Participativo – BP composto atualmente por Rodolfo Cabral Neves, cujo objetivo é elucidar as atividades serão realizadas, os objetivos dos testes, os objetos em estudo ou *assets* que serão testados, metodologias análise de riscos e restrições bem como as suas limitações e necessidades.

2. Objetivo

O teste de penetração - *pentest* tem como objetivo descobrir e identificar **todas** as vulnerabilidades nos sistemas sob investigação e melhorar a segurança dos sistemas testados.

3. Metodologia

A abordagem utilizada nos testes será do tipo *White-Box* para os servidores que se encontram na rede de homologação e produção, e *Black-Box* para a plataforma do Brasil Participativo – BP de homologação e produção. Durante o processo de testes, serão utilizadas algumas ferramentas de automação e outros serão realizados de forma manual, para não causar quaisquer instabilidades na rede ou nos servidores internos e manter sempre os sistemas disponíveis.

4. Escopo

Os testes terão os seguintes objetos:

1. Plataforma LAB-DECIDE (em ambiente de homologação)
    - Tipos de vulnerabilidades:
        - Exposição de dados sensíveis
        - Cross Site Scripting - XSS
        - Injection:
            - SQL Injection
            - Operating System Injection
        - File upload/inclusion
        - HTTP Verb Tampering
        - Insecure Direct Object References - IDOR
        - Broken Authentication
        - Denial of Service – Causado pelo mau tratamento de dados
2. Plataforma Brasil Participativo (em ambiente de produção)
    - As mesmas falhas que o item 1 (LAB-DECIDE)
3. Ambiente de produção:
    - IPs: 192.168.3.4, 192.168.3.6, 192.168.3.7, 192.168.3.9 e 192.168.3.10
    - Faixa de portas: 1 a 1000, 30000 a 32767 e 6444
    - Tipos de vulnerabilidades que se deseja encontrar:
        - Má configuração dos servidores
        - Softwares desatualizados
        - Senhas fracas
        - Problemas de autenticação
        - Injeção de comandos
4. Ambiente de homologação:
    - IPs: 192.168.3.21 e 192.168.3.22
    - Faixa de portas: as mesmas que o item 3 (do ambiente de produção)
    - Tipos de vulnerabilidades:
        - As mesmas que o item 3 (do ambiente de produção)

5. **Limitações**

Eis as atividades que **NÃO** serão realizadas durante o processo de testes:

- Alteração de qualquer arquivo configuração de algum servidor
- Alteração de qualquer informação sensível
- Exposição de qualquer informação sensível
- Comprometimento de qualquer servidor
- O teste de quaisquer servidores/aplicações que não estão descritos no escopo

6. Prazos

Os testes serão conduzidos a partir do momento da aprovação da empresa responsável pela infraestrutura, e terá duração de 1 mês e 2 semanas, podendo ser prorrogada de acordo a necessidades específicas.

Renato Coral Sampaio, Representante do LAPPIS

Rodolfo Cabral Neves, líder do time de segurança do LAPPIS