Operação CyberSleuth - Desafio de Segurança Cibernética

Introdução ao Cenário:

Você faz parte de uma equipe de segurança cibernética contratada pela **GlobalTech Inc.**, uma empresa multinacional que suspeita de vulnerabilidades críticas em sua rede interna com o intervalo de IPs **192.168.100.1/24**. Durante uma auditoria interna, foi identificado que a empresa possui dois ambientes web distintos:

1. **Ambiente de Desenvolvimento** (Portal do Aluno em Teste): Este ambiente está sendo utilizado pelos desenvolvedores para testar novas funcionalidades no **Portal do Aluno**. Suspeita-se que ele contém vulnerabilidades ainda não corrigidas, oferecendo uma superfície de ataque para intrusos.
2. **Ambiente de Produção** (Portal do Aluno): Este é o site utilizado pelos alunos da GlobalTech para acessar informações pessoais e acadêmicas. A empresa teme que vulnerabilidades presentes no ambiente de desenvolvimento possam ser exploradas para comprometer o ambiente de produção.

A máquina com o IP **192.168.100.10** hospeda o **Portal do Aluno em Teste** e possui a porta **22** aberta, sugerindo a presença de um serviço SSH. Sua missão é explorar as vulnerabilidades encontradas nesse ambiente, comprometendo o sistema e exibindo as **flags** durante a exploração.

Contexto:

A **GlobalTech Inc.** opera diversos sistemas críticos que suportam suas operações diárias, com dois portais principais:

1. **Portal do Aluno em Teste**: Usado para o desenvolvimento e testes do sistema de alunos. Este ambiente está isolado do ambiente de produção, mas acredita-se que contenha vulnerabilidades que podem ser exploradas.
2. **Portal do Aluno** (Produção): Este é o portal oficial acessado pelos alunos. Ele armazena informações sensíveis e precisa estar protegido de qualquer intrusão.

Objetivos da Missão:

1. **Análise de Vulnerabilidade no Portal do Aluno em Teste**:
    - Sua primeira tarefa é avaliar a segurança do **Portal do Aluno em Teste** no ambiente de desenvolvimento. Mapeie as portas e serviços disponíveis (incluindo o SSH na porta 22) e identifique falhas potenciais, como vulnerabilidades de **SQL Injection** e **força bruta** no login.
2. **Exploração e Acesso**:
    - Caso seja identificado que o portal de teste pode ser comprometido, utilize técnicas de ataque para explorar as vulnerabilidades e acessar o sistema.
    - Uma vez dentro do portal de teste, investigue a aplicação e veja se há formas de acessar ou influenciar o ambiente de produção, o **Portal do Aluno**.

3. **Acesso ao Portal de Produção**:
    - Se houver uma ligação entre o portal de teste e o portal de produção, descubra como utilizá-la para acessar o **Portal do Aluno** de maneira segura e discreta.
    - Identifique possíveis flags escondidas no sistema e mostre sua capacidade de explorar os sistemas com sucesso.
4. **Exibição das Flags**:
    - Após comprometer o ambiente de teste ou produção, capture as flags como evidência de que o sistema foi explorado com sucesso.

Conclusão Esperada:

Após o sucesso da missão, você deverá preparar um relatório detalhado contendo:

- **Vulnerabilidades encontradas**: Descreva as falhas descobertas no **Portal do Aluno em Teste** e como elas foram exploradas.
- **Etapas de Exploração**: Detalhe as etapas realizadas para comprometer os sistemas, incluindo ferramentas e técnicas usadas.
- **Flags Capturadas**: Apresente as flags encontradas durante a exploração.
- **Recomendações de Segurança**: Forneça recomendações sobre como a **GlobalTech Inc.** pode corrigir as vulnerabilidades e fortalecer a segurança do **Portal do Aluno** nos ambientes de teste e produção.

Recursos Disponíveis:

- **Acesso ao ambiente de desenvolvimento (Portal do Aluno em Teste)** hospedado na rede interna da GlobalTech, com o IP **192.168.100.10**.
- Ferramentas básicas de **teste de penetração.**

Nota aos Alunos:

Este cenário requer uma abordagem metódica e criativa para solucionar problemas complexos de segurança. Vocês deverão explorar e investigar o ambiente para identificar as vulnerabilidades, sem orientações diretas. A aplicação das melhores práticas de **segurança cibernética** será essencial para alcançar o objetivo final.

Critérios de Avaliação:

1. **Capacidade de identificar vulnerabilidades** e explorar falhas no ambiente de desenvolvimento (SQL Injection, força bruta, má configuração).
2. **Uso correto de ferramentas** de análise e ataque.
3. **Compreensão das conexões entre o ambiente de desenvolvimento e o de produção** e capacidade de transitar entre eles.

4. **Clareza e organização do relatório** final, com sugestões de como mitigar as vulnerabilidades encontradas.
5. **Eficiência na captura das flags** e na exploração das vulnerabilidades.