ISO 09

Penetration Test Report for   
ISO9

v.2.0

[lucas.bona@pucpr.edu.br](mailto:lucas.bona@pucpr.edu.br)

[silva.ary@pucpr.edu.br](mailto:silva.ary@pucpr.edu.br)

adriano.vale@pucpr.edu.br

OSID: Apache/2.4.29 (Ubuntu)

ISO9

Copyright © 2021 Offensive Security Ltd. All rights reserved.

No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distant learning, in any form or by any means such as any information storage, transmission or retrieval system, without prior written permission from Offensive Security.

Conteúdos

1.0 ISO9 Penetration Test Report 3

1.1 Introdução 3

1.2 Objetivo 3

1.3 Requisitos 3

2.0 Resumo 4

2.1 Recomendações 5

3.0 Metodologias 5

3.1 Coleta de Informação 5

3.2 Enumeração de Serviço 6

3.3 Pentest 7

3.4 Acesso Mantido 14

3.5 Limpeza 14

4.0 Informações Adicionais 14

1.0 ISO9 External Penetration Test Report

## 1.1 Introdução

O relatório do Pentest ISO9 contém todos os esforços realizados para aprovar o curso de Ethical Hacking. Este relatório inclui todos os elementos utilizados para passar no exame geral e será avaliado com base na correção e abrangência de todos os aspectos do exame. O propósito deste relatório é garantir que o estudante demonstre uma compreensão completa das metodologias de Pentesting, bem como o conhecimento técnico necessário para ser aprovado o curso.

## 1.2 Objetivos

O objetivo desta avaliação é realizar um teste interno de penetração na Offensive Security Lab e na rede de exames. O estudante tem a tarefa de seguir uma abordagem metódica para obter acesso aos objetivos estabelecidos. Este teste deve simular um teste de penetração real e como você começaria do início ao fim, incluindo o relatório geral. Uma página de exemplo já foi criada para você nas últimas seções deste documento, que deve fornecer informações suficientes sobre o que é esperado para passar neste curso. Use o relatório de exemplo como um guia para orientá-lo na elaboração do relatório.

## 1.3 Requisitos

The student will be required to fill out this penetration testing report fully and to include the following sections:

* Resumo e Recomendações
* Metodologias utilizadas e quais os passos dados
* Prints, passo a passo, código, provas
* Informações Adicionais

# 2.0 Resumo

Ary, Lucas e Adriano foram designados para realizar um teste externo (Back Box) de penetração em uma ISO fornecida pelo professor. O teste envolve ataques direcionados a uma máquina virtual. O foco deste teste era realizar ataques semelhantes aos de hackers e tentar realizar invasões no sistema da ISO. O objetivo geral dos estudantes era avaliar, identificar e explorar falhas e vulnerablilidades e relatar os resultados obtidos.Durante a realização do Pentest externa, foram identificadas várias vulnerabilidades preocupantes na ISO fornecida pelo professor. Durante os ataques, Ary, Lucas e Adriano identificaram diversas vulnerabilidades, dentre elas patches desatualizados e configurações de segurança deficientes. Durante os testes, os estudantes tiveram acesso de nível administrativo a várias máquinas.

Máquina 1 - Acesso obtido através de Brute Force

## 2.1 Recomendações

Os estudantes recomendam que os desenvolvedores atualizem a versão do Apache, já que a que foi encontrada (Apache/2.4.29) é uma versão considerada desatualizada, já que depois dela foram lançadas mais de 15 versões novas que corrigem falhas que surgiram nessa e nas versões posteriors.

# 3.0 Metodologias

A metodologia usada foi o OWASP, para a consulta do documento Owasp Top 10

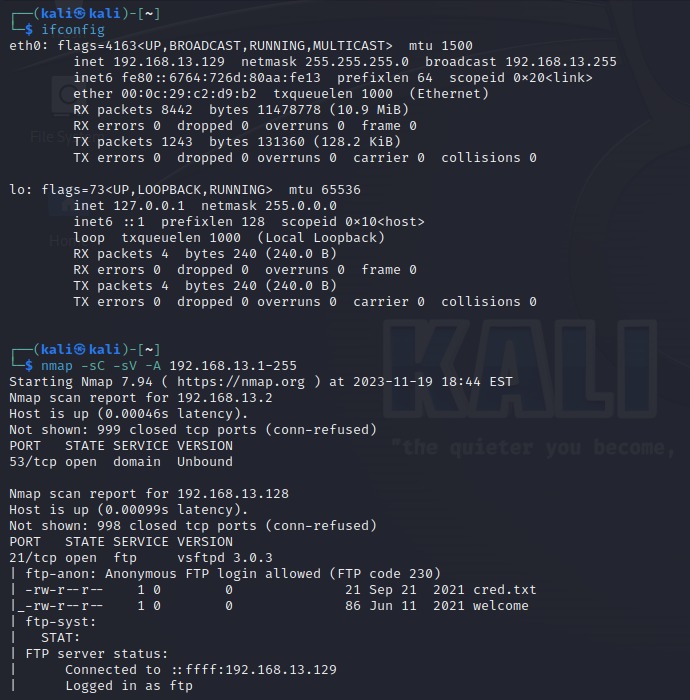
## 3.1 Coleta de Informação

Os alunos decobriram que o Sistema utiliza de protocolos HTTP, como head e get, que não tem a mesma segurança que no protocolo HTTPS. Além disso, foi descoberto 3 páginas: /go.php, /index.php e /login.php

**IP’s do SERVER**

192.168.236.130

192.168.13.128 – (ex)



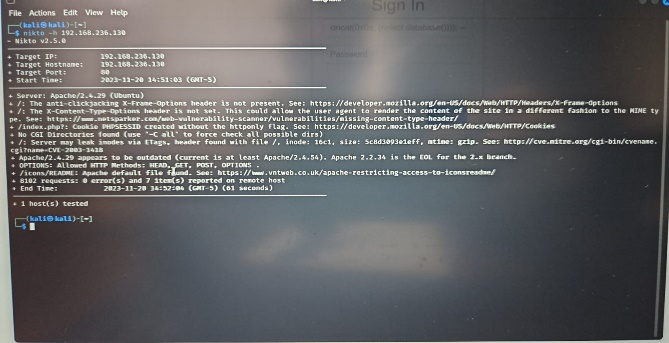
## 3.2 Numeração de Serviço

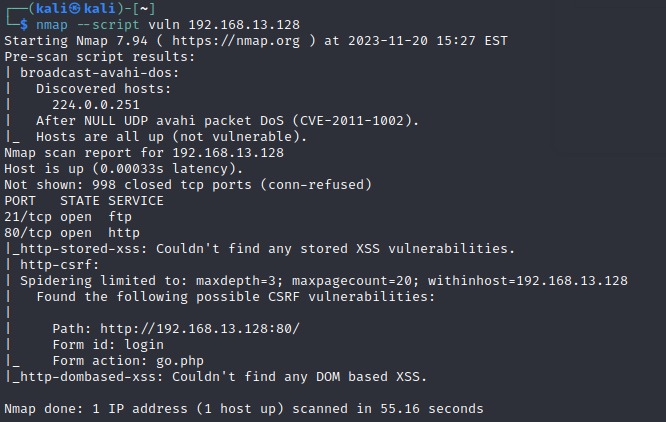
A fase de enumeração de serviços em um teste de penetração visa identificar quais serviços estão ativos em um sistema. Essa informação é valiosa para um atacante, pois revela detalhes sobre potenciais pontos de ataque. Entender quais aplicativos estão em execução fornece ao invasor informações essenciais antes de iniciar o teste de penetração. Em alguns casos, algumas portas podem não ser listadas.

|  |  |
| --- | --- |
| Server IP Address | Ports Open |
| 192.168.236.130 | TCP: 80 |
| 192.168.13.128 | TCP: 80, 21 |

## 3.3 Pentest

Durante o teste, os alunos conseguiram achar algumas vulnerabilidades, com ajuda das ferramentas Nmap, Nikto e WhatWeb para mapeamento do Sistema:





Texto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamente

|  |
| --- |
| **Vulnerabilidade**: Brute Force  **IP’s do Sistema**: 192.168.236.130 e 192.168.13.128  **Explicação**: Um ataque de força bruta é uma técnica para obter acesso não autorizado aos sistemas através da tentativa sistemática de adivinhar credenciais de usuário. Os ataques de força bruta envolvem o uso de programas automatizados que testam diversas combinações de nomes de usuário e senhas em alta velocidade até encontrar as corretas. Nesse teste, foram utilizadas ferramentas como Hydra para o Brute Force.  **Mitigação:** Para a mitigação de Força Bruta, ideias como limitação de tentativas de login, monitoramento de logins suspeitos em tempo real, atualizações regulares e bloqueio temporário após tentativas mal sucedidas..  **Ameaça:** Média  **Prints:** |
| **Vulnerabilidade**: CSRF – Cross Site Request Forgery  **IP’s do Sistema**: 192.168.236.130  **Explicação**: Ocorre quando um atacante engana um usuário autenticado para realizar ações não autorizadas em um aplicativo web no qual o usuário está logado. Isso é feito induzindo o usuário a executar solicitações não desejadas sem seu conhecimento. Um exemplo seria a inserção de código malicioso em uma página web visitada pelo usuário, levando o navegador a enviar solicitações falsificadas para o aplicativo web autenticado.  **Mitigação:** Para mitigar o CSRF, as aplicações geralmente utilizam tokens anti-CSRF incorporados em formulários para verificar a legitimidade das solicitações.  **Ameaça**: Crítica  **Prints**: | |

## 3.4 Acesso Mantido

…

## 3.5 Limpeza

A fase de "limpeza" da avaliação garante que resquícios do teste de penetração sejam removidos. Frequentemente, fragmentos de ferramentas ou contas de usuário são deixados nos computadores de uma organização, o que pode resultar em problemas de segurança no futuro.

Após concluir as ações planejadas, Ary, Lucas e Adriano removeram todas as contas de usuário e senhas, assim como outros programas instalados no sistema. A ISO9 não deveria precisar remover contas de usuário ou serviços do sistema.

# 4.0 Informações Adicionais