Relatório de Teste de Invasão #2:

Edição de HTML no Apache2

Objetivo:

Este relatório documenta o processo de edição de uma página HTML hospedada no Apache2 após a obtenção de acesso ao superusuário em um servidor Linux. A edição do arquivo `index.html` visa alterar o conteúdo visível, como a mensagem padrão "It works!" para informações personalizadas. O relatório descreve o processo detalhado de navegação pelo sistema de arquivos do servidor e edição do HTML por meio de comandos no terminal.

Autor: *Enzo Arrue Juan Fuso*
Faculdade: *Fatec São Caetano do Sul*
Curso: *Segurança da Informação*

Introdução:

Após o sucesso de um ataque que possibilita acesso ao usuário comum de um servidor, o próximo passo em muitos cenários de invasão envolve a escalada de privilégios para o superusuário (root). Neste caso, a edição de um arquivo HTML hospedado no servidor Apache2 serve para demonstrar o controle sobre a interface pública do sistema, ilustrando a vulnerabilidade. Ao modificar o arquivo `/var/www/html/index.html`*, é possível alterar o conteúdo exibido quando o servidor é acessado via navegador, evidenciando uma falha de segurança potencialmente explorável em ambientes sem as devidas proteções.*

Softwares/Ferramentas Utilizados:

VirtualBox (Serviço HTTP - Apache2), Navegador Web

Metodologia:

Contextualização*:** Após ter conseguido o acesso ao ***usuário comum do servidor, terá que passar para o superusuário para editar o HTML no Apache2.

Passo a Passo:
1-) su “nome_do_superusuário”
2-) Digitar a senha do superusuário que será pedida

Digitar os comandos para editar o HTML do Apache2 (deverá ser editado o retângulo laranja escrito “It works!” e colocar o nome dos integrantes do grupo).

No Google: Na barra de pesquisa digitar o IP do servidor, o Apache2 vai abrir uma parte no corpo com uma URL html (`/var/www/html/index.html`) que será usada como base para os comandos.

Comandos no WSL Superusuário:
1-) cd /var/www/html
2-) sudo nano /var/www/html/index.html

1. Editar o código html aberto e procurar por “<body>” ; “ ; e por fim a mensagem que deverá ser editada “It works!”

Assim que editado ctrl + O e ctrl + X, ir onde está aberto o apache 2 e restaurar a página ou abrir uma nova para verificar se foi mudado.

Recomendações:

Restrição de Acesso a Superusuário: Limitar o acesso ao superusuário e desabilitar login direto via SSH para o root são medidas que dificultam a escalada de privilégios.

Auditoria de Mudanças: Implementar um sistema de auditoria para monitorar e registrar alterações em arquivos críticos, como os hospedados no Apache, ajudando a identificar acessos indevidos.

Segurança do Apache2: Configurar permissões adequadas no servidor Apache2, permitindo apenas a edição de arquivos por usuários autorizados.

Links Complementares:

Guia de Edição de HTML no Linux - https://www.linux.com/training-tutorials/editing-html-files-linux-terminal/

Documentação oficial do Apache2 - https://httpd.apache.org/docs/2.4/

Ferramenta para verificar se o código HTML está de acordo com os padrões web - https://validator.w3.org/

Introdução ao HTML: Guia básico sobre HTML e suas funções - https://www.w3schools.com/html/