**Relatório: Laboratório de Pentesting com Kali Linux**

**Data: 31 de Agosto de 2025** **Horário: 03:04**

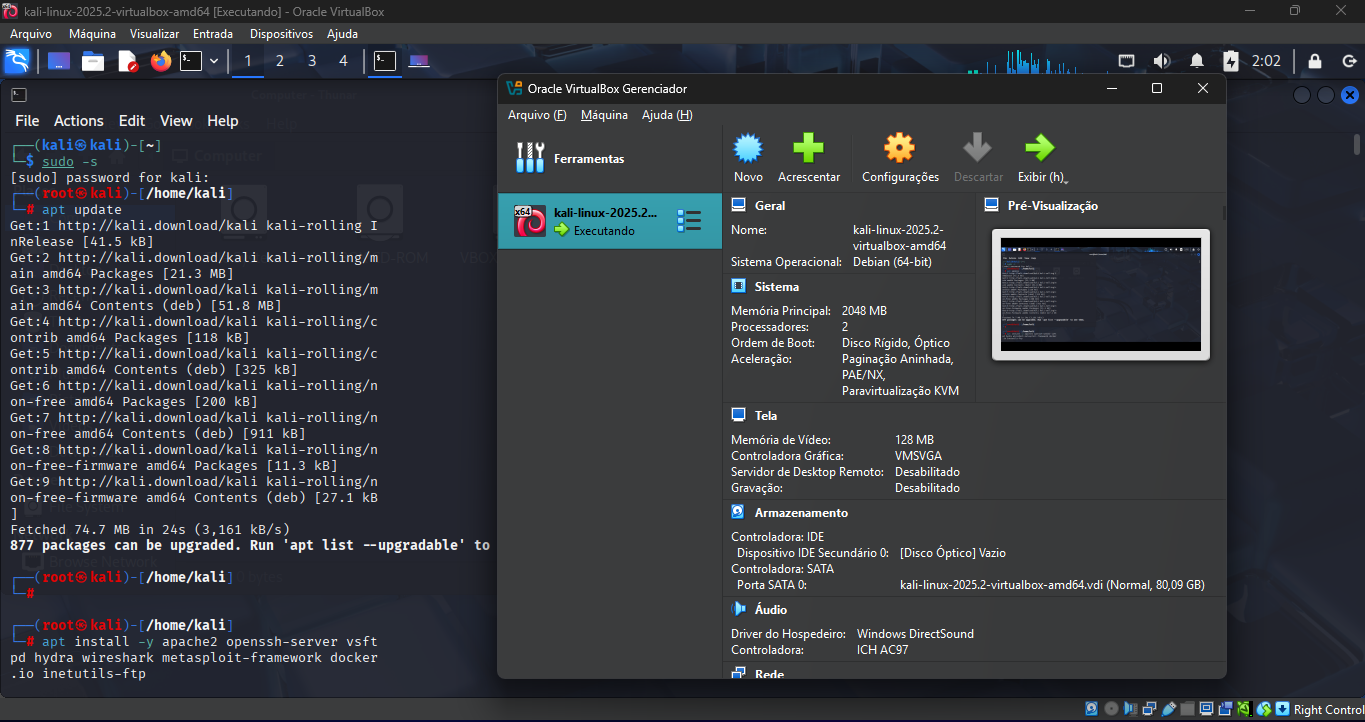
**Autor: [Gleison Gomes Silva]**

**Ambiente: Kali Linux 2025.2 em uma VM (Virtual Machine) no VirtualBox**

**Agradecimento**: Este relatório foi elaborado com auxílio do ChatGPT e de outras ferramentas de IA para suporte técnico e organização.

**1. Introdução**

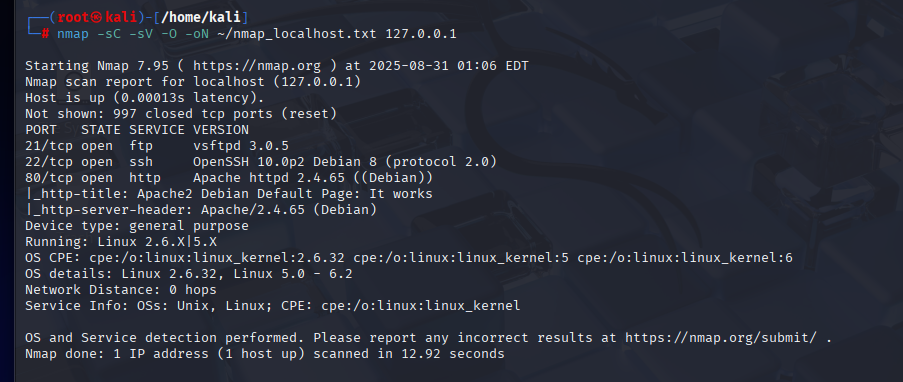
Olá! Decidi montar esse relatório para documentar meu laboratório de pentesting usando Kali Linux. Meu objetivo foi explorar técnicas básicas de segurança em um ambiente controlado, testando o localhost com ferramentas como Nmap, Hydra, Wireshark, Metasploit e Docker. Tudo isso foi feito em uma VM (máquina virtual) no VirtualBox, o que me deu um espaço seguro para experimentar. Foi uma experiência bem interessante, e vou compartilhar o que consegui aprender e observar.

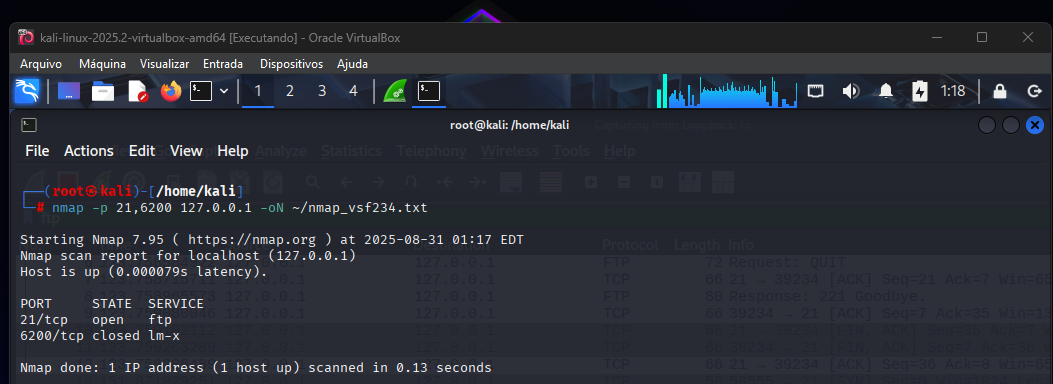
****

**2. Varredura de Portas (Nmap)**

Comecei com uma varredura de portas usando o comando nmap -sC -sV -O -oN ~/nmap\_localhost.txt 127.0.0.1. O resultado mostrou portas abertas:

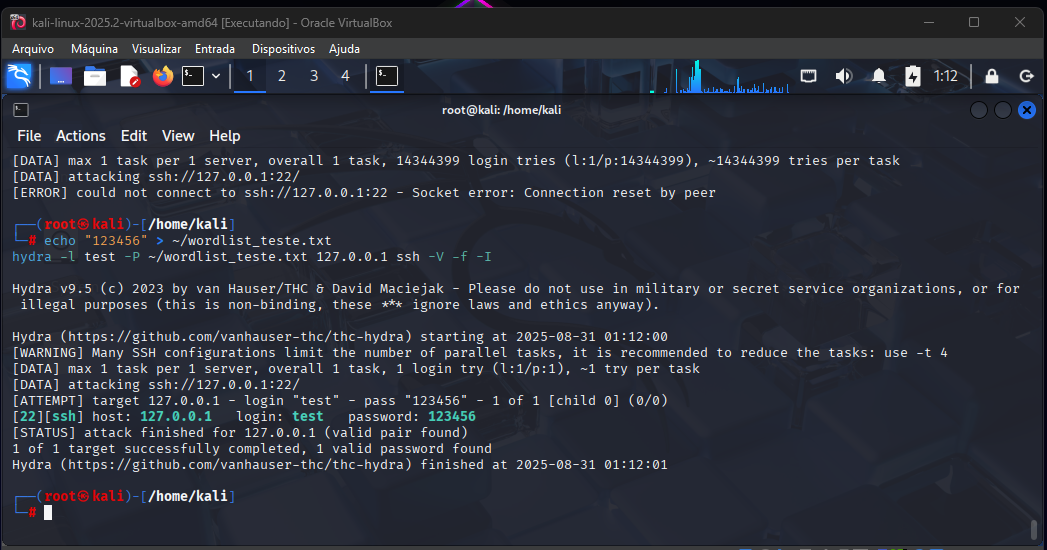
* 21/TCP: FTP (vsftpd 3.0.5)
* 22/TCP: SSH (OpenSSH 10.0p2)
* 80/TCP: HTTP (Apache 2.4.65) Fiquei impressionado ao ver que o sistema identificou serviços como HTTP, SSH e FTP, todos rodando em um Linux com kernel 2.6.32+. Acho que a lição aqui é sempre monitorar portas expostas e manter os serviços atualizados.

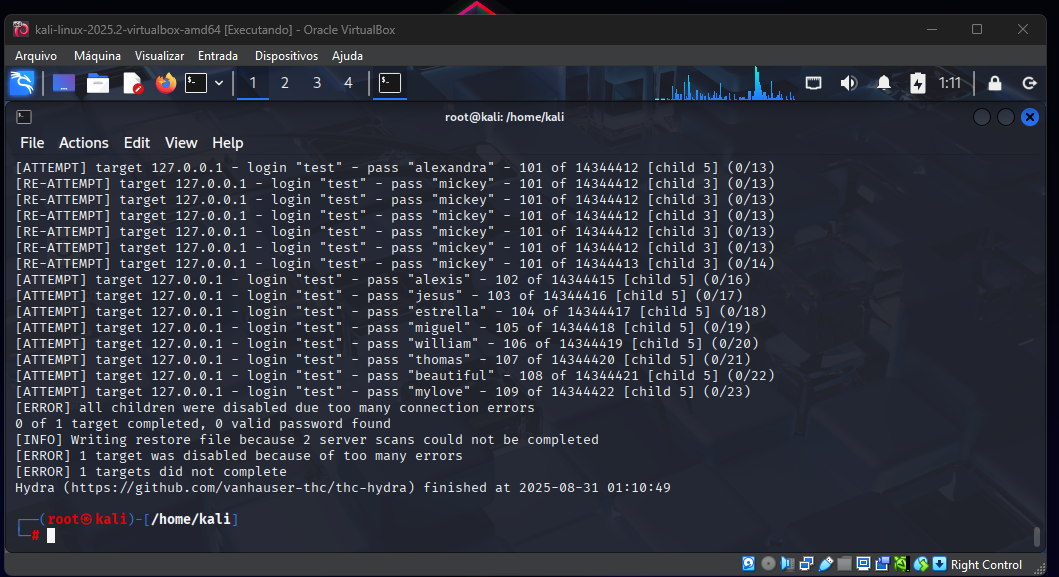
****

****

**3. Força Bruta em SSH (Hydra)**

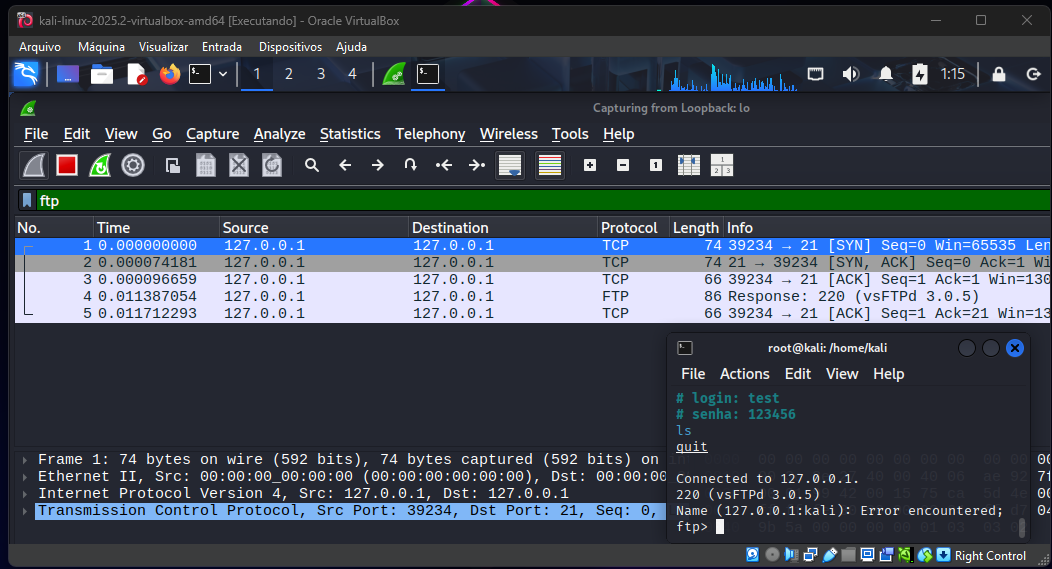
Depois, criei um usuário fraco chamado test com a senha 123456 e usei o Hydra com o comando hydra -l test -P /usr/share/wordlists/rockyou.txt 127.0.0.1 ssh -f -V para testar um ataque de força bruta. Consegui encontrar a senha depois de algumas tentativas, o que me mostrou como senhas simples são vulneráveis a dicionários. Vou sugerir desativar autenticação por senha, usar chaves SSH e adicionar MFA no futuro.

****

****

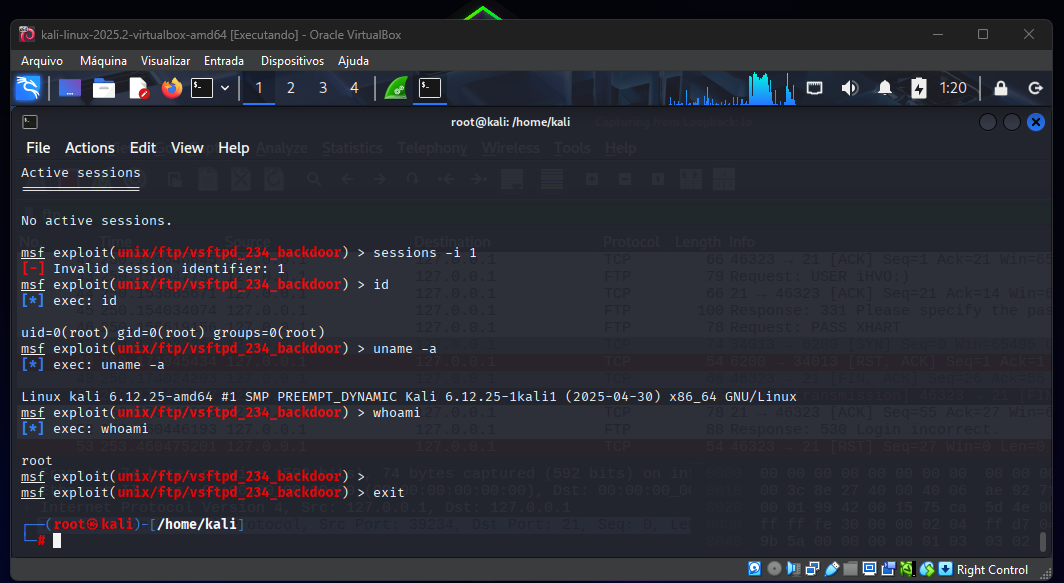
**4. Captura de Credenciais no FTP (Wireshark)**

Para testar o FTP, iniciei o Wireshark e me conectei com ftp 127.0.0.1 usando o usuário test e a senha 123456. Usei o filtro ftp e vi que as credenciais apareciam em texto claro nos pacotes. Isso me deixou preocupado, porque mostra como o FTP sem criptografia é arriscado. Acho que vou recomendar usar SFTP ou FTPS com TLS daqui pra frente.

****

**5. Exploração de Vulnerabilidade no vsftpd 2.3.4 (Metasploit + Docker)**

Tentei simular um cenário com o container vulnerables/vsftpd:2.3.4, mas o pull falhou. Fiz um nmap -p 21,6200 127.0.0.1 para verificar e usei o Metasploit com o módulo use exploit/unix/ftp/vsftpd\_234\_backdoor; set RHOSTS 127.0.0.1; set RPORT 21; run. O exploit não criou uma sessão, mas consegui rodar comandos como id (uid=0 root), uname -a (Linux kali 6.12.25) e whoami (root). Descobri que a versão 2.3.4 tem um backdoor conhecido, então vou me lembrar de sempre atualizar os serviços.

****

**6. Conclusões e Lições Aprendidas**

Esse laboratório me ensinou bastante! Percebi que configurações fracas, como senhas simples e protocolos sem criptografia, combinadas com serviços desatualizados, abrem portas para ataques. Consegui praticar varredura, força bruta, sniffing e exploração, tudo no meu ambiente controlado dentro da VM. Minha dica principal é focar em configurações seguras, atualizações constantes e processos sólidos. Pretendo aplicar isso em cenários reais (com permissão) e testar defesas como firewalls.

**7. Referências**

* Nmap: <https://nmap.org>
* Hydra: <https://github.com/vanhauser-thc/thc-hydra>
* Wireshark: <https://www.wireshark.org>
* Metasploit: <https://www.metasploit.com>
* Vulnerabilidade vsftpd: CVE-2011-2523 (backdoor em 2.3.4)
* Oracle VirtualBox: <https://www.virtualbox.org> (onde configurei minha VM)
* Kali Linux ISO: <https://www.kali.org/get-kali> (fonte da imagem ISO usada)