Pentest em redes abertas: estado atual da segurança observada em SSIDs abertos

Faculdade de Computação - Universidade Federal de Mato Grosso do Sul (UFMS)
Caixa Postal 549 - 79070-900 - Campo Grande - MS, Brazil
Gustavo Damico Dionisio

RESUMO

Este trabalho tem como objetivo avaliar a segurança de redes Wi-Fi públicas por meio de testes de intrusão, com o objetivo de identificar vulnerabilidades e verificar a possibilidade de acesso a informações disponíveis. Os resultados obtidos demonstram que, apesar da maioria das redes exigidas anteriormente, ainda persistem diversas vulnerabilidades passíveis de exploração por agentes mal-intencionados.

1. INTRODUÇÃO

A tecnologia tem evoluído rapidamente, revolucionando a forma como vivemos, trabalhamos e nos comunicamos. Com isso, as redes sem fio buscam atender às necessidades do mercado, tornando-se cada vez mais populares por todos os lugares. A internet começou a fazer parte de nossas vidas no ano de 1994. Naquele ano, os recursos da rede de internet, que até então eram restritos ao meio acadêmico e algumas comunidades, foram disponibilizados ao público em geral (Lins, 2013).

Isso nos leva a ficar atentos aos ataques de intrusão, pois atualmente vários locais oferecem uma rede hotspot (internet sem fio) para que os usuários possam se conectar, geralmente por meio de uma autenticação com senhas (Cesca & do Prado, 2023).

Segundo (Cesca & do Prado, 2023), ao longo do tempo, a internet transformou o comportamento e o cenário da sociedade, tornando a tecnologia mais acessível e integrada ao dia a dia das pessoas. As

empresas tiveram que se adaptar a essa nova realidade para se destacarem em um mercado cada vez mais competitivo. Desse modo, a tecnologia tem desempenhado um papel crucial para tornar as organizações mais eficientes, fornecendo informações que apoiam a tomada de decisões e contribuições para a obtenção de melhores resultados.

Vale ressaltar a importância da segurança. Redes de conexão sem fio (wireless) tendem a ser transparentes, o que pode representar um risco para empresas que não as gerenciam com o devido cuidado (Algar Telecom, 2022). Uma rede wifi pública, em que não há o controle direto de acesso, pode ser invadida por hackers. Nesse cenário, pessoas mal-intencionadas podem monitorar os dados transferidos nessa rede e acessar informações pessoais e privadas dos usuários.

Nesse contexto, este trabalho se propõe a investigar o nível de segurança que as empresas apresentam para manter protegidas as suas informações e os seus dados, evitando ataques por hackers maliciosos.

Como resultados, observamos que a maioria das empresas atualmente possui um certo nível de segurança em suas redes de internet sem fio disponibilizada aos usuários, o que impede o fácil acesso de hackers em busca de obter informações confidenciais.

2. REFERENCIAL TEÓRICO

Uma rede aberta de telecomunicação (em inglês: *Open-access network, OAN*) é uma rede destinada à telecomunicação que é dividida em camadas horizontais, em oposição àquelas de uma operadora tradicional, que, com a finalidade de prestar um serviço, verticaliza todas as camadas sob uma única empresa (M. Forzati, C. P. Larsen, C. Mattsson, 2010).

De acordo com (M. Forzati, C. P. Larsen, C. Mattsson, 2010), uma rede de telecomunicação é dividida em três camadas:

1. Infraestrutura

2. Comunicação
3. Serviço

O objetivo final do compartilhamento de redes é proporcionar uma maior quantidade de opções ao cliente final. A existência de uma rede aberta, onde diversos provedores possam acessar de maneira indiscriminada e com tratamento isonômico, derruba-se o maior obstáculo à entrada de novos competidores no mercado de telecomunicação, que é a construção de infraestrutura de redes (M. Forzati, C. P. Larsen, C. Mattsson 2010).

Um *firewall*, é um dispositivo de segurança de rede que monitora o tráfego de entrada e saída, e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança. Essas regras incluem critérios de filtragem, como o tipo de protocolo, os endereços IP de origem e destino, e as portas de origem e destino. Quando o firewall considera que uma rede é segura, ele estabelece uma conexão entre essa rede e o computador ou a rede interna que protege.

Normalmente, o objetivo do *firewall* é ajudar a evitar atividades mal-intencionadas e impedir que qualquer pessoa, dentro ou fora de uma rede privada, realize atividades não autorizadas na Web. (Erika Hoyer, Pedro Meirelles, Renan Protector, 2013).

Hotspot é um ponto de acesso para conexão Wi-Fi que permite que as pessoas se conectem a uma rede sem fio e utilizem a internet sem estarem presos a cabos. É um ponto físico, que é obtido a partir de equipamentos como roteador e um modem.

Em outras palavras, é um local que oferece internet sem fio, geralmente por meio de uma autenticação com senhas (Algar Telecom, 2022).

3. TRABALHOS RELACIONADOS

De acordo com (Almeida Jr, 2021), o processo de pentest precisa atender a vários requisitos, entre eles, economia de custo e confiança. (PICONI, R. D. C., 2016), cita que muitas empresas negligenciam medidas preventivas de segurança, principalmente em redes abertas, até sofrerem prejuízos.

Segundo os autores, essa segurança pode ser verificada periodicamente usando Pentest (PICONI, R. D. C., 2016). Para verificações em nível de enlace, é possível utilizar Arp Poison, como apresentado por (Mitola III, J., & Prys, M., 2024).

Como estudo de caso, foram exploradas algumas redes abertas e fechadas em determinados locais, utilizando três ferramentas, para a tentativa da realização dos testes de intrusão. Os resultados apontaram a possibilidade de descobrir redes sem fio próximas, bem como a tentativa de descoberta de senha da rede e outras informações importantes.

Como observado nos trabalhos relacionados, as ferramentas ARP, Nmap(portscan) e Aircrack-ng são utilizadas atualmente para a realização de Pentests utilizando o Kali Linux. Assim, neste trabalho, essas ferramentas foram utilizadas para compor os ataques exploratórios.

4. MATERIAIS E MÉTODOS

A ferramenta utilizada para a execução desse trabalho foi o Kali Linux, um sistema operacional que permite realizar "pentests, análises de vulnerabilidade e auditoria de segurança". Neste trabalho utilizamos a versão 2024.2, que é a versão mais recente atualmente. Inclui 18 novas ferramentas e o Gnome 46.

A primeira ferramenta do Kali utilizada para a realização dos testes de pentest foi ARP, que permite manipular e/ou exibir o cache de vizinhos de rede IPv4 do kernel. Com o comando arp, é possível adicionar entradas à tabela, excluir uma ou exibir o conteúdo atual apresentado.

Em seguida, dando continuidade aos testes, foi utilizado o Nmap(portscan), que por sua vez, permite fazer a identificação do estado

de uma porta em uma rede, com o seguinte objetivo de encontrar portas abertas e eventuais vulnerabilidades.

Ao final, foi utilizado a ferramenta Aircrack-ng, que realiza a avaliação da segurança de uma rede sem fio. Essa ferramenta serve para quebrar chaves WEP e WPA/WPA2-PSK do IEEE 802.11 e pode também recuperar a chave WEP, uma vez que um número suficiente de pacotes criptografados sejam capturados com o airodump-ng.

5. RESULTADOS

Para obter os resultados dessa pesquisa, utilizamos a ferramenta Kali Linux, por meio da qual foi possível a realização de vários testes. A Figura 1 apresenta o escaneamento das redes sem fio.

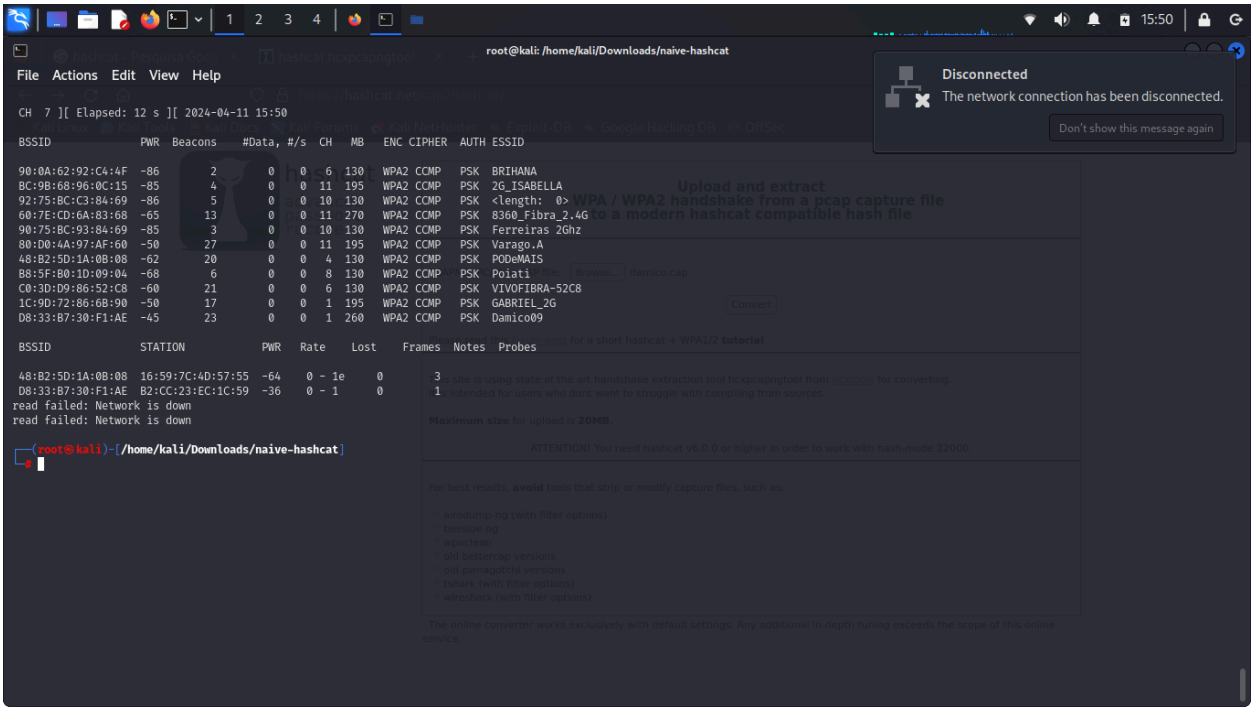

Figura 1: Testes realizados

Como apresentado na Figura 1, no primeiro caso foi realizado o escaneamento das redes sem fio próximas, em que conseguimos identificar algumas redes. Em seguida, foi realizado um teste de monitoramento de rede, apresentado na Figura 2.

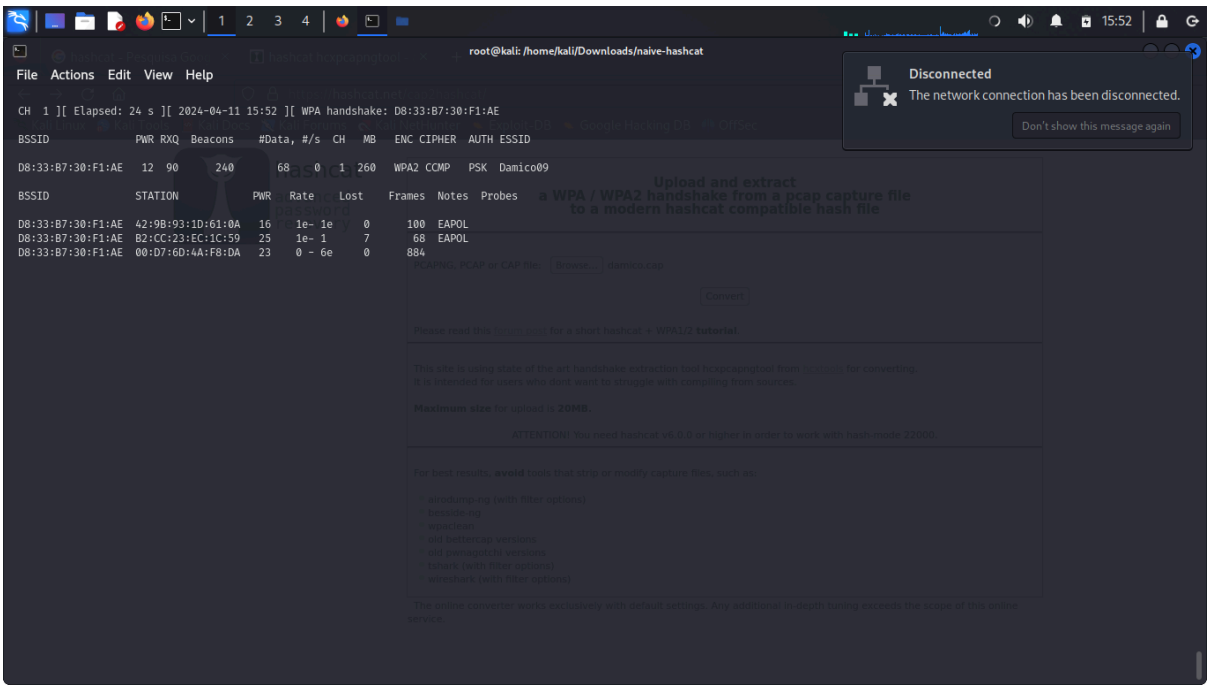

Figura 2: Testes realizados

Em um segundo momento, conforme apresentado na Figura 2, foi realizado o monitoramento da rede, aguardando um handshake para tentar descobrir a senha da rede. Em seguida, foi exibido o erro no teste de monitoramento da rede para a descoberta da senha, conforme apresentado na Figura 3.

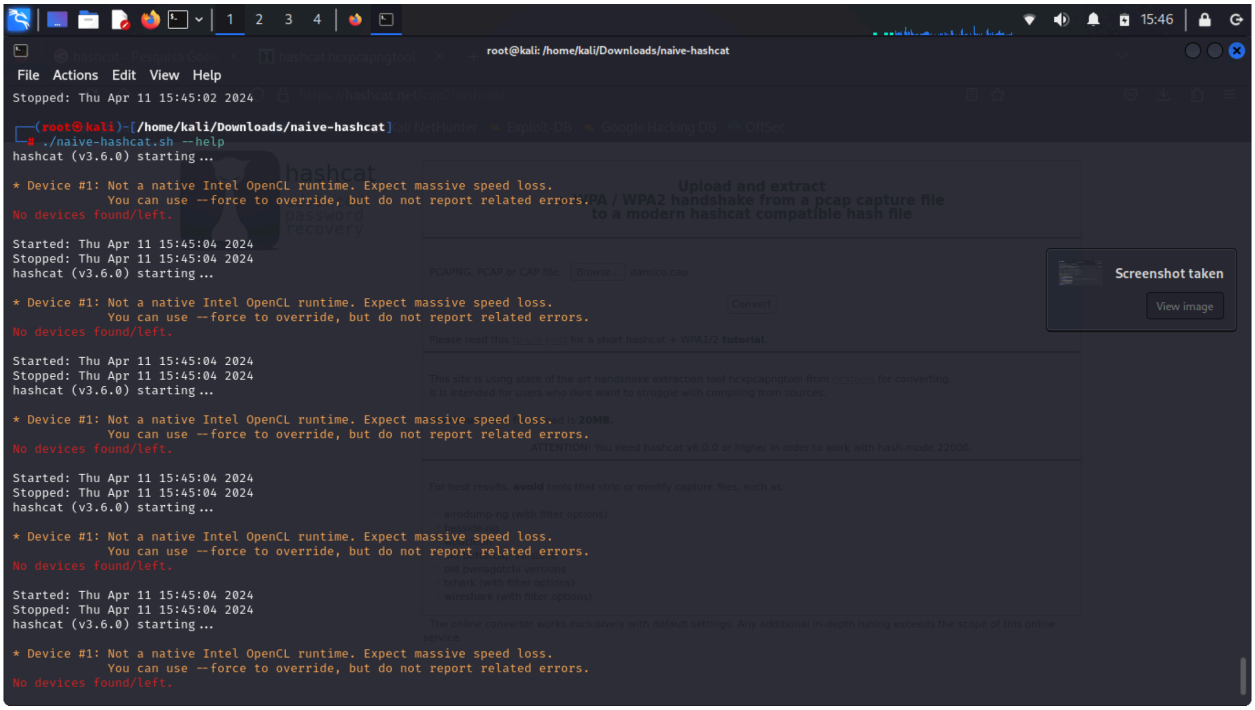

Figura 3: Testes realizados

Aqui, podemos ver o erro apresentado pela ferramenta na tentativa de descobrir a senha da rede, e ao mostrar o erro, é possível identificar as vulnerabilidades e avaliar a segurança dessas redes. Em seguida, foi realizado o teste para a descoberta da placa de rede, conforme apresentado na Figura 4.

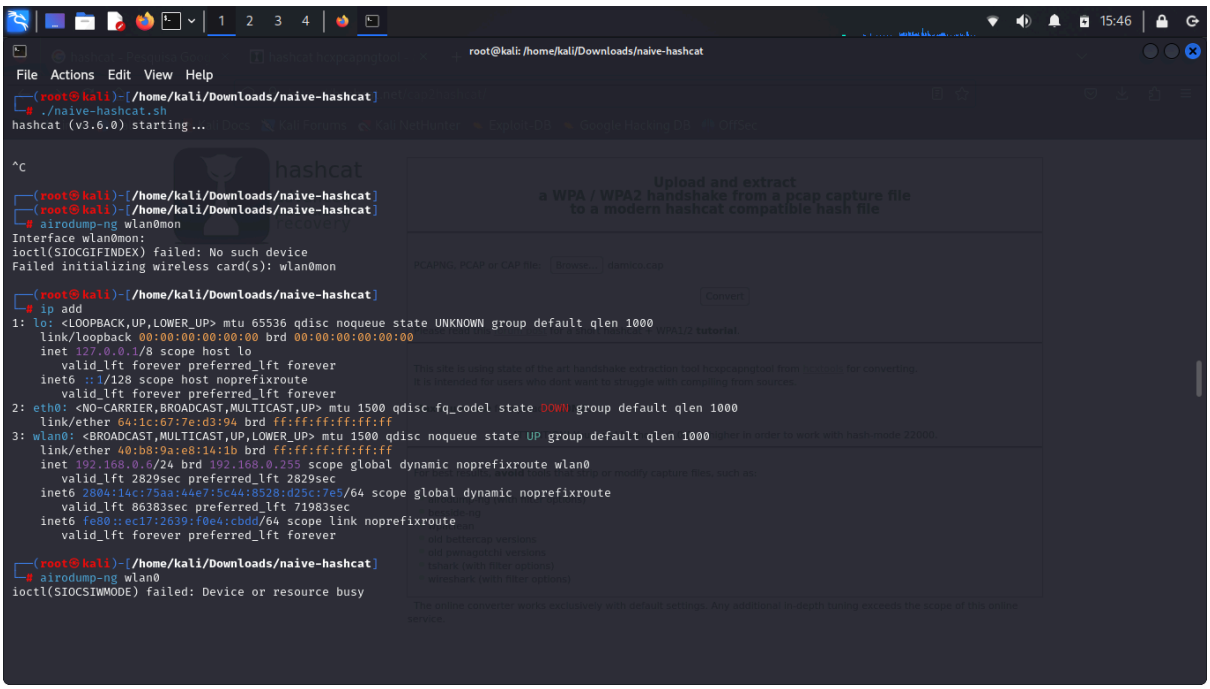

Figura 4: Testes realizados

Conforme a Figura 4, observa-se que foi realizado um teste para descobrir o nome da placa de rede, na qual, foi bem-sucedido, exibindo corretamente os dispositivos conectados e suas configurações.

Em um segundo momento da realização dos testes com a ferramenta Kali Linux, realizamos três tipos diferentes de testes, que serão apresentados a seguir: ARP(realiza um escaneamento de uma subrede, com o endereço mac de origem), IP(Verifica a conectividade, serviços e vulnerabilidades de um endereço IP) e PORTSCAN(Mostrar as portas do servidor online). A Figura 5 mostra o teste para identificar quais os dispositivos estavam conectados a uma determinada rede.

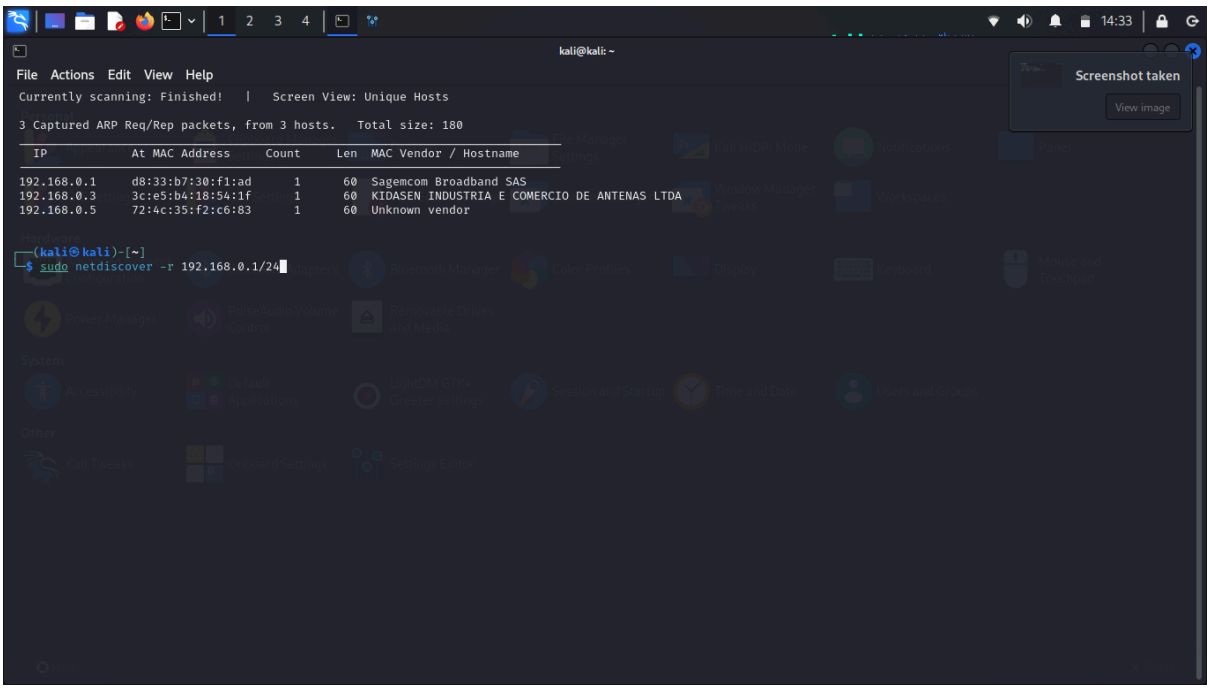

Figura 5: Testes realizados

A Figura 5 apresenta o teste realizado para a leitura dos dispositivos que estavam conectados à rede por meio do PORTSCAN. Logo, foram exibidos todos os dispositivos que estavam conectados à rede, como mostrado na Figura 6.

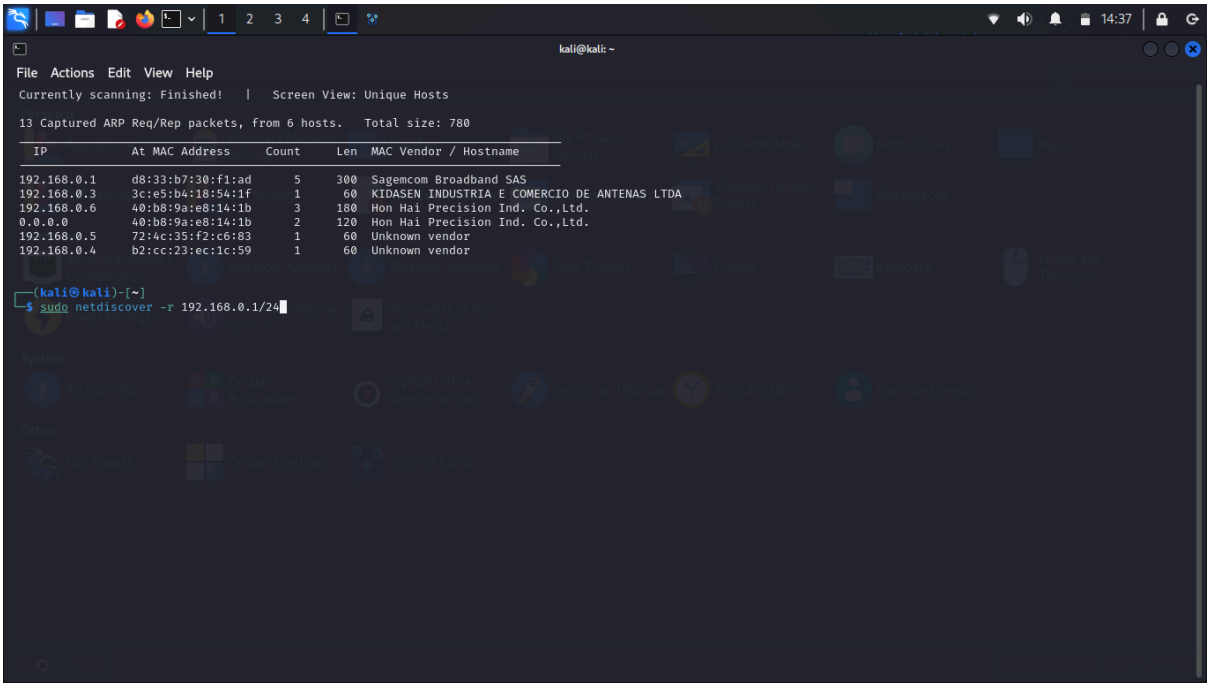

Figura 6: Testes realizados

Após realizar a leitura dos dispositivos conectados à rede, todos foram identificados. Em seguida, foi realizado o teste para escanear as portas do servidor *online,* conforme apresentado na Figura 7.

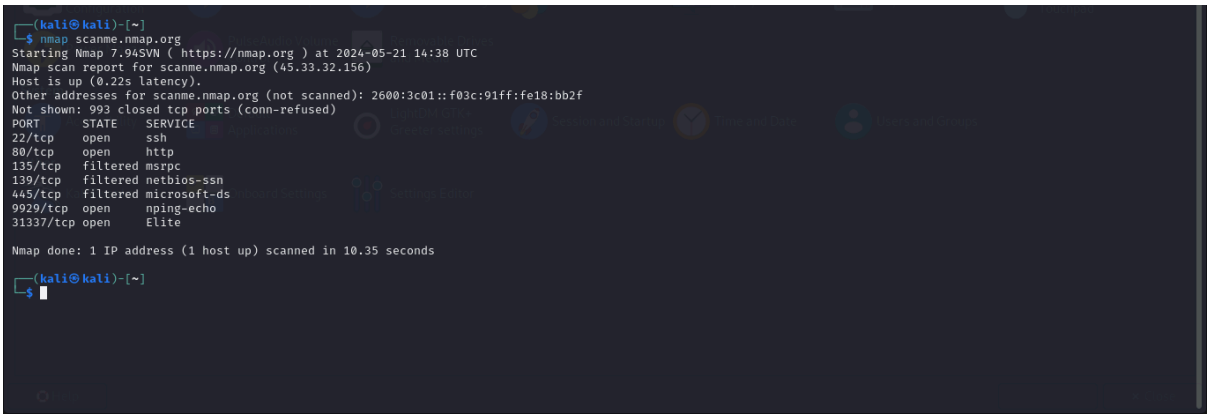

Figura 7: Testes realizados

Como apresentado na Figura 7, o teste realizado foi o escaneamento das portas do servidor online. Após a leitura das portas, foram encontradas 1000 portas, das quais 993 estão fechadas e não aparecem na lista,
enquanto as 7 portas exibidas possuem funções específicas.

- 22/tcp - Secure Shell(SSH) logins seguros, transferência de arquivos(scp, sftp) e encaminhamento de porta.
- 80/tcp - Hypertext Transfer Protocol (HTTP) usa tcp nas versões 1.x e 2.
- 135/tcp - Microsoft EPMAP(End Point Mapper) usado para gerenciar remotamente serviços, incluindo servidor DHCP, servidor DNS e WINS
- 139/tcp - Serviço de nomes NetBIOS, usado para registro e resolução de nomes.
- 445/tcp - Microsoft-DS (Serviço de diretório) Active Directory, compartilhamentos do Windows.
- 9929/tcp - Permite o envio e recebimento de pacotes para medir conectividade e outros parâmetros da rede.

- 31337/tcp - A porta é considerada um “ícone” em segurança cibernética e muitas vezes usada para simulações ou como exemplo em treinamentos.

Portas abertas em um servidor online podem apresentar diversos riscos à segurança, especialmente se estiverem associadas a serviços desnecessários, vulneráveis ou mal configurados. Entre os riscos estão a exposição de serviços vulneráveis, permitindo a exploração de falhas e a execução remota de código. Essas portas também podem ser alvo de ataques de força bruta, especialmente em serviços de acesso remoto. Serviços mal configurados em determinadas portas podem ser usados em ataques de amplificação DDoS e portas que não utilizam criptografia podem expor dados sensíveis. Além disso, portas abertas podem ser exploradas para acessar a rede interna ou propagar malware.

Em seguida, foi realizado o teste do escaneamento da rede interna, conforme apresentado na Figura 8.

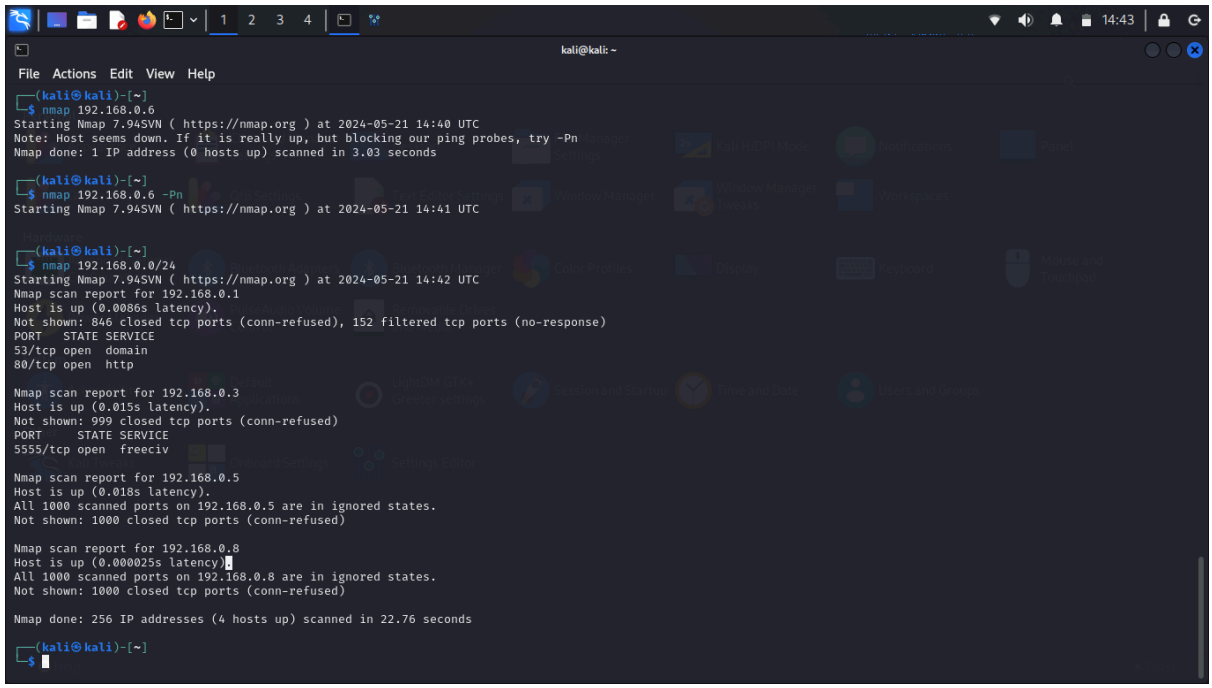

Figura 8: Testes realizados

A Figura 8 apresenta o escaneamento da rede interna (rede local), onde podemos ver as portas que estão abertas e suas conexões. A porta 53/tcp aberta indica que o serviço DNS está ativo e acessível, sendo essencial para traduzir nomes de domínio em endereço IP. No entanto, sua exposição pode trazer riscos como ataques de amplificação DNS, envenenamento de cache (DNS spoofing), vazamento de informações por transferência de zona (AXFR) e exploração de vulnerabilidades do serviço.

Caso o serviço não seja essencial, é preferível fechar a porta para reduzir ataques. Por fim, no último teste, foi realizado o escaneamento da rede utilizando o comando ARP, conforme apresentado na Figura 9.

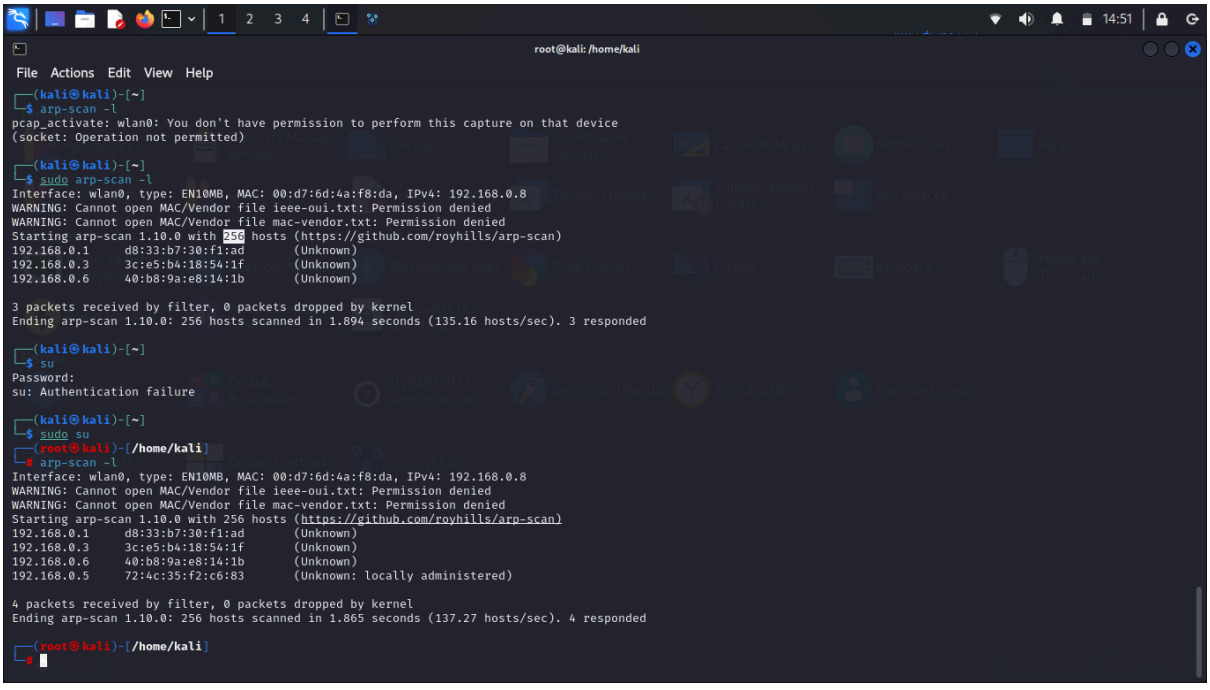

Figura 9: Testes realizados

Por fim, a Figura 9 apresenta o escaneamento da rede utilizando o comando ARP, que encarrega o Nmap e seus algoritmos otimizados de

fazer requisições. Caso obtenha uma resposta, o Nmap não precisa se preocupar com os pacotes ping baseados em IP.

Ao realizar testes de penetração(pentest), é fundamental garantir que certas informações não sejam divulgadas, como endereços IP e nomes de domínio, dispositivos de rede e infraestrutura, e dados de teste.

Algumas informações que podem ser reveladas, mas que representam possíveis pontos de vulnerabilidade, incluem: (Portas Abertas) saber quais portas estão abertas no sistema que podem ser explorados, (Configurações de segurança) políticas de segurança fracas ou mal configuradas podem ser um ponto de entrada; e (Informações de DNS) dados de DNS podem revelar subdomínios ou serviços internos que não estão protegidos.

Para corrigir as falhas encontradas nos testes realizados, recomenda-se ocultar o SSID, adotar protocolos seguros como WPA3, implementar criptografia de tráfego, usar IDS, ativar isolamento de cliente no roteador, restringir acessos por endereço MAC, fechar portas desnecessárias, configurar firewall e aplicar medidas como ARP estático, VLANs e Dynamic ARP Inspection para mitigar ataques de spoofing.

6. CONCLUSÃO

Este trabalho apresenta a evolução da tecnologia e a crescente popularização das redes sem fio, destacando a transformação que a internet trouxe para a vida cotidiana e para o ambiente empresarial, enfatizando a necessidade de adaptação.

O acesso à Internet é primordial nos dias atuais para as mais diversas atividades. Assim, o trabalho explorou o campo da segurança relacionado à intrusão nessas redes.

Após a realização desta pesquisa, chegamos à conclusão de que as redes sem fio, que podemos encontrar facilmente em diversos lugares que frequentamos no dia a dia, apesar das medidas adotadas para garantir a segurança, muitas redes públicas ainda apresentam vulnerabilidades significativas, suscetíveis à exploração por agentes mal-intencionados, colocando em risco as informações disponíveis. Isso dificulta o acesso e a

obtenção de algumas informações confidenciais, além de proteger pessoas e empreendimentos de possíveis comprometimentos.

Como trabalhos futuros, sugere-se investigar padrões de ataque e comportamento de redes, com o objetivo de desenvolver métodos de defesa mais robustos. Além disso, pode-se investigar o impacto das novas tecnologias, como protocolos de emergentes de segurança e redes IoT, avaliando vulnerabilidades específicas. A automação de testes com o uso da inteligência artificial, em que permite identificar falhas de forma mais eficiente.

7. REFERÊNCIAS

ALGAR TELECOM. **Hotspot Wi-Fi: O que é, como funciona e principais benefícios. Algar Telecom, 2022.** Disponível em: https://blog.algartelecom.com.br/wifi-hotspot/ Acesso em: 1 dez. 2024.

ALMEIDA JR., JA **Pentest em aplicações web: Avalie a segurança contra ataques web com testes de invasão no Kali Linux** . São Paulo: Casa do Código, 2021.

CASTRO, André. **As 10 principais ferramentas Android para auditorias de segurança e hackers . Portal GSTI, 2018.** Disponível em: https://www.portalgsti.com.br/2018/07/top-10-ferramentas-android-para-auditoria-de-seguranca-e-hackers.html Acesso em: 1 dez. 2024.

CESCA, J.; DO PRADO, ML **A Gestão da Tecnologia de Hotspot como Vantagem Competitiva** . Revista Tecnologia, 44, 1-16, 2023. Disponível em: https://ojs.unifor.br / tec /article /view / 13047. Acesso em: 1 dez. 2024.

DIAS, Kelvin Lopes. **Kali Linux - Aprenda sobre o Linux para Hackers .** Disponível em: https://academiadeforensedigital.com.br/kali-linux-aprenda-sobre-o-li

nux-para-hackers/. Acesso em: 1 dez. 2024.

FORZATI, M.; LARSEN, CP; MATTSSON, C. **Rede aberta de telecomunicações** . ICTON, 2010. Disponível em: https://pt.wikipedia.org/wiki/Rede_aberta_de_telecomunica%C3%A7%C3%B5es#:~:text=Rede%20aberta%20de%20telecomunica%C3%A7%C3%B5es%20 Acesso em: 1 dez. 2024.

HOYER, Erika; MEIRELLES, Pedro; PROTETOR, Renan. **Firewall** . UFRJ , 2013. Disponível em: https://www.gta.ufrj.br/grad/13_1/firewall/index.html Acesso em: 1 dez. 2024.

LINS, Bernardo Felipe Estellita. **A evolução da Internet: uma perspectiva histórica** . Cadernos Aslegis, v. 11-45, 2013.

MITOLA III, J.; PRYS, M. **Engenharia digital orientada para o ciberespaço** . Engenharia de Sistemas, v. 27, n. 1, pág. 109-119, 2024. Disponível em: https://incose.onlinelibrary.wiley.com/doi/full/10.1002/sys.21710 Acesso em: 1 dez. 2024.

PICONI, Roberto de Carvalho. **A importância do Pentest para os negócios de uma empresa**, 2016. Trabalho de conclusão de curso (Curso de Tecnologia em Segurança da Informação) - Faculdade de Tecnologia de Americana, Americana, 2016

RIBEIRO, Uirá. **As 7 principais ferramentas no Kali Linux para pentest . Certificação Linux, 2022.** Disponível em: https://www.certificacaolinux.com.br/ferramentas-kali-linux/ Acesso em: 1 dez. 2024.

TUBARÃO. **Pentest: as 10 melhores ferramentas usadas no mercado . Ostec, 2020.** Disponível em: https://ostec.blog/geral/pentest-as-10-melhores-ferramentas-usadas-n

o-mercado/?cn-reloaded=1 Acesso em: 1 dez. 2024.