PENTEST EM REDE WIFI: REALIZAR UM PENTEST REAL EM UMA REDE WI-FI DEMONSTRANDO AS VULNERABILIDADES[1]

Rafael Guilherme Ramos[2]
Dorival Moreira Machado Junior[3]

RESUMO

Pentest é a abreviatura do inglês Penetration Test cujo intuito é um teste contra invasores, o papel do Pentest é analisar minuciosamente a utilização da rede de uma empresa ou instituição, apresentarei ferramentas para realizar Pentest e também mostrarei as ferramentas que foram usado como testes em um ambiente próprio e controlado para não ter o risco de infringir nenhuma lei e prejudicar outras pessoas, fazer tais procedimentos em redes sem autorização podem acarretar penalidades para o invasor e até mesmo o profissional especializado, realizando métodos dos chamados hackers, este teste monitora os mesmos meios que invasores utilizam, dessa forma o pentest visa rastrear qualquer vulnerabilidade no sistema, rede e servidores que possa estar em risco de invasão. Neste projeto visamos realizar um Pentest em uma rede wi-fi real apurando suas vulnerabilidades e relatando-as para que assim as organizações possam investir na segurança de sua rede protegendo seus dados sigilosos.

Palavras-chave: Pentest; segurança; rede.

1 INTRODUÇÃO

Pentest é conhecido como teste de intrusão, é uma forma de explorar e detectar vulnerabilidades existentes nos sistemas e simular ataques, é um serviço muito utilizado em setores públicos, financeiros , grandes corporações e companhias que necessitam de um ambiente seguro e praticamente inviolável, tendo como objetivo principal realizar um Pentest real em uma rede wi-fi com os métodos White Hat , Black Hat e Gray Hat que irá apurar as vulnerabilidades de redes WI-FI e entregando relatórios demonstrado todas as falhas apontadas, assim as organizações poderão corrigir e manterem as suas redes seguras das invasões .

Algumas das ferramentas utilizadas para procedimentos de testes é Aircrack-ng e Nmap, serão utilizadas para quebra de segurança WPA[4] e WPA2 e enviar pacotes de broadcast, descoberta de portas de acesso e analisar suas vulnerabilidades, todos esses procedimentos foram realizados em um ambiente controlado e seguro, pois a execução pode haver penalidade previsto em leis que serão abordadas mais à frente.

Uma pesquisa da Kaspersky, empresa especializada em segurança virtual, identificou um aumento de 330%, ou mais que o quádruplo, no número de tentativas de ataques cibernéticos no Brasil em 2020. Foram mais de 402 mil invasões a sistemas corporativos (KASPERSKY, 2024).

---

[1] Artigo submetido em 04/11/2024, e apresentado à Libertas – Faculdades Integradas, como parte dos requisitos para obtenção do Título de Bacharel em Sistemas de Informação, em xx/xx/2024.

[2] Graduando em Sistemas de Informação pela Libertas – Faculdades Integradas – E-mail: 005633@libertas.edu.br.

[3] Professor-orientador. Doutor em Tecnologias da Inteligência e Designer Digital. Docente na Libertas – Faculdades Integradas – E-mail: dorivaljunior@libertas.edu.br.

[4] Abreviação de Wi-Fi Protect Acess - proteção de acesso ao Wi-Fi.

2. REFERENCIAL TEÓRICO

A partir desse ponto serão apresentadas 10 ferramentas para pentest que são mais ágeis que conta com uma documentação e fóruns para pesquisa, e que são muito utilizadas por profissionais de segurança cibernética e hackers em todo o mundo, foi explicado a usabilidade de cada ferramenta onde deve ser utilizada quando o assunto se trata de análise de rede, invasão, capturas de dados e quebras de senhas.

2.1.1 Metasploit

Conhecimento é poder, especialmente quando partilhado. Através de uma colaboração entre a comunidade de código aberto e o Rapid7, o Metasploit ajuda as equipes de segurança a fazer mais do que detectar vulnerabilidades, conduzir avaliações de segurança e melhorar a conscientização sobre segurança. É um framework e é uma das ferramentas mais usadas quando o assunto é Pentest, basicamente a sua funcionalidade é facilitar ou tornar o processo do ataque o mais simples possível, nele é possível encontrar vários exploits, que se tratam de softwares cujo objetivo é explorar algum tipo de vulnerabilidade ou falha que estejam ligadas ao software ou hardware de um computador, para as mais diversas vulnerabilidades já conhecidas e com vasto número de recursos que torna a tarefa de comprometer sistemas de forma rápida e eficaz. (PROFISSIONAIS TI, 2020).

2.1.2 Medusa

Medusa é um brute-forcer, que se trata de um software cujo objetivo é encontrar uma combinação de senha, de login rápido, paralelo e baseada em módulos. O objetivo é oferecer suporte ao maior número possível de serviços que permitam autenticação remota. Considera-se os seguintes itens como alguns dos principais recursos deste aplicativo:

Teste paralelo baseado em thread: É uma execução autônoma de um sequência no mesmo espaço de endereço da memória é compartilhada com outras sequências independentes de execução desse processo. Por exemplo, o teste de força bruta pode ser executado em várias máquinas com vários hosts, que é um dispositivo e um computador que oferece e consome serviços, um endereço de IP, um usuário ou uma senha.

Entrada flexível do usuário: As informações de destino (host/usuário/senha) podem ser especificadas de várias maneiras. Por exemplo, cada item pode ser uma única entrada ou um arquivo contendo várias entradas. Além disso, um formato de arquivo de combinação permite ao usuário refinar sua lista de destino.

Projeto modular: Cada módulo de serviço existe como um arquivo .mod, um tipo de arquivo que é utilizado como armazenamento independente. Isso significa que nenhuma modificação é necessária no aplicativo principal para estender a lista de serviços com suporte para força bruta.

De acordo com Mondloch (2016), existem vários protocolos de segurança suportados atualmente, como por exemplo, SMB, HTTP, POP3, MS-SQL, SSHv2, dentre outros.

2.1.3 Wireshark

É uma das melhores ferramentas de análise de protocolos de redes disponíveis. Com o Wireshark, pode -se analisar uma rede com grande detalhe para ver o que está acontecendo e, ainda possibilita uma captura de pacotes em tempo real, uma inspeção profunda a centenas de protocolos, pesquisa e filtragem dos pacotes (BOOT, 2017). Esta é uma ferramenta

multiplataforma e já se encontra presente no Kali Linux, mas também é possível instalar no Windows e no Mac. Conforme, certas características, você precisa de um adaptador de Wifi, com o modo promíscuo e monitoramento e seus recursos são:

Inspeção detalhada de centenas de protocolos, captura ao vivo e análise offline, visualizador de pacotes.

Dados de rede capturados podem ser navegados via GUI (Interface gráfica do utilizador) ou TShark (Wireshark baseado em terminal) no modo TTY, filtros de exibição mais poderosos, análise VoIP rica.

Leitura/gravação de diferentes tipos de arquivos capturados: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco IPlog IDS seguro, Microsoft Network Monitor, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek/TokenPeek/AiroPeek e muitos mais arquivos de captura Gzip 444 podem ser compactados dados ao vivo rapidamente. Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI e muito mais (dependendo da sua plataforma) Suporte de criptografia para muitos protocolos, incluindo IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP[5] e WPA/WPA2

Regras de coloração podem ser aplicadas a listas de pacotes para análise rápida e intuitiva e a saída pode ser exportada como XML, CSV ou texto simples (WIRESHARK, 1998).

2.1.4 John The Ripper

John é um poderoso quebrador de senhas. Não importa se é uma senha simples ou complexa, essa ferramenta pode fazer o trabalho por você. Hackers com más intenções e profissionais de segurança aproveitam essa ferramenta e conseguem quebrar senhas complexas, usando vários métodos de ataques. Alguns dos métodos disponíveis na ferramenta são quebra de senhas com Wordlist (lista de palavras que usa uma combinação de palavras e números comuns usados para testes, pesquisa e ataques) e quebra de senha simples com base nas informações fornecidas ou o processo de alteração, no qual a ferramenta realizará sucessivos testes de caracteres até encontrar a senha desejada. O método mais popular passa a ser feito pelas famosas Wordlists, uma vez que nos dias de hoje é fácil acessar dicionários de senhas vazadas pela Internet. A prática típica do Pentester é usar esta ferramenta para provar que as senhas utilizadas pelo cliente são fracas e podem ser quebradas facilmente. (BUCKBEE, 2023),

2.1.5 Nmap

Nmap (“Network Mapper”) é um utilitário de descoberta gratuito e de código aberto é uma ferramenta de auditoria e segurança. Existem muitos administradores de sistemas e redes que também acham útil o Nmap, para tarefas como inventário de rede, gerenciamento do planejamento de atualização de serviço e monitoramento de tempo de atividade de host ou serviço. O Nmap usa pacotes IP e diversas maneiras para determinar quais hosts estão disponíveis na rede. Quais os serviços esses hosts fornecem (nomes e versões de aplicativos), quais sistemas operacionais (e tipos de versões do SO) que eles executam, que tipos de filtros/firewalls eles usam. Ele foi projetado para verificar grandes redes rapidamente, mas funciona bem em um único host. O Nmap é executado em todos os principais sistemas operacionais de computador Linux, Windows e Mac OS. O Nmap foi nomeado “Produto de

[5] Abreviação para Wired Equivalent Privacy - Privacidade Equivalente com fio, uma espécie de proteção de rede.

Segurança do Ano" pelo Linux Journal, Info World, LinuxQuestions.Org e Codetalker Digest. Ele até apareceu em doze filmes , incluindo Matrix Reloaded , Die Hard 4 , Girl With the Dragon Tattoo e The Bourne Ultimatum . (NMAP, 2024).

2.1.6 Hydra

Com esta ferramenta você pode realizar ataques poderosos contra vários serviços de Internet, como FTP[6], Telnet[7] e SSH[8]. Seu comportamento é semelhante ao de John The Ripper, mas ele se concentra inteiramente em ataques cibernéticos. Hydra é uma ferramenta poderosa e flexível para testes de penetração, força bruta e ataques de dicionário (Wordlist) em diversas comunicações e serviços. Opções e recursos abrangentes de configuração permitem testar a segurança de redes, aplicativos web e serviços em vários locais.

Hydra é uma ferramenta poderosa construída em Python. É amplamente utilizado para avaliar a segurança de sites como gerenciamento de conteúdo e fóruns.

Quando configurado corretamente, todas as operações são realizadas automaticamente sem intervenção do usuário. Basicamente, basta configurá-lo e esperar que sua senha seja encontrada. (ACADITI, 2024.)

2.1.7 Aircrack-ng

Esta ferramenta pode ser considerada um conjunto de ferramentas projetadas para detectar e explorar problemas em redes Wi-Fi. Usando Aircrack-ng, há a possibilidade monitorar pacotes que trafegam pela rede, capturá-los e analisá-los e até mesmo comprometer a segurança da Internet. É utilizado por profissionais que precisam garantir a segurança das redes Wi-Fi, portanto, se o seu objetivo é quebrar senhas WEP, WPA/WPA2-PSK, o Aircrack-ng pode fazer o trabalho de monitoramento: Reúne e envia dados para arquivos para processamento por ferramentas de terceiros.

São os métodos utilizados para alcançar os objetivos:

> Ataques: Ataques de replicação via injeção de pacotes, autenticação, pontos de acesso falsos, etc.
> Testes: Verifique a placa WiFi e funcionalidade (scanning e injeção)
> Cracking: WEP e WPA PSK (WPA 1 2)
> Todas essas ferramentas são de linha de comando, o que permite mais digitação.

Muitas GUIs (Interface gráfica do usuário) utilizam esse método. Roda principalmente em Linux, mas também pode rodar em sistemas operacionais como Windows, macOS, Solaris, dentre outros (Aircrack-ng, 2009).

---

[6] Abreviação de File Transfer Protocol, trata-se de um protocolo de rede que é utilizado para transferência de arquivos entre computadores, com envio e recebimento de dados.

[7] Trata-se de um protocolo, com o qual é possível a comunicação e acesso remoto entre computadores.

[8] Abreviação de Secure Shell, trata-se de um protocolo de rede que é utilizado para que haja um acesso remoto seguro a sistemas, utilizando comunicação criptografada.

2.1.8 Reaver

(Kali Tools, 2016) “O Reaver foi projetado para ser um ataque robusto e prático contra PINs[9] de registrador Wi-Fi Protected Setup (WPS) para recuperar senhas WPA/WPA2”. Dependendo do ponto de acesso (AP) do alvo, para recuperar a senha de texto simples WPA/WPA2, a quantidade média de tempo para o método de força bruta on-line de transição é de 4 a 10 horas. Na prática, geralmente leva metade desse tempo para adivinhar o PIN WPS correto e recuperar a senha. Ao usar o ataque offline, se o AP estiver vulnerável, pode levar apenas uma questão de segundos a minutos.

2.1.9 Pixie WPS

Pixie WPS é escrita na linguagem de programação C[10], usada para bruteforce offline, o PIN WPS é explorado a pouca desordem ou inexistente de alguns pontos de acesso, é chamado de "ataque de poeira de duende" descoberto por Dominique Bongard. “Ao contrário do tradicional ataque de força bruta online, implementado em ferramentas como Reaver ou Bully que visam recuperar o PIN em poucas horas, esse método pode obter essa chave de segurança em questão de milissegundos a minutos, dependendo do alvo, se mais vulnerável “(Kali Tools, 2017) .

2.1.10 Wifite

O Wifite automatiza várias técnicas de ataque, tornando o processo de teste mais simples e rápido para atacar várias redes sem fio criptografadas com WEP/WPA/WPA2 e WPS. No início ele exige alguns parâmetros para trabalhar, mas o Wifite fará todo o trabalho duro. Atua de forma a capturar handshakes WPA, para autenticar automaticamente clientes conectados, falsificar seu endereço MAC[11] e manter segura as senhas crackeadas (SOLYD, 2023).

2.2 Leis

A realização do pentest para fins de estudo deve ser feito em um ambiente totalmente estável e controlado e em seu próprio domínio, pois há leis que penalizam a invasão sem o consentimento do proprietário(a).

Algumas dessas leis são a Lei dos Crimes Cibernéticos (Lei n° 12.737/2012), conhecida como Lei Carolina Dieckmann, foi a primeira a tipificar atos de crimes digitais como invasão de computadores e celulares, violação de dados de usuários e interrupção de sites (governamentais ou não) (BRASIL, 2012).

Outra lei muito conhecida é a Lei n° 12.965/2014, conhecida como Marco Civil da Internet, que surgiu para regular os direitos e deveres dos usuários da rede (BRASIL, 2014).

E por fim, temos a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), que surge para regular as atividades de coleta e tratamento de dados pessoais que as empresas armazenam de seus clientes, que alterou os artigos 7º, que prevê a exclusão de maneira

[9] Abreviação de Personal Identification Number - Número de identificação pessoal. Uma chave de segurança que tem como objetivo proteger informações.

[10] Método de compilação de softwares, uma linguagem de nível intermediária, que combina elementos de linguagens de alto nível.

[11] Abreviação de Media Access Control - Controle de Acesso de Mídia, um identificador de componentes de placa de computadores e afins.

definitiva de dados pessoais que são fornecidos para alguma situação na internet, a requerimento do cidadão, ou após terminar a relação entre as partes, e 16, que estipula ser vedada a guarda de dados que são excessivo, ou seja, para além da finalidade proposta, do Marco Civil da Internet (BRASIL, 2018).

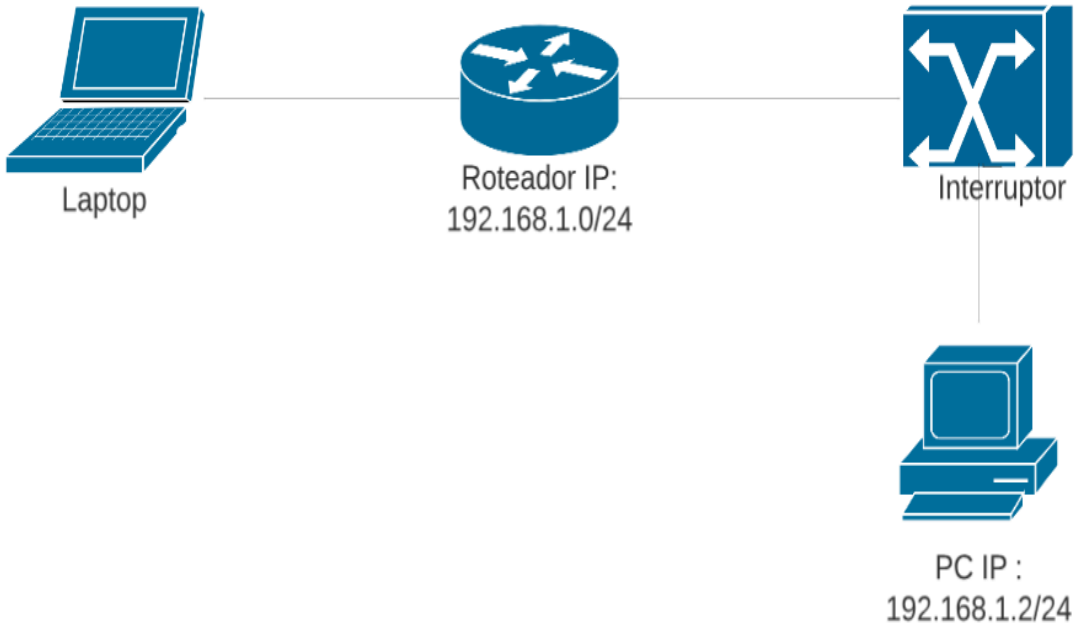
3. METODOLOGIA

Para a realização do Pentest para fins de estudo, foi necessário criar um ambiente controlado para podermos realizar os testes, que constituiu com os seguintes equipamentos um notebook com processador intel i5 de 7º geração, 12Gb de RAM e HDD de 500GB com o sistema operacional "Kali 2022.1 - 14th February, 2022 - The first 2022 Kali Rolling release". Kernel 5.15.0, Xfce 4.16.3, e foi utilizado um roteador TP Link TL-WR740N com taxa de dados wi-fi de 150Mbps compatível com o padrão 802.11b&g com criptografia WPA e WPA2.

3.1 Ambiente controlado para fins de estudo:

Para a realizar o pentest foi utilizada a ferramenta Aircrack-ng e Nmap, e essa escolha permitiu realizar testes com precisão, capturas de pacotes, envio de pacotes de broadcast, identificação de portas de comunicação vulneráveis e informações dos dispositivos conectados à rede. Todas essas informações podem trazer grandes prejuízos para as empresas, organizações governamentais e para usuários comuns, evidenciando a importância da realização do pentest para a descoberta das vulnerabilidades para que assim, os usuários possam se proteger.

Figura 1 –Ambiente de testes.



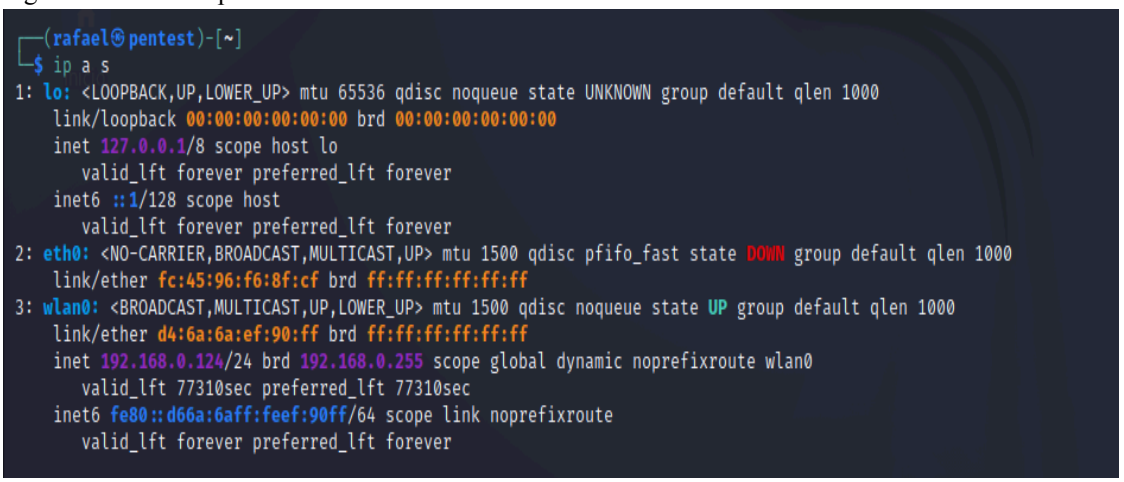
Fonte: Elaborado pelo autor.

3.2 Ferramenta utilizada: Aircrack-ng

Foi utilizada a ferramenta Aircrack-ng, para monitoramento, desautenticação de dispositivos da rede e quebra da criptografia de segurança assim revelando a senha do Wi-Fi, essa ferramenta foi escolhida por conter uma documentação detalhada e tutoriais disponíveis na internet, o seu funcionamento é feito por terminal no sistema operacional Kali Linux, para a execução do modos de ataque e varredura e monitoramento, utiliza-se uma série comandos que são digitados no terminal, nos passos serão apresentados a sua aplicação.

3.2.1 Verificar nome da placa de rede, utilizando o comando ip a s

Figura 2 – Verificar placa de rede.

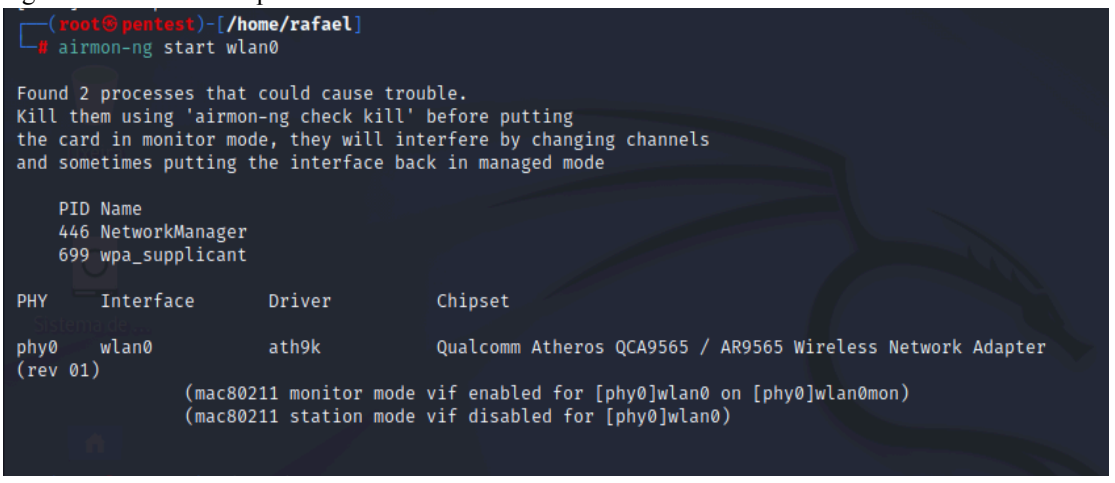


Fonte: Elaborado pelo autor.

3.2.2 Colocar a placa de rede em modo monitoramento

Utilizando o comando airmon-ng start wlan0, após executado, se a placa de rede suportar a mudança para monitoramento, esse processo permite que um computador com uma placa com interface de rede wireless (WNIC) realize monitoramento de todo o tráfego recebido da rede wireless. A placa de rede passará a ser wlan0mon, nesta etapa o dispositivo irá desconectar da rede automaticamente.

Figura 3 – Colocando a placa de rede em monitoramento.

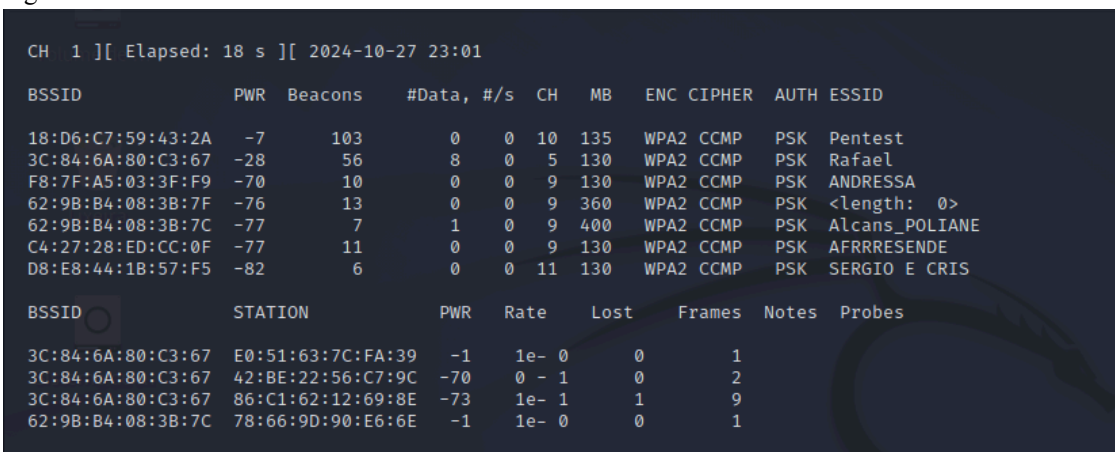


Fonte: Elaborado pelo autor.

3.2.3 Iniciando varredura

Para iniciar a varredura foi utilizado o comando airodump-ng wlan0mon, este, exibe todas as redes wi-fi próximas, trazendo informações como MAC do roteador, canal da frequência, tipo de criptografia, nome da rede, etc.

Figura 4 – Iniciando varredura.

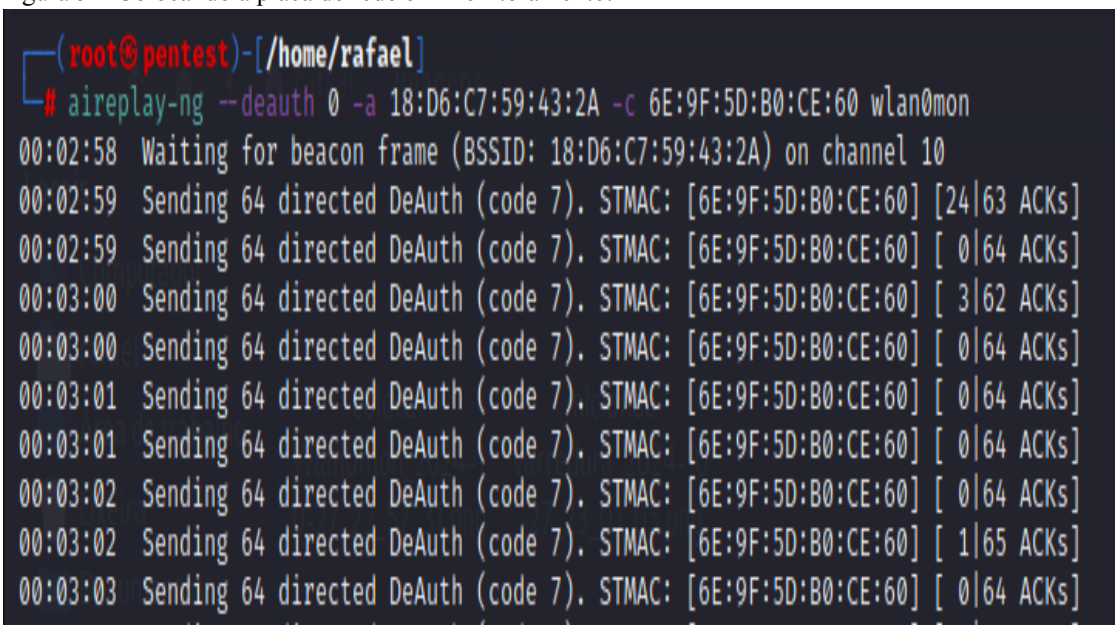


Fonte: Elaborado pelo autor.

3.2.4 Aireplay-ng

O comando aireplay-ng é responsável por enviar pacotes de broadcast de desautenticação, para enviar estes pacotes, utiliza-se o comando aireplay-ng --deauth 0 -a 18:D6:C7:59:43:2A -c 6E:9F:5D:B0:CE:60 wlan0mon, assim, irão para o roteador ESSID Pentest fazendo com que o dispositivo alvo desconecte da rede.

Figura 5 – Colocando a placa de rede em monitoramento.

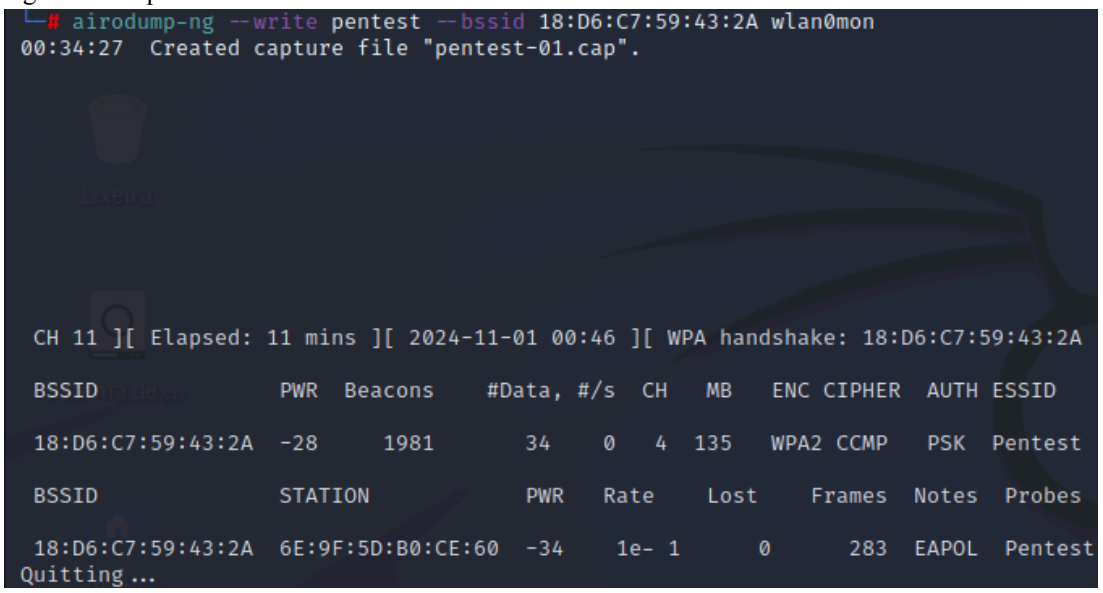


Fonte: Elaborado pelo autor.

3.2.5 Salvando informação para análise e quebra de senhas:

Para realizar a captura de informação de uma rede específica foi utilizado o seguinte comando airodump-ng --write pentest –bssid 18:D6:C7:59:43:2A wlan0mon, com este, irá gerar um arquivo para que seja feita análise de possível quebra da criptografia e revelar a senha do roteador

Figura 6 – Capturando dados.

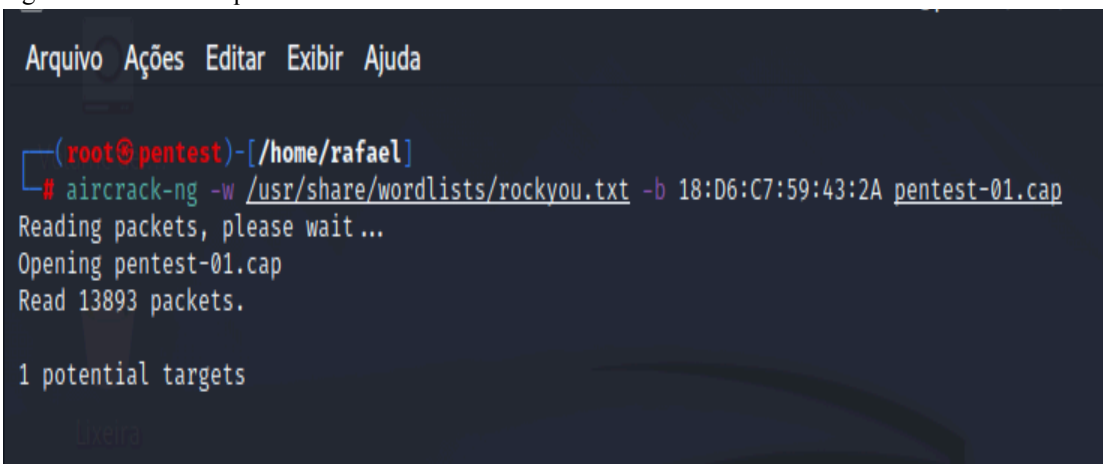


Fonte: Elaborado pelo autor.

3.2.6 Quebra de criptografia e revelando a senha:

Quebra da criptografia e revelando a senha de uma rede Wi-Fi utilizamos o seguinte comando aircrack-ng -w /usr/shre/wordlists/rockyou.txt -b 18:D6:C7:59:43:2A pentest-01.cap, esse método irá analisar o arquivo utilizando uma wordlists para a revelação da senha assim permitindo que o atacante possa se conectar a rede.

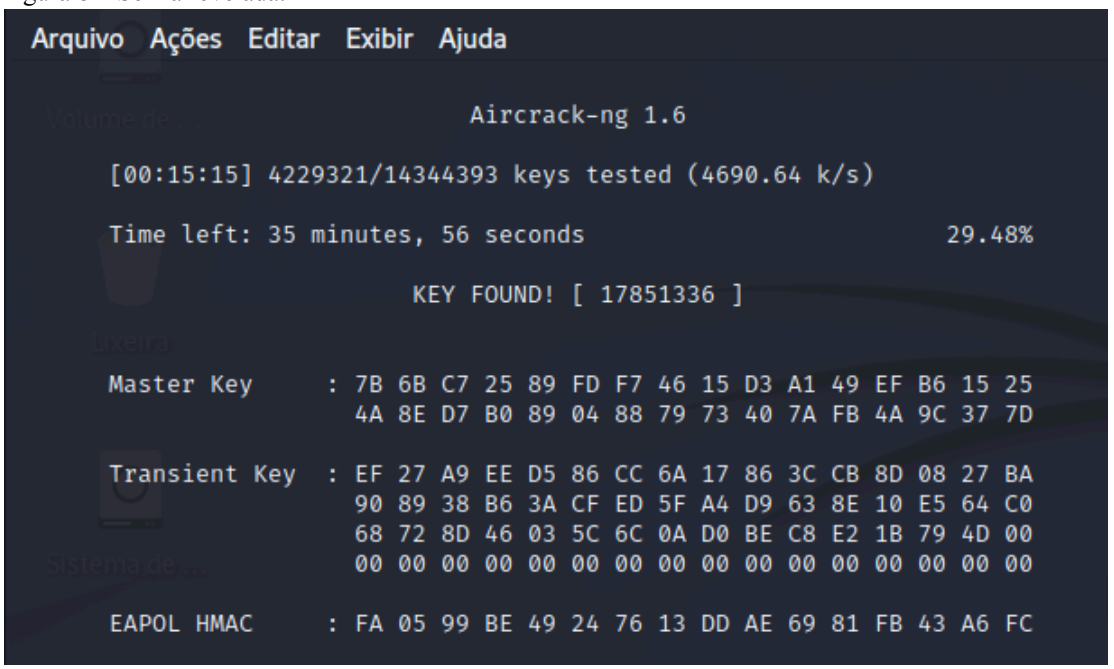
Figura 7 – Comando quebra de senha.



Fonte: Elaborado pelo autor.

Após a execução do comando citado, após algum tempo de execução, a senha e a análise são reveladas para uso do pentester.

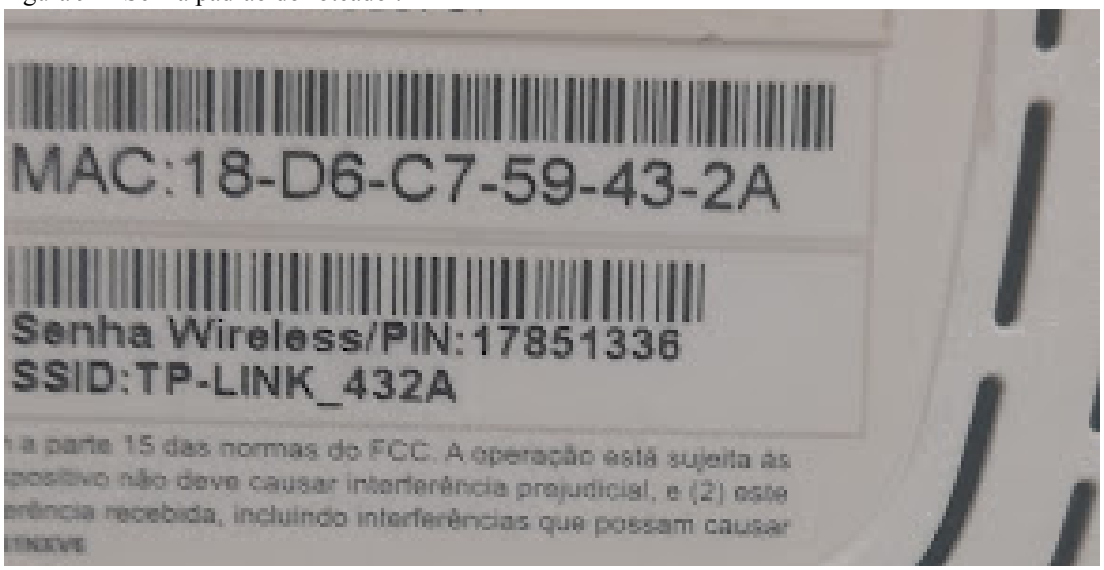
Figura 8 – Senha revelada.



Fonte: Elaborado pelo autor.

Na imagem abaixo, pode ser notada a senha do wireless/pin, e a mesma foi revelada conforme imagem anterior, confirmando assim, a veracidade da quebra da criptografia pela a ferramenta Aircrack-ng.

Figura 9 – Senha padrão do roteador.

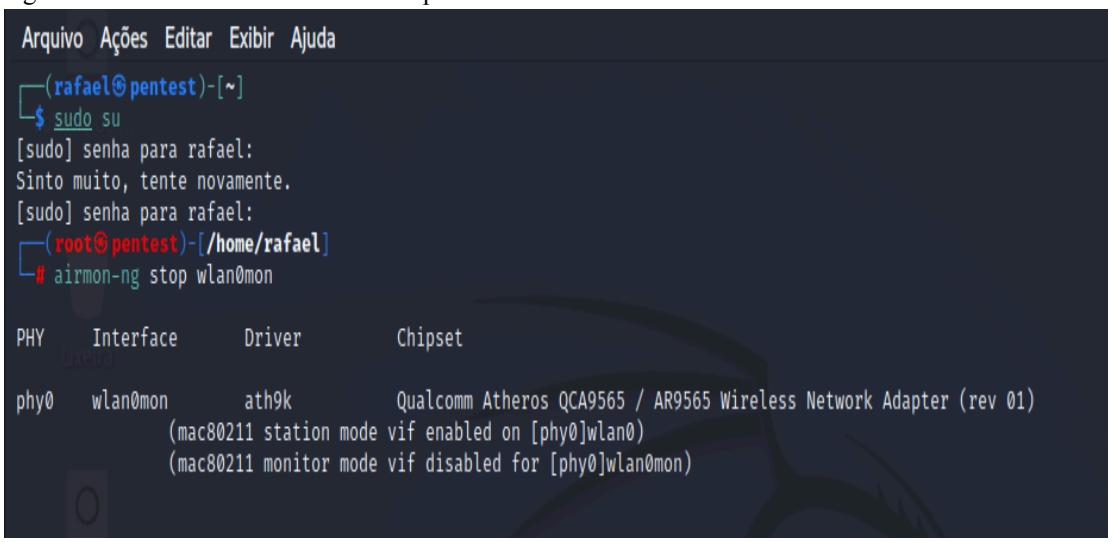


Fonte: Elaborado pelo autor.

3.2.7 Desativando o modo monitor da placa de rede:

Encerrando o processo e desativando o modo monitor da placa de rede Wi-Fi e voltando a sua funcionalidade normal, foi utilizado o comando airmon-ng stop wlan0mon.

Figura 9 – Desativar modo monitor da placa de rede.



Fonte: Elaborado pelo autor.

3.3 Ferramenta utilizada: Nmap

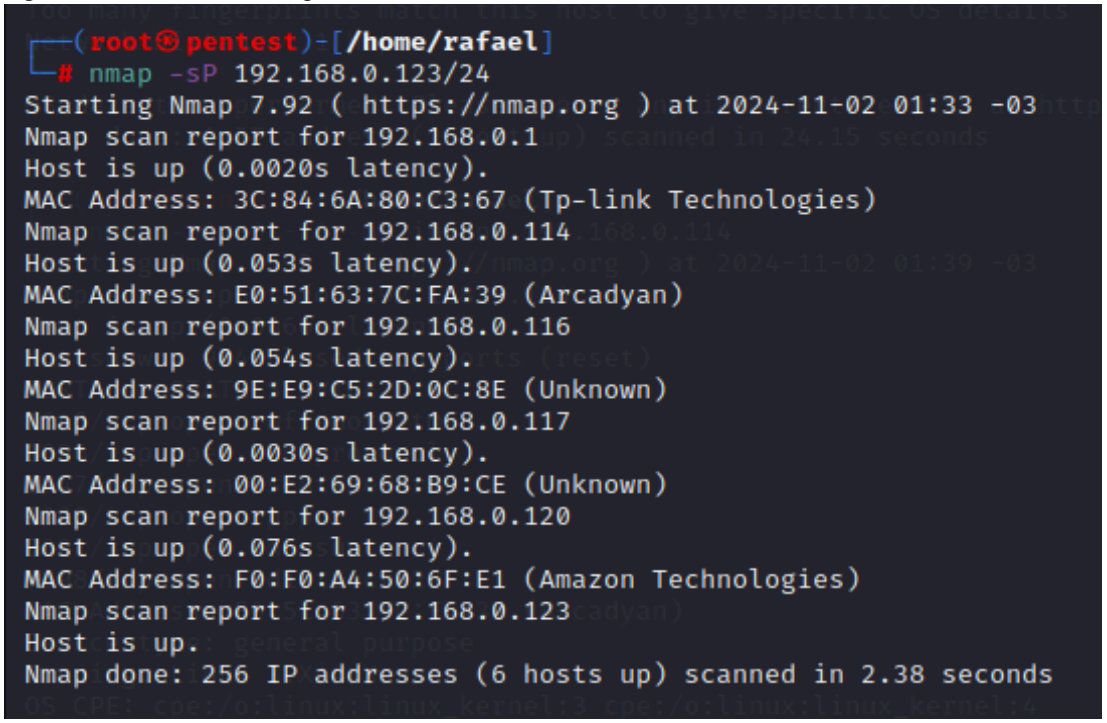
O uso dessa ferramenta foi para encontrar portas de comunicação ou acesso que estão abertas, gerar um relatório de máquina e varrer a rede por completo para detectar quais serviços ou dispositivos que possam estar vulneráveis, sua aplicação pode ser usada em outras áreas específicas como por exemplo,: fazer scam em um site, computadores e até mesmo em servidores. Como na ferramenta Aircrack-ng o Nmap conta com uma documentação detalhada e tutoriais disponíveis na internet, o seu funcionamento é feito por terminal no sistema operacional Kali Linux, utiliza uma série de comandos para fazer o escaneamento da rede ou em outras áreas da computação, e assim será apresentado nos próximos passos.

3.3.1 Descobrir endereços de ips em uma rede

Para encontrar diferentes IPs em uma rede usamos o comando nmap -sP 192.168.0.123/24, onde é apresentada uma lista de IPs conectados à rede, e algumas informações importantes como Mac Address[12] e IP.

[12] Endereço do identificador de componentes de placa de computadores e afins.

Figura 10 – Descoberta de Ip.

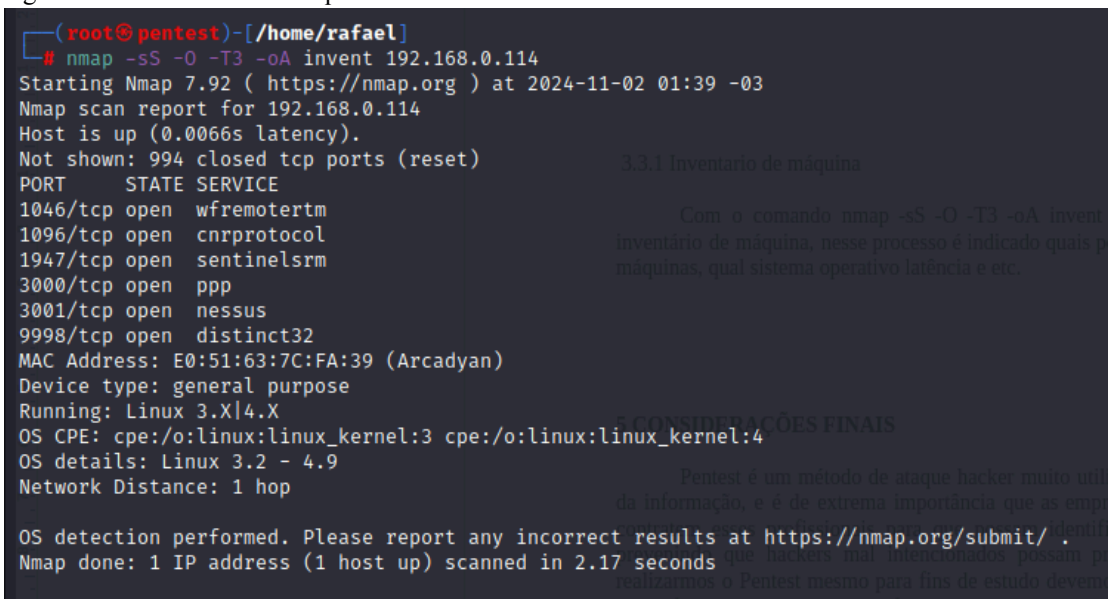


Fonte: Elaborado pelo autor.

3.3.2 Inventário de máquina

Após o comando nmap -sS -O -T3 -oA invent 192.168.0.114 foi possível realizar um inventário de máquina. Nesse processo é mostrado quais portas estão abertas, Mac Address das máquinas, qual sistema operacional, latência, etc.

Figura 10 – Inventário de máquina.

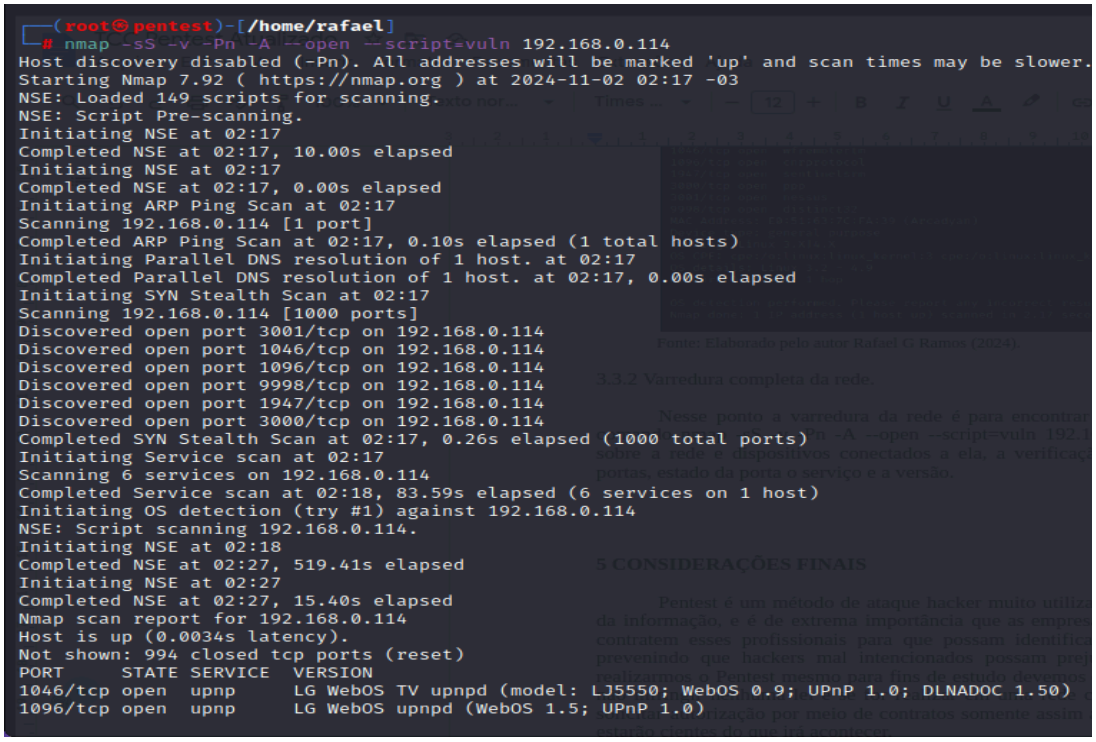


Fonte: Elaborado pelo autor.

3.3.2 Varredura completa da rede.

Nesse ponto, a varredura da rede tem como objetivo encontrar possíveis vulnerabilidades, sendo utilizado o comando nmap -sS -v -Pn -A --open --script=vuln 192.168.0.114, que lista inúmeras informações sobre a rede e dispositivos conectados a ela. A verificação nos mostra as informações de portas, o estado desta, o serviço e a versão.

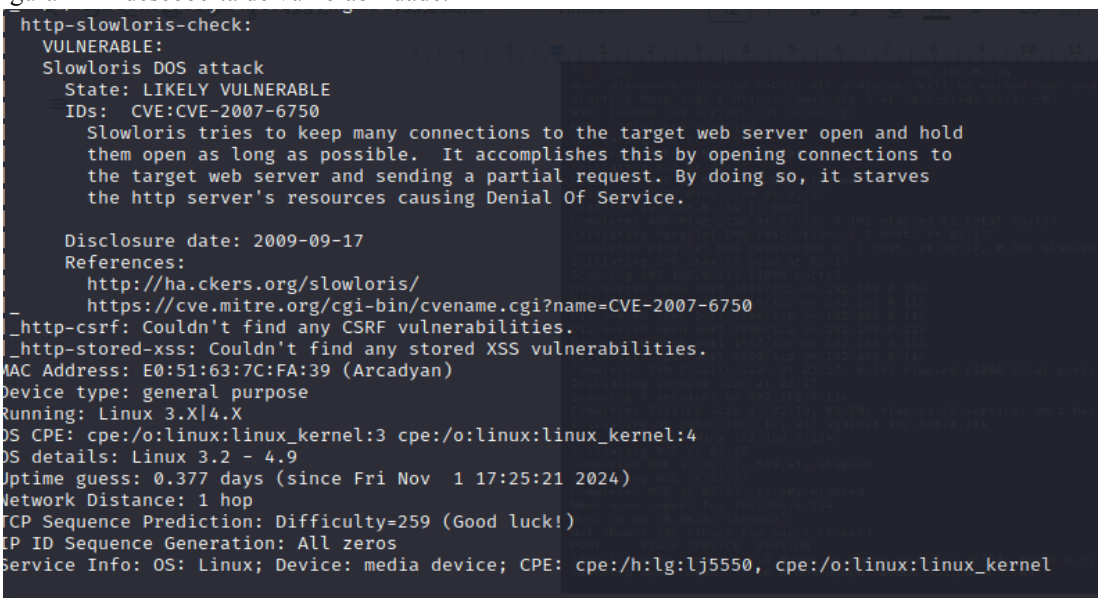
Figura 11 – Varredura da rede.



Fonte: Elaborado pelo autor.

Na imagem abaixo, é mostrado o resultado de um serviço com potencial vulnerável.

Figura 12 – descoberta de vulnerabilidade.



Fonte: Elaborado pelo autor.

4 CONSIDERAÇÕES FINAIS

Diante todo o exposto, o presente trabalho teve como foco Pentest em redes Wi-Fi, destacando metodologias, ferramentas e vulnerabilidades identificadas em ambientes controlados. O pentest é crucial para garantir a segurança de dados corporativos, especialmente frente ao aumento de ataques cibernéticos, como evidenciado por um crescimento de 330% nos últimos anos, conforme citado em pesquisa da Kaspersky.

Os profissionais de segurança da informação oferecem os serviços de consultorias cibernética em redes Wi-Fi e em outros setores como análise de sistemas, serviços e servidores, cujo objetivo consiste em identificar fragilidades em redes corporativas, propor medidas corretivas para fortalecer a segurança e agir em conformidade com legislações vigentes, como por exemplo a LGPD. Após esse processo, é feito um relatório das inseguranças encontradas, e estipulando intervenções que visam reduzir ou remediar os impactos negativos e políticas de segurança.

Com a implementação de medidas adaptativas e o fornecimento de serviços especializados, é possível oferecer soluções robustas, escaláveis e alinhadas às necessidades do cliente.

Na realização do trabalho, foram encontradas dificuldades que demandou a necessidade de atualizar scripts[13] devido a mudanças nas ferramentas utilizadas, causando atrasos no teste e exposição a novas desproteções devido a falhas em atualizações. Para solucionar este problema faz-se necessário criar sequências de comandos personalizados e modularizados, para garantir compatibilidade com atualizações futuras.

Realizar experiências em um ambiente controlado é essencial para evitar implicações legais e éticas, mas isso pode não refletir totalmente o comportamento em redes reais. Deve-se simular cenários complexos utilizando ambientes híbridos (real + virtual) para um melhor aproveitamento dos testes, estes são fundamentais para o mercado de trabalho, tendo em vista que permite que os profissionais de segurança cibernética desenvolvam habilidades, testem e criem ferramentas de defesa que são eficazes, seguras e que agem dentro dos parâmetros estipulados pela Lei.

Cada ferramenta apresentada exige um aprendizado específico e contínuo para acompanhar novas atualizações, realizar treinamentos com a equipe e formular uma documentação do processo, fazendo com que assim se possa deixar as defesas de redes, dados e sistemas, cada vez mais eficientes.

[13] Sequências de comandos que fornecem instruções para o computador realizar tarefas.

REFERÊNCIAS

Geekhunter. Pentest: o que é? Blog de TI. Disponível em: https://blog.geekhunter.com.br/o-que-e-pentest/.
Acesso em: 12 de setembro de 2023.

BOOT, Diego. Top 10 ferramentas de hacking WiFi no Kali Linux. Disponível em: https://imasters.com.br/devsecops/top-10-ferramentas-hacking-wifi-no-kali-linux.
Acesso em: 25 set. 2024.

As 8 ferramentas mais usadas do Kali Linux. Ninja do Linux, 2020. Disponível em: http://ninjadolinux.com.br/as-8-ferramentas-mais-usadas-do-kali-linux/.
Acesso em: 25 set. 2024.

PROFISSIONAIS TI. 10 ferramentas mais usadas para Pentest. 2020. Disponível em: https://www.profissionaisti.com.br/10-ferramentas-mais-usadas-para-pentest/.
Acesso em: 25 set. 2024.

BUCKBEE, Michael. John the Ripper: uma introdução ao decifrador de senhas de código aberto. 2023. Disponível em: https://www.varonis.com/pt-br/blog/john-the-ripper.
Acesso em: 25 set. 2024.

MONDLOCH, Joe. Medusa. 2016. Disponível em: https://en.kali.tools/?p=200.
Acesso em: 25 set. 2024.

Reaver (reaver-wps-fork-t6x) - Penetration Testing Tools, 2016. Disponível em: https://en.kali.tools/?p=346.
Acesso em: 25 set. 2024.

PixieWPS - Penetration Testing Tools. Disponível em: https://en.kali.tools/?p=334.
Acesso em: 25 set. 2024.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal dos delitos informáticos. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm.
Acesso em: 25 set. 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.
Acesso em: 25 set. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais(LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm.
Acesso em: 25 set. 2024.

Nmap. Nmap, 2009. Página inicial. Disponível em: https://nmap.org/.
Acesso em:25 set. 2024.

Aircrack-ng. Aircrack-ng, 2009. Página inicial. Disponível em: https://nmap.org/. Acesso em:25 set. 2024.

SOLYD. Wifite: a ferramenta para pentest em redes sem fio. 2023. Disponível em: https://blog.solyd.com.br/wifite-a-ferramenta-para-pentest-em-redes-sem-fio/. Acesso em: 25 set. 2024.

HYDRA: ferramenta de brute force para testes de segurança. Acaditi, 2024. Disponível em: https://acaditi.com.br/hydra-ferramenta-de-brute-force-para-testes-de-seguranca/. Acesso em: 25 set. 2024.

KASPERSKY. Home office motiva aumento de mais de 330% em ataques usando sistemas de acesso remoto no Brasil. 2020. Disponível em: https://www.kaspersky.com.br/about/press-releases/home-office-motiva-aumento-de-mais-de-330-em-ataques-usando-sistemas-de-acesso-remoto-no-brasil. Acesso em: 25 set. 2024.

WIRESHARK. About Wireshark. Disponível em: https://www.wireshark.org/about.html. Acesso em: 29 nov. 2024.