# **VPN em redes privadas:** criação de VPN para utilização em movimentos laterais

2º sgt (FAB) Huadson **Rudson** Araújo de Carvalho
2º sgt (FAB) **Ewerton** Mota dos Reis
3º sgt (FAB) **Nathália** Nascimento de **Souza**
3º sgt (FAB) **Kellen** Beatriz Ataide dos Santos

Acessar redes internas pode ser uma tarefa desafiadora devido a diversas medidas de segurança implementadas para proteger essas redes contra acesso não autorizado. Existem várias técnicas e ferramentas que podem ser utilizadas para tentar contornar essas medidas de segurança, dentre essas técnicas, a utilização de Virtual Private Network (VPN) se destaca como uma solução atrativa devido ao seu baixo custo, abordagem eficiente e versatilidade na exploração segura e anônima de redes.

A lateralização por VPN, também conhecida como VPN pivoting, consiste em utilizar uma conexão para redirecionar o tráfego de rede através de um servidor intermediário. Essa técnica oferece uma série de vantagens para os profissionais de segurança, pesquisadores e hackers éticos, ao permitir que explorem redes remotas sem comprometer sua identidade ou a segurança de seus dispositivos. (HAMMOUDEH, 2013)

A implantação da técnica pode ser facilitada pelo uso de contêineres. Esse recurso permite o compartilhamento e a implantação simplificada de imagens pré-configuradas, contendo as ferramentas necessárias para a exploração de redes. Essa abordagem aumenta a portabilidade das soluções de exploração e acelera o processo de configuração, tornando-a mais acessível e eficiente. (PIRES, 2020)

Outra possibilidade é sua aplicação em dispositivos móveis. Ao executar o servidor VPN em um dispositivo móvel, torna-se possível executar a técnica de VPN pivoting de maneira mais flexível, devido à facilidade de se transportar e conectar o dispositivo em redes wi-fi. Neste artigo, será explorado com maior profundidade algumas técnicas de lateralização utilizando VPN, suas aplicações práticas e suas limitações. Na prática, três técnicas de implementação da laterização com servidor VPN foram trabalhadas, sendo elas: com host debian, usando contêiner e também o uso de dispositivos móveis, conforme descrito nos apêndices A, B e C, respectivamente. A compreensão e domínio dessas técnicas podem fornecer uma base sólida para a exploração de redes privadas de forma simples, flexível e com boa performance.

A seguir, serão citados alguns casos onde podem ser aplicadas as técnicas de exploração usando VPN pivoting:

a) Pentest remoto em redes corporativas: permite que profissionais de segurança realizem testes de forma remota, explorando a infraestrutura de rede e avaliando a eficácia das medidas de segurança implementadas. Isso inclui a identificação de pontos fracos em firewalls, roteadores, servidores e outros dispositivos de rede, fornecendo insights para aprimorar a segurança e evitar possíveis ataques;

b) Pesquisa em segurança: pesquisadores de segurança e hackers éticos frequentemente utilizam este método para fins educacionais e de conscientização. Esses profissionais exploram ambientes controlados para descobrir e documentar vulnerabilidades em sistemas, aplicativos e dispositivos. Eles podem realizar análises aprofundadas em busca de falhas de segurança, que podem ser relatadas aos desenvolvedores ou fabricantes para que as correções adequadas sejam implementadas;

c) Testes de segurança em aplicativos web: o uso da VPN para movimentos laterais pode ser aplicada em testes de segurança de aplicativos web. Ao utilizer a técnica de tunelamento via VPN, os profissionais de segurança podem redirecionar o tráfego de um servidor intermediário para uma aplicação web em uma rede segregada, analisando as vulnerabilidades existentes, como injeções SQL, cross-site scripting e autenticação inadequada. Isso auxilia no fortalecimento da segurança das aplicações e na proteção dos dados dos usuários.

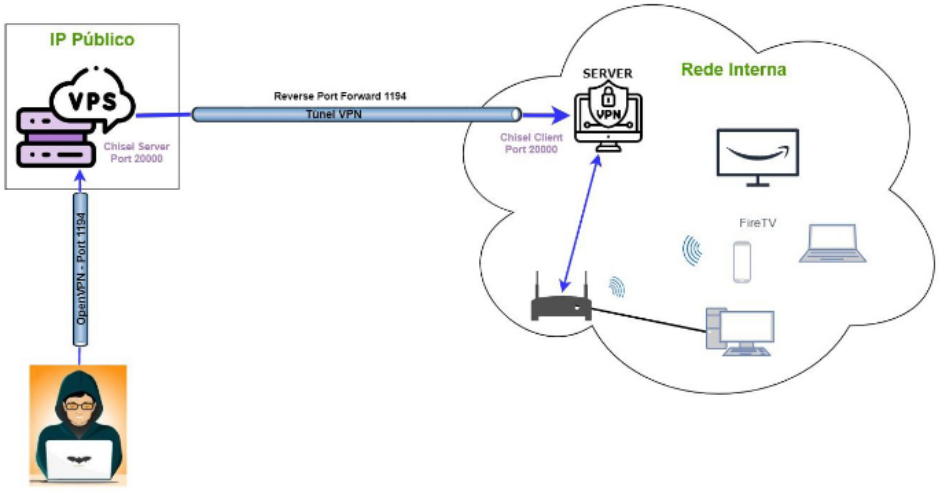
Para que essas atividades funcionem por lateralização, se faz necessário um conjunto de configurações que possibilitem o acesso à rede alvo.

Em uma situação ideal, o acesso a esses ambientes de teste poderiam ser fornecidos através de um serviço de VPN ou através de acesso físico no ambiente a ser testado.

Entretanto, caso não exista esse serviço disponível, um pentester pode levanter um ambiente de VPN próprio, diretamente na rede interna do ambiente a ser testado.

Na imagem abaixo, é possível visualizar como acontece o tráfego de dados para que a conexão entre o pentester e a rede interna a ser analisada seja feita através de um servidor VPN disponibilizado na rede local.

Figura 1 - Estrutura de funcionamento da lateralização por VPN.




Fonte: Autores (2023)

Para viabilizar o acesso a uma rede interna via necessário cumprir duas etapas, sendo elas: VPN conforme o cenário da imagem acima, é

Quadro 1 – Fases de criação do ambiente

| Passo | Funcionamento |
|---|---|
| 1 | Criação do servidor VPN no dispositivo que servirá como ponto de acesso para a rede alvo; |
| 2 | Inicialização do chisel server em uma VPS; |
| 3 | Execução do chisel client no mesmo dispositivo do VPN server. Esse passo tem como objetivo criar um reverse port forwarding, utilizando a VPS como pivô, de modo a direcionar o tráfego que chegue na porta 1194 da VPS para a porta 1194 da máquina com o servidor VPN, que estará na rede interna. |

Quadro 2 – Fases de conexão na VPN

| Passo | Funcionamento |
|---|---|
| 1 | A máquina atacante solicita pela internet à VPS conexão VPN na porta 1194 |
| 2 | A VPS por sua vez, recebe a solicitação na porta 1194 e através do túnel reverso criado pelo chisel, encaminha a requisição para a porta configurada para a estação com o VPN server na rede local; |
| 3 | O servidor VPN recebe a solicitação do cliente através do encaminhamento e retorna as informações para VPS através do encaminhamento do chisel; |
| 4 | Se estabelece uma conexão com o serviço na rede local. O pentester, então, pode se conectar aos dispositivos existentes na rede interna, através da VPN. O tráfego de dados é criptografado e transmitido de forma segura entre o cliente e o servidor VPN. |

Fonte: Autores (2023)

Neste momento, o atacante tem acesso à rede onde está o servidor de VPN, podendo explorar toda ela como se localmente lá estivesse. Cabe ressaltar que essa transferência de dados ocorre de maneira criptografada, garantindo a confidencialidade das informações transmitidas. A utilização do redirecionamento de portas com chisel permite que o cliente acesse os serviços através da internet de forma transparente, como se estivesse conectado diretamente à rede do alvo. (Pillora, 2022)

Os passos de configuração citados podem ser automatizados, com fito de facilitar ainda mais sua implementação e acelerar a configuração, pra isso, o uso de contêineres pré-configurados, como os disponíveis no Docker Hub, simplificam e agilizam a implementação dos servidores de VPN bem como sua lateralização,

fornecendo uma distribuição padronizada de ferramentas e ambientes. Isso reduz o tempo e o esforço necessários para preparar o ambiente de exploração, permitindo que os profissionais de segurança se concentrem diretamente nas atividades de teste e análise. (Positivo Tecnologia, 2017)

Além disso, a facilidade de uso dos contêineres é um fator que torna essa prática mais acessível, em poucos comandos é possível controlar o ambiente de exploração, iniciando, parando e reiniciando os contêineres conforme necessário. Em síntese, a utilização de contêineres pré-configurados oferecem benefícios práticos, como simplificação da implementação, portabilidade, segurança aprimorada e uma experiência de uso mais intuitiva, sendo amplamente adotada na comunidade de segurança para otimizar o processo de exploração de redes.

Outra possibilidade de técnica, seria o uso de dispositivo móvel operando kernel linux com OpenVPN server. O fato de ser um dispositivo de tamanho físico reduzido torna-o mais discreto, facilitando a anonimização física durante as atividades de exploração. Essa estratégia possibilita que os profissionais de segurança realizem testes em redes wi-fi de maneira anônima, assegurando que suas atividades não despertem atenção indesejada.

Em suma, a utilização de um dispositivo portátil com um kernel Linux e servidor VPN oferece uma combinação de mobilidade, segurança e anonimato físico no contexto de exploração de redes através de um ponto de acesso wireless. Essa abordagem possibilita que profissionais de segurança realizem a exploração na rede de maneira eficiente, discreta e segura. (D'Aquino, 2014).

Para a criação do servidor VPN em dispositivos móveis, iremos utilizar o NetHunter, que consiste em uma plataforma de segurança cibernética baseada no sistema operacional Kali Linux, projetada para dispositivos móveis Android. Ela fornece ferramentas e recursos para pentest e avaliação de vulnerabilidades, permitindo executar ferramentas do Kali em um dispositivo Android.

Vale ressaltar que o NetHunter na sua versão completa, está disponível somente em alguns modelos de aparelhos específicos.

Do exposto, percebe-se que o pivoteamento via VPN pode ser realizado de diferentes formas, cada uma tendo suas particularidades.

A adoção de contêineres pré-configurados agilizam a implantação do ambiente, através da utilização de máquinas previamente configuradas.

A criação do ambiente utilizando dispositivos móveis pode ser um pouco mais complexa, porém, tem como vantagem a discrição física e a mobilidade, permitindo que os profissionais de segurança realizem testes de penetração em redes de forma discreta e eficiente.

Portanto, as técnicas de exploração de rede utilizando movimentos laterais por VPN, mencionadas e trabalhadas neste projeto, podem proporcionar aos profissionais de segurança recursos para realizar análises e testes em redes de maneira remota, segura e eficaz.

Essas abordagens otimizam o processo de exploração, garantem a privacidade e a confidencialidade das informações, além de permitir que várias pessoas acessem o mesmo ambiente de testes, de maneira remota e sem a necessidade da criação de servidores de VPN da organização a ser testada.

## REFERÊNCIAS BIBLIOGRÁFICAS


D'AQUINO, Fernando. Kali NetHunter: o software que transforma o Android em uma arma hacker. Tecmundo. 2014. Disponível em: https://www.tecmundo.com.br/ataque-hacker/63603-kali-nethunter-software-transforma-o-android-arma-hacker.htm. Acesso em: 19 maio 2023.

HAMMOUDEH, Ayman. VPN Pivoting. Infosec. 2013 Disponível em:https://www.fir3net.com/security/concepts-and-terminology-security/vpn-pivoting-explained.html. Acesso em: 23 maio 2023.

KALI. Documentação nethunter. Kali Nethunter. 2023. Disponível em: <https://www.kali.org/docs/nethunter/>. Acesso em: 23 maio 2023.