Definição de ambiente de Pentest aplicado a redes abertas

Resumo
As configurações apresentadas foram fundamentais para a execução deste trabalho, uma vez que a ferramenta Kali Linux, é um sistema operacional baseado em Linux voltado para a segurança cibernética, e oferece um conjunto de ferramentas destinadas a testes de intrusão. Entre essas ferramentas destacam-se o Escaneamento de Redes, o Monitoramento de Dispositivos, o uso de protocolos como Nmap e ARP entre outras funcionalidades. Essas ferramentas permitem identificar, explorar e corrigir vulnerabilidades presentes em sistemas e redes, contribuindo para a segurança da infraestrutura tecnológica.

Kali Linux

- Kali Linux é uma distribuição GNU/Linux baseada no Debian, considerado o sucessor do Back Track. O projeto apresenta várias melhorias, além de mais aplicativos. É voltado principalmente para auditoria e segurança de computadores em geral. É desenvolvido e mantido pelo *Offensive Security Ltd.* Desde 21 de janeiro de 2016, é uma distribuição “rolling-release”.
- O Kali Linux dispõe de numerosos softwares pré-instalados, incluindo o Nmap (port scanner), Aircrack-ng (software para testes de segurança em rede de computadores).

Instalação
O Kali Linux permite a instalação em arquiteturas i386, amd64 e ARM (armel e armhf), para a arquitetura i386, a imagem do Kai, traz um kernel PAE por padrão, podendo assim ser executado em sistemas com mais de 4 GB de RAM. O sistema pode ser instalado a partir de um DVD ou um Live USB, também permite a instalação via rede.

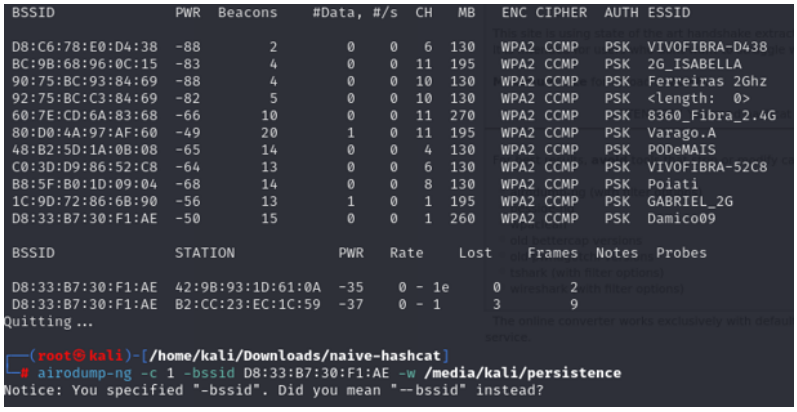
Ferramentas

- Escaneamento das redes
- Monitoramento da rede
- Leitura dos dispositivos conectados à rede
- Nmap (portscan)
- ARP

Essas ferramentas podem ser usadas para inúmeros propósitos, a maioria envolve exploração de falhas em uma rede de computadores ou aplicação, realização de descoberta de computadores na rede, ou escaneamento de um alvo específico na rede pelo endereço IP. Muitas ferramentas da versão passada foram eliminadas para focar nas mais populares e efetivas para testes de segurança.

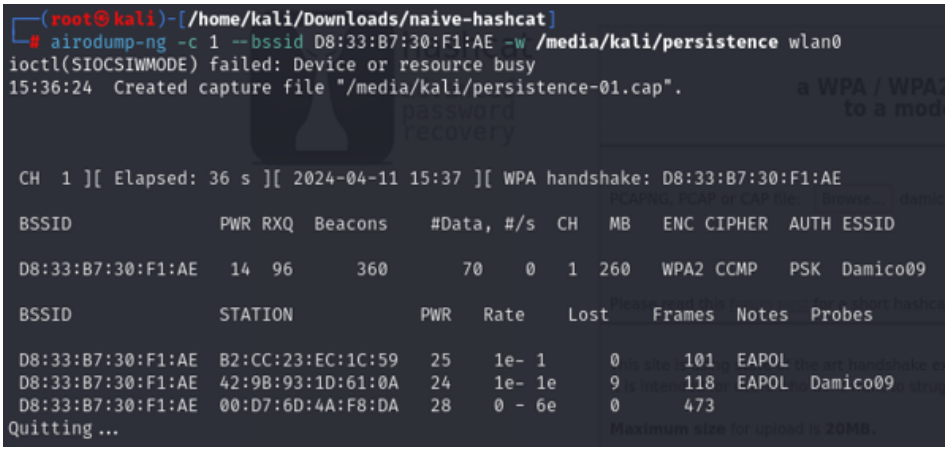
Escaneamento das redes

- Busca mostrar todas as redes locais disponíveis.
- Comando: **airodump-ng**



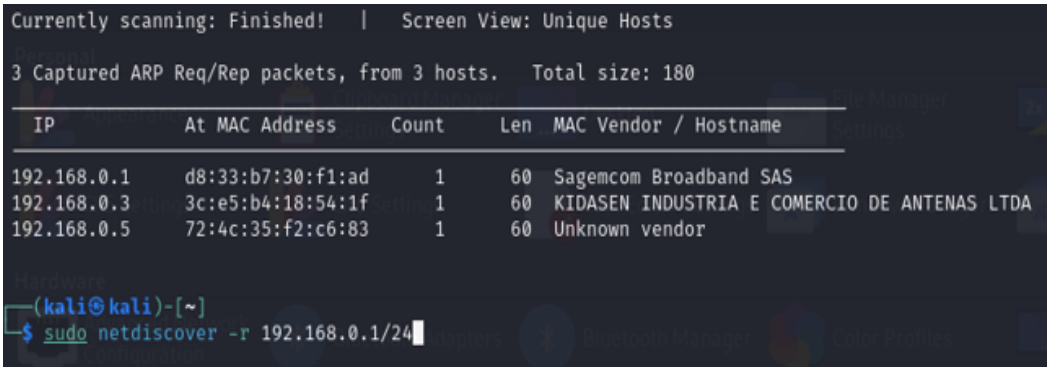
Monitoramento da rede

- Mostrar quais dispositivos estão conectados e quais vão se conectar
- Comando: **airodump-ng -c**



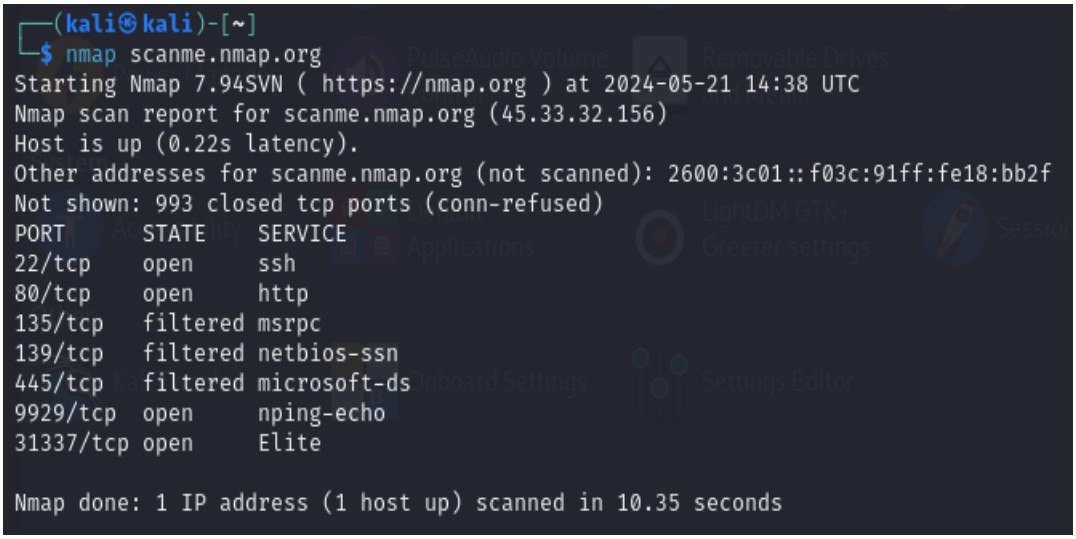
Leitura dos dispositivos conectados à rede

- Leitura limpa e apresenta os IPs associados
- Comando: **netdiscover -r**



Nmap(portscan)

- Mostrar as portas do servidor online
- Comando: **nmap scanme.nmap.org**



ARP

- Realizar um escaneamento de uma subrede, com o endereço mac de origem
- Comando: **arp-scan -l**