UFRR

Kali-Linux

Fernando Souza Rodrigues
Paulo Ferreira da Silva Júnior

UFRR

O que é o Kali Linux?

O Kali Linux é uma distribuição de segurança baseada no Debian, que tem como objetivo realizar testes de penetração e análise forense. Com mais de 600 ferramentas pré-instaladas, como scanners de vulnerabilidades, sniffers de rede e ferramentas de engenharia reversa, o Kali Linux é amplamente utilizado por profissionais de segurança cibernética. Ele possui uma interface gráfica de usuário (GUI) amigável e intuitiva, o que o torna acessível até para iniciantes. Além disso, o Kali Linux suporta a execução em máquinas virtuais.

UFRR

História do Kali Linux

O Kali Linux originou-se como o BackTrack Linux em 2006, uma distribuição focada em testes de penetração e análise forense. Em 2013, foi substituído pelo Kali Linux, que se tornou a distribuição de segurança mais popular do mundo. O Kali Linux é usado por hackers éticos, profissionais de segurança cibernética e pesquisadores para avaliar a segurança de sistemas e redes.

UFRR

Principais recursos do Kali Linux

O Kali Linux utiliza o kernel Linux 6.10, que traz melhorias em segurança, desempenho e suporte a novos hardwares. O kernel personalizado possui patches de segurança e módulos específicos para ferramentas de hacking e testes de penetração, tornando o sistema operacional robusto e seguro para profissionais de segurança cibernética. Isso permite que os usuários realizem suas atividades com eficácia e confiança.

UFRR

Principais recursos do Kali Linux

O Kali Linux é uma distribuição de segurança com mais de 600 ferramentas pré-instaladas. Ele inclui scanners de vulnerabilidades, sniffers de rede, ferramentas de engenharia reversa e muito mais. O Kali Linux é conhecido por suas ferramentas populares, como Metasploit, Nmap, Wireshark e Maltego. Além disso, ele suporta dispositivos ARM, permitindo seu uso em dispositivos móveis, proporcionando conveniência e flexibilidade aos usuários.

UFRR

Principais Softwares do Kali Linux

- ***Maltego:*** *é uma ferramenta de inteligência visual de código aberto. Ela ajuda na coleta e análise de informações, mapeando relacionamentos entre pessoas, empresas e domínios, auxiliando em investigações e análises.*

- ***Wireshark:*** *É uma ferramenta de análise de tráfego de rede. Ele permite capturar e examinar pacotes de dados em tempo real, ajudando a identificar problemas de rede.*

- ***Metasploit Framework:*** *É um conjunto de ferramentas de teste de penetração. Ele fornece uma plataforma para descoberta de vulnerabilidades, desenvolvimento de exploits e realização de ataques controlados para testar a segurança de sistemas e redes.*

UFRR

Principais Softwares do Kali Linux

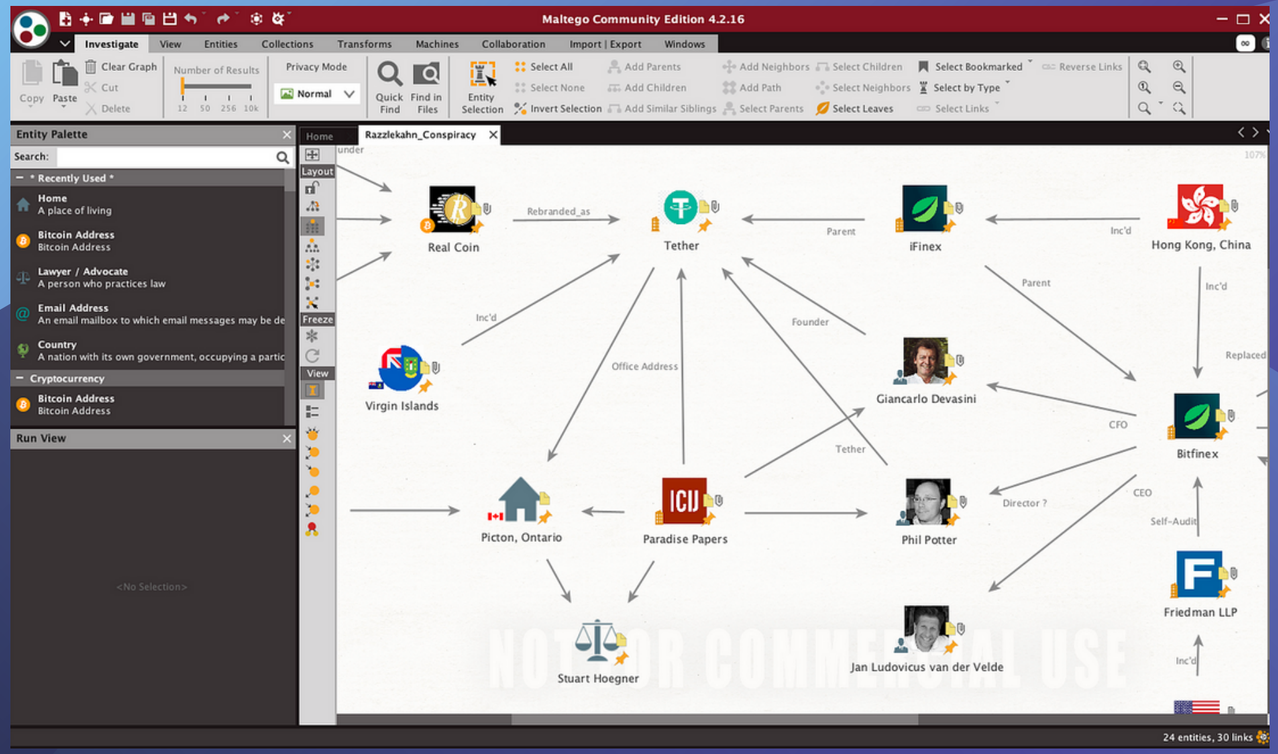
- ***Burp Suite:*** *é uma suíte de ferramentas para testes de segurança de aplicativos web. Ele possui recursos como proxy, scanner de vulnerabilidades e explorador de sequências de caracteres, usados para identificar e corrigir falhas de segurança em sites e aplicativos.*

- ***Nmap:*** *É um scanner de rede que permite descobrir hosts, serviços e portas em uma rede. Ele é usado para mapear e verificar a segurança da rede.*

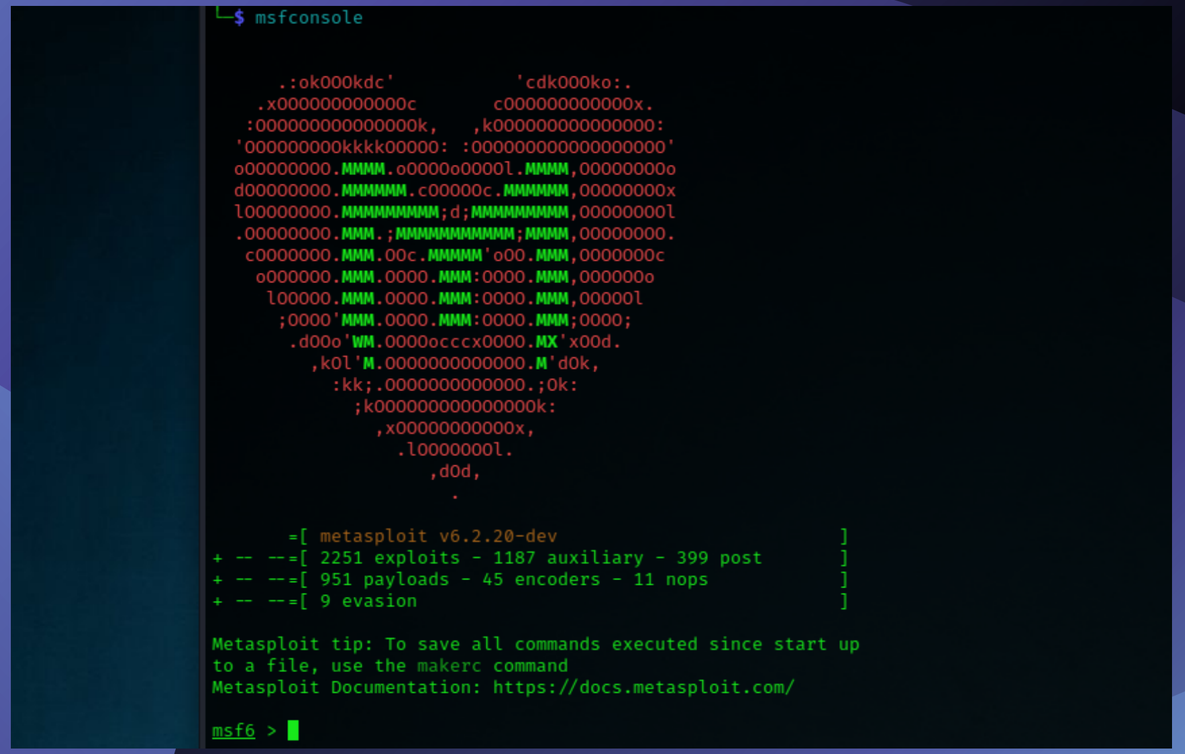
- ***Hydra:*** *é uma ferramenta de quebra de senhas e autenticação em serviços remotos. Ela realiza ataques de força bruta ou de dicionário para testar a força das senhas e identificar vulnerabilidades em sistemas autenticados.*

UFRR

Principais Softwares do Kali Linux



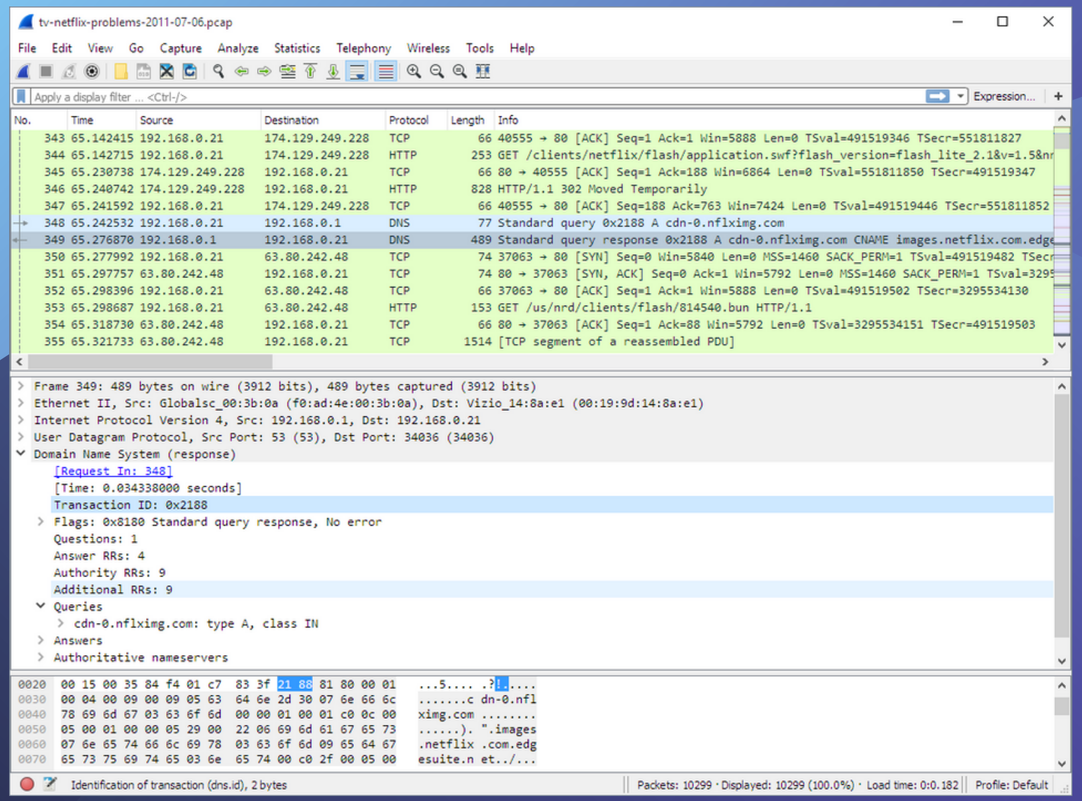
Maltego



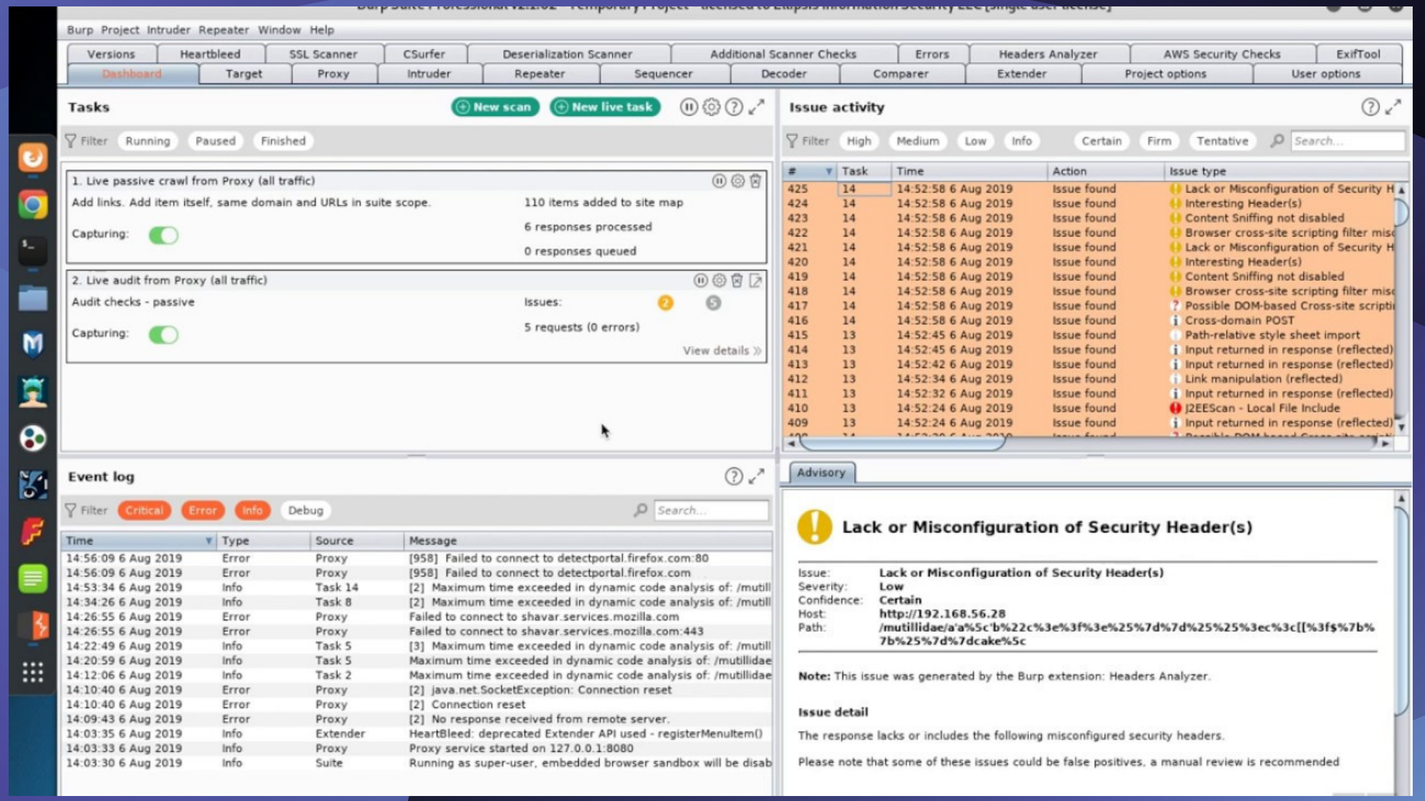
Metasploit

UFRR

Principais Softwares do Kali Linux



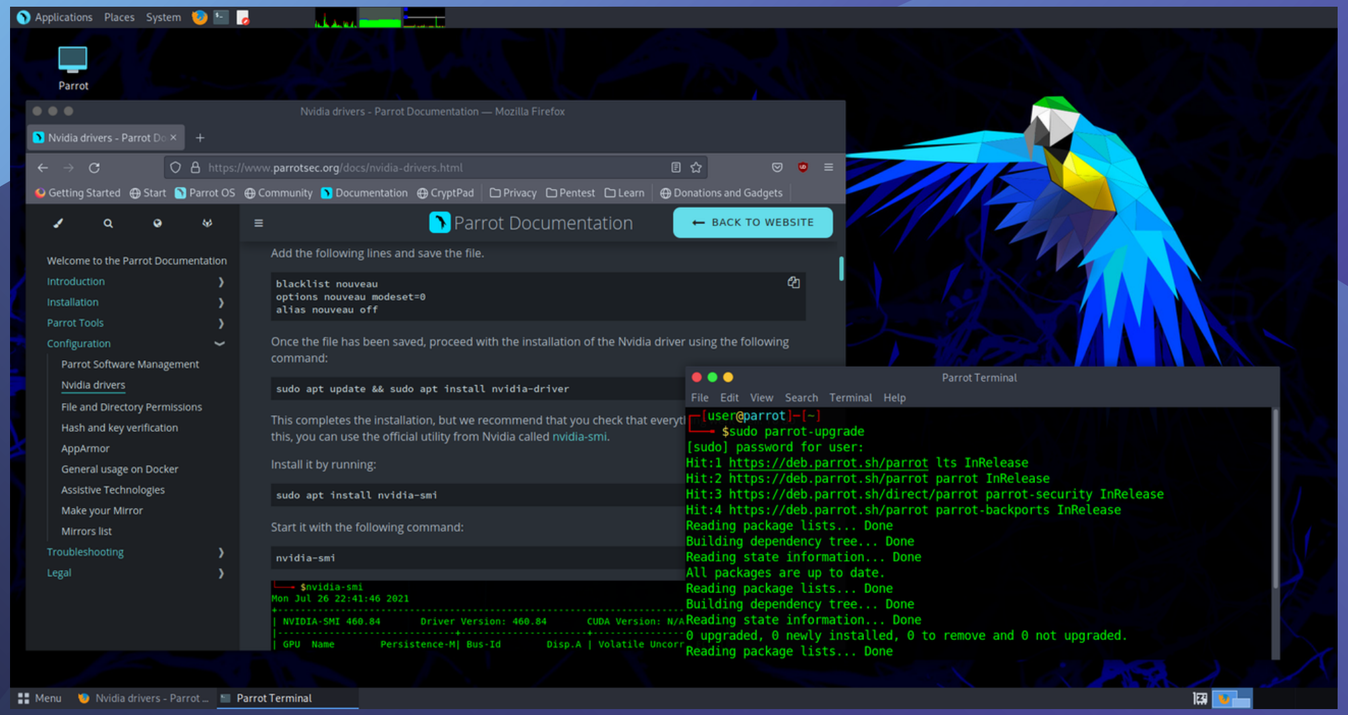
Whireshark



BurpSuit

UFRR

Spin-Offs



Parrot Security

BackBox

UFRR

Respostas referentes às perguntas feitas na apresentação

TPM2, SecureBoot e descriptografia de armazenamento automatizado:

- *Kali Linux tem suporte para o TPM 2.0 (Trusted Platform Module 2.0) que é um processador de criptografia instalado nas placas-mãe que oferece segurança durante a inicialização do sistema operacional.*

Gerenciador de Pacotes:

- *O gerenciador de pacotes padrão do Kali é o APT (Advanced Package Tool) que facilita a instalação, atualização, remoção e gerenciamento de pacotes de software. Além do APT, o Kali Linux também suporta o uso de outros gerenciadores de pacotes, como o dpkg (que é a ferramenta de baixo nível subjacente ao APT) e o aptitude. Os tipos de pacotes padrão aceitos pelo APT são .deb, extensão padrão dos sistemas derivados do Debian.*


LINUX
#MELHOR DISTRO DO LINUX
OBRIGADO. ☺