(Hardware)

1. Hardware Keylogger



O Keylogger de hardware é um dispositivo físico, comumente prototipado em portas USB, que é

desenvolvido para captar todas as teclas digitadas pelo usuário. Ele funciona plugado ao teclado da

vítima na porta USB fêmea do dispositivo e ao USB macho no computador. Tem a vantagem de não

ser detectado por antivírus, já que funciona como um extensor do teclado e ser pequeno, podendo

passar despercebido. O log das teclas digitadas pode tanto ser armazenado no dispositivo, quanto

transmitido por Wi-Fi, dependendo do modelo.

2. USB Rubber Ducky



O Rubber Ducky é um dispositivo que tem semelhança com um pen drive, com uma ponta USB

macho, e consegue simular um teclado. Tem como o objetivo de simular diversos ataques. No seu

interior, há um script que pode ser editado conforme a necessidade. É possível inserir instruções

para tentar roubar informações de redes, injetar teclas que possam causar algum tipo de dano ao

sistema ou deixar um backdoor.

3. Shark Jack

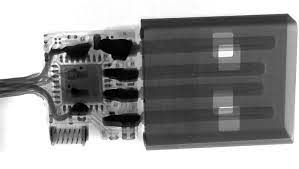


Shark Jack é um dispositivo voltado para ataques de rede. Possui uma porta rj45 na extremidade e

tem como objetivo coletar diversas informações referentes a infraestrutura e firewall e até

mesmo realizar injeções de comandos ao inseri-la em algum ponto de rede.

4. Cabo O.MG



Este cabo que aparenta ser um simples carregador de celular, na verdade, é um cabo malicioso que,

caso conectado a um computador, consegue capturar tudo o que for digitado e encaminhado para o

hacker a partir de um ponto de acesso Wi-Fi em uma interface web

5. RaspBerry



O Raspberry é um microcomputador totalmente modular, capaz de ser atrelado a outros

componentes e realizar diversas funções através de uma codificação. Consegue realizar ataques de

rastreamento, captação de ondas de rádio e até hackear redes Wi-Fi.

(Software)

1. Kali Linux



A mais famosa e querida entre os hackers éticos, a Kali é uma distro baseada no Debian e reúne

mais de 600 ferramentas forenses e pentest pré-instaladas disponíveis para o atacante utilizar e

sempre recebem atualizações continuamente. Possui a ferramenta NetHunter, capaz de realizar

testes de invasão em dispositivos Android.

2. Pentoo



A Pentoo uma distro conhecida por ter uma gama de testes de invasão e avaliações específicas para

redes e infraestruturas. Foi desenvolvida baseando-se na Gentoo e possui versões de 32 e 64 bits.

3. Parrot Security OS



A Parrot é uma distro mais leve e amigável que, assim como o Kali, é baseada no Debian e possui

inúmeros pentests e ferramentas específicas de mitigação de vulnerabilidades e de computação

forense. Ela utiliza repositórios do Kali para rodar as ferramentas, apesar de vir com em menor

quantidade. Diferente da Kali, a Parrot não possui suporte para dispositivos Android.

Dentro destas distribuições e de outros sistemas operacionais, podemos encontrar e instalar

inúmeras ferramentas de pentest. Veja abaixo algumas das mais populares.

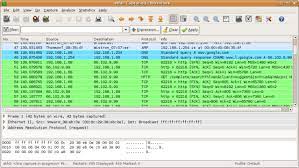
4. NMap



Já mencionado anteriormente no Footprint, é uma ferramenta extremamente rápida e eficaz capaz

de mapear toda a rede e dispositivos, além da utilização do firewall.

5. Wireshark

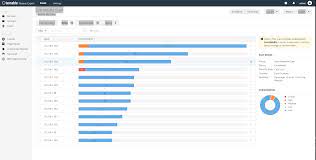


A Wireshark é uma das ferramentas com foco em redes mais populares no Linux. Ela consegue

realizar uma monitoração dos pacotes de dados que estão trafegando pela rede em tempo real,

emitir logs mais complexos e analisar os protocolos de rede.

6. Nessus



Esta ferramenta é capaz de escanear e detectar vulnerabilidades em um computador de maneira

remota. Ela não tem como objetivo acabar com a falha, mas sim realizar mais de 1200 verificações

predefinidas, identificando problemas e reportando. É uma ferramenta desenvolvida para quebrar

senhas(cracking). É possível realizar ataques de força bruta contra as senhas criptografadas e

trabalhar com dicionários. Seu ataque é focado em serviços offline.

7. Hydra



Hydra permite realizar procedimentos de ataque de força bruta contra serviços de autenticação

online, tendo suporte a dezenas de protocolos, como por exemplo os FTP’s, HTTP, Banco de dados,

SHH, entre outros.

8. Fern Wifi Cracker



É uma ferramenta que tem como objetivo quebrar a segurança de redes sem fio do tipo WPS, WEP

e WPA, executando ataques de força bruta e com dicionários.

OBS.: O Projeto Metasploit é um projeto de segurança de computadores que fornece informações

sobre vulnerabilidades de segurança e ajuda em testes de penetração e desenvolvimento de

assinaturas IDS. É propriedade da Rapid7, empresa de segurança sediada em Boston,

Massachusetts. Metasploit pode ser integrado com outras ferramentas de segurança, como Nmap

para varredura de rede. Sua força reside na extensa base de dados de exploits, payloads, e módulos

que permitem a automatização de ataques e exploração de falhas de segurança conhecidas.