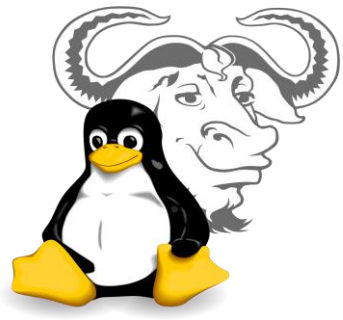
Vamos falar um pouco da história do GNU/LINUX, o que é Kernel, e também o porque do nome GNU/LINUX. Uma breve introdução sobre o que e distribuição(distro), falar um pouco de algumas das principais delas. Em seguida vamos falar também sobre as principais distribuição de "testes de penetração(pentest)".



O que é o GNU/LINUX ?

Muita gente confunde Linux com sistema operacional. Digamos que parcialmente não esteja errado. O Linux(núcleo, coração do sistema), ele e responsável pelo funcionamento do computador, faz a comunicação entre *HARDWARE*(teclado, mouse, impressora, monitor) e o *SOFTWARE(*os aplicativos em geral). A junção do Kernel com os demais programas responsáveis por interagir é o que denominamos sistema operacional.

O GNU/LINUX tem algumas características.

- Ele e um sistema multiusuário – Permite criar vários usuários e configurações individuais para vários usuários diferentes.
- E um sistema também multitarefa – Pode executar vários programas ao mesmo tempo.
- Multi-plataforma – Pode ser executado em uma grande variedade de computadores.

Em agosto de 1991, Linus Torvarlds, Filandês, estudante da Universidade de Helsinki na Finlândia, em uma lista de discussão na internet anunciou que estava criando um sistema operacional livre.

Em 5 de outubro do mesmo ano, Linus anuncio oficialmente a primeira versão do LINUX. Com o passar do tempo, o LINUX se tornou um dos mais populares sistemas. E assim foi continuamente desenvolvido pelo próprio Linus e por pessoas do mundo inteiro.

O que e o Kernel ?

Quando comecei a usar o GNU/LINUX, vi várias vezes a palavra Kernel, e me perguntava o que seria isso. Depois de várias pesquisadas, fuçadas fui entendendo pouco a pouco o que era o Kernel. Vou tentar ser bem específico e resumido para melhor entendimento sobre o Kernel.

O Kernel é o núcleo do sistema("O coração do sistema"), ele controla todo o

hardware. Mas o Kernel em si não funciona sozinho, não tem nenhuma utilidade, ele precisa de aplicativos, como os aplicativos precisam do Kernel. Um precisa do outro pra "sobreviver".

O Kernel tem atualizações constantes, para que a cada atualização possa ter mais suporte a novas tecnologias. São acrescentados novos módulos, ou melhora o suporte para módulos já existentes. Para ficar mais compreensível, módulos são a mesma coisas que os drivers no "*windows*". Os módulos são bastante úteis, com a atualização de novos módulos o administrador ou usuário pode apenas instalar o módulo novo. Também tem a necessidade de recompilar o kernel, não sendo obrigado, mais pelo fato de ganhar mais estabilidade, performance, e também aumentar o suporte ao *hardware.* Para um usuário leigo isso pode ser bastante complexo.

Porque GNU/LINUX ?

Muitas pessoas devem pensar o porque GNU/LINUX, é não apenas LINUX. Uma breve explicação sobre essa dúvida que talvez muita gente não saiba.

Bem, antes de explicar podemos levar em consideração uma analogia bem simples, chamar o sistema apenas de Linux, e o mesmo que você se referir a um carro somente pelo motor. O GNU seria todo o resto.

Como vimos na explicação acima, o Linux é apenas o Kernel. Quando falamos "sistema linux", "distribuição linux", está errado. Na realidade, distribuições ou sistemas baseados no Linux("kernel"). As expressões citadas falham não mencionando os programas que sempre completam o Kernel, entre eles estão os programas desenvolvido pelo projeto GNU. Então o modo de dizer GNU/LINUX reconhece a importância das contribuições feitas pelo projeto GNU.

O que são as distribuições Linux ?

De forma bem resumida, uma distribuição Linux, é um conjunto e *softwares*, ferramentas, utilitários, mantendo como base o Kernel do Linux. Existem diversificadas distribuições Linux. E algumas são criadas com interesses específicos. Exemplo: Mais suporte para web, firewall, banco de dados, entre outros serviços. Dentre essas distribuições que tem suas especificidades utilizam o kernel do Linux e tem seus utilitários, ferramentas.

A seguir vamos falar de algumas distribuições, as mais usadas. Lembrando que existem várias e várias distros, mais vamos conhecer algumas e suas funcionalidades.

Debian

Projeto Debian é uma associação de indivíduos que têm como causa comum criar um sistema operacional livre. O sistema operacional que criamos é chamado **Debian GNU/Linux**, ou simplesmente **Debian**.

Um sistema operacional é o conjunto de programas básicos e utilitários que fazem seu computador funcionar. No núcleo do sistema operacional está o kernel. O kernel é o programa mais fundamental no computador e faz todas as operações mais básicas, permitindo que você execute outros programas. Os sistemas Debian atualmente usam o kernel Linux. O Linux é uma peça de software criada inicialmente por Linus Torvalds com a ajuda de milhares de programadores espalhados por todo o mundo. No entanto, há trabalho em andamento para fornecer o Debian com outros kernels, primeiramente com o Hurd. O Hurd é um conjunto de servidores que rodam no topo de um micro kernel (como o Mach), os quais implementam diferentes características. O Hurd é software livre produzido pelo projeto GNU. Uma grande parte das ferramentas básicas que formam o sistema operacional são originadas do projeto GNU; daí os nomes: GNU/Linux e GNU/Hurd. Essas ferramentas também são ferramentas livres. Claro que o que todos queremos são aplicativos: programas que nos ajudam a conseguir fazer o que desejamos fazer, desde edição de documentos até a administração de negócios, passando por jogos e desenvolvimento de mais software. O Debian vem com mais de 43000 pacotes (softwares pré-compilados e empacotados em um formato amigável, o que faz com que sejam de fácil instalação em sua máquina) — todos eles são livres. É mais ou menos como uma torre: Na base dela está o kernel. Sobre ele todas as ferramentas básicas e acima estão todos os outros softwares que você executa em seu computador. No topo da torre está o Debian — organizando e arrumando cuidadosamente as coisas, de modo que tudo funcione bem quando todos esses componentes trabalham em conjunto.

Site: https://www.debian.org

Ubuntu 

A distro Ubuntu foi desenvolvido em outubro de 2004 pela empresa Canonical, fundada por Mark Shuttleworh, um empreendedor Sul-Africano. Ubuntu é uma distribuição derivada do Debian. Atualmente e uma das distribuições mais populares e usadas por usuários que migram do sistema Windows para o mundo GNU/LINUX. Ele visa preocupar muito com o usuário final(desktop). O Ubuntu tem o ambiente Unity como padrão, mais nada impede que o usuário instale outros ambientes, como KDE, GNOME, entre outras, mas isso não impede o usuário de instalar qualquer outra interface gráfica que vai agradar o seu gosto. Algumas versões. O Ubuntu tem versões LTS(Longo tempo de suporte), o que seria isso?! Ele recebe suporte com atualizações por cinco anos, por questão de suporte estendido, a versão LTS é indicada para usuários que buscam estabilidade. Ao contrário das versões comuns o usuário pode atualizar uma versão LTS diretamente para outra versão LTS, sendo assim não precisa passar pelas versões comuns. Já as versões comuns do Ubuntu recebem suporte da Canonical e as atualizações por um ano e cinco meses. Você pode atualizar para uma

versão mais recente e assim ter a garantia de mais um ano e seis meses de atualizações de segurança e também os programas.

Principais características do Ubuntu:

- Fácil de instalar;
- Fácil de usar;
- Fácil de instalar programas;
- Uma grande variedade de programas disponíveis;
- Muita compatibilidade com Hardware;
- Leve;
- Seguro;
- Gratuito;

FEDORA

Fedora(antigamente chamado Fedora Core), é uma distribuição Linux, baseada em pacotes RPM(Red Hah Package Manager), e usa o método de atualização yum(Yellowdog Updater, Modified), patrocinado pela Red Hat. Atualmente mantida pelo projeto Fedora. O sistema Fedora tem como padrão o ambiente gráfico GNOME, podendo ser mudado para KDE, XFCE, entre outros ambientes. As versões testes do Fedora foram iniciadas a partir de julho de 2003 e em março de 2004 saiu a primeira estável. O Fedora é um sistema que pode ser usado tanto para servidores quanto para desktop.

Principais características do Fedora:

- Fedora é completamente grátis e consiste em software livre ou aberto;
- Fácil utilização, mesmo para usuários inexperientes em GNU/LINUX;
- Instalador Anaconda, um dos mais fáceis utilizados atualmente.
- Inúmeros programas divididos por temas, que podem ser selecionados na instalação ou através do gerenciador de pacotes.

Entre várias outras características que torna o sistema confiável e estável.

centOS

O **CentOS**, abreviação de **Community Enterprise Operating System**, é uma distribuição Linux de classe Enterprise derivada de códigos fonte gratuitamente distribuídos pela Red Hat Enterprise Linux e mantida pelo CentOS Project. O CentOS, foi apontado como uma das melhores distros para o uso em servidores.[1] A numeração das versões é baseada na numeração do Red Hat Enterprise Linux. Por exemplo, o CentOS 4 é baseado noRed Hat Enterprise Linux 4. A diferença básica entre um e outro é o fornecimento de suporte pago na aquisição de um Red Hat Enterprise Linux. Funcionalmente, pode-se considerar os sistemas clones. CentOS proporciona um grande acesso aos softwares padrão da indústria, incluindo total compatibilidade com os pacotes de softwares preparados especificamente para os sistemas da Red Hat Enterprise Linux. Isso lhe dá o mesmo nível de segurança e suporte, através de updates, que outras soluções Linux Enterprise, porém sem custo. Suporta tanto ambientes de servidores para aplicações de missão crítica quanto ambientes de estações de trabalho e ainda possui uma versão Live CD. CentOS possui numerosas características, incluindo: uma comunidade activa e crescente, um rápido desenvolvimento e teste de pacotes, uma extensa rede para *downloads*, desenvolvedores acessíveis, múltiplos canais de suporte incluindo suporte em português e suporte comercial através de parceiros.

No dia 7 de janeiro de 2014 a Red Hat anunciou a incorporação do projeto e comunidade CentOS aos seus portfólio. Segundo anúncio essa incorporação trará benefícios para a comunidade de usuários de ambas as distribuições, gerando maiores inovações nos projetos livres adotados e para toda a arquitetura corporativa.

Distribuições para testes de penetração.

Existem várias distribuições voltadas principalmente para testes de penetração(*pentest*) , para que profissionais da área de Segurança da Informação possam trabalhar exclusivamente para a detecção de diversos tipos de vulnerabilidades. A seguir vou falar de algumas das principais distribuições utilizadas.

Kali Linux

A mais nova versão de uma distribuição voltada para testes de penetração(pentest). Disponibilizada pela *Offensive Security*, o Kali e uma distro completa para auditores, analistas de segurança, hackers éticos, etc, a procura de vulnerabilidades de diversos tipos, tais como: servidores, servidores web, redes sem fio(wifi), entre muitas outras

vulnerabilidades e tipo de serviços. O Kali na versão mais atual possui uma variedade de mais de trezentas ferramentas, novas ferramentas inclusas. São organizadas de acordo com o fluxo de trabalho pelos profissionais. A estrutura também permite que até usuários novatos possam encontrar ferramentas relacionadas a uma tarefa específica.

Site: https://www.kali.org

BackTrack

Sistema também voltado para testes de penetração(pentest), muito utilizado por auditores, analistas de segurança, hackers éticos, etc. A criação do sistema teve uma combinação de duas outras distribuições bem difundidas. *WHAX*, e Auditor. Foi criado e disponibilizado também pela *Offensive Security.*

Site: www.backtrack-linux .com

Vamos falar um pouco sobre semelhanças e as diferenças dos dois sistemas.

Existem algumas semelhanças entre o Kali Linux e BackTrack, ambos foram desenvolvidos pela mesma empresa(Offensive Security). O foco é o mesmo, voltado para o teste de penetração(pentest), usam um Kernel LINUX. Os dois sistemas podem ser executados através de um CD ou DVD, sem necessariamente instalar no seu HD, podendo usar normalmente o sistema, e utilizar as ferramentas disponibilizadas. Ambos usam o ambiente gráfico *GNOME*.

As diferenças por mais que sejam mínimas existem. O Kali Linux sendo o sucessor do BackTrack, foram feitas algumas atualizações. Além do nome, o Kali Linux foi desenvolvido em cima da distribuição Debian, já o BackTrack teve seu desenvolvimento em cima da distribuição Ubuntu. Versões de Kernel também foram uma das atualizações de ambos os sistemas. Uma atualização também que facilitou, foi em relação aos PATHS. O que isso significa?! Isso significa que o usuário não precisa fazer o caminho absoluto até determinada ferramenta, ele digitando apenas o nome da ferramenta já pode utilizar a mesma.

BackBox

Está entra as distribuições voltadas para pentest mais usadas. Baseada no Ubuntu. Também desenvolvida para realizar testes de penetração. Na versão mais recente da distribuição foram feitas várias atualizações, como atualização de Kernel, atualização de versão de sistema, usando agora o Ubuntu 14.04, entre outras atualizações. E um sistema bem leve, usa a interface gráfica XFCE, se tornando uma distro bem completa e leve.

Site: www.backbox .org

Finalizando, falamos então de três distribuições que estão entre as mais usadas por hackers éticos, profissionais da área de Segurança da Informação em geral, etc, para pentest. Essas estão apenas entre as três mais usadas. Porém existem várias outras distribuições com o mesmo foco, que é o teste de penetração. Vale ressaltar também que, podemos também pegar uma distribuição "cru", tais como Debian, Ubuntu, etc... E fazer ela como uma distribuição de pentest, complementando ela de acordo com as nossas necessidades, com as ferramentas que formos usar, para estudos e futuros testes de penetração.

Bibliografia:

www.vivaolinux .com.br

www.guiafoca .org

www.debian.org

pt.wikipedia.org/