NEaD
Núcleo de Educação a Distância

CYBER SECURITY

Faculdade IMPACTA

2

Arquitetura do Sistema Operacional Windows e Linux

Alex Sandro da Silva Feitosa

Resumo

Nessa aula, iremos falar sobre a arquitetura dos sistemas operacionais Windows e Linux, destacando algumas de suas principais características e diferenças. Além disso, vamos abordar de forma geral o que são protocolos de redes e qual a sua importância para a comunicação entre dispositivos em ambientes computacionais. É ideia é que possamos entender melhor como esses elementos funcionam juntos no mundo da tecnologia.

Introdução

Analisaremos a estrutura dos sistemas operacionais Windows e Linux, ressaltando suas particularidades e contrastes. Também discutiremos, de maneira introdutória, o papel dos protocolos de rede e sua relevância para a troca de informações entre dispositivos em ambientes computacionais. O objetivo é compreender como esses componentes interagem e sustentam o funcionamento da tecnologia.

1.1. Sistema Operacional Windows

1.1.1 DOS

O sistema operacional de disco (DOS) é um sistema operacional que o computador usa para habilitar os dispositivos de armazenamento de dados para ler e gravar arquivos.

DOS fornece um sistema de arquivos que organiza os arquivos de uma forma específica no disco.

MS-DOS, criado pela Microsoft, usou uma linha de comando como interface para as pessoas criarem programas e manipular arquivos de dados. Os comandos DOS são mostrados em negrito na saída de comando dada.

Com o MS-DOS, o computador tinha um conhecimento básico de trabalho de acessar a unidade de disco e carregar os arquivos do sistema operacional diretamente do disco como parte do processo de inicialização

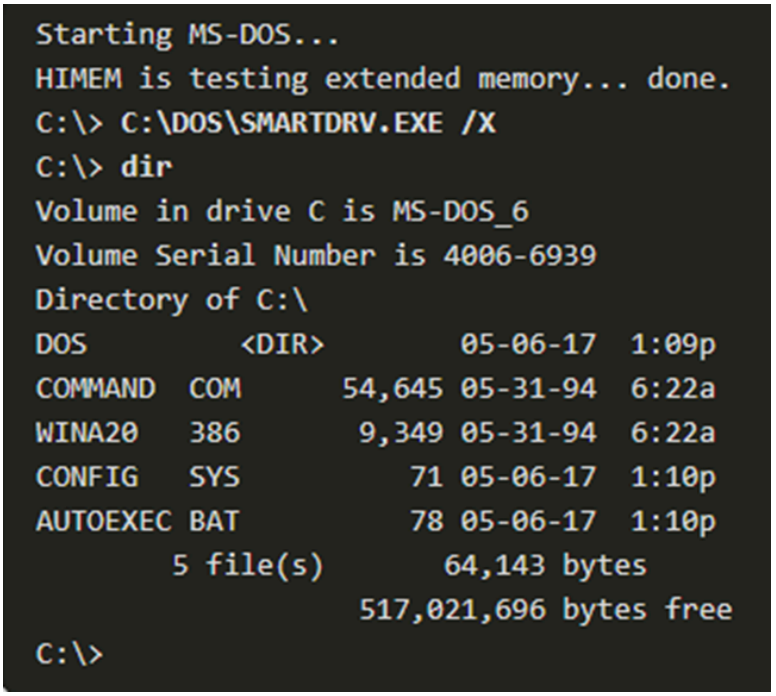
As primeiras versões do Windows consistiam em uma interface gráfica do usuário (GUI) que executava o MS-DOS, começando com o Windows 1.0 em 1985.

Em versões mais recentes do Windows, construído em New Technologies (NT), o próprio sistema operacional está no controle direto do computador e seu hardware.

Hoje, muitas coisas que costumavam ser realizadas através da interface de linha de comando do MS-DOS podem ser realizadas na GUI do Windows.

Para experimentar um pouco de MS-DOS, abra uma janela de comando digitando cmd no Windows Search e pressione Enter.

Figura 1.1 Prompt do MS-DOS



Fonte: CCNA Cyber OPS Associate v1, 2020.

A seguir lista alguns dos comandos do MS-DOS

dir - Mostra uma lista de todos os arquivos no diretório atual (pasta)
cd - Altera o diretório para o diretório indicado
cd.. - Muda o diretório para o diretório acima do diretório atual
cd\ - Muda o diretório para o diretório raiz (geralmente C:)

copy - Copia arquivos para outro local
del - Exclui um ou mais arquivos
find - Procura texto em arquivos
mkdir - Cria um novo diretório
ren - Renomeia um arquivo
help - Exibe todos os comandos que podem ser usados, com uma breve descrição

1.1.2 Versões do Windows

Desde 1993, houve mais de 20 versões do Windows baseadas no sistema operacional NT (SO).

Muitas edições foram desenvolvidas especificamente para estações de trabalho, profissionais, servidores, servidores avançados e servidores de datacenter, entre outras versões criadas para fins específicos.

O sistema operacional de 64 bits representou uma arquitetura totalmente nova, com um espaço de endereçamento de 64 bits em vez dos 32 bits anteriores.

Computadores e sistemas operacionais de 64 bits são compatíveis com programas mais antigos de 32 bits, mas programas de 64 bits não podem ser executados em hardware mais antigo de 32 bits.

A cada nova versão do Windows, o sistema operacional tornou-se mais refinado, incorporando novos recursos.

A Microsoft anunciou que o Windows 10 seria a última versão do Windows. Em vez de adquirir novos sistemas operacionais, os usuários passariam apenas a atualizar o Windows 10.

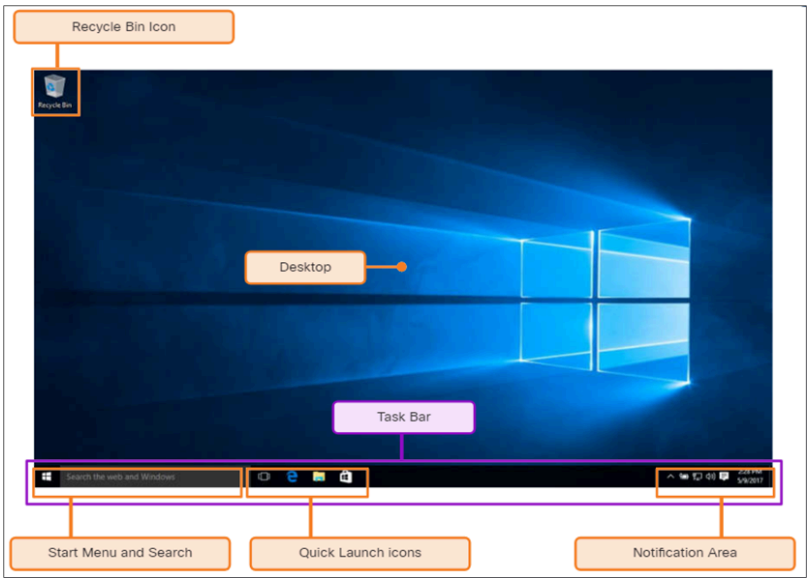
A seguir algumas versões comuns do Windows:

- **Windows 7:** Starter, Home Basic, Home Premium, Professional, Enterprise, Ultimate
- **Windows Server 2008 R2:** Foundation, Standard, Enterprise, Datacenter, Web Server, HPC Server, Itanium-Based Systems
- **Windows Home Server 2011:** Nenhum
- **Windows 8:** Windows 8, Windows 8 Pro, Windows 8 Enterprise, Windows RT
- **Windows Server 2012:** Foundation, Essentials, Standard, Datacenter
- **Windows 8.1:** Windows 8.1, Windows 8.1 Pro, Windows 8.1 Enterprise, Windows RT 8.1
- **Windows Server 2012r2:** Foundation, Essentials, Standard, Datacenter
- **Windows 10:** Home, Pro, Pro Education, Enterprise, Education, loT Core, Mobile, Mobile Enterprise
- **Windows Server 2016:** Essentials, Standard, Datacenter, Multipoint Premium Server, Storage Server, Hyper-V Server

- **Windows Server 2019:** Essentials, Standard, Datacenter,
- **Windows 11:** Home, Pro, Pro Business,

O Windows tem uma interface gráfica do usuário (GUI) para que os usuários trabalhem com arquivos de dados e software.

Figura 1.2 Tela do Windows



Fonte: CCNA Cyber OPS Associate v1, 2020.

A GUI (interface gráfica do usuário) possui uma área principal conhecida como Área de Trabalho. Ela pode ser personalizada com diferentes cores e imagens de fundo.

O Windows oferece suporte a múltiplos usuários, permitindo que cada um personalize sua própria Área de Trabalho.

A Área de Trabalho pode armazenar arquivos, pastas, atalhos para locais específicos, programas e aplicativos.

Ela também possui o ícone da Lixeira, onde os arquivos são armazenados temporariamente após serem excluídos. Os arquivos podem ser restaurados da Lixeira ou ela pode ser esvaziada, o que resulta na exclusão definitiva dos arquivos.

Na parte inferior da Área de Trabalho encontra-se a Barra de Tarefas.

À esquerda, está o Menu Iniciar, utilizado para acessar todos os programas instalados, opções de configuração e o recurso de pesquisa.

No centro, os usuários podem fixar ícones de inicialização rápida, que executam programas específicos ou abrem pastas ao serem clicados.

À direita da Barra de Tarefas está a Área de Notificação, que exibe informações resumidas e funções de diversos programas e recursos do sistema.

1.1.3 Vulnerabilidades do sistema operacional

Os sistemas operacionais consistem em milhões de linhas de código. Com todo esse volume de código, surgem vulnerabilidades.

Uma vulnerabilidade é uma falha ou fraqueza que pode ser explorada por um invasor para comprometer a integridade, a confidencialidade ou a disponibilidade das informações de um computador.

Para explorar uma vulnerabilidade do sistema operacional, o invasor utiliza técnicas ou ferramentas específicas.

Uma vez explorada, a vulnerabilidade pode fazer com que o computador se comporte de maneira não prevista pelo seu design original.

Geralmente, o objetivo é obter controle não autorizado do sistema, alterar permissões ou manipular e roubar dados.

A seguir algumas recomendações comuns de segurança do sistema operacional Windows:

1. Proteção contra vírus e malware

- O Windows usa, por padrão, o Windows Defender, que oferece um conjunto de ferramentas de proteção integradas ao sistema.
- Se o Windows Defender estiver desativado, o sistema se torna mais vulnerável a ataques e malwares.

2. Serviços desconhecidos ou não gerenciados

- Serviços não autorizados ou desnecessários podem criar vulnerabilidades.
- É importante monitorar e desabilitar serviços desnecessários para reduzir a superfície de ataque.

3. Criptografia

- Dados não criptografados podem ser facilmente interceptados e explorados.
- A criptografia é essencial, não apenas para desktops, mas especialmente para dispositivos móveis.

4. Política de segurança

- Uma política de segurança bem definida e aplicada ajuda a evitar acessos indevidos.
- O Gerenciador de Diretiva de Segurança Local permite configurar regras como políticas de senha, bloqueio de conta e controle de acesso.

5. Firewall

- O Windows inclui um Firewall que, por padrão, restringe a comunicação com dispositivos de rede.

- As regras do firewall devem ser revisadas periodicamente para garantir que ainda são relevantes e eficazes.

6. Proteções específicas

- Antivírus: Monitora e neutraliza vírus em tempo real.
- Adware: Detecta e remove programas que exibem anúncios indesejados.
- Phishing: Bloqueia sites e IPs conhecidos por tentativas de phishing.
- Spyware: Identifica e remove softwares espiões como keyloggers.
- Fontes confiáveis/não confiáveis: Avisa sobre programas ou sites potencialmente inseguros.

7. Permissões de arquivos e compartilhamento

- Evite conceder Controle Total ao grupo "Todos".
- Atribua apenas as permissões mínimas necessárias a cada usuário ou grupo.

8. Senhas fracas ou inexistentes

- Contas com senhas fracas são um dos principais vetores de ataque.
- Certifique-se de que todas as contas, especialmente a de Administrador, utilizem senhas fortes.

9. Login como Administrador

- Fazer login como administrador torna o sistema mais vulnerável, pois qualquer programa executado herda esses privilégios.
- O ideal é utilizar uma conta de Usuário Padrão e fornecer as credenciais de administrador apenas quando necessário.

10. Visualizador de Eventos

- O Visualizador de Eventos do Windows registra eventos de aplicativos, sistema e segurança.
- Fornece logs detalhados úteis para diagnóstico e solução de problemas.
- Inclui visualizações como Eventos Administrativos, além de logs de Segurança, identificáveis por IDs de evento.

11. Gerenciamento do Windows Update

- Mantenha o sistema atualizado com os patches e service packs mais recentes.
- O Windows verifica automaticamente o site do Windows Update em busca de atualizações críticas.
- As atualizações ajudam a corrigir falhas de segurança recém-descobertas.
- É possível configurar horários para evitar reinicializações durante o horário comercial.
- Existem também opções avançadas para definir como e quando as atualizações serão aplicadas.

12. Política de Segurança Local

- Define as regras de segurança em computadores que não fazem parte de um domínio.
- Inclui:
  - Diretrizes de senha (ex: comprimento mínimo, complexidade, validade).
  - Diretiva de bloqueio de conta para impedir tentativas de login por força bruta.
  - Configuração de bloqueio automático da estação de trabalho após o início do protetor de tela.
- A política pode ser exportada para ser aplicada em outros computadores com configurações semelhantes.
- O miniaplicativo Diretiva de Segurança Local permite configurar:
  - Direitos de usuário,
  - Regras de firewall,
  - Restrições de execução com o AppLocker.

1.1.4 Camada de abstração de hardware

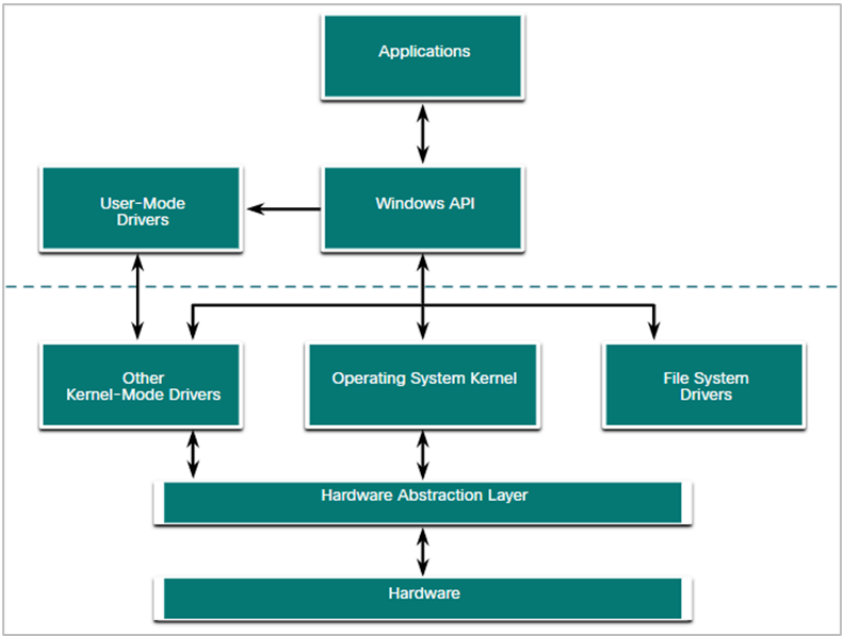
Uma Camada de Abstração de Hardware (HAL) é um software responsável por gerenciar toda a comunicação entre o hardware e o kernel.

O kernel é o núcleo do sistema operacional e possui controle total sobre o computador.

Ele gerencia todas as solicitações de entrada e saída, o uso da memória e o funcionamento de todos os periféricos conectados ao sistema.

A arquitetura básica do Windows é mostrada na figura.

Figura 1.3 Tela do Windows



Fonte: CCNA Cyber OPS Associate v1, 2020.

Os dois modos de operação da CPU em um computador com Windows instalado são o modo de usuário e o modo kernel.

Os aplicativos instalados são executados no modo de usuário, enquanto o código do sistema operacional é executado no modo kernel.

Todo o código executado no modo kernel compartilha o mesmo espaço de endereçamento de memória.

Já no modo de usuário, o código é executado em um espaço de endereço restrito, isolado pelo kernel. Para cada aplicativo, é criado um processo específico, garantindo que ele não interfira diretamente no funcionamento do sistema ou de outros programas.

1.1.5 Sistemas de arquivos do Windows

Um sistema de arquivos é uma forma de organizar as informações na mídia de armazenamento. Abaixo estão listados os sistemas de arquivos suportados (ou parcialmente compatíveis) com o Windows:

NTFS (New Technology File System) é o sistema de arquivos mais comumente utilizado ao instalar o Windows. Todas as versões do Windows e muitas distribuições Linux oferecem suporte total ao NTFS. O macOS pode ler partições NTFS, mas só pode gravar nelas com a instalação de drivers específicos.

A formatação em NTFS cria estruturas essenciais no disco para o gerenciamento de arquivos, incluindo:

Setor de Inicialização da Partição: Localizado nos primeiros 16 setores da unidade, contém o endereço da Tabela de Arquivos Mestre (MFT). Os últimos 16 setores armazenam uma cópia de backup desse setor.

Tabela de Arquivos Mestre (MFT): Contém os registros de todos os arquivos e diretórios da partição, incluindo atributos como permissões e carimbos de data/hora.

Arquivos do Sistema: Arquivos ocultos que armazenam informações sobre outros volumes e atributos dos arquivos.

Área de Arquivos: Região principal da partição onde os arquivos e diretórios são armazenados.

- exFAT (Extended File Allocation Table)
    - Este é um sistema de arquivos simples, suportado por muitos sistemas operacionais diferentes.
    - FAT tem limitações para o número de partições, tamanhos de partições e tamanhos de arquivo que ele pode endereçar, portanto, ele não é mais usado para discos rígidos ou unidades de estado sólido.

    - Tanto o FAT16 quanto o FAT32 estão disponíveis para uso, sendo o FAT32 o mais comum, pois tem muito menos restrições do que o FAT16.
- Sistema de Arquivos Hierárquico Plus (HFS+):
    - Este sistema de arquivos é usado em computadores MAC OS X e permite nomes de arquivos muito mais longos, tamanhos de arquivo e tamanhos de partição.
    - Embora não seja suportado pelo Windows sem software especial, o Windows é capaz de ler dados de partições HFS+.
- Sistema de arquivos estendido (EXT):
    - Este sistema de arquivos é usado com computadores baseados em Linux.
    - Embora não seja suportado pelo Windows, o Windows é capaz de ler dados de partições EXT com software especial.
- New Technology File System (NTFS):
    - Este é o sistema de arquivos mais comumente usado ao instalar o Windows. Todas as versões do Windows e Linux suportam NTFS.
    - Computadores Mac-OS X só podem ler uma partição NTFS. Eles são capazes de gravar em uma partição NTFS depois de instalar drivers especiais.

Setor de Inicialização da Partição: Refere-se aos primeiros 16 setores da unidade. Ele contém informações críticas, incluindo o local da Tabela de Arquivos Mestre (MFT). Os últimos 16 setores da unidade armazenam uma cópia de backup desse setor de inicialização.

Tabela de Arquivos Mestre (MFT): Esta tabela registra os locais de todos os arquivos e diretórios na partição. Também armazena atributos dos arquivos, como informações de segurança e carimbos de data e hora.

Arquivos do Sistema: São arquivos ocultos que armazenam informações sobre outros volumes e sobre os atributos dos arquivos do sistema.

Área de Arquivos: É a região principal da partição onde os arquivos e diretórios efetivamente são armazenados.

Observação: Ao formatar uma partição, os dados anteriores ainda podem ser recuperáveis, pois a formatação geralmente não apaga completamente os dados. Para reutilizar uma unidade com segurança, recomenda-se realizar um apagamento seguro. Esse processo consiste em sobrescrever os dados da unidade diversas vezes, garantindo que nenhuma informação anterior possa ser recuperada.

1.1.6 Processo de inicialização do Windows

Muitas ações ocorrem entre o botão liga/desliga é pressionado e o Windows está totalmente carregado. Este é o processo de inicialização do Windows. Existem dois tipos de firmware de computador:

Sistema básico de entrada-saída (BIOS): O processo começa com a fase de inicialização do BIOS na qual os dispositivos de hardware são inicializados e um POST é executado. Quando o disco do sistema é descoberto, o POST termina e procura o registro mestre de inicialização (MBR) .O BIOS executa o código MBR e o sistema operacional começa a carregar.

UEFI (Unified Extensible Firmware Interface): o firmware UEFI inicializa carregando arquivos de programa EFI (.efi) armazenados em uma partição de disco especial, conhecida como EFI System Partition (ESP).

Se o firmware é BIOS ou UEFI, depois que uma instalação válida do Windows é localizada, o arquivoBootmgr.exeé executado.

Bootmgr.exe lê o banco de dados de configuração de inicialização (BCD).

Se o computador estiver saindo da hibernação, o processo de inicialização continuará com Winresume.exe.

Se o computador estiver sendo inicializado a partir de um início a frio, o arquivo Winload.exe será carregado.

Winload.exe também usa KMCS (Kernel Mode Code Signing) para se certificar de que todos os drivers são assinados digitalmente.

Depois que os drivers foram examinados,Winload.exe executa Ntoskrnl.exe que inicia o kernel do Windows e configura a HAL.

Observação: Um computador que usa UEFI armazena o código de inicialização no firmware. Isso ajuda a aumentar a segurança do computador no momento da inicialização porque o computador entra diretamente no modo protegido.

Há dois itens de registro importantes que são usados para iniciar automaticamente aplicativos e serviços:

HKEY_LOCAL_MACHINE - Vários aspectos da configuração do Windows são armazenados nesta chave, incluindo informações sobre serviços que começam com cada inicialização.

HKEY_CURRENT_USER- Vários aspectos relacionados ao usuário conectado são armazenados nesta chave, incluindo informações sobre serviços que iniciam somente quando o usuário faz logon no computador.

Entradas diferentes nesses locais de registro definem quais serviços e aplicativos serão iniciados, conforme indicado pelo tipo de entrada.

Esses tipos incluem Run, RunOnce, RunServices, RunServicesOnce e Userinit. Essas entradas podem ser inseridas manualmente no registro, mas é muito mais seguro usar a ferramenta Msconfig.exe.

A ferramenta Msconfig é usada para exibir e alterar todas as opções de inicialização para o computador. Ele abre a janela Configuração do sistema.

No “System Configuration” contém cinco guias que contêm as opções de configuração.

- **Geral**
  - Três tipos de inicialização diferentes podem ser escolhidos aqui:
    - Normal carrega todos os drivers e serviços.
    - O diagnóstico carrega apenas drivers e serviços básicos.
    - Seletivo permite que o usuário escolha o que carregar na inicialização.
- **Inicialização do Sistema**
  - Qualquer sistema operacional instalado pode ser escolhido aqui para iniciar.
  - Existem também opções para a inicialização segura, que é usada para solucionar problemas de inicialização.
- **Serviços**
  - Todos os serviços instalados estão listados aqui para que possam ser escolhidos para iniciar na inicialização.
- **Startup**
  - Todos os aplicativos e serviços
  - configurados para iniciar automaticamente na inicialização podem ser ativados ou desabilitados abrindo o gerenciador de tarefas a partir desta guia.
- **Ferramentas**
  - Muitas ferramentas comuns do sistema operacional podem ser iniciadas diretamente a partir desta guia.

1.1.7 Desligamento do Windows

É sempre melhor executar um desligamento adequado para desligar o computador.O computador precisa de tempo para fechar cada aplicativo, desligar cada serviço e registrar quaisquer alterações de configuração antes que a energia seja perdida.

Durante o desligamento, o computador fechará os aplicativos do modo de usuário primeiro, seguido pelos processos do modo kernel.

Existem várias maneiras de desligar um computador Windows: Opções de energia do menu Iniciar, o desligamento do comando da linha de comando e usando Ctrl+Alt+Delete e clicando no ícone de energia.

Existem três opções diferentes para escolher ao desligar o computador:

Desligamento:Desliga o computador (desliga).

Reiniciar: Reinicializa o computador (desligar e ligar).

Hibernate: registra o estado atual do ambiente do computador e do usuário e o armazena em um arquivo. A hibernação permite que o usuário continue de onde parou muito rapidamente com todos os seus arquivos e programas ainda abertos.

1.1.8 Processos, threads e serviços

Um aplicativo do Windows é composto de processos.Um processo é qualquer programa em execução no momento.

Cada processo que é executado é composto de pelo menos um thread. Um thread é uma parte do processo que pode ser executado.

Para configurar processos do Windows, procure o Gerenciador de Tarefas.

Todos os threads dedicados a um processo estão contidos dentro do mesmo espaço de endereço, o que significa que esses threads podem não acessar o espaço de endereço de qualquer outro processo. Isso evita a corrupção de outros processos.

Alguns dos processos executados pelo Windows são serviços. Estes são programas que são executados em segundo plano para suportar o sistema operativo e as aplicações.

Os serviços fornecem funcionalidade de longa execução, como sem fio ou acesso a um servidor FTP.

Para configurar os Serviços do Windows, procure serviços.

Tenha muito cuidado ao manipular as configurações desses serviços. Encerrar um serviço pode afetar negativamente aplicativos ou outros serviços.

1.1.9 O Registro do Windows

O Windows armazena todas as informações sobre hardware, aplicativos, usuários e configurações do sistema em um banco de dados grande conhecido como o Registro.

O registro é um banco de dados hierárquico onde o nível mais alto é conhecido como- um ramo, abaixo que existem chaves, seguido por subchaves.

Os valores armazenam dados e são armazenados nas chaves e subchaves. Uma chave do Registro pode ter até 512 níveis de profundidade.

Segue abaixo as cinco hives do registro do Windows:

- HKEY_CURRENT_USER (HKCU): Contém informações sobre o usuário conectado no momento.
- HKEY_USERS (HKU): Contém informações relativas a todas as contas de usuário no host.
- HKEY_CLASSES_ROOT (HKCR): Contém informações sobre registros OLE (vinculação e incorporação de objetos). Ele permite que os usuários incorporem objetos de outros aplicativos em um único documento.
- HKEY_LOCAL_MACHINE (HKLM): Contém informações relacionadas ao sistema.
- HKEY_CURRENT_CONFIG (HKCC): Contém informações sobre o perfil de hardware atual.

As chaves do Registro e os valores nas seções podem ser criados, modificados ou excluídos por uma conta com privilégios administrativos.

A ferramenta regedit.exe é usada para modificar o registro.

Tenha muito cuidado ao usar esta ferramenta. Alterações menores no registro podem ter efeitos maciços ou mesmo catastróficos.

A navegação no registro é muito semelhante ao explorador de arquivos do Windows.

Use o painel esquerdo para navegar nas colmeias e na estrutura abaixo dele e use o painel direito para ver o conteúdo do item realçado no painel esquerdo.

O caminho é exibido na parte inferior da janela para referência.

As chaves do Registro podem conter uma subchave ou um valor. Os diferentes valores que as chaves podem conter são os seguintes:

REG_BINARY: Números ou valores booleanos

REG_DWORD: Números maiores que 32 bits ou dados brutos

REG_SZ: Valores de string

O registro também contém a atividade que um usuário executa durante o uso diário normal do computador.

Isso inclui o histórico de dispositivos de hardware, incluindo todos os dispositivos que foram conectados ao computador, incluindo o nome, o fabricante e o número de série.

1.1.10 CLI e PowerShell

A interface de linha de comando (CLI) do Windows pode ser usada para executar programas, navegar no sistema de arquivos e gerenciar arquivos e pastas.

Para abrir a CLI do Windows, procure cmd.exee clique no programa. Estas são algumas coisas a serem lembradas ao usar a CLI:

Os nomes de arquivo e caminhos não diferenciam maiúsculas de minúsculas, por padrão.

Os dispositivos de armazenamento recebem uma letra para referência. Isto seguido por dois pontos e barra invertida (\).

Comandos que têm opções opcionais usam a barra (/) para delinear entre o comando e a opção switch.

Você pode usar a tecla Tab para completar automaticamente comandos quando diretórios ou arquivos são referenciados.

O Windows mantém um histórico dos comandos inseridos durante uma sessão da CLI. Acesse comandos inseridos anteriormente usando as teclas de seta para cima e para baixo.

Para alternar entre dispositivos de armazenamento, digite a letra do dispositivo, seguida de dois pontos e pressione Enter.

Outro ambiente, chamado Windows PowerShell, pode ser usado para criar scripts para automatizar tarefas que a CLI normal não consegue criar.

O PowerShell também fornece uma CLI para iniciar comandos.

O PowerShell é um programa integrado no Windows.

Assim como a CLI, o PowerShell também pode ser executado com privilégios administrativos.

Estes são os tipos de comandos que o PowerShell pode executar:

- cmdlets- Esses comandos executam uma ação e retornam uma saída ou objeto para o próximo comando que será executado.
- Scripts do PowerShell- São arquivos com uma extensão .ps1 que contêm comandos do PowerShell executados.
- Funções do PowerShell- São partes de código que podem ser referenciadas em um script.

Para ver mais informações sobre o PowerShell e começar a usá-lo, digite help

Há quatro níveis de ajuda no Windows PowerShell:

- get-help PS comando - Exibe ajuda básica para um comando
- get-help PS comando [-examples] - Exibe ajuda básica para um comando com exemplos
- get-helpPS comando[-detailed] - Exibe ajuda detalhada para um comando com exemplos
- get-helpPS comando[-full] - Exibe todas as informações de ajuda de um comando com exemplos em maior profundidade

1.1.11 Comandos da Rede

O comando net é usado na administração e manutenção do sistema operacional.

O comando net suporta muitos subcomandos que o seguem e pode ser combinado com switches para focar na saída específica.

Para ver uma lista de muitos comandosnet, digitenet helpno prompt de comando.

A saída do comando mostra os comandos que o comandonetpode usar.

Para ver ajuda detalhada sobre qualquer um dos comandos net, digite C:\ >net help.

A seguir lista alguns comandos de rede comuns:

- **net accounts:** Define os requisitos de senha e logon para usuários
- **net session:** Lista ou desconecta sessões entre um computador e outros computadores na rede
- **net share:** Cria, remove ou gerencia recursos compartilhados
- **net start:** Inicia um serviço de rede ou lista os serviços de rede em execução
- **net stop:** Para um serviço de rede
- **net use:** Conecta, desconecta e exibe informações sobre recursos de rede compartilhados
- **net view:** Mostra uma lista de computadores e dispositivos de rede na rede
- **nslookup:** comando para testar o DNS
- **netstat:** comando utilziando para ver detalhes das conexões de rede ativas

1.2. Sitema Operacional Linux

1.2.1 O que é o Linux?

Linux é um sistema operacional criado em 1991.

O Linux é de código aberto, rápido, confiável e pequeno. Ele requer muito poucos recursos de hardware para ser executado e é altamente personalizável.

Linux faz parte de várias plataformas e pode ser encontrado em dispositivos de qualquer lugar, desde relógios de pulso a supercomputadores.

O Linux foi projetado para ser conectado à rede, o que torna muito mais simples escrever e usar aplicativos baseados em rede.

Uma distribuição Linux é o termo usado para descrever pacotes criados por diferentes organizações e incluir o kernel Linux com ferramentas personalizadas e pacotes de software.

O Linux é frequentemente o sistema operacional escolhido no Centro de Operações de Segurança (SOC). Estas são algumas das razões para escolher o Linux:

- Linux é open source - Qualquer pessoa pode adquirir Linux gratuitamente e modificá-lo para atender a necessidades específicas.
- A CLI do Linux é muito poderosa - A CLI (Command Line Interface) Linux é extremamente poderosa e permite que os analistas executem tarefas não apenas diretamente em um terminal, mas também remotamente.
- O usuário tem mais controle sobre o sistema operacional - O usuário administrador no Linux, conhecido como o usuário root, ou superusuário, pode modificar qualquer aspecto do computador com algumas teclas pressionadas.
- Ele permite um melhor controle de comunicação de rede - Controle é uma parte inerente do Linux.

A flexibilidade fornecida pelo Linux é um ótimo recurso para o SOC. Todo o sistema operacional pode ser adaptado para se tornar a plataforma de análise de segurança perfeita.

Computadores Linux que são usados no SOC geralmente contêm ferramentas de teste de penetração.

Um teste de penetração, também conhecido como Pentesting, é o processo de procurar vulnerabilidades em uma rede ou computador atacando-o.

Geradores de pacotes, scanners de porta e explorações de prova de conceito são exemplos de ferramentas Pentesting.

Kali Linux é uma distribuição Linux que contém muitas ferramentas de penetração juntas em uma única distribuição Linux.

1.2.2 Shell Linux

No Linux, o usuário se comunica com o SO usando a CLI ou a GUI.

O Linux geralmente inicia na GUI por padrão. Isso oculta a CLI do usuário.

Uma maneira de acessar a CLI a partir da GUI é por meio de um aplicativo de emulador de terminal. Esses aplicativos fornecem acesso do usuário ao CLI e são nomeados como uma variação da palavra terminal.

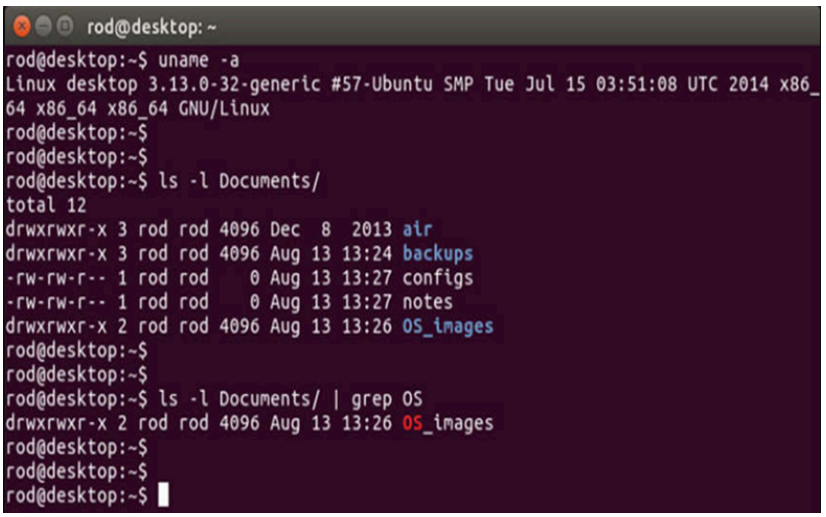
No Linux, emuladores de terminal populares são Terminator, eterm, xterm, konsole e gnome-terminal.

Fabrice Bellard criou JSLinux que permite que uma versão emulada do Linux seja executada em um navegador.

Observação: Os termos shell, console, janela do console, terminal da CLI e janela do terminal são frequentemente usados de forma intercambiável.

A figura abaixo mostra o gnome-terminal, um emulador de terminal Linux popular.

Figura 1.4 Terminal Linux



Fonte: CCNA Cyber OPS Associate v1, 2020.

1.2.3 Comandos básicos do linux?

Os comandos Linux são programas criados para executar uma tarefa específica.

Como os comandos são programas armazenados no disco, quando um usuário digita um comando, o shell deve encontrá-lo no disco antes que ele possa ser executado.

A seguir temos uma lista dos comandos básicos do Linux e suas funções:

mv - Move ou renomeia arquivos e diretórios.

chmod - Modifica as permissões do arquivo.

chown - Altera a propriedade de um arquivo.

pwd - Exibe o nome do diretório atual.

ps - Lista os processos que estão em execução no sistema.

su - Simula um login como outro usuário ou para se tornar um super usuário.

sudo - Executa um comando como um superusuário, por padrão, ou outro usuário nomeado.

grep - Usado para pesquisar cadeias de caracteres específicas em um arquivo ou outras saídas de comando.

ifconfig - Usado para exibir ou configurar informações relacionadas à placa de rede.

apt-get - Usado para instalar, configurar e remover pacotes no Debian e seus derivados.

iwconfig - Usado para exibir ou configurar informações relacionadas à placa de rede sem fio.

shutdown - Desliga o sistema e executa tarefas relacionadas ao encerramento, incluindo reiniciar, parar, colocar em suspensão ou expulsar todos os usuários conectados no momento.

passwd - Usado para alterar a senha.

man - Usado para exibir a documentação de um comando específico.

1.3. Protocolos de redes

1.3.1 Processo de comunicação de rede

As redes variam em tamanho. Eles variam de redes simples compostas por dois computadores a redes que conectam milhões de dispositivos.

Empresas e grandes organizações usam redes para fornecer consolidação, armazenamento e acesso a informações em servidores de rede. As redes fornecem e-mail, mensagens instantâneas e colaboração entre funcionários. Muitas organizações usam a conexão de sua rede à Internet para fornecer produtos e serviços aos clientes.

Rede ponto a ponto: Em pequenas empresas e residências, muitos computadores funcionam como servidores e clientes na rede. Esse tipo de rede é chamado de rede ponto a ponto.

Redes domésticas pequenas: Pequenas redes domésticas conectam alguns computadores entre si e à Internet.

Redes de pequenos escritórios e escritórios domésticos (SOHO): A rede SOHO permite que um escritório doméstico ou remoto se conecte a uma rede corporativa ou acesse recursos compartilhados e centralizados.

Redes médias a grandes: Eles são usados por empresas e escolas e podem ter vários locais com centenas ou milhares de hosts interconectados.

Redes mundiais: A internet é uma rede de redes que conecta centenas de milhões de computadores em todo o mundo.

Todos os computadores que estão conectados a uma rede e participam diretamente da comunicação em rede são classificados como hosts. Os hosts também são chamados de dispositivos finais, terminais ou nós.

Os servidores são simplesmente computadores com software especializado que permite que os servidores forneçam informações a outros dispositivos finais na rede.

Um servidor pode ser de propósito único, fornecendo apenas um serviço, como páginas da Web ou pode ser multiuso, fornecendo uma variedade de serviços, como páginas da Web, e-mail e transferências de arquivos.

Os computadores clientes possuem um software instalado que permite solicitar e exibir as informações obtidas do servidor. Um único computador pode executar vários tipos de software cliente.

O servidor de arquivos armazena arquivos corporativos e de usuários em um local central. Os dispositivos clientes acessam esses arquivos com softwares clientes, como o Windows Explorer.

O Servidor Web executa o software do servidor Web e os clientes usam o software navegador, como o Internet Explorer do Windows, para acessar as páginas Web no servidor.

O Servidor de e-mail executa o software do servidor de e-mail. Os clientes usam o software de cliente de e-mail, como o Microsoft Outlook, para acessar os e-mails no servidor.

Um usuário de rede típico normalmente usa algum tipo de dispositivo de computação para estabelecer muitas conexões com servidores de rede. Esses servidores podem estar localizados na mesma sala ou em todo o mundo.

Vejamos alguns exemplos.

- **Na escola**
  - Os alunos são incentivados a usar dispositivos como laptops e tablets para acessar recursos de aprendizagem.
  - Terry, conecta-se à rede wi-fi da escola e procura os recursos necessários usando um mecanismo de busca.
  - Sua pesquisa é enviada sem fio de seu dispositivo para a rede da escola. Os dados de pesquisa são endereçados para que ele possa encontrar seu caminho de volta para Terry.
  - A sequência de pesquisa de dados binários é codificada em ondas de rádio e é convertida em sinais elétricos que viajam na rede com fio da escola para alcançar a rede do provedor de serviços de Internet (ISP) da escola.
  - Uma combinação de tecnologias leva a pesquisa de Terry para o site do mecanismo de busca, onde a solicitação é processada pelos servidores do Search Engine.
  - Os resultados são então codificados e endereçados para sua escola e, eventualmente, para o dispositivo de Terry.
- **Durante o jogo**
  - Michelle usa um console de jogos para jogar contra outros jogadores. Sua rede se conecta a um ISP usando um roteador e um modem a cabo que permitem que sua rede doméstica se conecte a uma rede de TV a cabo pertencente ao ISP de Michelle.
  - Os cabos do bairro de Michelle se conectam a um ponto central em um poste telefônico e, em seguida, conectam a uma rede de fibra óptica que conecta muitos bairros servidos pelo provedor de internet de Michelle.
  - Quando Michelle conecta seu console de jogos a uma empresa que hospeda um jogo online popular, suas ações em seu jogo se tornam dados que são enviados para a rede de jogadores. Informações que identificam Michelle, o jogo que ela está jogando e a localização de rede de Michelle são adicionadas aos dados do jogo. Os dados que representam o jogo de Michelle são enviados em alta velocidade para a rede do provedor de jogos.

- Os resultados são devolvidos a Michelle na forma de gráficos e sons.

- **Em Consultas Médicas**
  - Um médico frequentemente precisa consultar outros especialistas em casos de pacientes. Seu hospital tomou assinatura de um serviço especial chamado Cloud que permite que dados médicos, incluindo raios-x de pacientes, sejam armazenados em um local central acessível pela internet.
  - Quando um paciente faz um raio-X, a imagem é digitalizada como dados. O hospital usa serviços de rede que criptografam os dados da imagem e as informações do paciente. Esses dados criptografados não podem ser interceptados e lidos à medida que viajam pela Internet para os data centers do provedor de serviços de nuvem. Os dados são endereçados para que possam ser roteados para o data center do provedor de nuvem para alcançar os serviços corretos que fornecem armazenamento e recuperação de imagens digitais de alta resolução.
  - Toda essa interação é digital e ocorre usando serviços em rede que são fornecidos pelo serviço de nuvem médica.

Os analistas de segurança cibernética precisam ter uma compreensão profunda de como as redes operam. Devem poder determinar a origem do tráfego e o seu destino.

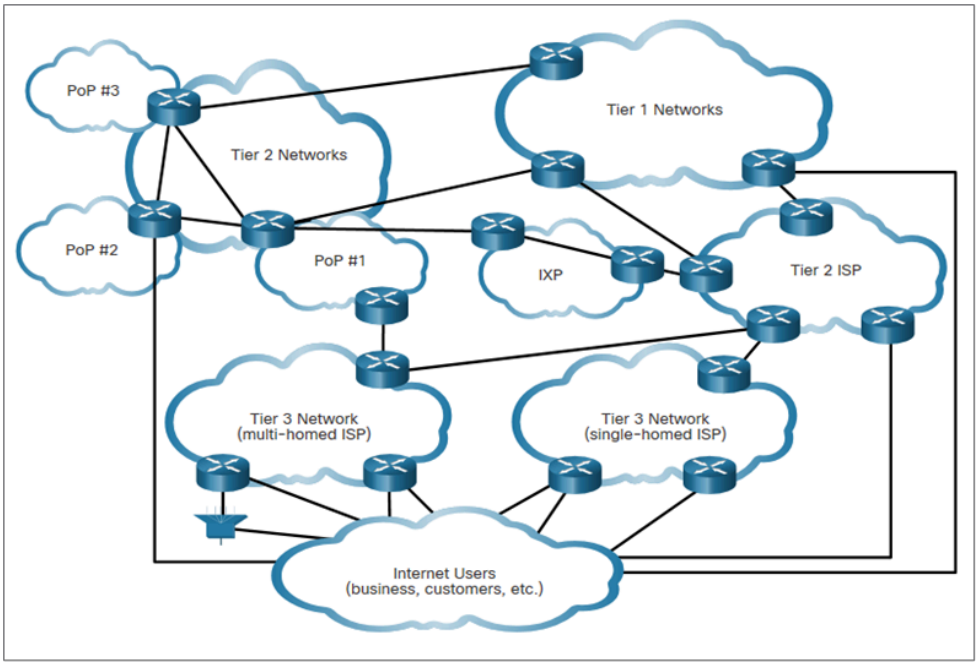
O tráfego de um computador para um servidor de Internet pode ocupar muitos caminhos.

Uma combinação de cabos de cobre e fibra óptica que passam por terra e sob o oceano transportam tráfego de dados. Essas conexões conectam instalações de telecomunicações e ISPs distribuídos em todo o mundo.

Os ISPs Globais de Nível 1 e Nível 2 conectam partes da Internet, geralmente por meio de um Ponto de Troca de Internet (IXP).

Redes maiores se conectam a redes Tier 2 por meio de um Ponto de Presença (PoP), que geralmente é um local no edifício onde as conexões físicas com o ISP são feitas. Os ISPs de Nível 3 conectam residências e empresas à Internet.

Figura 1.5 Terminal Linux



Fonte: CCNA Cyber OPS Associate v1, 2020.

Conclusão

Concluímos a aula com uma visão mais clara sobre as arquiteturas dos sistemas operacionais Windows e Linux, entendendo suas principais diferenças e características. Também reforçamos a importância dos protocolos de rede como base para a comunicação entre dispositivos. Esses conhecimentos ajudam a compreender melhor como os sistemas e redes se integram no cenário tecnológico atual.

Referências

Cisco Systems. **Cisco Networking Academy Program CCNA CyberOps Associate.** v1, 2020. Disponível em: <https://www.netacad.com>.

SÊMOLA, Marcos**. Gestão da segurança da informação**. Rio de Janeiro: Campus, 2003.

NAKAMURA, Emilio Tissato. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec, 2007.

THOMAS, Tom. **Segurança de redes: primeiros passos**. Tradução de Flávio MORGADO. Rio de Janeiro: Ciência Moderna, 2007.

BEAL, A. **Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. São Paulo: Atlas, 2005.

STALLINGS, W. **Network security: applications and standards**. 3.nd. New Jersey: Prentice Hall, 2006.

ASSOCIAÇÃO Brasileira de Normas Técnicas. NBR ISO/IEC 27001 E 27002 Tecnologia da informação.

WADLOW, Thomas A. **Segurança de redes: projeto e gerenciamento de redes seguras**. Rio de Janeiro: Campus, 2000.