**19/03/2020**

**Protocolo:** é o que possibilita as mensagens serem trocadas.

**16/03/2020**

**Aplicação:**

DHCP varias maquinas funcionam entre vários hosts sem que conflite o IP.

SNMP saber se o dispositivo esta online, para monitorar a rede.

SSH protocolo segura para poder acessar outra maquina

**Camada de Transporte**

TCP ele cria um canal entre dois pontos confiável, que é livre de erros garante que se eu enviei um pacote do ponto a pro ponto b ele garante q será entregue. Organização: SLIDE

UDP é mais simples que o TCP ele não é confiável, não a garantias de entrega, por exemplo: Live, não é necessário ser entregue tudo apenas que chegue da forma mais rápida possível. Organização: SLIDE

TCP x UDP

Orientado a conexão x não é orientada a conexão

É confiável X não é confiável UDP quer q chegue o mais conciso possível

Tem entrega ordenada X não tem entrega ordenada os pacotes não necessariamente chegam em ordem

Simplesmente manda os pacotes e o dispositivo tenta lidar da melhor forma possível

Camada Internet

IP o protocolo diz como o datagrama vai ser enviado, da origem pro destino que diz o caminho q ele vai seguir, dois protocolos ipv4 e ipv6, ipv4 esta entrando em extinção pois ele não tem os números validos. Pode virar de 000 e 252525, não são ips validos. Existem classificação .

Migração pro IPV6, ele tem uma gama imensa de IPs,

**Camada Física**

Pro coloco Ethernet domina o meio físico, melhor q o FPI

**Meios de transmissão de dados:** ele faz a transmissão de um ponto A para um ponto B, faz parte física da rede funcionar

**Cabeamento**

Cabeamento: tinha uma serie de limitações, tinha o máximo de velocidade 10mbits

Pares trançados: é composto por 4 fios de cobres, eles q montam a maioria das LANs hj em dia, dependendo ele pode ter uma taxa de transferência,

Cabos de fibra-óticas: permitem muito mais velocidade e transmissão de dados

Sem fios: usado para enviar e receber informação, estilo rádio.

Bluetooth

Wi-Fi: interno, última rede,

Infra-vermelho: feicho de luz que manda um infravermelho que manda um sinal por captação

CAMADA DE APLICAÇÃO

HTTP: é responsável pela transmissão de documentos hipermídia.

SMTP: esse é um padrão utilizado com eficiência na transferência de e-mail pela internet.

POP3: é para o recebimento de e-mail, leva-o para a máquina.

FTP: é responsável pela transferência de arquivos.

DNS: é um sistema permite que usuários encontrarem uma página por meio de nomes que estão no DNS.

DHCP: várias máquinas funcionam entre vários hosts sem que conflite o IP.

SNMP: para monitorar a rede.

SSH protocolo segura para poder acessar outra máquina.

CAMADA DE TRANSPORTE

TCP: ele cria um canal entre dois pontos confiáveis que é livre de erros, garante que se for enviado um pacote do ponto A para o ponto B, ele garante a entrega.

UDP: é mais simples que o TCP, ele não é confiável, não a garantia de entrega, ele tem o objetivo de fazer que os dados cheguem o mais conciso possível.

CAMADA DE INTERNET

IP: é o protocolo que diz como o datagrama vai ser enviado, da origem para o destino que mostra o caminho que ele irá seguir.

CAMADA DE INTERFACE DE REDES

Ethernet: domina o meio físico, melhor que o FPI.

A diferença entre o IPv4 e IPv6 é o número de endereços IP disponíveis em casa um dos protocolos. No IPv4 os endereços têm 32 bits (4 bytes), já o IPv6 têm 128 bits (16 bytes). São formados por combinações numéricas que estabelecem conexões entre computadores.

É usado para fornecer relatórios sobre os erros nas máquinas conectadas, ele não corrige estes erros mas os mostra para os protocolos das camadas vizinhas

O TCP é confiável, já o UDP não é confiável ele apenas quer que chegue o mais conciso possível.

TCP tem entrega ordenada, já o UDP não tem entrega ordenada, os pacotes não necessariamente chegam em ordem.

TCP tem um controle de fluxo, já o UDP simplesmente manda os pacotes e o dispositivo tenta lidar da melhor forma possível.

DHCP: várias máquinas funcionam entre várias hosts sem que conflite o IP.

SNMP: facilita a troca de informações de gerenciamento entre os dispositivos, possibilitando a monitoração da rede.

SSH: é um protocolo que faz a criptografia avançada de dados para poder acessar outra máquina de forma segura.

**02/04/2020**

**Segurança de Sistema**

É um conjunto de fatores que leva a segurança. Parte de princípio de segurança temos vários sub itens, que envolve a parte de acesso de rede de computadores:

Segurança de computadores: o que tu tem como sistema de segurança

Segurança pessoal:

Segurança de Aplicação: como estar sendo codificado as aplicações se está sendo tratado

Criptografia: como pode criptografar dados para termos segurança

Gestão de projetos: segurança do ativo

**Segurança da Informação**

Conservação de confiabilidade: estar disponível para um determinado tipo de pessoa. Através de ferramentas de criptografia; verificando se as pessoas tem senha para entrar naquele local; autenticidade para entrar no sistema. Segurança física, proteger sua senha fisicamente, não revelar para ninguém, não deixar a vista para outras pessoas

Integridade: saber q a informação está concisa, sem margem para dúvida. Através de backups, dados em diferentes locais (servidores).

Disponibilidade: a informação está disponível para o tipo de pessoa especifica. Não adianta ter uma informação muito segura, mas não ser disponível, ela tem que estar disponível quando necessário.

**Conceitos**

Ativo: qualquer bem ou ativo que a empresa possui. Informação é o principal ativo e bem que uma empresa possui, pois com ela você pode pode-se conseguir clientes de outras empresas fazendo a empresa perder muito.

Incidente: é quando algo acontece para que ocorra uma falha de segurança

Ameaça: é qualquer coisa q possa acontecer com um ativo, um exemplo é o vazamento de informações.

Tipos: naturais, tempestade; involuntárias, desconhecido; voluntarias, hackers.

Vulnerabilidade: é onde o risco se encontra, pode ser questão de processo. Geralmente os crackers usam das falhas para atacar as redes. Possibilita que ocorra um indecente de segurança.

Principais vulnerabilidade: deficiência no andamento

Probabilidade: probabilidade que algo possa acontecer

Impacto: oq o vazamento de dados pode causar

Risco: é uma expectativa de risco de dar algo errado

Ataque: exposição durante um determinado tempo e local

Tipos passivo:

Ativo: fraldar alguma coisa

Tipos de aqtaqe:

Vírus: ele faz basicamente ele explora uma falha no computador e se espalha do computador

Verme (Worm): mesma coisa mas não se espalha

Malwere: um software malicioso

BackDoor: deixa aperta uma fenda na segurança para que alguém possa acessar os dados

E S :Explorar uma falha de uma pessoa q esta no sistema

Website: criar um site e levar para outro

Spam:

Mensagem Bomba: baixar e-mails que possa ter um dado nele

War Dialing: explora falhas na sua aplicação

A base é ter política de privacidade

Obtivo ama

Propriedades da segurança da Informação

float salario\_g, salario\_t, salario\_o, final50, cinquenta;

char funcao;

printf("Qual sua função? ");

scanf("%c", &salario\_g);

printf("Qual seu salário? ");

scanf("%f", &salario\_g);

printf("Qual seu salário de técnico?");

scanf("%f", &salario\_t);

printf("Qual o salário do seu cargo?");

scanf("%f", &salario\_o);

if (salario\_g == final50)

{

cinquenta = (salario\_g\*0.5);

final50 = cinquenta+salario\_g;

printf("Seu salário agora é: R$ R$ %.2f", final50);

}