Tipos de ataques em redes:

Muitas são as técnicas que os atacantes utilizam hoje em dia para conseguir o acesso indevido a um sistema ou a um computador especifico, porem também existem os chamados ataques em redes onde o invasor tenta diferentes técnicas de ataque e metodologias para conseguir determinada informação, falaremos mais sobre algumas dessas formas de ataques mais comum que existem.

Man in the Middle:

E uma forma de ataque em que os dados que trafegam entra duas maquinas (cliente servidor) são interceptados e ate mesmo alterados pelo atacante, sem que a vitimas percebam. Em uma comunicação normal, os dois elementos se comunicam entre si sem interferência de através de um meio, uma rede local a internet ou ambas.

Durante o ataque man in the Middle a comunicação e interceptada por um indivíduo e retransmitida as partes envolvidas inicialmente de forma discricionária, o atacante pode decidir retransmitir os dados entra as partes envolvidas com dados inalterados, com altercações ou partes da informação bloqueada. Como os participantes legítimos não percebem que os dados estão sendo adulterados, tomam os como validos.

ARP Spoofing

E uma técnica onde em que um atacante de envia mensagens APR(address resolution protocol) com intuito de associar seu endereço MAC ao endereço IP de outro host, como por exemplo o endereço IP de do gateway fazendo com que todo o trafego seja redirecionado ao IP do atacante ao invés do IP do gateway.

O ARP spoofing permite que o atacante intercepte quadros de trafegados na rede, modifique os quadros e até mesmo capaz parar todo o trafego, esse tipo de ataque só ocorre em segmentos de redes local (LAN – Local Area Network), que usam ARP para fazer a resolução de endereços IP em endereços da camada de enlace.

DNS Spoofing

DNS spoofing , ou DNS cache poisoning é uma técnica em que os dados corrompidos do DNS são introduzidos no cache do resolvedor de DNS, fazendo com que o nome do servidor devolva um IP incorreto resultando em um redirecionamento incorreto ou mal intencionado.

Man in the Middle

E uma modalidade de ataque em que o atacante usa a placa de rede em modo promiscuo, com a ajuda do ARP Poisoning e com isso desencadear vários ataques a uma vítima ou mais.

Heartbleed

E uma falha em que o atacante consegue explorar uma vulnerabilidade na biblioteca OpenSSL na qual permite ele ler a memoria de um servidor ou de um cliente permitindo que ele recupere chaves SSL privadas no servidor.