****

**Faculdade de Ciências e Tecnologias**

**Licenciatura em Engenharia em Tecnologias e Sistemas de Informação**

**4º Ano – Laboral**

**Cadeira: Segurança de Redes**

**Tema: Resumo sobre Ataques às camadas ISO e ataque Man-In-The-Middle**

**Discente:**

Damuge Leonardo Francisco

**Docente:**

Dr. Sérgio Simbine

Maputo, Março de 2023

**ATAQUE ÀS CAMADAS ISO**

**ATAQUES QUE OCORREM EM DIFERENTES CAMADAS ISO**

1. **Camada física:** na camada física podem ocorrer erros no controle de acesso, Danos físicos ou destruição dos dados e hardware, detruição do hardware por questões ambientis como água, fumo ou fogo, desconexão de fios, ou falta de bakcup.
2. **Camada de enlance de dados:** Ataques à camada de enlace mais precisamente à sub-camada MAC, podem prejudicar a rede ao nível de pacote. Isso pode ser feito através de indução de colisões, danificação de pacotes de dados ou de controle. Podemos classificar os riscos comuns a camada 2 como: MAC spoofing (falsificação de endereço MAC), MAC Address able Overflow (estouro da tabela MAC), ataques DHCP, ataques ARP, ataques ao protocolo STP, ataques a VLANS e tempestades de broadcast (broadcast storms).
3. **Camada de rede:** Assim como todos os ataques DDoS, o objetivo de um ataque de camada 3 é tornar um programa, serviço, computador ou rede lentos ou travá-los, ou ocupar toda a capacidade para que ninguém mais possa receber o serviço.
4. **Camada de transporte:** Ao nível de transporte são deixadas, apenas, as suas atividades usuais como controle de fluxo, reordenamento de pacotes, recuperação de erro e controle de congestionamento.
5. **Camada de sessão:** Nesta camada ocorre o ataque de sequestro de sessão. Um atacante pode fazer-se passar por um utilizador autorizado para obter acesso a um domínio, servidor, website, aplicação web, ou rede cujo acesso é restringido através deste tipo de ataque.
6. **Camada de apresentaçao:** Nesta camada ocorre mais o ataque SSL hijacking, no qual um atacante realiza u sequstro de sessão na web.
7. **Camada de aplicação:** virus, worm, phishing, key loggers, backdoors, bugs e cavalos de troia são as ameaças de segurança mais couns nesta camada

O ataque DDoS costuma ocorrer, principalmente, nas camadas OSI 3, 4 e 7 — rede, transporte e aplicações, respectivamente — sempre se aproveitando do conceito de overflow, que é sobrecarregar a estrutura com um grande volume de solicitações, obstruindo o sistema e minando sua estabilidade.

**ATAQUE MAN IN THE MIDDLE (MITM)**

Um ataque man-in-the-middle é um tipo de ataque cibernético em que um ator mal-intencionado se insere em uma conversa entre duas partes, se faz passar por ambas as partes e obtém acesso às informações que as duas partes estavam tentando enviar uma à outra. Um ataque man-in-themiddle permite que um ator mal-intencionado intercepte, envie e receba dados destinados a outra pessoa, ou não destinados a serem enviados, sem que nenhuma das partes externas saiba até que seja tarde demais. Os ataques man-in-the-middle podem ser abreviados de várias maneiras, incluindo MITM, MitM, MiM ou MIM.

**Conceitos-chave de um ataque man-in-the-middle**

**Man-in-the-middle** é um tipo de ataque de espionagem que ocorre quando um ator malicioso se insere como um retransmissor/proxy em uma sessão de comunicação entre pessoas ou sistemas.

Um ataque MITM explora o processamento em tempo real de transações, conversas ou transferência de outros dados.

Os ataques man-in-the-middle permitem que os invasores interceptem, enviem e recebam dados que nunca deveriam ser para eles sem nenhuma das duas partea externas sabendo até que seja tarde demais.

**TIPOS DE ATAQUES MAN-IN-THE-MIDDLE**

* **Ponto de acesso não autorizado:** Os dispositivos equipados com placas sem fio geralmente tentam se conectar automaticamente ao ponto de acesso que está emitindo o sinal mais forte. Os invasores podem configurar seu próprio ponto de acesso sem fio e enganar os dispositivos próximos para ingressar em seu domínio. Todo o tráfego de rede da vítima agora pode ser manipulado pelo invasor. Isso é perigoso porque o invasor nem precisa estar em uma rede confiável para fazer isso — o invasor simplesmente precisa de uma proximidade física suficiente.

**Falsificação de ARP**

ARP é o Protocolo de Resolução de Endereço. Ele é usado para resolver endereços IP para endereços físicos MAC (controle de acesso à mídia) em uma rede local. Quando um host precisa falar com um host com um determinado endereço IP, ele faz referência ao cache ARP para resolver o endereço IP para um endereço MAC. Se o endereço não for conhecido, é feita uma solicitação solicitando o endereço MAC do dispositivo com o endereço IP.

Um invasor que deseja se passar por outro host pode responder a solicitações às quais não deveria estar respondendo com seu próprio endereço MAC.

Os invasores podem configurar seu próprio ponto de acesso sem fio e enganar os dispositivos próximos para ingressar em seu domínio. Todo o tráfego de rede da vítima agora pode ser manipulado pelo invasor. Isso é perigoso porque o invasor nem precisa estar em uma rede confiável

para fazer isso — o invasor simplesmente precisa de uma proximidade física suficiente.

Com alguns pacotes colocados com precisão, um invasor pode farejar o tráfego privado entre dois hosts. Informações valiosas podem ser extraídas do tráfego, como troca de tokens de sessão, fornecendo acesso total a contas de aplicativos que o invasor não deveria ter acesso.

**Falsificação de mDNS**

O DNS multicast é semelhante ao DNS, mas é feito em uma rede local (LAN) usando transmissão como ARP. Isso o torna um alvo perfeito para ataques de falsificação. O sistema de resolução de nomes locais deve tornar a configuração dos dispositivos de rede extremamente simples. Os usuários não precisam saber exatamente com quais endereços seus dispositivos devem se comunicar; eles deixam o sistema resolver isso para eles. Dispositivos como TVs, impressoras e sistemas de entretenimento usam esse protocolo, pois geralmente estão em redes confiáveis. Quando um aplicativo precisa saber o endereço de um determinado dispositivo, como tv.local, um invasor pode facilmente responder a essa solicitação com dados

falsos, instruindo-o a resolver para um endereço sobre o qual tem controle. Como os dispositivos mantêm um cache local de endereços, a vítima agora verá o dispositivo do invasor como confiável por um período de tempo.

**Falsificação de DNS**

Semelhante à maneira como o ARP resolve endereços IP para endereços MAC em uma LAN, o DNS resolve nomes de domínio para endereços IP. Ao usar um ataque de falsificação de DNS, o invasor tenta introduzir informações de cache DNS corrompidas em um host na tentativa de acessar outro host usando seu nome de domínio, como www.onlinebanking.com. Isso leva a vítima a enviar informações confidenciais a um host mal-intencionado, acreditando que está enviando informações a uma fonte confiável. Um invasor que já falsificou um endereço IP pode ter muito mais facilidade em falsificar o DNS simplesmente resolvendo o endereço de um servidor DNS para o endereço do invasor.

**Técnicas de ataque man-in-the-middle**

* **Sniffing**;
* **Ingeção de pacotes**: Um invasor também pode aproveitar o modo de monitoramento de seu dispositivo para injetar pacotes maliciosos em fluxos de comunicação de dados. Os pacotes podem se misturar com fluxos de comunicação de dados válidos, parecendo fazer parte da comunicação, mas de natureza maliciosa.. A injeção de pacotes geralmente envolve primeiro sniffing para determinar como e quando criar e enviar pacotes;
* **Sequestro de sessão**;
* **Decapagem de SSL**: Como o uso de HTTPS é uma proteção comum contra a falsificação de ARP ou DNS, os invasores usam a remoção de SSL para interceptar pacotes e alterar suas solicitações de endereço baseadas em HTTPS para ir para o endpoint equivalente a HTTP, forçando o host a fazer solicitações ao servidor não criptografadas. Informações confidenciais podem vazar em texto simples.

**Prevenção de ataques man-in-the-middle**

* **Criptografia WEP/WAP forte em pontos de acesso;**
* **Rede Privada Virtual**;
* **Forçar HTTPS**: O HTTPS pode ser usado para se comunicar com segurança por HTTP usando a troca de chaves público-privadas. Isso evita que um invasor tenha qualquer uso dos dados que ele pode estar farejando. Os sites devem usar apenas HTTPS e não fornecer alternativas de HTTP. Os usuários podem instalar plug-ins de navegador para impor sempre o uso de HTTPS nas solicitações;
* **Autenticação Baseada em Par de Chaves Públicas**: Os ataques man-in-the-middle normalmente envolvem a falsificação de uma coisa ou outra. A autenticação baseada em par de chaves públicas, como RSA, pode ser usada em várias camadas da pilha para ajudar a garantir se as coisas com as quais você está se comunicando são realmente as coisas com as quais deseja se comunicar.

**EXERCÍCIO 3**

**IP Adress spoofing**

O envio e recebimento de pacotes IP é a regra da comunicação pela internet e segue um procedimento simples. Cada pacote tem um cabeçalho que contém informações para o roteamento. Em um pacote confiável, o endereço de origem que está indicado no cabeçalho é o endereço do remetente real.

Porém, se um atacante consegue forjar o endereço IP, o endereço de origem indicado no cabeçalho será de outro dispositivo

Utilizando o IP Spoofing, um agente malicioso pode:

* Passar despercebido pelos sistemas de detecção de IP (a origem do ataque não poderá ser identificada);
* Evitar alertas dos sistemas baseados em assinaturas de reputação de IP (whitelists, blacklists).

**Como prevenir?**

* **Proteção contra IP Spoofing por Zona de Rede (Zone Protection)**: Garante que o sistema só aceite pacotes com endereços IP originados da Zona de Rede conhecida;
* **Firewall Autenticado**: As políticas que exigem que um usuário esteja autenticado no firewall para trafegar na rede.

***Spoofing* (alteração ou repetição  de informações de roteamento)**

Esse tipo de ataque pode causar *loops* na rede, atrair ou repelir tráfego, gerar mensagens de erro de rota falsas, dividir a rede, dentre outros danos. Tudo por ter como alvo principal os pacotes de controle responsáveis pelas informações de roteamento, através de repetições ou modificações dos mesmos.

**SSL Hijacking**

O Session ocorre quando o criminoso online se coloca entre o computador e o servidor do site sem revelar a identidade de ambos os pontos finais, obtém acesso à informação personificando-se.

Algumas maneiras de se proteger contra esse tipo de ataque são o uso do protocolo **https** e o uso de VPNs.

**Program Logic Flaw**

Uma falha lógica acontece quando um aplicativo (site, aplicativo móvel, webservice…) não se comporta como esperado. Ocorre quando algumas etapas lógicas ou um fluxo de trabalho podem ser evitados, contornados ou manipulados por um invasor. O invasor desvia um fluxo de trabalho em seu próprio interesse, não é um erro técnico em si.

**Como prevenir?**

A única solução real é realizar verificações por meio da validação de processos de negócios e requisitos técnico-funcionais em vários estágios do ciclo de desenvolvimento.

**EXERCIO 4**

1. Na minha opinião o tipo de ataque cibernético em Moçambique é o **phishing**. Infelizmente, no nosso país, as técnicas de engenharia social têm se alastrado e ganhando contornos alarmantes. Muitas pessoas caem nas armadilhas do cibercriminosos, as vezes por falta de conhecimento e outras por ignorância mesmo.
2. A camada do modelo OSI mais susceptível a ataques é a **camada de aplicação**. Esta camada é mais susceptível a ataques porque é a mais próxima ao usuário e este, muitas vezes é usado como vector para os cibercriminosos atacarem os sistemas computacionais.