Security problem

O nosso projeto consiste em DNS tunneling.

O DNS tunneling é uma técnica que encapsula tráfego de dados não relacionado ao DNS dentro de pacotes DNS meio de um modelo cliente-servidor.Dessa forma os pacotes passam despercebidos por restrições de segurança e firewalls.

Num ataque de DNS tunneling, um atacante regista um domínio este domínio vai apontar para um servidor onde o programa tunneling malware está instalado.

A vitima tem o seu computador afetado e dessa forma os pedidos DNS passam pelas firewalls (in and out) e chegam ao dns resolver. O dns Resolver encaminha a querie para o servidor command and control do atacante.

Importance of the security issue/solution

O DNS tunneling é um problema de segurança significativo que pode gerar consequências graves. Como o DNS não foi concebido para transferência de dados por vezes há falhas neste contexto e dessa forma ele representa um risco significativo para uma organização, abrangendo:

Exfiltração de Dados:

Propagação de Malware

Comando e Controle

Ataques DDoS (Negação de Serviço Distribuído)

Data Accquisition (Real World Scenario)

Para a Aquisição de Dados, vamos, entre o cliente e o servidor conectar os dispositivos a uma interface TAP pois permito nos ter uma visão completa da comunicação e Capturar os pacotes com o Wireshark nessa mesma interface.

Depois vão ser realizadas operações no cliente de forma a enviar queries DNS para o servidor.

E para esse efeito o cliente vai estar a Navegar na web.

Data Sources

Para definir o Comportamento Normal vamos gerar e Capturar o tráfego (pacotes DNS) entre um computador e um servidor DNS sem o dns Tunneling a fim de definir o comportamento normal da rede.

Comportamento Malicioso Capturar pacotes no mesmo computador onde já esteja estabelecido um túnel DNS entre um cliente e um servidor (atacante).