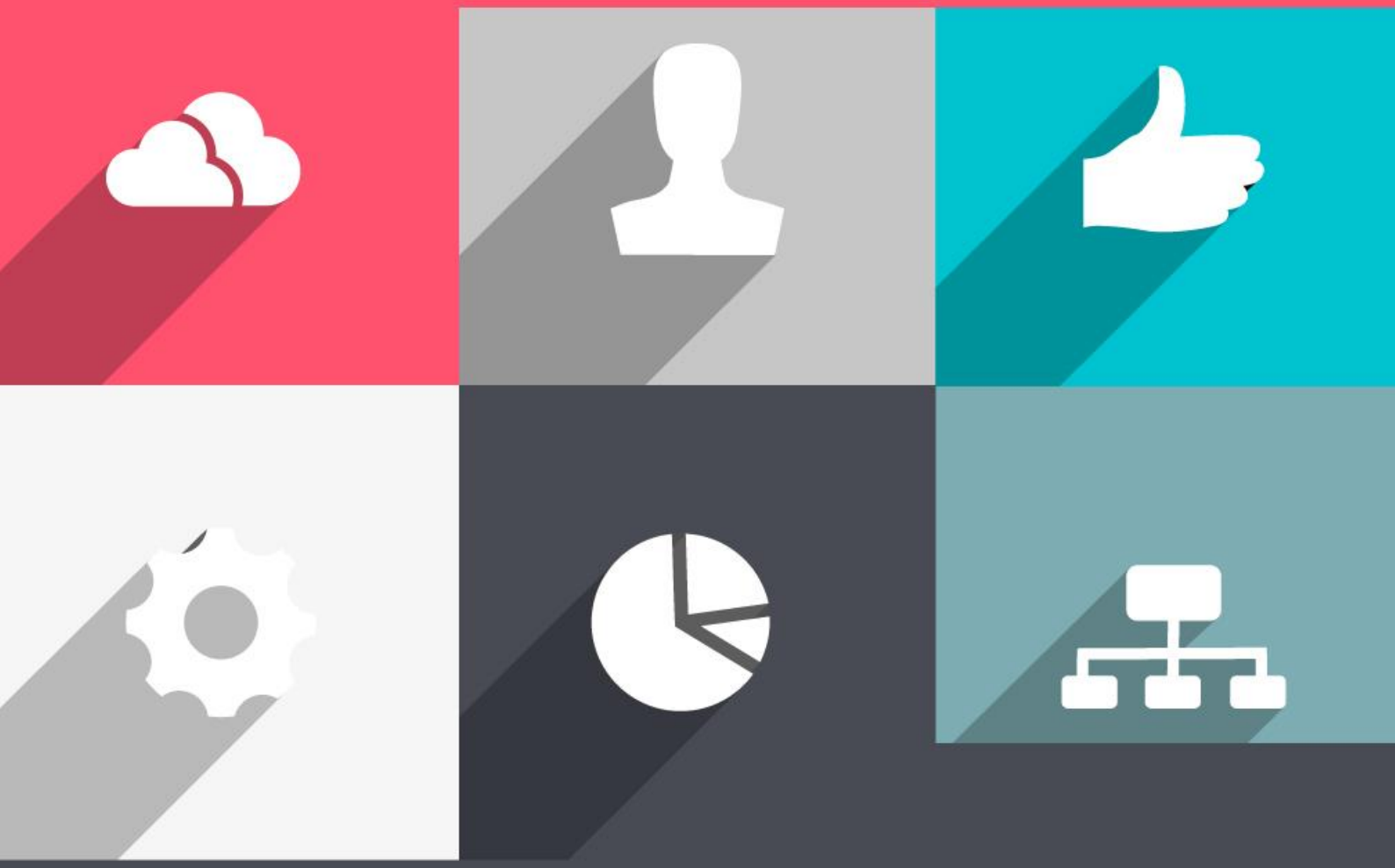


RELATÓRIO E MODELAGEM DE REDE DOMÉSTICA WIRELESS E ANÁLISE DE WEBSITES HTTP E HTTPS PARA CAPTURA DE PACOTES UTILIZANDO O GOOGLE HACKING E CISCO PACKET TRACER

Integrantes:
João Rebertt (202002690984)
Raul Victor da Silva Bastos(202002690968)
Henrique Paiva(202002691034)
Vitor Sousa Mesquita(201802163204)

Disciplina: Segurança Cibernética
Docente: Paulo
Semestre: 4°/ Turno: Noite
Data: 25/11/2021
Local: Estácio de Sá – Castanhal

Parte 1

Modelagem de rede Wireless e relatório utilizando o software Cisco Packet Tracer

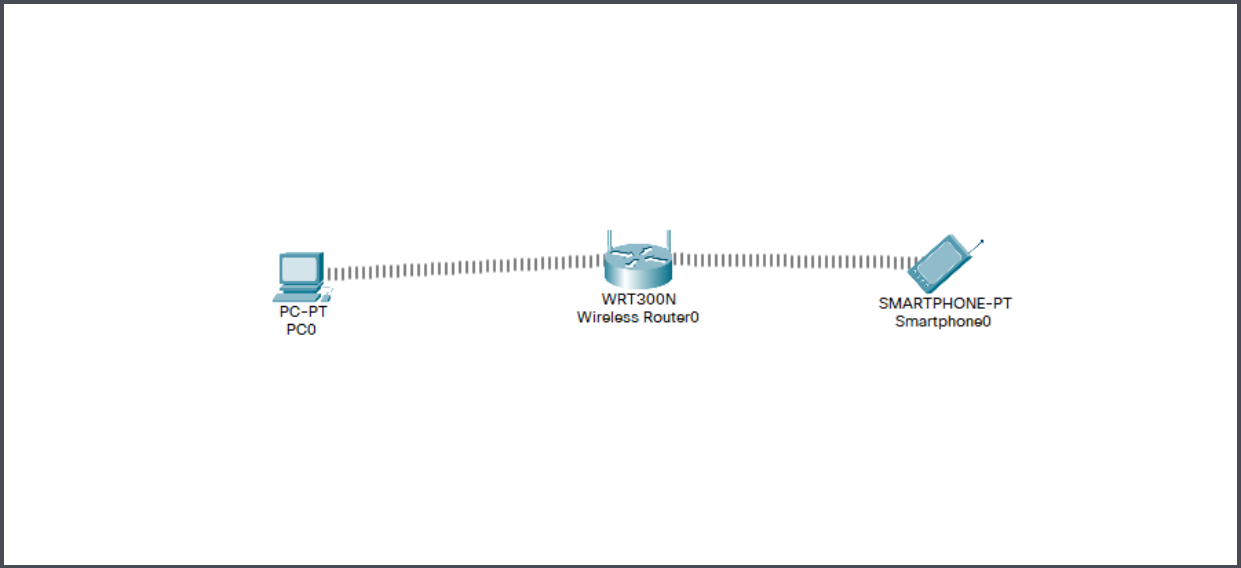


Figura 1 – Modelagem de uma rede wifi doméstica usando o Cisco Packet Tracer

A rede que modelamos é da minha própria casa, ela possui um dispositivo genérico PC-PT-PC0, um roteador WRT300N, um Smartphone-pt Smartphone0

o endereço IP é 192.168.0.101 do computador e 192.168.0.1 do smartphone. Funciona no protocolo DHCP (Dynamic Host Configuration Protocol) e o protocolo IPv4, todos estão conectados através de uma rede Wireless denominada RedesIP.

O protocolo de segurança é WPA2-PSK.

Problemas

- A senha do wifi é valeriadona, senha que pode ser facilmente associada ao proprietário da rede, logo um possivel ataque é (excluindo a engenharia social), o ataque de força bruta em que por meio de um software, são testadas a exaustão senhas possiveis e mais provaveis.

- Como a rede usa IP dinâmico há um problema citado no seguinte artigo:

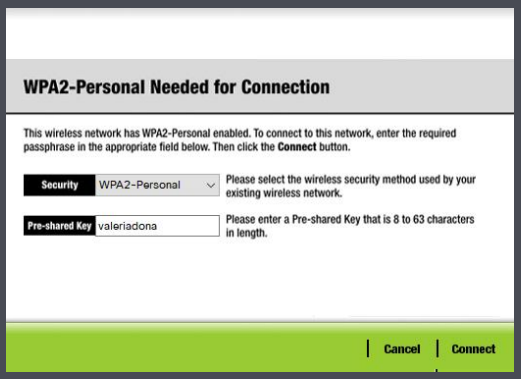
" A alocacao dinamica de enderecos nem sempre e' conveniente para todas as maquinas de uma rede. Maquinas que sao referenciadas pelos seus enderecos IPs, e nao por seus nomes, como os roteadores, por exemplo, devem ter um endereco IP fixo. Ha' casos em que um determinado recurso e' associado a um determinado endereco IP definido pelo DNS, e.g. e' comum associar um endereco IP a um servidor Web. Dessa forma, nao e' conveniente utilizar uma busca dinamica do endereco IP deste servidor. Pode-se utilizar alocacao manual, associando no servidor DHCP o endereco de MAC do servidor Web a seu endereco IP.

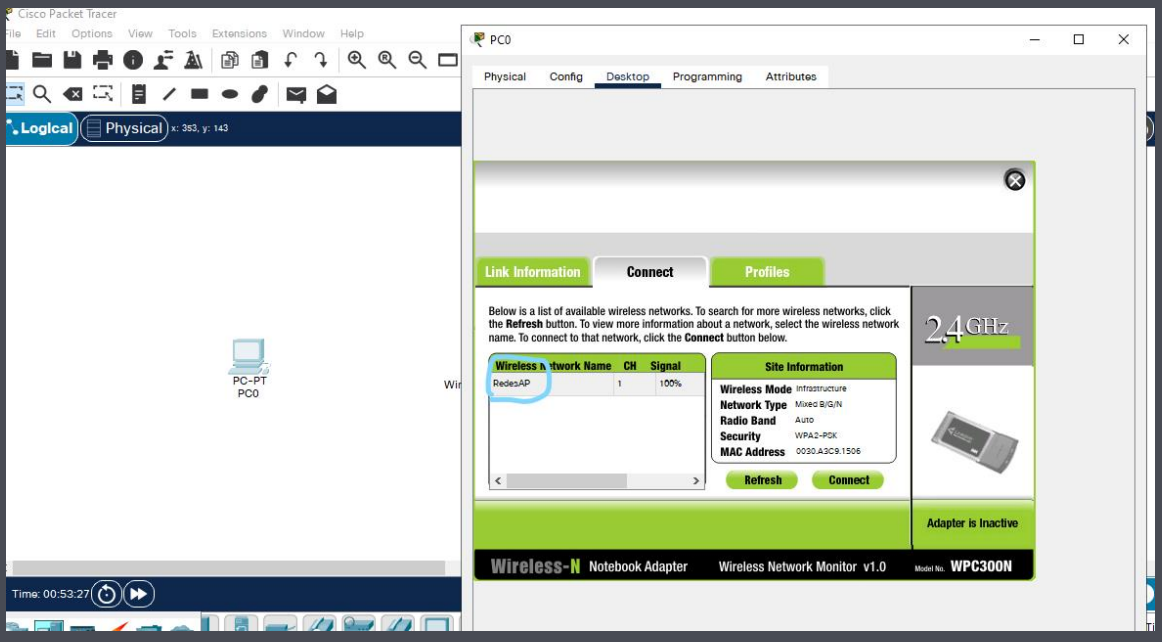
A alocacao dinamica pode tambem inviabilizar os esquemas de seguranca que baseiam-se em permitir ou coibir o acesso a determinados recursos atraves da identificacao do endereco IP ou do nome da maquina do solicitante (e.g. os comandos r's do UNIX ou os esquemas de controle de acesso por nome/enderecos IP do apache). Em redes onde este tipo de controle e' feito a nivel de maquina, e' necessario restringir o uso do DHCP dinamico.

O uso do DHCP dinamico pode vir a comprometer seriamente a seguranca de uma rede cujos pontos de acesso nao sao controlados, ou sao utilizados por usuarios nao confiaveis. Um usuario mal intencionado ou desavisado pode causar grandes transtornos, configurando um servidor DHCP nao oficial, por exemplo.

- Outro problema que pode não ser tão grave, é o WPA2, que embora seguro, ainda pode ser explorado no ataque denominado "Bug Krack", envolve a reutilização de uma chave de uso único fornecida na tentativa de conexão entre um aparelho e uma rede Wi-Fi, o hacker pode monitorar o trafego da rede e acabar utilizando para ataques mais elaborados, burlando a criptografia

Algumas imagens ilustrando os processos realizados:





Soluções

Resolução:

a senha foi alterada para: L@$@N#@=1
o protocolo foi alterado para STATIC mas manteve o endereço IP
e o protocolo de segurança agora é WPA3

Parte 2

Analise de pacotes de sites HTTP e HTTPS com o software Wireshark e a ferramenta Google Hacking

Objetivo do trabalho

1. Instalar o WireShark
2. Usar google hacking para achar site sem criptografia
3. Capturar pacotes abertos
4. Analisar os pacotes em busca de algo interessante
5. Procurar um site com criptografia
6. Capturar pacotes
7. Analisar e veja se consegue encontrar algo útil
8. Documentar todo o processo (Entrega)

Relatório

Como solicitado no objetivo listado ao campo acima, intuito de encontrar um site inseguro(http), com a informação do Google Hacking, foi encontrado o site: www.icel-manaus.com.br (186.202.54.26) que estava desprotegido sem nenhum tipo de segurança.

Os pacotes abertos encontrados foram os protocolos que estavam trafegando do método POST para MYSQL.

Fatores interessantes: Por utilizar o método POST conseguimos identificar os dados que estavam entrando no MYSQL, sendo um e-mail aleatório

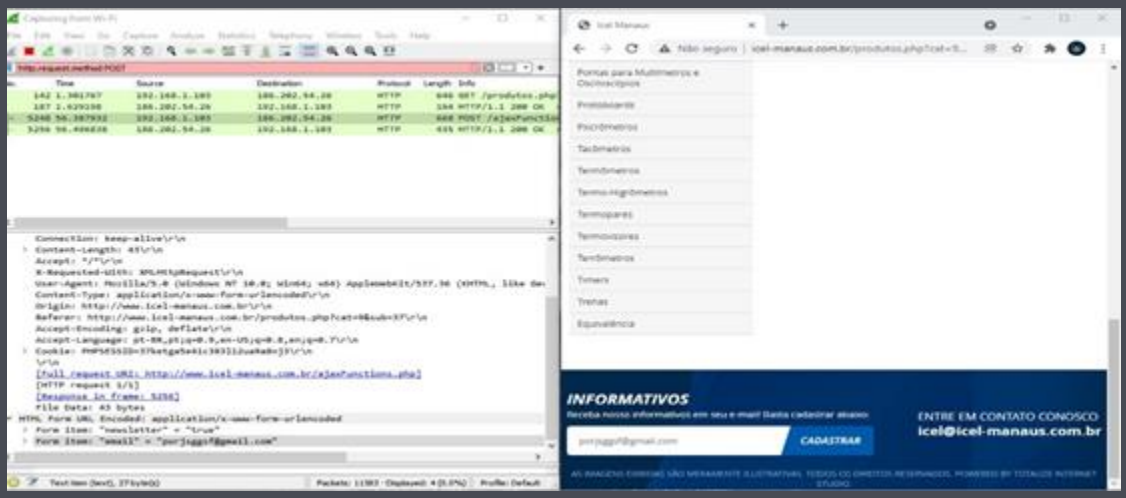


Figura 2 – Pacotes do site desprotegido

Ao procurar um site com criptografia escolhemos o www.aliexpress.com (23.46.118.203), porém não foi possível detectar nenhuma falha, pois o site está muito bem posicionado em suas regras de segurança, notamos que ele faz inúmeras requisições e transferência de dados (criptografados) por conta dos anúncios, compras, contagem de estoque e etc, que estão vindo do back-end.