

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

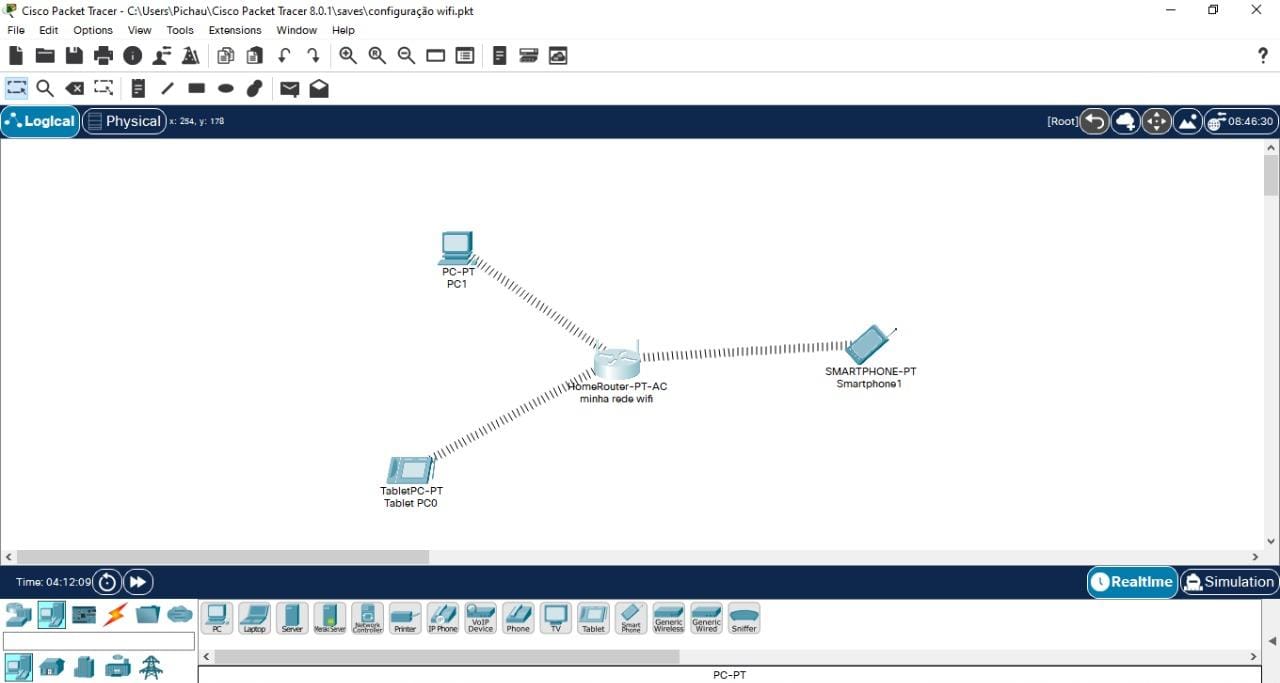


Figura 1 – Modelagem de uma rede wifi doméstica usando o Cisco Packet Tracer

A rede wi-fi alcança o básico de 100 metros varia de acordo com a disposição do ambiente e aplicação de antenas externas

- Opera numa frequência de 5Ghz, o que oferece grande confiabilidade, por ser uma frequência menos utilizada. Contém uma velocidade mais rápida que o padrão 802.11b (até54 Mbps), porém com um alcance operacional menor. A partir de 30 metros há redução de velocidade, mas em alcances menores fica entre 22 e 40 Mb

- A Velocidade de acesso depende bastante da distância ao ponto de acesso. A 20 metros a velocidade gira em torno de 11 Mbps. Em alcances de 80 a 100 metros a velocidade pode cair para 1 Mbps ou menos, o que pode causar perda de sinal e lentidão na conexão. A frequência é de 2.4 Ghz, o que pode ocasionar problemas com telefones sem.



Padrões de Segurança da rede

WEP: Wired Equivalent Privacy

Compatível com praticamente todos os dispositivos WiFi disponíveis no mercado. Justamente por ser tão popular, é também o mais sujeito a falhas de segurança e ataques

O padrão WEP se torna mais inseguro à medida que o poder de processamento dos computadores aumenta. Por ser um sistema de segurança de 128 bits (fator que define os caracteres possíveis, ou seja, o número máximo de combinações de senha), é possível descobrir a palavra-passe de uma rede WiFi desse tipo em poucos minutos por meio de de ataques

WPA: Wi-Fi Protected Access

Traz encriptação 256 bits e uma segurança muito maior para as redes. Além disso, sistemas de análise de pacotes para verificar alterações e invasões – e outras ferramentas foram implementadas para melhorar a segurança

Problema aqui é que a arquitetura WPA foi produzida de forma a não tornar os dispositivos WEP obsoletos, e sim atualizáveis. Com isso, uma série de elementos do protocolo antigo foi reaproveitada e, com ela, diversos dos problemas do antecessor também

WPA2: Wi-Fi Protected Access II

A diferença aqui é a maneira como o sistema lida com senhas e algoritmos, excluindo completamente a possibilidade de um ataque de força bruta. Sendo assim, esse é o tipo mais seguro da atualidade. Segundo especialistas, o risco de intrusões para usuários domésticos com WPA2 é praticamente zero.

Uma das poucas vulnerabilidades conhecidas atinge diretamente usuários corporativos e exige que o atacante possua acesso normal à rede sem fio. Uma vez conectado, o hacker poderia assumir o controle de outros dispositivos ligados à rede, incluindo dados contidos neles ou transferidos a partir das máquinas. isso se deve a programações de compatibilidade para ligação de roteadores antigos e modernos.



**Modos para deixar a rede mais segura e evitar ataques**

Para proteger melhor a rede deve Restringir o acesso a documentos ou pastas compartilhadas através de senhas Tanto no âmbito pessoal quanto profissional, se você desejar manter em sigilo qualquer tipo de arquivo, compartilhe-os sempre somente com o uso de senhas para abrir. Assim, reduz as chances de pessoas desavisadas acessarem e conseguirem ver os seus documentos as configurações de fato que precisam ser aplicadas na sua rede, é o protocolo EAP. Através dele é possível implementar diferentes métodos de autenticação, que podem se dar por certificados de segurança ou por senhas.

-Utilizar nome da rede ou senha padrão de fábrica: isso aumenta as chances dos invasores encontrarem os caminhos de acesso à rede

-Não proteger os pontos de acesso sem fio e outros componentes da rede: neste caso, pessoas mal intencionadas podem ter fácil acesso físico à rede

-Compartilhar senha wifi com um grande número de pessoas: essa vulnerabilidade se apresenta principalmente em empresas, quando os funcionários têm acesso à senha da rede wifi, pois ao sair do escritório podem ter seus aparelhos roubados e, se conectados àquela rede, a invasão torna-se mais fácil

-Compartilhar redes privadas com funcionários e visitantes: neste caso, é possível que as empresas compartilhem uma senha específica de internet sem fio sem que isso exponha a sua rede privada, e esta é uma boa prática.

Então para melhorar a rede tem que:

-instalar o roteador distante da rua ou de janelas e diminuir a intensidade do sinal

-proteger redes com senhas novas e utilizar duplo fator de autenticação para acesso

-Não salvar ou “esquecer” todas as redes acessadas após sair delas



-Manter o firmware do roteador sem fio e os softwares de sistema operacional, antivírus e firewall sempre atualizados

-Evitar acessar arquivos ou pastas com informações sigilosas em redes wifi externas.

-Utilizar protocolos de segurança como WPA versão 2 mas, se possível, dê preferência para a versão 3.



**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](http://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](http://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.

