Segurança de Redes
Prof. João Henrique Kleinschmidt
Prática 3 – Certificados digitais/TLS/AAA

Entregar um relatório respondendo as questões propostas e principais observações feitas durante a prática.

1 – Certificados digitais

a. Verifique em seu navegador se existem certificados instalados e dê exemplos.

b. Acesse um site seguro e obtenha o certificado digital do site.

c. Qual a validade do certificado? Quem emitiu este certificado? Qual a validade do certificado da autoridade certificadora? Qual a cadeia de certificados? Quais algoritmos e tamanhos de chaves foram utilizados?

d. Existem diversas ferramentas que podem ser utilizadas por qualquer usuário para gerar certificados, como o *keytool* do Java e OpenSSL. Qual a diferença de certificado gerado por você com uma destas ferramentas e os certificados obtidos no exercício 1.b?

2 – Capturando pacotes TLS

Abra o Wireshark e ative a captura de pacotes (Menu Capture→Interfaces).

Este exercício requer que haja um servidor HTTP capaz de suportar o serviço HTTPS (utiliza TLS – *Transport Layer Security*)

1. Acesse um site seguro (https://webmail.ufabc.edu.br, https://gmail.com, etc).

2. Você consegue ler os dados que trafegaram no Wireshark? Explique.

3. Identifique o processo de handshake do TLS. Quais são os pacotes trocados entre cliente e servidor? Observe os detalhes do todos os pacotes trocados no handshake. Descreva o processo e o que é possível observar (negociação de algoritmos de criptografia, certificados, etc).

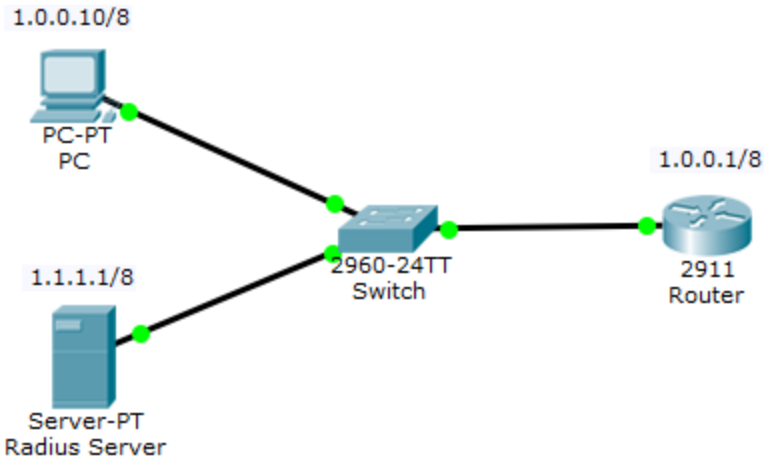
3 – Packet Tracer

O Packet Tracer é um simulador de redes desenvolvido pela Cisco. Pode simular e analisar o funcionamento de uma rede Ethernet, Wi-Fi, fibra óptica ou Internet das Coisas e monitorar os pacotes de dados.

3.1 – Configuração de um servidor RADIUS para AAA

O RADIUS (*Remote Authentication Dial In User Service*) é um protocolo de rede que fornece gerenciamento centralizado de Autenticação, Autorização e Contabilização (*Accounting* em inglês) para usuários que se conectam e utilizam um serviço de rede. Vamos usar o servidor RADIUS para autenticar o PC que irá configurar o roteador remotamente.

Configure a rede a seguir e teste a conectividade da mesma.



Dicas para configuração inicial da rede:

Configurar PC e servidor: na aba *Desktop*, acesse *IP configuration* e digite o endereço IP e máscara de rede.
Configurar roteador: na aba *Config*, selecione a interface de rede (ex:GigabitEthernet0/0): ligue (*on*) e configure IP e máscara.
Teste a conectividade da rede. No PC, vá no prompt de comando do Desktop e faça um ping no roteador e servidor.

Configuração do servidor RADIUS:

Configurar servidor:
Na aba *Services*, habilite AAA.
Em *Network configuration*, adicione *client name*, IP e *secret* (chave). O IP é o IP do roteador, escolha um nome e chave (ex:ufabc e aula). Escolha também o tipo de servidor (Radius)
Em *User setup*, escolha um nome de usuário e senha (ex: alunoseg e teste). Você pode adicionar outros usuários se quiser.

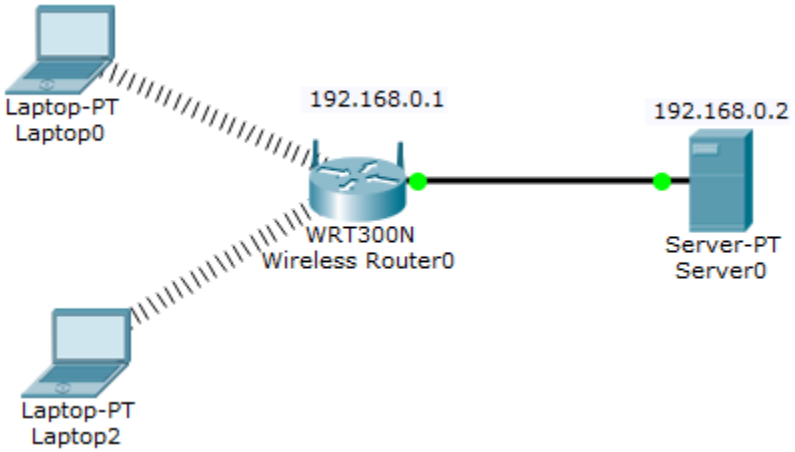
Configurar roteador:
Vá na CLI do roteador e execute:
Para entrar em modo privilegiado: *enable*
Para entrar no modo global: *configure terminal*
Informar ao roteador que irá usar um servidor para autenticação: *aaa new-model*
Iniciar autenticação e autorização Radius no roteador como método padrão:

aaa authentication enable default group radius
aaa authentication login default group radius
aaa authorization exec default group radius
Indicar IP do servidor e chave de acesso (como configurado no servidor)
radius-server host 1.1.1.1 key aula
hostname ufabc

Para acessar o roteador pelo PC:
Vá em *Desktop->prompt de comando* e faça uma conexão telnet:
telnet 1.0.0.1, digite usuário e senha (alunoseg e teste, ou outra que você tenha configurado)
Agora o cliente está autenticado e é possível configurar o roteador remotamente:
Digite
enable
show running-config (vê configurações)

3.2 – Configuração de um servidor RADIUS em uma rede sem fio

Neste exercício vamos usar um servidor Radius para autenticar os clientes de uma rede sem fio. Configure a rede como mostrado abaixo.



Para configurar o ponto de acesso sem fio.
Entre na aba *Config->wireless* ou na interface gráfica (Wireless) e altere o SSID da rede para Net-UFABC e modo de segurança WPA2-Enterprise. Insira o IP do servidor Radius e o segredo compartilhado (chave).

Para configurar o servidor Radius: siga as mesmas instruções do exercício anterior. Adicione dois usuários (um para cada laptop) no servidor Radius.

Configurar notebook: na aba *Physical* insira uma placa de rede sem fio. É necessário desligar o notebook, retirar a placa Ethernet e inserir a nova interface.
Na aba *Config* configure a placa de rede sem fio com o SSID da rede, autenticação WPA2 e usuário e senha configurados no servidor Radius. Em vez de configurar um IP estático, você pode ativar o DHCP (obtém IP diretamente do ponto de acesso sem fio).

Para verificar a conectividade da rede: faça o teste de ping dos notebooks para o servidor.