UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
CMP193/INF01015 – Gerência e Aplicações em Redes
PROFESSORES: Juliano Wickboldt e Jéferson Campos Nobre

Lista de Exercícios 03

Aula 08 - Aspectos Avançados e Segurança na Arquitetura de Gerenciamento da Internet (Aula prática)

***O exercício deve ser resolvido individualmente ou em dupla. A entrega deve ser realizada pelo Moodle, em um único documento (.pdf).**

Antes de começar...

Esse tutorial assume que você já fez os procedimentos para **Instalação do Net-SNMP no Ubuntu 16.04** e já fez as configurações necessárias para habilitar o agente SNMP e as aplicações do gerente SNMP (e.g., snmpwalk, snmpget, etc.).

Pelas configurações que fizemos no tutorial referenciado acima, você já deve ter condições pelo menos de consultar instâncias de objetos das MIBs instaladas no seu agente usando as versões 1 e 2c do SNMP. Para ter certeza de que está tudo funcionando teste os seguintes comandos:

```
# snmpwalk -c public -v1 <IP_MAQUINA_AGENTE> system
```

```
# snmpwalk -c public -v2c <IP_MAQUINA_AGENTE> system
```

Os resultados devem ser idênticos (uma lista de objetos e valores com informações básicas do sistema gerenciado disponíveis na MIB system).

Incluindo usuários e métodos de autenticação

Edite o seu arquivo de configuração do agente /etc/snmp/snmpd.conf e adicione as seguintes linhas:

```
rouser MD5User
```

```
rwuser MD5DESUser
```

Isso vai configurar dois usuários novos, um somente leitura (rouser) com nome MD5User e outro podendo fazer leitura e escrita (rwuser) com username MD5DESUser.

Pare o seu agente SNMP:

```
# sudo service snmpd stop
```

Edite o seu arquivo de configuração persistente do agente SNMP. Esse arquivo é **diferente do anterior**, geralmente fica em **/var/lib/snmp/snmpd.conf**. O agente vai ler esse arquivo uma única vez e aplicar as configurações de forma persistente.

Adicione as seguintes linhas nesse arquivo:

```
createUser MD5User MD5 "The Net-SNMP Demo Password"
```

```
createUser MD5DESUser MD5 "The Net-SNMP Demo Password" DES
```

Isso vai criar os usuários com as senhas criptografadas com com MD5. O Usuário que tem permissão de leitura e escrita (**MD5DESUser**) vai também usar criptografia no tráfego para garantir privacidade na comunicação.

Inicie o seu agente SNMP:

```
# sudo service snmpd start
```

Agora faça uma requisição usando SNMPv3 e o usuário que tem permissão de somente leitura:

```
# snmpgetnext -v 3 -u MD5User -a MD5 -A "The Net-SNMP Demo
Password" -l authNoPriv <IP_DO_AGENTE> sysUpTime
```

Isso vai fazer uma requisição autenticada, mas os dados não serão criptografados.

Agora, faça outra requisição com o outro usuário que usa tanto autenticação quanto criptografia:

```
# snmpgetnext -v 3 -u MD5DESUser -a MD5 -A "The Net-SNMP Demo
Password" -x DES -X "The Net-SNMP Demo Password" -l authPriv
<IP_DO_AGENTE> sysUpTime
```

Utilize o Wireshark, repita das duas chamadas e compare as mensagens trocadas para ver a diferença do tráfego criptografado vs. não-criptografado.

Desafio

Você consegue repetir o exercício anterior utilizando SHA e AES? Análise as diferenças em relação à atividade anterior.