Universidade do Minho - Dep.to Informática
2º Semestre, 2022/2023
Mestrado em Engenharia Informática
Gestão e Segurança de Redes

Ficha de Trabalho Prático Nº2
A. Secure SNMPkeyShare
B. Estudo sobre ameaças aos serviços DNS e DHCP
Versão 1.0

Objectivos:
- Consolidação dos conhecimentos sobre os protocolos, mecanismos e filosofias da arquitetura de gestão *Internet-standard Network Management Framework* (INMF), dando especial relevo aos aspetos de interação protocolar, segurança e controlo de acesso.

Observações:
- O trabalho deverá ser realizado ao longo de 30 a 40 horas efetivas de trabalho individual.

Requisitos:
- Acesso a sistema com, pelo menos, um pacote *freeware* instalado com suporte a SNMP (versão 2, no mínimo): **Net-SNMP**, CMU-SNMP, SCOTTY, etc.
- Utilização opcional de APIs de programação que facilitem a implementação de primitivas SNMPv2c ou SNMPv1.
- Utilização opcional de APIs de programação que facilitem a implementação de mecanismos de segurança para garantir autenticação e confidencialidade.

AVISOS:
- Não serão tolerados atropelos aos direitos de autor de qualquer tipo de *software*...

Bibliografia específica e material de apoio

Material de apoio:
- Manuais/Tutoriais do *net-snmp*;
- MIBs em `/usr/share/snmp/mibs` (ou diretoria equivalente da instalação);
- Recurso `http://net-snmp.sourceforge.net/wiki/index.php/Tutorials/`;
- Recurso `http://www.simpleweb.org/`;
- Recurso `http://www.snmplinks.org/`.

Bibliografia:

- M. Rose, *The Simple Book*, Second Edition, Prentice Hall, 1996.
- B. Dias, *Gestão de Redes*, PAPCC, Universidade do Minho, 1996.
- W. Stallings, *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2*, Addison-Wesley, 2000.
- D. Mauro, K. Schmidt, *Essential SNMP*, O'Reilly, 2001.
- Ver outros recursos na área de "Conteúdo" no BB da UC e no material fornecido no início do semestre.

A. Secure SNMPkeyShare

O principal objetivo da segunda parte do trabalho sobre o sistema SNMPKeyShare é a inclusão de mecanismos de segurança que garantam a utilização do serviço com um acesso autenticado (tanto do servidor/agente como do cliente/gestor) e confidencial (nos dois sentidos da comunicação). Indiretamente também se pode garantir a verificação da não alteração do conteúdo das mensagens.

Para garantir as funcionalidades de segurança enumeradas, a evolução do sistema resultante dos requisitos definidos no enunciado do TP1 pode seguir duas estratégias alternativas tradicionais:

i. Utilizar apenas mecanismos criptográficos base que dependam apenas de segredos/chaves simétricas (ou chaves privadas). Esta opção não obriga à implementação de nenhuma fase/processo/primitiva adicional ao protocolo já definido, mas obriga a que as chaves privadas de autenticação sejam conhecidas de antemão (no agente esta informação pode estar no ficheiro de configuração e no gestor a informação pode ser inserida localmente quando se arranca a aplicação).
ii. Utilizar um mecanismo criptográfico baseado em chaves assimétricas (ou chaves públicas) para permitir a troca inicial de chaves simétricas e utilizar depois mecanismos de autenticação e confidencialidade de chave privadas semelhantes à opção anterior.

De salientar que, a adição dos mecanismos de segurança não deve alterar o modelo comunicacional ou o modelo de informação previamente definido. Ou seja, é obrigatório utilizar o PDU definido anteriormente (ainda que se possam acrescentar alguns campos para a implementação dos mecanismos de segurança), não se devem acrescentar primitivas protocolares para além das três já especificadas e deve continuar a usar-se encapsulamento UDP. Também não devem introduzirem-se mecanismos de sessão que descaracterizem o carater assíncrono e não orientado à conexão do protocolo. Por outro lado, pode ser útil acrescentar algum objeto adicional à SNMPKeyShare MIB definida anteriormente.

B. Estudo sobre principais ameaças aos serviços DNS e DHCP

O objetivo deste trabalho alternativo é a realização dum estudo sobre as principais ameaças de segurança que os serviços fundamentais da Internet, como o DNS e o DHCP, podem sofrer. Este estudo deve contemplar, se possível, a apresentação de casos exemplificativos onde foram reportadas interrupções de serviço efetivas. O trabalho, que deve ser apresentado em forma de artigo ou relatório científico, deve incluir também uma secção sobre as melhores práticas e mecanismos de segurança atuais que ajudem a manter estes serviços sólidos do ponto de vista da segurança.

Relatório e outras recomendações

As recomendações genéricas para a escrita do relatório mantêm-se do primeiro trabalho. No entanto, sugere-se a entrega e apresentação dum único relatório para o TP1 e TP2, se for desenvolvida a opção A no TP2. No caso da realização da opção B no TP2, então devem ser entregues dois relatórios separados, um para o TP1 e outro para o TP2.