Universidade do Minho - Dep.to Informática
2º Semestre, 2021/2022
Mestrado em Engenharia Informática
Gestão e Segurança de Redes

Ficha de Trabalho Prático Nº2

SNMPv2cSec · Caso de Estudo

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 segurança e controlo de acesso.
- Consolidação dos conceitos principais sobre ameaças de segurança em aplicações/serviços distribuídos, métodos, tecnologias e estratégicas que permitem implementar garantias de segurança e efetivar níveis adequados de mitigação.

Observações:

- O trabalho deverá ser realizado ao longo de 20 a 30 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.

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.
- Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, *Security in Computing*, Prentice Hall, 2015.
- Security in Telecommunications and Information Technology, ITU-T, 2015.
- Man Y. Rhee, *Internet Security – Cryptographic Principles, Algorithms and Protocols*, Wiley, 2003.
- William Stallings, *Cryptography and Network Security Principles and Practices*, Prentice Hall, 2015.

Ver outros recursos na área de "Conteúdo" no BB da UC e no material fornecido no início do semestre.

A. Implementação dos mecanismos de segurança no SNMPv2cSec

Neste segundo trabalho prático pretende-se implementar os mecanismos e as estratégias que permitam garantir os níveis de segurança definidos para a arquitetura SNMPv2cSec descrita no enunciado do primeiro trabalho (ver Figura 1).

Nesse sentido, é importante que se façam a adaptações necessárias na MIBsec e no código do agente e do manager SNMPv2cSec para que, pelo menos, estes aspetos de segurança possam ser acautelados:

- Autenticação dos elementos intervenientes;
- Confidencialidade na comunicação entre o agente e o manager SNMPv2cSec;
- Verificação da integridade do conteúdo na comunicação entre o agente e o manager SNMPv2cSec.

Adicionalmente, podem ser discutidos e, eventualmente, implementados:

- Mecanismos de controlo de acesso definíveis para cada manager (sem usar *community strings*);
- Mecanismos de gestão de chaves/segredos através de tabelas adicionais na MIBsec (uma tabela adicional pode ser usada para gerir os aliases dos managers e outra tabela para gerir as chaves/segredos associadas a cada um deles);
- Estratégias comportamentais que permitam aumentar a segurança do sistema.

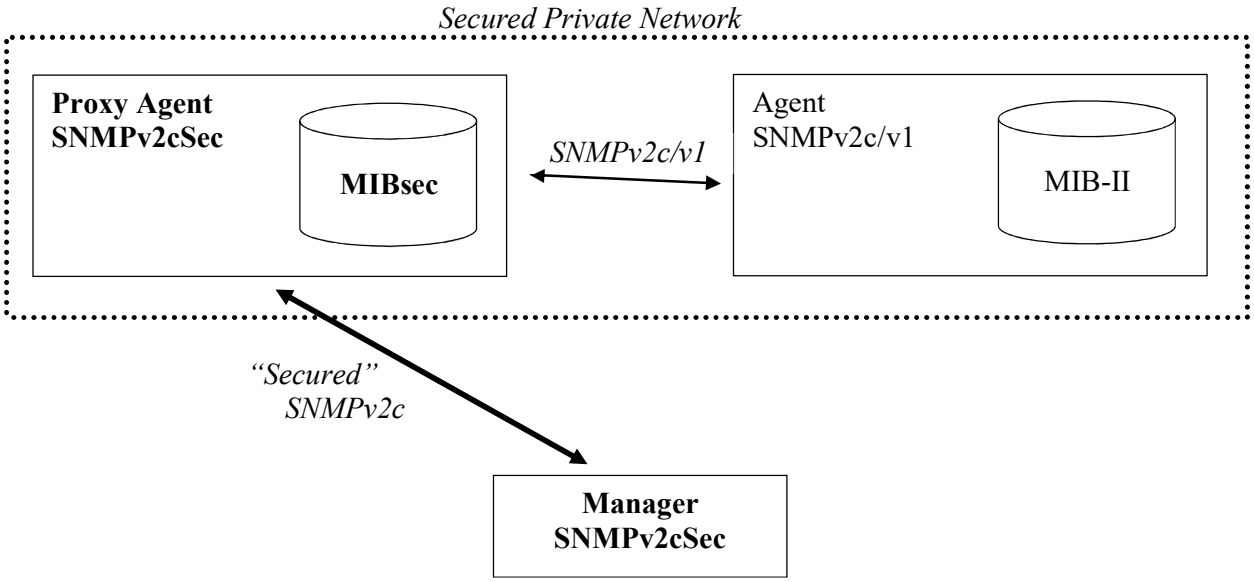

Figura 1: Interligação do agente proxy com um agente normal.

B. Caso de Estudo sobre Segurança

Em alternativa à implementação dos mecanismos de segurança no sistema SNMPv2cSec, este trabalho propõe aos alunos a escrita dum artigo que faça o estudo e a análise crítica dum caso mediático (no sentido em que seja facilmente identificado pela audiência típica deste tipo de artigo) em que um serviço ou sistema distribuído tenha sido atacado e efetivamente comprometido e em que a sua disrupção, quer pela gravidade das suas consequências técnicas quer pelo impacto social, tenha sido notada relevantemente pelos seus utilizadores e pela imprensa.

O artigo deve utilizar um formato científico, i.e., o seu conteúdo deve ser apresentado cientificamente, em que deve ser explicitamente referido aquilo que é factual e técnico e que pode ser referenciado por fontes credíveis, aquilo que é opinativo (se for baseado ou suportado em opiniões de terceiros devem ser apresentadas as referências das fontes e, eventualmente, justificada a sua credibilidade) e aquilo que é conjetural (justificando adequadamente a sua inclusão no artigo).

Ainda que o artigo possa ser construído utilizando uma estrutura pouco rígida, é obrigatório que este se inicie com um resumo/*abstract* e uma secção introdutória (ou de contextualização) e termine com uma secção de conclusões e outra de referências. Além disso, recomenda-se que a estrutura do artigo inclua:

- Uma descrição sobre a forma como o caso foi noticiado e o que se pode concluir das notícias públicas;
- Uma explicação técnica para que serve o sistema/serviço atacado e de que forma foi afetado;
- Uma análise das consequências não técnicas do ataque, incluindo eventuais motivações;
- Uma discussão de quais puderam ter sido as falhas dos mecanismos de segurança (incluindo as estratégias de mitigação) que levaram ao sucesso do ataque;
- Uma apresentação de medidas técnicas e comportamentais que poderiam ter evitado o ataque ou mitigado as suas consequências.

Relatório e Artigo

Na **alternativa A** deste trabalho os alunos devem atualizar ou produzir uma nova versão do relatório do trabalho anterior e que reflita a evolução do TP1 para o TP2. A entrega e defesa do trabalho completo (TP1 e TP2) deverá ser feito numa única sessão a agendar com o docente.

Na **alternativa B** deste trabalho os alunos devem entregar o artigo que deverá incluir na primeira página apenas o título, a identificação do autor (incluindo número de aluno) e o resumo. Apenas como orientação, o artigo completo, incluindo referências, deve conter entre 4000 e 5000 palavras. Não esquecer que os alunos que optem por esta alternativa no TP2, terão que apresentar (incluindo o relatório do TP1) e defender os dois trabalhos em sessões a agendar com o docente.