Mittuniversitetet
MID SWEDEN UNIVERSITY

Laboration: SNMPv3

Lennart Franked*

lab3.tex 1687 2014-03-23 09:45:16Z lenfra

Innehåll

1 Introduktion

Nu när ni är väl insatta i SNMP protokollet kan vi börjar kolla på SNMPv3. Den stora skillnaden mellan version 3 och de tidigare, är att i version 3 kan vi nu på ett säkert sätt autentisera oss gentemot agenten, samt säkra oss mot attacker som kan hota konfidentialiteten samt integriteten på SNMP-PDU:erna.

I denna laboration kommer vi först att förbereda vår SNMP agent för att börja använda version 3. När SNMPv3 väl är konfigurerat plockar vi bort möjligheterna att använda SNMPv2c, vilket innebär att er MRTG konfiguration måste anpassas därefter.

2 Syfte

Syftet med denna laboration är:

- Att ge er en inblick i SNMPv3.

- Att ni kan använda SNMP för att säkert kunna hämta data utan risk för attacker mot varken konfidentialiteten eller integriteten.

3 Läsanvisningar

Kapitel 7 i [9], kapitel 1 i [6], hela [7], [2], [1], [4], [3], [8].

4 Genomförande

Nedan följer de uppgifter ni skall utföra i denna laboration.

4.1 Introducerande frågeställningar

Innan ni påbörjar genomförandet att gå över till SNMPv3 skall ni besvara följande:

1. Nämn de stora skillnaderna mellan SNMPv2c och SNMPv3.
2. Redogör grundligt vilka säkerhetsmetoder som stöds av SNMPv3.
3. Det finns olika säkerhetsnivåer att välja mellan för SNMPv3, dessa är *Auth* och *Priv*. Redogör grundligt skillnaden mellan dessa.
4. Det går att begränsa vilka objekt som en användare får ta del utav, ge ett exempel då detta kan vara bra att tillämpa.
5. Vi kommer att använda oss utav User-Based Security i denna laboration. Det finns dock några svagheter med denna metod som ni läste om i [8], ge en sammanfattning över denna svaghet och vad ni bör tänka på när ni använder er utav denna säkerhetsmetod.

4.2 Konfigurera er SNMP agent

Skapa två användare: en för att läsa och skriva, samt en för att enbart läsa. Den första användaren skapar ni genom att använda de verktyg som finns tillgängligt i det SNMP program ni valt att använda. Den andra användaren skall ni skapa genom att använda SNMP protokollet direkt, använder ni Net-SNMP finns alla instruktioner ni behöver i [1].

Ni kan med fördel konfigurera er SNMP-klient att lägga in användarnamn och version automatiskt så att ni inte behöver ange detta vid varje förfrågan.

Efter att ni skapat dessa konton kan ni bekräfta att de fungerar, genom att göra en SNMP förfrågan mot valfritt objekt.

Avslutningsvis kan ni nu plocka bort möjligheterna att använda SNMPv2c och tillåt enbart autentiserad SNMPv3 trafik mot er agent.

4.3 MRTG

Då ni i en tidigare laboration konfigurerade MRTG med SNMPv2c, måste ni nu anpassa MRTG att istället använda SNMPv3 för att hämta data. Som vanligt hittar ni all information ni behöver för att uföra detta i MRTGs dokumentationen [5].

5 Examination

För att examineras på denna laboration ska ni lämna in följande:

- Svar på frågorna i avsnitt 4.1.
- Vad behövde ni göra för att utföra 4.2?
- En kort redogörelse för vad ni behövde göra för att anpassa MRTG till SNMPv3.

Detta ska lämnas in sammanställt i ett PDF-dokument.

Referenser

[1] *README.snmpv3.* /usr/share/doc/libsnmp-base/README.snmpv3. *Sökvägen är baserad på en installation utav Net-SNMP med hjälp utav APT på ett Debianbaserat system.* Finns även tillgänglig på `http://www.net-snmp.org`.

[2] Net-SNMP Tutorial – SNMPv3 Options, 2011. URL `http://www.net-snmp.org/tutorial/tutorial-5/commands/snmpv3.html`.

[3] Security, 2013. URL `http://www.net-snmp.org/wiki/index.php/TUT:Security`.

[4] SNMPv3 Options, 2013. URL `http://www.net-snmp.org/wiki/index.php/TUT:SNMPv3_Options`.

[5] Tobi Oetiker's MRTG - the multi router traffic grapher. URL `http://oss.oetiker.ch/mrtg/`. 2013.

[6] Blumenthal, U. och Wijnen, B. User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3). RFC 3414 (INTERNET STANDARD), december 2002. URL `http://www.ietf.org/rfc/rfc3414.txt`. Updated by RFC 5590.

[7] Case, J., Mundy, R., Partain, D., och Stewart, B. Introduction and Applicability Statements for Internet-Standard Management Framework. RFC 3410 (Informational), december 2002. URL `http://www.ietf.org/rfc/rfc3410.txt`.

[8] Hardaker, Wes. Limitations of SNMPv3/USM When Combined With EngineID Discovery, 2009. URL `http://pontifications.hardakers.net/computers/limitations-of-snmpv3usm-when-combined-with-engineid-discovery/`.

[9] Subramanian, Mani., Gonsalves, Timothy A., och Usha Rani, N. *Network management : principles and practice.* Dorling Kindersley, Noida, India, 2011. ISBN 978-81-317-3404-9.