Den kompletta studiehandledningen för DT037G Nätverksövervakning och -drift

Daniel Bosk och Lennart Franked*

studyguide.tex 1695 2014-03-24 10:44:35Z lenfra

Innehåll

1 Mål

Kursen syftar till att ge dig grundläggande kunskaper om drift och övervakning av nätverk. Protokollet SNMP utgör en central del och protokollets funktioner och säkerhet behandlas.

Mer specifikt kommer du efter kursen att uppfylla följande mål:

- dokumentera och skapa nätverksdokumentation,
- motivera och diskutera vad som bör dokumenteras i ett nätverk.
- Att ge dig en översiktlig bild över Simple Network Monitoring Protocol (SNMP), Structure of Management Information (SMI) och Management Information Base (MIB).

- Att känna till olika tekniker som används för att samla in data i ett switchat nätverk.
- Att installera och konfigurera en SNMP-agent.
- Att ge dig kunskaperna kring att skapa automatiserade övervakningar.
- Att låta dig skapa en baslinje över ditt eget nätverksanvändande.
- Tillämpa dina kunskaper från tidigare nätverkskurser för att kunna bedömma vad som är lämpligt att övervaka och om det uppstått något fel.
- 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.
- Att du ska utforma övervakning för ett mindre nätverk.
- Att du ska få vana att tillämpa SNMP i en driftmiljö.
- Att du självständigt ska lära dig en ny NMS-programvara.
- Att du ska genomföra en akademisk undersökning.
- Att du ska utforma övervakning för ett mindre nätverk.
- Att du ska få vana att arbeta med SNMP version 3.
- Att du självständigt ska lära dig en ny NMS-programvara.
- Att du ska genomföra en akademisk undersökning.
- Att du ska utforma övervakning för ett mindre nätverk.
- Att du ska få vana att arbeta med SNMP version 3.
- Att du självständigt ska lära dig en ny NMS-programvara.
- Att du ska genomföra en akademisk undersökning.
- Att du ska utforma övervakning för ett mindre nätverk.
- Att du ska få vana att arbeta med SNMP version 3.
- Att du självständigt ska lära dig en ny NMS-programvara.
- Att du ska genomföra en akademisk undersökning.
- Att du ska utforma övervakning för ett mindre nätverk.
- Att du ska få vana att arbeta med SNMP version 3.
- Att du självständigt ska lära dig en ny NMS-programvara.
- Att du ska genomföra en akademisk undersökning.

Kursvecka	Arbete
1	Kursstart
	L0 Nätverksdokumentation
2	L1 Datainsamling
3	L2 NMS
4	L3 Säkerhet
5	P4 Introduktion
6	P5 Teori
7	P6 Metod
8	P7 Resultat
9	P8 Diskussion
10	Muntlig presentation

Tabell 1: Ett förslag på schema för kursen anpassat efter en studietakt om halvtid.

2 Kursupplägg

Kursen består av nio uppgifter, varav de sista åtta är examinerande. Den första uppgiften är en förberedelseuppgift; de efterföljande tre är laborationer som behandlar en insamling av information med bland annat SNMP och Wireshark, Network Management Systems (NMS), Baselining, och avslutningsvis säkerhet; de sista fem uppgifterna är delar av ett större projekt där varje del motsvarar ett avsnitt i en akademisk rapport.

Som litteratur används utöver kurslitteraturen[19], material såsom Request for Comments-dokument (RFC) och andra webbresurser. Som referens har du också materialet från Cisco [10] som du kan använda som uppslagsverk under läsningen.

2.1 Schema

För att hålla en någorlunda jämn arbetsbelastning rekommenderas att du genomför och lämnar in en uppgift i veckan under hela kursens gång. Ett sammanfattat förslag på schemat finner du i tabell 1.

2.2 L0 Kartläggning av nätverk

Ingen litteratur behövs läsas inför denna laboration.

2.3 L1 Datainsamling

Du ska först läsa kapitel 3 till och med kapitel 6 i [19] därefter läser ni följande [3], [9].

Slutligen läser ni översiktligt följande RFC:er: [18], [8], [15], [14], [20], [11], [12], [17].

2.4 L2 NMS

Kapitel 8 och 9 i [19].

2.5 L3 Säkerhet

Kapitel 7 i [19], kapitel 1 i [6], hela [7], [2], [1], [5], [4], [13].

2.6 P4 Introduktion

Då projektet är det avslutande examinerande momentet ska du inför detta ha läst all literatur som ingår i kursen. Som stöd, utöver kurslitteraturen, har ni även kapitel 1 i *Rapportmall för tekniska rapporter* [16].

2.7 P5 Teori

Som stöd, utöver kurslitteraturen, har ni även kapitel 2 i *Rapportmall för tekniska rapporter* [16].

2.8 P6 Metod

Som stöd, utöver kurslitteraturen, har ni även kapitel 3 i *Rapportmall för tekniska rapporter* [16].

2.9 P7 Resultat

Som stöd, utöver kurslitteraturen, har ni även kapitel 5 och 6 i *Rapportmall för tekniska rapporter* [16].

2.10 P8 Diskussion

Som stöd, utöver kurslitteraturen, har ni även kapitel 7 i *Rapportmall för tekniska rapporter* [16].

3 Examination

Kursen examineras med de åtta uppgifterna L{1,2,3} och P{4,5,6,7,8}. Alla uppgifter betygsätts med antingen P för godkänt eller F för underkänt. I slutet finns möjlighet att genomföra en muntlig presentation av projektet och få ett slutbetyg i den sjuskaliga betygsskalan A-F. Utan muntlig presentation ges slutbetyget E om alla åtta uppgifterna är godkända, annars F.

Alla inlämningar och rapporter ska vara i ”godkännbart” skick; det vill säga, vara välformulerade, grammatiskt korrekta och utan stavfel, ha korrekta referenser, samt uppfylla samtliga krav i lydelsen.

Betyget Fx innebär möjlighet till komplettering. I denna kurs ska komplettering göras inom en vecka från retur. Utebliven komplettering resulterar att du hänvisas till nästa rättningstillfälle.

Allt inlämnat material ska vara skapade av dig själv, eller vid gruppuppgifter, skapat av dig eller någon av dina gruppmedlemmar. När du refererar och citerar andra verk måste korrekta källhänvisningar finnas och i fallet citering måste den citerade texten måste vara tydligt markerad. Om plagiat finns i dokumentet riskerar du att stängas av från studier under bestämd tid, högst 6 månader på grund av disciplinförseelse. Vid gruppuppgift riskerar alla gruppmedlemmar att

hållas ansvariga för disciplinförseelse om det av verket inte tydligt framgår vilka av medlemmarna som ansvarat för de plagierade delarna.

Om samarbete sker utan att detta har stöd i instruktionen för examinationen utgör det normalt en disciplinförseelse och studenterna riskerar att stängas av från studier under bestämd tid, högst sex månader. Om inget annat anges i lydelsen är uppgifterna individuella.

4 Vad händer om jag ej blir klar i tid?

Slutdatumena på denna kurs är av yttersta vikt.

De slutdatum som finns för dessa tillfällen är strikta. Om du missar slutdatumet för ett tillfälle hänvisas du till nästa tillfälle. Efter det tredje tillfället hänvisas du till tillfällena under nästkommande kursomgång.

För skriftliga inlämningsuppgifter gäller att dessa rättas en gång under kursens gång, senast i samband med slutdatum för inlämning, därefter ytterligare två gånger inom ett år. Totalt erbjuds tre rättningstillfällen per år. Därefter hänvisas du till nästa kursomgång. Sent inlämnade uppgifter underkänns. Möjlighet till förlängning kan ges, det ska dock finnas en mycket god anledning och förlängning ska anhållas om i god tid.

Ingen handledning planeras efter kursens slut, det vill säga efter det sista schemalagda handledningstillfället. Du rekommenderas därför starkt att följa kursens schema, tänk på att ha marginaler till slutdatum så att du hinner ta upp eventuellt problem vid ett handledningstillfälle. Vill du läsa om kursen kan du göra det genom att registrera om dig nästa gång kursen ges. Omregistrering på kurstillfälle sker i mån om plats, alla förstagångssökande och reserver kommer att prioriteras.

Om du känner att du inte kommer att hinna bli klar med kursen är det därför bättre att göra ett tidigt avbrott på kursen och söka om den inför nästa kurstillfälle. Tidigt avbrott kan registreras senast tre veckor från kursstart och då kommer du att räknas som en förstagångssökande nästa gång du söker kursen.

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] Network tap. URL `http://en.wikipedia.org/wiki/Network_tap`. Wiki, 2013.

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

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

[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] Case, J.D., Fedor, M., Schoffstall, M.L., och Davin, J. Simple Network Management Protocol (SNMP). RFC 1157 (Historic), maj 1990. URL http://www.ietf.org/rfc/rfc1157.txt.

[9] Cisco. Configuring SPAN and RSPAN. URL http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_55_se/configuration/guide/swspan.html. 2010.

[10] Cisco. Internetworking technology handbook. URL http://docwiki.cisco.com/wiki/Internetworking_Technology_Handbook. Wiki, 2012.

[11] Claise, B. Cisco Systems NetFlow Services Export Version 9. RFC 3954 (Informational), oktober 2004. URL http://www.ietf.org/rfc/rfc3954.txt.

[12] Claise, B. Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information. RFC 5101 (Proposed Standard), januari 2008. URL http://www.ietf.org/rfc/rfc5101.txt. Obsoleted by RFC 7011.

[13] 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/.

[14] McCloghrie, K., Perkins, D., och Schoenwaelder, J. Structure of Management Information Version 2 (SMIv2). RFC 2578 (INTERNET STANDARD), april 1999. URL http://www.ietf.org/rfc/rfc2578.txt.

[15] McCloghrie, K. och Rose, M. Management Information Base for Network Management of TCP/IP-based internets:MIB-II. RFC 1213 (INTERNET STANDARD), mars 1991. URL http://www.ietf.org/rfc/rfc1213.txt. Updated by RFCs 2011, 2012, 2013.

[16] Mittuniversitetet. Raportmall för tekniska rapporter, 2012. URL http://ver.miun.se/latex/miunthes/thesis/thesis.pdf.

[17] Quittek, J., Bryant, S., Claise, B., Aitken, P., och Meyer, J. Information Model for IP Flow Information Export. RFC 5102 (Proposed Standard), januari 2008. URL http://www.ietf.org/rfc/rfc5102.txt. Obsoleted by RFC 7012, updated by RFC 6313.

[18] Rose, M.T. och McCloghrie, K. Structure and identification of management information for TCP/IP-based internets. RFC 1155 (INTERNET STANDARD), maj 1990. URL http://www.ietf.org/rfc/rfc1155.txt.

[19] 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.

[20] Waldbusser, S., Cole, R., Kalbfleisch, C., och Romascanu, D. Introduction to the Remote Monitoring (RMON) Family of MIB Modules. RFC 3577 (Informational), augusti 2003. URL `http://www.ietf.org/rfc/rfc3577.txt`.