Nätverkssäkerhet 1DV425 - Laboration
Skadlig kod

Marcus Wilhelmsson
marcus.wilhelmsson@lnu.se

13 februari 2013

Instruktioner

Organisation och genomförande

Laborationen består av en förberedelseuppgift, ett antal kriterier som ska uppfyllas samt en analysdel. Redovisning av laborationen sker med hjälp av en rapport som skickas till kursansvarig i PDF-format.

Förberedelse
Innan laborationen genomförs måste den läsas genom och relevanta förberedelser göras. Detta kan innefatta, men är ej begränsat till, följande:
•Förståelse för de tekniker som används under laborationen.
•Uppslagning av termer.
•Planering av genomförande.

Finns en förberedelse till laborationen måste denna vara genomförd innan laborationen påbörjas.

Redovisning
Redovisning av laborationen sker i form av en skriftlig rapport. Laborationsrapporten ska bestå av en försättssida, innehållsförteckning, tankegångar och banor för de problem som behandlas i laborationen. I de fall det går att resonera kring ett problem eller komma fram till olika lösningar är det extra viktigt att dessa tolkningar ingår i rapporten och hur du har motiverat dem. Texten ska vara en läsbar och sammanhängande text som går att läsa utan att man har tillgång till detta laborations-PM, en punktlista eller liknande med kortfattade svar är alltså inte tillåten.

Förberedelseuppgift

Undersök ett antal tillgängliga antivirusprogramvaror. Välj den som enligt ditt tycke verkar bäst, du får gärna titta på externa tester gjorda av företag och organisationer.

Hur drabbas användare av skadlig kod?

Det är lätt att ta reda på vad antivirus har för funktionalitet och hur de enligt tillverkaren motverkar skadlig kod. Vad som däremot är svårare att läsa sig till kan vara hur den skadliga koden egentligen drabbar slutanvändaren.

•Börja med att skapa två EXAKT likadana virtuella maskiner från en template. Välj själv om du vill köra Windows XP, Windows Vista eller Windows 7. Försök att synka med de andra i samma laborationsgrupp så att ni tar olika operativsystemsversioner och service packs i den mån det går.
•Installera din antivirus-programvara på en av de virtuella maskinerna.
•Utför samma saker på båda maskinerna samtidigt:
    •Försök att hitta så många sidor som möjligt på nätet som försöker infektera datorn med skadlig kod. Testa sidorna i minst tre olika webbläsare.
    •Installera programvara i form av toolbars och annat “skräp”.
    •Ladda ner och installera ett antal virus från den virussamling som tillhandahålls av labbhandledaren.

Diskussionsuppgift

Under sista halvtimmen på laborationstillfället kommer resultatet av laborationen att diskuteras inom gruppen. Aktivt deltagande i dessa diskussioner är obligatoriskt för godkännande på laborationen.