Underrättelseverksamhet och spårning på Internet

Mattias Wecksten

2010

HÖGSKOLAN HHH HALMSTAD

Översikt

”En orientering av SCADA, konfiguration av brandväggar, spårning och analys av nätverkstrafik samt skydd mot nätverksattacker.”

Lärandemål: Kunskap & förståelse

- redogöra för centrala begrepp och modeller
- redogöra för avlyssningstekniker
- redogöra för olika former av skydd mot risker och hot

Lärandemål: Färdighet & förmåga

- analysera ett givet systems nätverkstrafik efter risker och hot
- planera och konstruera ett datorsystem med analys av trafik och skydd mot hot och risker

Lärandemål: Värderingsförmåga…

- förhålla sig till kostnaderna för olika former av risker och hot kontra kostnaderna för implementation av skyddsmekanismer

Huvudsakligt innehåll

Kursen ger en översikt av SCADA där säkerhetsspecifika aspekter granskas. En kortare översikt av hur man bygger en brandvägg ges samt en mer djupgående genomgång av olika reella attackvektorer samt motmedel till de samma. För att erbjuda ett perspektiv från verkligheten så ingår gästföreläsningar med talare från olika områden.

Undervisning

Kursen bedrivs genom föreläsningar, gästföreläsningar, obligatorisk laboration samt ett obligatoriskt projekt.

Examination

Kursen examineras genom laboration och projektrapport.

Kurslitteratur

- Rash, Michael. Linux Firewalls, No Starch Press, 2007
- Krutz, Ronald. Securing SCADA systems, Wiley, 2005

Schema

	1	2	3	4	5	6	7	8
Förel.	F1+ F2	F3	F4+ F5	F6	F7+ F8	F9	F10+ F11	
Labb				L1				
Sem.								
Proj.					P1		P2	
Ex.								T1

Föreläsningar

1. Introduktion
2. Vad är SCADA? Kritisk infrastruktur. (kap. SS1-2)
3. Utvecklingen. Svagheter och attackvektorer. (kap. SS3-4)
4. Säkerhet i teori och praktik. Standarder och referenser. (kap. SS5-6)
5. Ledning och implementering. Framtiden? (kap. SS7-8)

Föreläsningar

6. Repetition, IP-tables. (kap. LF1)
7. Attacker och försvar, Nätverk, Transport och Applikation. (kap. LF2-4)
8. PSAD: The Port Scan Attack Detector (kap. LF5-8)
9. Snort, Fwsnort, Psad. (kap. LF9-11)
10. Port knocking vs. SPA, fwknop, visualisering. (kap. LF12-14)