

Forensisk Analys av Nätverkstrafik

Erik Hjelmvik
< erik . hjelmvik [at] gmail . com >

Swedish Network Users' Society
Stockholm, 2010-09-29

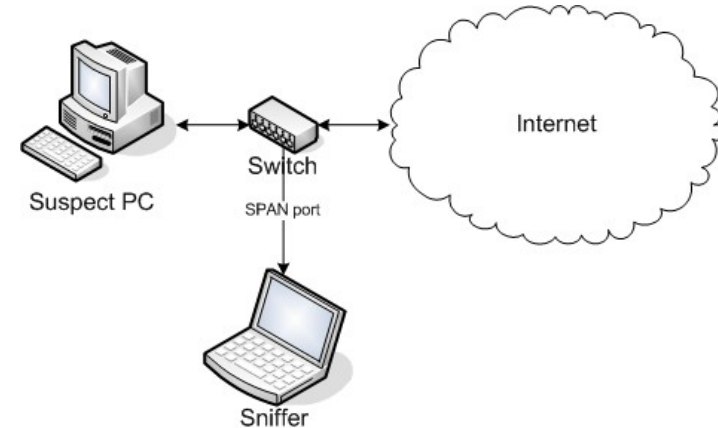
När används det?

- Polis
 - Avlyssning av en misstänkts datatrafik
- CERT på företag/organisationer
 - Analys av IT-säkerhetsincidenter

Hur fungerar det?

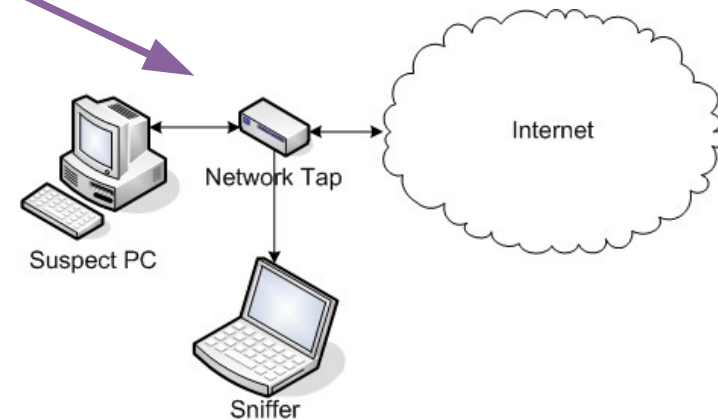
- Inkoppling

- SPAN-port
- Nätverks-TAP



- Inspelning

- Hårdvara:
NetWitness / Solera Networks
- Mjukvara:
tcpdump / dumpcap



Exempel: dumpcap

```
#  
# spela in allt till/från IP 213.1.2.3  
# Skapa en ny fil för varje 100MB  
# Dumpa trafiken till filen "wiretap.pcap"  
#  
> dumpcap -i 1 -f "host 213.1.2.3" -w  
wiretap.pcap -b filesize:100000
```

Demo: NetworkMiner

<http://www.dfrws.org/2008/challenge/submission.shtml> (suspect.pcap)



DFRWS 2008

Steve Vogon är misstänkt för att vara i kontakt med olagliga grupper. Steve tros ha använt sin privata laptop på företagsnätverket för sin suspekta verksamhet.

- Info om datorn som användes av Steve Vogon
- Aktiviteter:
 - Google-sökningar
 - E-post
 - Besökta webbsidor

Demo: NetworkMiner

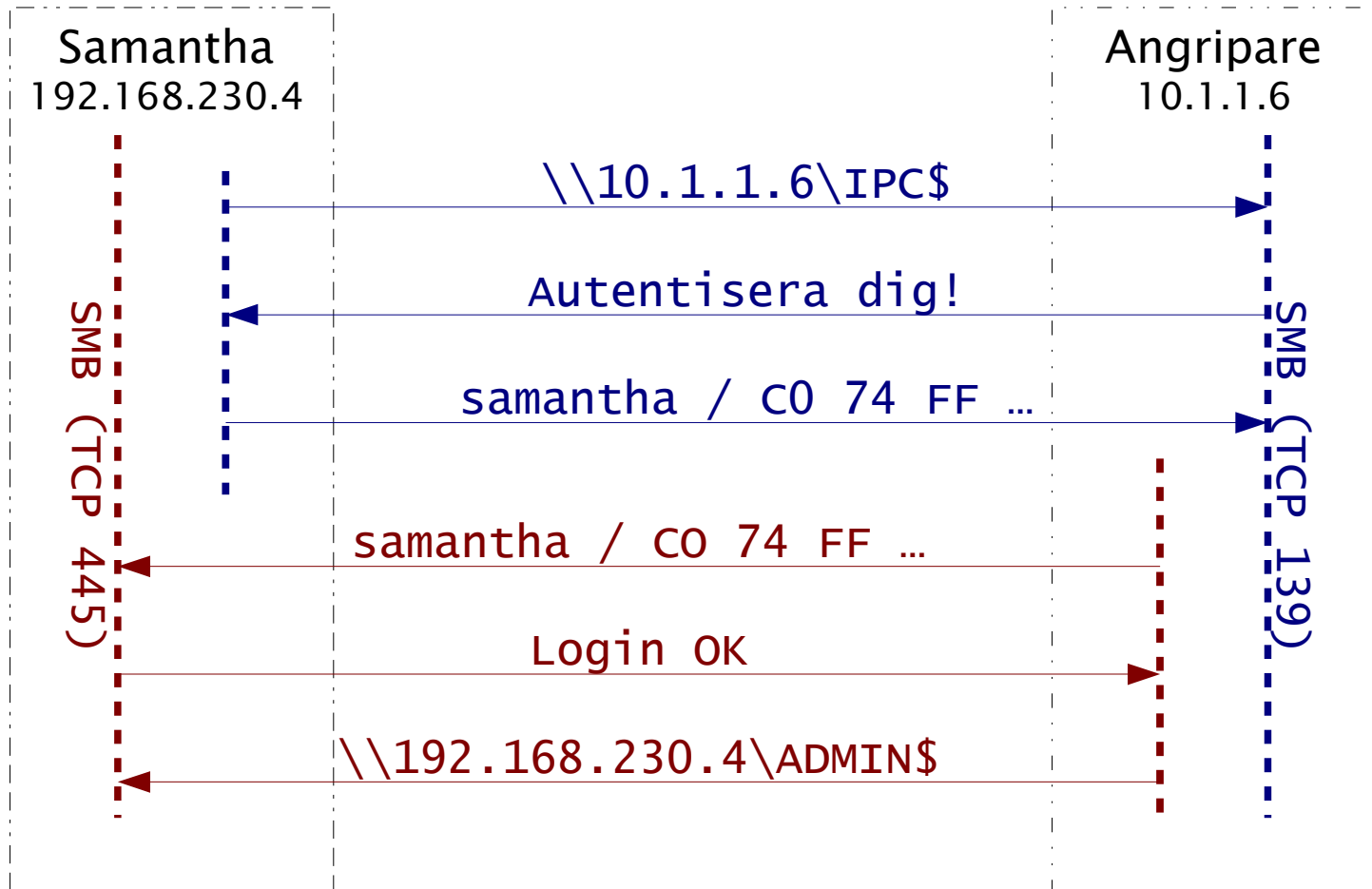
<http://taosecurity.blogspot.com/2009/02/sample-lab-from-tcpip-weapons-school-20.html> (case09.pcap)

TaoSecurity TCP/IP Weapons Scool

Samantha Athew får ett mail till sin personliga gmail-adress. Mailet innehåller en HTML-fil som sägs vara "a new cool Web page". Efter att ha öppnat HTML-filen betedde sig hennes dator konstigt.

- Vilken är Samanthis gmail-adress?
- Vad hände när Samantha öppnade den bifogade HTML-filen?

SMB-relay MITM attack



Testa NetworkMiner



<http://networkminer.sourceforge.net/>

