

RMI med prosjekt i distribuerte systemer TDAT3014

DETALJERT BRUKERMANUAL

20. januar 2014

Gruppedlemmer:

Andreas Mosti, Thomas Mowatt

*Et dokument om
Simple Network Server -
Produktet*

Tabell 1: Revisjonshistorikk

Dato	Versjon	Beskrivelse	Forfatter
02/02/13>	1.0	Established requirements document	Andreas Mosti og Thomas Mowatt
<25/02/13>	1.1	Edited document according to the feedback	Andreas Mosti og Thomas Mowatt
<28/04/13>	1.2	Final version	Andreas Mosti og Thomas Mowatt

Innhold

1	Introduksjon	4
1.1	Mål	4
1.2	Omfang	4
1.3	Definisjoner, akronymer, forkortelser	4
1.4	Referanser	4
1.5	Innholdsoversikt	4
2	Kort om Simple Network Server	4
3	Testoppsett	4
4	Installasjon og grunnoppsett	5
4.1	Virtualbox	5
4.2	Vagrant	5
4.3	Kildekode	6
4.4	Kjente oppsettsproblemer	6
5	Arbeidsflyt	7
6	Gjennomgang av nåværende funksjonalitet	8
6.1	1: Start firewall	8
6.2	2: Start apachemonitor	10
6.3	3: Start fail2ban (IPS Service)	12
6.4	4: Send mail	12
6.5	5: Start networkmonitor	13
7	Om kildekodens oppbygging	14

1 Introduksjon

1.1 Mål

Dette dokumentet er ment som brukermanual for Simple Network Server - produktet. Det vil inneholde alt som trengs for å kunne bruke løsningen fullt ut, inkludert avhengigheter og oppsett.

1.2 Omfang

Dette dokumentet omhandler bruk av hele systemet.
Beskrevet miljø er Linux (Debian - basert) og Mac OS X 10.9.
MERK: Prosjektet er tilgjengelig for Windows, men dette er ikke testet.

1.3 Definisjoner, akronymer, forkortelser

- SNS: Simple Network Server
- SSH: Secure Shell
- OS: Operating System
- LAMP: Linux Apache MySql PHP
- ISP: Internet Service Provider

1.4 Referanser

- Mitchell Hashimoto, Vagrant: Up and Running
- Visjonsdokument, Kravdokument og Arkitekturdokument
- Se fotnoter

1.5 Innholdsoversikt

2 Kort om Simple Network Server

Simple Network Server (SNS) er et ferdig, utvidbart virtuelt servermiljø basert på Ubuntu Linux som inneholder programvare og verktøy tilpasset faget LV473D -Nettverkssikkerhet.

3 Testoppsett

Denne manualen er skrevet ut ifra gjennomgang og bruk på våre testoppsett og fungerer 100%. Disse er idag:

- MacBook Pro Retina 13", OS X "Maverics" 10.9.1, 64 bit
- Debian "Wheezy" 3.2.51-1, 64 bit
- Ubuntu "Precise Pangolin" 12.04LTS, 32 bit

- Ubuntu "Precise Pangolin" 12.04LTS, 64 bit
- Ubuntu "Saucy Salamander" 13.10, 64 bit

4 Installasjon og grunnoppsett

For å ta i bruk Simple Network Server - oppsettet for første gang må man først installere to avhengigheter samt hente ned prosjektet. Vi begynner programvare som kreves:

4.1 Virtualbox

Siden SNS er en virtuell løsning, må virtualiseringsløsningen virtualbox tas i bruk. Virtualbox er gratis, og kan lastes ned via https://www.virtualbox.org/wiki/Download_Old_Builds for Linux og Mac. Pakken kan også lastes rett fra pakkerepoet til Debian / Ubuntu:

```
sudo apt-get install virtualbox
```

Eller via macports¹ på OS X:

```
sudo port install virtualbox
```

Testet og anbefalt versjon er virtualbox 4.1.18.

4.2 Vagrant

Den neste nødvendige programvaren er Vagrant. Vagrant er det virtuelle miljøet SNS benytter for å kjøre, og er ment for å lage virtuelle utviklermiljøer som fokuserer på å skape like utvikleroppsett for alle som jobber på et delt prosjekt, ved bruk av vagrant vil prosjektets oppsett se likt ut for alle som tar det i bruk. Som utviklerne av Vagrant selv beskriver det:

"Vagrant is a tool for building complete development environments. With an easy-to-use workflow and focus on automation, Vagrant lowers development environment setup time, increases development/production parity, and makes the "works on my machine" excuse a relic of the past."

For å installere Vagrant, last ned fra <http://downloads.vagrantup.com> for Linux og Mac. Pakken kan også lastes rett fra pakkerepoet til Debian / Ubuntu:

```
sudo apt-get install vagrant
```

Eller via macports på OS X:

```
sudo port install vagrant
```

Testet og anbefalt versjon av vagrant er 1.2.7. ²

¹<https://www.macports.org/>

²Vagrant: Up and Running av vagrantskaper Mitchell Hashimoto kan eventuelt brukes som støttelitteratur.

4.3 Kildekode

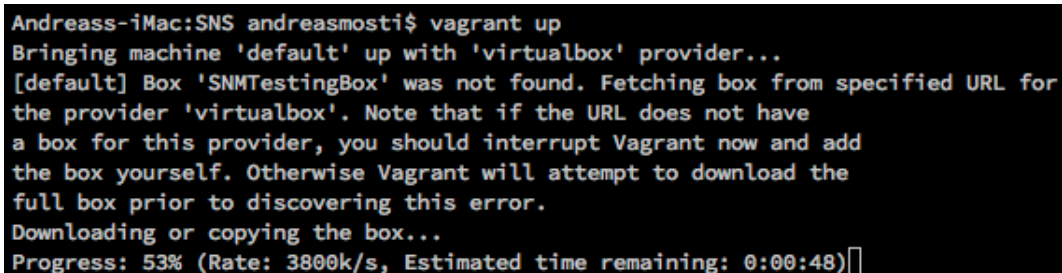
Selve kildekoden til SNS hentes fra github for enklest installasjon:

```
git clone https://github.com/andmos/SNS
```

Nå kjøres prosjektet for første gang enkelt:

```
cd SNS/  
vagrant up
```

Et virtuelt Ubuntu - image vil nå lastes ned (skjer kun ved første gangs kjøring) og prosjektfilene vil settes opp på dette imaget. Skjermbildet ved første gangs innhenting av image ser slik ut:

A terminal window with a black background and white text. The text shows the command 'vagrant up' being executed. It indicates that a machine named 'default' is being brought up using the 'virtualbox' provider. A message states that a box named 'SNMTestingBox' was not found, so it is fetching it from a specified URL. It notes that if the URL doesn't have a box for this provider, the user should interrupt Vagrant and add the box themselves. It then shows the box is being downloaded or copied, with a progress bar at 53% and an estimated time remaining of 0:00:48.

```
Andreass-iMac:SNS andreamosti$ vagrant up  
Bringing machine 'default' up with 'virtualbox' provider...  
[default] Box 'SNMTestingBox' was not found. Fetching box from specified URL for  
the provider 'virtualbox'. Note that if the URL does not have  
a box for this provider, you should interrupt Vagrant now and add  
the box yourself. Otherwise Vagrant will attempt to download the  
full box prior to discovering this error.  
Downloading or copying the box...  
Progress: 53% (Rate: 3800k/s, Estimated time remaining: 0:00:48)
```

Dette imaget er det vagrant kaller en "box". Den fungerer som grunnimage, og nedlastning skjer som sagt kun ved første gangs bygg av prosjektet. Ved alle nyoppsett av systemet vil imaget brukes som grunn-OS for prosjektfilene til SNS, eller en såkalt "sandbox". Boksen kan lokaliseres i den skjulte mappa ".vagrant.d" på hjemmekatalogen til brukeren din.

For å sjekke at den virtuelle maskinen fungerer som den skal, gå til <http://localhost:8080/> fra nettleseren din. Du vil da få opp denne siden:

Vagrant works!

This is the default web page for the Vagrant webserver!

The web server software on the Simple Network Server is running.

To access the Simple Network Server, go the SNS directory and do "vagrant ssh" from the terminal.

4.4 Kjente oppsettsproblemer

Den eneste feilen som har oppstått under testing er at versjonene av Virtualbox og Vagrant som ligger i repoene har vært ikke-kompatible med hverandre. Skulle dette oppstå ved oppsett, må man manuelt laste ned Virtualbox versjon 4.1.18 og legge denne inn. For 32 bit:

```
wget http://download.virtualbox.org/virtualbox/4.1.18/  
virtualbox-4.1_4.1.18-78361~Ubuntu~precise_i386.deb  
sudo dpkg -i virtualbox-4.1_4.1.18-78361~Ubuntu~precise_i386.deb
```

Og for 64 bit:

```
wget http://download.virtualbox.org/virtualbox/4.1.18/  
virtualbox-4.1_4.1.18-78361~Ubuntu~precise_amd64.deb  
sudo dpkg -i virtualbox-4.1_4.1.18-78361~Ubuntu~precise_amd64.deb
```

Merk: Dette er pakker for Ubuntu 12.04 LTS. For andre versjoner av OS X / Linux, last ned fra https://www.virtualbox.org/wiki/Download_Old_Builds_4_1

Skulle problemer med Vagrant oppstå, kan også denne installeres utenom pakkesystemet. Da kjøres følgende (32 bit):

```
wget http://files.vagrantup.com/packages/7ec0ee1d00a916f80b109a298bab08e391945243/  
vagrant_1.2.7_i686.deb  
sudo dpkg -i vagrant_1.2.7_i686.deb
```

Og for 64 bit - versjonen:

```
wget http://files.vagrantup.com/packages/7ec0ee1d00a916f80b109a298bab08e391945243/  
vagrant_1.2.7_x86_64.deb  
sudo dpkg -i vagrant_1.2.7_x86_64.deb
```

Igjen, dette er pakker for Ubuntu. For andre distroer og OS X, besøk <https://downloads.vagrantup.com/tags/v1.2.7>

Erfaringer under testing har knyttet kjente problemer opp mot Virtualbox, så begynn med den.

5 Arbeidsflyt

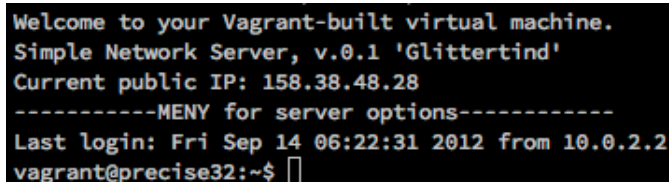
Arbeidsflyten for produktet er veldig enkel. Når man står i prosjektets mappe, startes den virtuelle maskinen enkelt ved

```
vagrant up
```

Og maskinen aksesseres via SSH ved

```
vagrant ssh
```

Man blir da møtt av følgende skjermbilde:



```
Welcome to your Vagrant-built virtual machine.  
Simple Network Server, v.0.1 'Glittertind'  
Current public IP: 158.38.48.28  
-----MENY for server options-----  
Last login: Fri Sep 14 06:22:31 2012 from 10.0.2.2  
vagrant@precise32:~$
```



og kan nå bruke alle verktøyene SNS tilbyr enkelt via kommandolinja, hovedsaklig via "meny" kommandoen for enkelhets skyld. Det er vert å merke seg at SNS - maskinen er en fullverdig virtuell Ubuntu - maskin, så all Linux - funksjonalitet utenfor prosjektets verktøy kan fritt brukes og / eller installeres. Når man er ferdig med maskinen, avslutter man SSH - sesjonen og skriver:

```
vagrant destroy
```

Alle endringer og oppsett på den virtuelle maskinen blir nå slettet. Har man foreks. rotet det til med filer, angrepet serveren slik at den ikke lengre kan brukes fullstendig eller liknende, er ikke det noe problem. Nåværende system slettes. For neste gangs bruk av SNS, kjører man enkelt og greit "vagrant up" igjen, og prosjektet settes opp på nytt fra bunn av.

6 Gjennomgang av nåværende funksjonalitet

For å benytte seg av funksjonaliteten som er bygget inn i SNS har vi laget en oppstartsmeny som enkelt og greit skal kunne guide deg til den funksjonaliteten du er ute etter (se kravdok). Du kommer til denne menyen når SNS er startet, og "vagrant ssh" er kjørt. Ved så å skrive "meny" fra kommandolinja, blir man møtt av følgende vindu:



```
vagrant@precise32:~$ meny

M E N Y
1. Start firewall
2. Start apachemonitor
3. Start fail2ban (IPS service)
4. Send Mail
5. Start Networkmonitor
6. Start Webproxy
7. Start VPN-Server
8. Start RADIUS
9. Start Snort (IDS service)
10. Look at database
ATTACK OPTIONS:
11. ForkBomb (exit with ctrl + c)
12. Portscan
13. NMAP - Analyse

Valg: 
```

I dette avsnittet går vi gjennom hver av disse valgene, med forslag til bruk og utvidelse.

6.1 1: Start firewall

Det første valget starter et skript som er tilpasset demonstrasjon av brannmur. Her er funksjonaliteten ganske enkel: et skript starte brannmurprogramvaren (ufw, abstraksjonslag oppå iptables) og laster inn en på forhånd oppsatt konfigurasjon som låser ned serveren, med unntak av portene som aktivt brukes i SNS som åpnes. Når skriptet er ferdig, dukker en oversikt over de åpne portene opp.

```
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
Rules updated
Rules updated (v6)
Rules updated
Rules updated (v6)
Rules updated
Rules updated (v6)
Rules updated
Rules updated (v6)
Rules updated
Rules updated (v6)
Rules updated
Rules updated (v6)
Rules updated
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing)
New profiles: skip

To
--
22/tcp          ALLOW IN    Anywhere
80/tcp          ALLOW IN    Anywhere
3306/tcp        ALLOW IN    Anywhere
25/tcp          ALLOW IN    Anywhere
3128/tcp        ALLOW IN    Anywhere
1886/tcp        ALLOW IN    Anywhere
22/tcp          ALLOW IN    Anywhere (v6)
80/tcp          ALLOW IN    Anywhere (v6)
3306/tcp        ALLOW IN    Anywhere (v6)
25/tcp          ALLOW IN    Anywhere (v6)
3128/tcp        ALLOW IN    Anywhere (v6)
1886/tcp        ALLOW IN    Anywhere (v6)

To edit firewall rules, run 'firewallUpdateRule'
vagrant@precise32:~$
```

Som vi ser av bildet, er de portene som er markert som åpne inn kun de som er ibruk av Simple Network Server. For å demonstrere brannmurendringern, kan skriptet 'firewallUpdateRule' kjøres rett fra kommando-linja. Dette skriptet er skrevet for enkelt og greit å gjøre endringer i aksesspolicyen til portene på serveren. Du velger om en port skal åpnes eller lukkes, og får da ny oversikt over portene på serveren. Dette for å lett kunne demonstrere brannmurens virkemåte. Eksempelet på bruk kan være å stenge port 80, for så å besøke <http://localhost:8080> og se at aksessen nå er sperret. Anne bruk kan være å kjøre portscanner mot serverens adresse og se på åpne porter.

```
To edit firewall rules, run 'firewallUpdateRule'
vagrant@precise32:~$ firewallUpdateRule
Allow or Deny [a|d]
d
Port to deny:
80
Rule updated
Rule updated (v6)
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing)
New profiles: skip

To          Action      From
--          -
22/tcp      ALLOW IN    Anywhere
80/tcp      DENY IN     Anywhere
3306/tcp    ALLOW IN    Anywhere
25/tcp      ALLOW IN    Anywhere
3128/tcp    ALLOW IN    Anywhere
1886/tcp    ALLOW IN    Anywhere
22/tcp      ALLOW IN    Anywhere (v6)
80/tcp      DENY IN     Anywhere (v6)
3306/tcp    ALLOW IN    Anywhere (v6)
25/tcp      ALLOW IN    Anywhere (v6)
3128/tcp    ALLOW IN    Anywhere (v6)
1886/tcp    ALLOW IN    Anywhere (v6)

vagrant@precise32:~$
```

Eksempel på bruk av 'firewallUpdateRule', port 80 blir sperret.

6.2 2: Start apachemonitor

Dette valget er ganske rett fram; et tilpasset skript deler skjermen i to og viser henholdsvis error og standard - loggen til webserveren apache2. Dette for å vise oppføringer som kommer når vi besøker sider hostet på webtjeneren, og kan vise hva som skjer når vi bestemmer oss for å "plage" LAMP - serveren.

```
1. vagrant@precise32: ~ (bash)
(Ubuntu) (internal dummy connection)"
127.0.0.1 - - [20/Jan/2014:11:14:16 +0000] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.2.22
(Ubuntu) (internal dummy connection)"
127.0.0.1 - - [20/Jan/2014:11:14:17 +0000] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.2.22
(Ubuntu) (internal dummy connection)"
127.0.0.1 - - [20/Jan/2014:11:14:17 +0000] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.2.22
(Ubuntu) (internal dummy connection)"
127.0.0.1 - - [20/Jan/2014:11:14:17 +0000] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.2.22
(Ubuntu) (internal dummy connection)"
127.0.0.1 - - [20/Jan/2014:11:14:17 +0000] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.2.22
(Ubuntu) (internal dummy connection)"
127.0.0.1 - - [20/Jan/2014:11:14:17 +0000] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.2.22
(Ubuntu) (internal dummy connection)"
10.0.2.2 - - [20/Jan/2014:12:32:42 +0000] "GET / HTTP/1.1" 200 490 "-" "Mozilla/5.0 (Macin
tosh; Intel Mac OS X 10.9; rv:26.0) Gecko/20100101 Firefox/26.0"
10.0.2.2 - - [20/Jan/2014:12:32:46 +0000] "GET / HTTP/1.1" 200 490 "-" "Mozilla/5.0 (Macin
tosh; Intel Mac OS X 10.9; rv:26.0) Gecko/20100101 Firefox/26.0"
10.0.2.2 - - [20/Jan/2014:12:32:46 +0000] "GET /favicon.ico HTTP/1.1" 404 500 "-" "Mozilla
/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26.0) Gecko/20100101 Firefox/26.0"
10.0.2.2 - - [20/Jan/2014:12:32:46 +0000] "GET /favicon.ico HTTP/1.1" 404 500 "-" "Mozilla
/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26.0) Gecko/20100101 Firefox/26.0"

or directory in Unknown on line 0
PHP Warning: PHP Startup: Unable to load dynamic library '/usr/lib/php5/20090626+lfs/mysq
li.so' - /usr/lib/php5/20090626+lfs/mysql.so: cannot open shared object file: No such fil
e or directory in Unknown on line 0
PHP Warning: PHP Startup: Unable to load dynamic library '/usr/lib/php5/20090626+lfs/pdo_
mysql.so' - /usr/lib/php5/20090626+lfs/pdo_mysql.so: cannot open shared object file: No su
ch file or directory in Unknown on line 0
[Mon Jan 20 11:14:16 2014] [notice] Apache/2.2.22 (Ubuntu) PHP/5.3.10-1ubuntu3.9 with Suho
sin-Patch configured -- resuming normal operations
[Mon Jan 20 11:14:17 2014] [notice] Graceful restart requested, doing restart
apache2: Could not reliably determine the server's fully qualified domain name, using 127.
0.1.1 for ServerName
PHP Warning: PHP Startup: Unable to load dynamic library '/usr/lib/php5/20090626+lfs/mysq
lnd.so' - /usr/lib/php5/20090626+lfs/mysqlnd.so: cannot open shared object file: No such f
ile or directory in Unknown on line 0
[Mon Jan 20 11:14:17 2014] [notice] Apache/2.2.22 (Ubuntu) PHP/5.3.10-1ubuntu3.9 with Suho
sin-Patch configured -- resuming normal operations
[Mon Jan 20 12:32:46 2014] [error] [client 10.0.2.2] File does not exist: /var/www/favicon
.ico
[Mon Jan 20 12:32:46 2014] [error] [client 10.0.2.2] File does not exist: /var/www/favicon
.ico
[0] 0:sh* "precise32" 12:33 20-Jan-14
```

Bildet viser eksempel på loggoppføring ved vanlig besøk på innhold hostet av webtjeneren. Leg merke til advarsel om fil som ikke eksisterer, denne feilen er framprovosert for å vise feil i loggen. Eksempel på bruk kan være å se hva som skjer i loggen om en modifisert get - request blir sendt.

6.3 3: Start fail2ban (IPS Service)

En av de mest effektive Intrusion Prevention System - tjenestene der ute er fail2ban. Den banner rett og slett IP - adresser som prøver seg på bruteforce - angrep på serveren. Tjenesten starter rett og slett fail2ban etter en gitt tid. For å demonstrere bruk av fail2ban kan python-skriptet "ssh_forcer.py" kjøres fra host - maskinen. Skriptet ligger på "SNS/bin/Client/ssh_forcer.py". Skriptet vil prøve å bruteforce SSH - login på SSN - serveren, passordforsøk på passordforsøk. Ved å aktivere fail2ban, kan man se at angrepsforsøkene stopper fordi IPen til slutt blir bannet. Effektiv demo av en IPS sine egenskaper: Den gjør aktive tiltak mot angriper.

```
] Starting fail2ban in 3 seconds to actively prevent bruteforce...
] Started
]

andreas@afrodite:~/Dev/SNS/bin/Client$ ./ssh_forcer.py
Incorrect password: 01234
Incorrect password: 01235
Incorrect password: 01236
Incorrect password: 01237
Incorrect password: 01238
Incorrect password: 01239
Incorrect password: 01245
No handlers could be found for logger "paramiko.transport"
name 'socket' is not defined
andreas@afrodite:~/Dev/SNS/bin/Client$ ]

an.log for Fail2ban v0.8.6
2014-01-20 14:11:09,541 fail2ban.jail : INFO Creating new jail 'ssh'
2014-01-20 14:11:09,560 fail2ban.jail : INFO Jail 'ssh' uses Gamin
2014-01-20 14:11:09,658 fail2ban.filter : INFO Added logfile = /var/log/auth.log
2014-01-20 14:11:09,665 fail2ban.filter : INFO Set maxRetry = 6
2014-01-20 14:11:09,667 fail2ban.filter : INFO Set findtime = 600
2014-01-20 14:11:09,668 fail2ban.actions: INFO Set banTime = 600
2014-01-20 14:11:09,732 fail2ban.jail : INFO Jail 'ssh' started
2014-01-20 14:12:13,246 fail2ban.server : INFO Stopping all jails
2014-01-20 14:12:13,928 fail2ban.jail : INFO Jail 'ssh' stopped
2014-01-20 14:12:13,943 fail2ban.server : INFO Exiting Fail2ban
2014-01-20 14:12:14,406 fail2ban.server : INFO Changed logging target to /var/log/fail2b
an.log for Fail2ban v0.8.6
2014-01-20 14:12:14,416 fail2ban.jail : INFO Creating new jail 'ssh'
2014-01-20 14:12:14,418 fail2ban.jail : INFO Jail 'ssh' uses Gamin
2014-01-20 14:12:14,455 fail2ban.filter : INFO Added logfile = /var/log/auth.log
2014-01-20 14:12:14,461 fail2ban.filter : INFO Set maxRetry = 6
2014-01-20 14:12:14,462 fail2ban.filter : INFO Set findtime = 600
2014-01-20 14:12:14,463 fail2ban.actions: INFO Set banTime = 600
2014-01-20 14:12:14,517 fail2ban.jail : INFO Jail 'ssh' started
2014-01-20 14:12:40,618 fail2ban.actions: WARNING [ssh] Ban 10.0.2.2
]
```

Bildet viser bruk av ssh_forcer og IPS - pakken. Her får angriper prøvd seg 7 ganger før fail2ban starter og får sendt IPen i "fengsel". Utvidelse her kan være bruteforce - forsøk på HTTP - serveren.

6.4 4: Send mail

Dette valget er ment som en demonstrasjon av hvor enkelt det er å sende epost med falsk avsender, som igjen kan føre til både phishingforsøk og spam. I dag regnes hele 80 - 85 % av all mailtrafikk som spam.³ Skriptet som starter mailsendingen spør deg om mottakeradresse (NB: ikke benytt skriptet uten at mottaker

³Kilde: https://en.wikipedia.org/wiki/Spam%28electronic%29cite_note-4

er klar over det!) og en ønsket avsenderadresser. Etter noen sekunder sendes mailen ut fra serveren, med en standard tekst som ligger lagret på `"/SNS/resources/doc/MailMessage"`.

OBS: For at denne funksjonaliteten skal funke kan man *ikke* være bak brannmur som stopper trafikk på SMTP - porten. Vanlige ISPer som Canal Digital osv. stopper trafikk her. Dette er derimot ikke et problem på HiST, hvor SNS hovedsaklig skal brukes.

```
vagrant@precise32:~$ mailSender
Enter recivers address:
andreas.mosti@gmail.com
Enter senders address:
Bill.Gates@microsoft.com
Sends email in 4 seconds:
Jan 20 15:35:15 precise32 sendEmail[22731]: Email was sent successfully!
For more advanced use of mail, use sendmail or similar.
vagrant@precise32:~$
```

Bill.Gates@microsoft.com
Til: Andreas Mosti <andreas.mosti@gmail.com>
Mail fra Simple Network Server

20. januar 2014 16:35
[Skjul detaljer](#)

1

Dette er en epost sendt fra Simple Network Server. Avsender er kanskje ikke den du tror, sjekk mail - headeren!

Her ser vi bruk av mailsender, hvor Bill Gates tilsynelatende har sendt mail. Men, som teksten sier, burde man sjekke mailheaderen for å se om avsender er den han er. Videre bruk av tjenesten kan være å lage til en phishing - mal som sendes, for å demonstrere hvor enkelt det er å lage en tilsynelatende ekte mail fra foreks. banken din. Et annet bruksmønster er å overvåke pakkene som går; tjenesten er lagt opp til å sende mail uten kryptering, så alt går i klartekst. Dette er også grunnen til at mailen venter 4 sekunder før den sendes, så foreks. Wireshark kan rettes mot serverens IP for se på pakkene som går.

6.5 5: Start networkmonitor

Dette valget er en nettverksmonitor satt sammen av programmene Nethogs og Iftop. Nethogs viser hvilke kjørende prosesser som genererer nettverkstrafikk, både innkommende og utgående, mens Iftop viser trafikk på eth0 - kortet, altså nettverkskortet på serveren. iftop viser hvilke IPer som blir kommunisert med, og hvor mye trafikk som går. Fordi SNS er bygget opp fra grun av med *kun* den funksjonaliteten vi ønsker for å demonstrere forskjellige aspekter ved faget Nettverkssikkerhet, vil det være få prosesser som kjører (SNS er programmert til å blokkere alle tjenestene fra oppstart, de blir kun aktive når du velge å bruke dem) som igjen fører til en ren og ryddig logg: den blir ikke oversvømt av prosesser som bruker nettverk. Dette verktøyet er derfor veldig fint å bruke for å demonstrere hvordan prosesser bruker trafikk inn / ut av serveren.

```
1. vagrant@precise32: ~ (ssh)
NetHogs version 0.8.0
```

PID	USER	PROGRAM	DEV	SENT	RECEIVED
24748	vagrant	sshd: vagrant@pts/0	eth0	0.839	0.105 KB/sec
?	root	unknown TCP		0.000	0.000 KB/sec
TOTAL				0.839	0.105 KB/sec

	12.5kb	25.0kb	37.5kb	50.0kb	62.5kb
10.0.2.15		=> 10.0.2.2		7.50kb	6.03kb 5.82kb
		<=		640b	512b 506b
10.0.2.15		=> tikk.signal.no		0b	61b 15b
		<=		0b	61b 15b
10.0.2.15		=> tim.des.no		0b	61b 15b
		<=		0b	61b 15b

	cum:	256kB	peak:	7.50kb	rates:	7.50kb	6.14kb	5.85kb
TX:								
RX:		23.2kB		1.06kb		640b	634b	536b
TOTAL:		279kB		8.12kb		8.12kb	6.76kb	6.37kb

```
[0] 0:sh* "precise32" 19:25 20-Jan-14
```

Det øverste vinduet er Nethogs, som her kun viser en aktiv prosess som bruker av nettverket, nemlig SSH, som jeg kommuniserer med serveren via.

Nedenfor ser vi iftop som melder om trafikk fra serveren til 10.0.2.2 som er hostmaskinens IP, samt trafikk til Signal, som er ISP der serveren står. Forslag bruk av denne netverksmonitoren er som nevnt å vise hvordan trafikk til / fra serveren vises, og man kan demonstrere hvor greit det er å holde orden på hvilke prosesser som bruker nettverksresurser i systemet. Skulle serveren bli kompromitert og bli en del av et botnet, kan man da helt klart se av monitoren om noe genererer mye trafikk.

7 Om kildekodens oppbygging

<her kommer beskrivelse av mappestruktur>