Reconnaissance

The Harvester

Target: Uia.no.
What can you find?
How many email addresses can you find?

```
# By running theharvester with arguments to collect all info on uia.no
theharvester -d uia.no -b all >> theharvesterlog.txt
```

```
# we get 32 e-mails, and a whole lot of IPs:
```

```
Agderpost@uia.no
Ingrid.t.angeltvedt@uia.no
Polyxeni.Vasilakopoulou@uia.no
carl.e.moe@uia.no
christian.holden@uia.no
csirt@uia.no
daniel.goller@uia.no
einar.d.bohn@uia.no
evuopptakr@uia.no
gro.frivold@uia.no
helge.hoynes@uia.no
henrin10@uia.no
janl13@student.uia.no
john.ploger@uia.no
lars.nesland@uia.no
laszlo.erdodi@uia.no
liv.b.friestad@uia.no
malintm@uia.no
maurice.isabwe@uia.no
nils.k.hansen@uia.no
oystein.sylta@uia.no
oyvind.nesland@uia.no
pixel-1535705160721266-web-@uia.no
pixel-1535705163152655-web-@uia.no
pixel-1535705165219071-web-@uia.no
```

```
post@uia.no
rl@uia.no
robert.larsen@uia.no
sigurd.m.assev@uia.no
sta@uia.no
terje.gjosater@uia.no
tina.l.barken@uia.no


[-] Resolving hostnames IPs...
158.36.36.189:2Femco.project.uia.no
158.36.36.189:2Femrg.project.uia.no
158.36.166.164:Old.uia.no
158.37.221.30:beta.uia.no
158.37.221.137:cair.uia.no
158.36.36.189:ciem.prosjekt.uia.no
89.221.244.49:ciem.uia.no
158.36.166.165:coastalresearch.uia.no
158.36.36.189:emco.project.uia.no
158.36.36.189:emrg.project.uia.no
158.36.166.159:eras.uia.no
158.36.51.146:foto.uia.no
128.39.145.244:grimstad-mp.uia.no
158.36.52.10:grimstad.uia.no
158.37.220.165:home.uia.no
158.36.166.182:iscram2015.uia.no
158.36.166.165:jois.uia.no
158.36.166.184:journal.uia.no
158.36.166.229:kompetanse.uia.no
158.36.87.8:kristiansand-mp.uia.no
158.36.232.72:krs-158-36-232-72.studby.uia.no
158.37.220.166:kurs.uia.no
52.48.240.72:libguides.uia.no
89.221.250.26:makromedia.uia.no
158.36.52.21:media.uia.no
158.36.52.11:mesh.uia.no
158.36.36.40:ns1.uia.no
158.36.51.40:ns2.uia.no
158.36.166.164:old.uia.no
```

```
158.37.220.31:owa.uia.no
158.36.36.189:prosjekt.uia.no
158.36.166.174:skolebibliotek.uia.no
158.36.166.172:student.uia.no
188.138.32.138:tflip.uia.no
158.37.220.133:tools.uia.no
158.36.166.174:www.skolebibliotek.uia.no
158.37.220.160:www.uia.no
[+] Virtual hosts:
==================
89.221.244.49       www.brgruppen.no
89.221.244.49       gardsbruk.no
89.221.244.49       univa.no
89.221.244.49       www.ostereng.no
89.221.244.49       legalspania.com
89.221.244.49       strai.no
89.221.244.49       www.hovdenhytteservice.no
89.221.244.49       www.univa.no
89.221.244.49       smso-agder.no
89.221.244.49       mkirken.no
89.221.244.49       arna-misjonsmenighet.no
89.221.244.49       frimisjonen.no
89.221.244.49       nsft.net
89.221.244.49       misjonskirka.net
89.221.244.49       ciem
89.221.244.49       intranett.otera.no
89.221.244.49       bigcatering.no
89.221.244.49       www.svc.as
89.221.244.49       torinokledet.no
89.221.244.49       morfarbarn.no
89.221.244.49       aaneslandlimtre.no
89.221.244.49       www.heimover.no
89.221.244.49       haugeinstitute.org
89.221.244.49       infomap.no
89.221.244.49       www.ufotrafikkskole.no
89.221.244.49       saevind.no
89.221.244.49       www.saevind.no
89.221.244.49       www.interfreight.no
89.221.244.49       stemmerettsjubileet.no
```

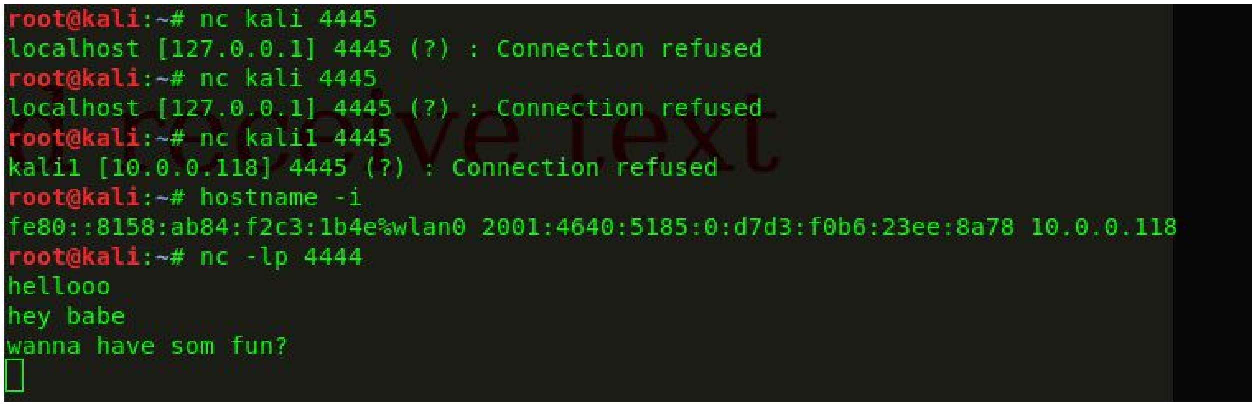
89.221.244.49	www.kjellevikhansen.no
89.221.244.49	www.odderoya.no
89.221.244.49	www.progressia.no
89.221.244.49	ciem.uia.no
89.221.244.49	www.smso-agder.no
89.221.244.49	www.arna-misjonsmenighet.no
89.221.244.49	www.morfarbarn.no
89.221.244.49	odderoya.no
89.221.244.49	www.legalspania.com
158.36.166.165	jois.uia.no
158.36.166.165	wisenet.uia.no
158.36.166.165	coastalresearch.uia.no
158.36.166.165	friluft.uia.no
158.36.166.165	www.ladyklukk.no
158.36.166.165	kik.uia.no
158.36.166.165	mcg.uia.no
52.48.240.72	libguides.ucc.ie
52.48.240.72	library.worc.ac.uk
52.48.240.72	libguides.hull.ac.uk
52.48.240.72	parisdescartes.libguides.com
52.48.240.72	biblioguias.unex.es
52.48.240.72	hv.se.libguides.com
52.48.240.72	libguides.stir.ac.uk
52.48.240.72	libguides.ioe.ac.uk
52.48.240.72	biblioguias.ulpgc.es
52.48.240.72	libguides.qub.ac.uk
52.48.240.72	libguides.city.ac.uk
52.48.240.72	guides.library.lincoln.ac.uk
52.48.240.72	www.natolibguides.info
52.48.240.72	libguides.shu.ac.uk
89.221.250.26	www.bastionen.no
89.221.250.26	wpc.lmk.no
89.221.250.26	www.jegu.no
89.221.250.26	nmf.nu
89.221.250.26	www.roligheden.no
89.221.250.26	www.broderiservice.no
89.221.250.26	www.lundsvagen-batforening.no
89.221.250.26	utedusj.no
89.221.250.26	x-rayukh.no

89.221.250.26	www.kordacapo.no
89.221.250.26	www.batforerproven.com
89.221.250.26	www.ah-ark.no
89.221.250.26	torpo.no
89.221.250.26	dahr.no
89.221.250.26	moester.no
89.221.250.26	www.sgk.no
89.221.250.26	www.vhfkurs.no
89.221.250.26	www.tauboll.no
89.221.250.26	www.hvesser.no
89.221.250.26	www.b&#229;tf&#248;rerpr&#248;ven.com
89.221.250.26	vulcanriders-sweden.org
89.221.250.26	www.nmf.nu
89.221.250.26	www.saterglantan.se
158.36.166.174	www.skolebibliotek.uia.no
158.37.220.160	www.uia.no
158.37.220.160	www.allevarer.no
158.37.220.160	libguides.uia.no

Netcat

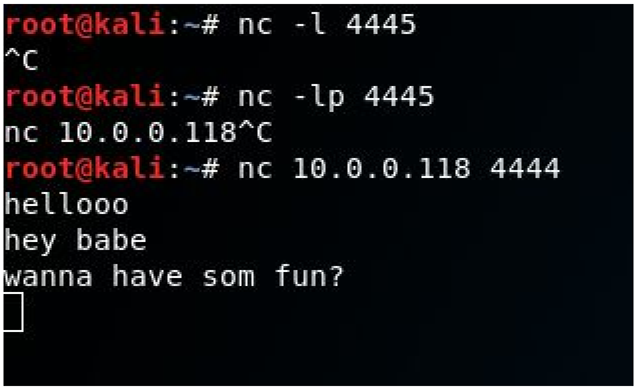
1. Establish a chat session

Machine who is listening:



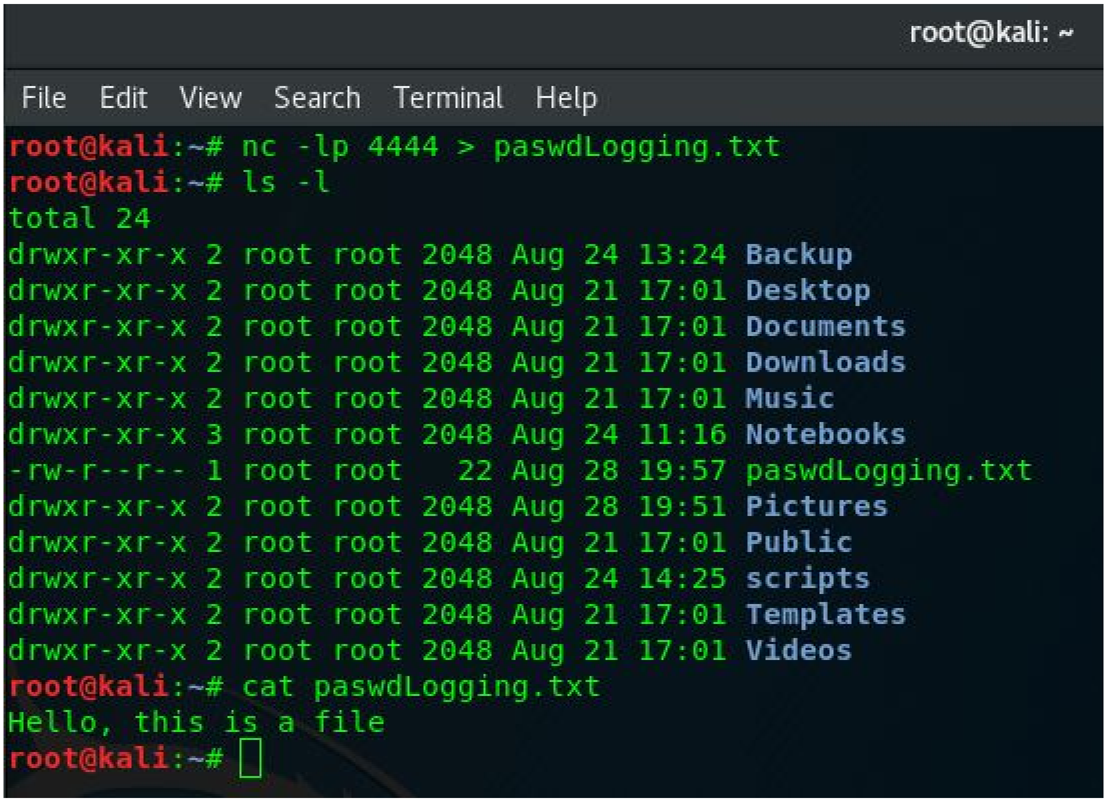
```
root@kali:~# nc kali 4445
localhost [127.0.0.1] 4445 (?) : Connection refused
root@kali:~# nc kali 4445
localhost [127.0.0.1] 4445 (?) : Connection refused
root@kali:~# nc kali1 4445
kali1 [10.0.0.118] 4445 (?) : Connection refused
root@kali:~# hostname -i
fe80::8158:ab84:f2c3:1b4e%wlan0 2001:4640:5185:0:d7d3:f0b6:23ee:8a78 10.0.0.118
root@kali:~# nc -lp 4444
hellooo
hey babe
wanna have som fun?
```

Machine making contact:



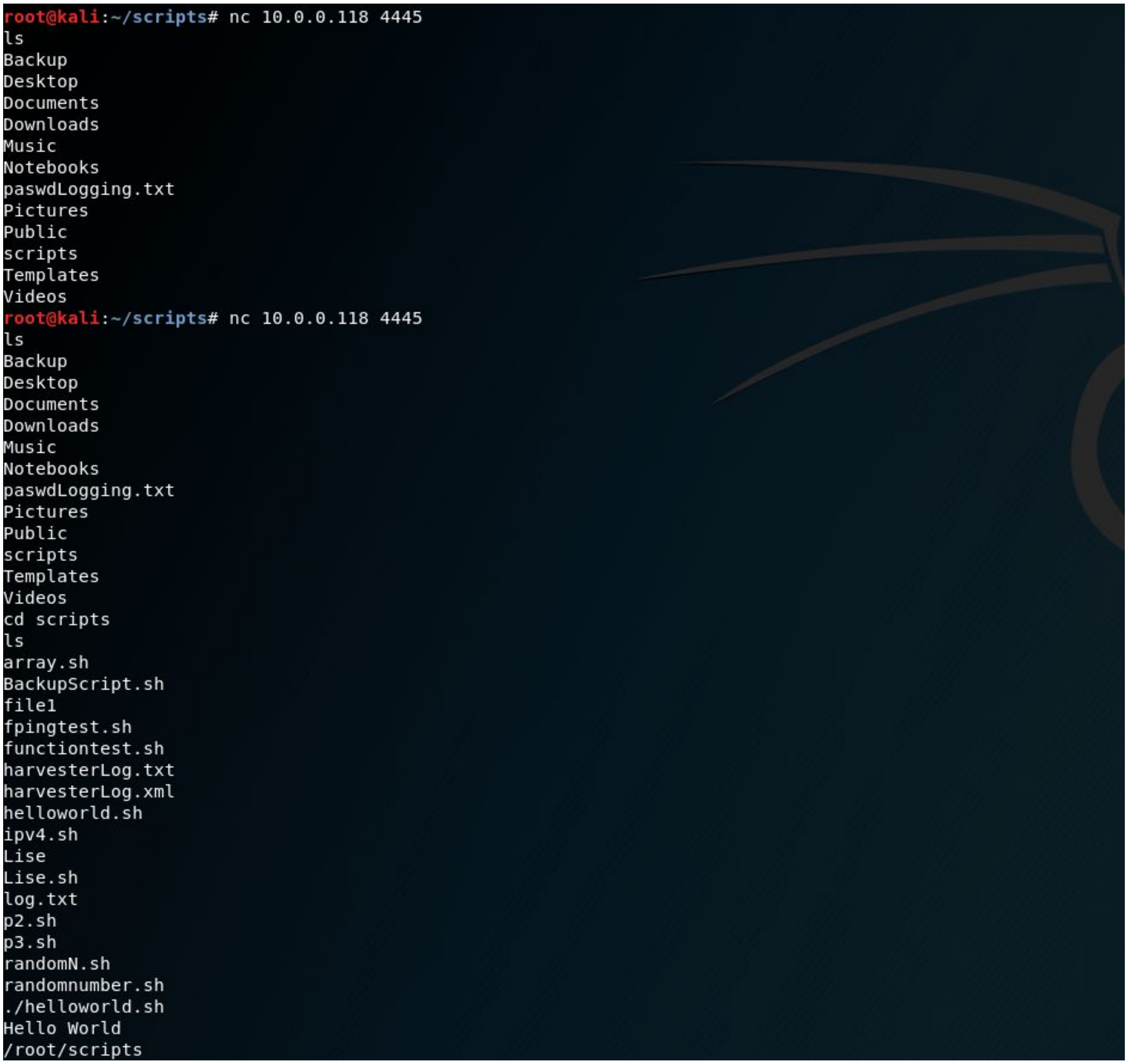
```
root@kali:~# nc -l 4445
^C
root@kali:~# nc -lp 4445
nc 10.0.0.118^C
root@kali:~# nc 10.0.0.118 4444
hellooo
hey babe
wanna have som fun?
```

2. Transfer files between machines



```
root@kali:~# nc -lp 4444 > paswdLogging.txt
root@kali:~# ls -l
total 24
drwxr-xr-x 2 root root 2048 Aug 24 13:24 Backup
drwxr-xr-x 2 root root 2048 Aug 21 17:01 Desktop
drwxr-xr-x 2 root root 2048 Aug 21 17:01 Documents
drwxr-xr-x 2 root root 2048 Aug 21 17:01 Downloads
drwxr-xr-x 2 root root 2048 Aug 21 17:01 Music
drwxr-xr-x 3 root root 2048 Aug 24 11:16 Notebooks
-rw-r--r-- 1 root root   22 Aug 28 19:57 paswdLogging.txt
drwxr-xr-x 2 root root 2048 Aug 28 19:51 Pictures
drwxr-xr-x 2 root root 2048 Aug 21 17:01 Public
drwxr-xr-x 2 root root 2048 Aug 24 14:25 scripts
drwxr-xr-x 2 root root 2048 Aug 21 17:01 Templates
drwxr-xr-x 2 root root 2048 Aug 21 17:01 Videos
root@kali:~# cat paswdLogging.txt
Hello, this is a file
root@kali:~# 
```

3. Export a shell



```
root@kali:~/scripts# nc 10.0.0.118 4445
ls
Backup
Desktop
Documents
Downloads
Music
Notebooks
paswdLogging.txt
Pictures
Public
scripts
Templates
Videos
root@kali:~/scripts# nc 10.0.0.118 4445
ls
Backup
Desktop
Documents
Downloads
Music
Notebooks
paswdLogging.txt
Pictures
Public
scripts
Templates
Videos
cd scripts
ls
array.sh
BackupScript.sh
file1
fpingtest.sh
functiontest.sh
harvesterLog.txt
harvesterLog.xml
helloworld.sh
ipv4.sh
Lise
Lise.sh
log.txt
p2.sh
p3.sh
randomN.sh
randomnumber.sh
./helloworld.sh
Hello World
/root/scripts
```