SensePost

Automation - Deus ex Machina or Rube Goldberg Machine?

How far can automation be taken? How much intelligence can be embodied in code? How generic can automated IT security assessment tools really be? This presentation will attempt to show which areas of attacks lend themselves to automation and which aspects should best be left for manual human inspection and analyses.

SensePost will provide the audience a glimpse of BiDiBLAH - an attempt to automate a focussed yet comprehensive assessment. The tool provides automation for:

- Finding networks and targets
- Fingerprinting targets
- Discovering known vulnerabilities on the targets
- Exploiting the vulnerabilities found
- Reporting

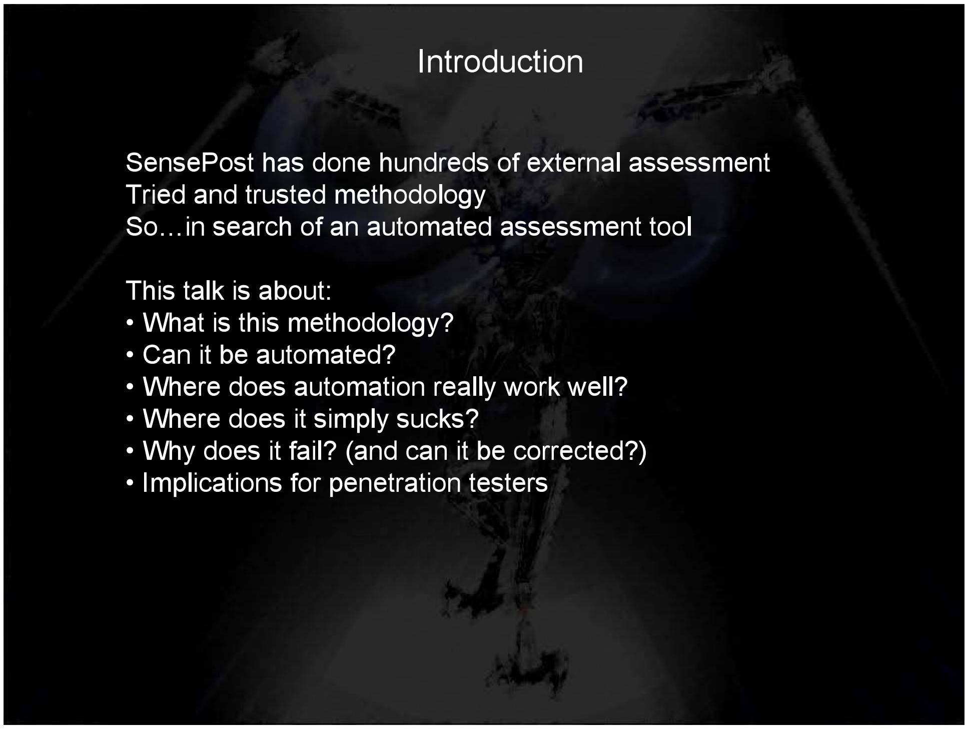
Roelof Temmingh *is the Technical Director of SensePost where his primary function is that of external penetration specialist. Roelof is internationally recognized for his skills in the assessment of web servers. He has written various pieces of PERL code as proof of concept for known vulnerabilities, and coded the world-first anti-IDS web proxy "Pudding". He has spoken at many International Conferences and in the past year alone has been a keynote speaker at SummerCon (Holland) and a speaker at The Black Hat Briefings. Roelof drinks tea and smokes Camels.*

Haroon Meer *is currently SensePost's Director of Development (and coffee drinking). He specializes in the research and development of new tools and techniques for network penetration and has released several tools, utilities and white-papers to the security community. He has been a guest speaker at many Security forums including the Black Hat Briefings. Haroon doesnt drink tea or smoke camels.*

Charl van der Walt *is a founder member of SensePost. He studied Computer Science at UNISA, Mathematics at the University of Heidelberg in Germany and has a Diploma in Information Security from the Rand Afrikaans University. He is an accredited BS7799 Lead Auditor with the British Institute of Standards in London. Charl has a number of years experience in Information Security and has been involved in a number of prestigious security projects in Africa, Asia and Europe. He is a regular speaker at seminars and conferences nationwide and is regularly published on internationally recognized forums like SecurityFocus. Charl has a dog called Fish.*

Assessment automation:
Deux ex Machina
||
Rube Goldberg
Machine?

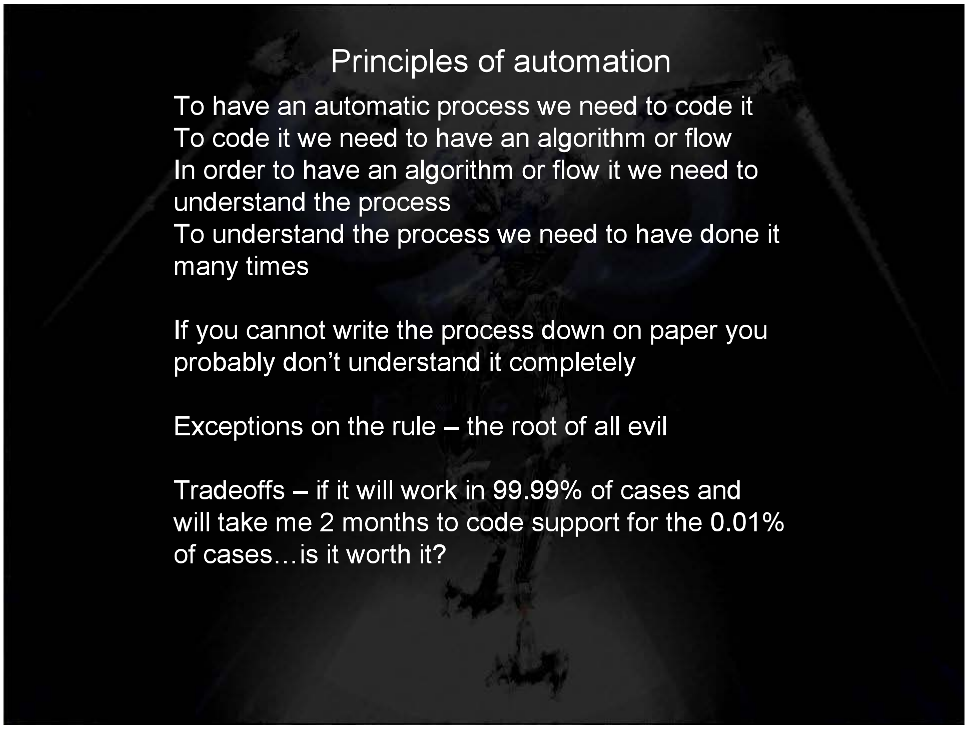
2005
LAS VEGAS



Introduction

SensePost has done hundreds of external assessment
Tried and trusted methodology
So…in search of an automated assessment tool

This talk is about:
- What is this methodology?
- Can it be automated?
- Where does automation really work well?
- Where does it simply sucks?
- Why does it fail? (and can it be corrected?)
- Implications for penetration testers



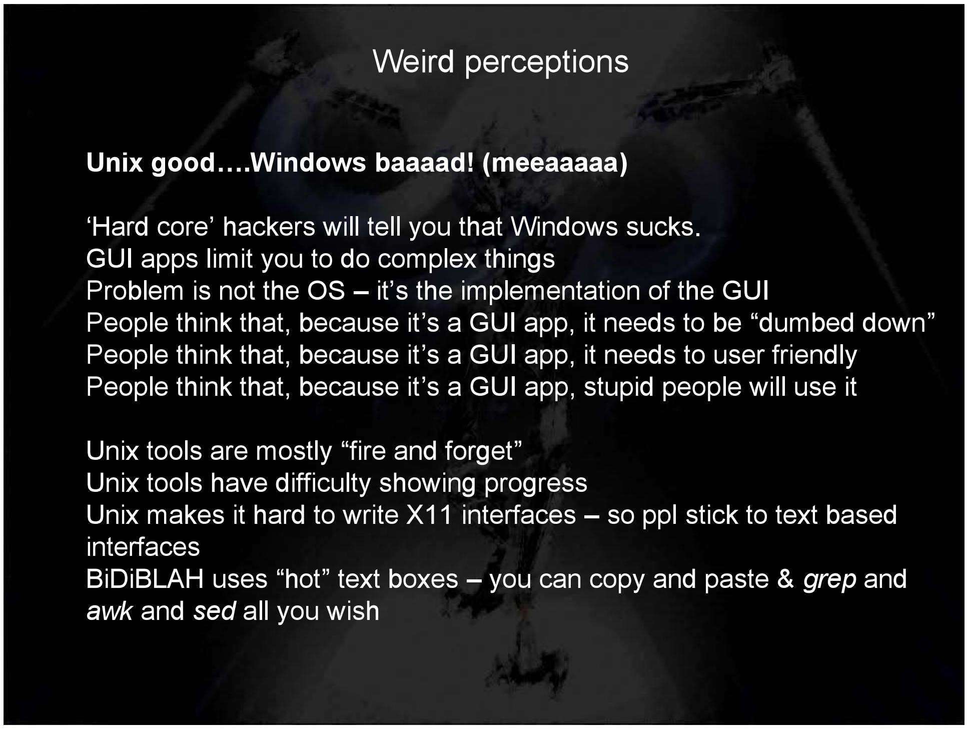
Principles of automation

To have an automatic process we need to code it
To code it we need to have an algorithm or flow
In order to have an algorithm or flow it we need to understand the process
To understand the process we need to have done it many times

If you cannot write the process down on paper you probably don't understand it completely

Exceptions on the rule – the root of all evil

Tradeoffs – if it will work in 99.99% of cases and will take me 2 months to code support for the 0.01% of cases…is it worth it?

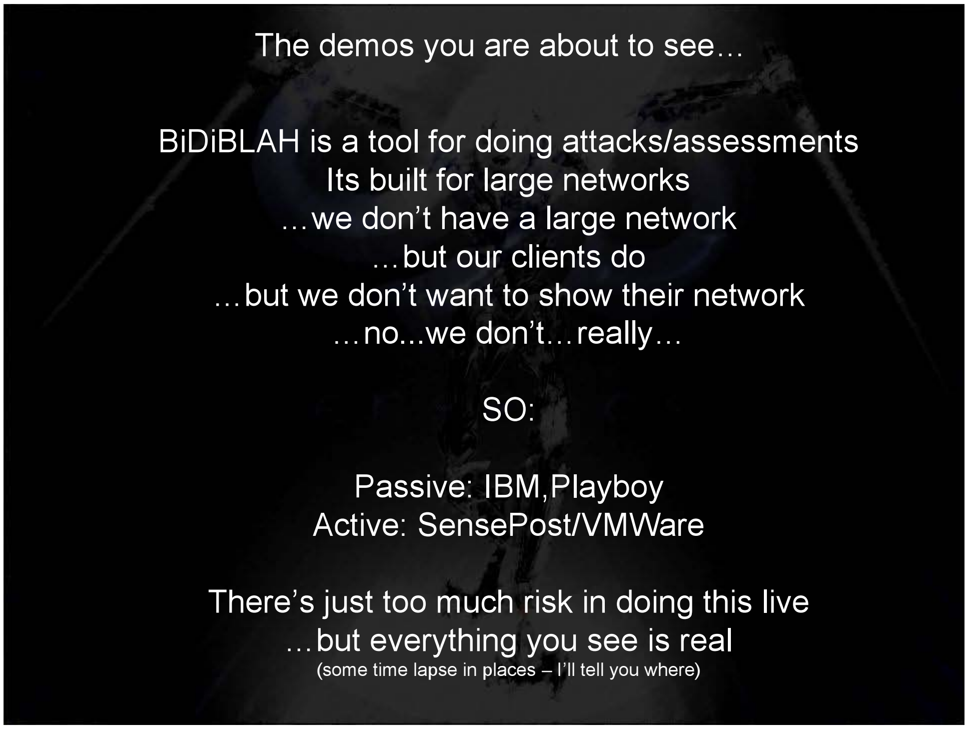


Weird perceptions

Unix good….Windows baaaad! (meeaaaaa)

'Hard core' hackers will tell you that Windows sucks.
GUI apps limit you to do complex things
Problem is not the OS – it's the implementation of the GUI
People think that, because it's a GUI app, it needs to be "dumbed down"
People think that, because it's a GUI app, it needs to user friendly
People think that, because it's a GUI app, stupid people will use it

Unix tools are mostly "fire and forget"
Unix tools have difficulty showing progress
Unix makes it hard to write X11 interfaces – so ppl stick to text based interfaces
BiDiBLAH uses "hot" text boxes – you can copy and paste & *grep* and *awk* and *sed* all you wish



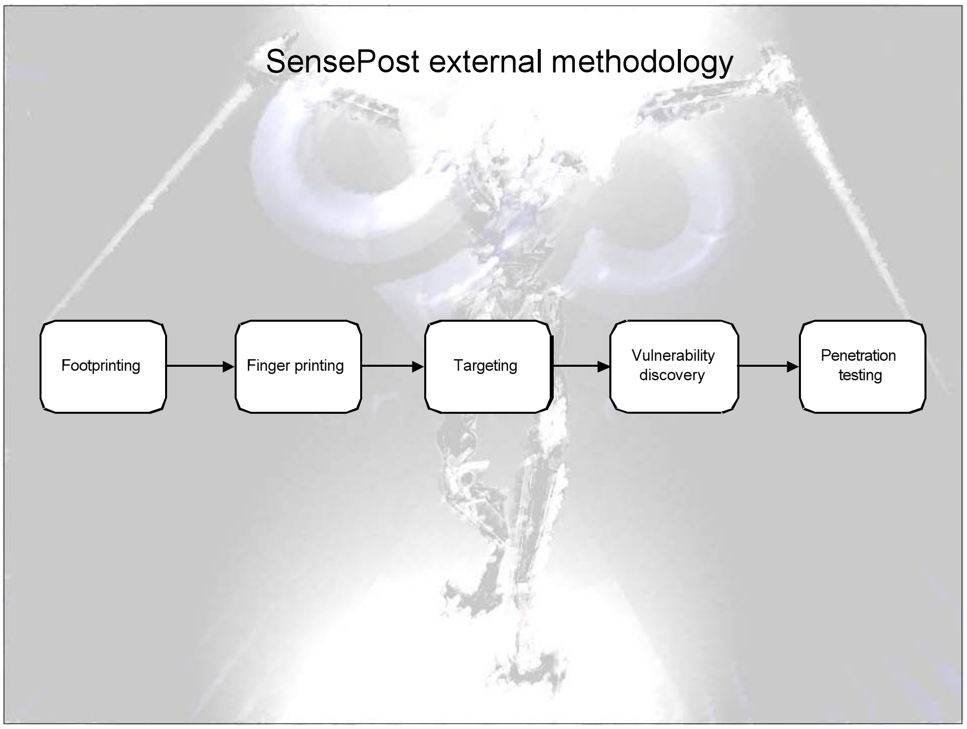
The demos you are about to see…

BiDiBLAH is a tool for doing attacks/assessments
Its built for large networks
…we don't have a large network
…but our clients do
…but we don't want to show their network
…no...we don't…really…

SO:

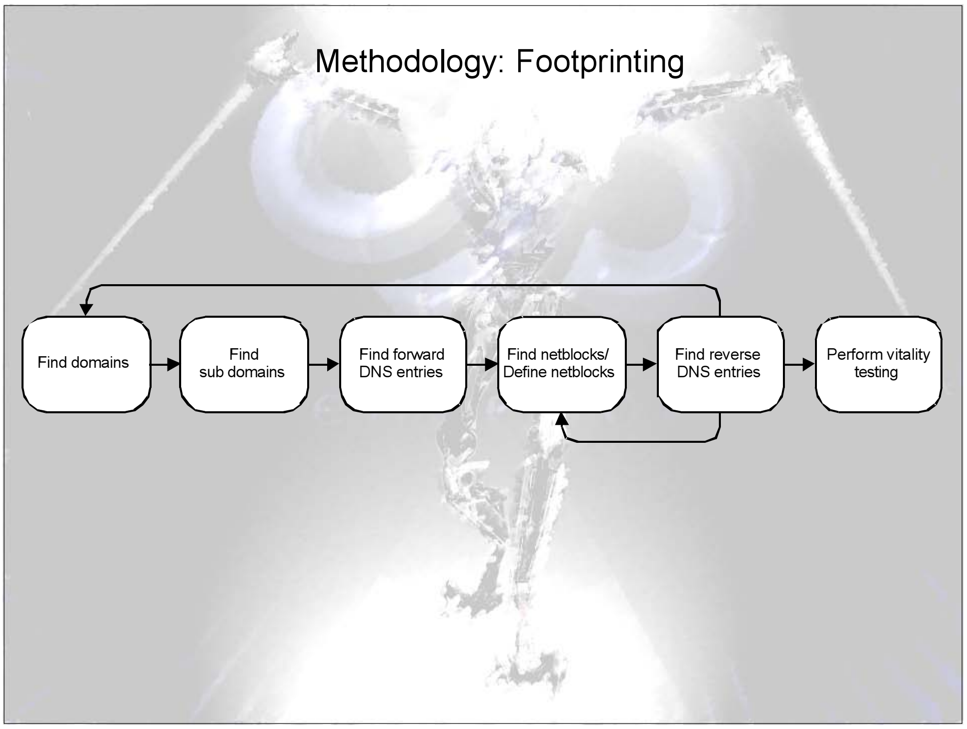
Passive: IBM,Playboy
Active: SensePost/VMWare

There's just too much risk in doing this live
…but everything you see is real
(some time lapse in places – I'll tell you where)



SensePost external methodology

Footprinting → Finger printing → Targeting → Vulnerability discovery → Penetration testing



Methodology: Footprinting

Find domains

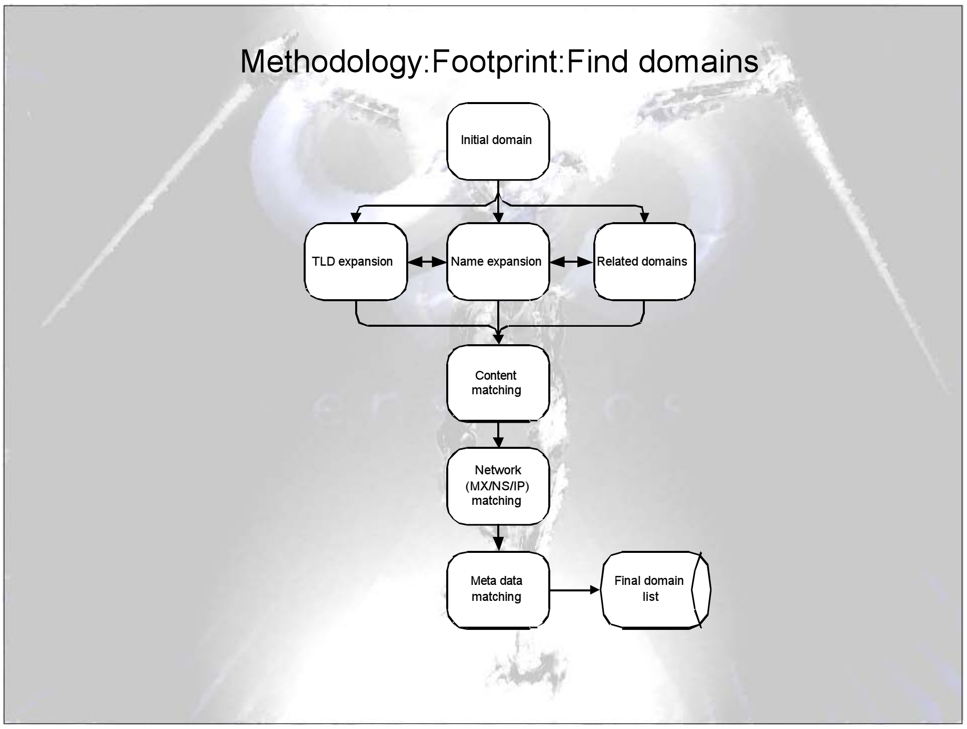
Find sub domains

Find forward DNS entries

Find netblocks/ Define netblocks

Find reverse DNS entries

Perform vitality testing



Methodology:Footprint:Find domains

Initial domain

TLD expansion

Name expansion

Related domains

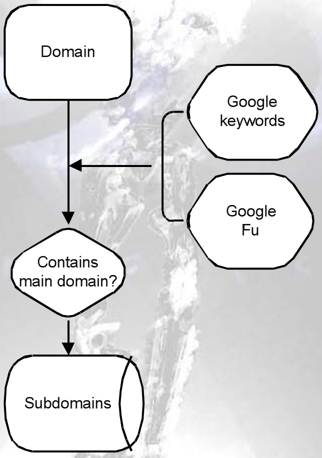
Content matching

Network (MX/NS/IP) matching

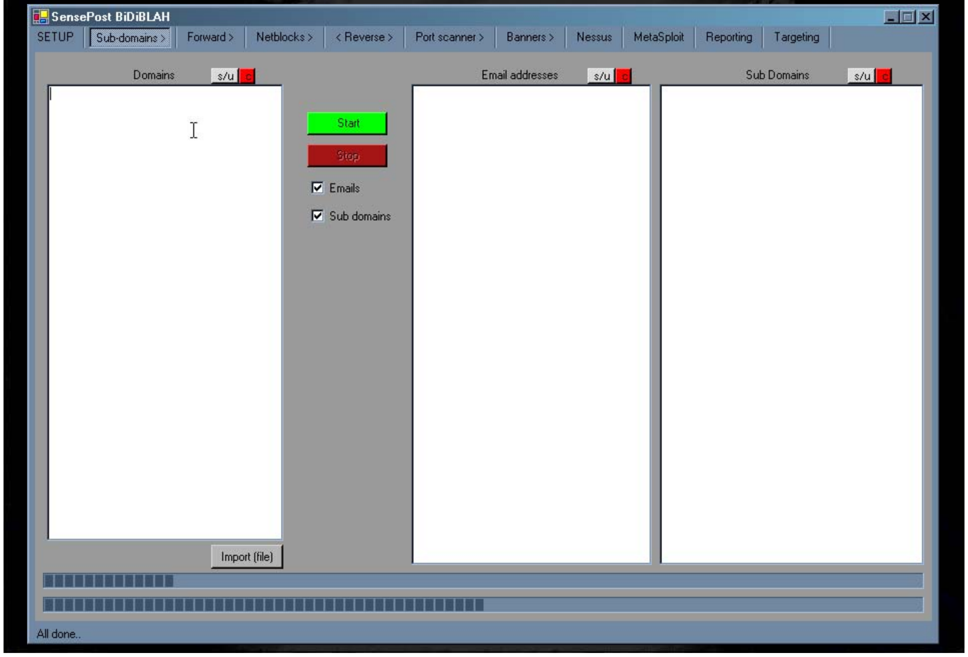
Meta data matching

Final domain list

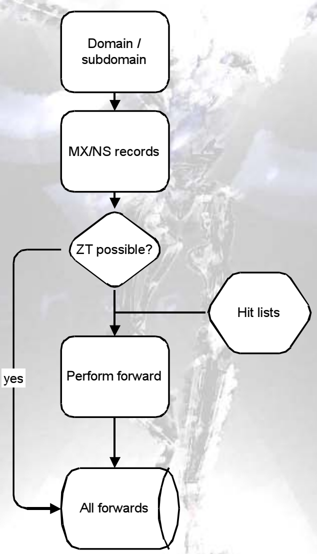
Methodology: Footprinting: Find subdomains



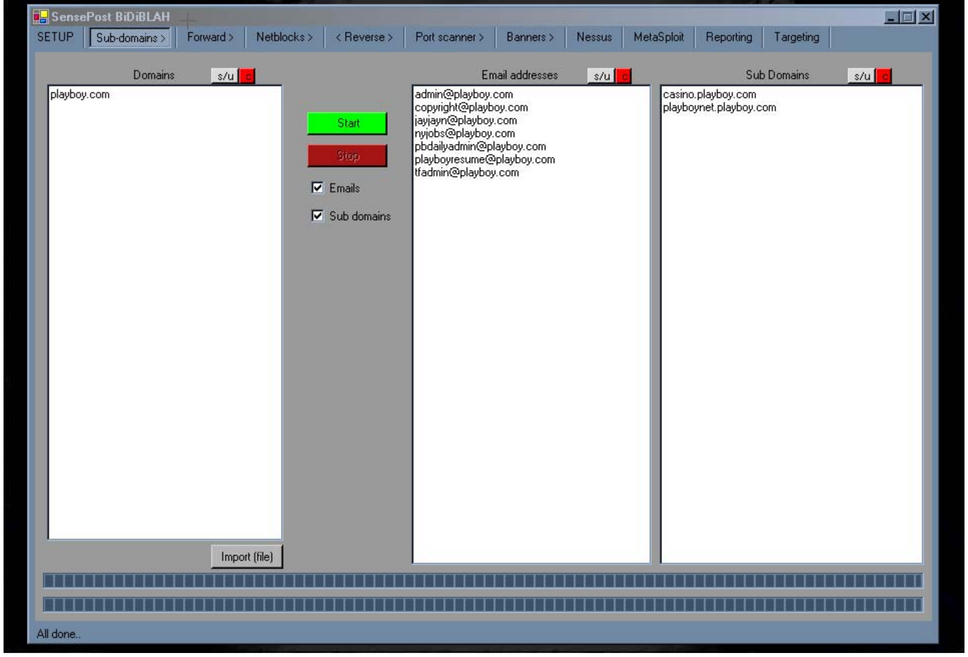
Video – BiDiBLAH's footprinting : Sub domains



Methodology: Footprinting: Forward DNS entries



Video – BiDiBLAH's footprinting : Forwards



Domains: playboy.com

☑ Emails

☑ Sub domains

Email addresses:

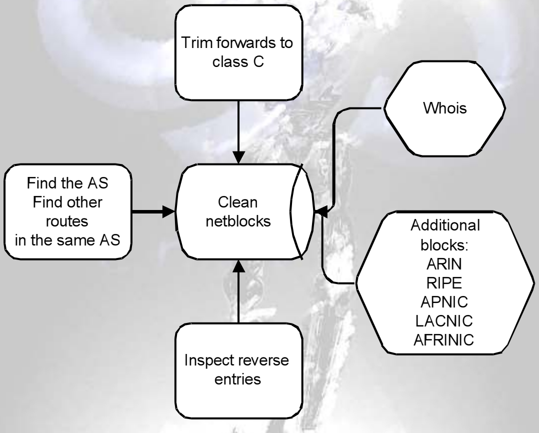
admin@playboy.com
copyright@playboy.com
jayjayn@playboy.com
nyjobs@playboy.com
pbdailyadmin@playboy.com
playboyresume@playboy.com
tfadmin@playboy.com

Sub Domains:

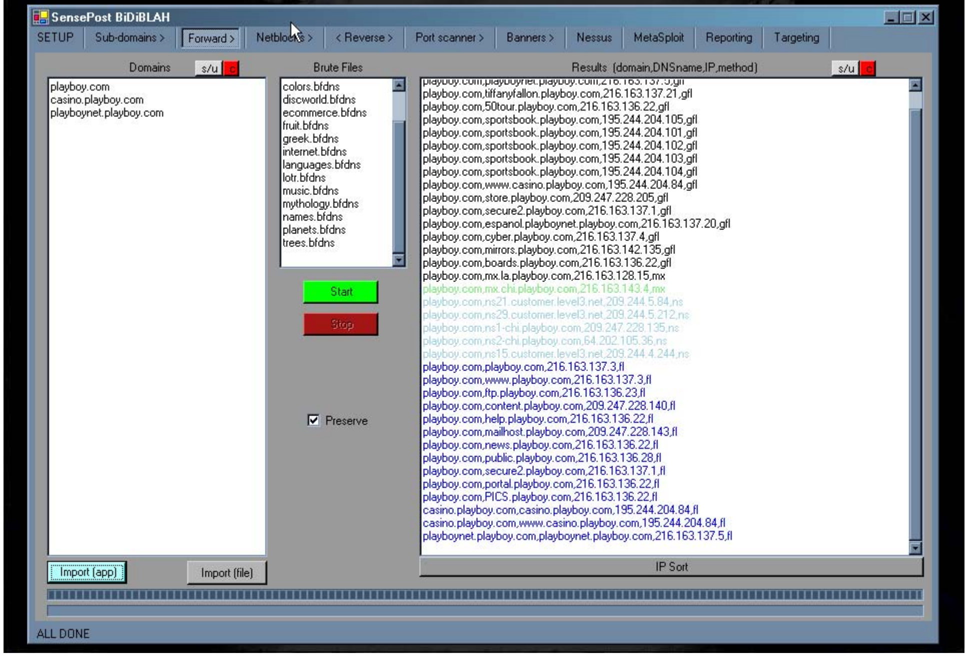
casino.playboy.com
playboynet.playboy.com

All done..

Methodology: Footprint: Netblocks


Trim forwards to class C
Whois
Find the AS Find other routes in the same AS
Clean netblocks
Additional blocks: ARIN RIPE APNIC LACNIC AFRINIC
Inspect reverse entries

Video – BiDiBLAH footprinting : NetBlocks



Domains

```
playboy.com
casino.playboy.com
playboynet.playboy.com
```

Brute Files

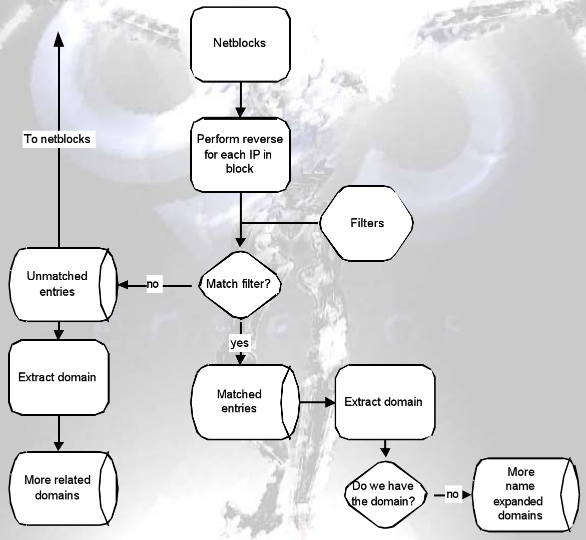
```
colors.bfdns
discworld.bfdns
ecommerce.bfdns
fruit.bfdns
greek.bfdns
internet.bfdns
languages.bfdns
lotr.bfdns
music.bfdns
mythology.bfdns
names.bfdns
planets.bfdns
trees.bfdns
```

☑ Preserve

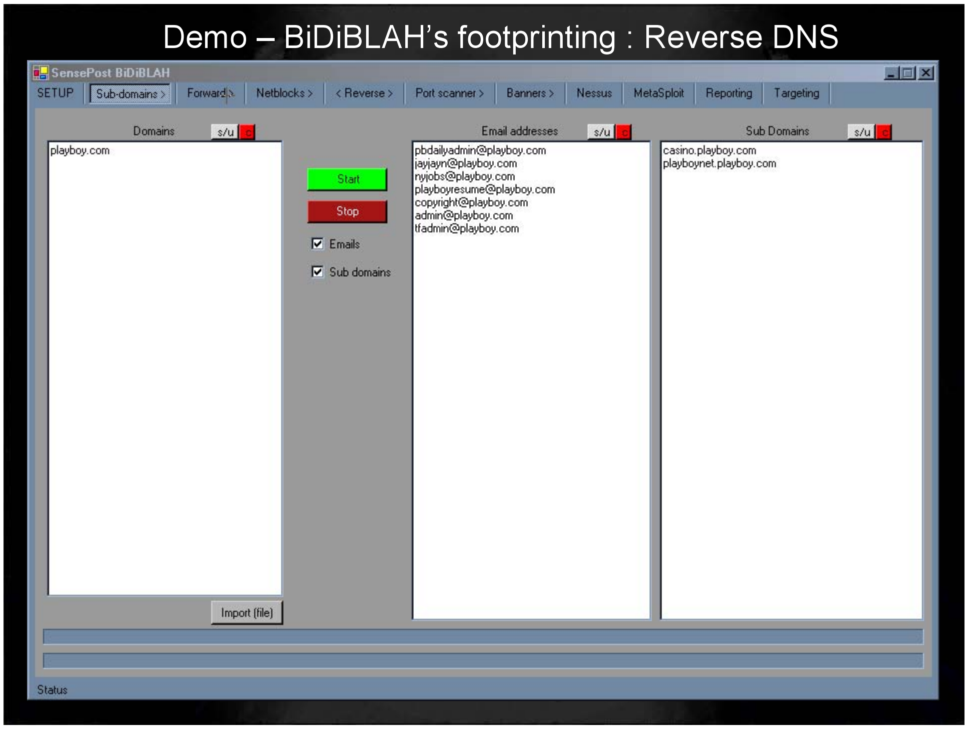
Results (domain,DNSname,IP,method)

```
playboy.com,playboynet.playboy.com,216.163.137.5,gfl
playboy.com,tiffanyfallon.playboy.com,216.163.137.21,gfl
playboy.com,50tour.playboy.com,216.163.136.22,gfl
playboy.com,sportsbook.playboy.com,195.244.204.105,gfl
playboy.com,sportsbook.playboy.com,195.244.204.101,gfl
playboy.com,sportsbook.playboy.com,195.244.204.102,gfl
playboy.com,sportsbook.playboy.com,195.244.204.103,gfl
playboy.com,sportsbook.playboy.com,195.244.204.104,gfl
playboy.com,www.casino.playboy.com,195.244.204.84,gfl
playboy.com,store.playboy.com,209.247.228.205,gfl
playboy.com,secure2.playboy.com,216.163.137.1,gfl
playboy.com,espanol.playboynet.playboy.com,216.163.137.20,gfl
playboy.com,cyber.playboy.com,216.163.137.4,gfl
playboy.com,mirrors.playboy.com,216.163.142.135,gfl
playboy.com,boards.playboy.com,216.163.136.22,gfl
playboy.com,mx.la.playboy.com,216.163.128.15,mx
playboy.com,mx.chi.playboy.com,216.163.143.4,mx
playboy.com,ns21.customer.level3.net,209.244.5.84,ns
playboy.com,ns29.customer.level3.net,209.244.5.212,ns
playboy.com,ns1-chi.playboy.com,209.247.228.135,ns
playboy.com,ns2-chi.playboy.com,64.202.105.36,ns
playboy.com,ns15.customer.level3.net,209.244.4.244,ns
playboy.com,playboy.com,216.163.137.3,fl
playboy.com,www.playboy.com,216.163.137.3,fl
playboy.com,ftp.playboy.com,216.163.136.23,fl
playboy.com,content.playboy.com,209.247.228.140,fl
playboy.com,help.playboy.com,216.163.136.22,fl
playboy.com,mailhost.playboy.com,209.247.228.143,fl
playboy.com,news.playboy.com,216.163.136.22,fl
playboy.com,public.playboy.com,216.163.136.28,fl
playboy.com,secure2.playboy.com,216.163.137.1,fl
playboy.com,portal.playboy.com,216.163.136.22,fl
playboy.com,PICS.playboy.com,216.163.136.22,fl
casino.playboy.com,casino.playboy.com,195.244.204.84,fl
casino.playboy.com,www.casino.playboy.com,195.244.204.84,fl
playboynet.playboy.com,playboynet.playboy.com,216.163.137.5,fl
```

Methodology: Footprint: Reverse DNS



Demo – BiDiBLAH's footprinting : Reverse DNS



☑ Emails

☑ Sub domains

Domains:

```
playboy.com
```

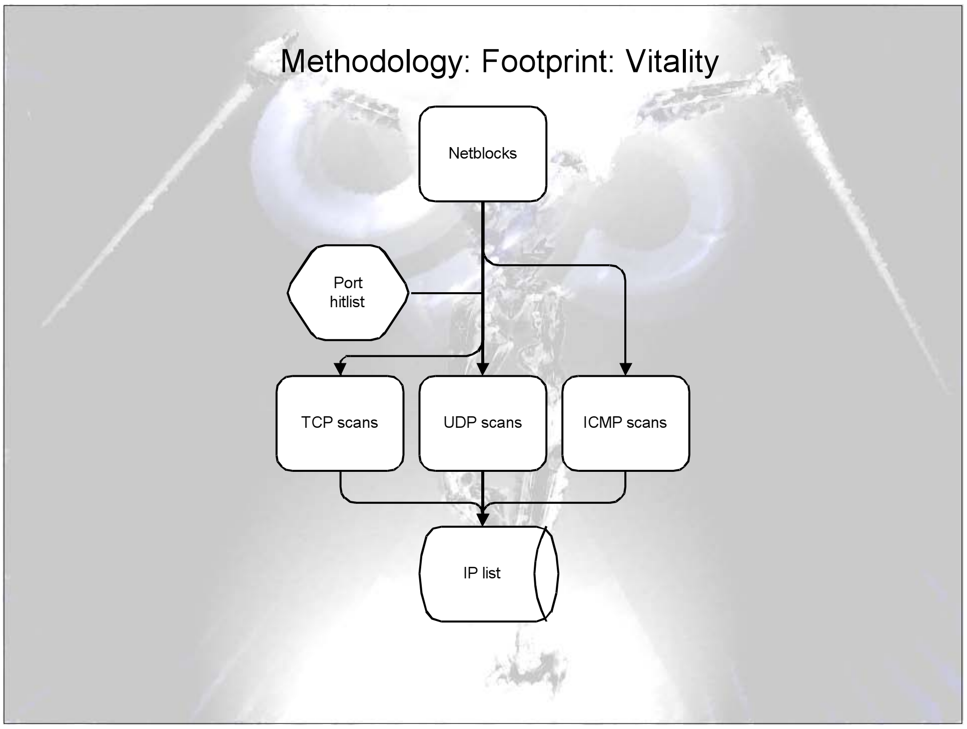
Email addresses:

```
pbdailyadmin@playboy.com
jayjayn@playboy.com
nyjobs@playboy.com
playboyresume@playboy.com
copyright@playboy.com
admin@playboy.com
tfadmin@playboy.com
```

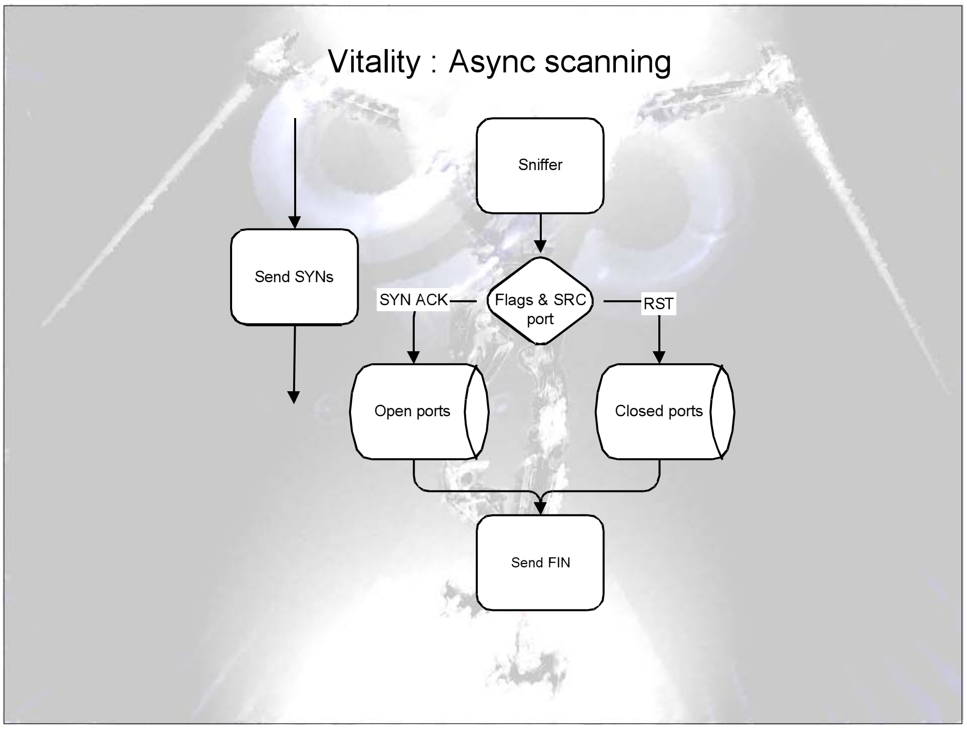
Sub Domains:

```
casino.playboy.com
playboynet.playboy.com
```

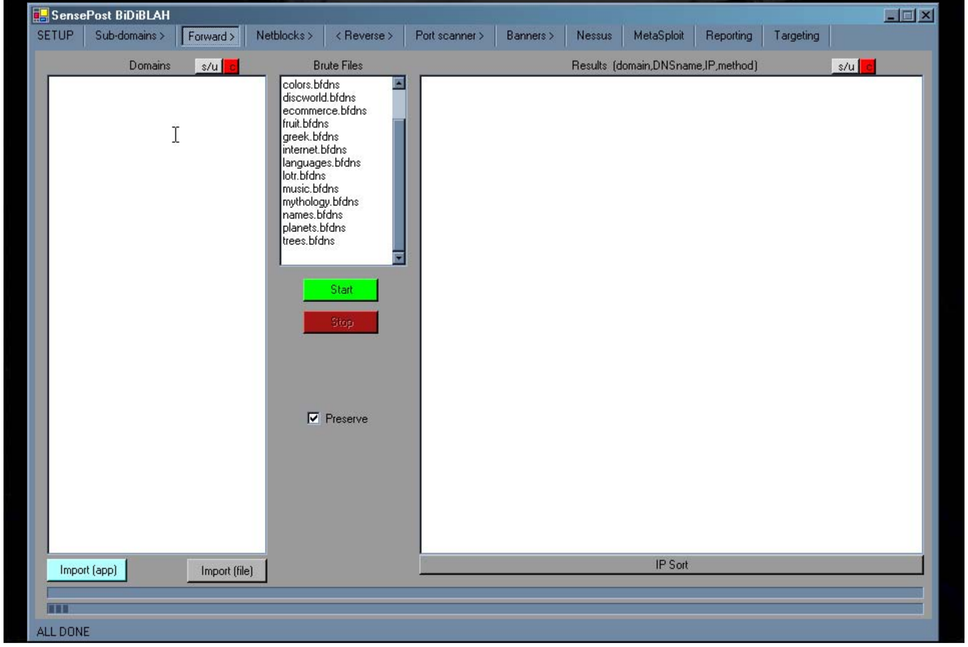
Methodology: Footprint: Vitality



Vitality : Async scanning



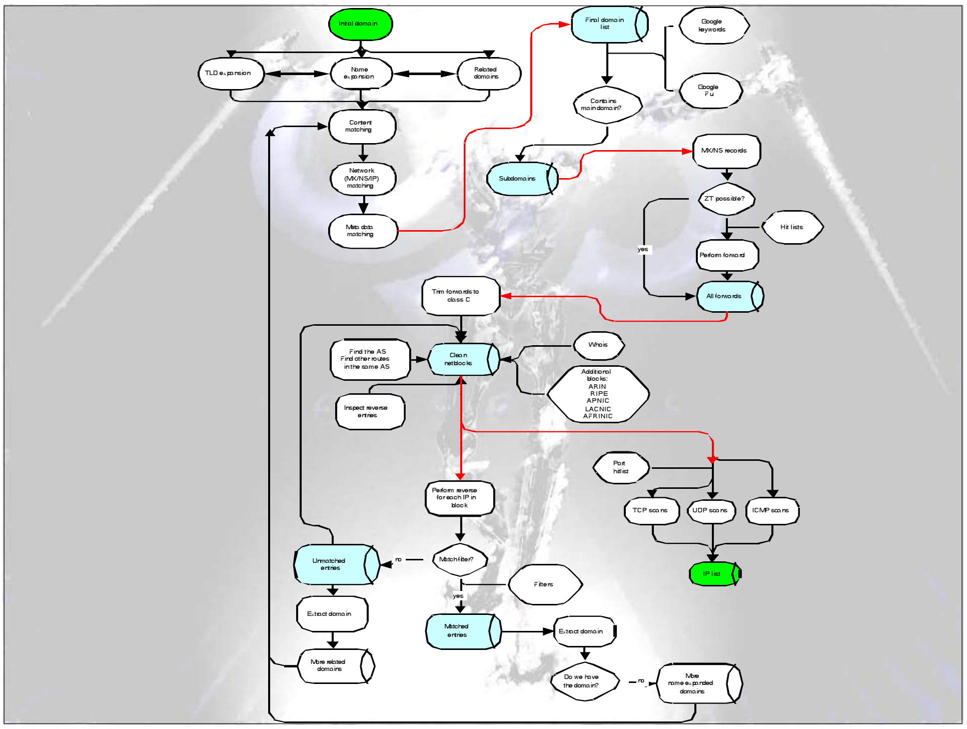
Video - BiDiBLAH – Vitality (SensePost network)

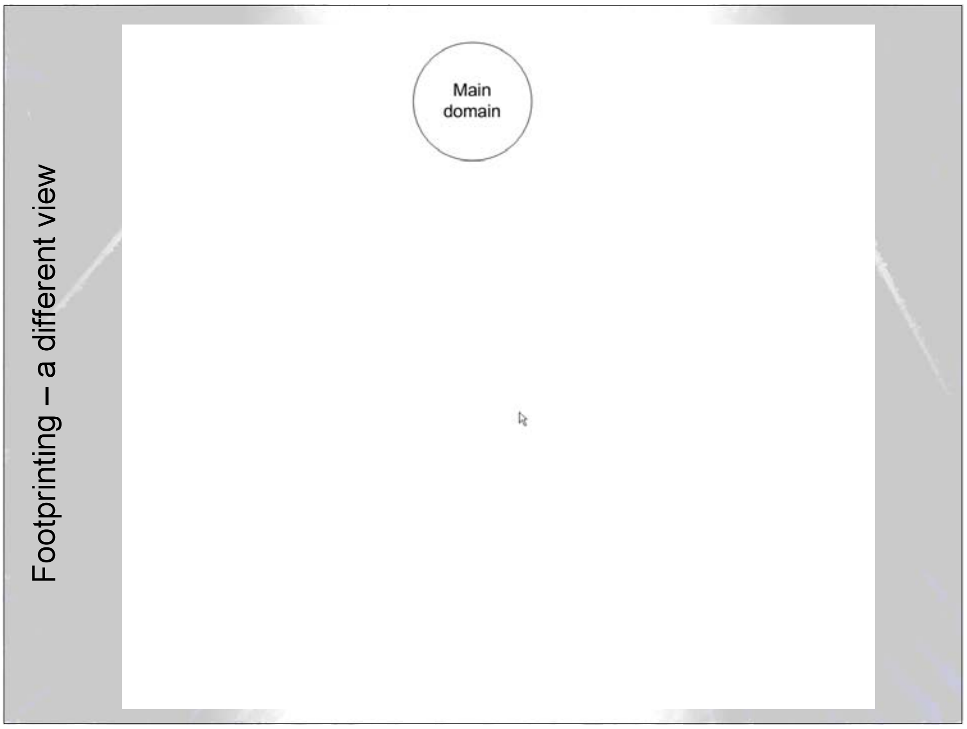


colors.bfdns
discworld.bfdns
ecommerce.bfdns
fruit.bfdns
greek.bfdns
internet.bfdns
languages.bfdns
lotr.bfdns
music.bfdns
mythology.bfdns
names.bfdns
planets.bfdns
trees.bfdns

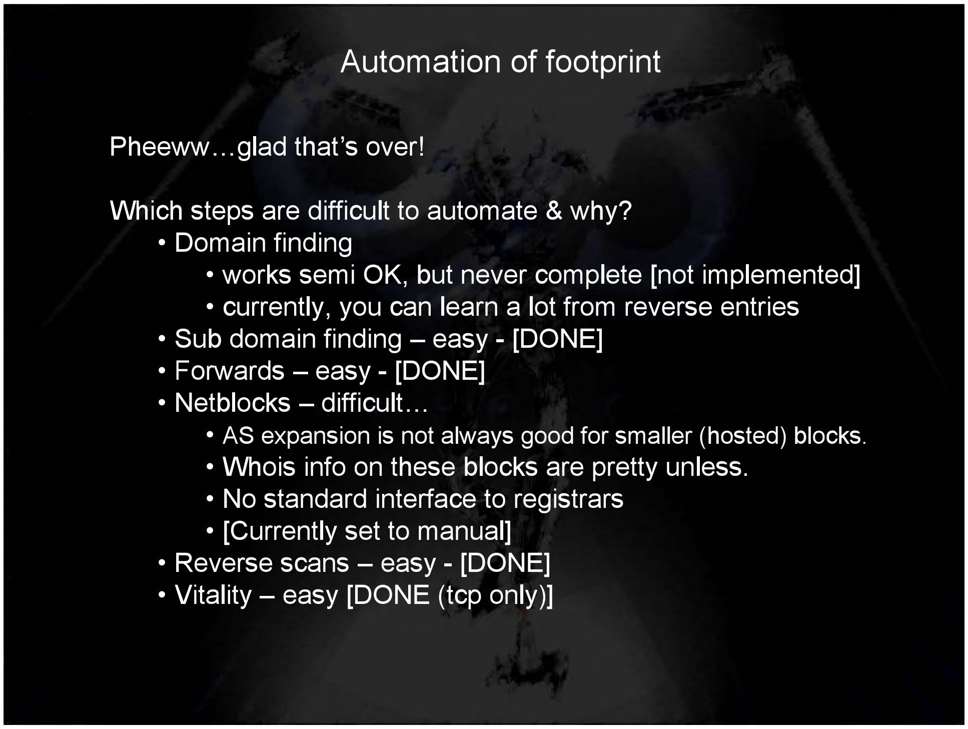
☑ Preserve

ALL DONE





Footprinting – a different view

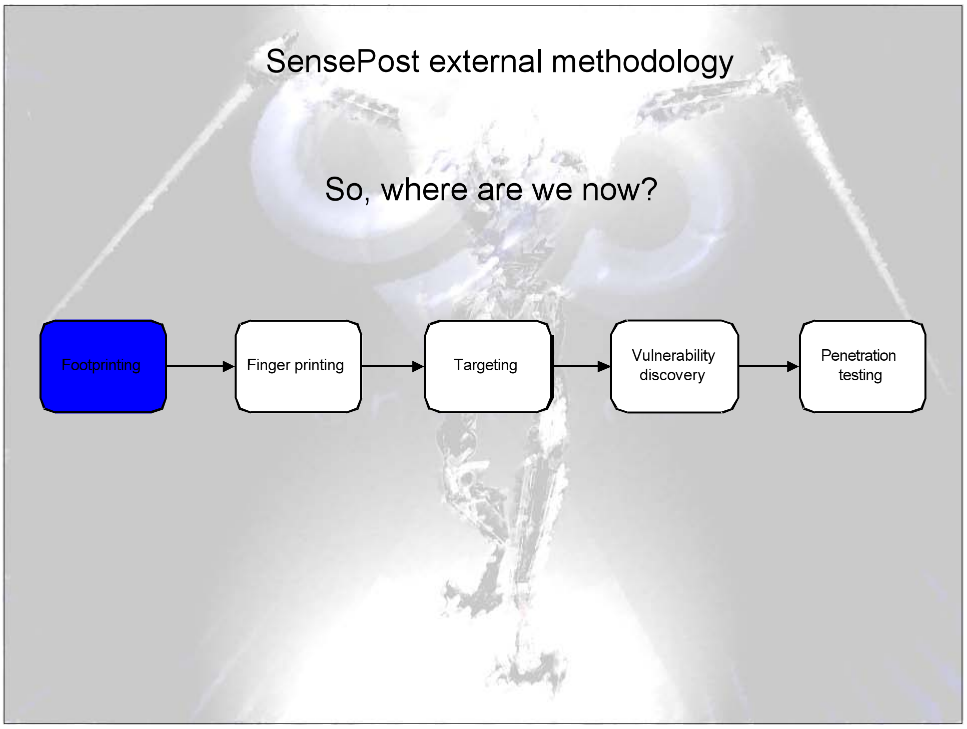


Automation of footprint

Pheeww…glad that's over!

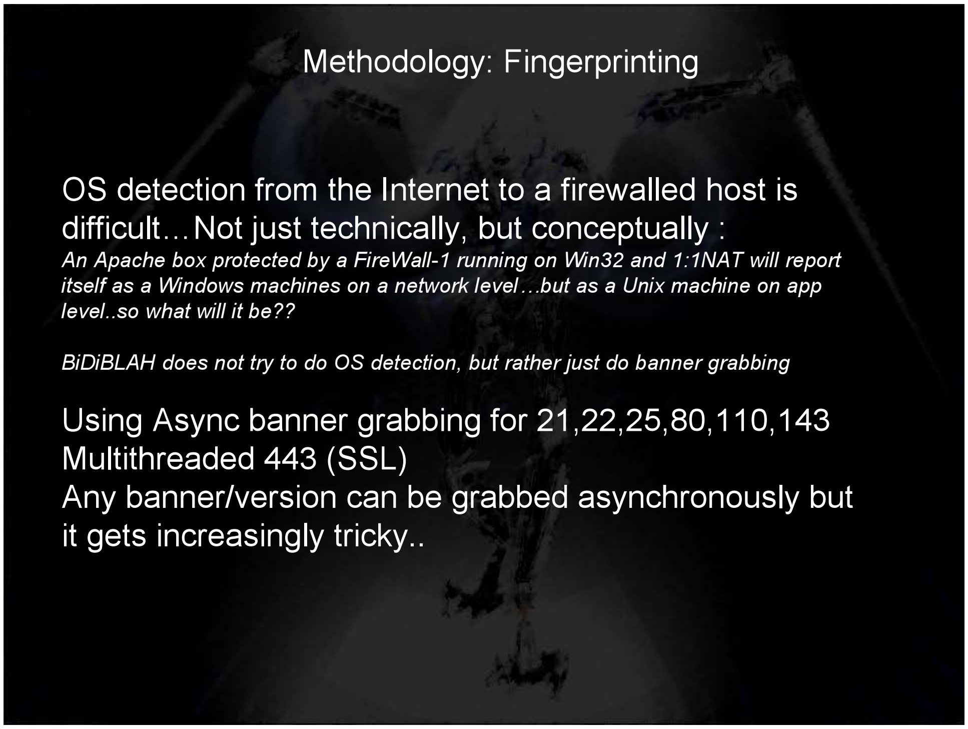
Which steps are difficult to automate & why?

- Domain finding
  - works semi OK, but never complete [not implemented]
  - currently, you can learn a lot from reverse entries
- Sub domain finding – easy - [DONE]
- Forwards – easy - [DONE]
- Netblocks – difficult…
  - AS expansion is not always good for smaller (hosted) blocks.
  - Whois info on these blocks are pretty unless.
  - No standard interface to registrars
  - [Currently set to manual]
- Reverse scans – easy - [DONE]
- Vitality – easy [DONE (tcp only)]



SensePost external methodology

So, where are we now?



Methodology: Fingerprinting

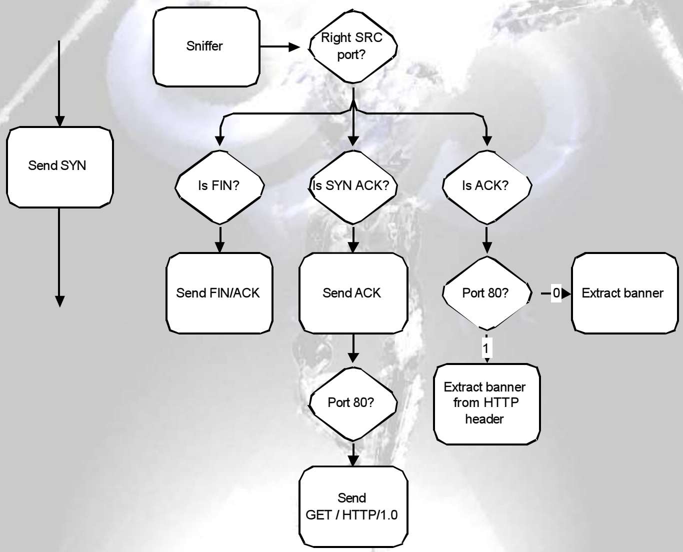
OS detection from the Internet to a firewalled host is difficult…Not just technically, but conceptually :

An Apache box protected by a FireWall-1 running on Win32 and 1:1NAT will report itself as a Windows machines on a network level…but as a Unix machine on app level..so what will it be??

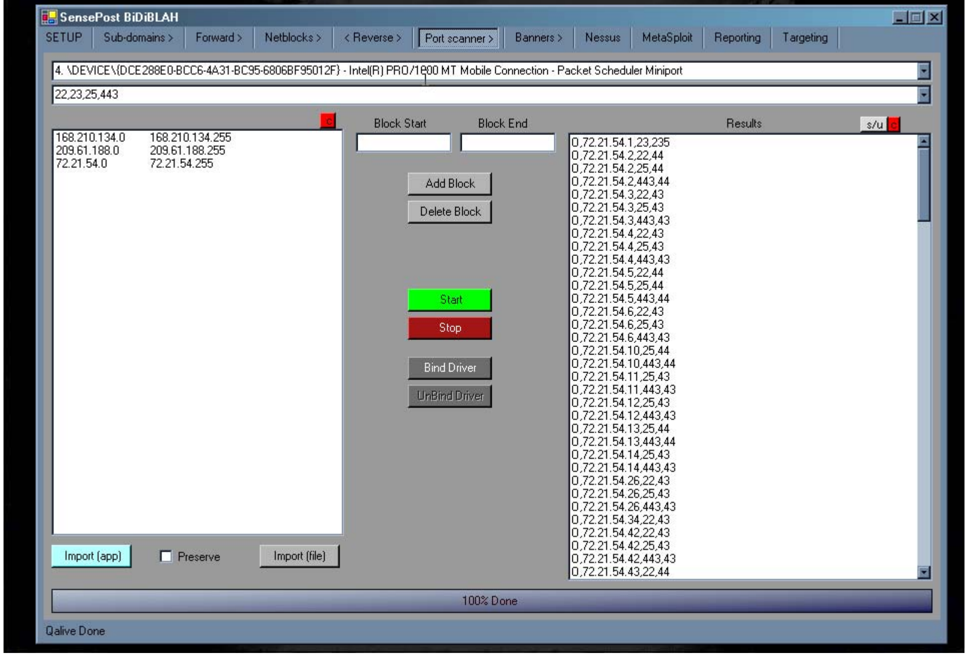
BiDiBLAH does not try to do OS detection, but rather just do banner grabbing

Using Async banner grabbing for 21,22,25,80,110,143
Multithreaded 443 (SSL)
Any banner/version can be grabbed asynchronously but it gets increasingly tricky..

Async banner grabbing – the process



Video - BiDiBLAH: Async banner grabbing



4. \DEVICE\{DCE288E0-BCC6-4A31-BC95-6806BF95012F} - Intel(R) PRO/1000 MT Mobile Connection - Packet Scheduler Miniport

22,23,25,443

```
168.210.134.0      168.210.134.255
209.61.188.0       209.61.188.255
72.21.54.0         72.21.54.255
```

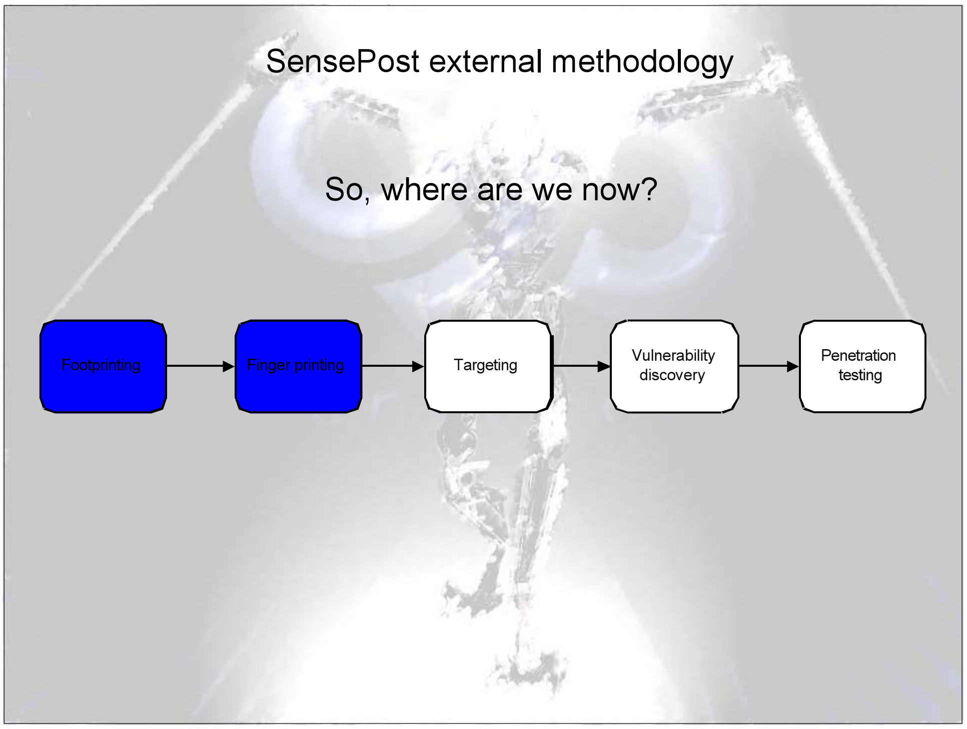
□ Preserve

Results

```
0,72.21.54.1,23,235
0,72.21.54.2,22,44
0,72.21.54.2,25,44
0,72.21.54.2,443,44
0,72.21.54.3,22,43
0,72.21.54.3,25,43
0,72.21.54.3,443,43
0,72.21.54.4,22,43
0,72.21.54.4,25,43
0,72.21.54.4,443,43
0,72.21.54.5,22,44
0,72.21.54.5,25,44
0,72.21.54.5,443,44
0,72.21.54.6,22,43
0,72.21.54.6,25,43
0,72.21.54.6,443,43
0,72.21.54.10,25,44
0,72.21.54.10,443,44
0,72.21.54.11,25,43
0,72.21.54.11,443,43
0,72.21.54.12,25,43
0,72.21.54.12,443,43
0,72.21.54.13,25,44
0,72.21.54.13,443,44
0,72.21.54.14,25,43
0,72.21.54.14,443,43
0,72.21.54.26,22,43
0,72.21.54.26,25,43
0,72.21.54.26,443,43
0,72.21.54.34,22,43
0,72.21.54.42,22,43
0,72.21.54.42,25,43
0,72.21.54.42,443,43
0,72.21.54.43,22,44
```

100% Done

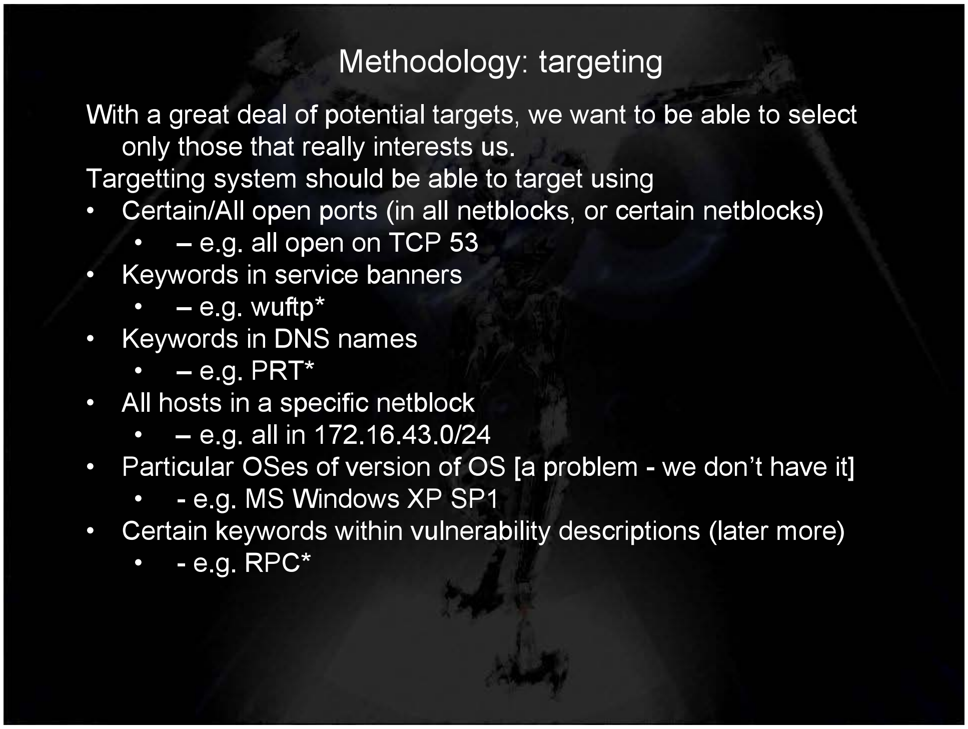
Qalive Done



SensePost external methodology

So, where are we now?

Footprinting → Finger printing → Targeting → Vulnerability discovery → Penetration testing



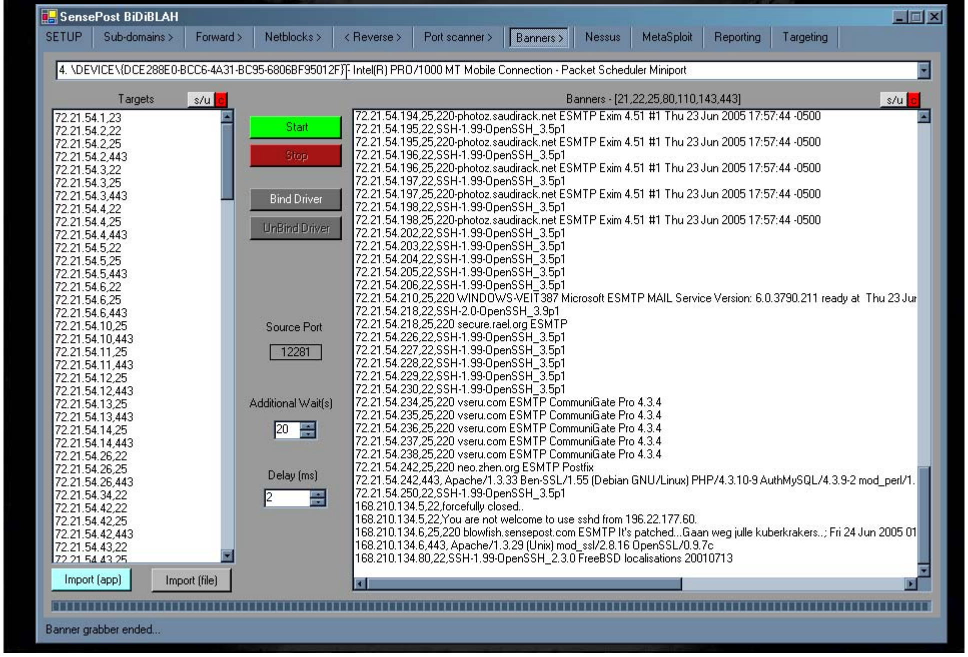
Methodology: targeting

With a great deal of potential targets, we want to be able to select only those that really interests us.

Targetting system should be able to target using

- Certain/All open ports (in all netblocks, or certain netblocks)
  - – e.g. all open on TCP 53
- Keywords in service banners
  - – e.g. wuftp*
- Keywords in DNS names
  - – e.g. PRT*
- All hosts in a specific netblock
  - – e.g. all in 172.16.43.0/24
- Particular OSes of version of OS [a problem - we don’t have it]
  - - e.g. MS Windows XP SP1
- Certain keywords within vulnerability descriptions (later more)
  - - e.g. RPC*

Video – BiDiBLAH - Targeting



4. \DEVICE\{DCE288E0-BCC6-4A31-BC95-6806BF95012F} - Intel(R) PRO/1000 MT Mobile Connection - Packet Scheduler Miniport

Targets

```
72.21.54.1,23
72.21.54.2,22
72.21.54.2,25
72.21.54.2,443
72.21.54.3,22
72.21.54.3,25
72.21.54.3,443
72.21.54.4,22
72.21.54.4,25
72.21.54.4,443
72.21.54.5,22
72.21.54.5,25
72.21.54.5,443
72.21.54.6,22
72.21.54.6,25
72.21.54.6,443
72.21.54.10,25
72.21.54.10,443
72.21.54.11,25
72.21.54.11,443
72.21.54.12,25
72.21.54.12,443
72.21.54.13,25
72.21.54.13,443
72.21.54.14,25
72.21.54.14,443
72.21.54.26,22
72.21.54.26,25
72.21.54.26,443
72.21.54.34,22
72.21.54.42,22
72.21.54.42,25
72.21.54.42,443
72.21.54.43,22
72.21.54.43,25
```

Source Port: 12281

Additional Wait(s): 20

Delay (ms): 2

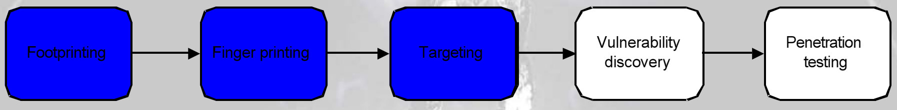
Banners - [21,22,25,80,110,143,443]

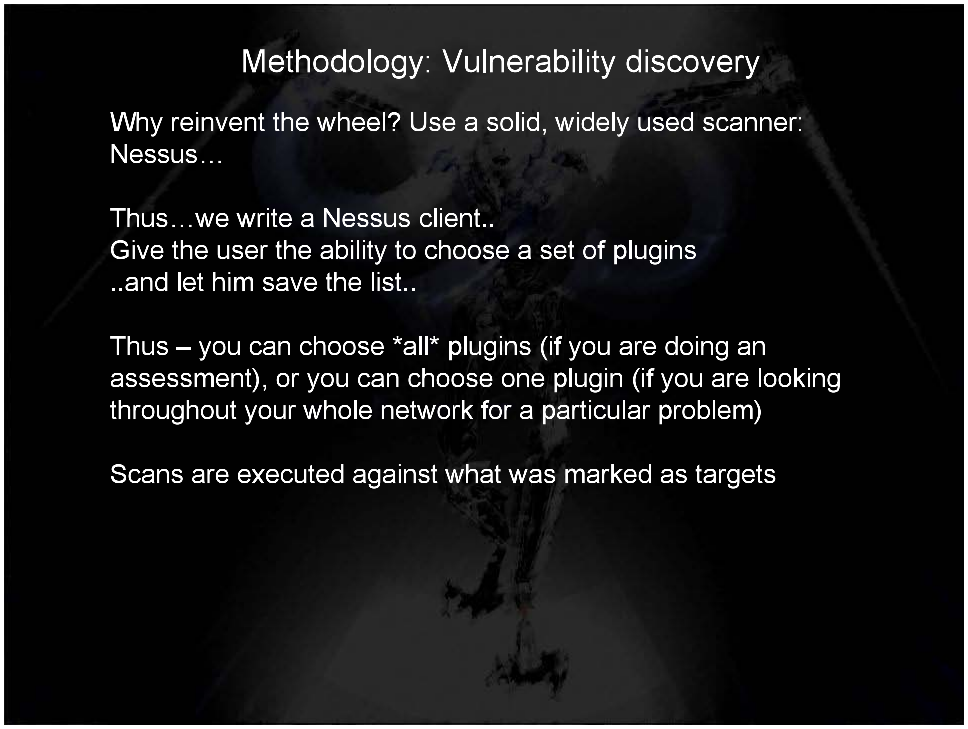
```
72.21.54.194,25,220-photoz.saudirack.net ESMTP Exim 4.51 #1 Thu 23 Jun 2005 17:57:44 -0500
72.21.54.195,22,SSH-1.99-OpenSSH_3.5p1
72.21.54.195,25,220-photoz.saudirack.net ESMTP Exim 4.51 #1 Thu 23 Jun 2005 17:57:44 -0500
72.21.54.196,22,SSH-1.99-OpenSSH_3.5p1
72.21.54.196,25,220-photoz.saudirack.net ESMTP Exim 4.51 #1 Thu 23 Jun 2005 17:57:44 -0500
72.21.54.197,22,SSH-1.99-OpenSSH_3.5p1
72.21.54.197,25,220-photoz.saudirack.net ESMTP Exim 4.51 #1 Thu 23 Jun 2005 17:57:44 -0500
72.21.54.198,22,SSH-1.99-OpenSSH_3.5p1
72.21.54.198,25,220-photoz.saudirack.net ESMTP Exim 4.51 #1 Thu 23 Jun 2005 17:57:44 -0500
72.21.54.202,22,SSH-1.99-OpenSSH_3.5p1
72.21.54.203,22,SSH-1.99-OpenSSH_3.5p1
72.21.54.204,22,SSH-1.99-OpenSSH_3.5p1
72.21.54.205,22,SSH-1.99-OpenSSH_3.5p1
72.21.54.206,22,SSH-1.99-OpenSSH_3.5p1
72.21.54.210,25,220 WINDOWS-VEIT387 Microsoft ESMTP MAIL Service Version: 6.0.3790.211 ready at  Thu 23 Jur
72.21.54.218,22,SSH-2.0-OpenSSH_3.9p1
72.21.54.218,25,220 secure.rael.org ESMTP
72.21.54.226,22,SSH-1.99-OpenSSH_3.5p1
72.21.54.227,22,SSH-1.99-OpenSSH_3.5p1
72.21.54.228,22,SSH-1.99-OpenSSH_3.5p1
72.21.54.229,22,SSH-1.99-OpenSSH_3.5p1
72.21.54.230,22,SSH-1.99-OpenSSH_3.5p1
72.21.54.234,25,220 vseru.com ESMTP CommuniGate Pro 4.3.4
72.21.54.235,25,220 vseru.com ESMTP CommuniGate Pro 4.3.4
72.21.54.236,25,220 vseru.com ESMTP CommuniGate Pro 4.3.4
72.21.54.237,25,220 vseru.com ESMTP CommuniGate Pro 4.3.4
72.21.54.238,25,220 vseru.com ESMTP CommuniGate Pro 4.3.4
72.21.54.242,25,220 neo.zhen.org ESMTP Postfix
72.21.54.242,443, Apache/1.3.33 Ben-SSL/1.55 (Debian GNU/Linux) PHP/4.3.10-9 AuthMySQL/4.3.9-2 mod_perl/1.
72.21.54.250,22,SSH-1.99-OpenSSH_3.5p1
168.210.134.5,22,forcefully closed..
168.210.134.5,22,You are not welcome to use sshd from 196.22.177.60.
168.210.134.6,25,220 blowfish.sensepost.com ESMTP It's patched...Gaan weg julle kuberkrakers..; Fri 24 Jun 2005 01
168.210.134.6,443, Apache/1.3.29 (Unix) mod_ssl/2.8.16 OpenSSL/0.9.7c
168.210.134.80,22,SSH-1.99-OpenSSH_2.3.0 FreeBSD localisations 20010713
```

Banner grabber ended...

SensePost external methodology

So, where are we now?





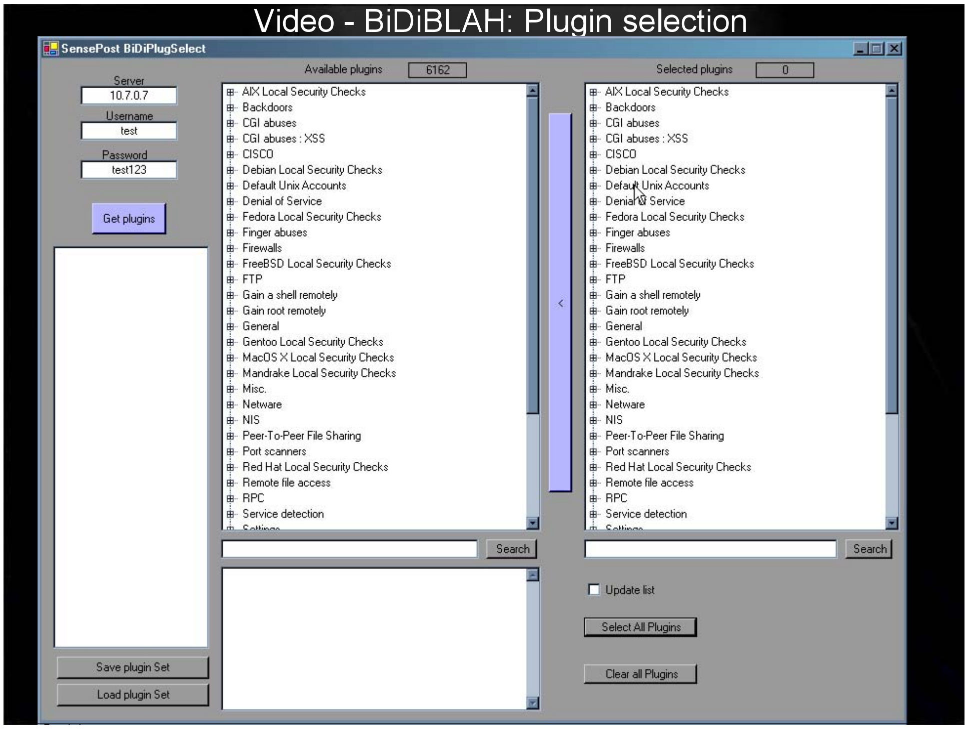
Methodology: Vulnerability discovery

Why reinvent the wheel? Use a solid, widely used scanner: Nessus…

Thus…we write a Nessus client..
Give the user the ability to choose a set of plugins
..and let him save the list..

Thus – you can choose *all* plugins (if you are doing an assessment), or you can choose one plugin (if you are looking throughout your whole network for a particular problem)

Scans are executed against what was marked as targets



Video - BiDiBLAH: Plugin selection

SensePost BiDiPlugSelect

Server: 10.7.0.7
Username: test
Password: test123

Available plugins: 6162

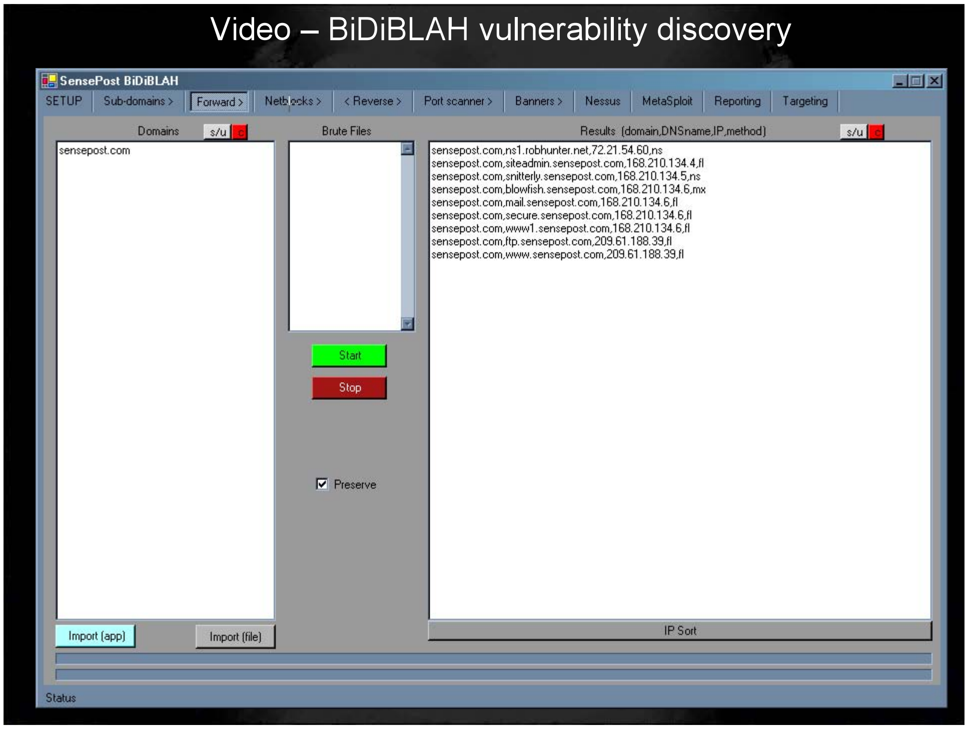
- AIX Local Security Checks
- Backdoors
- CGI abuses
- CGI abuses : XSS
- CISCO
- Debian Local Security Checks
- Default Unix Accounts
- Denial of Service
- Fedora Local Security Checks
- Finger abuses
- Firewalls
- FreeBSD Local Security Checks
- FTP
- Gain a shell remotely
- Gain root remotely
- General
- Gentoo Local Security Checks
- MacOS X Local Security Checks
- Mandrake Local Security Checks
- Misc.
- Netware
- NIS
- Peer-To-Peer File Sharing
- Port scanners
- Red Hat Local Security Checks
- Remote file access
- RPC
- Service detection

Selected plugins: 0

- AIX Local Security Checks
- Backdoors
- CGI abuses
- CGI abuses : XSS
- CISCO
- Debian Local Security Checks
- Default Unix Accounts
- Denial of Service
- Fedora Local Security Checks
- Finger abuses
- Firewalls
- FreeBSD Local Security Checks
- FTP
- Gain a shell remotely
- Gain root remotely
- General
- Gentoo Local Security Checks
- MacOS X Local Security Checks
- Mandrake Local Security Checks
- Misc.
- Netware
- NIS
- Peer-To-Peer File Sharing
- Port scanners
- Red Hat Local Security Checks
- Remote file access
- RPC
- Service detection

☐ Update list

Video – BiDiBLAH vulnerability discovery



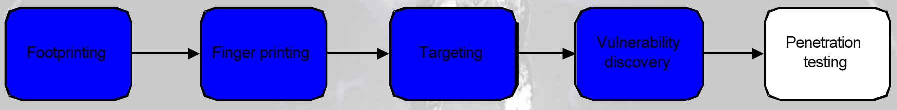
Domains: sensepost.com

☑ Preserve

```
sensepost.com,ns1.robhunter.net,72.21.54.60,ns
sensepost.com,siteadmin.sensepost.com,168.210.134.4,fl
sensepost.com,snitterly.sensepost.com,168.210.134.5,ns
sensepost.com,blowfish.sensepost.com,168.210.134.6,mx
sensepost.com,mail.sensepost.com,168.210.134.6,fl
sensepost.com,secure.sensepost.com,168.210.134.6,fl
sensepost.com,www1.sensepost.com,168.210.134.6,fl
sensepost.com,ftp.sensepost.com,209.61.188.39,fl
sensepost.com,www.sensepost.com,209.61.188.39,fl
```

SensePost external methodology

So, where are we now?



Methodology: Vulnerability exploitation

Why reinvent the wheel? Use a solid, widely used exploitation framework: MetaSploit!

Thus…we write a MetaSploit client..

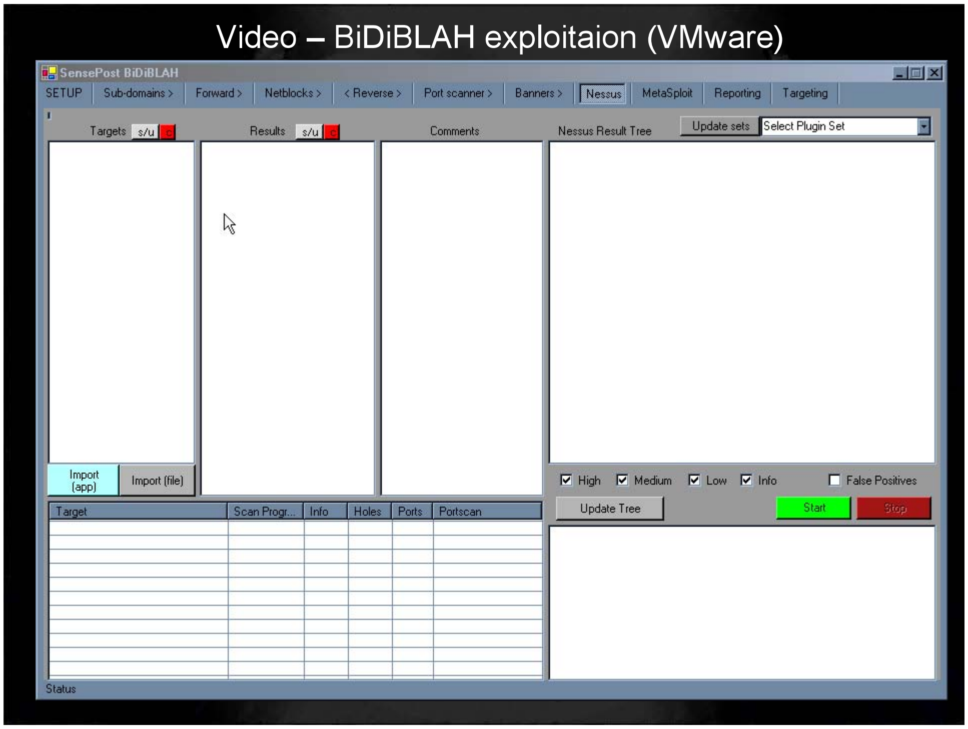
Problem with MetaSploit – its very operating system specific ….and we DON'T HAVE that…

Don't specify target and hope for the best – hopefully it will brute force.

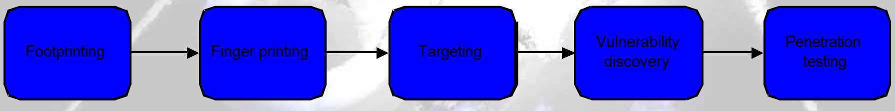
Use Nessus to identify the weakness, MetaSploit to exploit it
Thus … we need a NessusID to MetaSploit sploit name list
We built it (thanks GP), and wrote plugins as needed
Hopefully it can be an attribute of the sploit (looks at HD..)

RHOST, SSL, LHOST – all known to us
RPORT known via Nessus scanner
Let the user choose the playload and additional parameters

Video – BiDiBLAH exploitaion (VMware)



SensePost external methodology



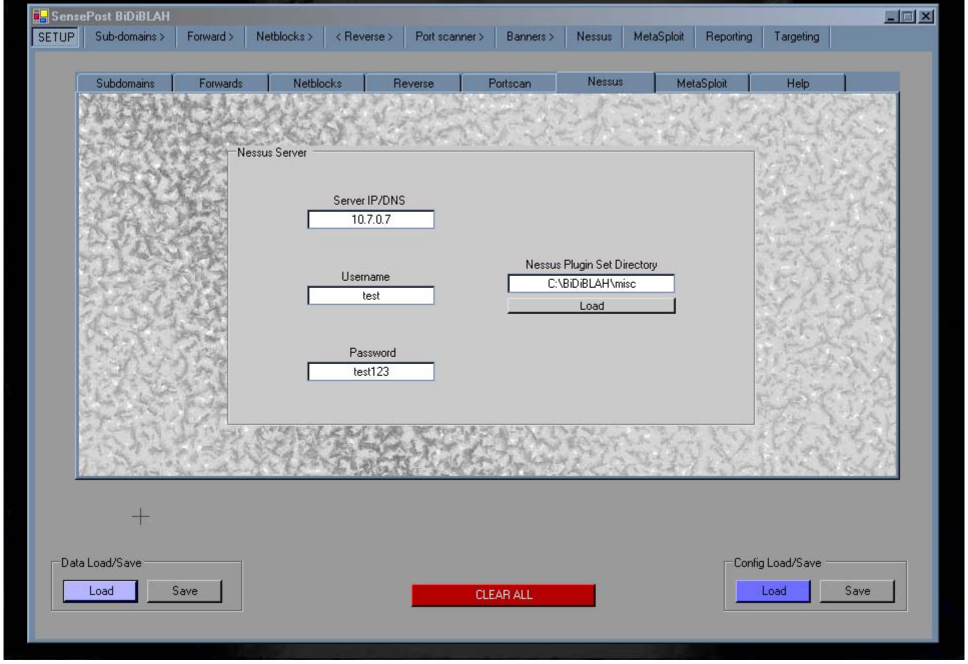
So…we are done?

In a perfect world…yes...

In the real world we have false positives, we have to moderate Nessus results, and we have to write

!=*|||(ing reports!!!

Video: advance targeting and reporting



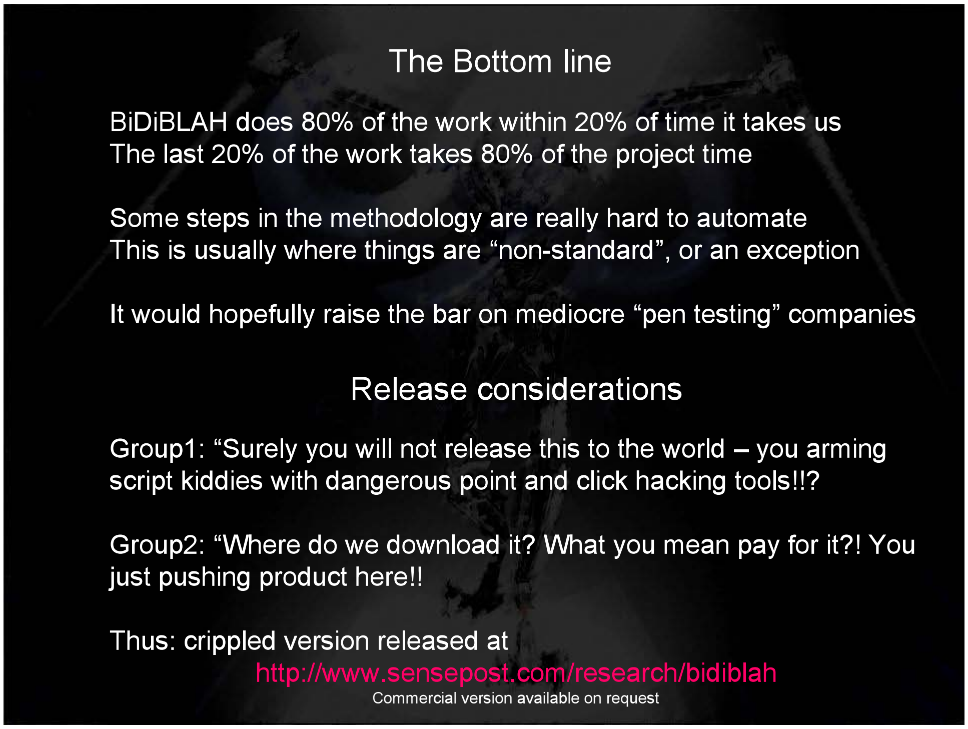
Nessus Server

Server IP/DNS: 10.7.0.7

Username: test

Password: test123

Nessus Plugin Set Directory: C:\BiDiBLAH\misc



The Bottom line

BiDiBLAH does 80% of the work within 20% of time it takes us
The last 20% of the work takes 80% of the project time

Some steps in the methodology are really hard to automate
This is usually where things are "non-standard", or an exception

It would hopefully raise the bar on mediocre "pen testing" companies

Release considerations

Group1: "Surely you will not release this to the world – you arming script kiddies with dangerous point and click hacking tools!!?

Group2: "Where do we download it? What you mean pay for it?! You just pushing product here!!

Thus: crippled version released at
http://www.sensepost.com/research/bidiblah
Commercial version available on request

sensepost
blackhat
2005

EXTRA: E-Or release

Web APPLICATION assessment tool
•http://www.sensepost.com/research/eor