DERBYCON 2012

PENETRATION TESTING FROM A HOT TUB TIME MACHINE

Presented by:

Eric Smith
Chris Gates

ABOUT US

- Senior Partners – LARES Consulting
- Penetration Testers
- Professional Unicorn Hunters
- Mostly trouble makers

- Twitter
- Chris Gates: @carnal0wnage
- Eric Smith: @infosecmafia

- Blog
- carnal0wnage.attackresearch.com

FRIENDSHIP

It doesn't matter what colour you are

DISCLAIMER

- Not releasing 0days, not releasing tools
- Zero exploits will be shown
- Not demoing lab projects that fail IRL
- Security isn’t that sexy
- This is not a demo of MS08-067
- 1 part flashback + 2 parts reminder

MOTIVATION

- We see a lot of dirty/scary/shocking <adjective>
- Corporations are NOT getting better over time
- Penetration testers ARE getting lazier over time
- Basic shit gets you owned, if you don’t test it, others will eventually
- Stop with smoke and mirrors to sell your value. **RESULTS** sell value
- Step away from the scan + exploit mentality

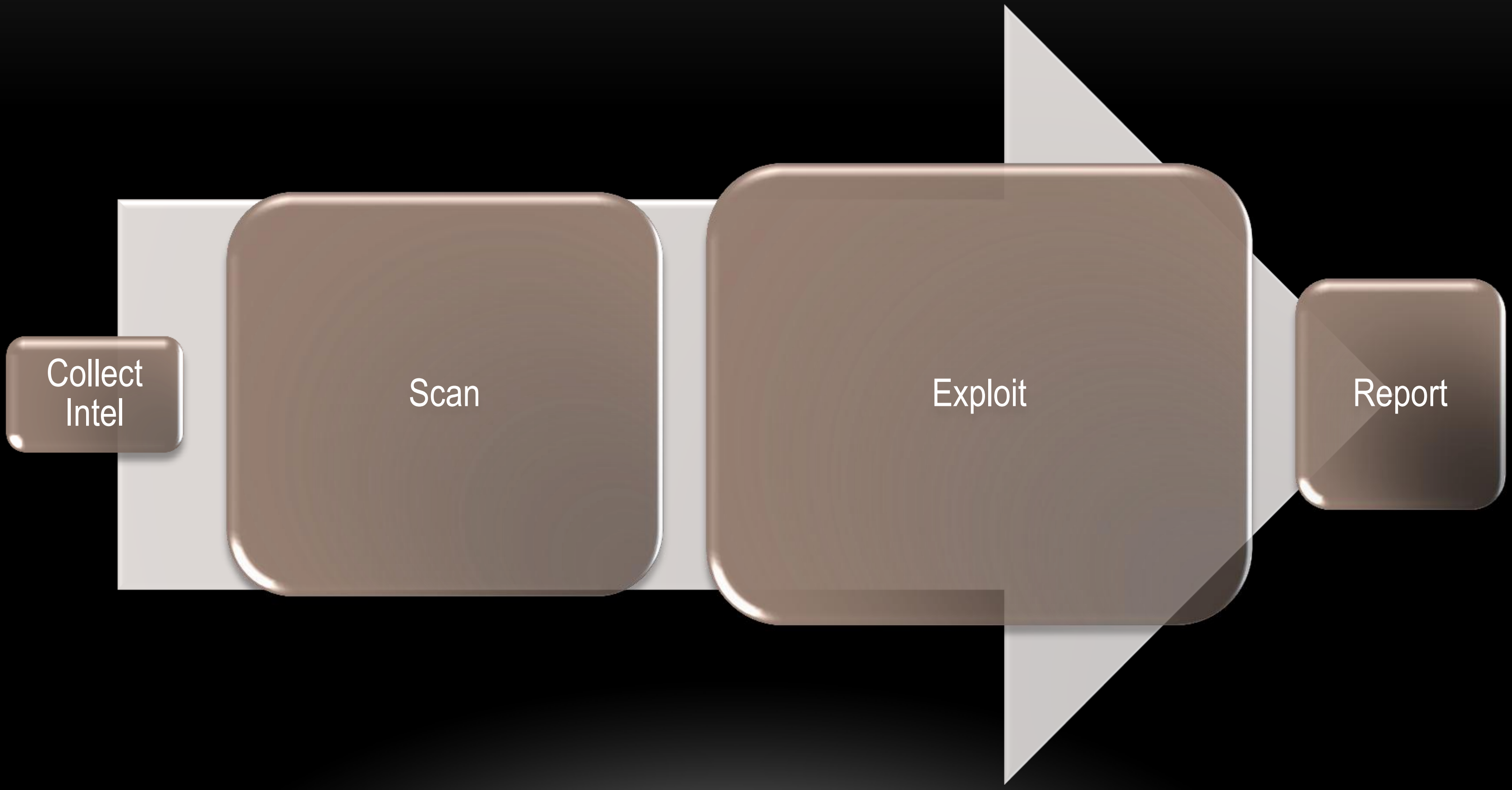
NEWS FLASH: 0-DAYS DON'T MATTER!

- I <3 0day, why?
  - It keeps people on edge!
  - BUT
  - 0days never seem to f* work IRL, well 1 days do - Maybe
  - If its in an exploit framework then AV is blocking it. THAT they are actually good at.
  - If I had a (good) 0day I wouldn't waste it on a pen-test
  - 0days provide ZERO value to your client

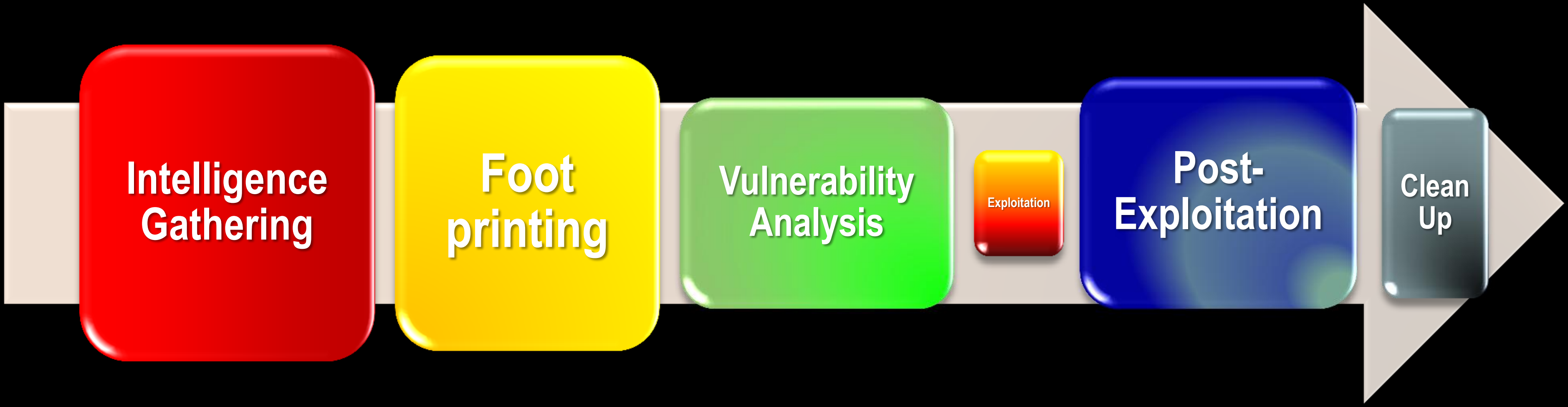
REALITY CHECK

- Good hackers don’t use expensive vulnerability scanners
- Good hackers don’t use automated penetration testing
- Attackers don’t have a scope or timeframes
- Attackers don’t stop after first successful exploit

TODAY’S UGLY METHODOLOGY



THE RIGHT WAY TO DO IT



www.pentest-standard.org

OSINT: OPEN SOURCE INTELLIGENCE GATHERING

- Often excluded from penetration testing
- It’s the easiest way to learn about your target w/o being detected
- Hackers do it, so should you
- Profiling will expedite your chances for success
- Basis to formulate your own attack matrix

OSINT VALUE

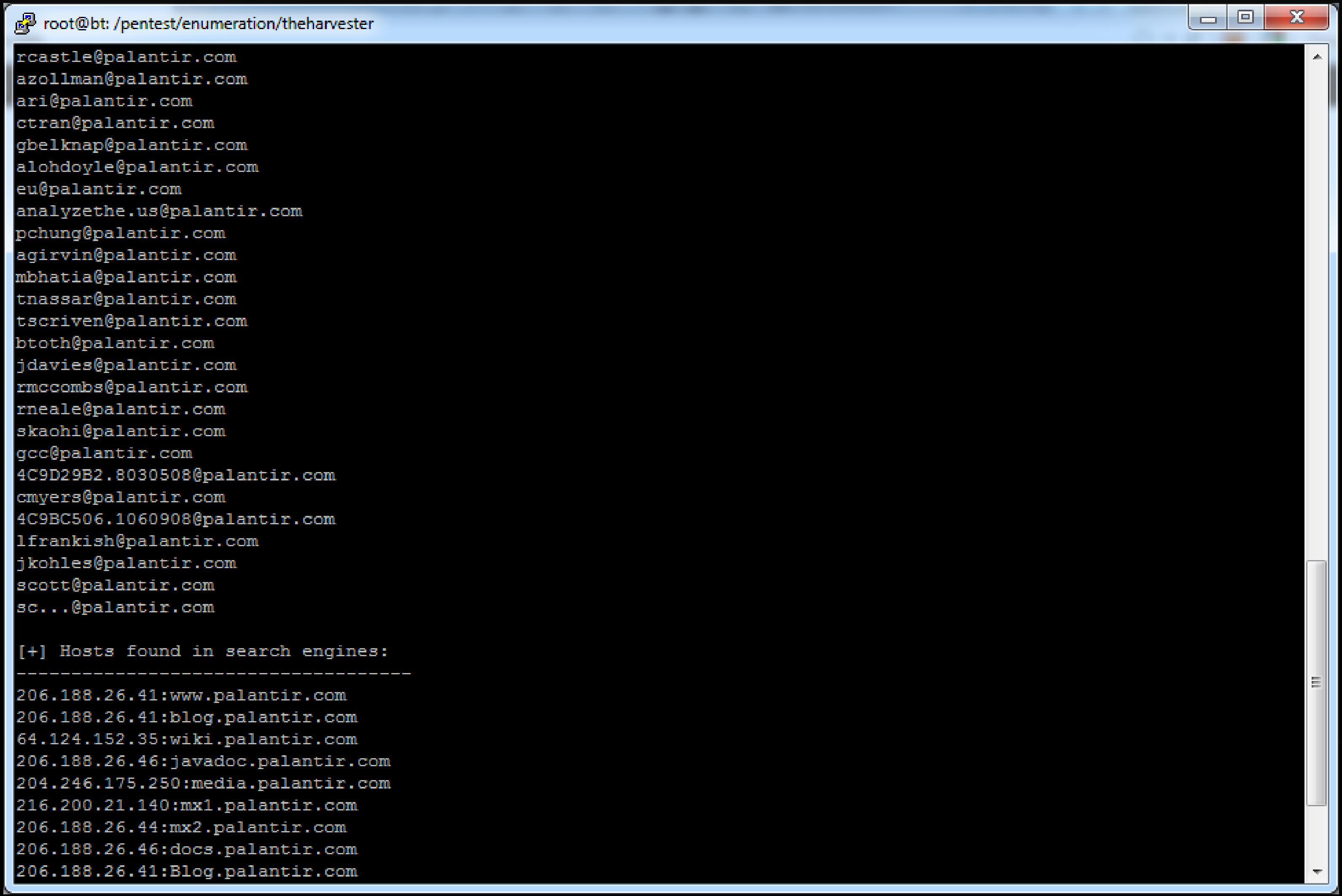
- It’s free!
- Someone/Something else already did most of it for you
- Develop a Process/Methodology == Habit
- Do it EVERY time: *Unicorns* show up occasionally. You can’t take the attitude that “I'll never find/see X”
- Put eyes on EVERYTHING!
- Don't rely on $OSINT-tool to tell you what’s important
- Don’t rely on $scanner to tell you what’s vulnerable

OSINT - EXTERNAL

- Support Tools
  - Harvester, FOCA, Shodan, Maltego, Deep Magic
  - Metasploit Auxiliary Modules
  - Nmap scripts (NSE)
  - Roll your own (ruby, python, bash)
- No substitute for your eyes and brain
  - Is information X important or not?
  - How can it be applied throughout an engagement?
  - What's the value and potential damage of the Intel?

OSINT - EXTERNAL

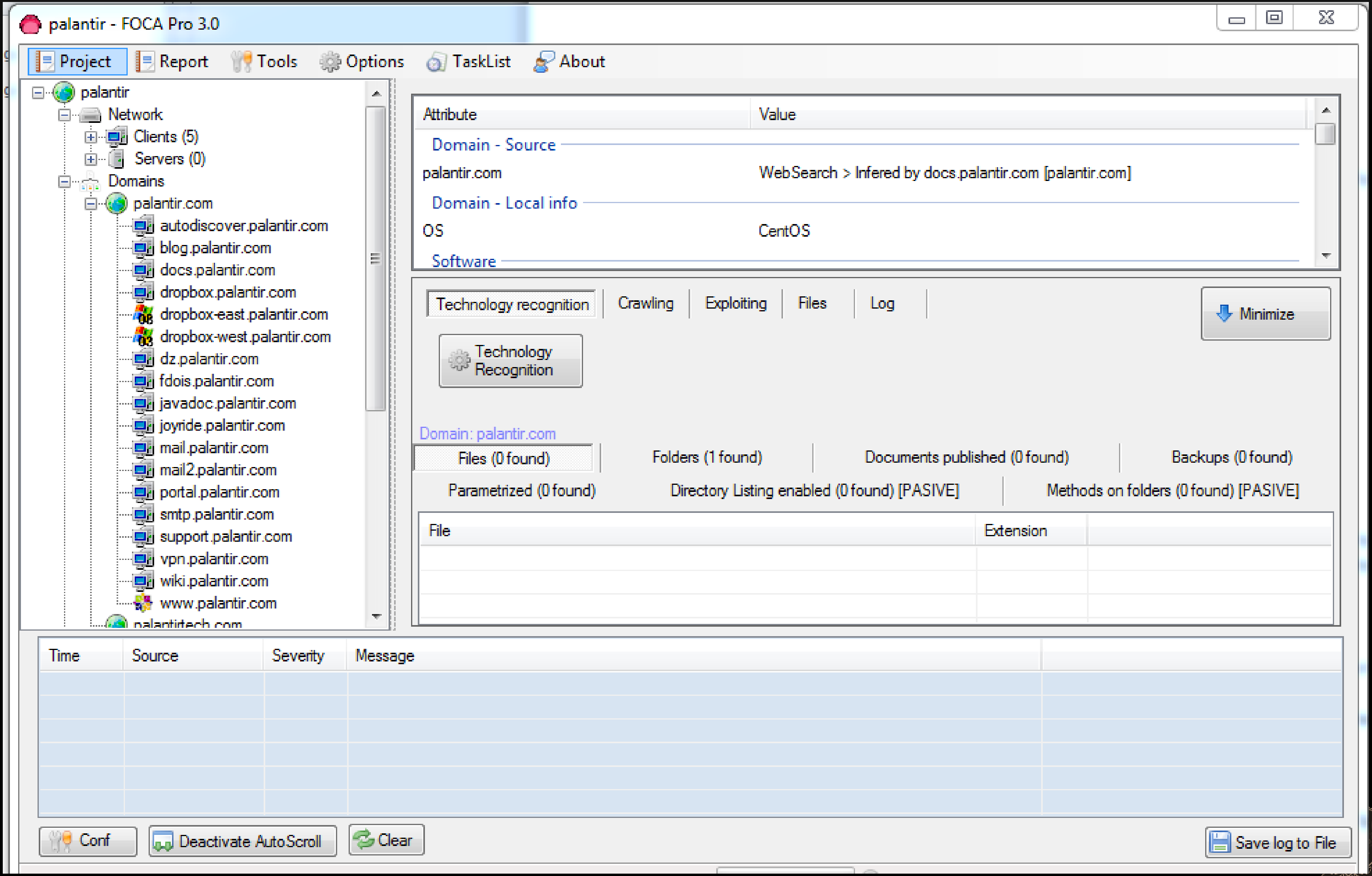
Harvester



```
rcastle@palantir.com
azollman@palantir.com
ari@palantir.com
ctran@palantir.com
gbelknap@palantir.com
alohdoyle@palantir.com
eu@palantir.com
analyzethe.us@palantir.com
pchung@palantir.com
agirvin@palantir.com
mbhatia@palantir.com
tnassar@palantir.com
tscriven@palantir.com
btoth@palantir.com
jdavies@palantir.com
rmccombs@palantir.com
rneale@palantir.com
skaohi@palantir.com
gcc@palantir.com
4C9D29B2.8030508@palantir.com
cmyers@palantir.com
4C9BC506.1060908@palantir.com
lfrankish@palantir.com
jkohles@palantir.com
scott@palantir.com
sc...@palantir.com

[+] Hosts found in search engines:
------------------------------------
206.188.26.41:www.palantir.com
206.188.26.41:blog.palantir.com
64.124.152.35:wiki.palantir.com
206.188.26.46:javadoc.palantir.com
204.246.175.250:media.palantir.com
216.200.21.140:mx1.palantir.com
206.188.26.44:mx2.palantir.com
206.188.26.46:docs.palantir.com
206.188.26.41:Blog.palantir.com
```

OSINT -- EXTERNAL

- FOCA (network)



- palantir
  - Network
    - Clients (5)
    - Servers (0)
  - Domains
    - palantir.com
      - autodiscover.palantir.com
      - blog.palantir.com
      - docs.palantir.com
      - dropbox.palantir.com
      - dropbox-east.palantir.com
      - dropbox-west.palantir.com
      - dz.palantir.com
      - fdois.palantir.com
      - javadoc.palantir.com
      - joyride.palantir.com
      - mail.palantir.com
      - mail2.palantir.com
      - portal.palantir.com
      - smtp.palantir.com
      - support.palantir.com
      - vpn.palantir.com
      - wiki.palantir.com
      - www.palantir.com
    - palantirtech.com

Attribute	Value
Domain - Source	
palantir.com	WebSearch > Infered by docs.palantir.com [palantir.com]
Domain - Local info	
OS	CentOS
Software	

Domain: palantir.com

Files (0 found) | Folders (1 found) | Documents published (0 found) | Backups (0 found)

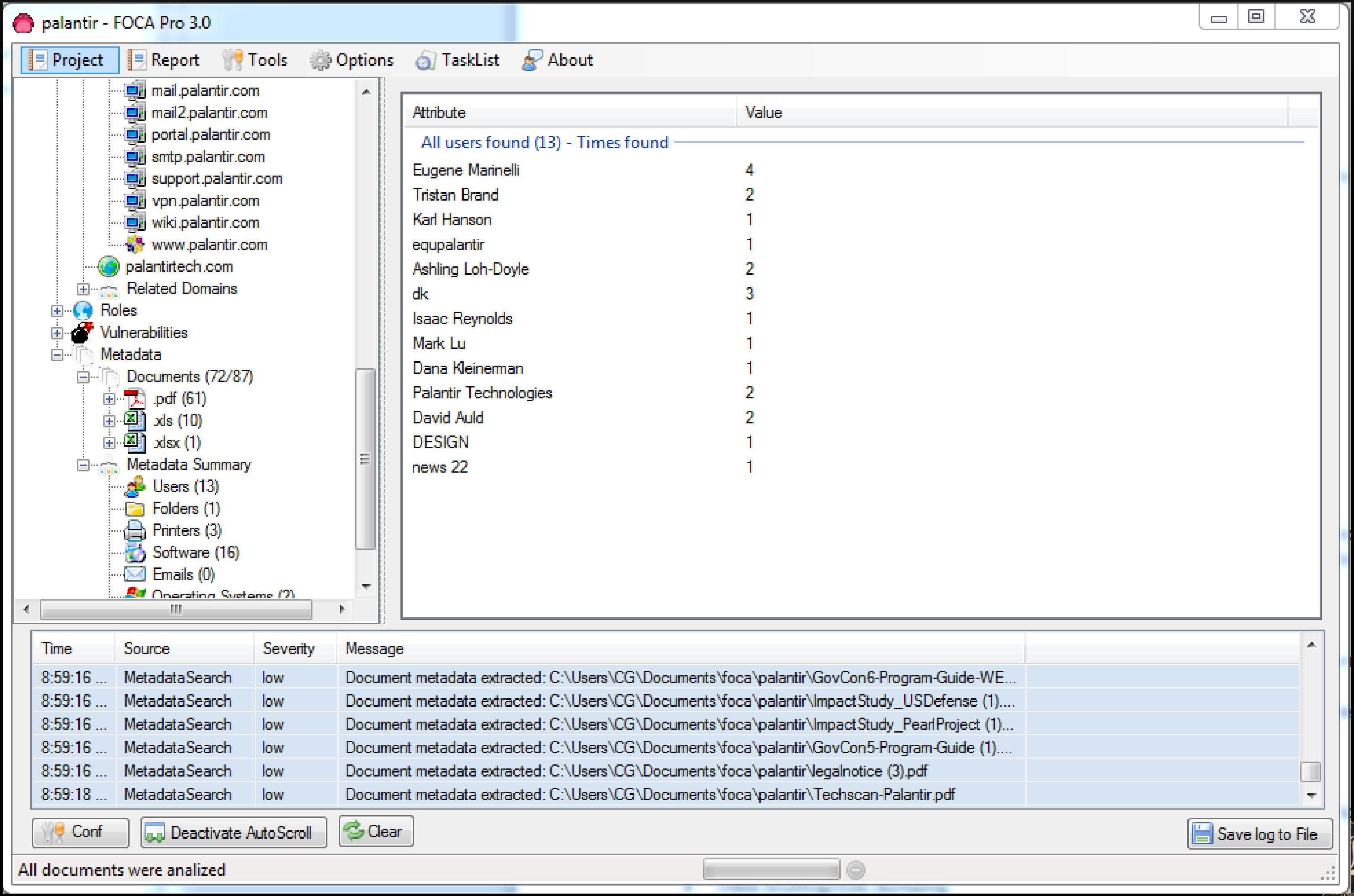
Parametrized (0 found) | Directory Listing enabled (0 found) [PASIVE] | Methods on folders (0 found) [PASIVE]

File	Extension

Time	Source	Severity	Message

OSINT -- EXTERNAL

- FOCA (document metadata)



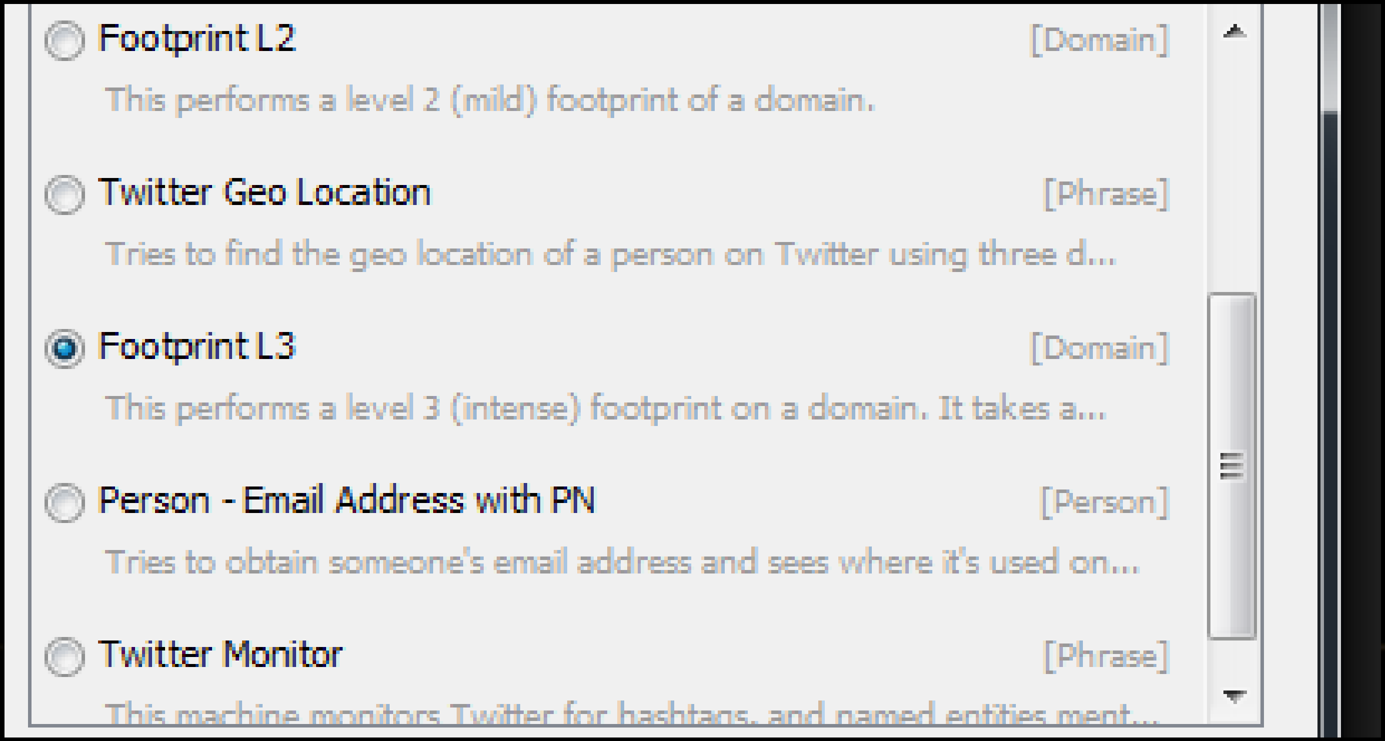
Attribute	Value
All users found (13) - Times found	
Eugene Marinelli	4
Tristan Brand	2
Karl Hanson	1
equpalantir	1
Ashling Loh-Doyle	2
dk	3
Isaac Reynolds	1
Mark Lu	1
Dana Kleinerman	1
Palantir Technologies	2
David Auld	2
DESIGN	1
news 22	1

```
Time        Source          Severity  Message
8:59:16 ... MetadataSearch  low       Document metadata extracted: C:\Users\CG\Documents\foca\palantir\GovCon6-Program-Guide-WE...
8:59:16 ... MetadataSearch  low       Document metadata extracted: C:\Users\CG\Documents\foca\palantir\ImpactStudy_USDefense (1)....
8:59:16 ... MetadataSearch  low       Document metadata extracted: C:\Users\CG\Documents\foca\palantir\ImpactStudy_PearlProject (1)...
8:59:16 ... MetadataSearch  low       Document metadata extracted: C:\Users\CG\Documents\foca\palantir\GovCon5-Program-Guide (1)....
8:59:16 ... MetadataSearch  low       Document metadata extracted: C:\Users\CG\Documents\foca\palantir\legalnotice (3).pdf
8:59:18 ... MetadataSearch  low       Document metadata extracted: C:\Users\CG\Documents\foca\palantir\Techscan-Palantir.pdf
```

All documents were analized

OSINT -- EXTERNAL

- Maltego Radium
  - New addition is "Machines" to automate common tasks
  - Like various levels of foot printing



○ Footprint L2 [Domain]
This performs a level 2 (mild) footprint of a domain.

○ Twitter Geo Location [Phrase]
Tries to find the geo location of a person on Twitter using three d...

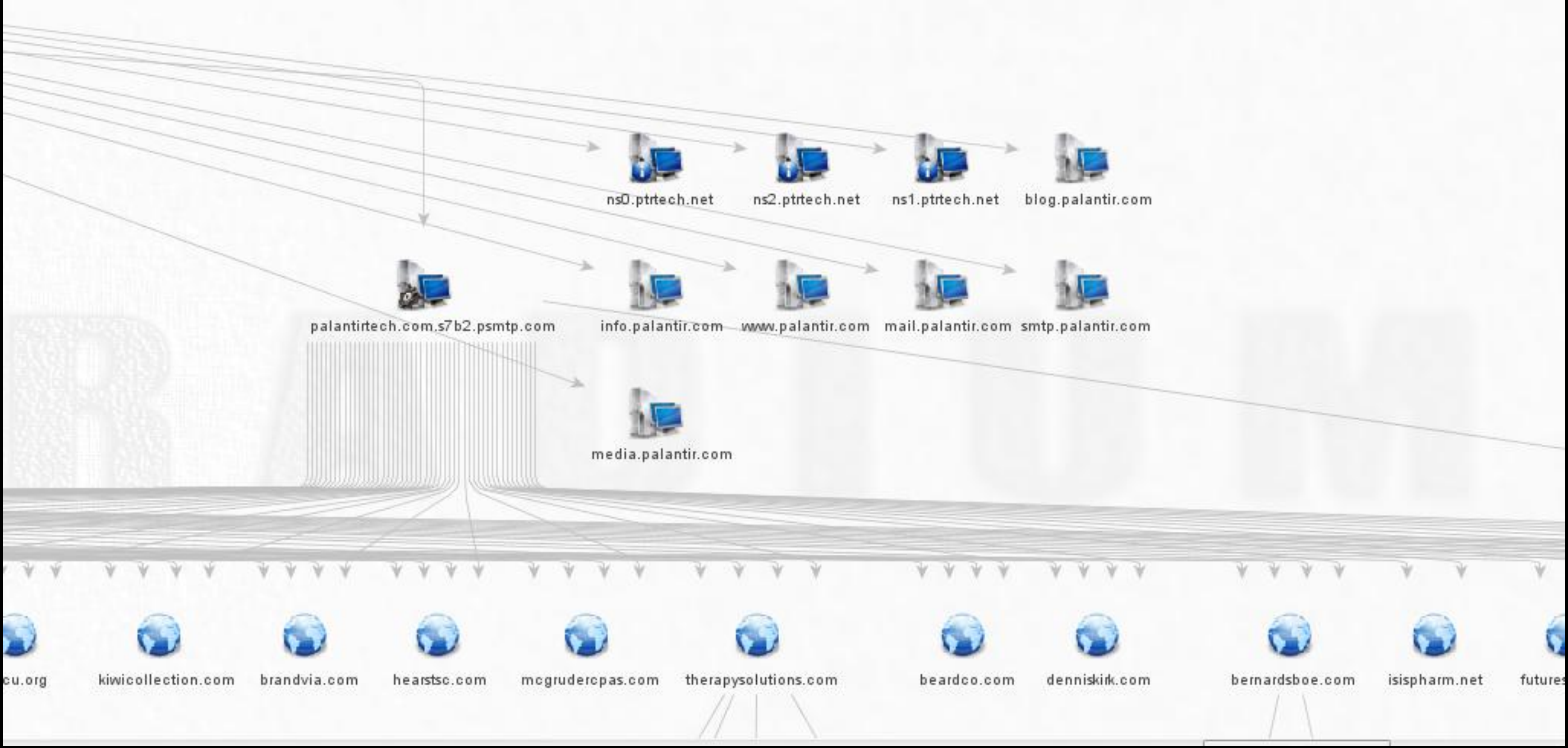
● Footprint L3 [Domain]
This performs a level 3 (intense) footprint on a domain. It takes a...

○ Person - Email Address with PN [Person]
Tries to obtain someone's email address and sees where it's used on...

○ Twitter Monitor [Phrase]
This machine monitors Twitter for hashtags, and named entities ment...

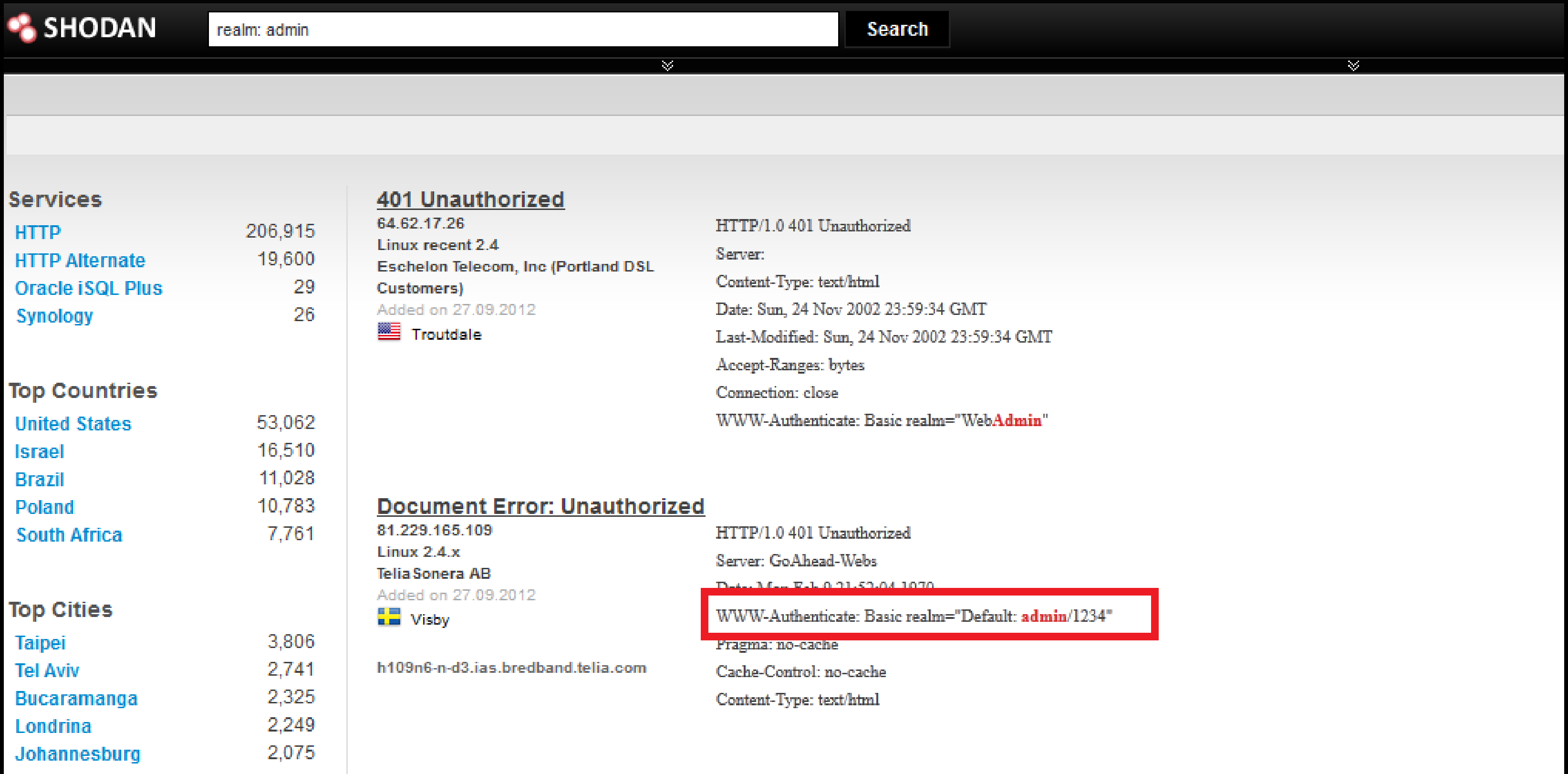
OSINT -- EXTERNAL

- Maltego Radium



OSINT -- EXTERNAL

- Shodan



Services

HTTP	206,915
HTTP Alternate	19,600
Oracle iSQL Plus	29
Synology	26

Top Countries

United States	53,062
Israel	16,510
Brazil	11,028
Poland	10,783
South Africa	7,761

Top Cities

Taipei	3,806
Tel Aviv	2,741
Bucaramanga	2,325
Londrina	2,249
Johannesburg	2,075

401 Unauthorized

64.62.17.26
Linux recent 2.4
Eschelon Telecom, Inc (Portland DSL Customers)
Added on 27.09.2012
🇺🇸 Troutdale

```
HTTP/1.0 401 Unauthorized
Server:
Content-Type: text/html
Date: Sun, 24 Nov 2002 23:59:34 GMT
Last-Modified: Sun, 24 Nov 2002 23:59:34 GMT
Accept-Ranges: bytes
Connection: close
WWW-Authenticate: Basic realm="WebAdmin"
```

Document Error: Unauthorized

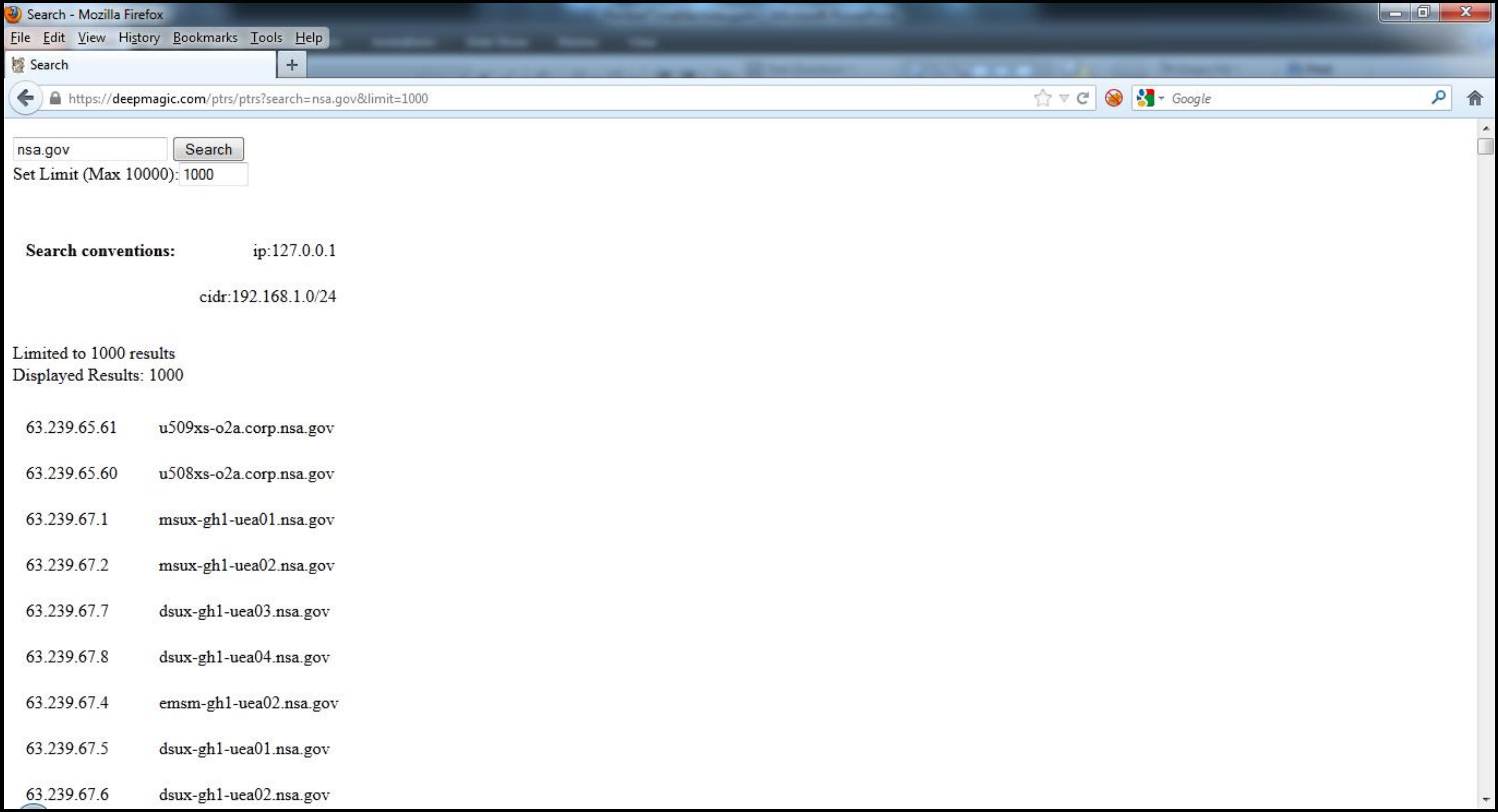
81.229.165.109
Linux 2.4.x
Telia Sonera AB
Added on 27.09.2012
🇸🇪 Visby

h109n6-n-d3.ias.bredband.telia.com

```
HTTP/1.0 401 Unauthorized
Server: GoAhead-Webs
Date: Mon Feb 9 21:52:04 1970
WWW-Authenticate: Basic realm="Default: admin/1234"
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html
```

OSINT -- EXTERNAL

- Deep Magic


Search - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Search
https://deepmagic.com/ptrs/ptrs?search=nsa.gov&limit=1000
Google

nsa.gov Search

Set Limit (Max 10000): 1000

Search conventions: ip:127.0.0.1

cidr:192.168.1.0/24

Limited to 1000 results
Displayed Results: 1000

63.239.65.61	u509xs-o2a.corp.nsa.gov
63.239.65.60	u508xs-o2a.corp.nsa.gov
63.239.67.1	msux-gh1-uea01.nsa.gov
63.239.67.2	msux-gh1-uea02.nsa.gov
63.239.67.7	dsux-gh1-uea03.nsa.gov
63.239.67.8	dsux-gh1-uea04.nsa.gov
63.239.67.4	emsm-gh1-uea02.nsa.gov
63.239.67.5	dsux-gh1-uea01.nsa.gov
63.239.67.6	dsux-gh1-uea02.nsa.gov

OSINT -- EXTERNAL

- Metasploit Auxiliary Modules
- Email Enumeration
- DNS enumeration
- SMTP
- Etc…

OSINT -- EXTERNAL

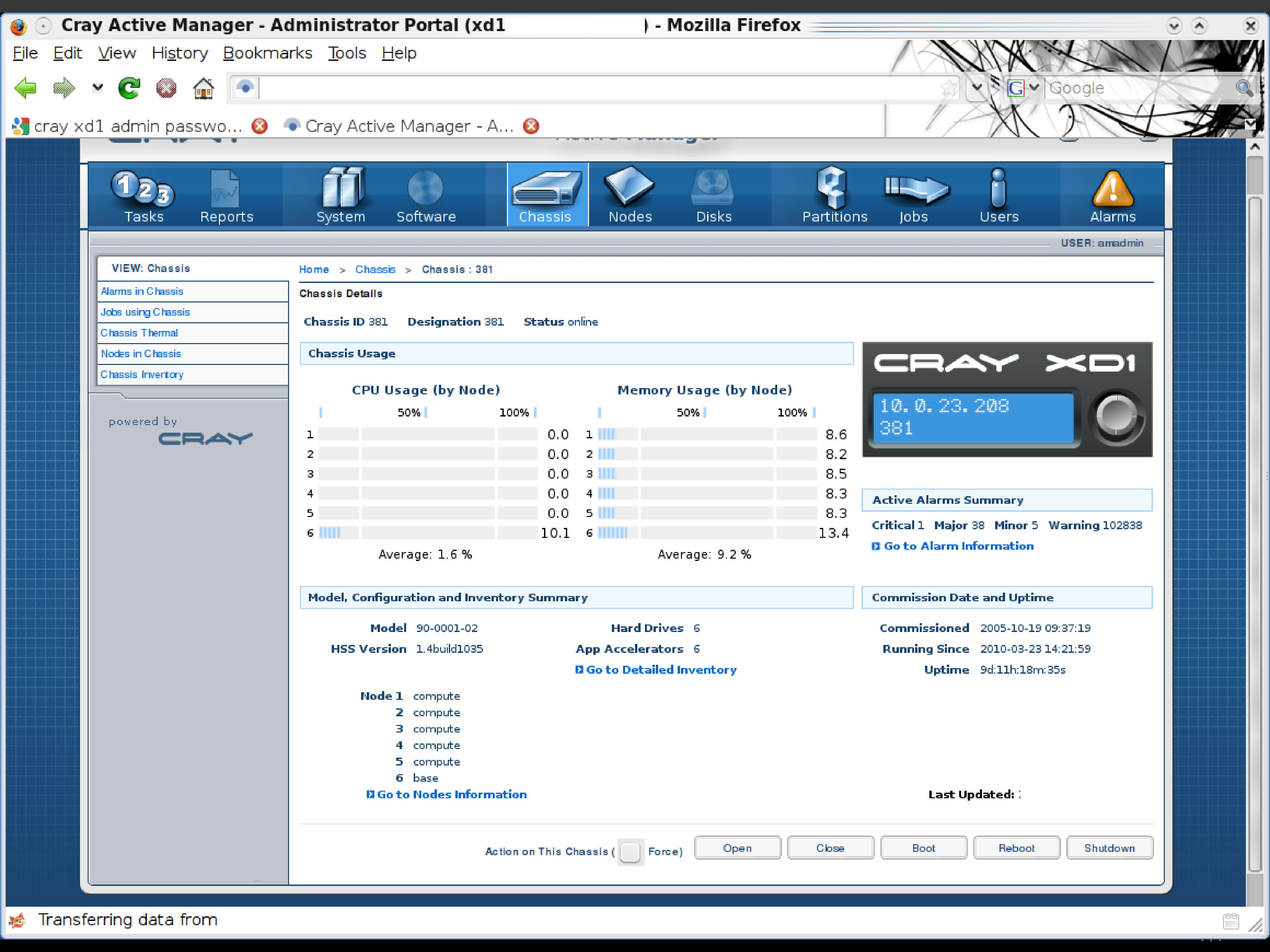
- Neat examples of network level stuff

  ```
  user@ubuntu:~$ host -t MX domain.net
  domain.net mail is handled by 10 barracuda01.domain.net.
  domain.net mail is handled by 10 barracuda02.domain.net.
  ```

- Zone Transfers
  - Rare but still pop up
  - Reveal authentication portals, system role, additional IP space

OSINT -- EXTERNAL

- You need to put eyes on everything!
  - SVN/CVS repos – usernames/file access/source code/passwords/keys
  - Directory listing – info leakage – credentials, etc.
  - Internal IP leakage – useful later during compromise, targeted attacks
  - Send bounce email – get internal IPs, server names, system type, etc.
  - Eyes on everything + Default passwords ==



USER: amadmin

Home > Chassis > Chassis : 381

Chassis Details

Chassis ID 381 **Designation** 381 **Status** online

Chassis Usage

CPU Usage (by Node)	
1	0.0
2	0.0
3	0.0
4	0.0
5	0.0
6	10.1

Average: 1.6 %

Memory Usage (by Node)	
1	8.6
2	8.2
3	8.5
4	8.3
5	8.3
6	13.4

Average: 9.2 %

10.0.23.208
381

Active Alarms Summary

Critical 1 **Major** 38 **Minor** 5 **Warning** 102838

Go to Alarm Information

Model, Configuration and Inventory Summary

Model 90-0001-02
HSS Version 1.4build1035

Hard Drives 6
App Accelerators 6
Go to Detailed Inventory

Node 1	compute
2	compute
3	compute
4	compute
5	compute
6	base

Go to Nodes Information

Commission Date and Uptime

Commissioned 2005-10-19 09:37:19
Running Since 2010-03-23 14:21:59
Uptime 9d:11h:18m:35s

Last Updated: :

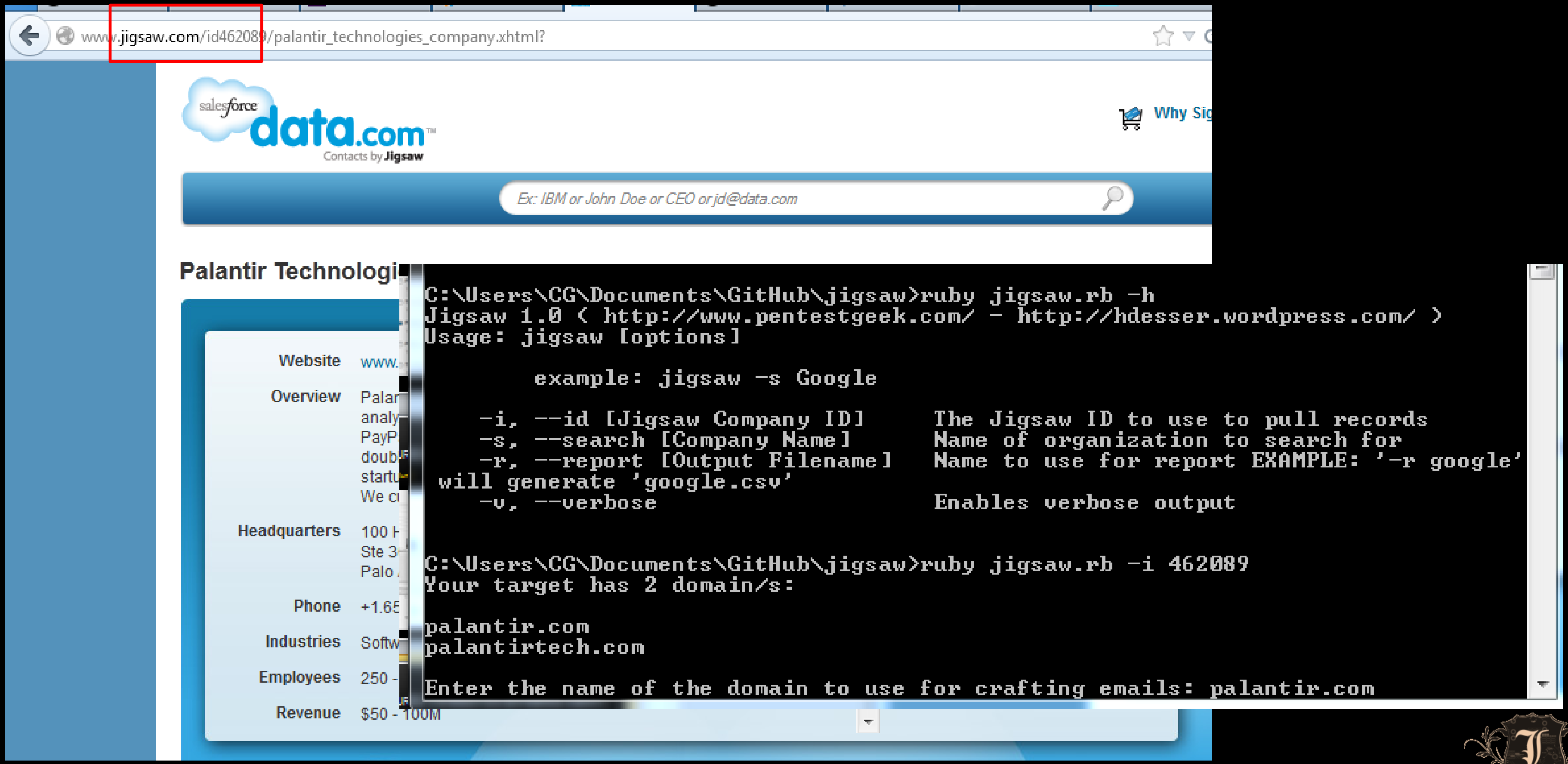
Action on This Chassis (□ Force)

OSINT -- EXTERNAL

- LinkedIN
  - See my talk from yesterday ☺
  - New Hires – EXCELLENT targets
    - Minimal training
    - Weaker Passwords – Changme1[23], Welcome1[23]]
    - Unfamiliar with personnel, policies and procedures

OSINT -- EXTERNAL

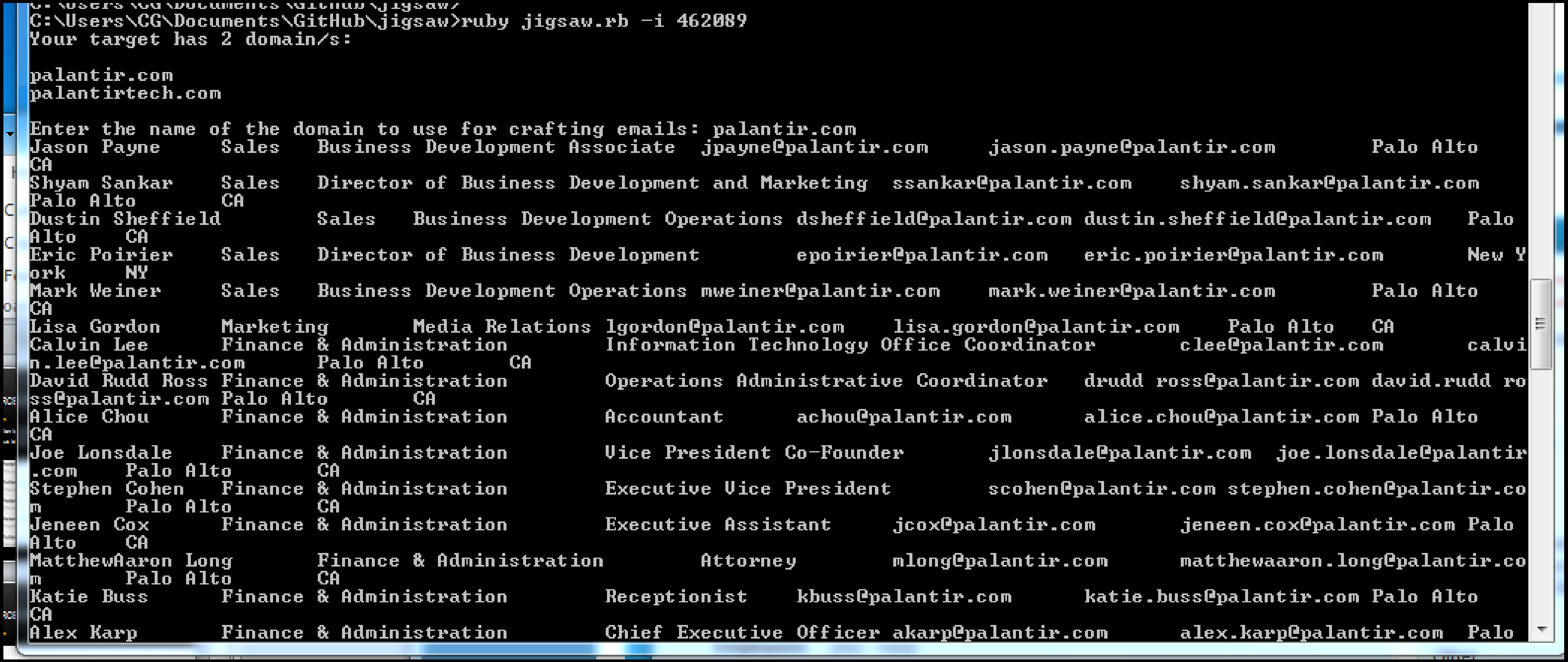
- jigsaw.rb
  - https://github.com/pentestgeek/jigsaw



```
C:\Users\CG\Documents\GitHub\jigsaw>ruby jigsaw.rb -h
Jigsaw 1.0 ( http://www.pentestgeek.com/ - http://hdesser.wordpress.com/ )
Usage: jigsaw [options]

        example: jigsaw -s Google

    -i, --id [Jigsaw Company ID]      The Jigsaw ID to use to pull records
    -s, --search [Company Name]       Name of organization to search for
    -r, --report [Output Filename]    Name to use for report EXAMPLE: '-r google'
 will generate 'google.csv'
    -v, --verbose                     Enables verbose output


C:\Users\CG\Documents\GitHub\jigsaw>ruby jigsaw.rb -i 462089
Your target has 2 domain/s:

palantir.com
palantirtech.com

Enter the name of the domain to use for crafting emails: palantir.com
```

OSINT -- EXTERNAL

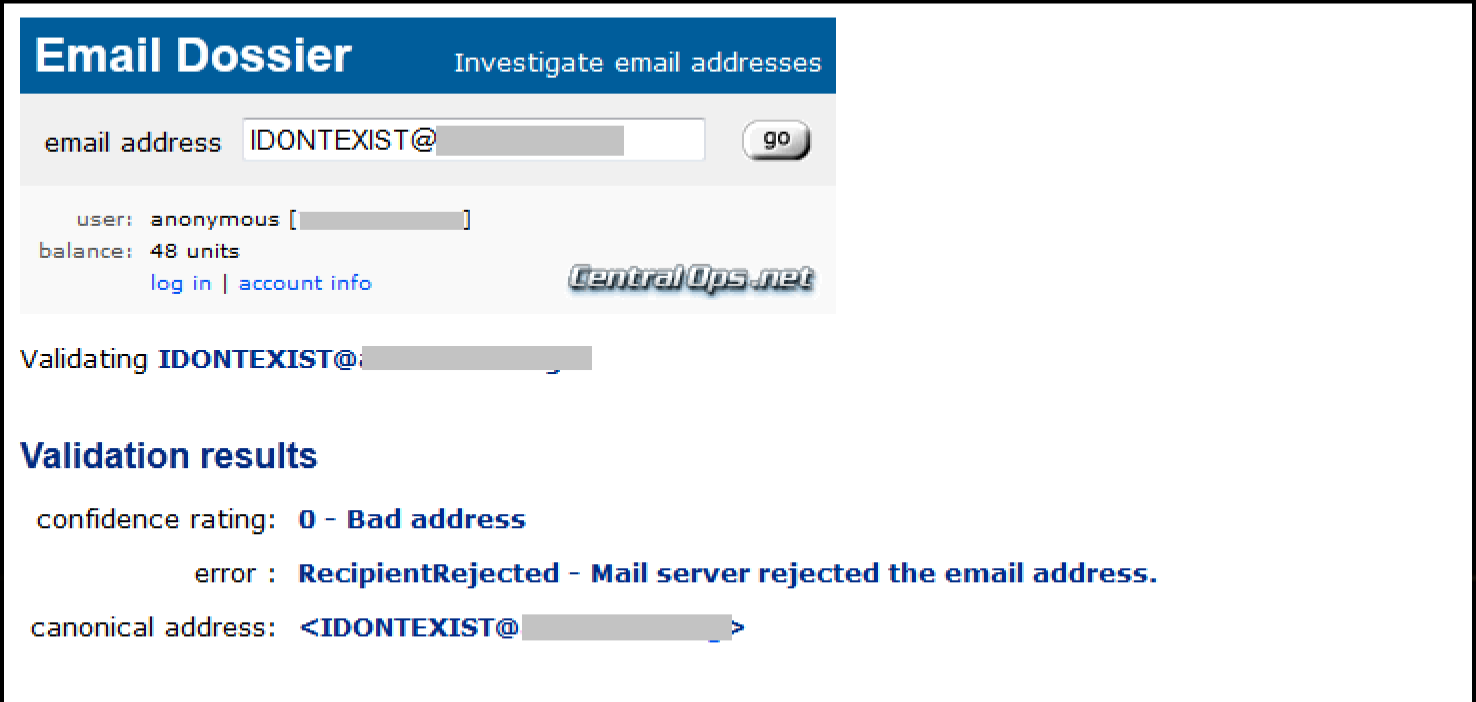
- Jigsaw.rb



```
C:\Users\CG\Documents\GitHub\jigsaw>
C:\Users\CG\Documents\GitHub\jigsaw>ruby jigsaw.rb -i 462089
Your target has 2 domain/s:

palantir.com
palantirtech.com

Enter the name of the domain to use for crafting emails: palantir.com
Jason Payne     Sales   Business Development Associate  jpayne@palantir.com     jason.payne@palantir.com        Palo Alto
CA
Shyam Sankar    Sales   Director of Business Development and Marketing  ssankar@palantir.com    shyam.sankar@palantir.com
Palo Alto       CA
Dustin Sheffield        Sales   Business Development Operations dsheffield@palantir.com dustin.sheffield@palantir.com   Palo
Alto    CA
Eric Poirier    Sales   Director of Business Development        epoirier@palantir.com   eric.poirier@palantir.com       New Y
ork     NY
Mark Weiner     Sales   Business Development Operations mweiner@palantir.com    mark.weiner@palantir.com        Palo Alto
CA
Lisa Gordon     Marketing       Media Relations lgordon@palantir.com    lisa.gordon@palantir.com    Palo Alto   CA
Calvin Lee      Finance & Administration        Information Technology Office Coordinator       clee@palantir.com       calvi
n.lee@palantir.com      Palo Alto       CA
David Rudd Ross Finance & Administration        Operations Administrative Coordinator   drudd ross@palantir.com david.rudd ro
ss@palantir.com Palo Alto       CA
Alice Chou      Finance & Administration        Accountant      achou@palantir.com      alice.chou@palantir.com Palo Alto
CA
Joe Lonsdale    Finance & Administration        Vice President Co-Founder       jlonsdale@palantir.com  joe.lonsdale@palantir
.com    Palo Alto       CA
Stephen Cohen   Finance & Administration        Executive Vice President        scohen@palantir.com stephen.cohen@palantir.co
m       Palo Alto       CA
Jeneen Cox      Finance & Administration        Executive Assistant     jcox@palantir.com       jeneen.cox@palantir.com Palo
Alto    CA
MatthewAaron Long       Finance & Administration        Attorney        mlong@palantir.com      matthewaaron.long@palantir.co
m       Palo Alto       CA
Katie Buss      Finance & Administration        Receptionist    kbuss@palantir.com      katie.buss@palantir.com Palo Alto
CA
Alex Karp       Finance & Administration        Chief Executive Officer akarp@palantir.com      alex.karp@palantir.com  Palo
```

OSINT -- EXTERNAL

- Using this information to insert foot in ass
- How many of you check to see if you can validate emails via the target's email servers?
    - Pro-Tip → the msf module for this is jacked



Email Dossier Investigate email addresses

email address IDONTEXIST@[redacted]

user: anonymous [[redacted]]
balance: 48 units
log in | account info

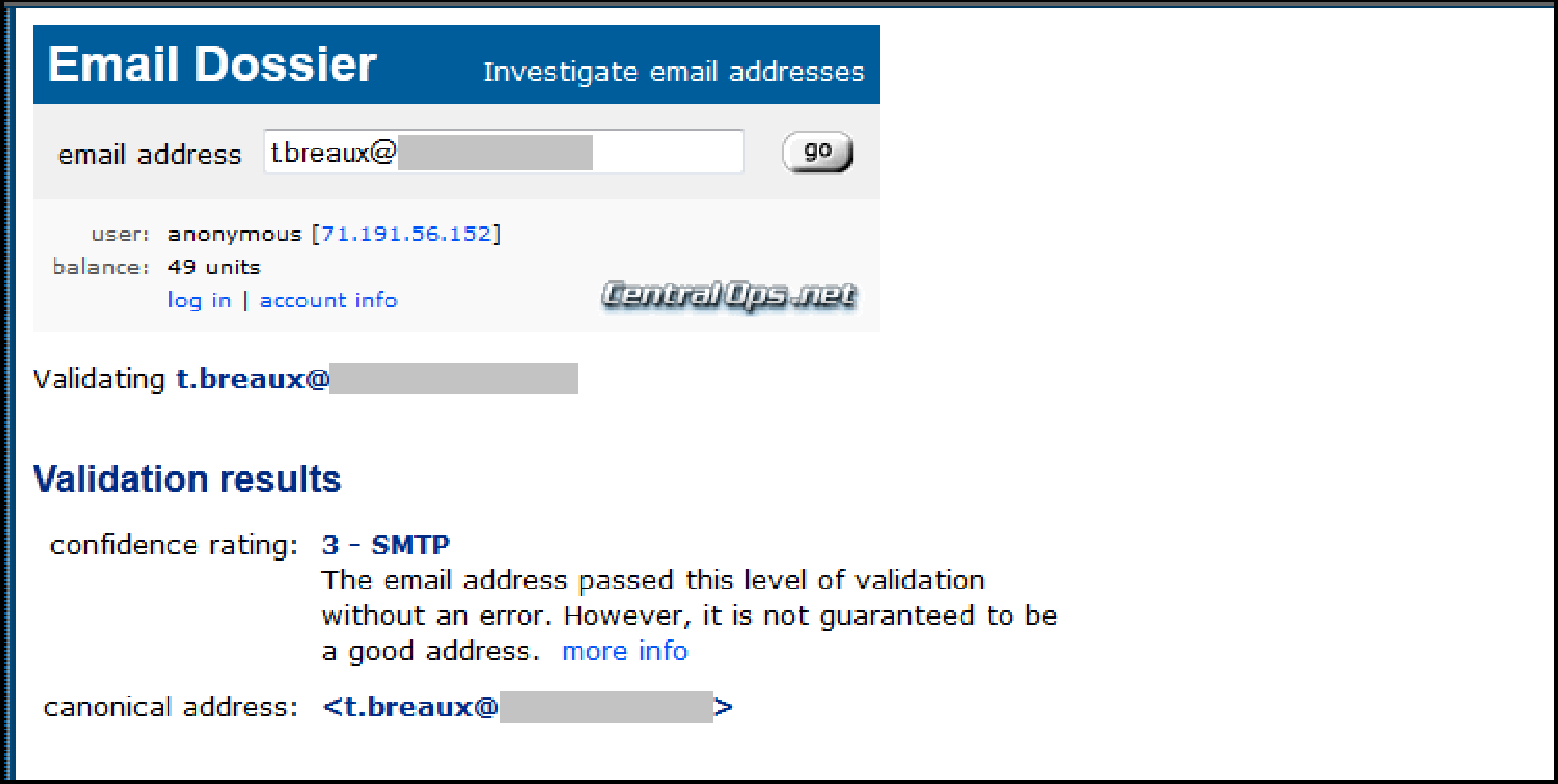
Validating **IDONTEXIST@**[redacted]

Validation results

confidence rating: **0 - Bad address**
error : **RecipientRejected - Mail server rejected the email address.**
canonical address: **<IDONTEXIST@**[redacted]**>**

OSINT -- EXTERNAL

Validated



Email Dossier Investigate email addresses

email address t.breaux@[redacted]

user: anonymous [71.191.56.152]
balance: 49 units
log in | account info

Validating **t.breaux@**[redacted]

Validation results

confidence rating: **3 - SMTP**
The email address passed this level of validation without an error. However, it is not guaranteed to be a good address. more info

canonical address: **<t.breaux@**[redacted]**>**

OSINT – DESIRED RESULTS

- Attack/Threat Matrix
  - IP Ranges/Host names
  - Authentication Portals and Types
  - Username/Email List
  - Contact Information/Geo Data
  - Credentials (possible)
  - The list is endless…

OSINT -- INTERNAL

- Just as important as external profiling
- Follow a repeatable methodology/develop a habit
- Prioritize the value of your targets and task lists
- Intel from external OSINT applies to internal systems (file server names, usernames, etc.)
- DHCP leases, DNS zone xfer/lookups, packet captures, ARP, etc.

ATTACK TIME!

SMART BRUTE FORCING

- Throw away the 600MB dictionary files
- You will most likely lock accounts if you blow your wad
- Build a generic accounts list
  - Take old SAM files, pull out common names
  - Build a generic account list
  - Lucky punches are common
  - Invoices/invoices, training/training, helpdesk/helpdesk
  - Go build your own ☺
- Space out your runs. 2-3 passwords every few hours.
- Smarter Passwords – Welcome1[23], Password1[23], Summer12, Company1[23]
- CeWL – Custom Wordlist Generator – Robin Wood
- Use your intelligence from OSINT activities

OWA BRUTING

- Tons of ways to do it but they all have limitations
  - Owabf.py
  - Wmat – custom pattern files
  - Metasploit auxiliary module
  - Burp Intruder
    - PRO TIP: Cookie needs to be reset after a successful login
    - Major Content Length change = successful login

OWA GAL DUMPING

- Useful if you land a weak password and want to try it on more users
- OWA 2007 and older have the GAL available for downloading (sometimes)
- OWA 2010 requires another step:

```
<params><canary>9f2202c7807a47c0820abb316d58b3b9</canary><St><ADVL
VS sId="YqPmr+NBl0eJUY0tnMEtqA==" mL="1" sC="52" sO="0"
ckI="BxMAAA==" ckii="87" clcid="1033"
cPfdDC="dc02.FOO.LOCAL"/></St><SR>4000</SR><RC>100</RC></params>
```

uri="sip:owned@foo.net"></div>

LOTUS NOTES BRUTING

- Penetration Tester’s WET DREAM
- Names.nsf == GOLD!
- Since forever Lotus Notes has suffered from hash disclosure via one account
- Tons of ways to do it but they all have limitations
  - Metasploit auxiliary module
  - Domino Hunter script
  - Nmap NSE script
  - Burp Intruder
- JtR hash cracking – dominosec/lotus5

CITRIX ACCESS

- Published Application Enumeration
- IP address/System name enumeration
- Username enumeration (sometimes)
- Burp Intruder
- Other tools:
  - Metasploit auxillary modules
  - Nmap NSE scripts
  - Defcon 10: Citrix PA Scan/Proxy
  - Citrix Access Gateway software – ICA creation

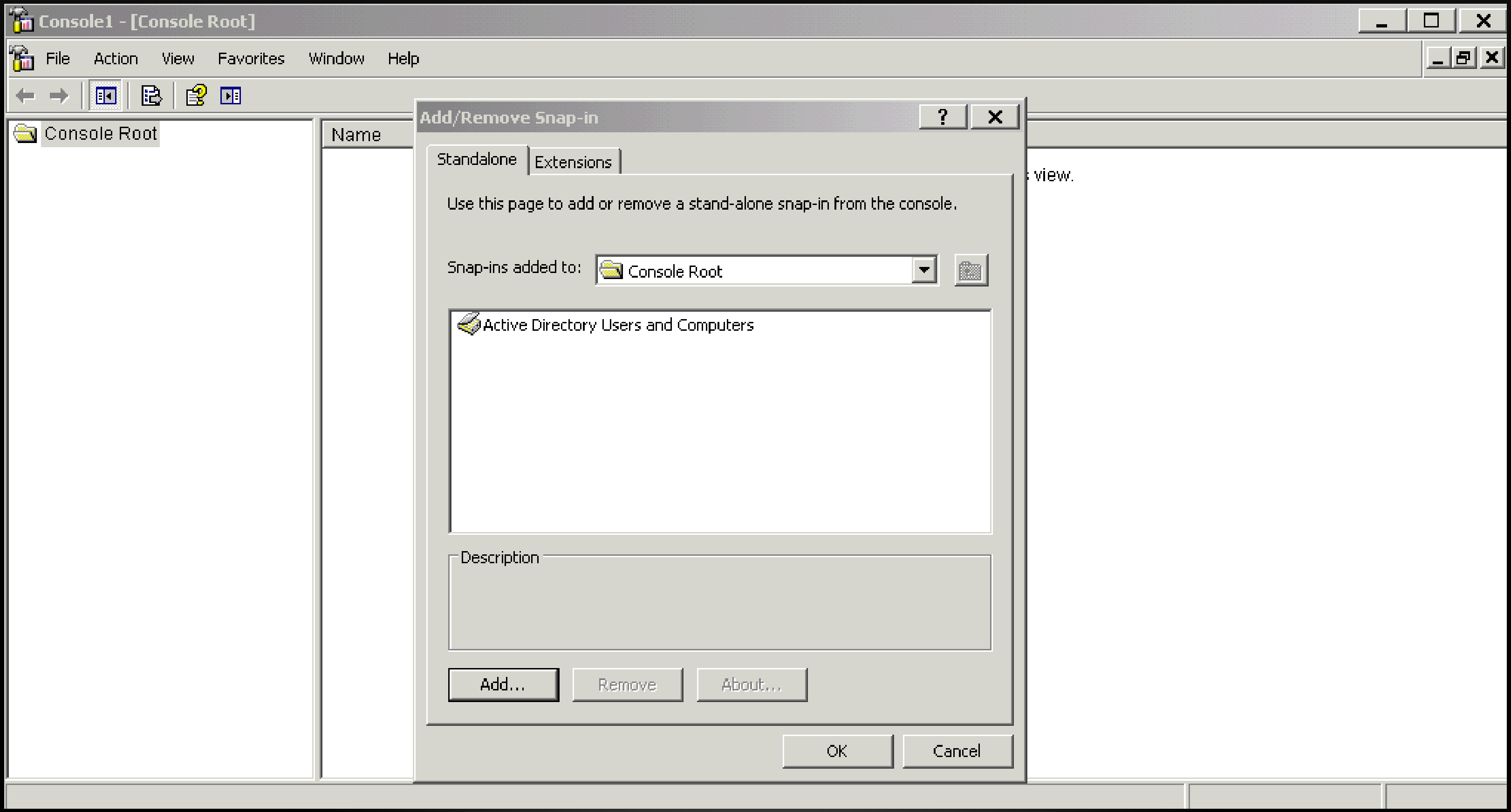
CITRIX – APPLICATION BREAKOUT

- One published application is usually all you need
- Old tricks still work
  - File open – force browse %SYSTEMROOT%
  - Help file – search
  - Unknown file type – open with – explorer
  - IKAT
  - See old talks on Citrix for refresher ☺

CITRIX – NEW(ER) DIRTY SECRETS

- System Information – File Open
- Explorer -> mmc.exe
  - Remote manage system
  - Add local administrator account
  - Remote Desktop access
  - Drop binary -> exploit -> pivot -> ….

CITRIX – MMC

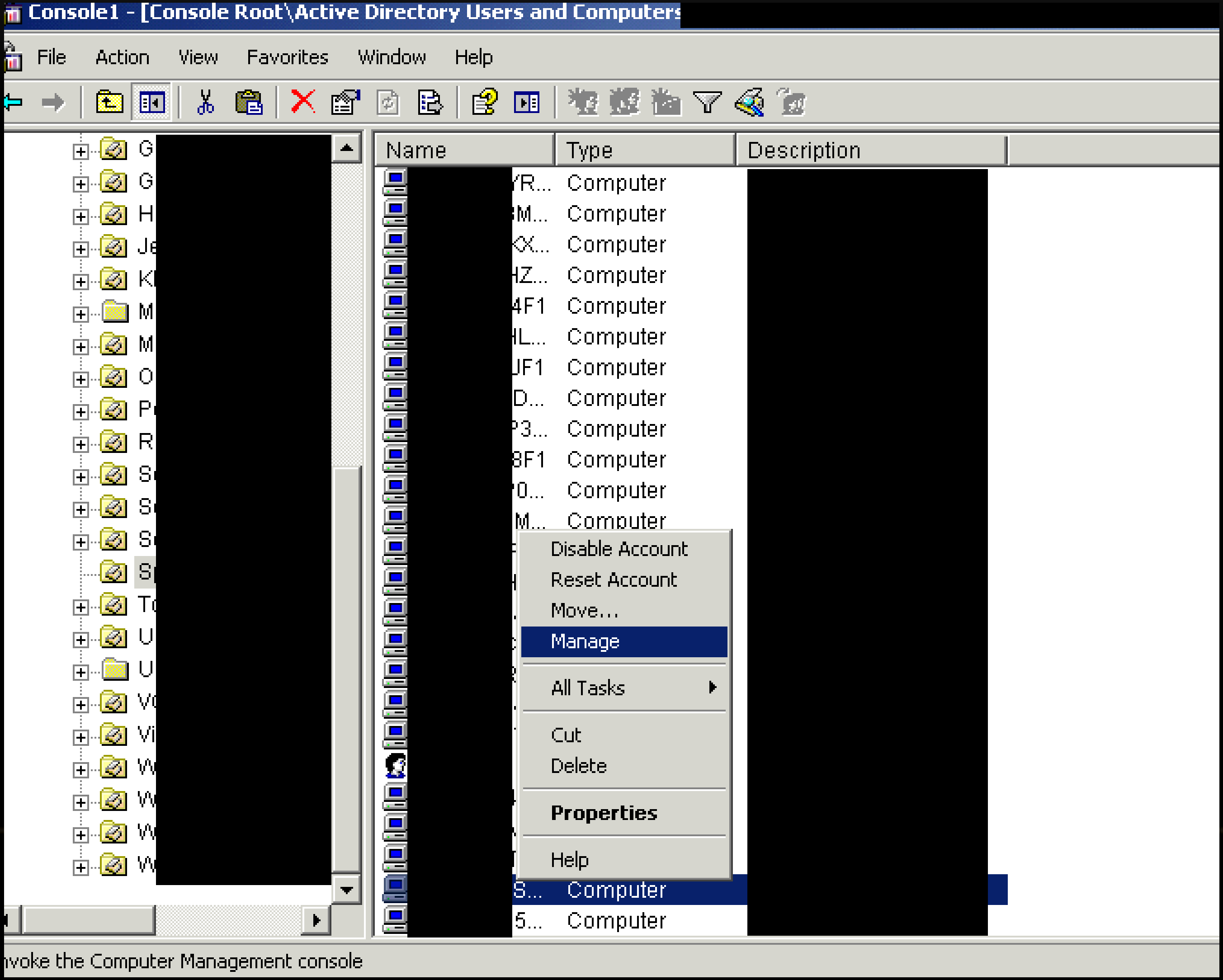


Use this page to add or remove a stand-alone snap-in from the console.

Snap-ins added to: Console Root

Active Directory Users and Computers

CITRIX – MMC SEXINESS



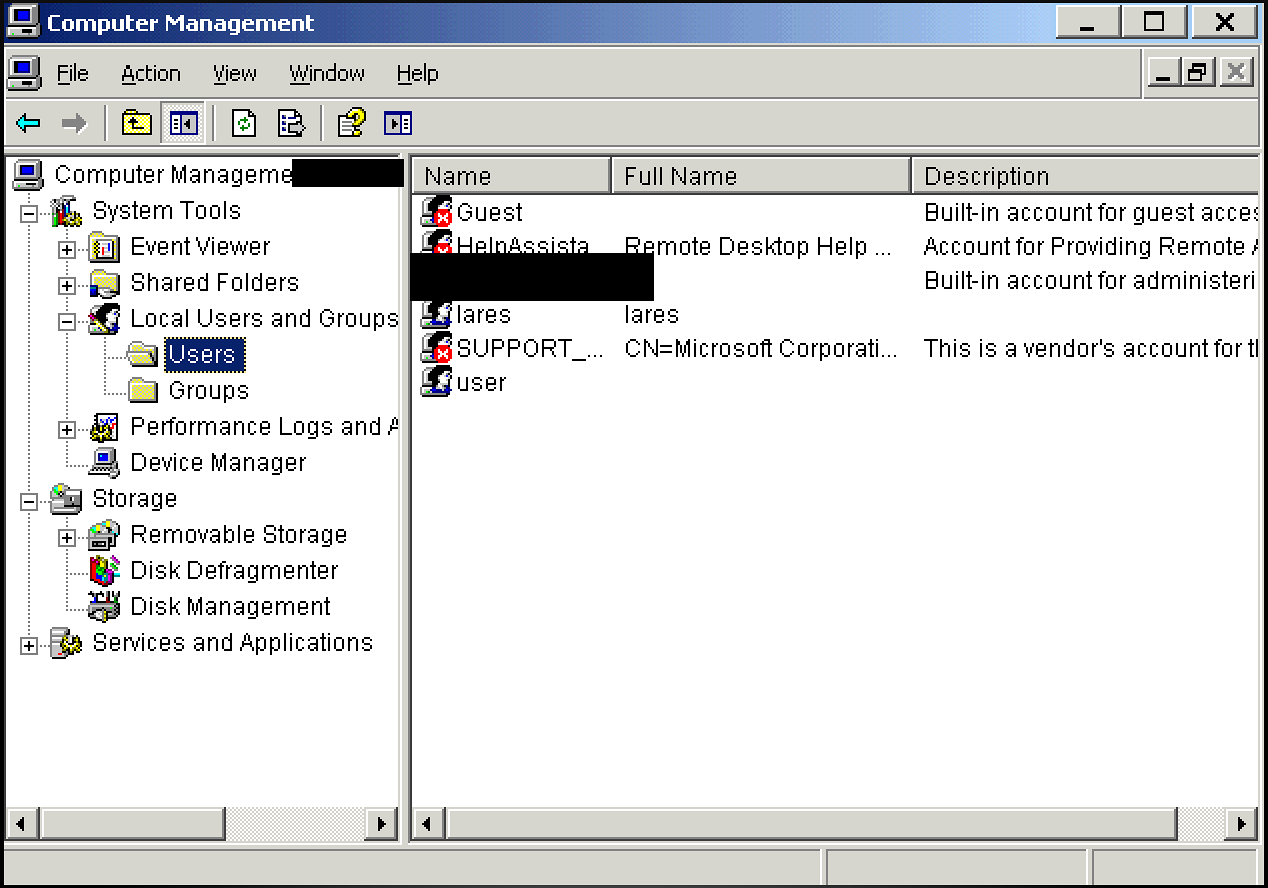
Console1 - [Console Root\Active Directory Users and Computers

[redacted]

Name	Type	Description
[redacted]YR...	Computer	[redacted]
[redacted]M...	Computer	[redacted]
[redacted]KX...	Computer	[redacted]
[redacted]HZ...	Computer	[redacted]
[redacted]4F1	Computer	[redacted]
[redacted]HL...	Computer	[redacted]
[redacted]UF1	Computer	[redacted]
[redacted]D...	Computer	[redacted]
[redacted]P3...	Computer	[redacted]
[redacted]8F1	Computer	[redacted]
[redacted]P0...	Computer	[redacted]
[redacted]M...	Computer	[redacted]
[redacted]S...	Computer	[redacted]
[redacted]5...	Computer	[redacted]

nvoke the Computer Management console

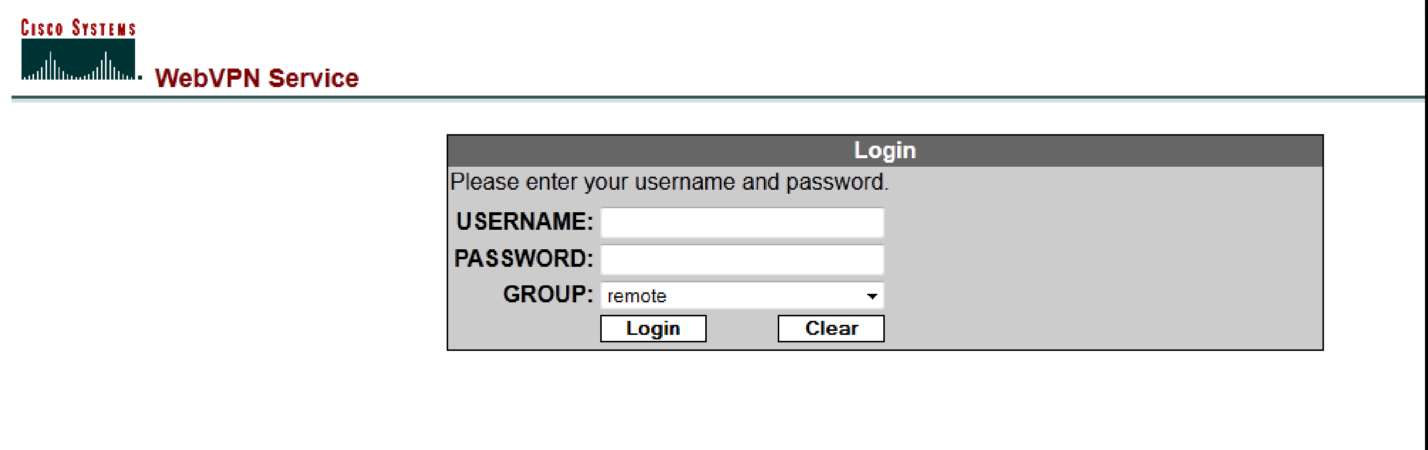
CITRIX – MMC PWNED



Name	Full Name	Description
Guest		Built-in account for guest acces
HelpAssista	Remote Desktop Help ...	Account for Providing Remote /
[redacted]		Built-in account for administeri
lares	lares	
SUPPORT_...	CN=Microsoft Corporati...	This is a vendor's account for tl
user		

SSL VPN BRUTE FORCING

- If its single factor its worth doing SMART brute forcing



Cisco Systems

WebVPN Service

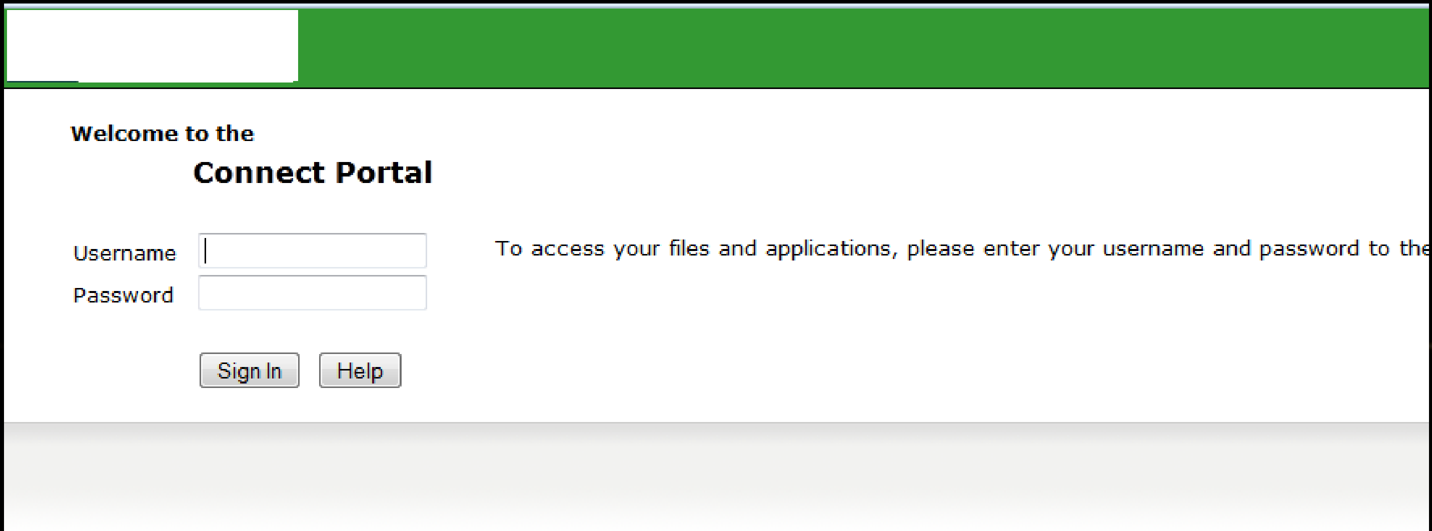
Login

Please enter your username and password.

USERNAME:

PASSWORD:

GROUP: remote



Welcome to the

Connect Portal

Username

Password

To access your files and applications, please enter your username and password to the

VPN PRIVILEGES

- 9/10 times the VPN drops you right on the network with everyone else
- This effectively bypasses NAC and everything else you implemented

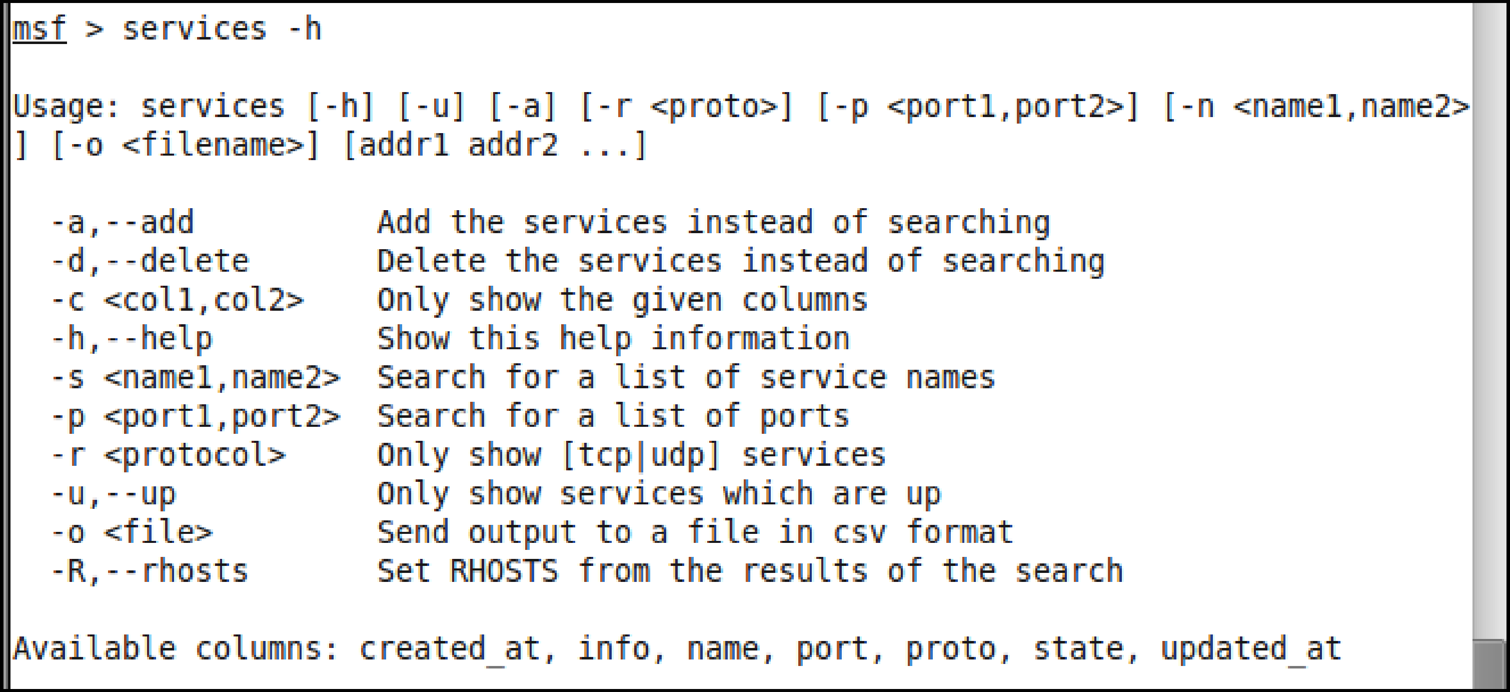
FILE UPLOAD

- WebDav
- HTTP METHOD Abuse (PUT/DELETE)
- RFI/LFI
- The List goes on…

EXPOSED SERVICES – ADMIN INTERFACES

- Admin Interfaces listening on random ports can be gold.
- Finding them amongst all the crap can be challenging.
- Possible Methodology
  - Nmap your range
  - Import into metasploit
  - Use the db_ searches to pull out all hosts you want
  - Some ruby to make them into a piece of html
  - Use linky to open everything

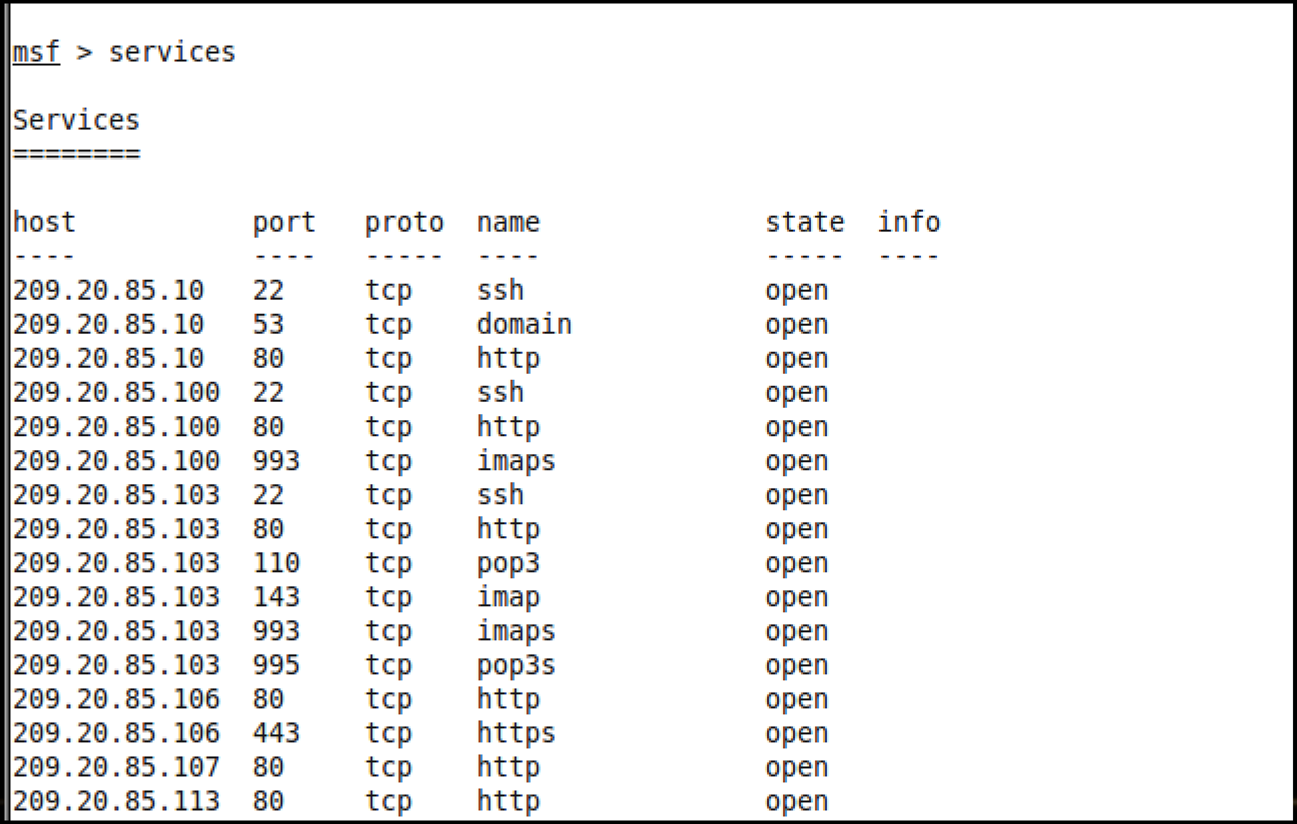
EXPOSED SERVICES – ADMIN INTERFACES



```
msf > services -h

Usage: services [-h] [-u] [-a] [-r <proto>] [-p <port1,port2>] [-n <name1,name2>
] [-o <filename>] [addr1 addr2 ...]

  -a,--add          Add the services instead of searching
  -d,--delete       Delete the services instead of searching
  -c <col1,col2>    Only show the given columns
  -h,--help         Show this help information
  -s <name1,name2>  Search for a list of service names
  -p <port1,port2>  Search for a list of ports
  -r <protocol>     Only show [tcp|udp] services
  -u,--up           Only show services which are up
  -o <file>         Send output to a file in csv format
  -R,--rhosts       Set RHOSTS from the results of the search

Available columns: created_at, info, name, port, proto, state, updated_at
```

EXPOSED SERVICES – ADMIN INTERFACES

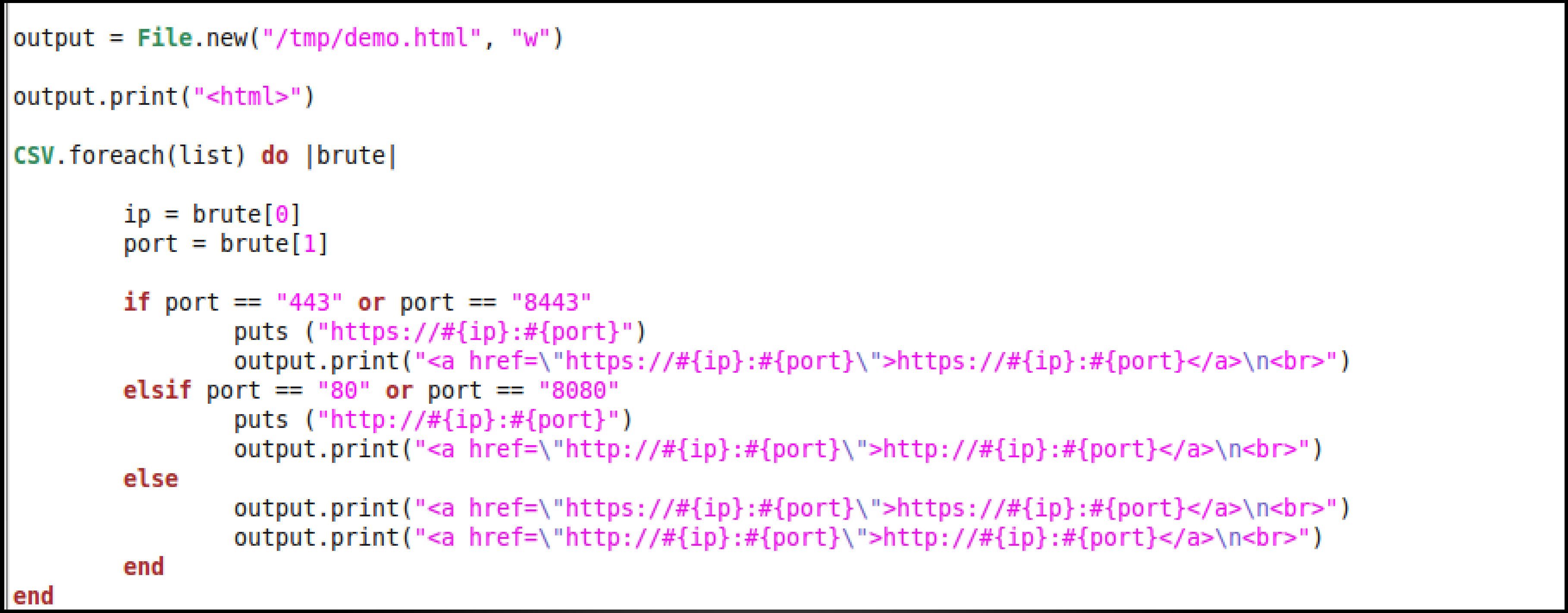
- msf > services -o /tmp/demo.csv



```
msf > services

Services
========

host            port   proto  name              state  info
----            ----   -----  ----              -----  ----
209.20.85.10    22     tcp    ssh               open
209.20.85.10    53     tcp    domain            open
209.20.85.10    80     tcp    http              open
209.20.85.100   22     tcp    ssh               open
209.20.85.100   80     tcp    http              open
209.20.85.100   993    tcp    imaps             open
209.20.85.103   22     tcp    ssh               open
209.20.85.103   80     tcp    http              open
209.20.85.103   110    tcp    pop3              open
209.20.85.103   143    tcp    imap              open
209.20.85.103   993    tcp    imaps             open
209.20.85.103   995    tcp    pop3s             open
209.20.85.106   80     tcp    http              open
209.20.85.106   443    tcp    https             open
209.20.85.107   80     tcp    http              open
209.20.85.113   80     tcp    http              open
```

EXPOSED SERVICES – ADMIN INTERFACES

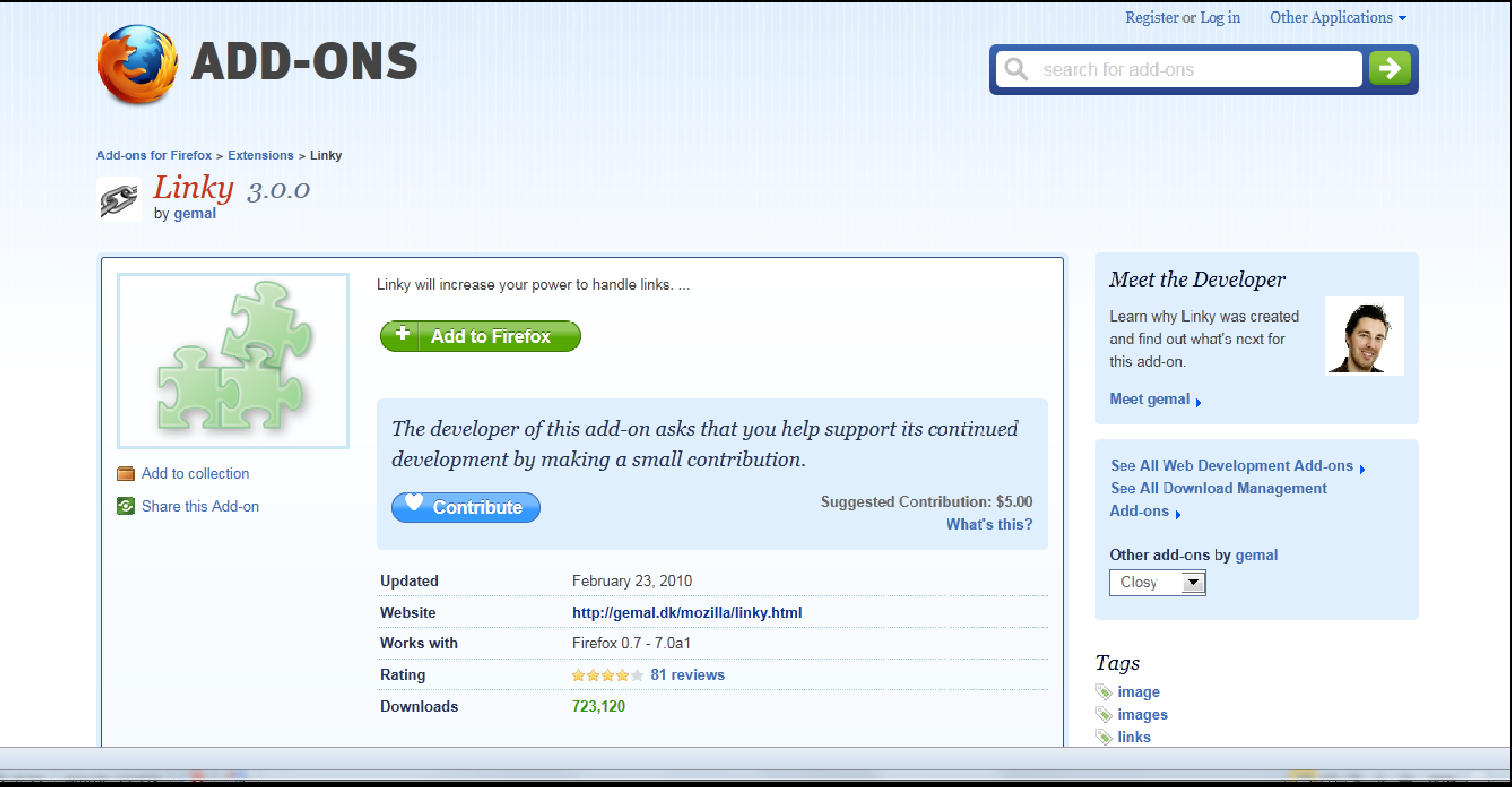
- Ruby



```
output = File.new("/tmp/demo.html", "w")

output.print("<html>")

CSV.foreach(list) do |brute|

        ip = brute[0]
        port = brute[1]

        if port == "443" or port == "8443"
                puts ("https://#{ip}:#{port}")
                output.print("<a href=\"https://#{ip}:#{port}\">https://#{ip}:#{port}</a>\n<br>")
        elsif port == "80" or port == "8080"
                puts ("http://#{ip}:#{port}")
                output.print("<a href=\"http://#{ip}:#{port}\">http://#{ip}:#{port}</a>\n<br>")
        else
                output.print("<a href=\"https://#{ip}:#{port}\">https://#{ip}:#{port}</a>\n<br>")
                output.print("<a href=\"http://#{ip}:#{port}\">http://#{ip}:#{port}</a>\n<br>")
        end
end
```

EXPOSED SERVICES – ADMIN INTERFACES

- Linky



Add-ons for Firefox > Extensions > Linky

Linky 3.0.0

by gemal

Linky will increase your power to handle links. ...

The developer of this add-on asks that you help support its continued development by making a small contribution.

Suggested Contribution: $5.00
What's this?

Updated	February 23, 2010
Website	http://gemal.dk/mozilla/linky.html
Works with	Firefox 0.7 - 7.0a1
Rating	★★★★☆ 81 reviews
Downloads	723,120

Meet the Developer

Learn why Linky was created and find out what's next for this add-on.

Meet gemal

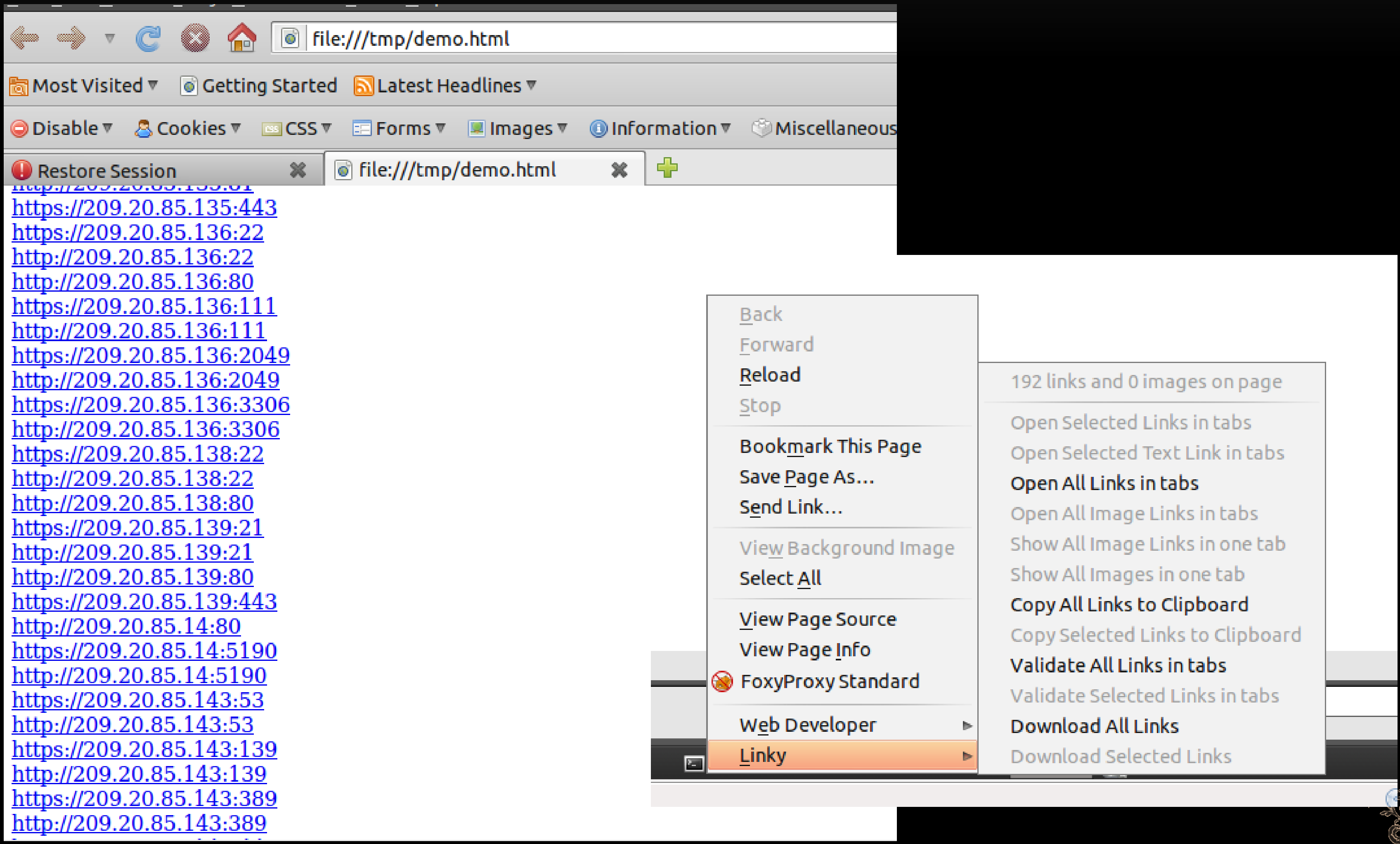
See All Web Development Add-ons
See All Download Management Add-ons

Other add-ons by gemal

Tags

image
images
links

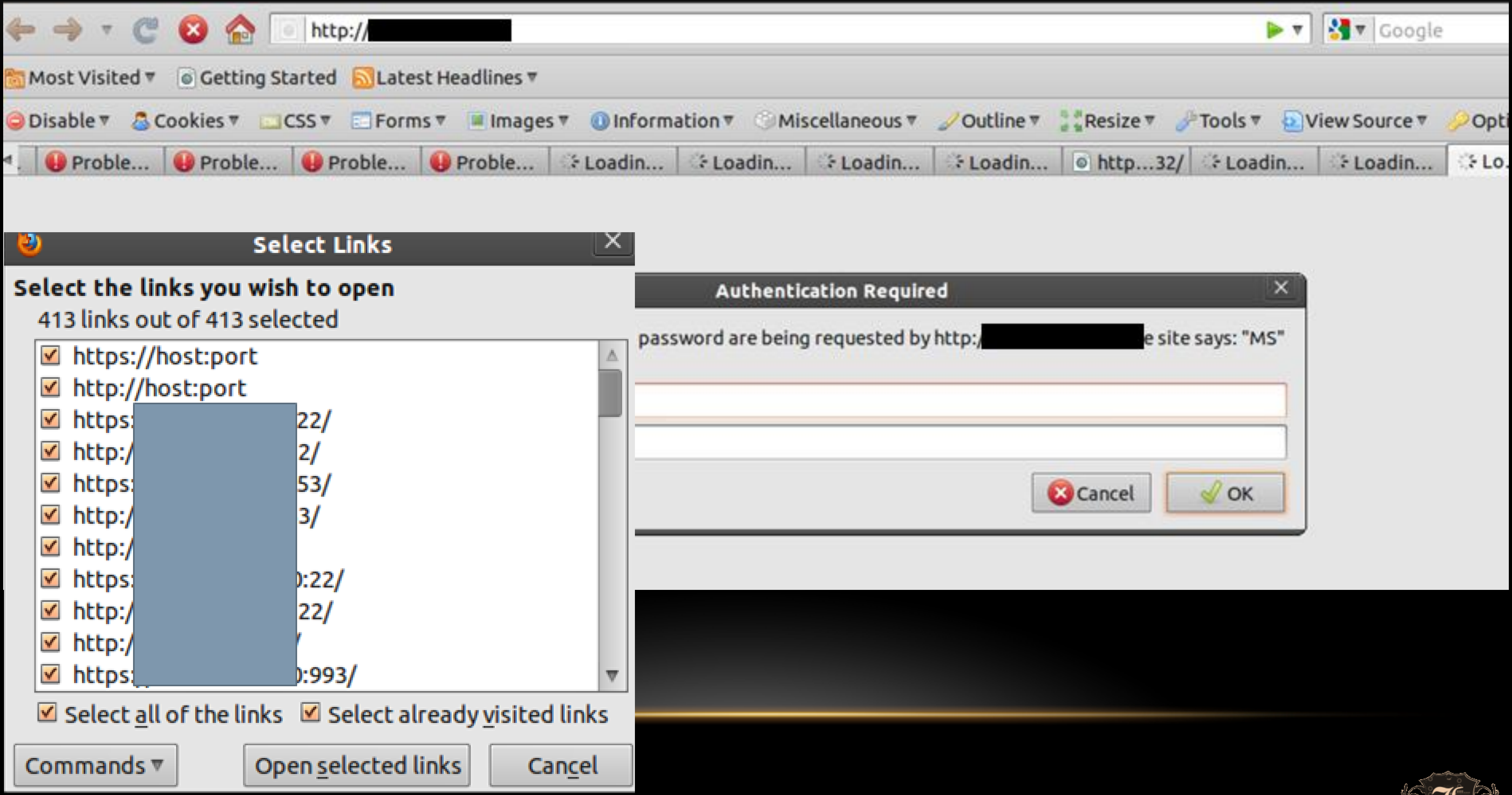
EXPOSED SERVICES – ADMIN INTERFACES



https://209.20.85.135:443
https://209.20.85.136:22
http://209.20.85.136:22
http://209.20.85.136:80
https://209.20.85.136:111
http://209.20.85.136:111
https://209.20.85.136:2049
http://209.20.85.136:2049
https://209.20.85.136:3306
http://209.20.85.136:3306
https://209.20.85.138:22
http://209.20.85.138:22
http://209.20.85.138:80
https://209.20.85.139:21
http://209.20.85.139:21
http://209.20.85.139:80
https://209.20.85.139:443
http://209.20.85.14:80
https://209.20.85.14:5190
http://209.20.85.14:5190
https://209.20.85.143:53
http://209.20.85.143:53
https://209.20.85.143:139
http://209.20.85.143:139
https://209.20.85.143:389
http://209.20.85.143:389

Back
Forward
Reload
Stop
Bookmark This Page
Save Page As…
Send Link…
View Background Image
Select All
View Page Source
View Page Info
FoxyProxy Standard
Web Developer
Linky
192 links and 0 images on page
Open Selected Links in tabs
Open Selected Text Link in tabs
Open All Links in tabs
Open All Image Links in tabs
Show All Image Links in one tab
Show All Images in one tab
Copy All Links to Clipboard
Copy Selected Links to Clipboard
Validate All Links in tabs
Validate Selected Links in tabs
Download All Links
Download Selected Links

EXPOSED SERVICES – ADMIN INTERFACES



Select Links

Select the links you wish to open

413 links out of 413 selected

- ☑ https://host:port
- ☑ http://host:port
- ☑ https:[redacted]22/
- ☑ http:/[redacted]2/
- ☑ https:[redacted]53/
- ☑ http:/[redacted]3/
- ☑ http:/[redacted]
- ☑ https:[redacted]:22/
- ☑ http:/[redacted]22/
- ☑ http:/[redacted]/
- ☑ https:[redacted]:993/

☑ Select all of the links ☑ Select already visited links

Commands ▾ | Open selected links | Cancel

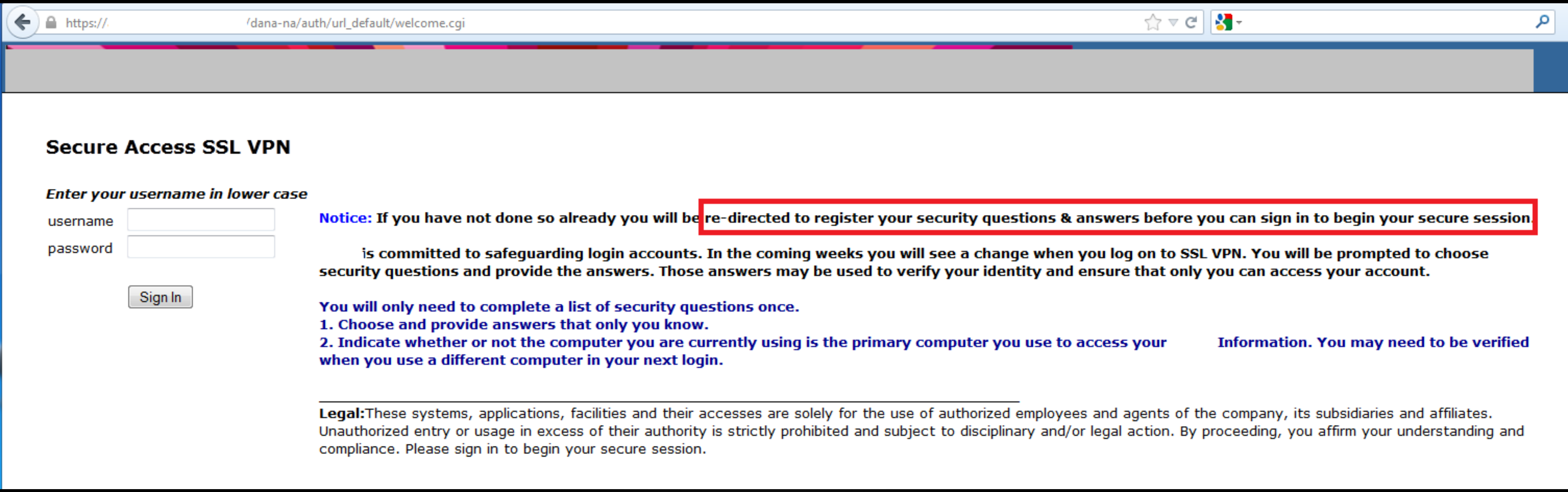
Authentication Required

password are being requested by http:[redacted]e site says: "MS"

Cancel | OK

JUNIPER SECRET QUESTION BYPASS

- Is the below a dead end or a way in?



https:// /dana-na/auth/url_default/welcome.cgi

Secure Access SSL VPN

Enter your username in lower case

username

password

Notice: If you have not done so already you will be re-directed to register your security questions & answers before you can sign in to begin your secure session.

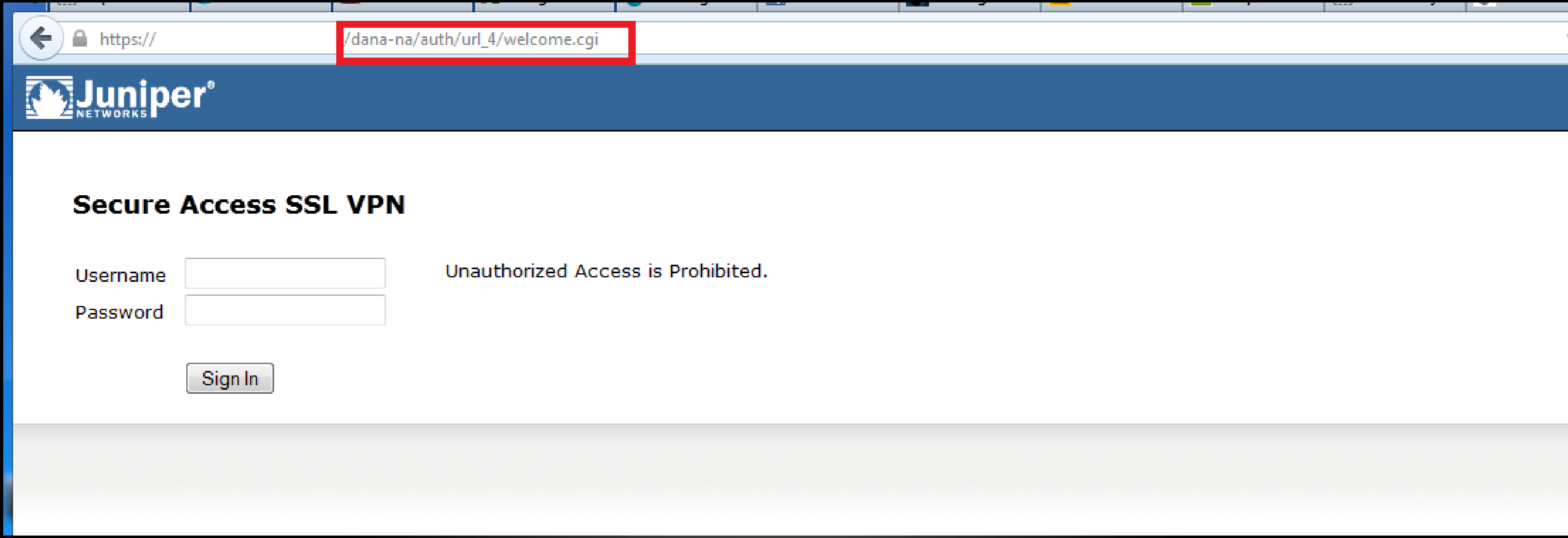
is committed to safeguarding login accounts. In the coming weeks you will see a change when you log on to SSL VPN. You will be prompted to choose security questions and provide the answers. Those answers may be used to verify your identity and ensure that only you can access your account.

You will only need to complete a list of security questions once.
1. Choose and provide answers that only you know.
2. Indicate whether or not the computer you are currently using is the primary computer you use to access your Information. You may need to be verified when you use a different computer in your next login.

Legal: These systems, applications, facilities and their accesses are solely for the use of authorized employees and agents of the company, its subsidiaries and affiliates. Unauthorized entry or usage in excess of their authority is strictly prohibited and subject to disciplinary and/or legal action. By proceeding, you affirm your understanding and compliance. Please sign in to begin your secure session.

JUNIPER SECRET QUESTION BYPASS

- Is the below a dead end or a way in?
- **How about now?**



https:// /dana-na/auth/url_4/welcome.cgi

Secure Access SSL VPN

Username

Password

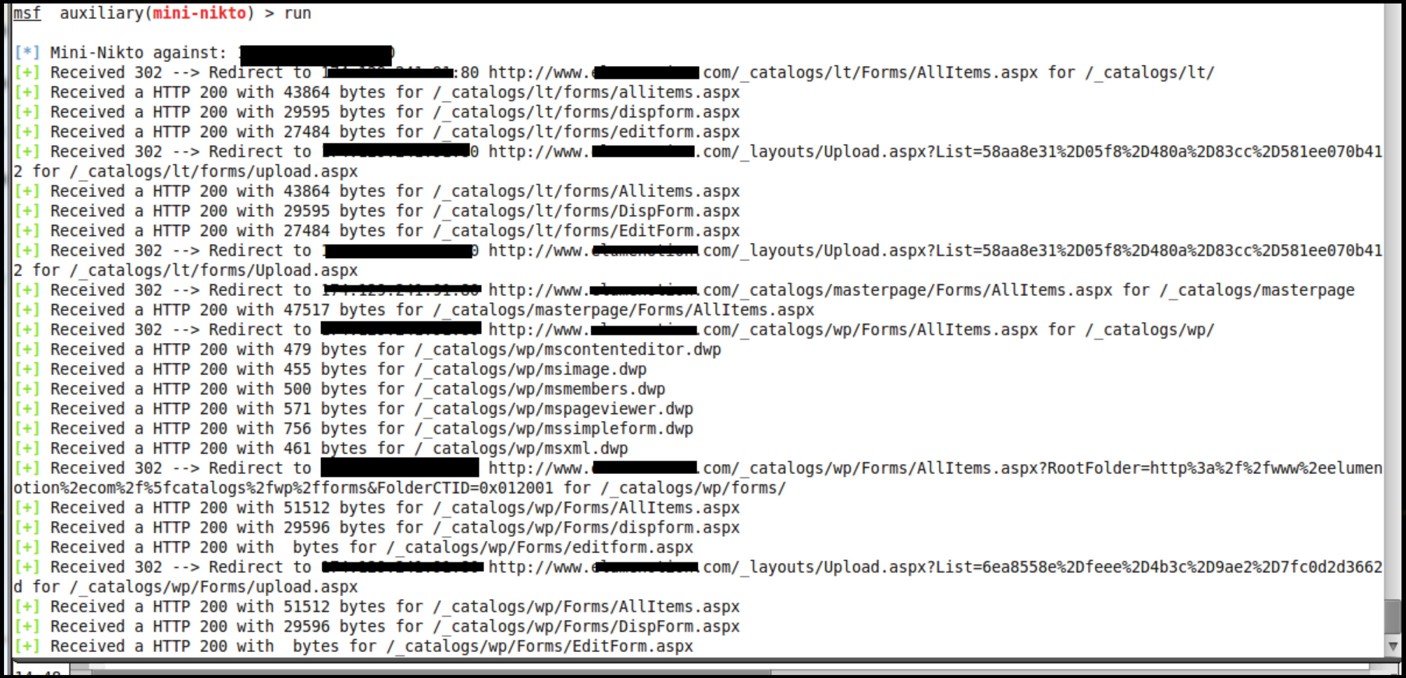
Unauthorized Access is Prohibited.

SHAREPOINT VALUE

- Misconfigured SharePoint can be *really* useful
  - User/Domain Enumeration
  - Access to useful files
- Authenticated access to SharePoint is *always* useful
  - That’s really another talk…but its mint
  - Go ask Nickerson

SHAREPOINT INTEL HUNTING

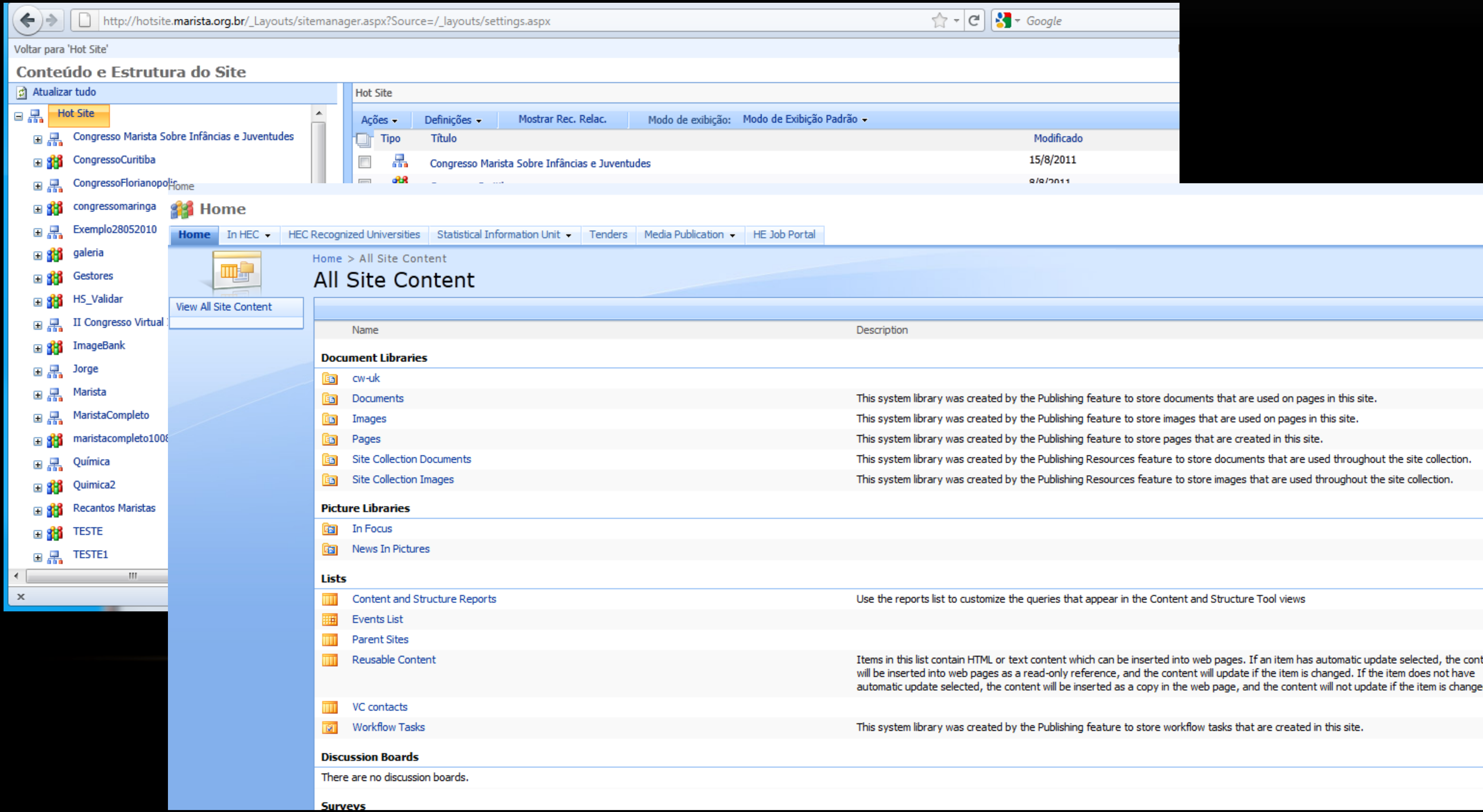
- Stach and Liu's SharePoint Diggity tools
  - http://www.stachliu.com/resources/tools/sharepoint-hacking-diggity-project/
- Roll your own
  - http://code.google.com/p/fuzzdb/source/browse/trunk/Discovery/PredictableRes/Sharepoint.fuzz.txt



```
msf  auxiliary(mini-nikto) > run

[*] Mini-Nikto against: [redacted]
[+] Received 302 --> Redirect to [redacted]:80 http://www.[redacted] com/_catalogs/lt/Forms/AllItems.aspx for /_catalogs/lt/
[+] Received a HTTP 200 with 43864 bytes for /_catalogs/lt/forms/allitems.aspx
[+] Received a HTTP 200 with 29595 bytes for /_catalogs/lt/forms/dispform.aspx
[+] Received a HTTP 200 with 27484 bytes for /_catalogs/lt/forms/editform.aspx
[+] Received 302 --> Redirect to [redacted] http://www.[redacted].com/_layouts/Upload.aspx?List=58aa8e31%2D05f8%2D480a%2D83cc%2D581ee070b41
2 for /_catalogs/lt/forms/upload.aspx
[+] Received a HTTP 200 with 43864 bytes for /_catalogs/lt/forms/Allitems.aspx
[+] Received a HTTP 200 with 29595 bytes for /_catalogs/lt/forms/DispForm.aspx
[+] Received a HTTP 200 with 27484 bytes for /_catalogs/lt/forms/EditForm.aspx
[+] Received 302 --> Redirect to [redacted] http://www.[redacted] com/_layouts/Upload.aspx?List=58aa8e31%2D05f8%2D480a%2D83cc%2D581ee070b41
2 for /_catalogs/lt/forms/Upload.aspx
[+] Received 302 --> Redirect to [redacted] http://www.[redacted].com/_catalogs/masterpage/Forms/AllItems.aspx for /_catalogs/masterpage
[+] Received a HTTP 200 with 47517 bytes for /_catalogs/masterpage/Forms/AllItems.aspx
[+] Received 302 --> Redirect to [redacted] http://www.[redacted] com/_catalogs/wp/Forms/AllItems.aspx for /_catalogs/wp/
[+] Received a HTTP 200 with 479 bytes for /_catalogs/wp/mscontenteditor.dwp
[+] Received a HTTP 200 with 455 bytes for /_catalogs/wp/msimage.dwp
[+] Received a HTTP 200 with 500 bytes for /_catalogs/wp/msmembers.dwp
[+] Received a HTTP 200 with 571 bytes for /_catalogs/wp/mspageviewer.dwp
[+] Received a HTTP 200 with 756 bytes for /_catalogs/wp/mssimpleform.dwp
[+] Received a HTTP 200 with 461 bytes for /_catalogs/wp/msxml.dwp
[+] Received 302 --> Redirect to [redacted] http://www.[redacted] com/_catalogs/wp/Forms/AllItems.aspx?RootFolder=http%3a%2f%2fwww%2eelumen
otion%2ecom%2f%5fcatalogs%2fwp%2fforms&FolderCTID=0x012001 for /_catalogs/wp/forms/
[+] Received a HTTP 200 with 51512 bytes for /_catalogs/wp/Forms/AllItems.aspx
[+] Received a HTTP 200 with 29596 bytes for /_catalogs/wp/Forms/dispform.aspx
[+] Received a HTTP 200 with  bytes for /_catalogs/wp/Forms/editform.aspx
[+] Received 302 --> Redirect to [redacted] http://www.[redacted] com/_layouts/Upload.aspx?List=6ea8558e%2Dfeee%2D4b3c%2D9ae2%2D7fc0d2d3662
d for /_catalogs/wp/Forms/upload.aspx
[+] Received a HTTP 200 with 51512 bytes for /_catalogs/wp/Forms/AllItems.aspx
[+] Received a HTTP 200 with 29596 bytes for /_catalogs/wp/Forms/DispForm.aspx
[+] Received a HTTP 200 with  bytes for /_catalogs/wp/Forms/EditForm.aspx
```

SHAREPOINT

- Open Access



http://hotsite.marista.org.br/_Layouts/sitemanager.aspx?Source=/_layouts/settings.aspx
Google
Voltar para 'Hot Site'

Conteúdo e Estrutura do Site

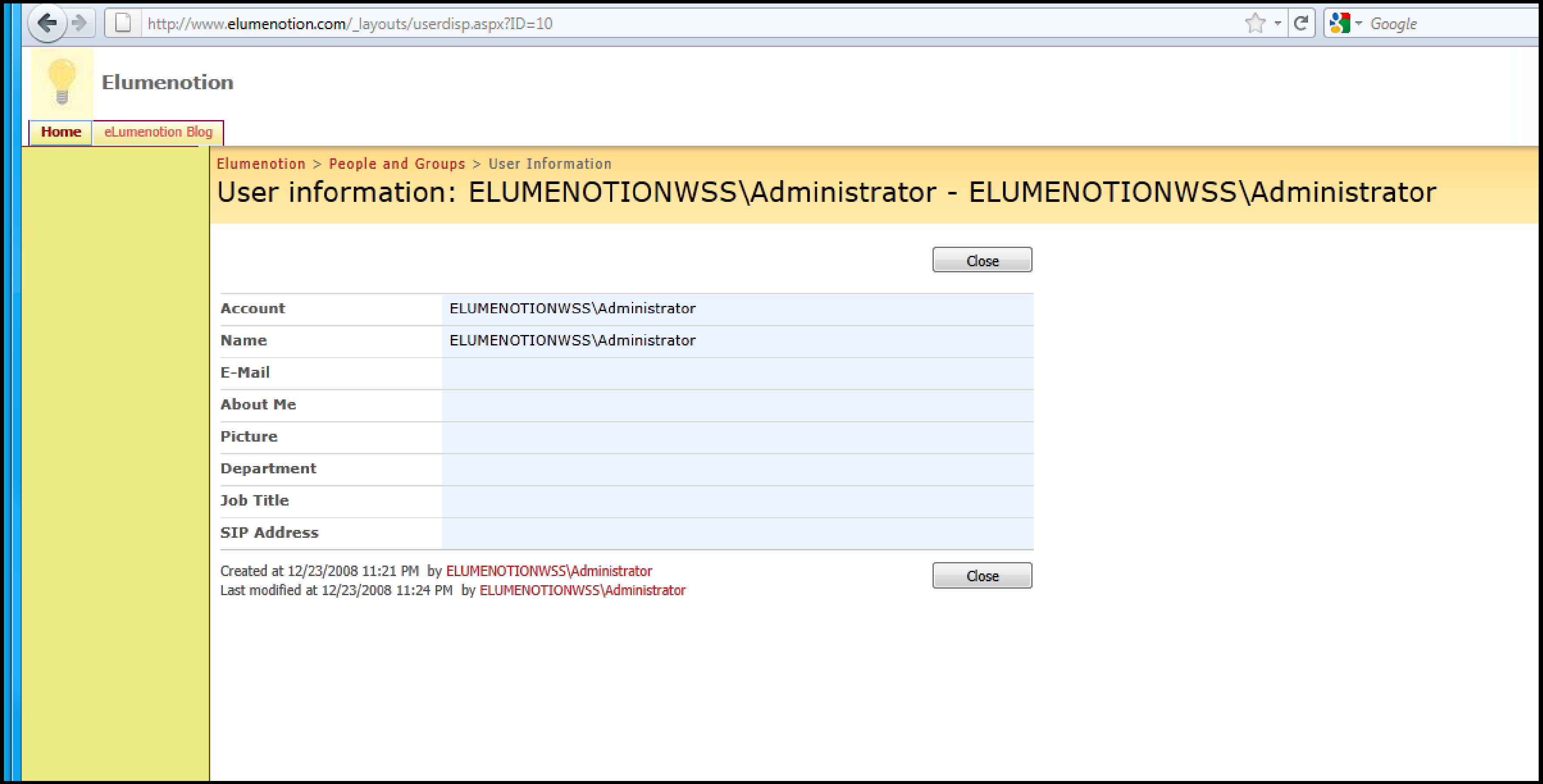
Tipo	Título	Modificado
	Congresso Marista Sobre Infâncias e Juventudes	15/8/2011

All Site Content

Name	Description
Document Libraries	
cw-uk	
Documents	This system library was created by the Publishing feature to store documents that are used on pages in this site.
Images	This system library was created by the Publishing feature to store images that are used on pages in this site.
Pages	This system library was created by the Publishing feature to store pages that are created in this site.
Site Collection Documents	This system library was created by the Publishing Resources feature to store documents that are used throughout the site collection.
Site Collection Images	This system library was created by the Publishing Resources feature to store images that are used throughout the site collection.
Picture Libraries	
In Focus	
News In Pictures	
Lists	
Content and Structure Reports	Use the reports list to customize the queries that appear in the Content and Structure Tool views
Events List	
Parent Sites	
Reusable Content	Items in this list contain HTML or text content which can be inserted into web pages. If an item has automatic update selected, the cont will be inserted into web pages as a read-only reference, and the content will update if the item is changed. If the item does not have automatic update selected, the content will be inserted as a copy in the web page, and the content will not update if the item is change
VC contacts	
Workflow Tasks	This system library was created by the Publishing feature to store workflow tasks that are created in this site.
Discussion Boards	
There are no discussion boards.	
Surveys	

SHAREPOINT

- User Enumeration



http://www.elumenotion.com/_layouts/userdisp.aspx?ID=10
Google
Elumenotion
Home
eLumenotion Blog
Elumenotion > People and Groups > User Information

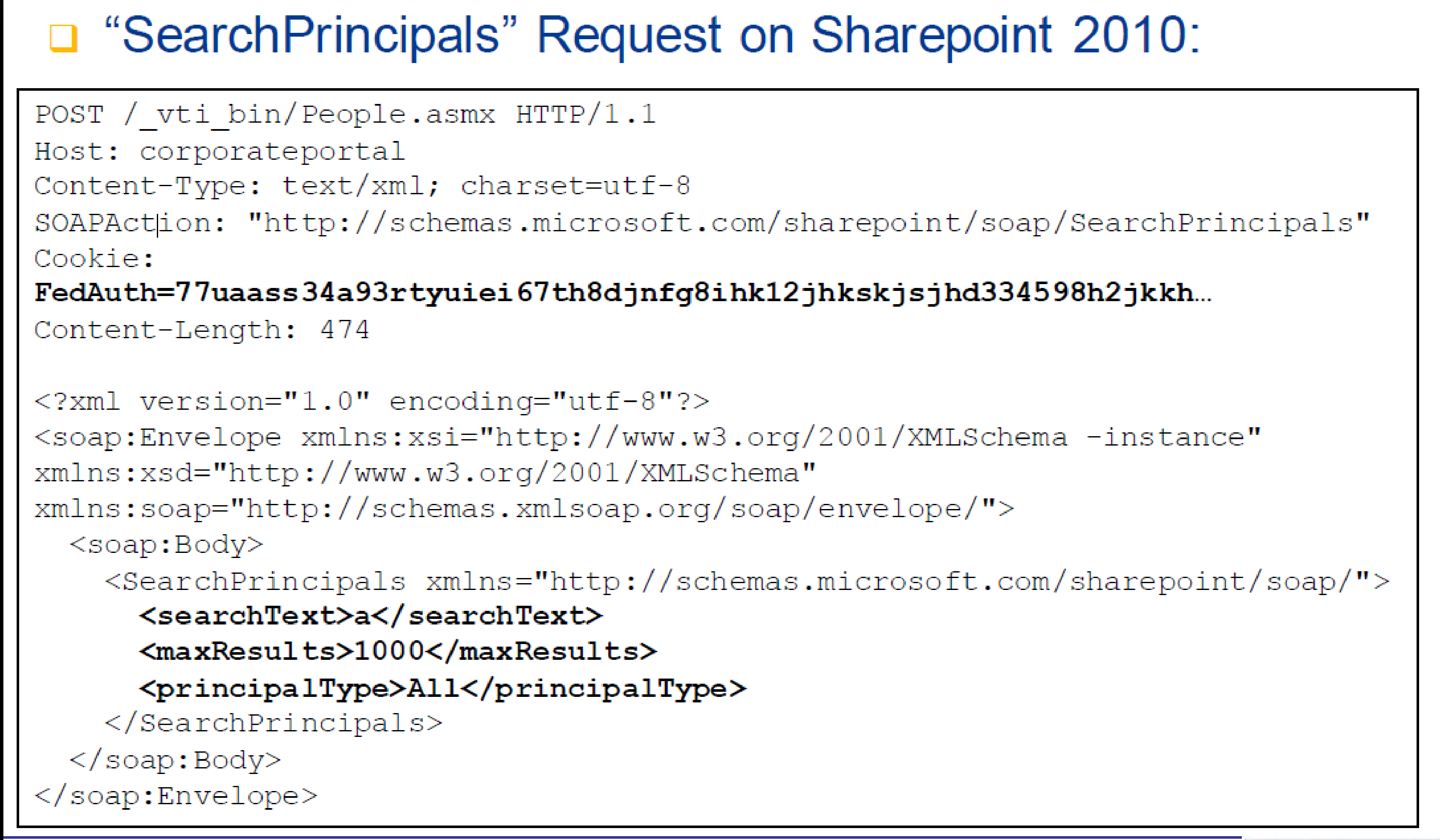
User information: ELUMENOTIONWSS\Administrator - ELUMENOTIONWSS\Administrator

Account	ELUMENOTIONWSS\Administrator
Name	ELUMENOTIONWSS\Administrator
E-Mail	
About Me	
Picture	
Department	
Job Title	
SIP Address	

Created at 12/23/2008 11:21 PM by ELUMENOTIONWSS\Administrator
Last modified at 12/23/2008 11:24 PM by ELUMENOTIONWSS\Administrator

SHAREPOINT

- Can (ab)use web services calls to get account info

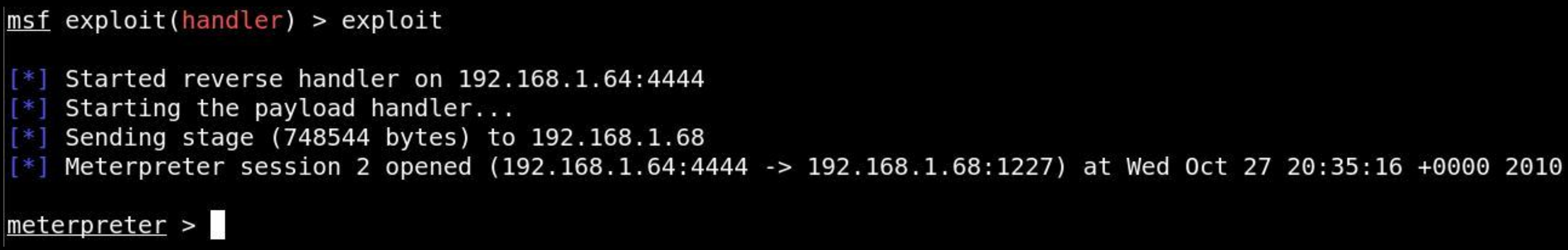


❑ “SearchPrincipals” Request on Sharepoint 2010:

```
POST /_vti_bin/People.asmx HTTP/1.1
Host: corporateportal
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://schemas.microsoft.com/sharepoint/soap/SearchPrincipals"
Cookie:
FedAuth=77uaass34a93rtyuiei67th8djnfg8ihk12jhkskjsjhd334598h2jkkh…
Content-Length: 474

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema -instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <SearchPrincipals xmlns="http://schemas.microsoft.com/sharepoint/soap/">
      <searchText>a</searchText>
      <maxResults>1000</maxResults>
      <principalType>All</principalType>
    </SearchPrincipals>
  </soap:Body>
</soap:Envelope>
```

INTERNAL PWNAGE

- Now what?



```
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.64:4444
[*] Starting the payload handler...
[*] Sending stage (748544 bytes) to 192.168.1.68
[*] Meterpreter session 2 opened (192.168.1.64:4444 -> 192.168.1.68:1227) at Wed Oct 27 20:35:16 +0000 2010

meterpreter > 
```

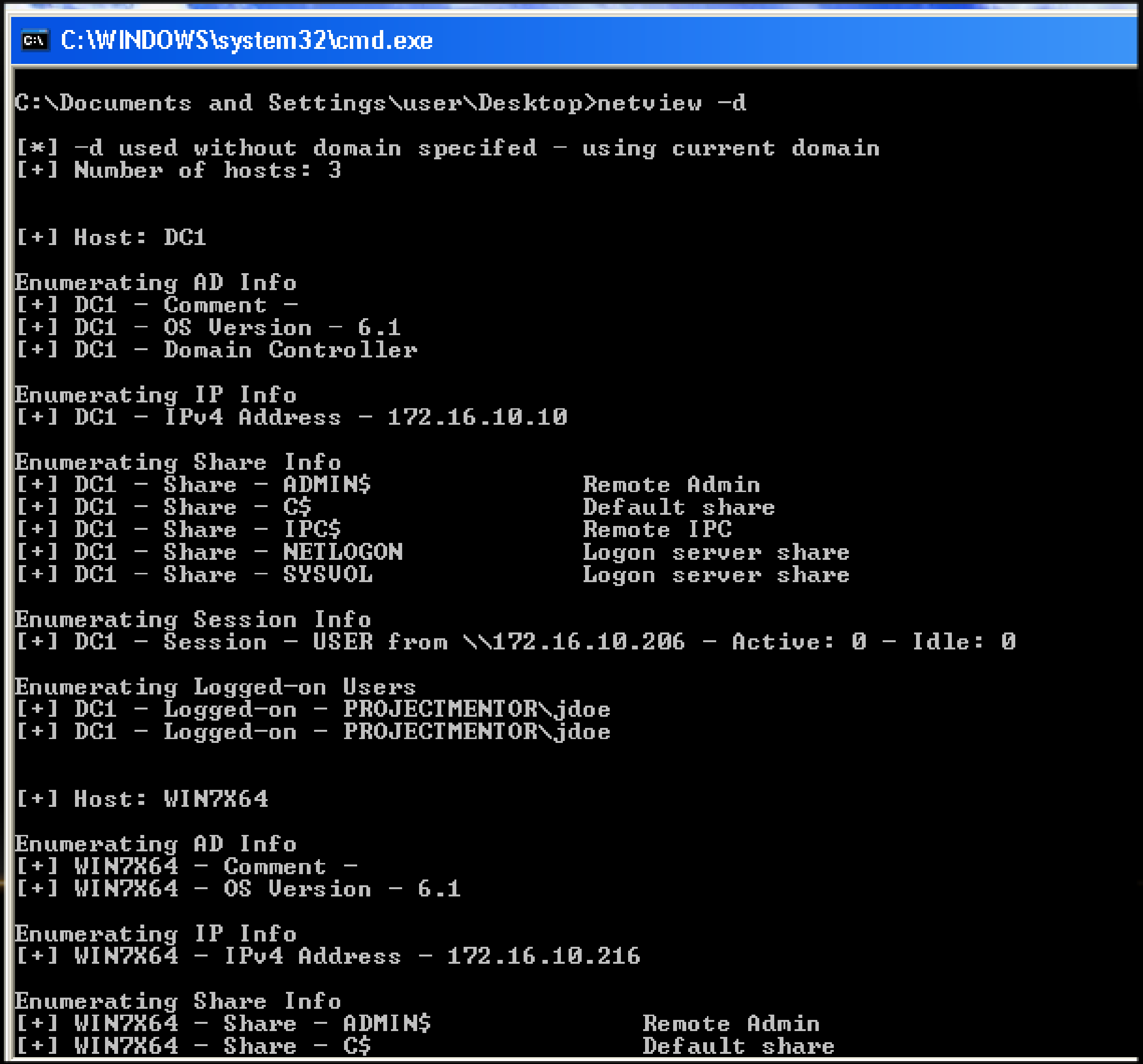
- If you think you are done. You’ve missed the point!

DOMAIN ENUMERATION (OLD SCHOOL)

- Ipconfig/ifconfig
- Tells you:
  - Dual homed?
  - Ipv6?
  - Domain Controllers/Domain Name(s)
- Net commands
  - Still works most of the time
  - Disabled? Use dsquery/dsget
- Internal Zone Transfers

DOMAIN ENUMERATION (NEW SCHOOL)

- Mubix's netview



```
C:\Documents and Settings\user\Desktop>netview -d

[*] -d used without domain specifed - using current domain
[+] Number of hosts: 3


[+] Host: DC1

Enumerating AD Info
[+] DC1 - Comment -
[+] DC1 - OS Version - 6.1
[+] DC1 - Domain Controller

Enumerating IP Info
[+] DC1 - IPv4 Address - 172.16.10.10

Enumerating Share Info
[+] DC1 - Share - ADMIN$              Remote Admin
[+] DC1 - Share - C$                  Default share
[+] DC1 - Share - IPC$                Remote IPC
[+] DC1 - Share - NETLOGON            Logon server share
[+] DC1 - Share - SYSVOL              Logon server share

Enumerating Session Info
[+] DC1 - Session - USER from \\172.16.10.206 - Active: 0 - Idle: 0

Enumerating Logged-on Users
[+] DC1 - Logged-on - PROJECTMENTOR\jdoe
[+] DC1 - Logged-on - PROJECTMENTOR\jdoe


[+] Host: WIN7X64

Enumerating AD Info
[+] WIN7X64 - Comment -
[+] WIN7X64 - OS Version - 6.1

Enumerating IP Info
[+] WIN7X64 - IPv4 Address - 172.16.10.216

Enumerating Share Info
[+] WIN7X64 - Share - ADMIN$              Remote Admin
[+] WIN7X64 - Share - C$                  Default share
```

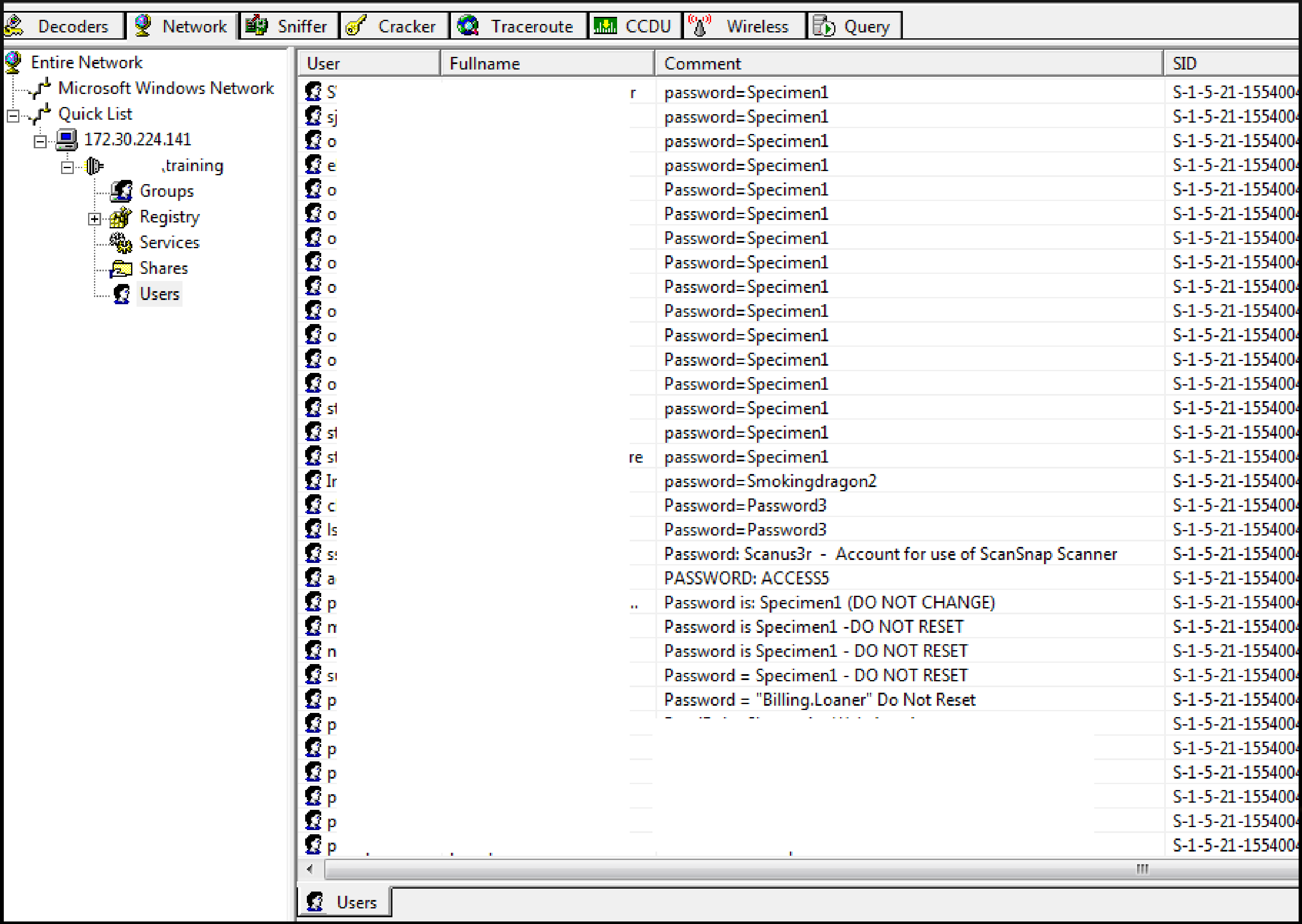
DOMAIN ENUMERATION

- Subnets with DC’s are usually the server / production subnets
- You at least have a quick starting point for looking for low hanging fruit.
- Net view /domain:DOMAINNAME
- Dsquery/dsget
  - Windows server
  - dsquery * -scope subtree -attr "cn" "operatingSystem" "operatingSystemServicePack" -filter "(&(objectclass=computer)(objectcategory=computer)(operatingSystem=Windows Server*))" -limit 0 > mylist.txt
  - Window XP
  - dsquery * -scope subtree -attr "cn" "operatingSystem" "operatingSystemServicePack" -filter "(&(objectclass=computer)(objectcategory=computer)(operatingSystem=Windows XP*))" -limit 0 > mylist.txt

USER ENUMERATION

- Net commands
  - Net user /domain
- Dsquery | dsget
  - List users and comments
  - dsquery user “DC=company,DC=NET" -limit 0 | dsget user -samid -display -desc > company-user-and-comments.txt
- Metasploit Aux modules
  - use auxiliary/scanner/smb/smb_enumusers
  - use auxiliary/scanner/smb/smb_enumusers_domain
- Cain still works great
  - Plus gives you nuggets of gold like…

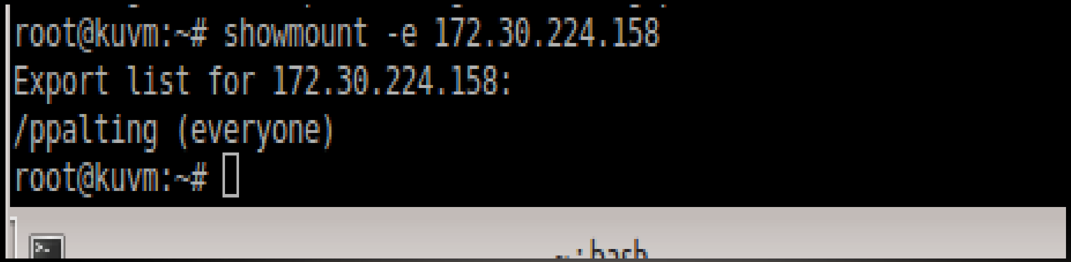
USER COMMENT FIELDS



User	Fullname	Comment	SID
S	r	password=Specimen1	S-1-5-21-155400
sj		password=Specimen1	S-1-5-21-155400
o		password=Specimen1	S-1-5-21-155400
e		password=Specimen1	S-1-5-21-155400
o		Password=Specimen1	S-1-5-21-155400
o		Password=Specimen1	S-1-5-21-155400
o		Password=Specimen1	S-1-5-21-155400
o		Password=Specimen1	S-1-5-21-155400
o		Password=Specimen1	S-1-5-21-155400
o		Password=Specimen1	S-1-5-21-155400
o		Password=Specimen1	S-1-5-21-155400
o		Password=Specimen1	S-1-5-21-155400
o		Password=Specimen1	S-1-5-21-155400
st		password=Specimen1	S-1-5-21-155400
st		password=Specimen1	S-1-5-21-155400
st	re	password=Specimen1	S-1-5-21-155400
Ir		password=Smokingdragon2	S-1-5-21-155400
c		Password=Password3	S-1-5-21-155400
ls		Password=Password3	S-1-5-21-155400
s:		Password: Scanus3r - Account for use of ScanSnap Scanner	S-1-5-21-155400
a		PASSWORD: ACCESS5	S-1-5-21-155400
p	..	Password is: Specimen1 (DO NOT CHANGE)	S-1-5-21-155400
n		Password is Specimen1 -DO NOT RESET	S-1-5-21-155400
n		Password is Specimen1 - DO NOT RESET	S-1-5-21-155400
s		Password = Specimen1 - DO NOT RESET	S-1-5-21-155400
p		Password = "Billing.Loaner" Do Not Reset	S-1-5-21-155400
p			S-1-5-21-155400
p			S-1-5-21-155400
p			S-1-5-21-155400
p			S-1-5-21-155400
p			S-1-5-21-155400
p			S-1-5-21-155400

OPEN NFS SHARES

- Exported home directories
- Server names
- Usernames
- Passwords?
- Backup files
- Showmount -e



```
root@kuvm:~# showmount -e 172.30.224.158
Export list for 172.30.224.158:
/ppalting (everyone)
root@kuvm:~# 
```

OPEN SMB SHARES

- You have to look in them to find useful stuff
- Scanner wont tell you that documentX is important
- Metasploit
  - use auxiliary/scanner/smb/smb_enumshares
- Enum.exe
- Loose permissions on file servers
  - World readable user home directories on SAN/NAS devices

FILE MOVEMENT

- Clipboard/Buffer
- Remote Desktop
- Network mapped drives
- External drop sites
  - WebDAV file server
- BITS

MSSQL ENUMERATION

- OSQL -L

MSSQL

```
msf  auxiliary(mssql_ping) > run

[*] SQL Server information for 172.30.0.70:
[+]    ServerName      = RBRLIVE12
[+]    InstanceName    = MSSQLSERVER
[+]    IsClustered     = No
[+]    Version         = 8.00.194
[+]    tcp             = 1433
[+]    np              = \\RBRLIVE12\pipe\sql\query
[*] SQL Server information for 172.30.0.162:
[+]    ServerName      = LOGISTICS02
[+]    InstanceName    = SQL1
[*] SQL Server information for 172.30.0.185:
[+]    ServerName      = RBRLIVE11
```

ORACLE

- Outdated Oracle on Windows can yield shell
- Can be difficult to get it to play nice with metasploit
- Isqlplus doesn’t honor routes in metasploit

QUICK ELEVATION

- Group Policy Preference Exploit
  - Metasploit Post Module
    - Post/windows/gather/credentials/gpp
- Domain users part of local administrator group
- Similar usernames with Domain Admin accounts
- Password reuse

INTERNAL PWNAGE RECAP

- Resist the urge to scan all things
- Use OSINT and enumeration to your advantage
- DHCP leases are awesome
- Dns zone xfer – what do we learn again from external slides?
- Dig/nslookup domains – reveal server subnets, system naming convention, system role, etc
- Dsquery examples
- Enumeration against systems (enum.exe, dsquery, cain, msf aux, etc)
  - NetBIOS never left

INTERNAL PWNAGE RECAP

- Active Directory comment fields
- SQL enumeration (Cain, dsquery, sqlrecon, msf aux)
  - Be smart about SA account (blank, password, SA, etc.) and lockouts
- Terminal Servers enumeration (Cain, dsquery)
- NFS shares/mounts/info leakage (files, users, server names, etc)
- SVN/CVS entries – access to source code – web.config files – immediate access
- SharePoint – basic user/weak permissions/easy searchable for info to elevate/backups
- Citrix access with basic user – great way to elevate (shown during external slides)
- File servers – weak permissions/easy searching for “password” files, ssh keys, home directories, etc.

POOR MAN’S PERSISTENCE

- Sticky keys / magnifier
- Cat passwords.txt
- Cisco PCF file
- VPN/GRE Tunnel
- All user’s startup
- Pasword1 ☺

THE DOCTOR IS IN

- Are you positive your last assessment was accurate?

- Password auditing
- Data discovery/classification
- System hardening
- Segmentation
- Egress filtering
- Least privilege models