



# Offensive Countermeasures: Making Attackers Lives Miserable

**Paul Asadoorian**

**PaulDotCom**

**John Strand**

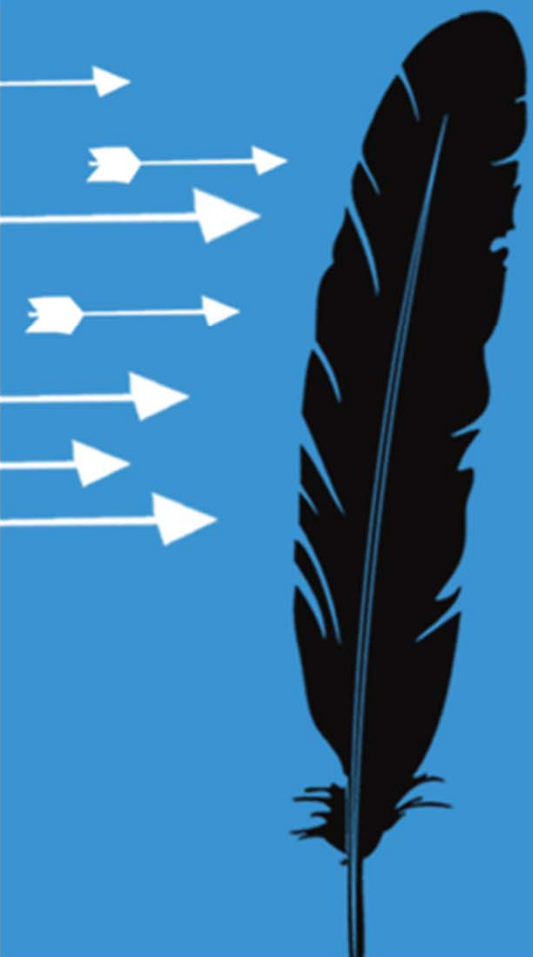
**PaulDotCom, SANS Senior  
Instructor**

Session ID: STAR-303

Session Classification: Intermediate

**RSACONFERENCE2012**

# Offensive Countermeasures



# Goal

- What is the definition of Insanity?
  - “Doing the same thing over and over again and expecting different results.”- Einstein
- Is the security industry insane?
- Maybe we can start making attackers lives difficult
- But, not by doing the same things we have been doing
- Three components:
  - Annoyance
  - Attribution
  - Attack



# Case Study: Consent to University Network Terms

- Sysadmin hacks into threatening machine
  - Gathered evidence used against student using temp/temp creds
  - Student's consent to university terms justifies sysadmin
  - U.S. v. Heckenkamp
- Kevin Poulsen, "Court Okays Counter-Hack of eBay Hacker's Computer," Threat Level, April 6, 2007,
  - [http://blog.wired.com/27bstroke6/2007/04/court\\_okays\\_cou.html](http://blog.wired.com/27bstroke6/2007/04/court_okays_cou.html)

*"A federal appeals court just shot down an attempt by confessed superhacker Jerome Heckenkamp to overturn his computer crime convictions, which were an end result of information provided by a university sysadmin who broke into Heckenkamp's computer to gather evidence."*



# Case Study: MSFT Court Order - Botnet

- Civil lawsuit 2010
- Court issues order to suspend the domains associated with the Waledac botnet
- MSFT takes “other technical measures” to degrade the botnet
  - [www.google.com/buzz/benwright214/PcJTmLbEwit/Cyber-Defense-Law-Botnet-Computer-Crime-Lawsuit](http://www.google.com/buzz/benwright214/PcJTmLbEwit/Cyber-Defense-Law-Botnet-Computer-Crime-Lawsuit)

*“Notice that Microsoft is not doing this in the dark. It is working through our open public court system, so that Microsoft is transparent and accountable and all can see what is happening and evaluate it.”*



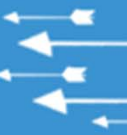
# Let's Pretend I'm a Lawyer

- I'm advising you to:
  - Discuss
  - Document
  - Plan
- **Consult with others, reveal your plans!**
- Hiding intentions means you think what you are doing is "wrong"
- Rule of thumb: Don't be evil
  - While it can seem like a lot of fun, it can get you in big trouble



# Okay, Let's Stop Pretending

- Could this get you into trouble?
  - Possibly. There is still some debate on how to do it properly
- There are a few things we can avoid to keep us from getting in trouble
  - Don't ever put malware where it is publicly accessible
  - Don't make it too easy to get to
- Use warning banners...



# Look at Your Warning Banner

- There is a lot in there about permission
- There are a number of technologies that will “check” your system before it accesses the network
  - OpenVPN scripts (Like a NAC Check)
  - Windows 2008 Network Access Protection
- Is it possible to use this as a means to gather some information about an attacker system?
- Put in your warning banner that you can do what you want!



# Example: Eric Needed a Warning Banner

- What does a kitchen knife, a crutch, and ductape have to do with anything?
- It is illegal to set up lethal traps for trespassers
- However, if you tell them there may be evil things on your network/property you warned them

"super went to open the door, felt resistance and found the rigged contraption"-- a big knife duct-taped to a crutch, which was installed with an elastic cord. The super was not injured.

Eric Stetz was arrested and charged with reckless endangerment for a vicious-looking booby trap.

[http://gothamist.com/2008/04/06/homemade\\_booby.php](http://gothamist.com/2008/04/06/homemade_booby.php)



**WARNING:** There is a knife duct taped to a crutch attached to an elastic band. Enter at your own risk!

- Would this have kept Eric Stetz out of trouble?



# FREE VASECTOMY

- This likely would not have kept Eric Stetz out of trouble...



# Annoyance



- Stressing out the attackers...



# Annoyance: HoneyPorts

- Forces attackers to make a full connection to avoid spoofing pitfalls
- Attackers and testers hate this...



```
@echo off for /L %%i in (1,1,1) do @for /f
"tokens=3" %%j in ('netstat -nao ^| find
^":3333^"' ) do@for /f "tokens=1 delims=:" %%k in
("%%j") do netsh advfirewall firewall add
rulename="WTF" dir=in remoteip=%%k localport=any
protocol=TCP action=block
```





# Annoyance: HoneyPorts

- Works on Linux too of course, same concept
- Must have working copy of Netcat on your system
- Should be modified to log entries and report back to enterprise SIEM

```
[root@linux ~]# while [ 1 ] ; echo "started" ;  
do IP=`nc -v -l -p 2222 2>&1 1> /dev/null |  
grep from | cut -d[ -f 3 | cut -d] -f 1`;  
iptables -A INPUT -p tcp -s ${IP} -j DROP ;  
done
```



# Infinitely Recursive Directories

Can seriously mess  
up an attacker's day

Can also crash some  
services

Possibly Backups

Possibly...

Special thanks to  
Mark Baggett

Did we mention he is  
smart and sexy?



What Mark Baggett may look like

# How to do it in Windows

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\John>cd \

C:\>mkdir \goaway

C:\>cd goaway
```

```
C:\goaway>mklink /D dir1 c:\goaway\
symbolic link created for dir1 <==>> c:\goaway\
```

[illegible]

```
C:\goaway>mklink /D dir2 c:\goaway\
```

# Effect?

## Dir /S will continue forever

# The S is for recurSSSSSive

# Hello Ed Skoudis...

# Metrepreter will continue for ever

Or until you kill it on the victim

# Whichever comes first

Even if the session is killed  
Which can be kind of  
annoying

[illegible]

# Annoyance: Setting Traps

***THIS LOOKS LIKE A TRAP***



***I CAN TELL FROM SEEING  
QUITE A FEW TRAPS IN MY TIME***



# SpiderTrap & WebLabyrinth

- Spidertrap: Small Python script to trap web spiders
- Ben Jackson created a PHP version called WebLabyrinth
- It is PHP so you can load it in your web infrastructure
- Has a number of cool features
  - Gently tells Googlebot to go away
  - Random HTTP codes
  - **\*NEW\*** Database support
  - **\*NEW\*** Alerting with IDS-style rules
- David Bowie Approved



# Keeping it "Real"

```
root@OCM:/var/www/html/labyrinth
File Edit Tabs Help

include_once('config.inc.php');
include_once('labyrinth.inc.php');

if(preg_match("/Google/", $_SERVER['HTTP_USER_AGENT'])){
    header("HTTP/1.0 404 Not Found");
    print "o/~ Whatever you're looking for / Hey! Don't come around here no
    more...";
}

#Randomly generate an error just to "Keep it real"
$error_chance = rand(0,100);

if ($error_chance == 16){
    header("HTTP/1.1 404 Not Found");
}elseif ($error_chance == 23){
    header("HTTP/1.1 403 Forbidden");
}elseif ($error_chance == 42){
    #Included just for the WTF Factor
    header("HTTP/1.1 402 Payment Required");
}

:█
```



# Wget: Falling into the Trap

```
root@OCM:/var/www/html/labyrinth
File Edit Tabs Help
[root@OCM labyrinth]# wget -r http://127.0.0.1/labyrinth
--2011-01-18 09:25:43-- http://127.0.0.1/labyrinth/ODM5MDYyNg/MTk4MzEzOTY
Connecting to 127.0.0.1:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3448 (3.4K) [text/html]
Saving to: "127.0.0.1/labyrinth/ODM5MDYyNg/MTk4MzEzOTY"

100%[=====>] 3,448      --.-K/s   in 0s

2011-01-18 09:25:43 (478 MB/s) - "127.0.0.1/labyrinth/ODM5MDYyNg/MTk4MzEzOTY" s
aved [3448/3448]

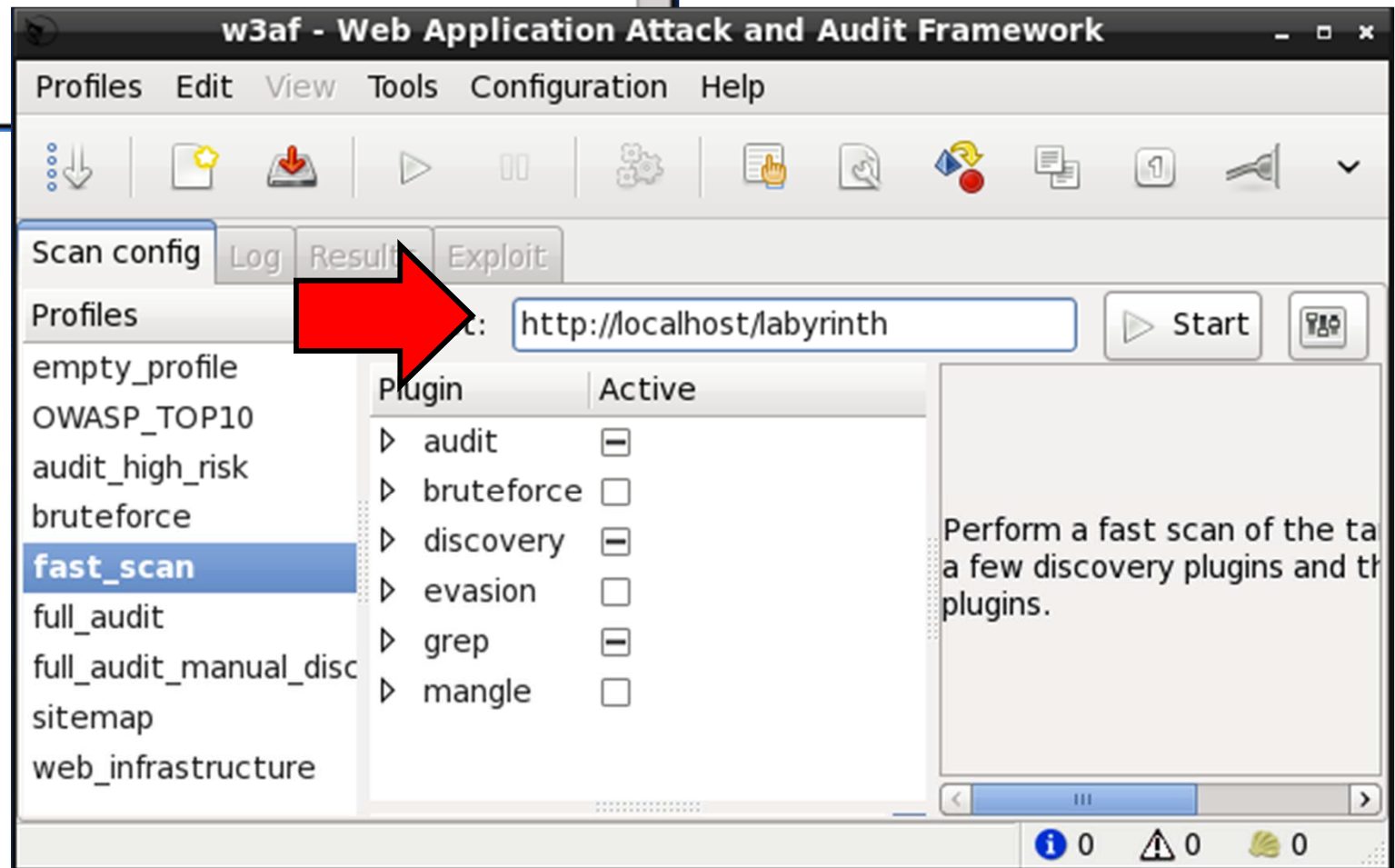
--2011-01-18 09:25:43-- http://127.0.0.1/labyrinth/ODM5MDYyNg/MTExMTQ1NQ
Connecting to 127.0.0.1:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2983 (2.9K) [text/html]
Saving to: "127.0.0.1/labyrinth/ODM5MDYyNg/MTExMTQ1NQ"

100%[=====>] 2,983      --.-K/s   in 0s
```

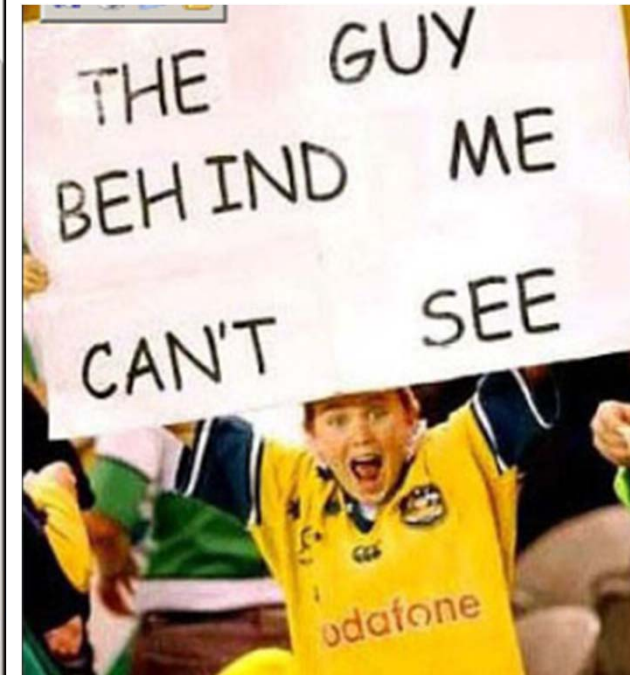
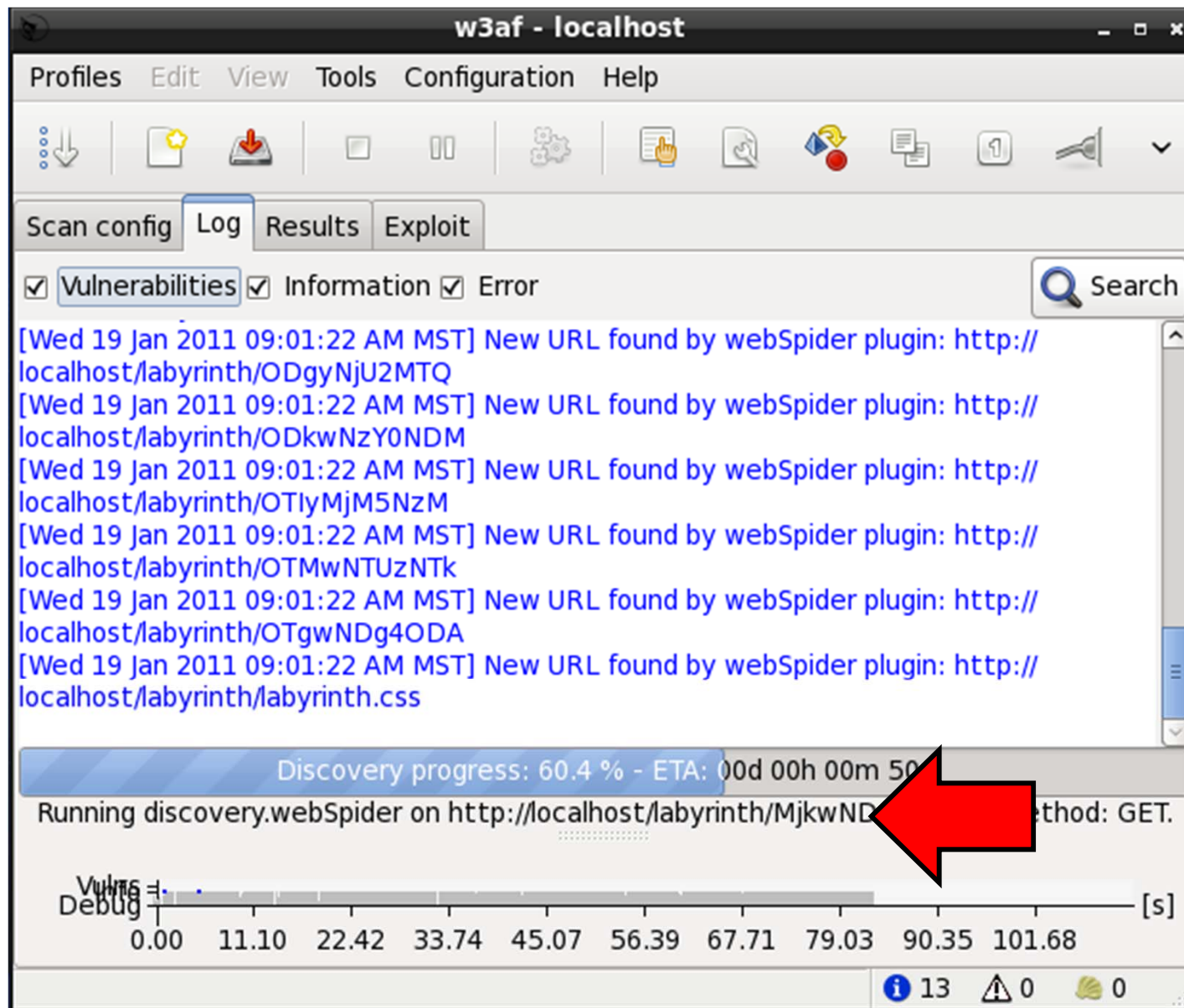


# Now for W3AF

```
student@OCM:~/tools/w3af
File Edit Tabs Help
[student@OCM ~]$ cd /home/student/tools/w3af/
[student@OCM w3af]$
[student@OCM w3af]$ ./w3af_gui
```



# This is Going to Take a While...



# Attribution



- I can still see you...



# Word Web-Bugs

- Feature built into exploit frameworks for penetration testing
- This tactic works great at tracking intellectual property
- Not all ways of attribution need to result in shell access
- Far less likely to crash a system
- Embed this code in a spreadsheet called SSN.xls and watch how fast an attacker runs the macros
- Callback should go to a closely monitored system

**This is like Spy Stuff,  
like James Bond...**

**“Ohhhhhh James...”**



# How Does it Work?

- It simply inserts a reference to a css running on the system, in this case, running Core IMPACT
- When the doc is opened it tries to open the URL
- Direct connection!

-----  
Request received from 192.168.123.156:

- GET /rpt/766f30a860603cea/ONLOADWINDOWsljhObIHAMf4rpRrFmpsLAaa/  
ntlm.css HTTP/1.1

- Request time: Wed May 12 06:34:43 2010

- Request headers:

Accept: \*/\*

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0;  
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media  
Center PC 6.0; MSOffice 12)

Accept-Encoding: gzip, deflate

Host: 192.168.123.159

Connection: Keep-Alive  
-----

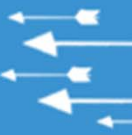


# Attribution: Decloak

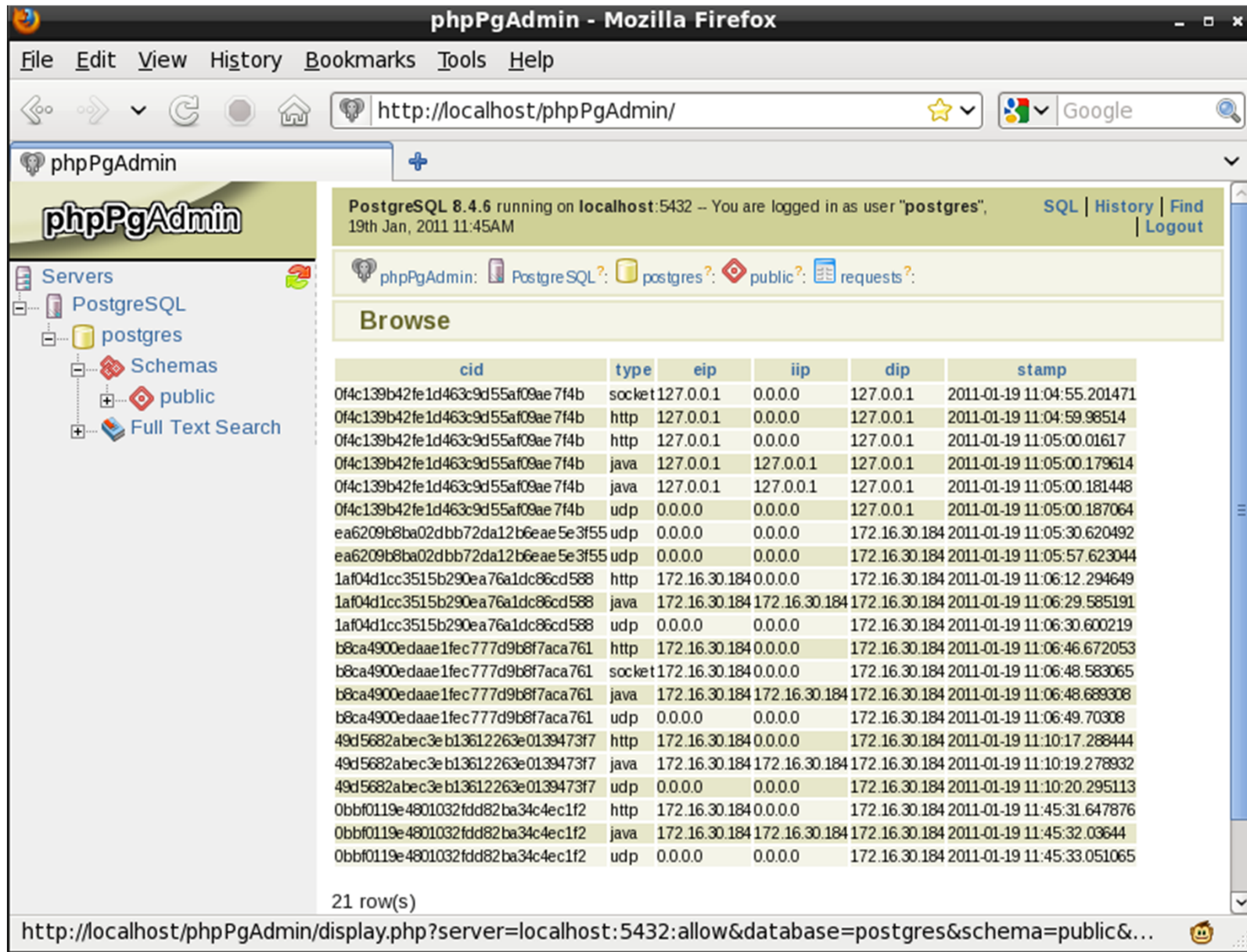
- From the Metasploit project
  - More information  
<http://decloak.net/>
  - Great place to redirect users from robots.txt
  - Many attackers and penetration testers will use proxies and/or Tor to hide their IP address
  - Decloak can reveal the real IP address of the scanner



*“This tool demonstrates a system for identifying the real IP address of a web user, regardless of proxy settings, using a combination of client-side technologies and custom services.”*



# Viewing the Data



The screenshot shows the phpPgAdmin web interface in a Mozilla Firefox browser. The browser's address bar displays `http://localhost/phpPgAdmin/`. The phpPgAdmin interface includes a sidebar with a tree view of the database structure: **Servers** > **PostgreSQL** > **postgres** > **Schemas** > **public**. The main content area shows the status of PostgreSQL 8.4.6 running on localhost:5432, with the user 'postgres' logged in. Below this, a 'Browse' section displays a table of network connections.

cid	type	eip	iip	dip	stamp
0f4c139b42fe1d463c9d55af09ae7f4b	socket	127.0.0.1	0.0.0.0	127.0.0.1	2011-01-19 11:04:55.201471
0f4c139b42fe1d463c9d55af09ae7f4b	http	127.0.0.1	0.0.0.0	127.0.0.1	2011-01-19 11:04:59.98514
0f4c139b42fe1d463c9d55af09ae7f4b	http	127.0.0.1	0.0.0.0	127.0.0.1	2011-01-19 11:05:00.01617
0f4c139b42fe1d463c9d55af09ae7f4b	java	127.0.0.1	127.0.0.1	127.0.0.1	2011-01-19 11:05:00.179614
0f4c139b42fe1d463c9d55af09ae7f4b	java	127.0.0.1	127.0.0.1	127.0.0.1	2011-01-19 11:05:00.181448
0f4c139b42fe1d463c9d55af09ae7f4b	udp	0.0.0.0	0.0.0.0	127.0.0.1	2011-01-19 11:05:00.187064
ea6209b8ba02d5bb72da12b6eae5e3f55	udp	0.0.0.0	0.0.0.0	172.16.30.184	2011-01-19 11:05:30.620492
ea6209b8ba02d5bb72da12b6eae5e3f55	udp	0.0.0.0	0.0.0.0	172.16.30.184	2011-01-19 11:05:57.623044
1af04d1cc3515b290ea76a1dc86cd588	http	172.16.30.184	0.0.0.0	172.16.30.184	2011-01-19 11:06:12.294649
1af04d1cc3515b290ea76a1dc86cd588	java	172.16.30.184	172.16.30.184	172.16.30.184	2011-01-19 11:06:29.585191
1af04d1cc3515b290ea76a1dc86cd588	udp	0.0.0.0	0.0.0.0	172.16.30.184	2011-01-19 11:06:30.600219
b8ca4900eaae1fec777d9b8f7aca761	http	172.16.30.184	0.0.0.0	172.16.30.184	2011-01-19 11:06:46.672053
b8ca4900eaae1fec777d9b8f7aca761	socket	172.16.30.184	0.0.0.0	172.16.30.184	2011-01-19 11:06:48.583065
b8ca4900eaae1fec777d9b8f7aca761	java	172.16.30.184	172.16.30.184	172.16.30.184	2011-01-19 11:06:48.689308
b8ca4900eaae1fec777d9b8f7aca761	udp	0.0.0.0	0.0.0.0	172.16.30.184	2011-01-19 11:06:49.70308
49d5682abec3eb13612263e0139473f7	http	172.16.30.184	0.0.0.0	172.16.30.184	2011-01-19 11:10:17.288444
49d5682abec3eb13612263e0139473f7	java	172.16.30.184	172.16.30.184	172.16.30.184	2011-01-19 11:10:19.278932
49d5682abec3eb13612263e0139473f7	udp	0.0.0.0	0.0.0.0	172.16.30.184	2011-01-19 11:10:20.295113
0bbf0119e4801032fdd82ba34c4ec1f2	http	172.16.30.184	0.0.0.0	172.16.30.184	2011-01-19 11:45:31.647876
0bbf0119e4801032fdd82ba34c4ec1f2	java	172.16.30.184	172.16.30.184	172.16.30.184	2011-01-19 11:45:32.03644
0bbf0119e4801032fdd82ba34c4ec1f2	udp	0.0.0.0	0.0.0.0	172.16.30.184	2011-01-19 11:45:33.051065

21 row(s)

http://localhost/phpPgAdmin/display.php?server=localhost:5432:allow&database=postgres&schema=public&...



# To Norway!!

Google Bookmark

This page has been translated from Norwegi... to English Show original



# SKATTELISTER.NO

PEOPLE

F.eks: Ola Nordmann Oslo

Search

[Click here for advanced search](#)

SEE CHARTS

Zip:  View

Year of birth:  View

County: All Norway View

Original Text:

Søk

[Show alternative trans](#)

## AKERSHUS

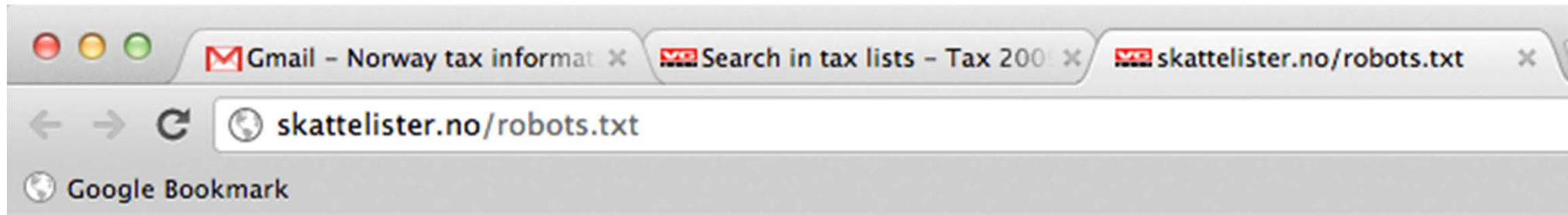
- [Asker](#)
- [Aurskog-Høland](#)
- [Bærum](#)
- [Eidsvold](#)
- [Enebakk](#)
- [Bold](#)
- [Frogn](#)
- [Gjerdrum](#)
- [Hurdal](#)
- [Lørenskog](#)
- [Nannestad](#)
- [Nes](#)
- [Nesodden](#)
- [Nittedal](#)
- [Oppegård](#)
- [Rælingen](#)
- [Skedsmo](#)
- [Ski](#)
- [Sørums](#)
- [Ullensaker](#)
- [Vestby](#)
- [Ås](#)

## AUST-AGDER

- [Arendal](#)
- [Birkirkens](#)
- [Evje and Hornes](#)
- [Froland](#)
- [Iveland](#)
- [Lillesand](#)
- [Valle](#)
- [Vangshol](#)

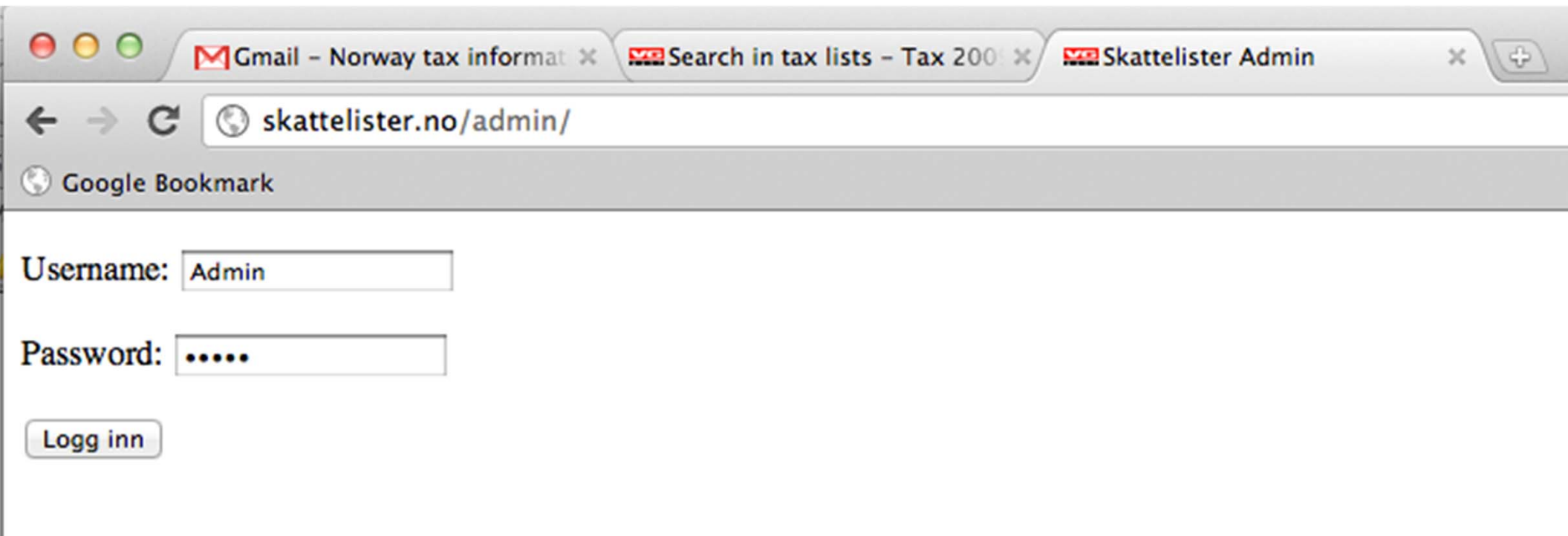


# Where Would You Go?



```
User-agent: *  
Disallow: /admin
```

# You Don't Think?

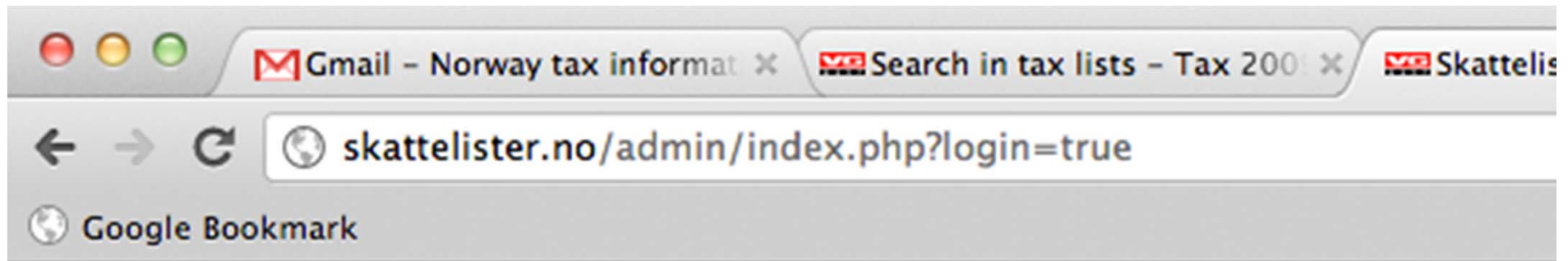


The screenshot shows a web browser window with three tabs: "Gmail - Norway tax informat", "Search in tax lists - Tax 200", and "Skattelister Admin". The address bar shows the URL "skattelister.no/admin/". Below the address bar is a "Google Bookmark" bar. The main content area displays a login form with the following elements:

- A label "Username:" followed by a text input field containing the text "Admin".
- A label "Password:" followed by a password input field containing five dots ".....".
- A button labeled "Logg inn" (Log in) located below the password field.

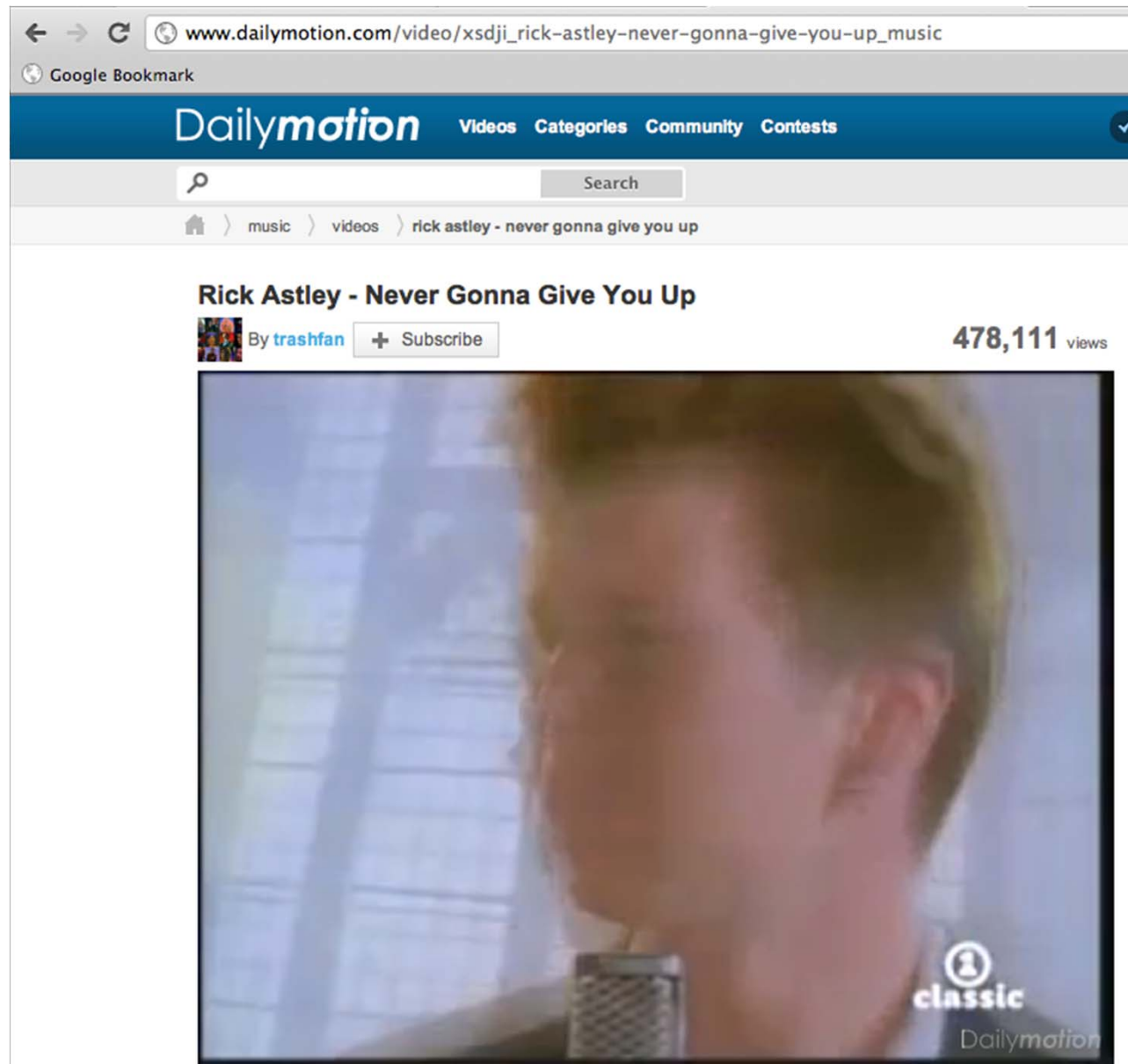


# What the .... Is that?



Trodde du virkelig det skulle være så enkelt?

# Never Going You Give You Up!



# Attack



- Gopher is an old protocol too...



# Attack: Java Payload

- If we can get an attacker to load a Java payload, why not give them something interesting, like a Metasploit payload?
- Java payloads are awesome for penetration testers, no vulnerabilities required!
- They can also be useful for attackers...

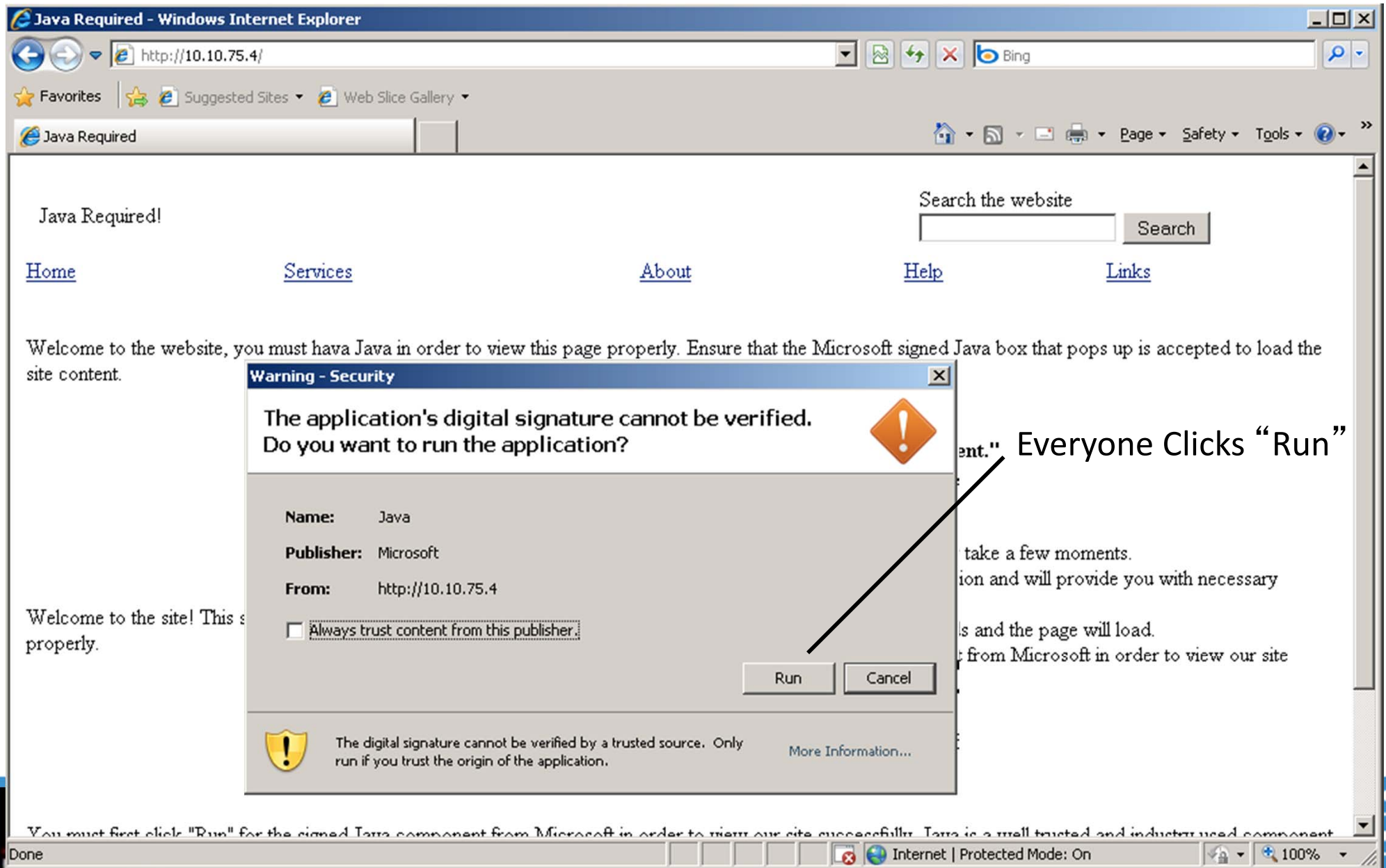


# Evil Java Application

- Embed a malicious Java Application in a non-production web server
  - Usually in a directory that is noindex and/or nofollow in robots.txt
- The attacker/victim will get a pop-up asking if they want to open the Java application
- They will, attackers tend to be very curious
- The payload can be flexible (Shell, Rootkit, VNC)
- You can automatically run enumeration scripts when the attacker/victim runs the application



# Browsing to Your Site



# Not Pretty.. But it Works

```
root@OCM:/opt/set
File Edit Tabs Help
0.19:45762) at Mon Jan 24 10:01:57 -0700 2011
[*] Session ID 23 (172.16.30.213:8081 -> 172.16.30.19:45762) proces
sing AutoRunScript 'migrate -f'
[-] Error: Command shell sessions do not support migration
[*] Sending stage (36 bytes) to 172.16.30.19
[*] Command shell session 24 opened (172.16.30.213:8081 -> 172.16.3
0.19:45764) at Mon Jan 24 10:01:57 -0700 2011
[*] Session ID 24 (172.16.30.213:8081 -> 172.16.30.19:45764) proces
sing AutoRunScript 'migrate -f'
[-] Error: Command shell sessions do not support migration
[*] Command shell session 25 opened (172.16.30.213:8081 -> 172.16.3
0.19:45766) at Mon Jan 24 10:01:57 -0700 2011
[*] Session ID 25 (172.16.30.213:8081 -> 172.16.30.19:45766) proces
sing AutoRunScript 'migrate -f'
[-] Error: Command shell sessions do not support migration
[*] Command shell session 26 opened (172.16.30.213:8081 -> 172.16.3
0.19:45768) at Mon Jan 24 10:01:57 -0700 2011
[*] Session ID 26 (172.16.30.213:8081 -> 172.16.30.19:45768) proces
sing AutoRunScript 'migrate -f'
[-] Error: Command shell sessions do not support migration

msf exploit(handler) > sessions -i 1
```



# Precautions and Usage

- Put this on the inside of the network
- Careful an attacker doesn't redirect your users
- Make sure no one can take over your Metasploit instance
- Don't have to do any thing with the shell
  - You can autorun certain non-damaging commands
  - ping your system
  - Think “security checks”



## ■ Listen

- <http://pauldotcom.com/radio> (24/7)
- Podcast in iTunes (audio/video)

## ■ Watch

- Live! <http://pauldotcom.com/live>
- "TV" <http://pauldotcom.blip.tv>

