Alexander Cannell

CSIS 3650

09/13/2012

Activity 1 Chapter 4:

Using who is on networksolutions.com I got this

Domain Name: MIT.EDU

Registrant:

Massachusetts Institute of Technology

Cambridge, MA 02139

UNITED STATES

Administrative Contact:

Mark Silis

Massachusetts Institute of Technology

MIT Room W92-167, 77 Massachusetts Avenue

Cambridge, MA 02139-4307

UNITED STATES

(617) 324-5900

mark@mit.edu

Technical Contact:

MIT Network Operations

Massachusetts Institute of Technology

MIT Room W92-167, 77 Massachusetts Avenue

Cambridge, MA 02139-4307

UNITED STATES

(617) 253-8400

network@mit.edu

Name Servers:

STRAWB.MIT.EDU 18.71.0.151

W20NS.MIT.EDU 18.70.0.160

BITSY.MIT.EDU 18.72.0.3

Domain record activated: 23-May-1985

Domain record last updated: 18-Jun-2010

Domain expires: 31-Jul-2013

Domain Name: SUU.EDU

Registrant:

Southern Utah University

Network Services, Attn: M Zufelt

351 W University Blvd

Cedar City, UT 84720

UNITED STATES

Administrative Contact:

DNS Hostmaster

Southern Utah University

Network Services, Attn. M Zufelt

351 W University Blvd

Cedar City, UT 84720

UNITED STATES

(435) 586-5436

hostmaster@suu.edu

Technical Contact:

DNS Hostmaster

Southern Utah University

Network Services, Attn. M Zufelt

351 W University Blvd

Cedar City, UT 84720

UNITED STATES

(435) 586-5436

hostmaster@suu.edu

Name Servers:

NS.SUU.EDU 134.250.2.3

NS2.SUU.EDU 134.250.6.3

NS3.SUU.EDU 205.120.169.3

Domain record activated: 12-Feb-1990

Domain record last updated: 25-Jun-2012

Domain expires: 31-Jul-2013

Domain Name: WEBER.EDU

Registrant:

Weber State University

3850 University Circle

Ogden, UT 84408

UNITED STATES

Administrative Contact:

Network Operations

Weber State University

2405 University Circle

Ogden, UT 84408-2405

UNITED STATES

(801) 626-7007

noc@weber.edu

Technical Contact:

Network Operations

Weber State University

2405 University Circle

Ogden, UT 84408-2405

UNITED STATES

(801) 626-7007

noc@weber.edu

Name Servers:

DNS1.WEBER.EDU 137.190.1.2, 2001:1948:210::2

DNS4.WEBER.EDU 137.190.234.2, 2001:1948:214::2

DNS6.WEBER.EDU 205.120.163.5

NS.UEN.NET

NS2.UEN.NET

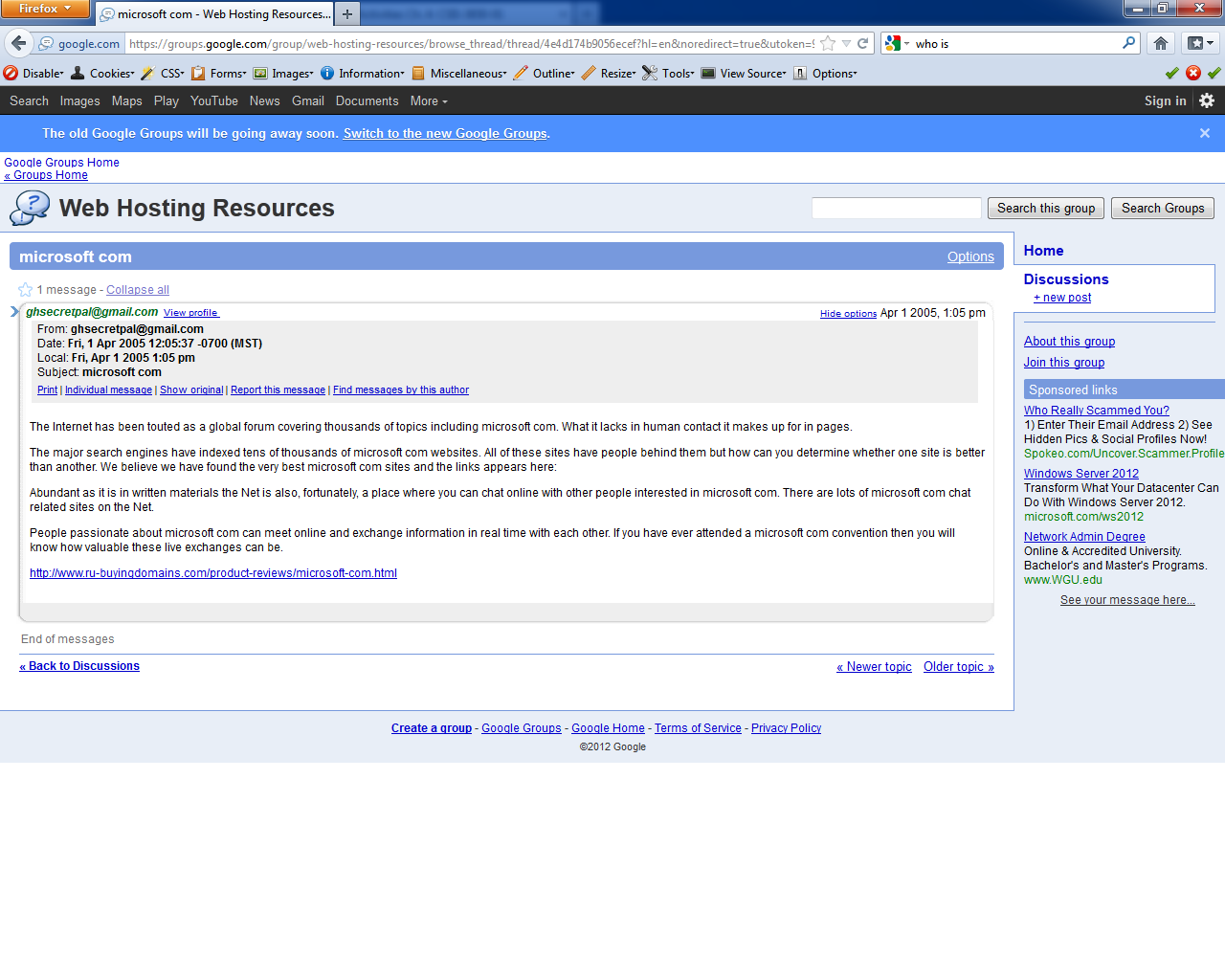
Domain record activated: 20-Dec-1989

Domain record last updated: 17-May-2012

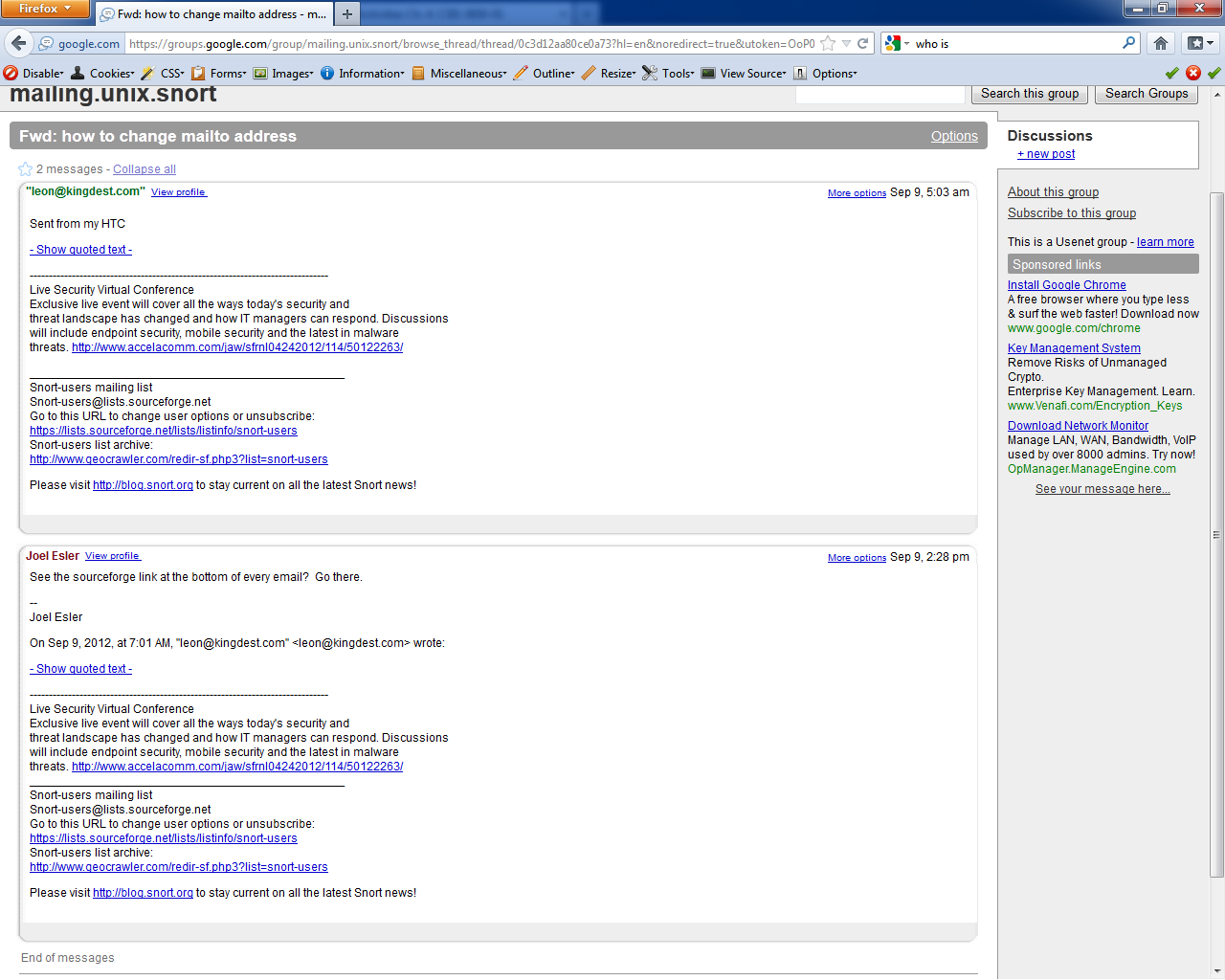
Domain expires: 31-Jul-2013

Activity 2 Chapter 4

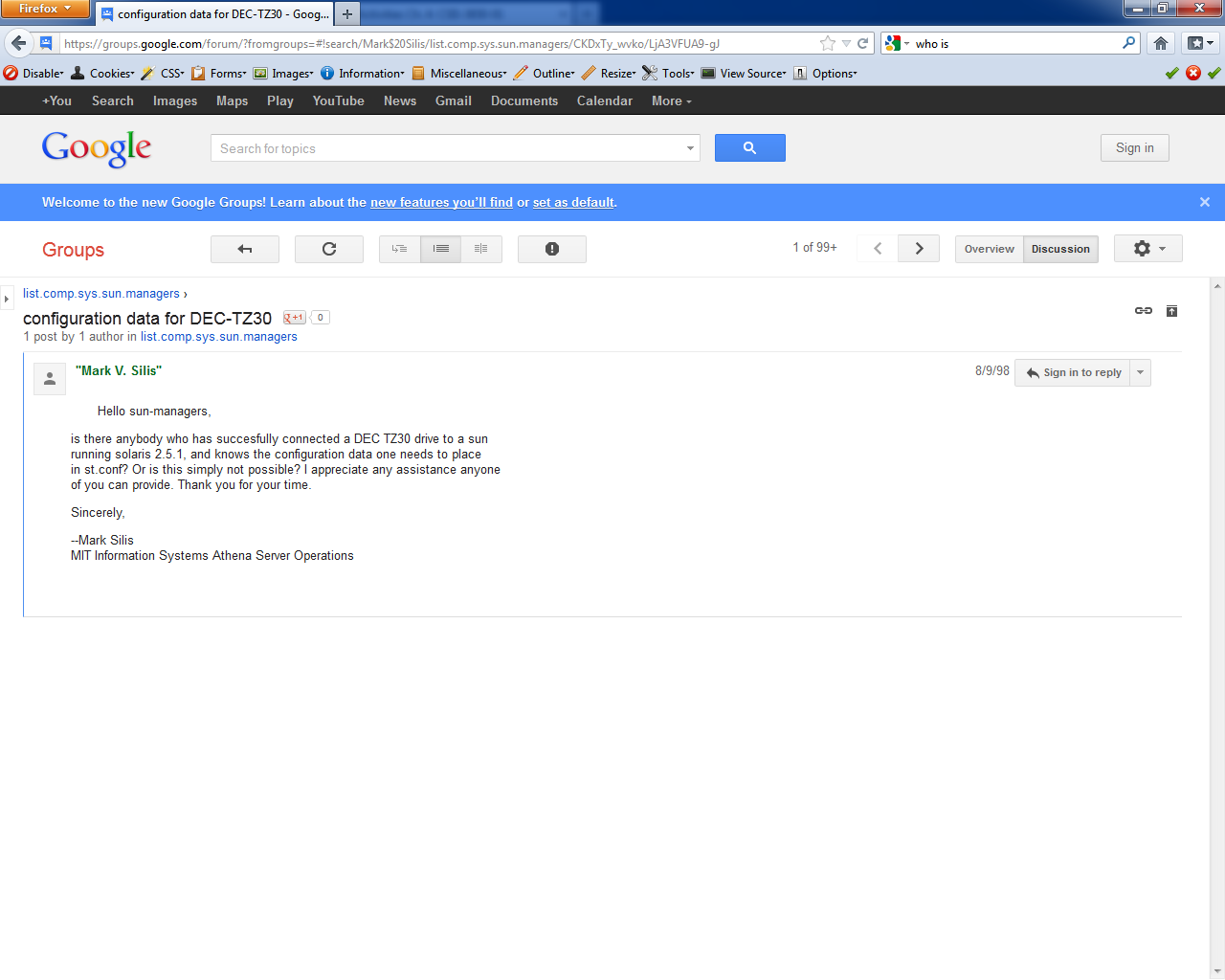
@microsoft.com



@sourcefire.com



I typed in Mark Silis from the mit.edu it brought up an email from mark



Options command

InfoSecInstitute ~ # nc mit.edu 80 Activity 3 Chapter 4:

OPTIONS / HTTP/1.1

HOST: 127.0.0.1

HTTP/1.1 200 OK

Date: Thu, 13 Sep 2012 17:08:17 GMT

Server: Apache/1.3.41 (Unix) mod\_ssl/2.8.31 OpenSSL/0.9.8j

Content-Length: 0

Allow: GET, HEAD, OPTIONS, TRACE

X-Cnection: close

Head command

InfoSecInstitute ~ # nc mit.edu 80

HEAD / HTTP/1.0

HTTP/1.1 200 OK

Date: Thu, 13 Sep 2012 17:11:37 GMT

Server: Apache/1.3.41 (Unix) mod\_ssl/2.8.31 OpenSSL/0.9.8j

Last-Modified: Thu, 13 Sep 2012 04:01:06 GMT

ETag: "10e81eac-3533-50515a82"

Accept-Ranges: bytes

Content-Length: 13619

Connection: close

Content-Type: text/html

nc –h command

[v1.10]

connect to somewhere: nc [-options] hostname port[s] [ports] ...

listen for inbound: nc -l -p port [-options] [hostname] [port]

options:

-e prog program to exec after connect [dangerous!!]

-g gateway source-routing hop point[s], up to 8

-G num source-routing pointer: 4, 8, 12, ...

-h this cruft

-i secs delay interval for lines sent, ports scanned

-l listen mode, for inbound connects

-n numeric-only IP addresses, no DNS

-o file hex dump of traffic

-p port local port number

-r randomize local and remote ports

-s addr local source address

-t answer TELNET negotiation

-u UDP mode

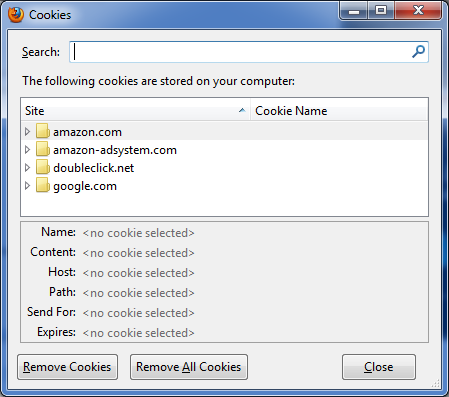
-v verbose [use twice to be more verbose]

-w secs timeout for connects and final net reads

-z zero-I/O mode [used for scanning]

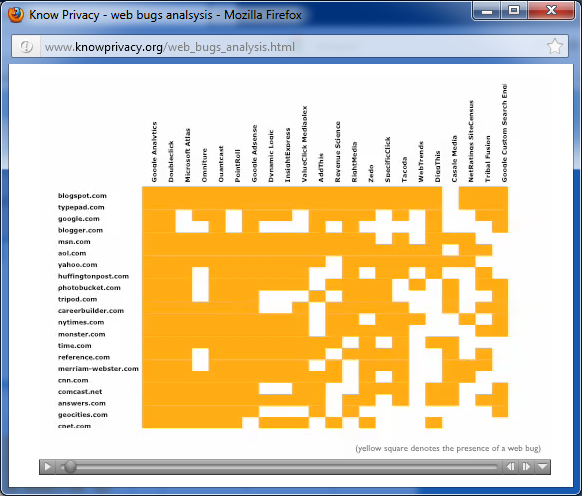
port numbers can be individual or ranges: lo-hi [inclusive]

Activity 4 Chapter 4:



I found the cookies for amazon but I didn’t see any personal information posted inside these cookies.

Activity 5 Chapter 4:



* Blogspot.com
* Typepad.com
* Google.com
* Blogger.com
* msn.com

Activity 6 Chapter 4:

[v1.10]

connect to somewhere: nc [-options] hostname port[s] [ports] ...

listen for inbound: nc -l -p port [-options] [hostname] [port]

options:

-e prog program to exec after connect [dangerous!!]

-g gateway source-routing hop point[s], up to 8

-G num source-routing pointer: 4, 8, 12, ...

-h this cruft

-i secs delay interval for lines sent, ports scanned

-l listen mode, for inbound connects

-n numeric-only IP addresses, no DNS

-o file hex dump of traffic

-p port local port number

-r randomize local and remote ports

-s addr local source address

-t answer TELNET negotiation

-u UDP mode

-v verbose [use twice to be more verbose]

-w secs timeout for connects and final net reads

-z zero-I/O mode [used for scanning]

port numbers can be individual or ranges: lo-hi [inclusive]

InfoSecInstitute ~ # dig @BITSY.mit.edu

; <<>> DiG 9.3.2-P1 <<>> @BITSY.mit.edu

; (1 server found)

;; global options: printcmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33684

;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 14

;; QUESTION SECTION:

;. IN NS

;; ANSWER SECTION:

. 512837 IN NS h.root-servers.net.

. 512837 IN NS m.root-servers.net.

. 512837 IN NS j.root-servers.net.

. 512837 IN NS i.root-servers.net.

. 512837 IN NS g.root-servers.net.

. 512837 IN NS e.root-servers.net.

. 512837 IN NS l.root-servers.net.

. 512837 IN NS d.root-servers.net.

. 512837 IN NS b.root-servers.net.

. 512837 IN NS f.root-servers.net.

. 512837 IN NS k.root-servers.net.

. 512837 IN NS a.root-servers.net.

. 512837 IN NS c.root-servers.net.

;; ADDITIONAL SECTION:

d.root-servers.net. 599237 IN A 128.8.10.90

d.root-servers.net. 599237 IN AAAA 2001:500:2d::d

k.root-servers.net. 599237 IN A 193.0.14.129

k.root-servers.net. 599237 IN AAAA 2001:7fd::1

g.root-servers.net. 599237 IN A 192.112.36.4

m.root-servers.net. 599237 IN A 202.12.27.33

m.root-servers.net. 599237 IN AAAA 2001:dc3::35

c.root-servers.net. 599237 IN A 192.33.4.12

b.root-servers.net. 599237 IN A 192.228.79.201

e.root-servers.net. 599237 IN A 192.203.230.10

i.root-servers.net. 599237 IN A 192.36.148.17

i.root-servers.net. 599237 IN AAAA 2001:7fe::53

j.root-servers.net. 599237 IN A 192.58.128.30

j.root-servers.net. 599237 IN AAAA 2001:503:c27::2:30

;; Query time: 68 msec

;; SERVER: 18.72.0.3#53(18.72.0.3)

;; WHEN: Thu Sep 13 17:28:34 2012

;; MSG SIZE rcvd: 512

InfoSecInstitute ~ # dig @BITSY.mit.edu mit.edu.axfr

; <<>> DiG 9.3.2-P1 <<>> @BITSY.mit.edu mit.edu.axfr

; (1 server found)

;; global options: printcmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 33651

;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:

;mit.edu.axfr. IN A

;; AUTHORITY SECTION:

. 10800 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2012091300 1800 900 604800 86400

;; Query time: 81 msec

;; SERVER: 18.72.0.3#53(18.72.0.3)

;; WHEN: Thu Sep 13 17:30:13 2012

;; MSG SIZE rcvd: 105

; <<>> DiG 9.3.2-P1 <<>> @BITSY.mit.edu mit.edu axfr

; (1 server found)

;; global options: printcmd

; Transfer failed.