Category: Security

Security 160299-1 1
Security 160299-1
Rec'd copy of subpoena for
"Any and All log data pertaining to dialup connection identified as ppp-062.dialup.umbc.edu on 01/20/99 @09:36:44

Name: ppp-062.dialup.umbc.edu
Address: 130.85.97.62

Mark's records:

The following log entries indicate that tnadee1 was using that IP address at 9:26am on January 20, 1999. I can not find a record of this user in PH. Rob said that the records may be lost. The telephone number that this user dialed in from, on January 20, 1999, was 410-744[redacted]

Wed Jan 20 01:16:18 1999
NAS-Identifier = 130.85.2.204
NAS-Port = 3
User-Name = "tnadee1"
Client-Port-DNIS = "7191094"
Caller-Id = "410744[redacted]
Acct-Status-Type = 3
Acct-Authentic = RADIUS
User-Service = Framed-User
Acct-Session-Id = "000063B1"
Framed-Protocol = PPP
Framed-Address = 130.85.97.62
Acct-Delay-Time = 0

Wed Jan 20 11:29:32 1999
NAS-Identifier = 130.85.2.204
NAS-Port = 3
User-Name = "tnadee1"
Client-Port-DNIS = "7191094"
Caller-Id = [redacted]
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
User-Service = Framed-User
Acct-Session-Id = "000063B1"
Framed-Protocol = PPP
Framed-Address = 130.85.97.62
Acct-Input-Octets = 979129
Acct-Output-Octets = 15262314
Acct-Input-Packets = 16587
Acct-Output-Packets = 32832

Acct-Session-Time = 36797
Acct-Delay-Time = 0

Time: 07:49:46.951567
Src: resnet-32.resnet.umbc.edu.1920
Dst: www.hotmail.com.pop-3
Type: S

Time: 07:49:47.533046
Src: resnet-32.resnet.umbc.edu.1920
Dst: www.hotmail.com.pop-3
Type: S

Time: 07:49:48.032991
Src: resnet-32.resnet.umbc.edu.1920
Dst: www.hotmail.com.pop-3
Type: S

Time: 07:49:48.532893
Src: resnet-32.resnet.umbc.edu.1920
Dst: www.hotmail.com.pop-3
Type: S

Time: 08:00:45.075542
Src: cisco2-dw.umbc.edu
Dst: www.hotmail.com
Type: icmp
time exceeded
in-transit

Time: 08:01:28.254645
Src: cisco2-dw.umbc.edu
Dst: www.hotmail.com
Type: icmp
time exceeded
in-transit

Time: 08:02:08.727341
Src: cisco2-dw.umbc.edu
Dst: www.hotmail.com
Type: icmp
time exceeded
in-transit

Time: 08:52:43.775241
Src: rsm1.umbc.edu
Dst: www.hotmail.com
Type: icmp time exceeded

in-transit [tos
0xc0]

Security 160299-1 2

Time: 08:52:44.030615
Src: rsm1.umbc.edu
Dst: www.hotmail.com
Type: icmp
time exceeded
in-transit [tos
0xc0]

Time: 08:52:44.317893
Src: rsm1.umbc.edu
Dst: www.hotmail.com
Type: icmp
time exceeded
in-transit [tos
0xc0]

Time: 09:07:14.263754
Src: rsm1.umbc.edu
Dst: www.hotmail.com
Type: icmp
time exceeded
in-transit [tos
0xc0]

Time: 09:36:35.144417
Src: umbc9.umbc.edu.5497
Dst: www.hotmail.com.finger
Type: S

Time: 10:01:30.634501
Src: rsm1.umbc.edu
Dst: www.hotmail.com
Type: icmp
time exceeded
in-transit [tos
0xc0]

Time: 10:18:14.415584
Src: saturn.umbc.edu
Dst: www.hotmail.com
Type: icmp
time exceeded
in-transit [tos

0xc0]

Note the finger of hotmail.com from umbc9 at 09:36:35.

---

ph> query name="nade*"

---

name: tahir nadeem
curriculum: bs ifsm
homepage: http://www.gl.umbc.edu/~ntahir1/
email to: [redacted]

---

name: nader momeni
curriculum: undc
email to: [redacted]

---

name: bhatti nadeem
email to: [redacted]

---

name: hosni nader
email to: [redacted]

---

name: kilada nader
curriculum: undc
email to: [redacted]

---

ph> query alias=ntahir1 return all

---

alias: ntahir1
name: tahir nadeem
email: [redacted]
curriculum: bs ifsm
type: person
validated: 1998/11/22
created: 1996/09/04
homepage: http://www.gl.umbc.edu/~ntahir1/
group: research
vms_uic: 13389.80
vms_username: [redacted]
unix_uid: 13389
inst_created: 96/9/5
res_created: 1998/9/28
afs_created: 1998/06/15

[andy@gecko] January 45 > ^tnadee^ntahir
grep ntahir 160299-1.syslog.dump

Jan 20 01:18:28 umbc9 login[18637]: failed: ?@ppp-062.dialup.umbc.edu as ntahir1^[OB
Jan 20 01:18:36 umbc9 login[18637]: ?@ppp-062.dialup.umbc.edu as ntahir1