Network Defence on the cheap

Investigating Honeypots

Chris Moore
University College Plymouth,
St Mark & St John

What is a Honeypot?

Definition:

A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource.

Lance Spitzner

Chris says:

They are an interesting way to find out what is happening on your network.

Poll

Audience participation

- Who is running a honeypot

Legal Bits

- Is it Legal
- Or Entrapment

They come in uninvited, so anything left is fair game

•IP addresses - to block
•
•Vulnerabilities - to patch
•
•Source code - to analyse

Types of Honeypot

Complex Ones

- Research
- Honeynets
- Real systems
- Risky

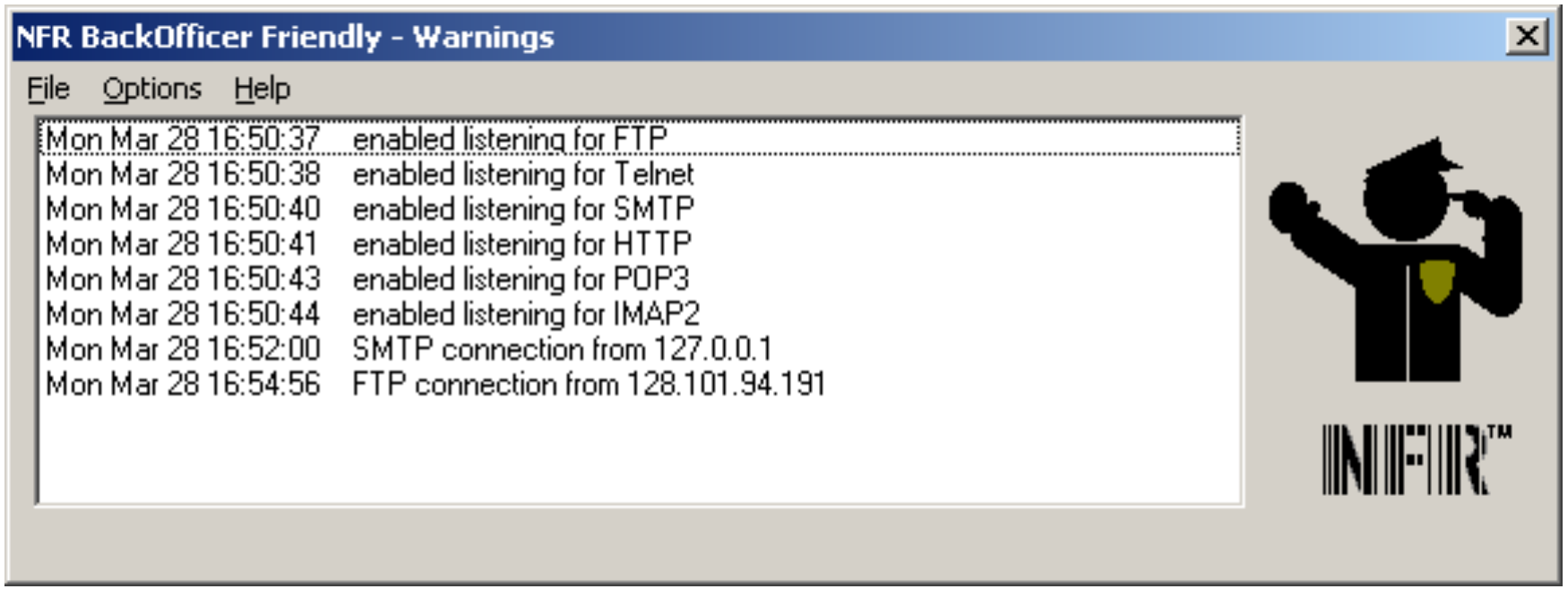
Simple Ones

- Production networks
- Simulation system
- Reduced Risk

Which O/S

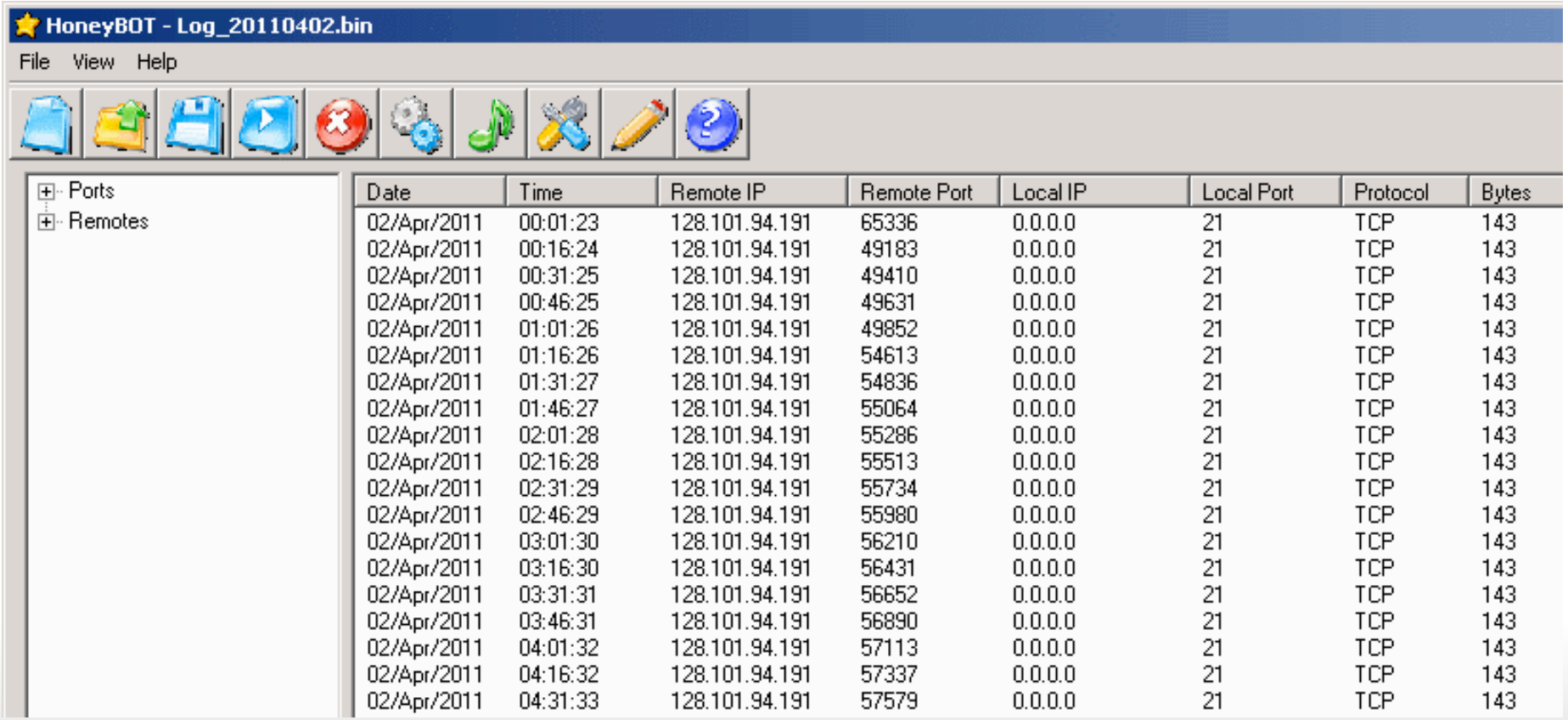
- Windows
  - Simple – install and run
  - Compromise / take over
- *nix
  - Complex install
    - Get
    - Tar
    - Make
  - Emulates Windows so less chance to compromise

BOF - BackOfficer Friendly



URL: http://www.nfr.com/products/bof/ If you can find it …

HoneyBot



Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
02/Apr/2011	00:01:23	128.101.94.191	65336	0.0.0.0	21	TCP	143
02/Apr/2011	00:16:24	128.101.94.191	49183	0.0.0.0	21	TCP	143
02/Apr/2011	00:31:25	128.101.94.191	49410	0.0.0.0	21	TCP	143
02/Apr/2011	00:46:25	128.101.94.191	49631	0.0.0.0	21	TCP	143
02/Apr/2011	01:01:26	128.101.94.191	49852	0.0.0.0	21	TCP	143
02/Apr/2011	01:16:26	128.101.94.191	54613	0.0.0.0	21	TCP	143
02/Apr/2011	01:31:27	128.101.94.191	54836	0.0.0.0	21	TCP	143
02/Apr/2011	01:46:27	128.101.94.191	55064	0.0.0.0	21	TCP	143
02/Apr/2011	02:01:28	128.101.94.191	55286	0.0.0.0	21	TCP	143
02/Apr/2011	02:16:28	128.101.94.191	55513	0.0.0.0	21	TCP	143
02/Apr/2011	02:31:29	128.101.94.191	55734	0.0.0.0	21	TCP	143
02/Apr/2011	02:46:29	128.101.94.191	55980	0.0.0.0	21	TCP	143
02/Apr/2011	03:01:30	128.101.94.191	56210	0.0.0.0	21	TCP	143
02/Apr/2011	03:16:30	128.101.94.191	56431	0.0.0.0	21	TCP	143
02/Apr/2011	03:31:31	128.101.94.191	56652	0.0.0.0	21	TCP	143
02/Apr/2011	03:46:31	128.101.94.191	56890	0.0.0.0	21	TCP	143
02/Apr/2011	04:01:32	128.101.94.191	57113	0.0.0.0	21	TCP	143
02/Apr/2011	04:16:32	128.101.94.191	57337	0.0.0.0	21	TCP	143
02/Apr/2011	04:31:33	128.101.94.191	57579	0.0.0.0	21	TCP	143

http://www.atomicsoftwaresolutions.com/honeybot.php

Nepenthes

Janet said no...

...But suggested Nepenthes

Honeypot emulator, running under *nix

```
apt get install nepenthes
```

URL: http://www.zonums.com

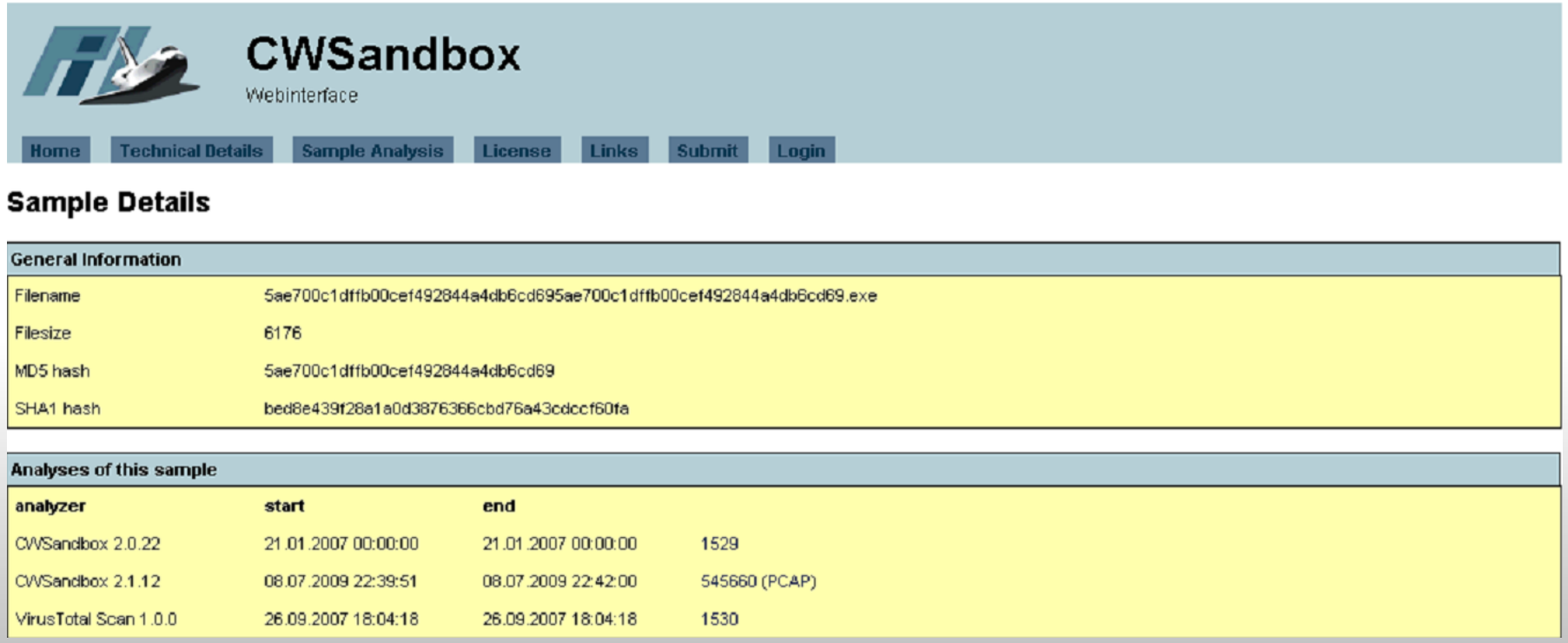
Nepenthes

```
[03042011 14:13:08 debug net mgr] Accepted Connection Socket TCP  (accept) 128.1
01.100.36:4066 -> 128.101.100.182:135
[03042011 14:13:08 debug net mgr] Accepted Connection Socket TCP  (accept) 128.1
01.100.36:4067 -> 128.101.100.182:135
[03042011 14:13:08 debug net mgr] Accepted Connection Socket TCP  (accept) 128.1
01.100.36:4068 -> 128.101.100.182:135
[2010-10-15T13:15:52] 128.101.99.32 -> 128.101.100.182 http://www.example.com/
[2010-10-15T13:16:09] 128.101.99.32 -> 128.101.100.182 http://127.0.0.1:2301/
[2010-10-15T13:16:13] 128.101.99.32 -> 128.101.100.182 http://192.168.0.1/
[2010-10-15T13:16:53] 128.101.99.32 -> 128.101.100.182 https://128.101.100.182:8
0/
[03042011 14:13:08 debug net handler] Dialogue DCOMDialogue inactive, returned C
L_DROP
[03042011 14:13:08 debug net handler] Socket TCP  (accept) 128.101.100.36:4068 -
> 128.101.100.182:135
 has no active Dialogues left, closing
[03042011 14:13:08 debug net mgr] Deleting Socket TCP  (accept) 128.101.100.36:4
068 -> 128.101.100.182:135 due to closed connection
[03042011 14:13:08 spam net handler] <in virtual nepenthes::TCPSocket::~TCPSocke
t()>
[03042011 14:13:08 spam net handler] Socket TCP  (accept) 128.101.100.36:4068 ->
 128.101.100.182:135 clearing DialogueList (1 entries)
[03042011 14:13:08 spam net handler]    Removing Dialogue "DCOMDialogue"
[03042011 14:13:08 warn handler dia] Unknown DCOM Shellcode (Buffer 116 bytes) (
State 0)
[03042011 14:13:08 spam mgr event] <in virtual uint32_t nepenthes::EventManager:
:handleEvent(nepenthes::Event*)>
[03042011 14:13:08 spam mgr event] <in virtual uint32_t nepenthes::EventManager:
:handleEvent(nepenthes::Event*)>
```

Report on captured Malware

Logs

Send it off to submit.norman for analysis



CWSandbox

Webinterface

Home | Technical Details | Sample Analysis | License | Links | Submit | Login

Sample Details

General Information	
Filename	5ae700c1dffb00cef492844a4db6cd695ae700c1dffb00cef492844a4db6cd69.exe
Filesize	6176
MD5 hash	5ae700c1dffb00cef492844a4db6cd69
SHA1 hash	bed8e439f28a1a0d3876366cbd76a43cdccf60fa

Analyses of this sample			
analyzer	**start**	**end**	
CWSandbox 2.0.22	21.01.2007 00:00:00	21.01.2007 00:00:00	1529
CWSandbox 2.1.12	08.07.2009 22:39:51	08.07.2009 22:42:00	545660 (PCAP)
VirusTotal Scan 1.0.0	26.09.2007 18:04:18	26.09.2007 18:04:18	1530

Sandbox Report

Scan Summary | File Changes | Registry Changes | Network Activity | Technical Details

Registry Changes by all processes

Create or Open	
Changes	HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun "windows auto update" = msblast.exe
	HKEY_LOCAL_MACHINESOFTWAREMicrosoftRpcSecurityService "10" HKEY_LOCAL_MACHINESYSTEMControlSet001ControlSecurityProviders "SecurityProviders" HKEY_LOCAL_MACHINESYSTEMControlSet001ControlLsaSspiCachemsapsspc.dll "Name" HKEY_LOCAL_MACHINESYSTEMControlSet001ControlLsaSspiCachemsapsspc.dll "Comment" HKEY_LOCAL_MACHINESYSTEMControlSet001ControlLsaSspiCachemsapsspc.dll "Capabilities" HKEY_LOCAL_MACHINESYSTEMControlSet001ControlLsaSspiCachemsapsspc.dll "RpcId" HKEY_LOCAL_MACHINESYSTEMControlSet001ControlLsaSspiCachemsapsspc.dll "Version" HKEY_LOCAL_MACHINESYSTEMControlSet001ControlLsaSspiCachemsapsspc.dll "Type" HKEY_LOCAL_MACHINESYSTEMControlSet001ControlLsaSspiCachemsapsspc.dll "TokenSize" HKEY_LOCAL_MACHINESYSTEMControlSet001ControlLsaSspiCachedigest.dll "Name" HKEY_LOCAL_MACHINESYSTEMControlSet001ControlLsaSspiCachedigest.dll "Comment"

Scanner Results

Scan Engine	Version	Signature Version	Result
AhnLab-V3	2007.9.22.0	20070924	Win32/Blaster.worm.6176
AntiVir	7.6.0.15	20070926	Worm/Lovsan.F.1
Authentium	4.93.8	20070926	W32/Msblast.A
Avast	4.7.1043.0	20070926	Win32:Lovesan-D
AVG	7.5.0.488	20070926	Worm/Lovsan.A
BitDefender	7.2	20070926	Worm.Lovesan.A
CAT-QuickHeal	9.00	20070926	W32.Mblast.A
ClamAV	0.91.2	20070926	Worm.Blaster.A

Findings

Home

•Lots of attacks, 350 / day

University WAN

•Fewer attacks – 50 / day - JANET

University LAN

•Smart tills

Tippingpoint ?

What's Next

Dionaea

URL: http://dionaea.carnivore.it/

Mwcollect

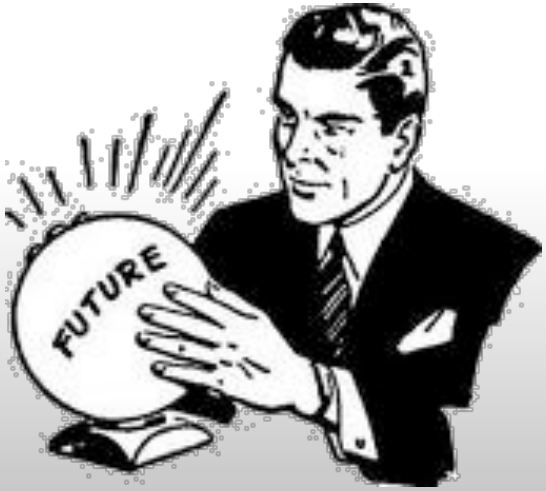
URL: http://code.mwcollect.org/

Cuckoo

URL: http://www.cuckoobox.org/index.php

Carnivore

URL http://src.carnivore.it/carniwwwhore/



Dionaea http://networkdefense.com.au/2010/06/12/first-experiences-with-dionaea/

1. Stuff from APT
apt-get install libglib2.0-dev libssl-dev libcurl4-openssl-dev libreadline-dev libsqlite3-dev python-dev libtool automake autoconf build-essential subversion git-core flex bison pkg-config

2. gettext / glib
apt-get install gettext
wget
http://ftp.gnome.org/pub/gnome/sources/glib/2.20/glib-2.20.4.tar.bz2
tar xfj glib-2.20.4.tar.bz2
rm glib-2.20.4.tar.bz2
cd glib-2.20.4/
./configure --prefix=/opt/dionaea
make
make install
cd ..

3. liblcfg
git clone git://git.carnivore.it/liblcfg.git liblcfg
cd liblcfg/code
autoreconf -vi
./configure --prefix=/opt/dionaea
make install
cd /usr/local/src

4. libemu
git clone git://git.carnivore.it/libemu.git libemu
cd libemu
autoreconf -vi
./configure --prefix=/opt/dionaea
make install
cd ..

5. libnl (optional)
git clone git://git.kernel.org/pub/scm/libs/netlink/libnl.git
cd libnl
autoreconf -vi
export LDFLAGS=-Wl,-rpath,/opt/dionaea/lib
./configure --prefix=/opt/dionaea
make
make install
cd ..

6. libev
wget
http://dist.schmorp.
tar xfz libev-3.9.tar.
rm libev-3.9.tar.gz
cd libev-3.9
./configure --prefix=
make install
cd ..

Dionaea Logs - View the ‘opens’

Applications Places System

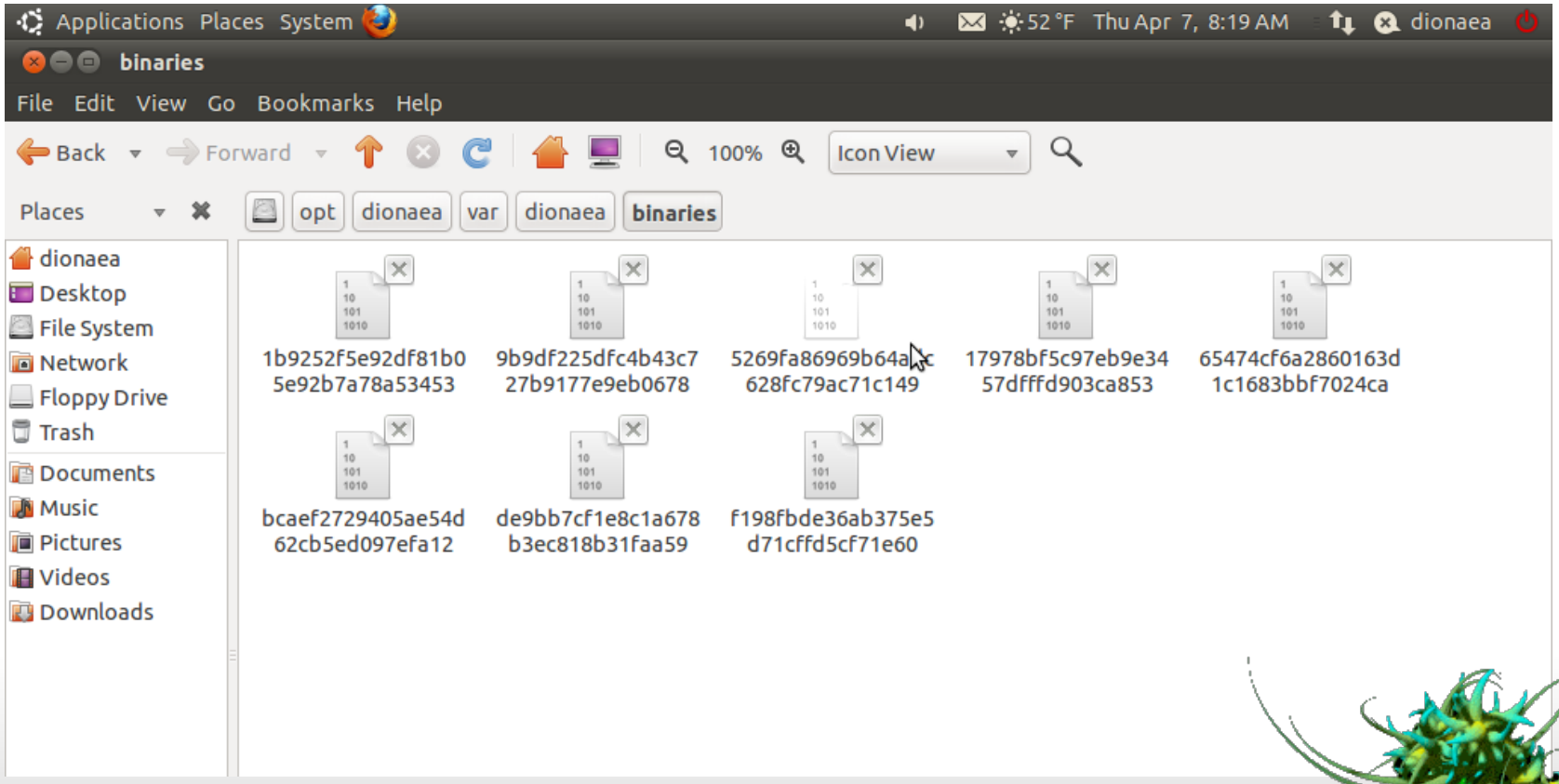
root@ubuntu: ~

File Edit View Search Terminal Tabs Help

root@ubuntu: ~ | root@ubuntu: ~ | tarkus@ubuntu: /etc

```
[07042011 09:43:13] pcap pcap.c:190-debug: reject local:'128.101.87.73:1080' remote:'193.105.134.91:17439'
[07042011 09:53:18] pcap pcap.c:180-debug: 128.101.87.73:1080 -> 46.161.11.100:54658
[07042011 09:53:18] pcap pcap.c:190-debug: reject local:'128.101.87.73:1080' remote:'46.161.11.100:54658'
^C
root@ubuntu:~# more  /opt/dionaea/var/log/dionaea.log  | grep "g: 128"
[05042011 10:55:51] pcap pcap.c:180-debug: 128.101.87.73:22 -> 128.101.99.31:34927
[05042011 10:55:52] pcap pcap.c:180-debug: 128.101.87.73:22 -> 128.101.99.31:55407
[05042011 10:55:52] pcap pcap.c:180-debug: 128.101.87.73:22 -> 128.101.99.31:39023
[05042011 11:04:24] pcap pcap.c:180-debug: 128.101.87.73:20 -> 128.101.99.31:43270
[05042011 11:04:25] pcap pcap.c:180-debug: 128.101.87.73:20 -> 128.101.99.31:39174
[05042011 11:04:25] pcap pcap.c:180-debug: 128.101.87.73:20 -> 128.101.99.31:39174
[05042011 11:04:26] pcap pcap.c:180-debug: 128.101.87.73:21 -> 128.101.99.31:43271
[05042011 11:06:11] pcap pcap.c:180-debug: 128.101.87.73:22 -> 128.101.99.31:35113
[05042011 11:06:11] pcap pcap.c:180-debug: 128.101.87.73:22 -> 128.101.99.31:59689
[05042011 11:06:12] pcap pcap.c:180-debug: 128.101.87.73:22 -> 128.101.99.31:35113
[05042011 11:06:12] pcap pcap.c:180-debug: 128.101.87.73:23 -> 128.101.99.31:35115
[05042011 11:06:12] pcap pcap.c:180-debug: 128.101.87.73:23 -> 128.101.99.31:55595
[05042011 11:06:13] pcap pcap.c:180-debug: 128.101.87.73:23 -> 128.101.99.31:51499
[05042011 11:06:13] pcap pcap.c:180-debug: 128.101.87.73:24 -> 128.101.99.31:47404
[05042011 11:06:13] pcap pcap.c:180-debug: 128.101.87.73:24 -> 128.101.99.31:51500
[05042011 11:06:14] pcap pcap.c:180-debug: 128.101.87.73:24 -> 128.101.99.31:55596
[04052011 20:11:19] pcap pcap.c:180-debug: 128.101.87.73:53 -> 128.101.99.31:39641
[04052011 20:11:20] pcap pcap.c:180-debug: 128.101.87.73:53 -> 128.101.99.31:51929
[04052011 20:11:20] pcap pcap.c:180-debug: 128.101.87.73:53 -> 128.101.99.31:35545
[06042011 20:20:11] pcap pcap.c:180-debug: 128.101.87.73:80 -> 128.101.99.31:47698
[06042011 11:44:49] pcap pcap.c:180-debug: 128.101.87.73:1080 -> 46.161.11.100:54658
[06042011 12:13:41] pcap pcap.c:180-debug: 128.101.87.73:1080 -> 193.105.134.91:17439
[06042011 12:45:35] pcap pcap.c:180-debug: 128.101.87.73:8080 -> 219.235.240.36:9479
[06042011 12:54:41] pcap pcap.c:180-debug: 128.101.87.73:1080 -> 46.161.11.100:54658
[06042011 12:56:20] pcap pcap.c:180-debug: 128.101.87.73:3389 -> 217.72.77.134:2125
[06042011 12:56:21] pcap pcap.c:180-debug: 128.101.87.73:3389 -> 217.72.77.134:2125
[06042011 12:56:21] pcap pcap.c:180-debug: 128.101.87.73:3389 -> 217.72.77.134:2125
[06042011 13:21:36] pcap pcap.c:180-debug: 128.101.87.73:445 -> 2.93.234.48:4978
[06042011 13:21:38] pcap pcap.c:180-debug: 128.101.87.73:445 -> 2.93.234.48:4978
[06042011 13:21:38] pcap pcap.c:180-debug: 128.101.87.73:445 -> 2.93.234.48:4978
[06042011 13:25:13] pcap pcap.c:180-debug: 128.101.87.73:1080 -> 193.105.134.91:17439
[06042011 14:04:38] pcap pcap.c:180-debug: 128.101.87.73:1080 -> 46.161.11.100:54658
[06042011 14:36:50] pcap pcap.c:180-debug: 128.101.87.73:1080 -> 193.105.134.91:17439
[06042011 15:14:32] pcap pcap.c:180-debug: 128.101.87.73:1080 -> 46.161.11.100:54658
[06042011 15:35:28] pcap pcap.c:180-debug: 128.101.87.73:135 -> 81.177.144.9:6000
```

Dionaea – Binaries collected



Thoughts...

- Virtual Machines - Standard now?
-
- Anyone converted ?
- Thinking
- Will do
- Will NOT do - Security / other

Links

http://dionaea.carnivore.it/