Protocol Detection Capabilities in Bro - The Practical Approach

ROGER LARSEN

Project - Spring 2012
IMT-4641-Computational Forensics
Gjøvik University College

Thursday 21st June, 2012

Abstract

Network Intrusion Detection Systems (NIDS) capability in protocol analyses is crucial. The TCP/IP suite have a standard scheme which predefines port numbers for each protocol by IANA[1][4]. However, both benign and evil software are continuously getting more and more sophisticated and do not follow these predefined schemes. In this article we test Bro's protocol detection capability with a honeypot server as the target and NMAP as network scanner. Will Bro manage to detect the protocols generated against our honeypot?

1 Introduction

Network intrusion detection systems (NIDS) are our next generation of typical security mechanisms in every organization. To resist today's malware and malicious attacks from Internet (initially, then from our own client computers), we need to filter/scan the network traffic. NIDS are especially designed for detecting malware/malicious attacks in our network.

The NIDS are classified in two different categoriez; *signature/misuse* based and *anomaly*. Signature/misuse based NIDS know the signature/pattern on malicious malware/attack. The anomaly based NIDS need an initial learning phase to create a baseline of the network traffic and will generate alarms based on statistical variations regarding its baseline.

We will in this paper use Bro NIDS [2] [16], known to be anomaly based, and test its protocol detection capabilities.

1.1 Motivation / Limitation / Outline

Our motivation for this paper is to explore Bro's protocol detection capabilities in practice.

We will focus on TCP/IP protocols in the Application Layer unless otherwise stated. This project is the main part of our 5 ECTS[3] course: Computational Forensics, spring 2012. We

[1]IANA - Internet Assigned Numbers Authority. IANA is globally responsible of coordinating Internet protocol resources.

[2]Bro (or the long version: "The Bro Network Security Monitor") are Unix-based software that are capable of passively monitor network traffic for suspicious behaviour.

[3]ESTC - European Credit Transfer and Accumulation System `http://ec.europa.eu/education/lifelong-learning-policy/ects_en.htm`

are most practical in this paper - please support your reading with our more theoretical article *Protocol detection in Bro* [4] [8].

We start this article with a short description of NIDS in general. Further we explain our lab setup. Bro's protocol detection capabilities are challenged. Finally we discuss and summarize our findings.

2 Bro Test Lab

2.1 Bro Test Lab - Network

Below in figure 1 You find our Bro Test Lab Network.

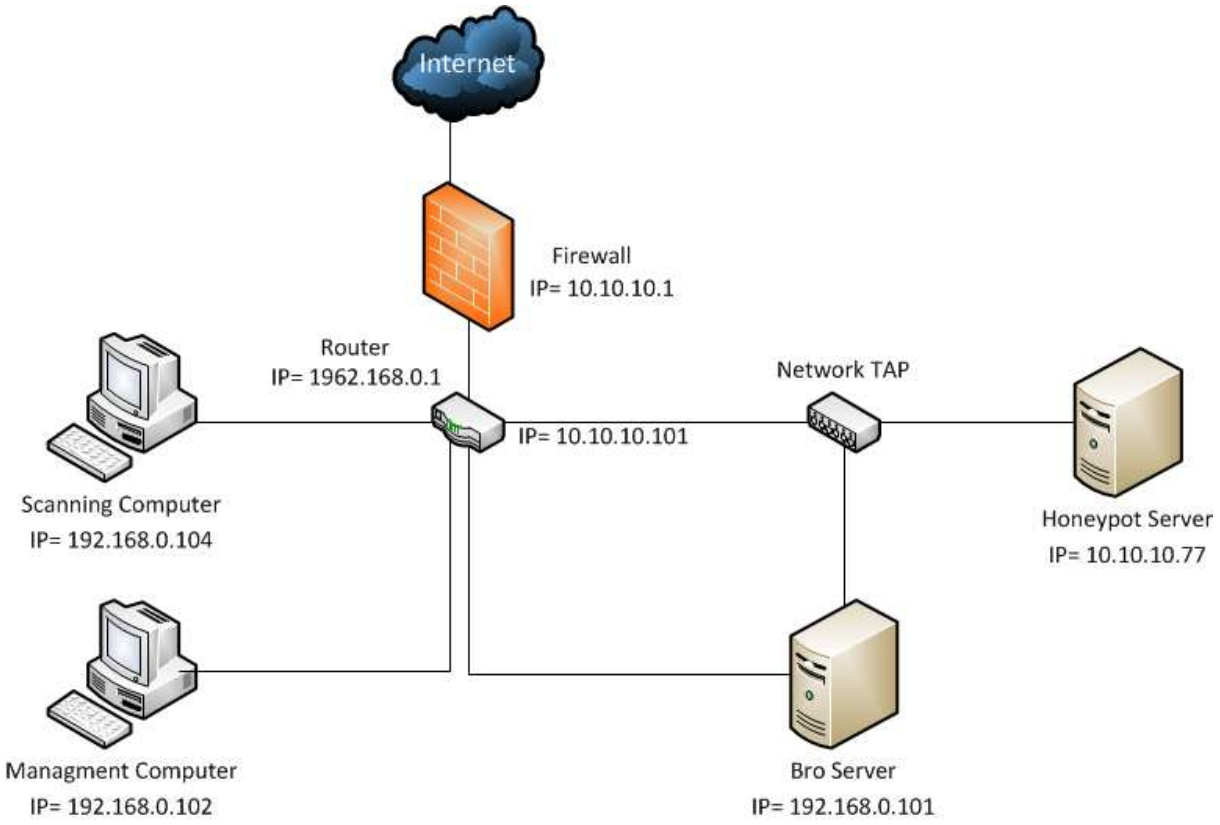

Figure 1: Test lab setup details with IP addresses.

[4] *Protocol detection in Bro* are the report in course Digital Forensics II, spring 2012.

2.2 Bro Test Lab - Details Summary

Item	Description
The Scanning Comp.	**Physical:** Acer Aspire 5630 (new in May 2008) **Os base:** Microsoft Windows XP Professional (up to date Thursday 21st June, 2012) [11]. **Software, network scanner:** NMAP (Network Mapper).
The Mgmt. Comp.	**Physical:** DELL Latitude E6510 (new in February 2011) **Os base:** Microsoft Windows 7 Professional 64bit (up to date Thursday 21st June, 2012) [10]. **Software, terminal emulator:** Secure CRT.
The TAP	**Physical**: An IP TV Probe with TAP functionality [3]. It have only Fast Ethernet capabilities. **Os base:** Proprietary software by BRIDGE Technology co AS for IP TV testing [3] - not so interesting in this context.
The Honeypot Server	**Physical:** Dell Optiplex GX-280 (new in 2008) **Os base:** Linux Debian 6.0.5 (kernel 2.6.32-5-686) [5]. **Software:** Dionaea honeypot.
The Bro Server	**Physical:** Dell Optiplex GX-280 (new in 2008) with two Fast Ethernet interfaces installed (one for management). **Os base:** FreeBSD 9.0-RELEASE #0 (Jan 3, 2012) [19]. **Software:** Bro version 5.0 released January 11, 2012 [13].

Table 1: Test lab equipment description.

2.3 Bro Test Lab - Description of Components

The Scanning Computer

NMAP (NEtwork MApper) network scanner is a well known vulnerability scanner developed by Gordon (Fyodor) Lyon [5]. This powerful scanner have several options and are capable of scanning every TCP and UDP port for known services. We used version 6.01 (due to 2012-05-21) which is a [9].

We executed the so-called *Slow comprehensive scan*:

```
nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 -script "default or (discovery and safe)" 10.10.10.77
```

The log from NMAP are in appendix B. Please note that this computer had some serious problem with the internal hardware clock - it was always something between 20:00 and 22:00.

The Management Computer

We only used an terminal software on our management computer. This software was *Secure CRT* by VanDyke Software [6]. This terminal emulating software have the possibility to log all terminal sessions, which is very important in our tests.

[5]Gordon (Fyodor) Lyon, about: `http://insecure.org/fyodor/`

[6]VanDyke Software Inc. 4848 Tramway Ridge Dr. NE, Suite 101 Albuquerque, NM 87111-2873, USA. `http://www.vandyke.com/`

The Dionaea Honeypot Details

The Dionaea is a so-called low-interaction honeypot designed for capturing/collecting malware. Dionaea is developed by Paul Baecher and Markus Koetter [1]. We used Dionaea version 0.1.0 installed May 15, 2012. Dionaea emulates several known vulnerabilities from several operating systems. Dionaea can be customized for specific malware, we have used the default setup described at the developers web page. Dionaea is a commonly used honeypot in research communities [15] [2].

The server had previously SSH and HTTP services installed before the Dionaea software. The complete service list is under the Dioanea column in table 3.

Bro will in general drop sessions that are not complete. By using the honeypot we get an answer from our scanning and Bro will detect the whole connection as completed.

We started Dionaea with the following command: `/opt/dionaea/bin/dionaea -l all,-debug -L '*'`

Bro Version and configuration

Bro version 5.0 was compiled and installed from source code found in Bro's GIT repository May 20, 2012 [7].

We did not change much in Bro's configuration files. The only one file we changed was the file that informed Bro to what the local/trusted network was: `$PREFIX/etc/networks.cfg`. See appendix B.

We controlled Bro from the Bro Control (aka `broctl`). Bro Control was started with the following command: `$PREFIX/bin/broctl`

Bro Control have several nice commands available - see figure 2.

[7] Bro's GIT repository: `git://git.bro-ids.org/bro.git`. GIT is a open source repository and version control software initially developed by Linus Torvald [7]

```
BroControl Version 1.0-35

   capstats <nodes> [secs]       - report interface statistics (needs capstats)
   check <nodes>                 - check configuration before installing it
   cleanup [--all] <nodes>       - delete working dirs on nodes (flushes state)
   config                        - print broctl configuration
   cron                          - perform jobs intended to run from cron
   cron enable|disable|?         - enable/disable "cron" jobs
   df <nodes>                    - print nodes' current disk usage
   diag <nodes>                  - output diagnostics for nodes
   exec <shell cmd>              - execute shell command on all nodes
   exit                          - exit shell
   install                       - update broctl installation/configuration
   netstats <nodes>              - print nodes' current packet counters
   nodes                         - print node configuration
   print <id> <nodes>            - print current values of script variable at nodes
   peerstatus <nodes>            - print current status of nodes' remote connections
   process <trace> [Bro options] - runs Bro offline on trace file
   quit                          - exit shell
   restart [--clean] <nodes>     - stop and then restart processing
   scripts [-c] <nodes>          - Lists the Bro scripts the nodes will be loading
   start <nodes>                 - start processing
   status <nodes>                - summarize node status
   stop <nodes>                  - stop processing
   update <nodes>                - update configuration of nodes on the fly
   top <nodes>                   - show Bro processes ala top

Commands provided by plugins:

   ps.bro [<nodes>]              - Shows Bro processes currently running on nodes' systems.
```

Table 2: Bro Control commands.

Bro's configuration are listed out from Bro Control in appendix A.

Bro's Log Files

Bro's log files are placed in `logs` folder folder (texttt($PREFIX/logs)):

`communication.log` – Bro's own log over main and child processes in addition to some statistics
`conn.log` – connection log: log over every completed connections
`dns.log` – DNS[8] service log
`dpd.log` – log containing Dynamic Protocol Detection log
`http.log` – log containing HTTP activity
`ssl.log` – log containing the analyzing results regarding SSL/TLS handshaking and encryption establishment process
`weird.log` – log containing unknown/strange activity that is logged for possible later analyzing
`known_hosts.log` – log containing list of hosts that had a complete TCP handshake that actual day.
`known_services.log` – log containing list of IP addresses that had complete TCP handshakes with other hosts on known services.
`software.log` – log containing list of known software detected

[8]DNS = Domain Name System.

The log files are in clear text/ASCII and are organized with columns headings with space/TAB between. See figure 4.

2.4 Comments

Why a mix of 4 different operating systems?

Bro and Dionaea are both open source software that need Unix/Linux/BSD operating system platform. Why both Debian Linux[9] and FreeBSD[10] ? We have better knowledge regarding Debian Linux vs FreeBSD (appr. 5 year vs 1 year experience). We tried some hours to get Bro installed on both Debian Linux platform and later Ubuntu Linux Server 6.0 (which is based on Debian Linux) - with several error messages and no working Bro software. We ended up with FreeBSD, which gave us a much smoother installation. Bro is BSD licensed and we conclude with our experience that FreeBSD (or any other BSD based operating system) will in general give an easier installation phase for at least present version. The network scanning software NMAP are available on Windows platform. We had available the two computer with Microsoft Windows 7 and one with Microsoft Windows XP at our work.

The four different different operating systems have most likely not any influence regarding our test results.

3 Test Results

We ran our NMAP scan against the Dionaea server 10 times - with Bro server on the TAP. Please find our test results in table 3. We used the these log files from Bro; (i) `communication.log`, (ii) `conn.log`, (iii) `known_services.log`, (iv) `dpd.log` and (v)(`weird.log`.

#	Dionaea	NMAP	Bro	Descr.	Comment
1	FTP	FTP	FTP	21/tcp	File Transfer Protocol
2	SSH	SSH	SSH	22/tcp	Secure SHell
3	WINS	TCPWRAPPER		42/tcp	Microsoft Net-bios/LanManager
4	HTTP	HTTP	HTTP	80/tcp	
5	RPC-BIND	RPC-BIND		111/tcp	Remote Procedure Call
6	MS-RCP	MS-RCP(?)		135/tcp	Microsoft RCP
7	HTTPS	HTTPS	SSL/HTTPS	443/tcp	
8	MS-DS	MS-DS		445/tcp	Microsoft Domain Name System
9	MS-SQL-S	MS-SQL-S		1433/tcp	Microsoft SQL Secure
10	MYSQL	MS-SQL		3306/tcp	Microsoft SQL
11	SIP	SIP		5060/tcp	Session Initiation Protocol (VoIP)
12	SIP-TLS	SSL/SIP	SSL	5061/tcp	Session Initiation Protocol TLS (Secure) (VoIP)

Table 3: Table of our test results.

[9]Debian Linux is open source licensed by SPI (Software in the Public Interest, Inc.) and GNU General Public License; either version 2 and several others [6].

[10]FreeBSD are free software copyrighted by UC Berkeley's Berkeley Software Distribution ("BSD") [18].

3.1 Comments to Results

We have only scanned TCP ports. I will here refer to the line numbers in table 3 and comments only the Bro column:
2 – NMAP calles this TCPWRAPPER but found the correct protocol and port.
7 – SSL are correct detected. HTTPS may also be set up with Transport Layer Security (TLS) [14].
12 – SSL is not correct detected (should have been TLS).

Bro logs extensively - we have listed only the interesting parts and in addition cut out the rightmost part of Bro's log to fit our report format - see figures 4 5. Please read the attached log file for complete understanding (`Bro_conn-log.cvs`).

```
ts                  uid       id.orig_h    id.orig_p id.resp_h    id.resp_p proto service duration
time                string      addr          port      addr          port      enum  string  interval

1340183364.820765 2f1LbmYeGka 10.10.10.101 53    10.10.10.77 80   tcp -0.000073
1340183364.821030 QhcLJGZ44ia 10.10.10.101 53    10.10.10.77 443   tcp -0.000068
-
1340183364.933996 kTH4NzkOAOk 10.10.10.101 53    10.10.10.77 80     tcp -0.000059
-
1340183366.008156 NniFkC4ZMEe 10.10.10.101 53    10.10.10.77 80   tcp http 93.402979
-
1340183687.205162 SbCJoQ6l32h 10.10.10.101 1830    10.10.10.77 22   tcp ssh 0.027361
1340183687.205162 SbCJoQ6l32h 10.10.10.101 1830    10.10.10.77 22   tcp ssh 0.027361
1340183687.205449 O84Z0XuJIkh 10.10.10.101 1831    10.10.10.77 42   tcp -5.006565
1340183687.206050 ydACjGDYBP5 10.10.10.101 1833    10.10.10.77 111   tcp -6.037684
1340183687.206213 7ceWGIAs3r6 10.10.10.101 1835    10.10.10.77 135   tcp -11.039525
1340183687.206865 d4IU50kzkzg 10.10.10.101 1836    10.10.10.77 445   tcp -6.108067
1340183687.207019 b4RTwBHotOh 10.10.10.101 1834    10.10.10.77 21   tcp -0.695973
1340183687.207990 pchZhZVvJX5 10.10.10.101 1837    10.10.10.77 1433   tcp -11.038818
1340183687.208587 GLFtbIZp7J9 10.10.10.101 1838    10.10.10.77 3306   tcp -1.160474
1340183687.208758 uwZDnqnIwzl 10.10.10.101 1839    10.10.10.77 5060   tcp -11.039280
1340183687.209045 25ewipGHS0l 10.10.10.101 1840    10.10.10.77 5061   tcp -11.210053
-
1340183706.205942 5isJp9LkuAb 10.10.10.101 1882    10.10.10.77 5061   tcp ssl 0.043424
-
1340183703.255001 XhWoT9caji 10.10.10.101 1880    10.10.10.77 135   tcp -5.007633
```

Table 4: Log file CONN.LOG (partly) from test against Dionaea honeypot.

The log from our test against Dionaea honeypot showed us that several protocols where not detected by Bro. The following log are from our rather random results (browsing and other administrative work on our management computer). It shows us that HTTPS are recognized from Bro.

```
ts              uid        id.orig_h   id.orig_p id.resp_h  id.resp_p proto service duration
time             string       addr          port  addr        port  enum  string  interval

1340217694.435875 mPQdiCQhOai 10.10.10.100 52915 204.154.94.81  443 tcp https 35.452156
```

Table 5: Log file CONN.LOG (partly) from other traffic to Internet.

We where a bit puzzled by the weak results from Bro's protocol detection. One common factor is that Dionaea is a honeypot that are using several Microsoft services (5 of 12 in total). Bro have correctly detected 4 of 12 services - none of these are Microsoft services. A deeper look into Bro's configuration and perhaps BinPAC and script functionality may have increased our detection rate [12]. We may also consider setting up proper services in stead of this Dionaea which are more specialized on catching malware.

Practical experience

We wasted some hours regarding our initial use of Bro Control. We entered the application + started Bro + exit. This was not working (strange enough). We did not get any logs at all this way ... We ended up using two terminal windows against Bro; (i) one with Bro Control active and (ii) an other for parsing logs. This way we managed to get logs as expected.

4 Further Work

We would further NIDS evaluating like to capture some network traffic with The Time Machine [17] (software for bulk capturing network traffic for later replay). Other interesting project will be to develop a server specialized for NIDS testing. This server could have several protocols activated together with the time machine software for replay of connections.

5 Summary

We have in this article challenged the NIDS Bro regarding protocol detection capabilities. We used NMAP as our network scanner to generate traffic against the honeypot Dionaea. We ended up with fewer protocols detected in Bro then we expected. Can out test configuration and the use of Dionaea honeypot take the blame? Where we too hasty regarding our testing procedure and ignored any learning processes in Bro? We have; (i) learned to install and operate Bro, (ii) got familiar and manage to change Bro's configuration and we have learned to read Bro's extensive logs. All together we have gained our goals with our project - though our results where a bit surprising. Now we are looking forward to be able to work with this kind of interesting software in the future.

Appendix A — Bro's networks.cfg.

Bro's configuration file networks.cfg

The file is located under the /etc folder (texttt$PREFIX/etc/networks.cfg). The only change we did was adding a "hash" sign (#) in front of the line that started with 10.0.0.0/8 (which comment out this actual IP subnet):

```
# List of local networks in CIDR notation, optionally followed by a
# descriptive tag.

#     10.0.0.0/8          Private IP space
192.168.0.0/16      Private IP space
```

Table 6: The networks.cfg file .

We have listed some output of commands in Bro's Bro Control

```
[BroControl] > config
bindir = /usr/local/bro/bin
bro = /usr/local/bro/bin/bro
bro-crashed = 0
bro-pid = 2689
bro-port = 47760
broargs =
brobase = /usr/local/bro
broctlconfigdir = /usr/local/bro/spool
broversion = 2.0-372
capstatspath = /usr/local/bro/bin/capstats
cfgdir = /usr/local/bro/etc
cflowaddress =
cflowpassword =
cflowuser =
commtimeout = 10
compresslogs = 1
cron = 0
croncmd =
cronenabled = 1
debug = 0
debuglog = /usr/local/bro/spool/debug.log
havenfs = 0
helperdir = /usr/local/bro/share/broctl/scripts/helpers
home =
libdir = /usr/local/bro/lib
libdirinternal = /usr/local/bro/lib/broctl
localnetscfg = /usr/local/bro/etc/networks.cfg
lockfile = /usr/local/bro/spool/lock
logdir = /usr/local/bro/logs
logexpireinterval = 0
logrotationinterval = 3600
mailalarmsto = root@localhost
mailfrom = Big Brother <bro@brodil>
mailreplyto =
mailsubjectprefix = [Bro]
mailto = root@localhost
makearchivename = /usr/local/bro/share/broctl/scripts/make-archive-name
memlimit = unlimited
mindiskspace = 5
nodecfg = /usr/local/bro/etc/node.cfg
os = freebsd
pfringclusterid = 0
```

```
plugindir = /usr/local/bro/lib/broctl/plugins
policydir = /usr/local/bro/share/bro
policydirsiteinstall = /usr/local/bro/spool/installed-scripts-do-not-touch/site
policydirsiteinstallauto = /usr/local/bro/spool/installed-scripts-do-not-touch/auto
postprocdir = /usr/local/bro/share/broctl/scripts/postprocessors
prefixes = local
savetraces = 0
scriptsdir = /usr/local/bro/share/broctl/scripts
sendmail = /usr/sbin/sendmail
sigint = 0
sitepluginpath =
sitepolicymanager = local-manager.bro
sitepolicypath = /usr/local/bro/share/bro/site
sitepolicystandalone = local.bro
sitepolicyworker = local-worker.bro
spooldir = /usr/local/bro/spool
standalone = 1
statefile = /usr/local/bro/spool/broctl.dat
staticdir = /usr/local/bro/share/broctl
statsdir = /usr/local/bro/logs/stats
statslog = /usr/local/bro/spool/stats.log
stoptimeout = 60
test.enabled = 0
test.foo = 1
time = /usr/bin/time
timefmt = %d %b %H:%M:%S
timemachinehost =
timemachineport = 47757/tcp
tmpdir = /usr/local/bro/spool/tmp
tmpexecdir = /usr/local/bro/spool/tmp
tracesummary = /usr/local/bro/bin/trace-summary
version = 1.0-35
[BroControl] >
[BroControl] >
[BroControl] > df
                           total  avail  capacity
       bro      /dev/ada0p2   34G    28G   10.8 %
[BroControl] >
[BroControl] >
[BroControl] > diag
[bro]

==== No reporter.log

==== stderr.log
pcap bufsize = 0

listening on rl0, capture length 8192 bytes

unlimited
unlimited

==== stdout.log
unlimited
524288
unlimited

==== .cmdline
-i rl0 -U .status -p broctl -p broctl-live -p standalone -p local -p bro local.bro broctl broctl/standalone broctl/auto

==== .env_vars
PATH=/usr/local/bro/bin:/usr/local/bro/share/broctl/scripts:/sbin:/bin:/usr/sbin:/usr/bin:/usr/games:/usr/local/sbin:/usr/local/bin
BROPATH=/usr/local/bro/spool/installed-scripts-do-not-touch/site::/usr/local/bro/spool/installed-scripts-do-not-touch/auto:/usr/loca
CLUSTER_NODE=

==== .status
RUNNING [net_run]

==== No prof.log

==== No packet_filter.log

==== No loaded_scripts.log
[BroControl] >
[BroControl] >
[BroControl] > netstats
```

```
      bro: 1340137538.167466 recvd=59291 dropped=0 link=59291
[BroControl] >
[BroControl] >
[BroControl] >
[BroControl] > nodes
           bro - addr=127.0.0.1 aux_scripts= brobase= count=1 ether= host=localhost interface=rl0 name=bro test_mykey= type=standal
[BroControl] >
[BroControl] >
[BroControl] > scripts
bro is ok.
  #separator \x09
  #set_separator        ,
  #empty_field  (empty)
  #unset_field  -
  #path loaded_scripts
  #fields       name
  #types        string
  /usr/local/bro/share/bro/base/init-bare.bro
    /usr/local/bro/share/bro/base/const.bif.bro
    /usr/local/bro/share/bro/base/types.bif.bro
    /usr/local/bro/share/bro/base/strings.bif.bro
    /usr/local/bro/share/bro/base/bro.bif.bro
    /usr/local/bro/share/bro/base/reporter.bif.bro
    /usr/local/bro/share/bro/base/event.bif.bro
    /usr/local/bro/share/bro/base/frameworks/logging/__load__.bro
      /usr/local/bro/share/bro/base/frameworks/logging/./main.bro
        /usr/local/bro/share/bro/base/logging.bif.bro
      /usr/local/bro/share/bro/base/frameworks/logging/./postprocessors/__load__.bro
        /usr/local/bro/share/bro/base/frameworks/logging/./postprocessors/./scp.bro
        /usr/local/bro/share/bro/base/frameworks/logging/./postprocessors/./sftp.bro
      /usr/local/bro/share/bro/base/frameworks/logging/./writers/ascii.bro
      /usr/local/bro/share/bro/base/frameworks/logging/./writers/dataseries.bro
  /usr/local/bro/share/bro/base/init-default.bro
    /usr/local/bro/share/bro/base/utils/site.bro
      /usr/local/bro/share/bro/base/utils/./patterns.bro
    /usr/local/bro/share/bro/base/utils/addrs.bro
    /usr/local/bro/share/bro/base/utils/conn-ids.bro
    /usr/local/bro/share/bro/base/utils/directions-and-hosts.bro
    /usr/local/bro/share/bro/base/utils/files.bro
    /usr/local/bro/share/bro/base/utils/numbers.bro
    /usr/local/bro/share/bro/base/utils/paths.bro
    /usr/local/bro/share/bro/base/utils/strings.bro
    /usr/local/bro/share/bro/base/utils/thresholds.bro
    /usr/local/bro/share/bro/base/frameworks/notice/__load__.bro
      /usr/local/bro/share/bro/base/frameworks/notice/./main.bro
      /usr/local/bro/share/bro/base/frameworks/notice/./weird.bro
      /usr/local/bro/share/bro/base/frameworks/notice/./actions/drop.bro
      /usr/local/bro/share/bro/base/frameworks/notice/./actions/email_admin.bro
      /usr/local/bro/share/bro/base/frameworks/notice/./actions/page.bro
      /usr/local/bro/share/bro/base/frameworks/notice/./actions/add-geodata.bro
      /usr/local/bro/share/bro/base/frameworks/notice/./extend-email/hostnames.bro
      /usr/local/bro/share/bro/base/frameworks/cluster/__load__.bro
        /usr/local/bro/share/bro/base/frameworks/cluster/./main.bro
          /usr/local/bro/share/bro/base/frameworks/control/__load__.bro
            /usr/local/bro/share/bro/base/frameworks/control/./main.bro
      /usr/local/bro/share/bro/base/frameworks/notice/./actions/pp-alarms.bro
    /usr/local/bro/share/bro/base/frameworks/dpd/__load__.bro
      /usr/local/bro/share/bro/base/frameworks/dpd/./main.bro
    /usr/local/bro/share/bro/base/frameworks/signatures/__load__.bro
      /usr/local/bro/share/bro/base/frameworks/signatures/./main.bro
    /usr/local/bro/share/bro/base/frameworks/packet-filter/__load__.bro
      /usr/local/bro/share/bro/base/frameworks/packet-filter/./main.bro
      /usr/local/bro/share/bro/base/frameworks/packet-filter/./netstats.bro
    /usr/local/bro/share/bro/base/frameworks/software/__load__.bro
      /usr/local/bro/share/bro/base/frameworks/software/./main.bro
    /usr/local/bro/share/bro/base/frameworks/communication/__load__.bro
      /usr/local/bro/share/bro/base/frameworks/communication/./main.bro
    /usr/local/bro/share/bro/base/frameworks/metrics/__load__.bro
      /usr/local/bro/share/bro/base/frameworks/metrics/./main.bro
      /usr/local/bro/share/bro/base/frameworks/metrics/./non-cluster.bro
    /usr/local/bro/share/bro/base/frameworks/intel/__load__.bro
      /usr/local/bro/share/bro/base/frameworks/intel/./main.bro
    /usr/local/bro/share/bro/base/frameworks/reporter/__load__.bro
      /usr/local/bro/share/bro/base/frameworks/reporter/./main.bro
    /usr/local/bro/share/bro/base/protocols/conn/__load__.bro
      /usr/local/bro/share/bro/base/protocols/conn/./main.bro
```

```
      /usr/local/bro/share/bro/base/protocols/conn/./contents.bro
      /usr/local/bro/share/bro/base/protocols/conn/./inactivity.bro
    /usr/local/bro/share/bro/base/protocols/dns/__load__.bro
      /usr/local/bro/share/bro/base/protocols/dns/./consts.bro
      /usr/local/bro/share/bro/base/protocols/dns/./main.bro
    /usr/local/bro/share/bro/base/protocols/ftp/__load__.bro
      /usr/local/bro/share/bro/base/protocols/ftp/./utils-commands.bro
      /usr/local/bro/share/bro/base/protocols/ftp/./main.bro
      /usr/local/bro/share/bro/base/protocols/ftp/./file-extract.bro
    /usr/local/bro/share/bro/base/protocols/http/__load__.bro
      /usr/local/bro/share/bro/base/protocols/http/./main.bro
      /usr/local/bro/share/bro/base/protocols/http/./utils.bro
      /usr/local/bro/share/bro/base/protocols/http/./file-ident.bro
      /usr/local/bro/share/bro/base/protocols/http/./file-hash.bro
      /usr/local/bro/share/bro/base/protocols/http/./file-extract.bro
    /usr/local/bro/share/bro/base/protocols/irc/__load__.bro
      /usr/local/bro/share/bro/base/protocols/irc/./main.bro
      /usr/local/bro/share/bro/base/protocols/irc/./dcc-send.bro
    /usr/local/bro/share/bro/base/protocols/smtp/__load__.bro
      /usr/local/bro/share/bro/base/protocols/smtp/./main.bro
      /usr/local/bro/share/bro/base/protocols/smtp/./entities.bro
      /usr/local/bro/share/bro/base/protocols/smtp/./entities-excerpt.bro
    /usr/local/bro/share/bro/base/protocols/ssh/__load__.bro
      /usr/local/bro/share/bro/base/protocols/ssh/./main.bro
    /usr/local/bro/share/bro/base/protocols/ssl/__load__.bro
      /usr/local/bro/share/bro/base/protocols/ssl/./consts.bro
      /usr/local/bro/share/bro/base/protocols/ssl/./main.bro
      /usr/local/bro/share/bro/base/protocols/ssl/./mozilla-ca-list.bro
    /usr/local/bro/share/bro/base/protocols/syslog/__load__.bro
      /usr/local/bro/share/bro/base/protocols/syslog/./consts.bro
      /usr/local/bro/share/bro/base/protocols/syslog/./main.bro
  /usr/local/bro/spool/installed-scripts-do-not-touch/site/local.bro
    /usr/local/bro/share/bro/policy/misc/loaded-scripts.bro
    /usr/local/bro/share/bro/policy/tuning/defaults/__load__.bro
      /usr/local/bro/share/bro/policy/tuning/defaults/./packet-fragments.bro
      /usr/local/bro/share/bro/policy/tuning/defaults/./warnings.bro
    /usr/local/bro/share/bro/policy/frameworks/software/vulnerable.bro
    /usr/local/bro/share/bro/policy/frameworks/software/version-changes.bro
    /usr/local/bro/share/bro/policy/protocols/ftp/software.bro
    /usr/local/bro/share/bro/policy/protocols/smtp/software.bro
    /usr/local/bro/share/bro/policy/protocols/ssh/software.bro
    /usr/local/bro/share/bro/policy/protocols/http/software.bro
    /usr/local/bro/share/bro/policy/protocols/dns/detect-external-names.bro
    /usr/local/bro/share/bro/policy/protocols/ftp/detect.bro
    /usr/local/bro/share/bro/policy/protocols/conn/known-hosts.bro
    /usr/local/bro/share/bro/policy/protocols/conn/known-services.bro
    /usr/local/bro/share/bro/policy/protocols/ssl/known-certs.bro
      /usr/local/bro/share/bro/policy/protocols/ssl/cert-hash.bro
    /usr/local/bro/share/bro/policy/protocols/ssl/validate-certs.bro
    /usr/local/bro/share/bro/policy/protocols/ssh/geo-data.bro
    /usr/local/bro/share/bro/policy/protocols/ssh/detect-bruteforcing.bro
    /usr/local/bro/share/bro/policy/protocols/ssh/interesting-hostnames.bro
    /usr/local/bro/share/bro/policy/protocols/http/detect-MHR.bro
    /usr/local/bro/share/bro/policy/protocols/http/detect-sqli.bro
  /usr/local/bro/share/bro/broctl/__load__.bro
    /usr/local/bro/share/bro/broctl/./main.bro
      /usr/local/bro/share/bro/policy/frameworks/control/controllee.bro
        /usr/local/bro/share/bro/policy/frameworks/communication/listen.bro
  /usr/local/bro/share/bro/broctl/standalone.bro
    /usr/local/bro/spool/tmp/check-config-bro/standalone-layout.bro
    /usr/local/bro/share/bro/policy/misc/trim-trace-file.bro
  /usr/local/bro/share/bro/broctl/auto.bro
    /usr/local/bro/spool/tmp/check-config-bro/local-networks.bro
    /usr/local/bro/spool/tmp/check-config-bro/broctl-config.bro
  /usr/local/bro/share/bro/broctl/check.bro
[BroControl] >
```

Appendix B — NMAP Log.

```
Starting Nmap 6.01 ( http://nmap.org ) at 2012-04-10 20:52 Vest-Europa (sommertid)
NSE: Loaded 177 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:52
Completed NSE at 20:52, 0.16s elapsed
Pre-scan script results:
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
Initiating Ping Scan at 20:52
Scanning 10.10.10.77 [7 ports]
Completed Ping Scan at 20:52, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:52
Completed Parallel DNS resolution of 1 host. at 20:52, 0.08s elapsed
Initiating SYN Stealth Scan at 20:52
Scanning 10.10.10.77 [1000 ports]
Discovered open port 22/tcp on 10.10.10.77
Discovered open port 445/tcp on 10.10.10.77
Discovered open port 111/tcp on 10.10.10.77
Discovered open port 21/tcp on 10.10.10.77
Discovered open port 3306/tcp on 10.10.10.77
Discovered open port 135/tcp on 10.10.10.77
Discovered open port 42/tcp on 10.10.10.77
Discovered open port 5060/tcp on 10.10.10.77
Discovered open port 5061/tcp on 10.10.10.77
Discovered open port 80/tcp on 10.10.10.77
Discovered open port 443/tcp on 10.10.10.77
Discovered open port 1433/tcp on 10.10.10.77
Completed SYN Stealth Scan at 20:52, 2.98s elapsed (1000 total ports)
Initiating UDP Scan at 20:52
Scanning 10.10.10.77 [1000 ports]
Increasing send delay for 10.10.10.77 from 0 to 50 due to max_successful_tryno increase to 5
Increasing send delay for 10.10.10.77 from 50 to 100 due to max_successful_tryno increase to 6
Warning: 10.10.10.77 giving up on port because retransmission cap hit (6).
Increasing send delay for 10.10.10.77 from 100 to 200 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 10.10.10.77 from 200 to 400 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 6.09% done; ETC: 21:00 (0:07:58 remaining)
Increasing send delay for 10.10.10.77 from 400 to 800 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 9.33% done; ETC: 21:03 (0:09:53 remaining)
UDP Scan Timing: About 12.40% done; ETC: 21:04 (0:10:43 remaining)
UDP Scan Timing: About 29.49% done; ETC: 21:06 (0:10:05 remaining)
UDP Scan Timing: About 36.54% done; ETC: 21:06 (0:09:19 remaining)
Discovered open port 111/udp on 10.10.10.77
UDP Scan Timing: About 42.66% done; ETC: 21:07 (0:08:34 remaining)
UDP Scan Timing: About 48.19% done; ETC: 21:07 (0:07:49 remaining)
UDP Scan Timing: About 53.49% done; ETC: 21:07 (0:07:04 remaining)
UDP Scan Timing: About 58.91% done; ETC: 21:07 (0:06:17 remaining)
UDP Scan Timing: About 64.53% done; ETC: 21:07 (0:05:27 remaining)
UDP Scan Timing: About 69.94% done; ETC: 21:07 (0:04:39 remaining)
UDP Scan Timing: About 75.34% done; ETC: 21:07 (0:03:51 remaining)
UDP Scan Timing: About 80.70% done; ETC: 21:07 (0:03:02 remaining)
UDP Scan Timing: About 85.66% done; ETC: 21:07 (0:02:15 remaining)
UDP Scan Timing: About 90.96% done; ETC: 21:07 (0:01:25 remaining)
UDP Scan Timing: About 96.17% done; ETC: 21:07 (0:00:36 remaining)
Completed UDP Scan at 21:08, 978.45s elapsed (1000 total ports)
Initiating Service scan at 21:08
Scanning 27 services on 10.10.10.77
Discovered open port 5060/udp on 10.10.10.77
Discovered open|filtered port 5060/udp on 10.10.10.77 is actually open
Service scan Timing: About 48.15% done; ETC: 21:09 (0:00:41 remaining)
Completed Service scan at 21:10, 126.28s elapsed (27 services on 1 host)
Initiating RPCGrind Scan against 10.10.10.77 at 21:10
Completed RPCGrind Scan against 10.10.10.77 at 21:10, 0.03s elapsed (2 ports)
Initiating OS detection (try #1) against 10.10.10.77
Retrying OS detection (try #2) against 10.10.10.77
WARNING:  OS didn't match until try #2
Initiating Traceroute at 21:10
Completed Traceroute at 21:10, 0.02s elapsed
Initiating Parallel DNS resolution of 1 host. at 21:10
Completed Parallel DNS resolution of 1 host. at 21:10, 0.01s elapsed
NSE: Script scanning 10.10.10.77.
Initiating NSE at 21:10
Completed NSE at 21:13, 160.39s elapsed
Nmap scan report for 10.10.10.77
Host is up (0.00022s latency).
```

```
Not shown: 1973 closed ports
PORT      STATE         SERVICE              VERSION
21/tcp    open          ftp                  Dionaea honeypot ftpd
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
|_banner: 220 Welcome to the ftp service
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
22/tcp    open          ssh                  OpenSSH 5.5p1 Debian 6+squeeze2 (protocol 2.0)
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
| ssh2-enum-algos:
|   kex_algorithms (4)
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group-exchange-sha1
|       diffie-hellman-group14-sha1
|       diffie-hellman-group1-sha1
|   server_host_key_algorithms (2)
|       ssh-rsa
|       ssh-dss
|   encryption_algorithms (13)
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|       arcfour256
|       arcfour128
|       aes128-cbc
|       3des-cbc
|       blowfish-cbc
|       cast128-cbc
|       aes192-cbc
|       aes256-cbc
|       arcfour
|       rijndael-cbc@lysator.liu.se
|   mac_algorithms (7)
|       hmac-md5
|       hmac-sha1
|       umac-64@openssh.com
|       hmac-ripemd160
|       hmac-ripemd160@openssh.com
|       hmac-sha1-96
|       hmac-md5-96
|   compression_algorithms (2)
|       none
|_      zlib@openssh.com
| ssh-hostkey: 1024 07:48:2e:64:13:f7:80:12:5b:1e:72:90:cf:79:6e:03 (DSA)
|_2048 b6:dc:91:82:92:57:97:51:79:f0:55:5b:9e:26:04:58 (RSA)
|_banner: SSH-2.0-OpenSSH_5.5p1 Debian-6+squeeze2
42/tcp    open          tcpwrapped
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
80/tcp    open          http                 Apache httpd 2.2.16 ((Debian))
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
|_http-google-malware: [ERROR] No API key found. Update the variable APIKEY in http-google-malware or set it in the argument http-g
| http-grep:
|_  ERROR: Argument http-grep.match was not set
|_http-date: Mon, 18 Jun 2012 11:49:04 GMT; +68d16h38m22s from local time.
|_http-methods: GET HEAD POST OPTIONS
| http-headers:
|   Date: Mon, 18 Jun 2012 11:49:07 GMT
|   Server: Apache/2.2.16 (Debian)
|   Vary: Accept-Encoding
|   Connection: close
|   Content-Type: text/html;charset=UTF-8
|
|_  (Request type: HEAD)
|_http-title: Index of /
| http-email-harvest:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.10.10.77
|   rdd@cert.org
|   diver@users.sourceforge.net
|   kjohnson@secureideas.net
|   roman@danyliw.com
|_  base@secureideas.net
| http-auth-finder:
```

```
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.10.10.77
|   url                               method
|   http://10.10.10.77/base/          FORM
|_  http://10.10.10.77/base/index.php  FORM
111/tcp   open          rpcbind (rpcbind V2) 2 (rpc #100000)
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
| rpcinfo:
|   program version   port/proto  service
|   100000  2            111/tcp  rpcbind
|   100000  2            111/udp  rpcbind
|   100024  1          38339/udp  status
|_  100024  1          58290/tcp  status
135/tcp   open          msrpc?
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
443/tcp   open          ssl/http             Apache httpd 2.2.16 ((Debian))
|_http-google-malware: [ERROR] No API key found. Update the variable APIKEY in http-google-malware or set it in the argument http-g
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
| http-grep:
|_  ERROR: Argument http-grep.match was not set
|_http-title: Index of /
|_http-date: Mon, 18 Jun 2012 11:49:04 GMT; +68d16h38m22s from local time.
| ssl-cert: Subject: commonName=pig1.lysglimt.net
| Issuer: commonName=pig1.lysglimt.net
| Public Key type: rsa
| Public Key bits: 2048
| Not valid before: 2011-09-01 20:54:19
| Not valid after:  2021-08-29 20:54:19
| MD5:   88f6 c790 9da2 74b1 ac1d 9462 11c8 7d56
|_SHA-1: 2f53 f672 efbe b02e 824b 008b 1944 5da6 9fd0 a385
|_http-methods: GET HEAD POST OPTIONS
| http-headers:
|   Date: Mon, 18 Jun 2012 11:49:07 GMT
|   Server: Apache/2.2.16 (Debian)
|   Vary: Accept-Encoding
|   Connection: close
|   Content-Type: text/html;charset=UTF-8
|
|_  (Request type: HEAD)
| http-auth-finder:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.10.10.77
|   url                                method
|   https://10.10.10.77/base/          FORM
|_  https://10.10.10.77/base/index.php  FORM
| http-email-harvest:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.10.10.77
|   rdd@cert.org
|   diver@users.sourceforge.net
|   kjohnson@secureideas.net
|   roman@danyliw.com
|_  base@secureideas.net
| ssl-google-cert-catalog:
|_  No DB entry
445/tcp   open          microsoft-ds         Dionaea honeypot smbd
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
1433/tcp  open          ms-sql-s             Microsoft SQL Server 2000 8.00.528.00; SP1+
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
| ms-sql-query:
|   (Use --script-args=ms-sql-query.query='<QUERY>' to change query.)
|   [10.10.10.77:1433]
|_    ERROR: No login credentials
| ms-sql-hasdbaccess:
|   [10.10.10.77:1433]
|_    ERROR: No login credentials.
| ms-sql-tables:
|   [10.10.10.77:1433]
|_    ERROR: No login credentials.
| ms-sql-dump-hashes:
| [10.10.10.77:1433]
|_  ERROR: No login credentials
| ms-sql-config:
|   [10.10.10.77:1433]
```

```
|_    ERROR: No login credentials
3306/tcp  open          mysql               MySQL 5.0.54
| mysql-audit:
|_  No audit rulebase file was supplied (see mysql-audit.filename)
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
| mysql-info: Protocol: 10
| Version: 5.0.54
| Thread ID: 1729232896
| Some Capabilities: Connect with DB, Compress, Transactions, Secure Connection
| Status: Autocommit
|_Salt: aaaaaaaa
| banner: 4\x00\x00\x00\x0A5.0.54\x00\x00\x00\x12gaaaaaaaa\x00,\xA2!\x02\
|_x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00            \x00
5060/tcp  open          sip                 (SIP end point; Status: 200 OK)
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
5061/tcp  open          ssl/sip             (SIP end point; Status: 200 OK)
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
|_sslv2: server still supports SSLv2
| ssl-cert: Subject: commonName=Nepenthes Development Team/organizationName=dionaea.carnivore.it/countryName=DE
| Issuer: commonName=Nepenthes Development Team/organizationName=dionaea.carnivore.it/countryName=DE
| Public Key type: rsa
| Public Key bits: 2048
| Not valid before: 2012-06-18 08:59:14
| Not valid after:  2013-06-18 08:59:14
| MD5:   ff46 80f9 664b f3d0 afb4 e6ce 5df0 82e4
|_SHA-1: bb5c 8bc8 7d52 3327 b32a 5a3d dd8a de5c ffb0 8893
| ssl-google-cert-catalog:
|_  No DB entry
69/udp    open|filtered tftp
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
111/udp   open          rpcbind (rpcbind V2) 2 (rpc #100000)
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
| rpcinfo:
|   program version   port/proto  service
|   100000  2           111/tcp  rpcbind
|   100000  2           111/udp  rpcbind
|   100024  1         38339/udp  status
|_  100024  1         58290/tcp  status
639/udp   open|filtered msdp
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
983/udp   open|filtered unknown
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
1234/udp  open|filtered search-agent
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
2223/udp  open|filtered rockwell-csp2
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
5060/udp  open          sip                 (SIP end point; Status: 200 OK)
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
17321/udp open|filtered unknown
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
17663/udp open|filtered unknown
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
19154/udp open|filtered unknown
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
25931/udp open|filtered unknown
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
31681/udp open|filtered unknown
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
49640/udp open|filtered unknown
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
```

```
51554/udp open|filtered unknown
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
51905/udp open|filtered unknown
| dns-client-subnet-scan:
|_  ERROR: dns-client-subnet-scan.domain was not specified
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at http:/
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port5060-TCP:V=6.01%I=7%D=4/10%Time=4F848540%P=i686-pc-windows-windows%
SF:r(SIPOptions,10A,"SIP/2\.0\x20200\x20OK\r\nContent-Length:\x200\r\nVia:
SF:\x20SIP/2\.0/TCP\x20nm;branch=foo\r\nFrom:\x20sip:nm@nm;tag=root\r\nAcc
SF:ept:\x20application/sdp\r\nTo:\x20sip:nm2@nm2\r\nContact:\x20sip:nm2@nm
SF:2\r\nCSeq:\x2042\x20OPTIONS\r\nAllow:\x20REGISTER,\x20OPTIONS,\x20INVIT
SF:E,\x20CANCEL,\x20BYE,\x20ACK\r\nCall-ID:\x2050000\r\nAccept-Language:\x
SF:20en\r\n\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port5061-TCP:V=6.01%T=SSL%I=7%D=4/10%Time=4F84854E%P=i686-pc-windows-wi
SF:ndows%r(SIPOptions,10A,"SIP/2\.0\x20200\x20OK\r\nContent-Length:\x200\r
SF:\nVia:\x20SIP/2\.0/TCP\x20nm;branch=foo\r\nFrom:\x20sip:nm@nm;tag=root\
SF:r\nAccept:\x20application/sdp\r\nTo:\x20sip:nm2@nm2\r\nContact:\x20sip:
SF:nm2@nm2\r\nCSeq:\x2042\x20OPTIONS\r\nAllow:\x20REGISTER,\x20OPTIONS,\x2
SF:0INVITE,\x20CANCEL,\x20BYE,\x20ACK\r\nCall-ID:\x2050000\r\nAccept-Langu
SF:age:\x20en\r\n\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port5060-UDP:V=6.01%I=7%D=4/10%Time=4F848535%P=i686-pc-windows-windows%
SF:r(SIPOptions,110,"SIP/2\.0\x20200\x20OK\r\nContent-Length:\x200\r\nVia:
SF:\x20SIP/2\.0/UDP\x20nm;branch=foo;rport\r\nFrom:\x20sip:nm@nm;tag=root\
SF:r\nAccept:\x20application/sdp\r\nTo:\x20sip:nm2@nm2\r\nContact:\x20sip:
SF:nm2@nm2\r\nCSeq:\x2042\x20OPTIONS\r\nAllow:\x20REGISTER,\x20OPTIONS,\x2
SF:0INVITE,\x20CANCEL,\x20BYE,\x20ACK\r\nCall-ID:\x2050000\r\nAccept-Langu
SF:age:\x20en\r\n\r\n");
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:kernel:2.4
OS details: DD-WRT v24-sp1 (Linux 2.4.36)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

Host script results:
|_path-mtu: PMTU == 1500
|_smbv2-enabled: Server doesn't support SMBv2 protocol
|_ipidseq: All zeros
| firewalk:
| HOP  HOST           PROTOCOL  BLOCKED PORTS
|_0    192.168.0.104  udp       69,639,983,1234,2223,17321,17663,19154,25931,31681
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   NetBIOS computer name: HOMEUSER-3AF6FE
|   Workgroup: WORKGROUP
|_  System time: 2012-06-18 10:59:13 UTC+1
| smb-mbenum:
|_  ERROR: MSRPC: NetServerEnum2 call failed
| qscan:
| PORT  FAMILY  MEAN (us)   STDDEV       LOSS (%)
| 1     0       87500.00    107108.72    0.0%
| 21    0       115600.00   280998.30    0.0%
| 22    0       559600.00   1441788.41   0.0%
| 42    0       3862600.00  11885253.59  0.0%
| 80    0       2846900.00  8827273.10   0.0%
| 111   0       206200.00   478042.72    0.0%
| 135   0       37400.00    52652.32     0.0%
| 443   0       43800.00    51475.56     0.0%
|_445   0       56400.00    75026.22     0.0%
| ms-sql-info:
|   [10.10.10.77:1433]
|     Version: Microsoft SQL Server 2000 SP1+
|       Version number: 8.00.528.00
|       Product: Microsoft SQL Server 2000
|       Service pack level: SP1
|       Post-SP patches applied: Yes
|_    TCP port: 1433
```

```
TRACEROUTE (using port 1025/tcp)
HOP RTT     ADDRESS
1   0.00 ms 10.10.10.77

NSE: Script Post-scanning.
Initiating NSE at 21:13
Completed NSE at 21:13, 0.00s elapsed
Read data files from: C:\Programfiler\Nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1276.70 seconds
           Raw packets sent: 2593 (108.139KB) | Rcvd: 2157 (104.311KB)
```

References

[1] Paul Baecher and Markus Koetter. *dionaea, catches bugs*. Accessed 2012-06-16. June 2012. URL: http://dionaea.carnivore.it/.

[2] Gilles Berger-Sabbatel and Andrzej Duda. "Analysis of Malware Network Activity". In: *Multimedia Communications, Services and Security*. Ed. by Andrzej Dziech and Andrzej Czyzewski. Vol. 149. Communications in Computer and Information Science. 10.1007/978-3-642-21512-4. Springer Berlin Heidelberg, 2011, pp. 207–215. ISBN: 978-3-642-21512-4. URL: http://dx.doi.org/10.1007/978-3-642-21512-4.

[3] *BRIDGE Technology co as*. Accessed 2012-06-16. June 2012. URL: http://www.bridgetech.tv/.

[4] M. Cotton et al. *Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry*. Internet Draft (draft-ietf-tsvwg-iana-ports-10.txt). Feb. 2011. URL: http://tools.ietf.org/id/draft-ietf-tsvwg-iana-ports-10.txt.

[5] Debian Project. *Debian*. Accessed: 2012-06-17. URL: http://www.debian.org/intro/about.

[6] Debian Project. *Debian Licensing*. Accessed: 2012-06-17. URL: http://www.debian.org/legal/licenses/index.en.html.

[7] *Git*. Accessed: 2012-06-18. URL: http://git-scm.com/about.

[8] Roger Larsen. *Protocol Detection Capabilities in Bro*. Tech. rep. IMT-4022 Digital Forensics II, spring 2012. Gjøvik University College, June 2012.

[9] Gordon Fyodor Lyon. *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. USA: Insecure, 2009. ISBN: 0979958717, 9780979958717.

[10] Microsoft. *What is Windows 7?* Accessed: 2012-06-17. Microsoft Corp. June 2012. URL: http://windows.microsoft.com/en-US/windows7/products/what-is.

[11] Microsoft. *What is Windows XP?* Accessed: 2012-06-17. Microsoft Corp. June 2012. URL: http://windows.microsoft.com/en-us/windows/products/windows-xp.

[12] Ruoming Pang et al. "binpac: a yacc for writing application protocol parsers". In: *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*. IMC '06. Rio de Janeriro, Brazil: ACM, 2006, pp. 289–300. ISBN: 1-59593-561-4. DOI: 10.1145/1177080.1177119. URL: http://doi.acm.org/10.1145/1177080.1177119.

[13] The Bro Project. *Downloads*. The Bro Team. May 2012. URL: http://www.bro-ids.org/download/index.html.

[14] E. Rescorla. *HTTP Over TLS*. RFC 2818 (Informational). Updated by RFC 5785. Internet Engineering Task Force, May 2000. URL: http://www.ietf.org/rfc/rfc2818.txt.

[15] Miroslaw Skrzewski. "Network Malware Activity, A View from Honeypot Systems". In: *Computer Networks*. Ed. by Andrzej Kwiecien, Piotr Gaj, and Piotr Stera. Vol. 291. Communications in Computer and Information Science. 10.1007/978-3-642-31217-5. Springer Berlin Heidelberg, 2012, pp. 198–206. ISBN: 978-3-642-31217-5. URL: http://dx.doi.org/10.1007/978-3-642-31217-5.

[16] The Bro Project. *The Bro Network Security Monitor*. Accessed 2011-09-14. URL: http://bro-ids.org/.

[17] The Bro Project et al. *The Time Machine*. Accessed 2012-05-29. Technische Universität Berlin, the Technische Universität München, and the ICSI (University of California Berkeley). May 2012.

[18] The FreeBSD Project. *The 4.4BSD Copyright*. Accessed: 2012-06-17. June 2012. URL: `http://www.freebsd.org/copyright/license.html`.

[19] The FreeBSD Project. *The FreeBSD Project*. Accessed: 2012-06-17. June 2012. URL: `http://www.freebsd.org/about.html`.