INTEL GATHERING FOR PENETRATION TESTERS: OPENING DOORS WITH METADATA

Chris Patten

Packet Research

# WHOAMI

- Security practitioner…not an expert
- Focus on cross disciplinary assessments
  - Breach Assessments (Red Team)
  - Penetration Testing (Layer 1-8)
  - Social Engineering (i.e. Layer 8)
  - Wireless Assessments
  - Physical Security Assessments
  - Blended Assessments
- Developer and general code monkey
- Break | smash | reassemble | do it all over again
- Founder | Principal of Packet Research

WHAT IS AN EFFECTIVE PEN TEST?

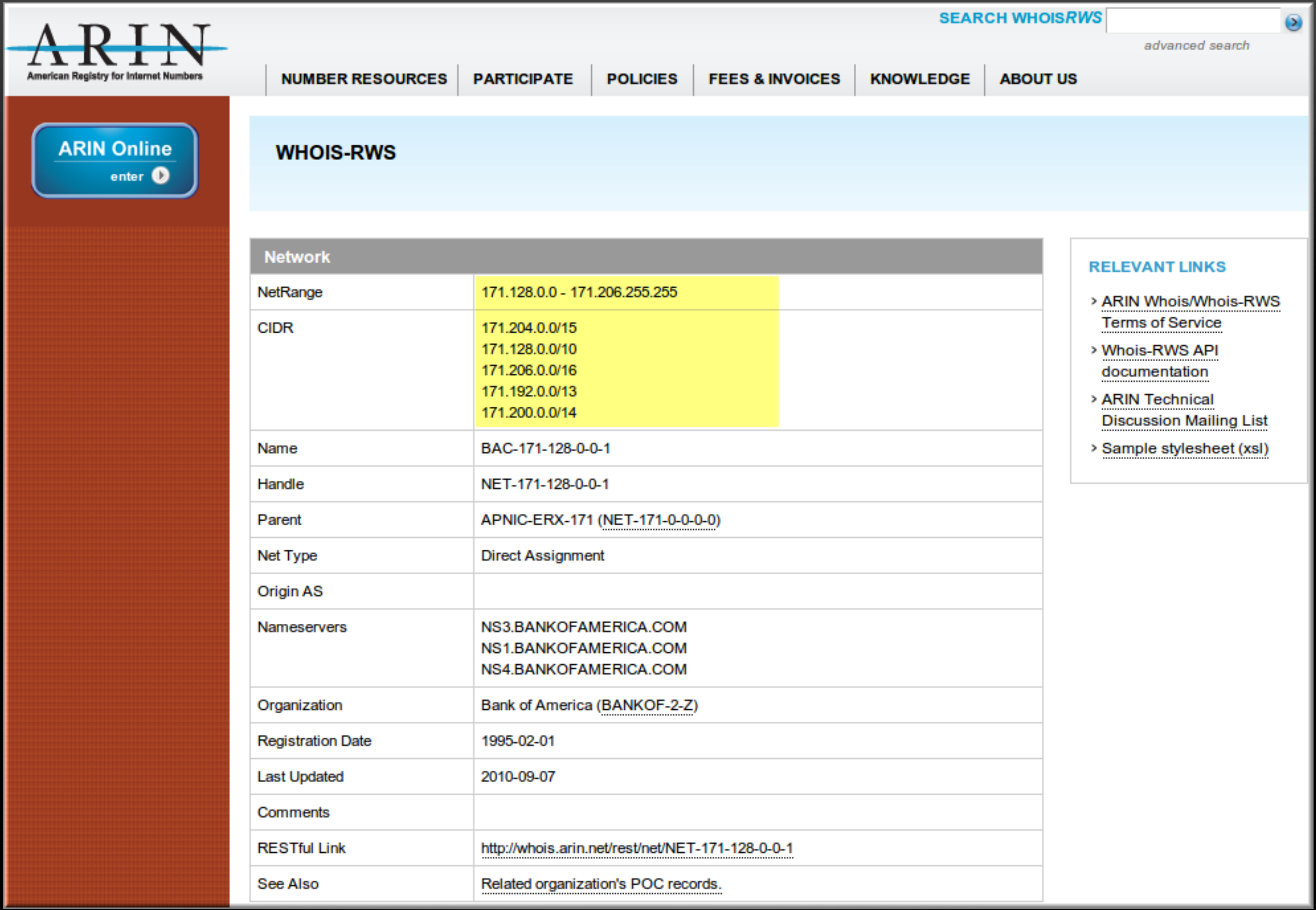
- Part of an overall security assessment framework
- Builds on previously identified vulnerabilities
    - Vulnerability Assessment phase
    - Manual human inspection
- Creates impact, not just “It is vulnerable”
    - Not enough to declare “local root” or “domain admin”
- Scoping is everything
    - What will adversely affect the business?
    - Financial loss, brand defamation, recipe for the secret sauce
    - Defines the “success” and “failure” criteria
    - Provides actionable “severity” and “prioritization”

WHY IS INTEL SO IMPORTANT TO A PEN TEST?

- Validates the target
- Identifies supporting data to construct an attack
- Uncovers vulnerabilities that may have gone undetected
- Materializes the public exposure of an organization
- Increases the probability that an attack will be successful

THE CASE STUDY (FINANCIAL INSTITUTION)

- Passive reconnaissance only
- Never touch the target with active scan packets
- Use publicly available toolsets to gather info
- Identify external points of access
    - Web authentication forms
    - VPN | Citrix | OWA
- Examine data for the goods
- Use the data to build the attack

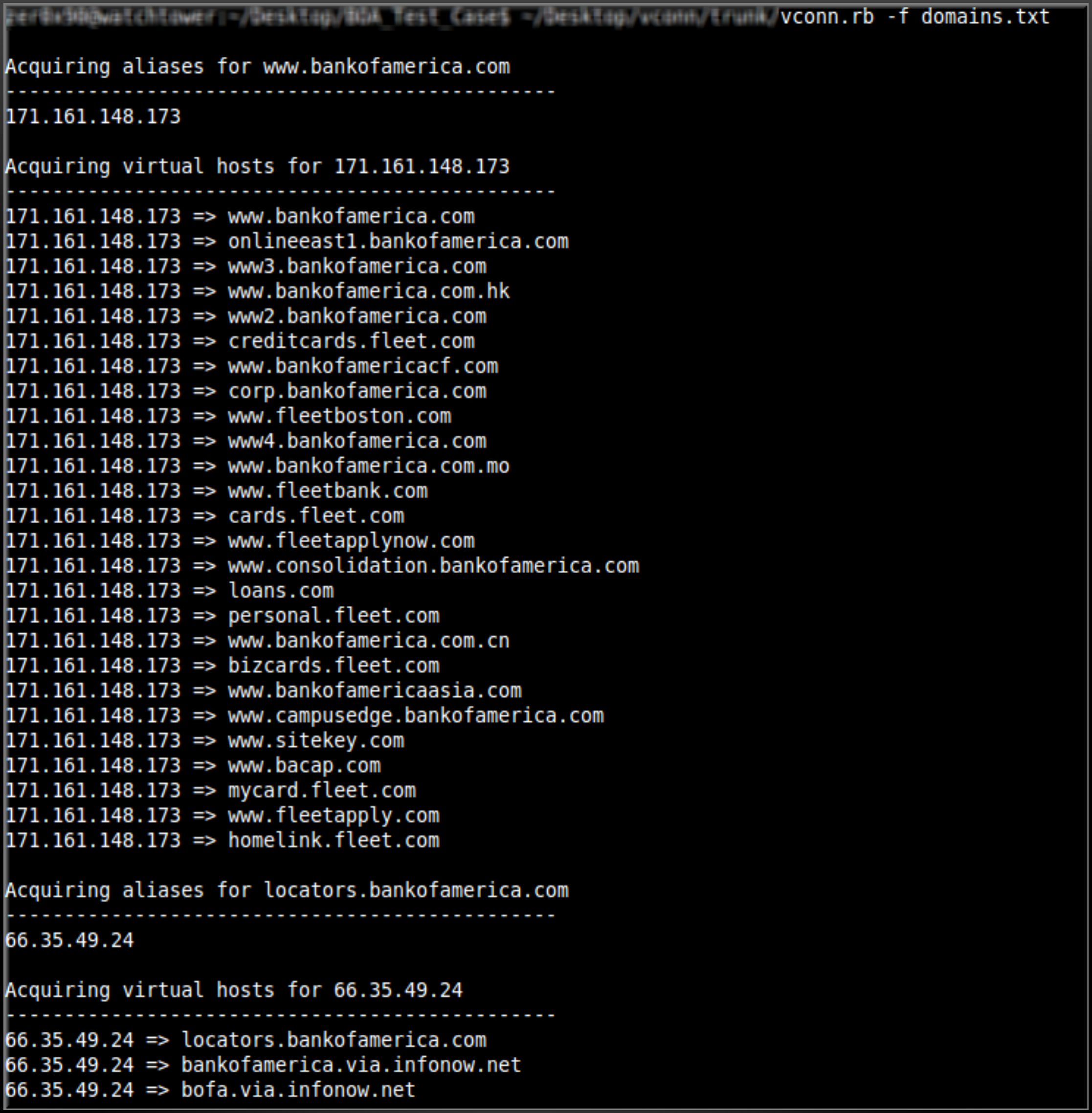


WHOIS-RWS

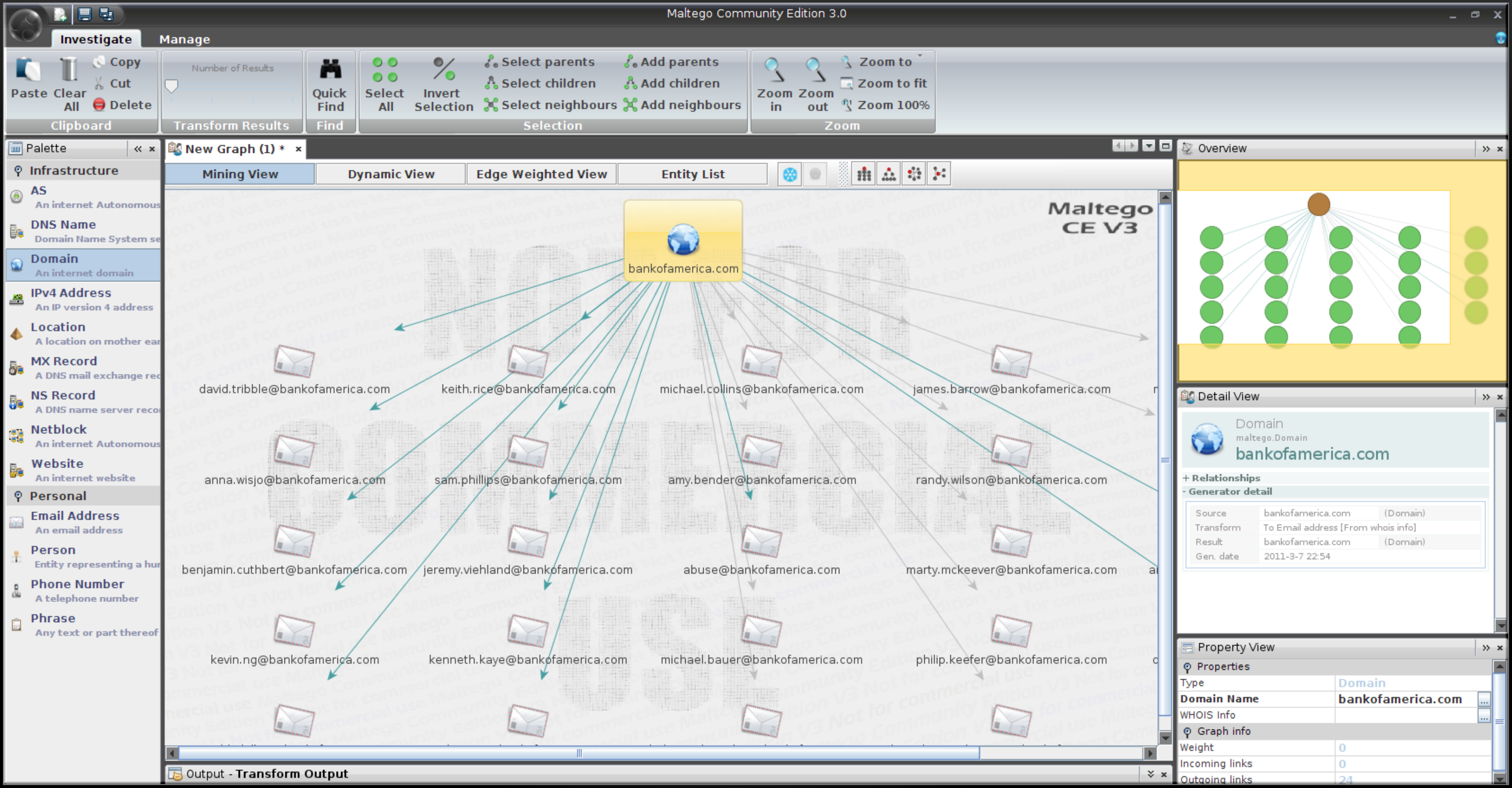
Network	
NetRange	171.128.0.0 - 171.206.255.255
CIDR	171.204.0.0/15 171.128.0.0/10 171.206.0.0/16 171.192.0.0/13 171.200.0.0/14
Name	BAC-171-128-0-0-1
Handle	NET-171-128-0-0-1
Parent	APNIC-ERX-171 (NET-171-0-0-0-0)
Net Type	Direct Assignment
Origin AS	
Nameservers	NS3.BANKOFAMERICA.COM NS1.BANKOFAMERICA.COM NS4.BANKOFAMERICA.COM
Organization	Bank of America (BANKOF-2-Z)
Registration Date	1995-02-01
Last Updated	2010-09-07
Comments	
RESTful Link	http://whois.arin.net/rest/net/NET-171-128-0-0-1
See Also	Related organization's POC records.

RELEVANT LINKS

- ARIN Whois/Whois-RWS Terms of Service
- Whois-RWS API documentation
- ARIN Technical Discussion Mailing List
- Sample stylesheet (xsl)

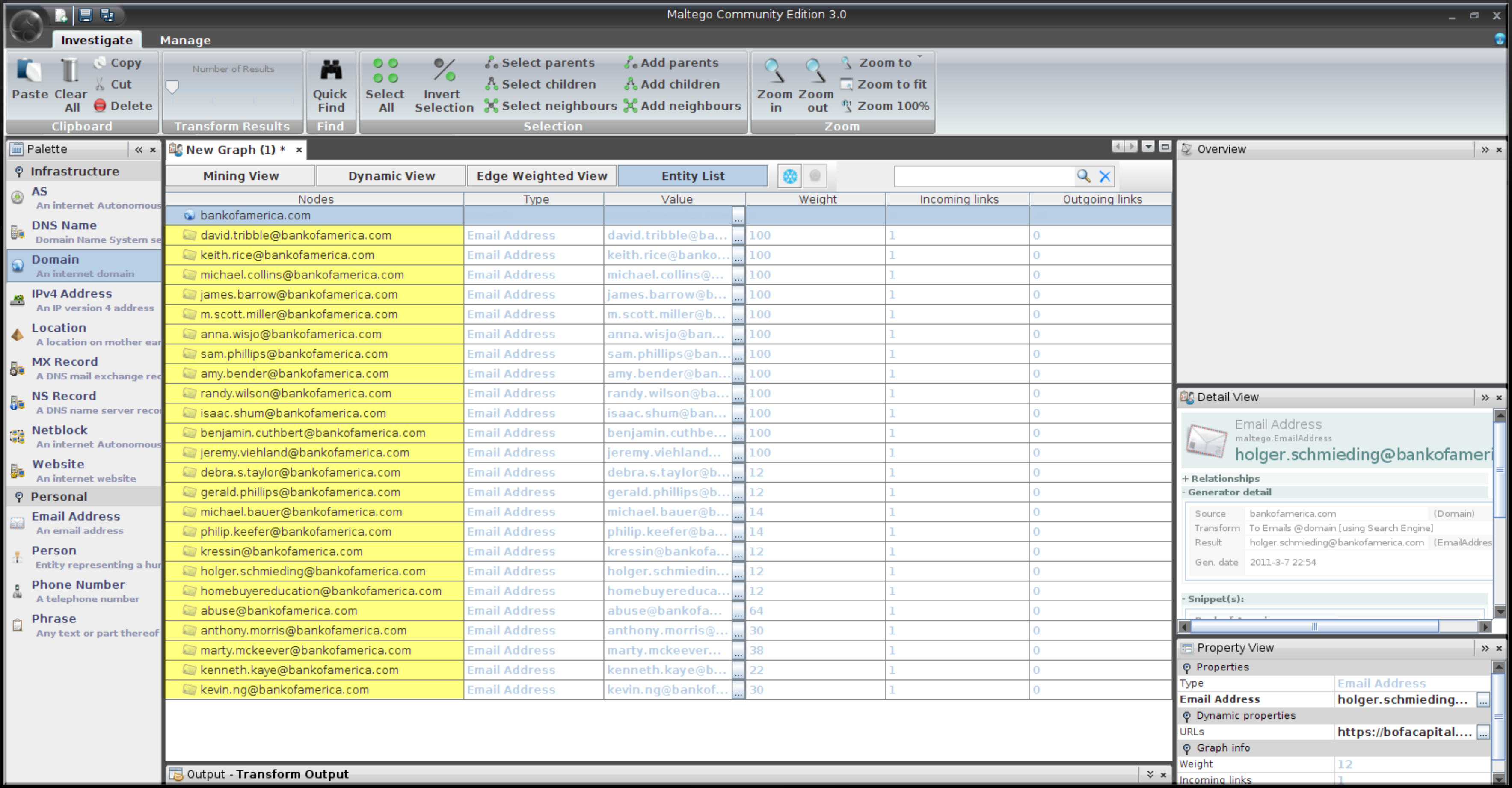


```
[redacted]vconn.rb -f domains.txt

Acquiring aliases for www.bankofamerica.com
-----------------------------------------------
171.161.148.173

Acquiring virtual hosts for 171.161.148.173
-----------------------------------------------
171.161.148.173 => www.bankofamerica.com
171.161.148.173 => onlineeast1.bankofamerica.com
171.161.148.173 => www3.bankofamerica.com
171.161.148.173 => www.bankofamerica.com.hk
171.161.148.173 => www2.bankofamerica.com
171.161.148.173 => creditcards.fleet.com
171.161.148.173 => www.bankofamericacf.com
171.161.148.173 => corp.bankofamerica.com
171.161.148.173 => www.fleetboston.com
171.161.148.173 => www4.bankofamerica.com
171.161.148.173 => www.bankofamerica.com.mo
171.161.148.173 => www.fleetbank.com
171.161.148.173 => cards.fleet.com
171.161.148.173 => www.fleetapplynow.com
171.161.148.173 => www.consolidation.bankofamerica.com
171.161.148.173 => loans.com
171.161.148.173 => personal.fleet.com
171.161.148.173 => www.bankofamerica.com.cn
171.161.148.173 => bizcards.fleet.com
171.161.148.173 => www.bankofamericaasia.com
171.161.148.173 => www.campusedge.bankofamerica.com
171.161.148.173 => www.sitekey.com
171.161.148.173 => www.bacap.com
171.161.148.173 => mycard.fleet.com
171.161.148.173 => www.fleetapply.com
171.161.148.173 => homelink.fleet.com

Acquiring aliases for locators.bankofamerica.com
-----------------------------------------------
66.35.49.24

Acquiring virtual hosts for 66.35.49.24
-----------------------------------------------
66.35.49.24 => locators.bankofamerica.com
66.35.49.24 => bankofamerica.via.infonow.net
66.35.49.24 => bofa.via.infonow.net
```



Source	bankofamerica.com	(Domain)
Transform	To Email address [From whois info]	
Result	bankofamerica.com	(Domain)
Gen. date	2011-3-7 22:54	

Type	Domain
Domain Name	bankofamerica.com
WHOIS Info	
Weight	0
Incoming links	0
Outgoing links	24



Nodes	Type	Value	Weight	Incoming links	Outgoing links
bankofamerica.com					
david.tribble@bankofamerica.com	Email Address	david.tribble@ba...	100	1	0
keith.rice@bankofamerica.com	Email Address	keith.rice@banko...	100	1	0
michael.collins@bankofamerica.com	Email Address	michael.collins@...	100	1	0
james.barrow@bankofamerica.com	Email Address	james.barrow@b...	100	1	0
m.scott.miller@bankofamerica.com	Email Address	m.scott.miller@b...	100	1	0
anna.wisjo@bankofamerica.com	Email Address	anna.wisjo@ban...	100	1	0
sam.phillips@bankofamerica.com	Email Address	sam.phillips@ban...	100	1	0
amy.bender@bankofamerica.com	Email Address	amy.bender@ban...	100	1	0
randy.wilson@bankofamerica.com	Email Address	randy.wilson@ba...	100	1	0
isaac.shum@bankofamerica.com	Email Address	isaac.shum@ban...	100	1	0
benjamin.cuthbert@bankofamerica.com	Email Address	benjamin.cuthbe...	100	1	0
jeremy.viehland@bankofamerica.com	Email Address	jeremy.viehland...	100	1	0
debra.s.taylor@bankofamerica.com	Email Address	debra.s.taylor@b...	12	1	0
gerald.phillips@bankofamerica.com	Email Address	gerald.phillips@b...	12	1	0
michael.bauer@bankofamerica.com	Email Address	michael.bauer@b...	14	1	0
philip.keefer@bankofamerica.com	Email Address	philip.keefer@ba...	14	1	0
kressin@bankofamerica.com	Email Address	kressin@bankofa...	12	1	0
holger.schmieding@bankofamerica.com	Email Address	holger.schmiedin...	12	1	0
homebuyereducation@bankofamerica.com	Email Address	homebuyereduca...	12	1	0
abuse@bankofamerica.com	Email Address	abuse@bankofa...	64	1	0
anthony.morris@bankofamerica.com	Email Address	anthony.morris@...	30	1	0
marty.mckeever@bankofamerica.com	Email Address	marty.mckeever...	38	1	0
kenneth.kaye@bankofamerica.com	Email Address	kenneth.kaye@b...	22	1	0
kevin.ng@bankofamerica.com	Email Address	kevin.ng@bankof...	30	1	0

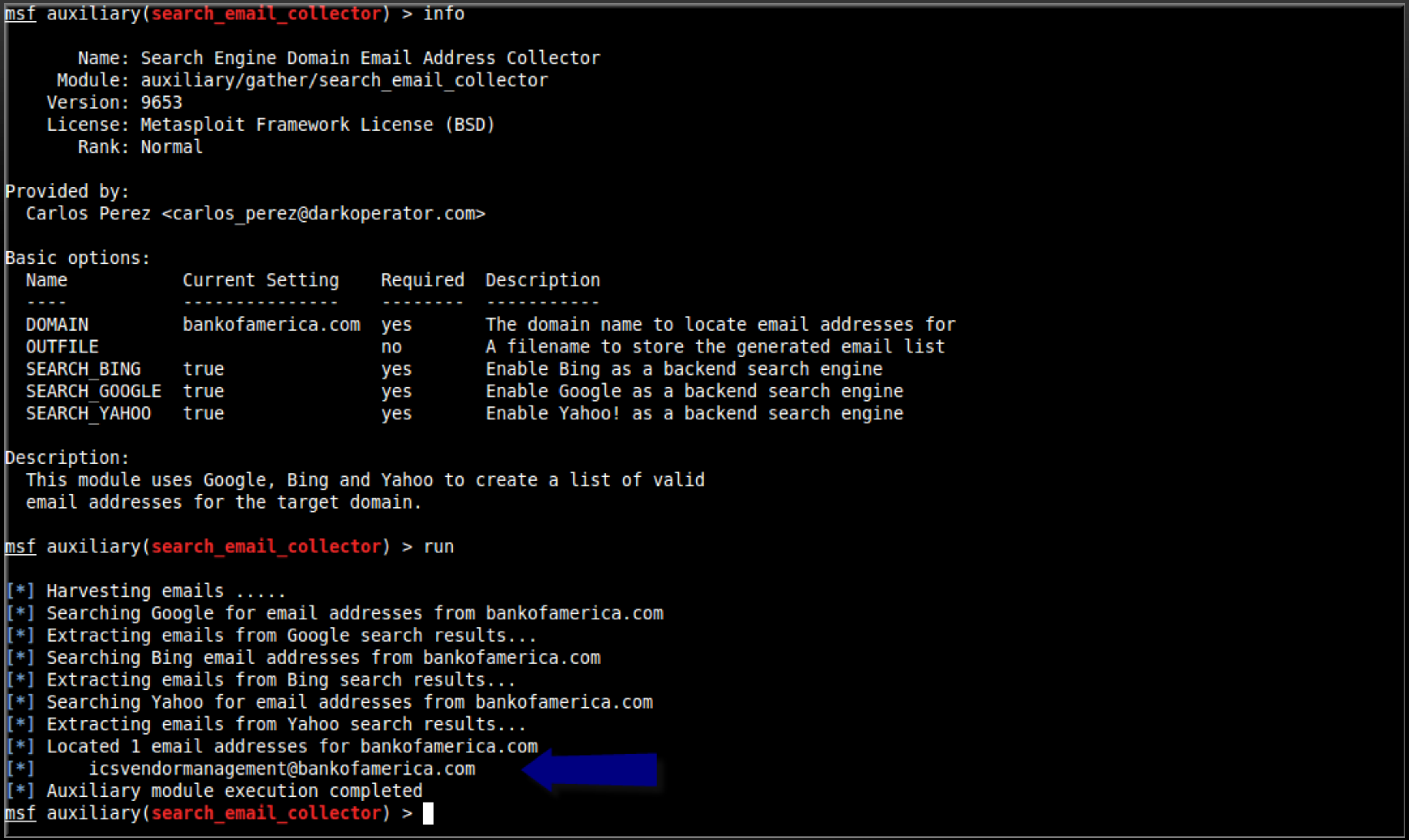
Email Address
maltego.EmailAddress
holger.schmieding@bankofameri

+ Relationships
- Generator detail

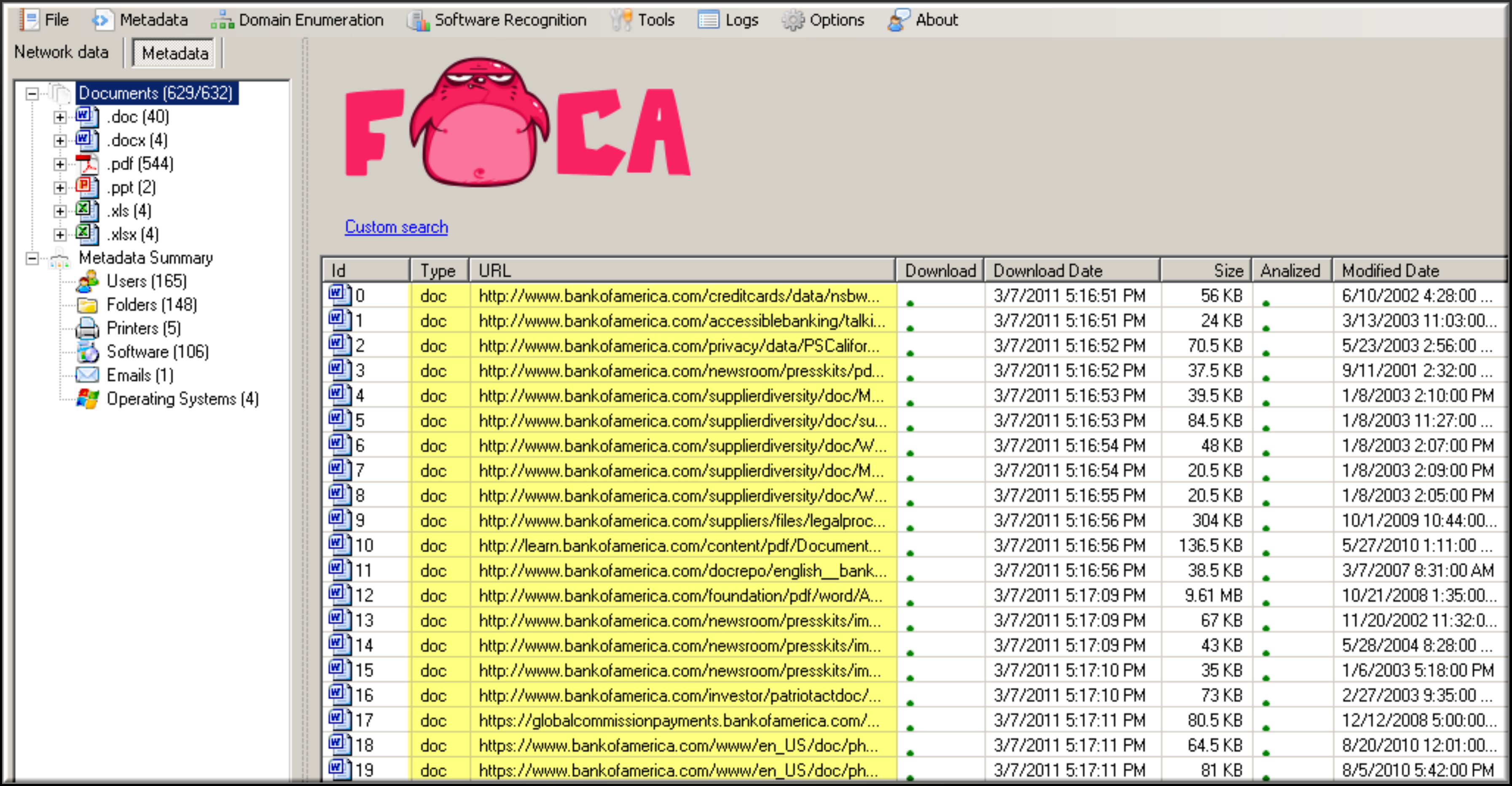
Source	bankofamerica.com	(Domain)
Transform	To Emails @domain [using Search Engine]	
Result	holger.schmieding@bankofamerica.com	(EmailAddres
Gen. date	2011-3-7 22:54	

- Snippet(s):

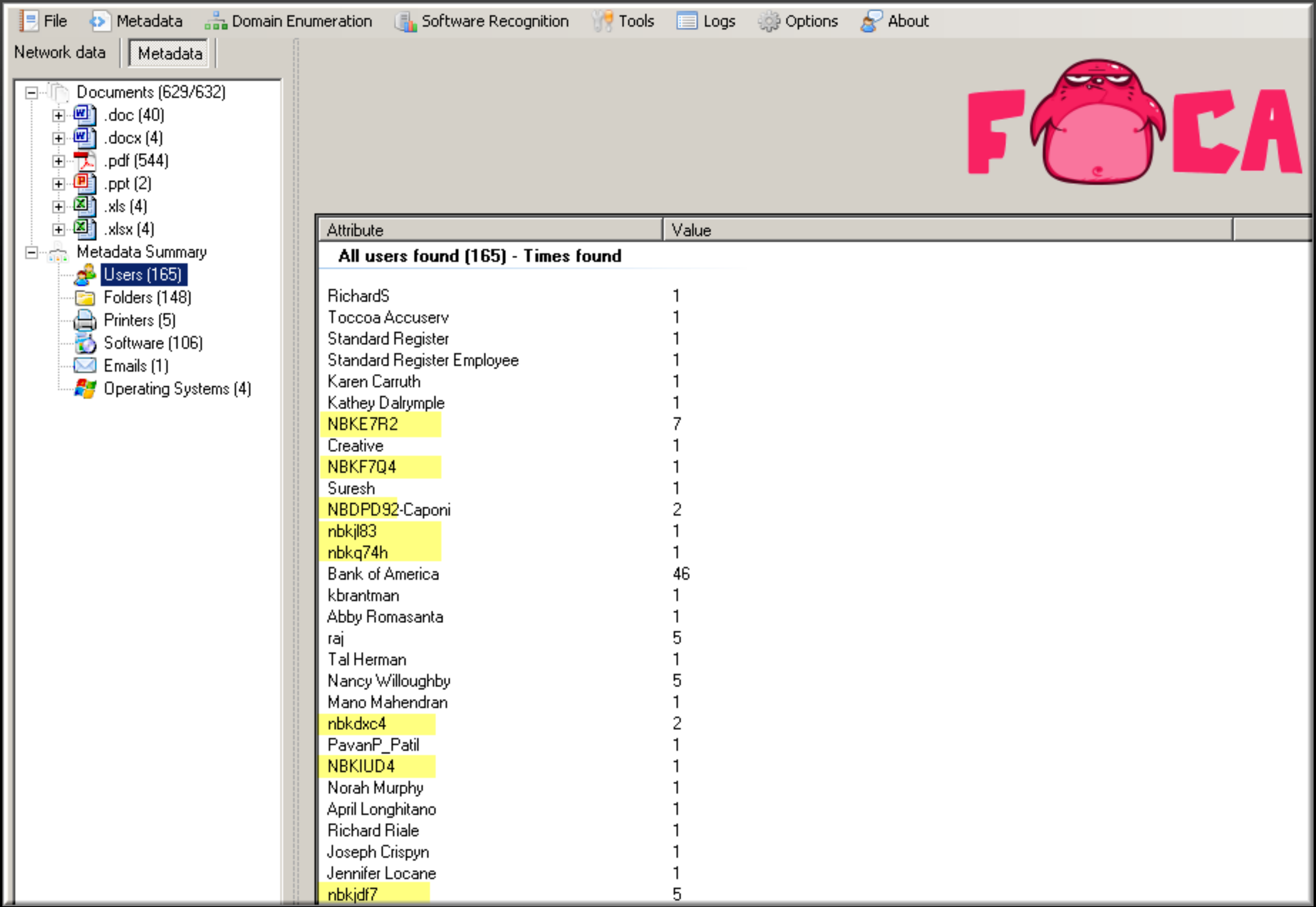
Properties	
Type	Email Address
Email Address	holger.schmieding...
Dynamic properties	
URLs	https://bofacapital....
Graph info	
Weight	12
Incoming links	1



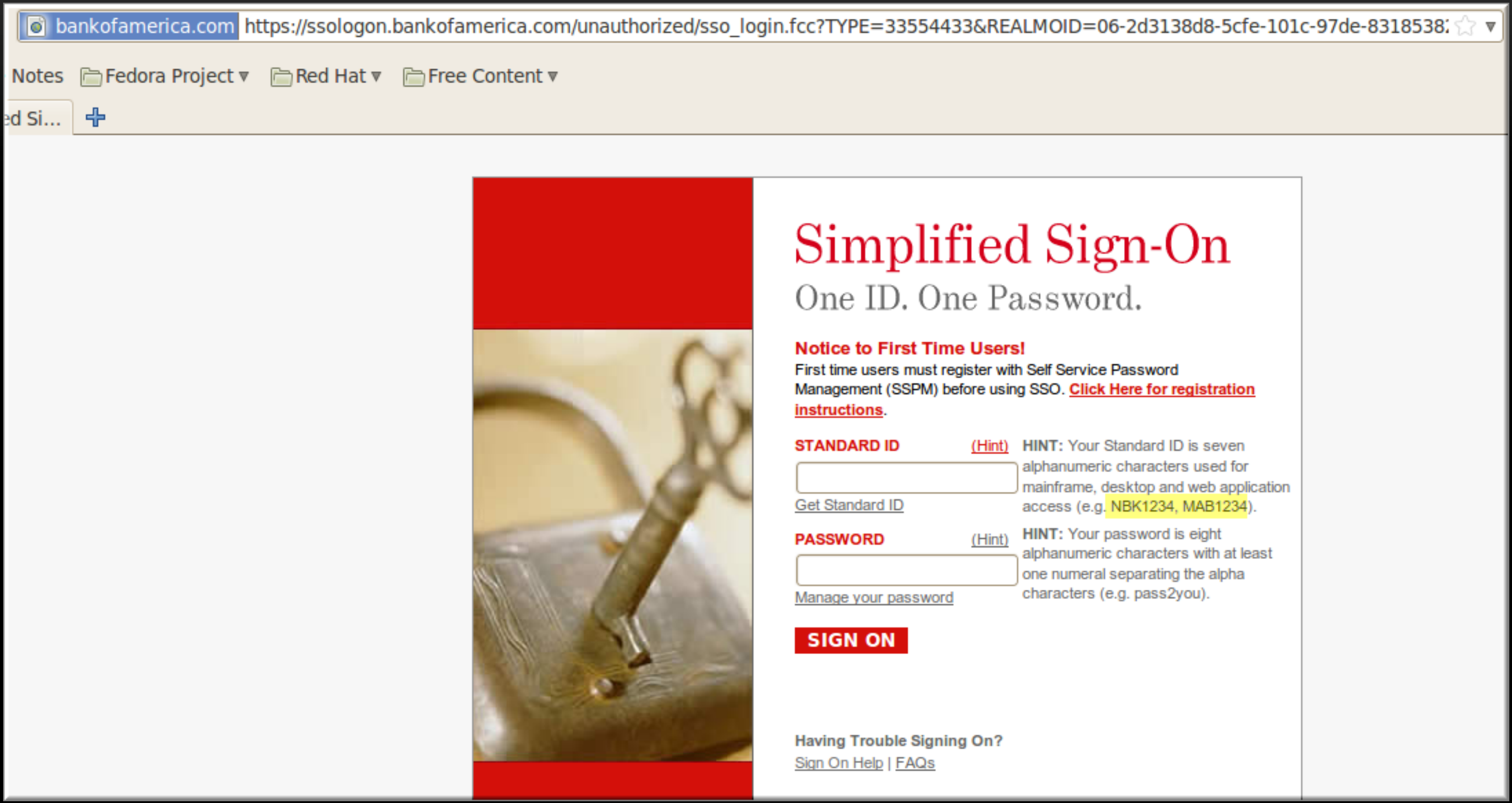
```
msf auxiliary(search_email_collector) > info

       Name: Search Engine Domain Email Address Collector
     Module: auxiliary/gather/search_email_collector
    Version: 9653
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Carlos Perez <carlos_perez@darkoperator.com>

Basic options:
  Name           Current Setting   Required  Description
  ----           ---------------   --------  -----------
  DOMAIN         bankofamerica.com yes       The domain name to locate email addresses for
  OUTFILE                          no        A filename to store the generated email list
  SEARCH_BING    true              yes       Enable Bing as a backend search engine
  SEARCH_GOOGLE  true              yes       Enable Google as a backend search engine
  SEARCH_YAHOO   true              yes       Enable Yahoo! as a backend search engine

Description:
  This module uses Google, Bing and Yahoo to create a list of valid
  email addresses for the target domain.

msf auxiliary(search_email_collector) > run

[*] Harvesting emails .....
[*] Searching Google for email addresses from bankofamerica.com
[*] Extracting emails from Google search results...
[*] Searching Bing email addresses from bankofamerica.com
[*] Extracting emails from Bing search results...
[*] Searching Yahoo for email addresses from bankofamerica.com
[*] Extracting emails from Yahoo search results...
[*] Located 1 email addresses for bankofamerica.com
[*]     icsvendormanagement@bankofamerica.com
[*] Auxiliary module execution completed
msf auxiliary(search_email_collector) > 
```



Id	Type	URL	Download	Download Date	Size	Analized	Modified Date
0	doc	http://www.bankofamerica.com/creditcards/data/nsbw...	●	3/7/2011 5:16:51 PM	56 KB	●	6/10/2002 4:28:00 ...
1	doc	http://www.bankofamerica.com/accessiblebanking/talki...	●	3/7/2011 5:16:51 PM	24 KB	●	3/13/2003 11:03:00...
2	doc	http://www.bankofamerica.com/privacy/data/PSCalifor...	●	3/7/2011 5:16:52 PM	70.5 KB	●	5/23/2003 2:56:00 ...
3	doc	http://www.bankofamerica.com/newsroom/presskits/pd...	●	3/7/2011 5:16:52 PM	37.5 KB	●	9/11/2001 2:32:00 ...
4	doc	http://www.bankofamerica.com/supplierdiversity/doc/M...	●	3/7/2011 5:16:53 PM	39.5 KB	●	1/8/2003 2:10:00 PM
5	doc	http://www.bankofamerica.com/supplierdiversity/doc/su...	●	3/7/2011 5:16:53 PM	84.5 KB	●	1/8/2003 11:27:00 ...
6	doc	http://www.bankofamerica.com/supplierdiversity/doc/W...	●	3/7/2011 5:16:54 PM	48 KB	●	1/8/2003 2:07:00 PM
7	doc	http://www.bankofamerica.com/supplierdiversity/doc/M...	●	3/7/2011 5:16:54 PM	20.5 KB	●	1/8/2003 2:09:00 PM
8	doc	http://www.bankofamerica.com/supplierdiversity/doc/W...	●	3/7/2011 5:16:55 PM	20.5 KB	●	1/8/2003 2:05:00 PM
9	doc	http://www.bankofamerica.com/suppliers/files/legalproc...	●	3/7/2011 5:16:56 PM	304 KB	●	10/1/2009 10:44:00...
10	doc	http://learn.bankofamerica.com/content/pdf/Document...	●	3/7/2011 5:16:56 PM	136.5 KB	●	5/27/2010 1:11:00 ...
11	doc	http://www.bankofamerica.com/docrepo/english__bank...	●	3/7/2011 5:16:56 PM	38.5 KB	●	3/7/2007 8:31:00 AM
12	doc	http://www.bankofamerica.com/foundation/pdf/word/A...	●	3/7/2011 5:17:09 PM	9.61 MB	●	10/21/2008 1:35:00...
13	doc	http://www.bankofamerica.com/newsroom/presskits/im...	●	3/7/2011 5:17:09 PM	67 KB	●	11/20/2002 11:32:0...
14	doc	http://www.bankofamerica.com/newsroom/presskits/im...	●	3/7/2011 5:17:09 PM	43 KB	●	5/28/2004 8:28:00 ...
15	doc	http://www.bankofamerica.com/newsroom/presskits/im...	●	3/7/2011 5:17:10 PM	35 KB	●	1/6/2003 5:18:00 PM
16	doc	http://www.bankofamerica.com/investor/patriotactdoc/...	●	3/7/2011 5:17:10 PM	73 KB	●	2/27/2003 9:35:00 ...
17	doc	https://globalcommissionpayments.bankofamerica.com/...	●	3/7/2011 5:17:11 PM	80.5 KB	●	12/12/2008 5:00:00...
18	doc	https://www.bankofamerica.com/www/en_US/doc/ph...	●	3/7/2011 5:17:11 PM	64.5 KB	●	8/20/2010 12:01:00...
19	doc	https://www.bankofamerica.com/www/en_US/doc/ph...	●	3/7/2011 5:17:11 PM	81 KB	●	8/5/2010 5:42:00 PM



Attribute	Value
All users found (165) - Times found	
RichardS	1
Toccoa Accuserv	1
Standard Register	1
Standard Register Employee	1
Karen Carruth	1
Kathey Dalrymple	1
NBKE7R2	7
Creative	1
NBKF7Q4	1
Suresh	1
NBDPD92-Caponi	2
nbkjl83	1
nbkq74h	1
Bank of America	46
kbrantman	1
Abby Romasanta	1
raj	5
Tal Herman	1
Nancy Willoughby	5
Mano Mahendran	1
nbkdxc4	2
PavanP_Patil	1
NBKIUD4	1
Norah Murphy	1
April Longhitano	1
Richard Riale	1
Joseph Crispyn	1
Jennifer Locane	1
nbkjdf7	5


bankofamerica.com
https://ssologon.bankofamerica.com/unauthorized/sso_login.fcc?TYPE=33554433&REALMOID=06-2d3138d8-5cfe-101c-97de-8318538:
Notes
Fedora Project ▾
Red Hat ▾
Free Content ▾
ed Si...

Simplified Sign-On

One ID. One Password.

Notice to First Time Users!

First time users must register with Self Service Password Management (SSPM) before using SSO. **Click Here for registration instructions**.

STANDARD ID (Hint)

Get Standard ID

HINT: Your Standard ID is seven alphanumeric characters used for mainframe, desktop and web application access (e.g. NBK1234, MAB1234).

PASSWORD (Hint)

Manage your password

HINT: Your password is eight alphanumeric characters with at least one numeral separating the alpha characters (e.g. pass2you).

Having Trouble Signing On?

Sign On Help | FAQs

A LITTLE PREVENTION GOES A LONG WAY

- Continually educate through security awareness
- Create a corporate policy regarding published content
- Provide the necessary tools to scrub metadata
  - Microsoft Document Inspector (Office 2007+)
  - BeCyPDFMetaEdit (Free) | Adobe Acrobat Pro (Not-Free)
- Data Loss Prevention Solutions
  - Network based – filters metadata at the perimeter
  - Endpoint based – analyses data and enforces security policy

THANK YOU!

Have questions, want to discuss further, grab a beer?

Chris Patten

(813) 480-6505

cpatten@packetresearch.com

http://www.linkedin.com/in/christopherpatten

REFERENCES

- http://office.microsoft.com/en-us/excel-help/remove-hidden-data-and-personal-information-from-office-documents-HA010037593.aspx
- http://www.becyhome.de/becypdfmetaedit/description_eng.htm
- http://www.informatica64.com/DownloadFOCA/
- http://www.paterva.com/web5/
- http://www.metasploit.com/