Global Information Assurance Certification Paper

Using Open Source Reconnaissance Tools for Business Partner Vulnerability Assessment

GIAC (GCIH) Gold Certification

Author: Susanne Young, sforslev@well.com

Advisor: Stephen Northcutt

Accepted: January 30, 2014

Abstract

The security of business partners can adversely affect a company. Third party data breaches can cost significantly more per lost record than local data breaches and acquisitions are more likely to be successful if security is addressed during the purchase. Even though it may be difficult to get security information directly from a business partner there are ways of performing a basic security assessment of a company using public information. Open source tools such as search engines, Shodan, Search Diggity, and recon-ng can provide a valuable profile of a company's strengths and weaknesses. By utilizing these tools as a part of the due diligence process businesses will be able to make a more informed decision during an acquisition or when choosing a vendor.

Introduction

1.1

All businesses, no matter what their goals, depend on a network of contacts to survive and grow. Equipment vendors, consultants, law and marketing firms make it possible to find and serve customers. The growth of the global Internet means that customers and suppliers may found anywhere, sometimes only being connected by email or websites.

The ubiquity of Internet connected systems means that attackers do not have to be close to their targets. Every Internet connected system is directly accessible from any other Internet connected system (Schneier, 2000). The same technology that makes it easier to find customers also makes it easier for criminals and vandals to find victims.

The estimated cost per record of a data breach has risen to $188 per record (Ponemon Institute, 2013). A single breach such as the Adobe breach of October 2013 can result in the loss of 130 million records so it is worthwhile to spend much less money and effort on security beforehand then to clean up after a breach.

According to the Ponemon Institute, third party errors leading to breaches can add as much as $43 to the average cost per record (Ponemon Institute, 2013). Since a breached database may have thousands of records, it's important to pay attention to your business partner's security as well as your own.

Even if your company is required to comply with data security standards such as PCI DSS (PCI Security Standards Council, 2010), your law firm or marketing consultant is probably not covered. Many businesses have no regulatory requirements and will only be careful if their customers require evidence of a computer security program.

There is also a tendency to think that a business is so small that they could not possibly be a target. This is false. At the very least an unprotected computer is a place to store malware, pornography, or stolen information from other companies. Criminals frequently drain small business bank accounts with banking malware (Symantec, 2013) and recently computers have

Susanne Young, sforslev@well.com

been taken over to manufacture bitcoins directly (Krebs, 2013). This is essentially stealing electricity.

In addition to vulnerabilities on internal systems, most business will have websites, email servers, and DNS servers available on the Internet. These systems will show services and banners, sometimes with exact software versions listed. If external systems are not kept up to date, they will be discovered by attackers and will provide easy entry to internal systems.

A compromised supplier can cause a lot of damage to a company. In August 2013, Melbourne IT, an Australian DNS register reseller was hacked through a phishing email which allowed the Syrian Electronic Army to change DNS records for the New York Times to point to their own servers. In this case, no matter how good security was at the New York Times, a supplier's lax security opened them up to embarrassment and damage (Stilgherrian, 2013).

1.2

Every perimeter is being constantly scanned by possible intruders looking for weaknesses. There's no reason to spend time crafting a phishing email and setting up infected websites when your target has an ancient, easily exploited apache install, a SQL injection flaw on your login page, or a router with a default password sitting on the Internet for anyone to enter. It is also possible to find the versions of internal software from metadata in published documents.

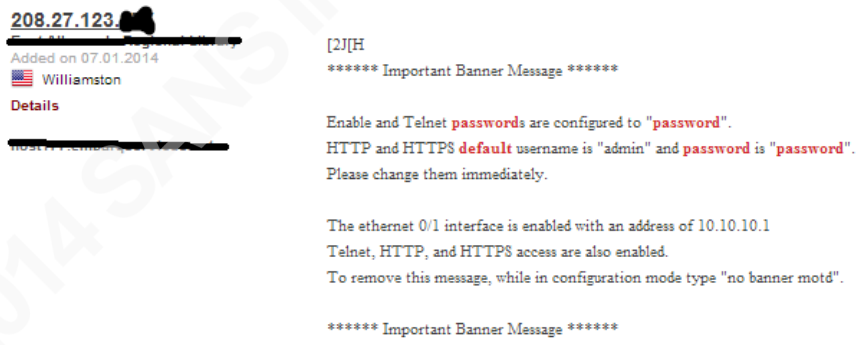


Figure 1.2-1 Default passwords visible on banner

1.3

Susanne Young, sforslev@well.com

A certain amount of information has to be available to allow customer browsers to render information. Default installs of web servers, email servers, or other services can unintentionally give much more information than is necessary in service banners. Default installs can also include unintended services such as FTP or VNC along with the intended programs or passwords may not be set correctly. For example, the passwords of 100,000 IEEE members were inadvertently exposed on an FTP server in 2012 by having plain text log files exposed on a public FTP site (Kaplan, 2012).

Many systems are exposed through VNC, which can be installed to allow systems to be remotely managed. If a password isn't set, the systems may be totally open to the world, as security researcher Paul McMillen found in an Internet scan on the default VNC port 5900 in 2013 (Zetter, 2013). Even if there's a password, old versions of VNC have serious vulnerabilities and passwords are always vulnerable to brute force attacks.

VNC is commonly installed by default on blade servers to allow the systems to be managed remotely since they may not be directly connected to a monitor and keyboard. It should never be exposed to the Internet.

1.4

Vendors are not the only concern. If a company is considering a merger or acquisition, it is important to not negatively impact security with the transaction. An Accenture Consulting study of 57 mergers and acquisitions from 1997 to 1999 showed that companies who conducted IT due diligence during the vetting process had better financial results than companies who did not (Sundberg, Tan, Baublits, Lee, Stanis & Tanriverdi, 2006). It makes sense that if computer systems are poorly maintained, other parts of the business may also be in disarray. Security support should be part of the analysis that will ensure that an acquisition will bring value to a company (Halibozek & Kovacich, 2005).

2. Problems assessing vulnerabilities of business partners, acquisitions, and investments.

2.1

Susanne Young, sforslev@well.com

There are both practical and ethical issues involved in assessing the security of systems you do not own. Trying to break into computer systems that you do not own is illegal, even if you are doing it to test their security (Electronic Frontier Foundation, 2013). This is why it is best to use public information, so there will be no legal repercussions from the assessment.

Simply asking for vulnerability information from a business partner may not be successful. This is considered highly confidential information and it could damage the company if it was inadvertently released. This is assuming the company has the information.

Not all companies have a formal vulnerability management program even though they may have competent IT support. A small or even medium sized company may not have knowledgeable security staff to conduct the scan or the money to hire a consultant. Even companies with this information may just feel they don't want to take the time to provide it.

Doing an unannounced vulnerability scan of someone else's perimeter is not a good way to either start or continue a business relationship. An intense scan can cause a website to crash or fill up available bandwidth. The increased traffic could even result in increased web hosting costs. When companies scan their own systems it is generally done during defined maintenance windows to avoid interfering with production systems. For example, IBM warns against scanning ports running HACMP services since this can cause a system crash (IBM 2008).

I have worked in environments where there were ports we excluded from vulnerability scans on certain critical systems since the vendor warned that scanning may lock up services or crash the server. I've also had a home router and an old DVR that would crash when scanned.

2.2

There are methods that will allow you to gather publicly available information and make good judgments about the security of websites without conducting intrusive scans.

All Internet services must provide some basic information to the outside world. These are banners that will tell client computers the services available. Headers can be seen by using Chrome developer tools when browsing the website or by using a proxy application such as the Burp Suite from http://portswigger.net/burp/ or Paros Proxy from http://sourceforge.net/projects/paros/ with any web browser.

Susanne Young, sforslev@well.com

For example, the following banner shows the web software for a public site:

```
HTTP/1.0 200 OK
Date: Wed, 25 Sep 2013 14:37:35 GMT
Server: Apache
Last-Modified: Mon, 11 Jul 2011 23:55:14 GMT
Accept-Ranges: bytes
Content-Length: 279
Connection: close
Content-Type: text/html
```

This is a good result in that it does not show the exact version of the Apache software being used. This makes it more difficult for someone to find an exploit to break into the website while still providing enough information for a browser to correctly connect to it.

The following finding is not as good. This website appears to be a default web page running on Windows NT. Windows NT 4.0 has not been actively supported since 2004. There are likely to be many unpatched vulnerabilities on this system.

```
HTTP/1.0 200 OK
Server: Microsoft-IIS/4.0
Content-Location: http://xxx.xxx.xxx.xxx/Default.htm
Date: Sun, 29 Sep 2013 20:27:55 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Thu, 07 Sep 2000 21:54:50 GMT
ETag: "071cd3g1689c01:21xx"
Content-Length: 218
```

2.3

Wholesale Internet scanning is an ethical gray area. Extensive portscans with tools such as Nmap are considered hostile and could cause denial of service conditions. However, lightweight scans grabbing banners from common services are usually not noticed. There are projects that scan large parts of the Internet this way and then provide the information on their websites.

These websites provide good way to check out a possible investment or acquisition target while not running any scans. Example projects are Shodan and What Web. While most companies would rather not be scanned by these projects, they don't seem to be harming their targets except by consolidating and allowing searches of information that's basically public anyway.

Susanne Young, sforslev@well.com

Another source of information is the Internet Census 2012. This is a result of the Carna Botnet. This is a survey conducted by infecting devices found on the Internet that did not have passwords or used logins such as root/root or admin/admin. The botnet infected these devices and then mapped the immediate area and spread itself to any other unsecured systems it found. The results are posted at http://internetcensus2012.bitbucket.org/paper.html.

The Carna botnet is possibly an illegal misuse of computer systems even though it does not seem that it was meant to be malicious. The authors are anonymous and may face jail time if they're discovered. That said, the information is public and it is a good idea to check the census for systems that could affect you. The census is searchable at http://www.exfiltrated.com/querystart.php.

2.4

It is also possible to find websites and software versions by using Google (Long, Temmingh, Petkov, CP, Stewart & Langley, 2008). Put in a Google search for "intitle:index.of "Apache 2.2.22 at" to get a listing of servers running that version of Apache. Add a site name to find software on that site. There are hundreds of possible queries for vulnerable software or sensitive documents such as password files, vulnerability scans, or configuration files. These can be found on all search engines although vulnerability searches known as "Google Dorks" are the best documented.

Be careful with these queries. There are bots that search for targets using Google, so there are safeguards against dangerous searches. You may be asked to prove your humanity with a captcha puzzle designed to tell human from machine if you use certain search terms.

Until you know your searches are safe do all testing on a home machine. If Google decides there's a botnet on your address it may block all search activity from your site. This does not make co-workers happy if it happens at the office. Take it from the voice of experience. I had this happen several years ago when I first tried some of the searches in the Google Hacking Database now found at http://www.exploit-db.com/google-dorks/ .

Susanne Young, sforslev@well.com

It is possible to do basic port scans with a search engine. By using the site operator in a Google search you can look for sites with websites on ports other than 80 or 443. Try the search "site:/*.com:*" to get a list of .com sites indexed by Google on ports other than 80 or 443.

Search engines are also a good way of collecting contacts. Search intext:"@sitename.com" to find contact names for a company. It is possible to find mailing list archives this way which can give information on technologies used and problems with those technologies. This can be very useful for situational awareness - if a company has a big software rollout planned and their developers are asking panicky questions on mailing lists, it may be a good idea to postpone your investment. Career sites such as Monster.com will also give information on technologies used through their job postings.

2.5

The history of a website can be interesting. http://www.domaintools.com will provide the DNS registration history of a website. http://www.whoisrequest.org will provide DNS information and also provide name server history going back to 2002. Both these sites will give you websites that share ip addresses and lists of domain names registered to the organization. Domain Tools has extensive services available for a subscription fee. Domain Tools is frequently used in criminal investigations to find out more information about malicious websites.

DNS registration information can also reveal unannounced new product lines. Companies will frequently register websites for products before they're announced. Tech journalists monitor the companies they cover this way to get an idea of the next big thing from Apple or Samsung (Wauters, 2011).

Netcraft is also useful for finding website technologies and enumerating domains. Go to http://www.netcraft.com/ and enter the website name in the "What's that site running?" box to see the installed software and netblock information for a website.

2.6

Once you know what software the company you are evaluating is running, search for it on http://www.cvedetails.com. This website will allow you to search for vulnerabilities on common software. It has very comprehensive information arranged logically. It is one of the few sites that

will give a good list of vulnerabilities arranged in a neat list for a specific version of software. It is the site I go to whenever I get a question about exactly what vulnerabilities a certain technology has and how it compares to a later version. The severity of the vulnerabilities is given too. Here's a screenshot of a search for vulnerabilities on Apache 2.2.22. Vulnerabilities with high scores will be a red flag and indicate problems with IT maintenance.

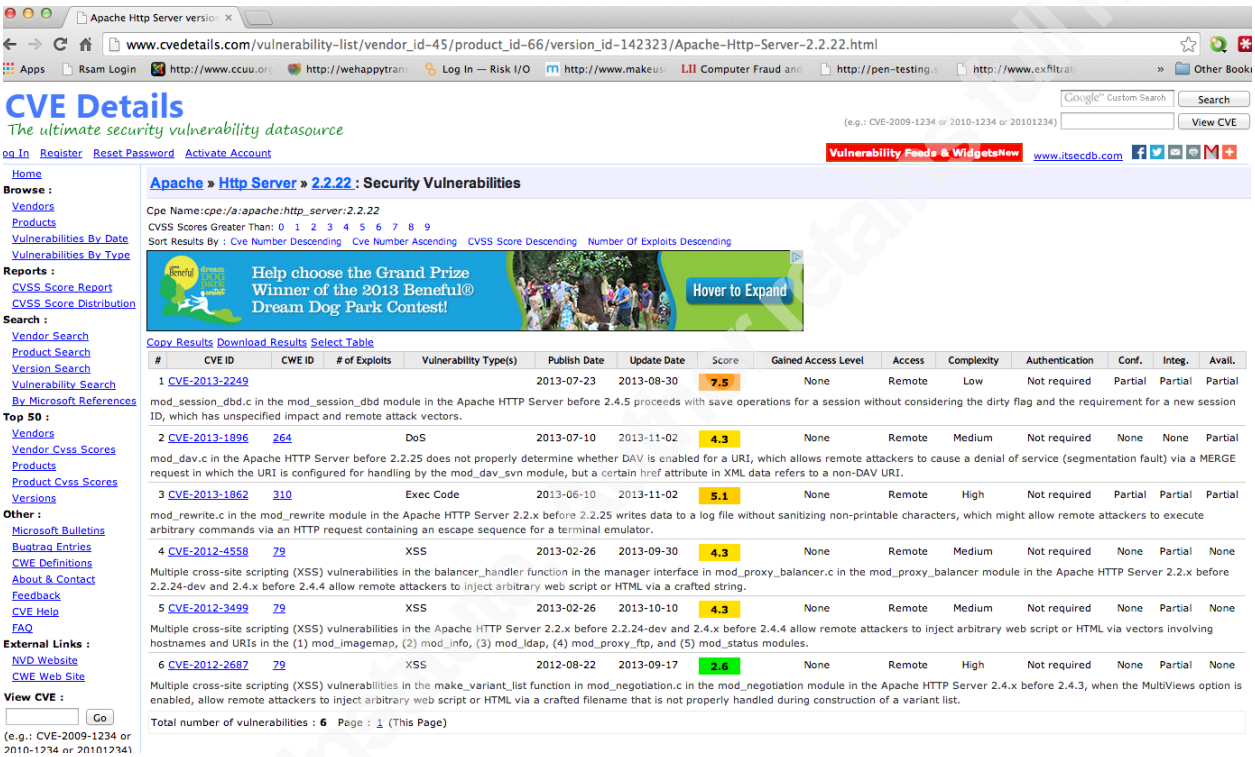


Figure 2.6-1: The CVE Details Website

3 Tools for Non-Intrusive Vulnerability Assessment

3.1 Enumeration

Inventory is the first step in a vulnerability assessment. Since it is possible that not all the company systems on the Internet have DNS information registered, use DNS based tools such as Domain Tools, Whois Request, or Robtex to find possible ip address ranges for a company. For example, look up cnn.com on http://www.robtex.com

Susanne Young, sforslev@well.com

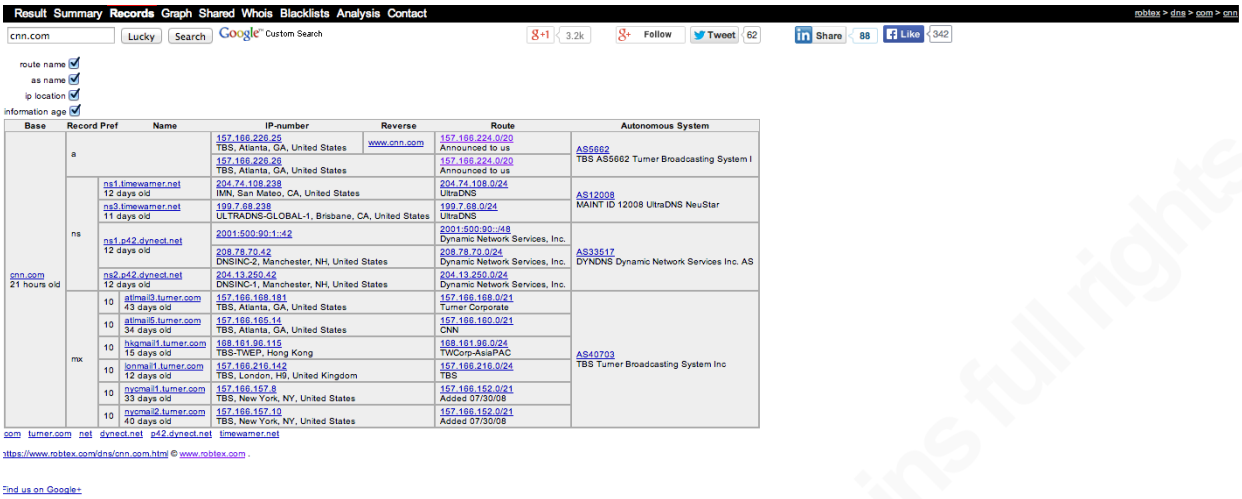


Figure 3.1-1: Robtex Results for cnn.com

Network ranges owned by the organization are shown under the Routes column. Start searching with those ip ranges along with obvious domain names. An organization may have websites hosted with other companies in ranges they don't own so it is important to also look at both names and addresses. If you are checking your own company, get a list of routable ip ranges your company uses. Even if a range is usually only used internally, there may be some test systems exposed on the Internet.

3.2 Search Diggity

There is a very useful front end for searching called Search Diggity from Bishop Fox, downloadable from http://www.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools/ . It is a Windows GUI providing a front end for searching Google, Bing, and Shodan. It is possible to perform a basic security assessment on a company using this tool. Everything that can be done on the web can be done in this application and the results are easily exported to text files for reporting.

Susanne Young, sforslev@well.com

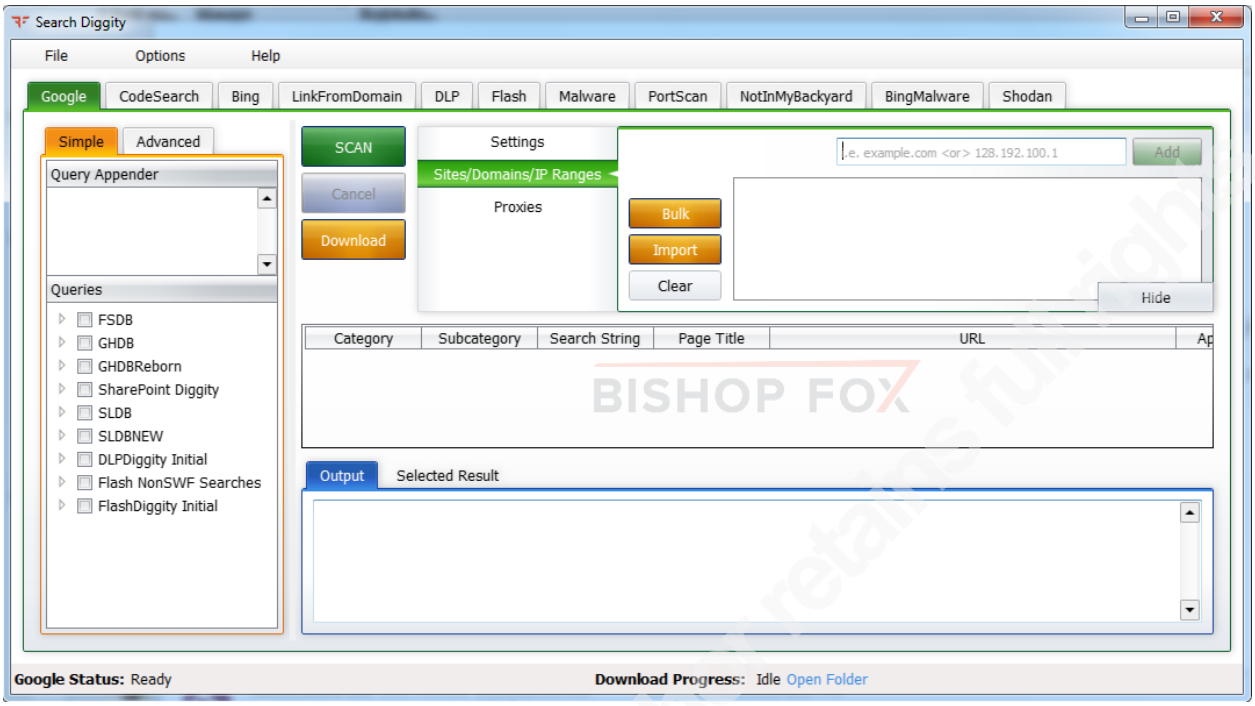


Figure 3.2-1: The Search Diggity Interface

There are built in queries for common vulnerabilities using Google and Bing, a very friendly front end for Shodan searches, and searches for malware and links. The app requires an API for Google, Bing, and Shodan. The API for Shodan is inexpensive, around $20 for full access to all searches and the API depending on current promotions. Basic Google and Bing API access is available for free with upgrades available at a variety of prices.

The API licenses can be obtained at the following locations:

Bing - http://datamarket.azure.com/dataset/bing/search

Google - Login to Google and go to https://code.google.com/apis/console/

Shodan - Click the Buy button at http://www.shodanhq.com/

The Shodan page is an excellent place to start enumeration. Shodan indexes many ports so it will pick up mail servers, netbios, VNC, and other ports that are not indexed by other search engines. The Shodan web site at http://www.shodanhq.com offers xml search result downloads for

Susanne Young, sforslev@well.com

purchased credits but Search Diggity will allow the searches to be saved as text files that are easier to manage in spreadsheets.

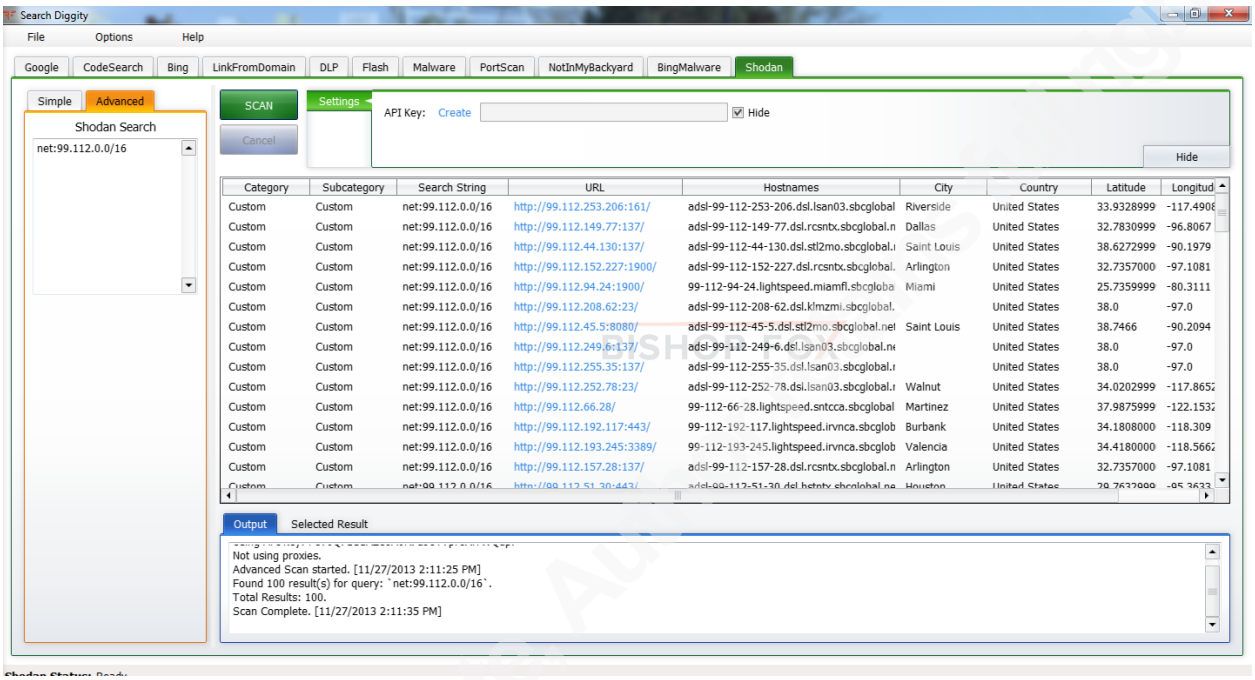


Figure 3.2-2 Shodan Search on Search Diggity

There is a limit of 100 results per search so choose your terms carefully. Once a list of hosts to evaluate is found, look for unusual open ports, unsecured test networks or devices that seem out of place. Further searches are possible. Search by organization, keyword (try "default password"), or technology.

Use the Google hacking or Bing hacking databases to look for cross site scripting problems on your sites or use the Shodan options to search for default passwords. Another useful option is the LinkFromDomain tab. It will show indexed links from the site to other sites. This can help to further enumerate the domain and give an idea of the company's business partners.

Susanne Young, sforslev@well.com

Many search terms will still trigger alerts on Google and your searches may be blocked for a period of time even when using the API so it is still important to use a test network when trying out search terms. I've found Bing to be a little more forgiving of questionable searches.

The Malware tab combines the linkfromdomain: operator with a Google Safe Browsing check on all the links to find links from the site that connect to known malware domains. This will help make sure that a site is not unknowingly downloading malware to visitors.

It is worthwhile to try all the tabs in Search Diggity. It is an incredibly flexible tool that requires no programming skills to use.

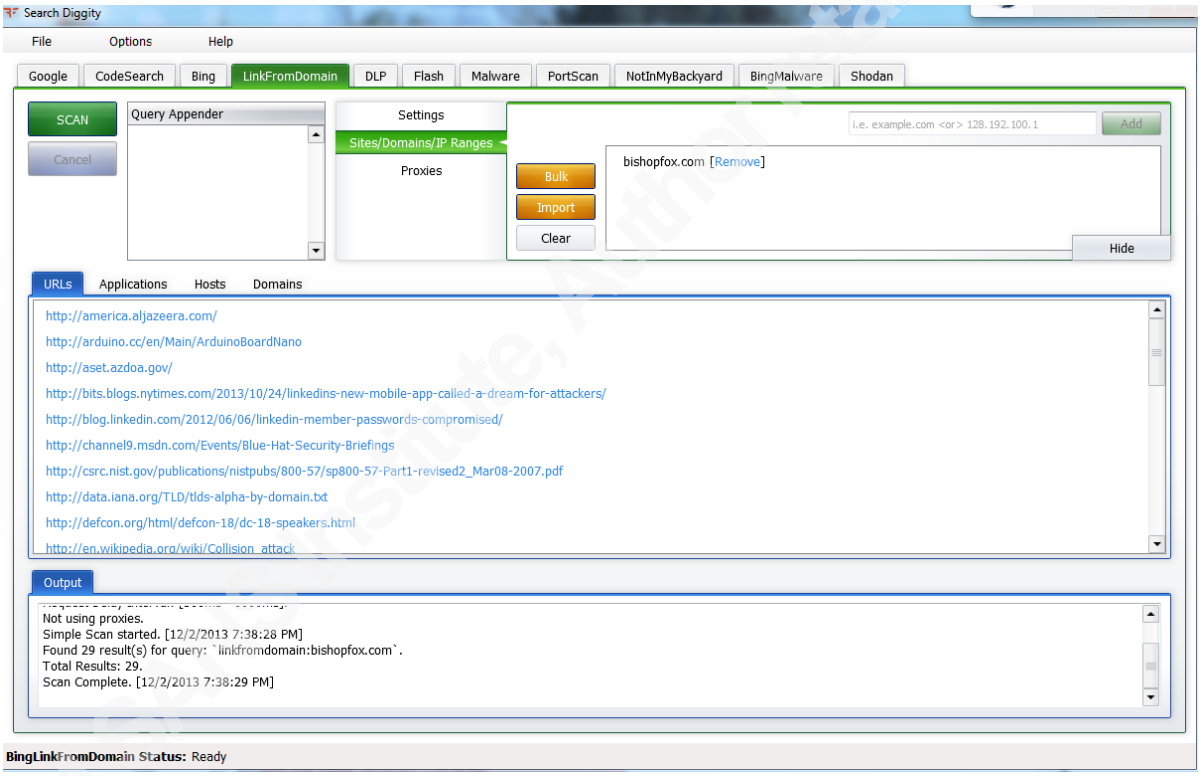


Figure 3.2-3: Search Diggity LinkFromDomain search

3.3 Internet Census 2012

Enumeration is also possible using the Internet Census 2012 at http://www.exfiltrated.com/querystart.php. This is the census put together by the Carna botnet (Lemos, 2013). While the way the information was gathered was unethical, the information itself

is now public and is a good source for enumerating exposed systems. The information is probably not being updated so the utility of the database will decrease as time goes on.

3.4 Foca

Foca is a tool that is similar to Search Diggity. It is a Windows based application and is available in both free and professional versions. When a website or domain is input, Foca searches for subdomains, technology, and files using Google or Bing. When it finds files, Foca will download the files you choose and extract metadata from them.

Metadata can provide very useful information. It can contain user names, software versions, printer definitions, server names, and directory paths. Is your business partner using an ancient version of Office that's vulnerable to common exploits? Does it look like they're aware of metadata possibly being an issue? Foca lets you have a peek inside the target network using publicly available documents. Larry Pesce has a great paper on metadata in the SANS Reading room http://www.sans.org/reading-room/whitepapers/privacy/document-metadata-the-silent-killer--32974 and there is a good introductory video on Foca at http://www.irongeek.com/i.php?page=videos/using-foca-to-collect-metadata-about-an-organization.

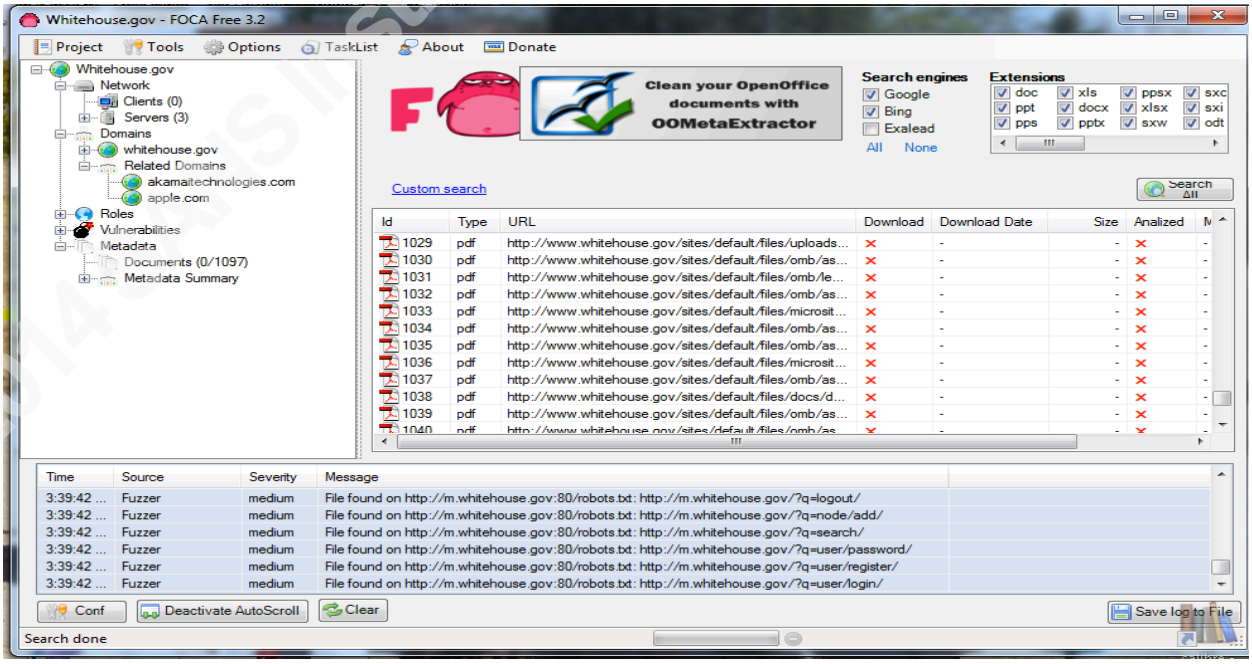


Figure 3.4-1: Foca Search

Susanne Young, sforslev@well.com

Foca also does basic checks on server technology, will enumerate subdomains and check Shodan for the organization's servers, open ports, and technologies. It will touch the target when downloading documents but otherwise it works through search engines and Shodan without touching the target domain. It is worth running against your own domain to make sure your marketing department isn't giving away too much information in their online pdf files.

3.5 Malware and Spam Detection

The last thing you want is to have your site or a business partner's site serving up malware to customers instead of your products. Fortunately it is easy to test sites against many malware detection engines at http://www.urlvoid.com and http://www.ipvoid.com. They look for malware sites, spam sites and phishing sites. You should definitely check your email or social network marketing company on these sites since you would not want to hire a spammer.

3.6 Automating Searches with Recon-ng

The preceding checks are useful and can be provide vulnerability information but not all the tools provide good reports that can be used in a corporate environment. It is also much easier to run a script and work on something else while it runs. There is a command line tool called Recon-ng that will query Google and Shodan and run many of the same queries that the previous GUI and web based tools can run. It is written to work like the Metasploit framework but for reconnaissance.

Recon-ng is written in Python so it runs on many platforms but all examples here will be run in OS X. It runs well on most Linux versions too. It is written and maintained by Tim Tomes at https://bitbucket.org/LaNMaSteR53/recon-ng/overview. It is designed to help automate penetration tests but it is useful for general enumeration as well.

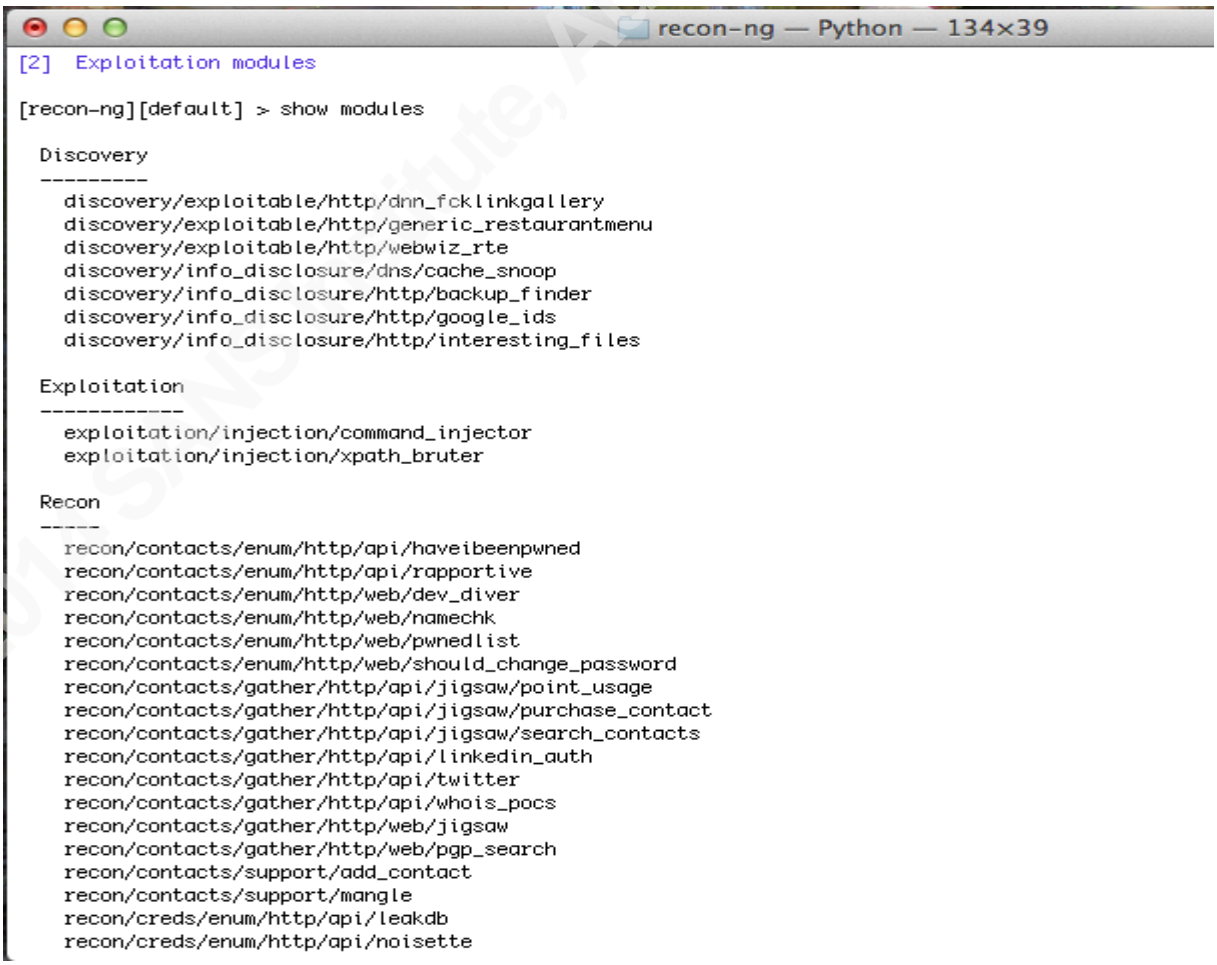
3.6.1 Installing Recon-ng

Clone recon-ng with the command "git clone https://LaNMaSteR53@bitbucket.org/LaNMaSteR53/recon-ng.git". After the installation, just change to the recon-ng directory and run ./recon-ng to start the framework.

Susanne Young, sforslev@well.com

Figure 3.6.1-1 Starting recon-ng

Once you're in recon-ng, list the available modules with the show modules command.



Susanne Young, sforslev@well.com

Figure 3.6.1-2 Listing recon-ng modules

If you have a domain in mind, a good module to start with is the recon/hosts/gather/http/web/google_site module. The syntax is easy, to use the module, just type "use recon/hosts/gather/http/web/google_site". To see the information required by the site, type the word "info". Set the domain to Microsoft in this case by typing "set domain microsoft.com". When the options are set, use the run command to enumerate the domain.

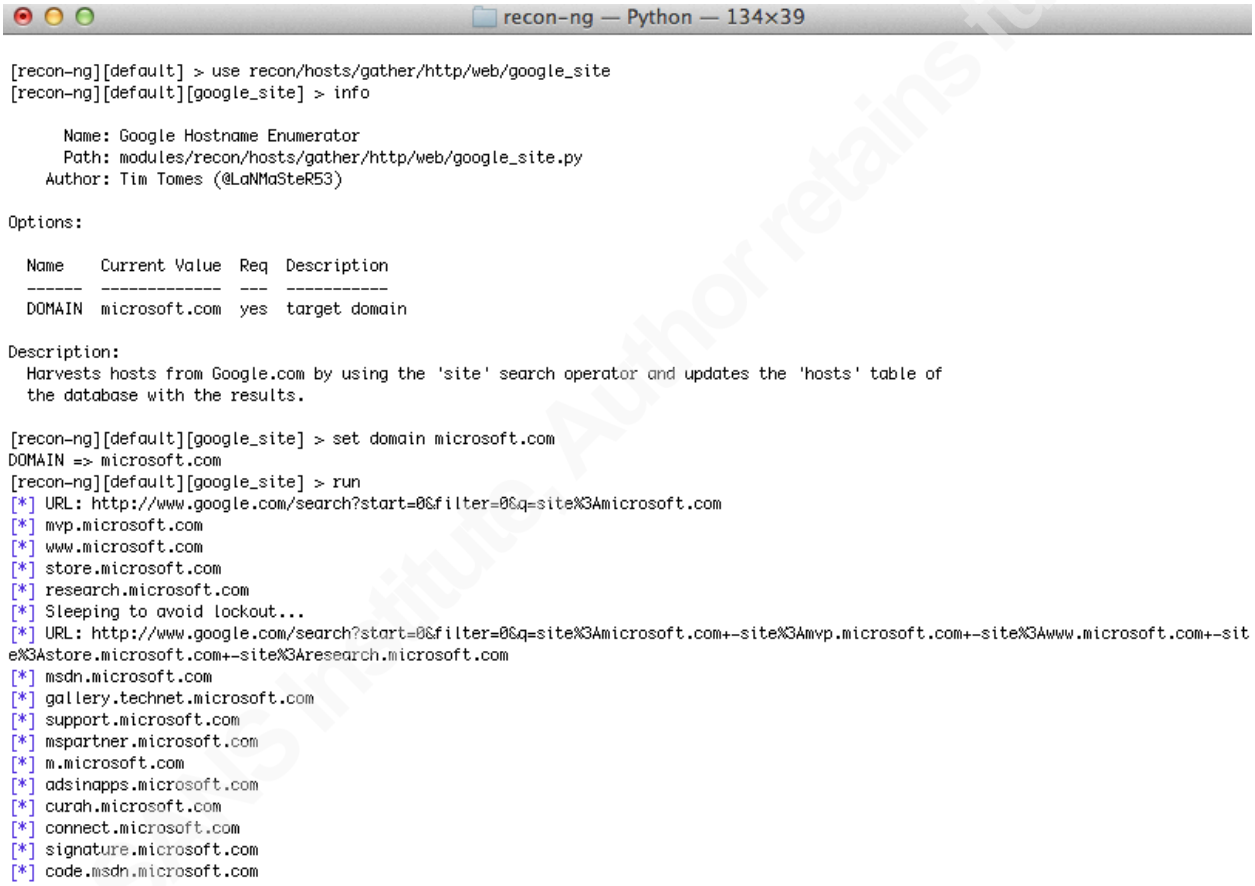


Figure 3.6.1-3 Identifying hosts with recon-ng

This will populate the hosts table with all system names found on Google in the microsoft.com domain. List the hosts found with the command "show hosts".

The next step in enumeration is to resolve the addresses. There is a module to resolve the addresses called recon/hosts/enum/dns/resolve. Just enter "use recon/hosts/enum/dns/resolve" and then enter "run". The default options are usually fine for this command.

Susanne Young, sforslev@well.com

View the addresses with the show hosts command.

recon-ng — Python — 134×39

```
[recon-ng][default][resolve] > show hosts

+-------------------------------------------------------------------------------------------------------+
|                    host                    |    ip_address    | region | country | latitude | longitude |
+-------------------------------------------------------------------------------------------------------+
| adsinapps.microsoft.com                    | 168.62.20.37     |        |         |          |           |
| advertise.bingads.microsoft.com            | 65.52.100.46     |        |         |          |           |
| advertising.microsoft.com                  | 65.52.100.46     |        |         |          |           |
| aer.microsoft.com                          | 94.245.126.214   |        |         |          |           |
| answers.microsoft.com                      | 65.55.121.50     |        |         |          |           |
| appdev.microsoft.com                       | 64.4.59.84       |        |         |          |           |
| apps.microsoft.com                         | 134.170.30.203   |        |         |          |           |
| careers.microsoft.com                      | 64.4.11.23       |        |         |          |           |
| clicktoattend.microsoft.com                | 65.55.57.98      |        |         |          |           |
| code.msdn.microsoft.com                    | 65.52.103.91     |        |         |          |           |
| commerce.microsoft.com                     | 168.62.198.20    |        |         |          |           |
| community.bingads.microsoft.com            | 207.46.118.231   |        |         |          |           |
| connect.microsoft.com                      | 65.52.103.84     |        |         |          |           |
| consumersecuritysupport.microsoft.com      | 157.56.56.69     |        |         |          |           |
| corp.sts.microsoft.com                     | 131.107.113.238  |        |         |          |           |
| curah.microsoft.com                        | 168.61.161.66    |        |         |          |           |
| cvp.membership.microsoft.com               | 65.55.58.186     |        |         |          |           |
| data.choice.microsoft.com                  | 131.253.40.60    |        |         |          |           |
| download.microsoft.com                     | 63.216.54.112    |        |         |          |           |
| download.microsoft.com                     | 63.216.54.41     |        |         |          |           |
| events.microsoft.com                       | 65.55.58.192     |        |         |          |           |
| events.microsoft.com                       | 64.4.11.31       |        |         |          |           |
| familysafety.microsoft.com                 | 207.46.201.254   |        |         |          |           |
| gallery.technet.microsoft.com              | 65.52.103.91     |        |         |          |           |
| go.microsoft.com                           | 64.4.11.25       |        |         |          |           |
| ie.microsoft.com                           | 137.117.90.63    |        |         |          |           |
| ieonline.microsoft.com                     | 204.79.197.200   |        |         |          |           |
| learning.microsoft.com                     | 64.4.30.197      |        |         |          |           |
| m.microsoft.com                            | 65.55.186.235    |        |         |          |           |
| mbs.microsoft.com                          | 131.107.96.163   |        |         |          |           |
| msdn.microsoft.com                         | 157.56.148.19    |        |         |          |           |
| msevents.microsoft.com                     | 64.4.11.31       |        |         |          |           |
| mspartner.microsoft.com                    | 64.4.30.177      |        |         |          |           |
+-------------------------------------------------------------------------------------------------------+
```

Figure 3.6.1-4 Resolved hosts

Now that the hosts are enumerated, it is time to use some of the other modules to look for problems.

The module Builtwith will identify the technology used on the systems in the hosts database. The results are very detailed with a boxed summary for each url. If a software version is given, see if it is the latest. You can check software against CVE Details at http://www.cvedetails.com for reported vulnerabilities and to find the current versions.

The results for advertising.microsoft.com are interesting:

Susanne Young, sforslev@well.com

```
--------------------------------------------------
[*] Name: Omniture SiteCatalyst
[*] FirstDetected: /Date(1324213200000)/
[*] Tag: analytics
[*] Link: http://www.omniture.com/
[*] LastDetected: /Date(1361710800000)/
[*] Description: Omniture SiteCatalyst provides your website with actionable, real-time in
telligence regarding
    online strategies and marketing initiatives.
--------------------------------------------------

  +-----------------------------------------+
  |     Tag     |            Name           |
  +-----------------------------------------+
  | Profile URL | advertising.microsoft.com |
  | Framework   | ASP.NET 2.0               |
  | Analytics   | CrazyEgg                  |
  | Analytics   | Preact                    |
  | Analytics   | Optify                    |
  | Analytics   | Facebook Domain Insights  |
  | Analytics   | Omniture SiteCatalyst     |
  +-----------------------------------------+

[recon-ng][default][builtwith] >
```

Figure 3.6.1-5 Builtwith results for advertising.microsoft.com

ASP.NET 2.0 is pretty old. Right now the latest version is 4.5 and CVE Details shows a number of problems with version 2.0. This information will not be written to a table but it can be captured by running the spool command to write the output to a text file.

It is also possible to get contacts from Linkedin and Jigsaw. Jigsaw fees are high but Linkedin will give you a basic API for free. You will have to buy a business account to get contacts that are not closely connected to you but it is cheap enough that most companies would pay for it. The contacts modules are more useful for pentesting than for vulnerability assessment but by using the modules recon/contacts/enum/http/web/haveibeenpwned and recon/contacts/enum/http/web/pwnedlist you can see if any of the contacts show up in major breaches.

These checks can be scripted by using the recon-ng command line utility or by running a resource file with commands inside the program. Here is a resource file that will search Shodan, Google, and Baidu for hosts, resolve the ip addresses, resolve the location of the servers, list the technologies used on the servers, find contacts, see if they show up in any data breaches and check urlvoid for adverse reports. It will spool all output to a text file and print out the host and contact tables into an html report

Susanne Young, sforslev@well.com

Substitute your target company name where it says “Target Company” in the file and put the primary domain in as the domain option. At the end of the resource file choose a name for the html file where the contact and host tables will be output. Just save the following commands in a text file in the recon-ng directory and run it with the command line ./resource-ng –r your file name here.txt.

```
workspace "Target Company"
set domain targetcompany.com
set company "Target Company"
spool start targetcompany.out
use recon/hosts/gather/http/web/google_site
run
use recon/hosts/gather/http/web/baidu_site
run
use recon/hosts/enum/dns/resolve
run
use recon/hosts/geo/http/api/ipinfodb
run
use recon/hosts/gather/http/web/census_2012
run
use recon/contacts/gather/http/web/pgp_search
run
use recon/contacts/gather/http/api/linkedin_auth
run
use recon/hosts/enum/http/api/whatweb
run
use recon/hosts/enum/http/api/builtwith
run
use recon/hosts/enum/http/web/xssed
run
use recon/hosts/enum/http/web/urlvoid
run
use recon/contacts/enum/http/web/haveibeenpwned
run
spool stop
use reporting/html_report
set filename ./company.html
run
```

Recon-ng is being actively developed and modules are changing frequently. Check https://bitbucket.org/LaNMaSteR53/recon-ng for updates and documentation.

Susanne Young, sforslev@well.com

Conclusions

Vulnerability management, the identification and remediation of vulnerabilities in computer software, is an important part of a good information security program (Pironti, 2006). However vendors and acquisition targets are under no legal obligation to provide this information. These business partners can provide a point of entry for hackers and information thieves. This is illustrated by a November 2013 breach where T-Mobile customer information was stolen from a business partner (Greenberg, 2014). It can be difficult to get necessary vulnerability information from vendors and business partners but there are ways to gain information without disrupting relationships. Open source tools such as search engines, Shodan, Search Diggity, and Recon-ng can provide a company security profile without directly accessing target firms. Companies will be able to make a more informed decision on vendors and acquisitions by utilizing open source reconnaissance techniques.

References

Electronic Frontier Foundation. (2013, April 24). Computer fraud and abuse act (cfaa). Retrieved from https://ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_(CFAA)

Greenberg, A. (2014, January 6). Undisclosed number of T-Mobile customers impacted in data breach. SC Magazine, Retrieved from http://www.scmagazine.com/undisclosed-number-of-t-mobile-customers-impacted-in-data-breach/article/327905/

Halibozek, E., & Kovacich, G. (2005). Mergers and acquisitions security: Corporate restructuring and security management. (p. 57). Burlington MA: Elsevier Butterworth-Heinemann.

IBM. (2008, November 26). HAMCP/port scan faq. Retrieved from http://www-01.ibm.com/support/docview.wss?uid=isg3T1000505

Kaplan, D. (2012, September 25). Passwords of 100k ieee members lie bare on ftp server. SC Magazine, Retrieved from http://www.scmagazine.com/passwords-of-100k-ieee-members-lie-bare-on-ftp-server/article/260721/

Susanne Young, sforslev@well.com

Krebs, B. (2013, July 18). [Web log message]. Retrieved from http://krebsonsecurity.com/2013/07/botcoin-bitcoin-mining-by-botnet/

Lemos, R. (2013, April 4). Carna compromise delivers data, but casts suspicions. Retrieved from http://www.darkreading.com/advanced-threats/carna-compromise-delivers-data-but-casts/240152227?itc=edit_in_body_cross

Long, J., Temmingh, R., Petkov, P. ". D., CP, , Stewart, J., & Langley, R. (2008). Google hacking for penetration testers volume 2. (p. 103). Burlington MA: Syngress Publishing, Inc.

PCI Security Standards Council. (2010, October). Payment card industry (PCI) data security standard requirements and security assessment procedures v 2.0. Retrieved from https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

Pironti, J. (2006). Key elements of a threat and vulnerability management program. ISACA Journal, 3, Retrieved from http://www.isaca.org/Journal/Past-Issues/2006/Volume-3/Pages/Key-Elements-of-a-Threat-and-Vulnerability-Management-Program1.aspx

Ponemon Institute. (2013, May). 2013 cost of data breach study: global analysis . Retrieved from https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

Schneier, B. (2000). Secrets and lies. (p. 20). Indianapolis, IN: Wiley.

Stilgherrian. (2013, August 30). Melbourne it breach highlights need for security culture. Retrieved from http://www.zdnet.com/au/melbourne-it-breach-highlights-need-for-security-culture-7000020049/

Sundberg, B., Tan, Z., Baublits, T., Lee, H., Stanis, G., & Tanriverdi, H. (2006). A framework for conducting it due diligence in mergers and acquisitions. ISACA Journal, 6, Retrieved from http://www.isaca.org/Journal/Past-Issues/2006/Volume-6/Pages/JOnline-A-Framework-for-Conducting-IT-Due-Diligence-in-Mergers-and-Acquisitions1.aspx

Symantec. (2013, December 4). Dangerous new banking trojan neverquest is an evolution of an older threat. Retrieved from http://www.symantec.com/connect/blogs/dangerous-new-banking-trojan-neverquest-evolution-older-threat

Susanne Young, sforslev@well.com

Wauters, R. (2011, June 9). Apple registered at least 50 product domain names on wwdc day. Retrieved from http://techcrunch.com/2011/06/09/apple-registered-close-to-50-product-domain-names-on-wwdc-day

Zetter, K. (2013, November 08). Power plants and other vital systems are totally exposed on the internet. Wired, Retrieved from http://www.wired.com/threatlevel/2013/11/internet-exposed/

Susanne Young, sforslev@well.com