Reconnaissance Phase:

When conducting reconnaissance, use the following tools to gather as much information as possible about the target organization. These tools will passively gather information (I.E. it is OK to run these tools before the project is started, and before an Ethical Hacking Agreement is signed, because you are not actively scanning, yet.)

theharvester

**usage:**

theharvester -d “targetDomain” -b “datasources” -f “outputtToFileName”

**Example:**

theharvester -d und.edu -b google

**Run once more and record output for recon-ng (this may take a few minutes):**

theharvester -d und.edu -b google > ~/Documents/recon/harvester.txt

**Clean up the harvester.txt file for recon-ng:**

grep @und.edu harvester.txt > emails.txt

grep “:” harvester.txt | sed ‘/ /d’ | grep –v empty | sed 's/:/,/' > HostsAndIPs.csv

**Recon-ng**

Start with: recon-ng

show modules <- shows all available modules

show keys <- shows all available api keys

**Start by adding in your API keys:**

keys add shodan\_api <key here>

keys add bing api <key here>

**Create a new workspace, so that everything you do will be saved in one spot:**

workspaces add UND

**add the company name and domain to the workspace:**

add companies (will prompt you to enter company name)

add domains (will prompt you to enter domain, repeat if there are more than one)

view with the show commands:

show companies

show domains

show schema (shows the entire database and everything that recon-ng has collected)

**Import the information gathered from theharvester:**

use import/list <- this is the module to import lists

show schema <- Again this will show you all the tables

show options <- shows the options the import list module wants

set TABLE contacts

set COLUMN email

set FILENAME /home/jamie/Documents/recon/emails.txt

show contacts

run

**Now that emails are imported, import hosts and IP addresses:**

use import/csv\_file

set TABLE hosts

set HAS\_HEADER false

set FILENAME /home/jamie/Documents/recon/HostAndIPs.csv

set CSV\_0 host

set CSV\_1 ip\_address

run

**Review your import:**

show hosts

Now that you have a workspace with some basic info, gather some more information.

**Use the metacrawler to identify documents:**

use recon/domains-contacts/metacrawler

run <- will find documents

set EXTRACT true

run <- will now find documents and try to extract metadata (this will probably take a while)

**Copy and paste into a file, then clean out what we want:**

grep Author: meta.txt | cut –d “:” -f 2 | cut –d “ “ -f 2,3 | sort –u | grep , | grep –v IndirectOb | sed ‘s/ //’ > last-first.csv

grep Author: meta.txt | cut –d “:” -f 2 | cut –d “ “ -f 2,3 | sort –u | grep “ “ | grep –v , | sed ‘s/ /,/’ > first-last.csv

grep Author: meta.txt | cut –d “:” -f 2 | cut –d “ “ -f 2,3 | sort –u | grep –F . | sed ‘s/\./,/’ >> first-last.csv

**Import the new names from the Metadata scan:**

use import/csv\_file

set TABLE contacts

set HAS\_HEADER false

set FILENAME /home/jamie/Documents/recon/first-last.csv

set CSV\_0 first\_name

set CSV\_1 last\_name

run

show contacts

set FILENAME /home/jamie/Documents/recon/last-first.csv

set CSV\_0 last\_name

set CSV\_1 first\_name

run

show contacts

**Convert those names you just gathered into emails:**

use recon/contacts-contacts/mangle

set PATTERN (set to whatever you need default is FN.LN)

set DOMAIN und.edu

set MAX-LENGTH (whatever is needed default is 30)

run

show contacts

**use Bing Linkedin Search for names (If Bing isn’t working you can skip this)**

use recon/companies-contacts/bing\_linkedin\_cache

set LIMIT 2

run

show contacts

**Convert those names you just gathered into emails:**

use recon/contacts-contacts/mangle

set PATTERN <fn>.<mn> (set to whatever you need default is FN.LN)

set DOMAIN und.edu

set MAX-LENGTH (whatever is needed default is 30)

run

show contacts

**Check Data breaches for these contacts:**

use recon/contacts-credentials/hibp\_breach

run

use recon/contacts-credentials/hibp\_paste

run

show credentials

At this point we hopefully have a nice list email addresses, and maybe even some credentials. Now we should gather some information about external hosts.

**Use the hackertarget module to identify more hosts:**

use recon/domains-hosts/hackertarget

show options (notice the current value for SOURCE is default, its going to use the domains specified by the workplace)

run

show hosts to see the new hosts

**Use shodan to search for additional hosts: (If shodan isn’t working you can skip it)**

use recon/domains-hosts/shodan\_hostname

run

show hosts

**Search with Bing API: (If Bing isn’t working you can skip it)**

use recon/domains-hosts/bing\_domain\_api

run

show hosts

**Brute force other possible hostnames:**

use recon/domains-hosts/brute\_hosts

run

show domains

**Use the hostname resolver to try to find more IP addresses:**

use recon/hosts-hosts/resolve

run

show hosts

**Use the Shodan API to find open ports: (If Shodan isn’t working you can skip it)**

use recon/hosts-ports/shodan\_ip

run

show ports

Miscellaneous commands:

**Brute force other possible TLD’s:**

use recon/domain-domain/brute-suffix

run

show domains

**If you have IP addresses but not hostnames use the reverse resolver:**

use recon/hosts-hosts/reverse\_resovle

run

show hosts

**Use the whois miner to identify netblocks and locations:**

use recon/companies-multi/whois\_miner

run

show locations

show netblocks

Exporting and Reporting:

**Generate a nice html report:**

use reporting/html

set CREATOR (your name)

set CUSTOMER UND

run

**Export a list of IP addresses to scan:**

use reporting/list

show info

run