

# PWN DEFEND

## Hacking 101

Web Recon

Version 0.9

#pwnDefend

# Welcome

Welcome to the second short course in our hacking 101 series for pwnDefend! The intention behind this is to give people new to the security testing/hacking world some basic information on how to perform web recon using a range of open source and web based tools.

This series has been created by Daniel Card (UK\_Daniel\_Card) and is aimed to educate and help people with some basic tools, techniques and practises.

**Please only use this information for good! Ensure you use these tools where you either own the assets or have the owners permission! Check local laws and don't break them! #hack4good**

# Introduction

This course aims to teach the basics of web recon

By the end of the course you should be familiar with both passive and active recon using a range of tools and services, however please note, this isn't a how to guide on all the things! You will need to do some exploration with the tools and techniques.

# Learning Goals

- Understand how to conduct passive and active recognisance against a target
- Understand the range of options available to get data on a target
- Understand the pros and cons for different methods and toolsets

# Course Requirements

Whilst you should be able to follow the content here without a huge level of experience it's advisable to have some knowledge in the following areas:

- OS fundamentals LINUX and WINDOWS
- Basic TCP/IP Network knowledge
- Experience using a hypervisor such as ORACLE Virtual Box, Hyper-V, VMware player etc.
- Be able to use a web browser and have an internet connection



# Why we care?

- Recognisance gives us the ability to leverage intel on the target to assist in achieving our goals.
- By understanding our targets internet presence we can better understand our targets purpose, their data exposure and we can get a feel for their security posture.

# Situation

- We are conducting reconnaissance as part of an engagement to understand the targets risk profile based on its internet presence.
- We are tasked with identifying likely vulnerable areas to assist in planning a further downstream attack.

# Active vs Passive Recon

- Passive recon will not touch the target network and will use public sources of information
- Active recon will create traffic that if not proxied will show traffic from the attacker to the target
  - It can be wise to use TORGHOST, VPNs or anonymising proxies

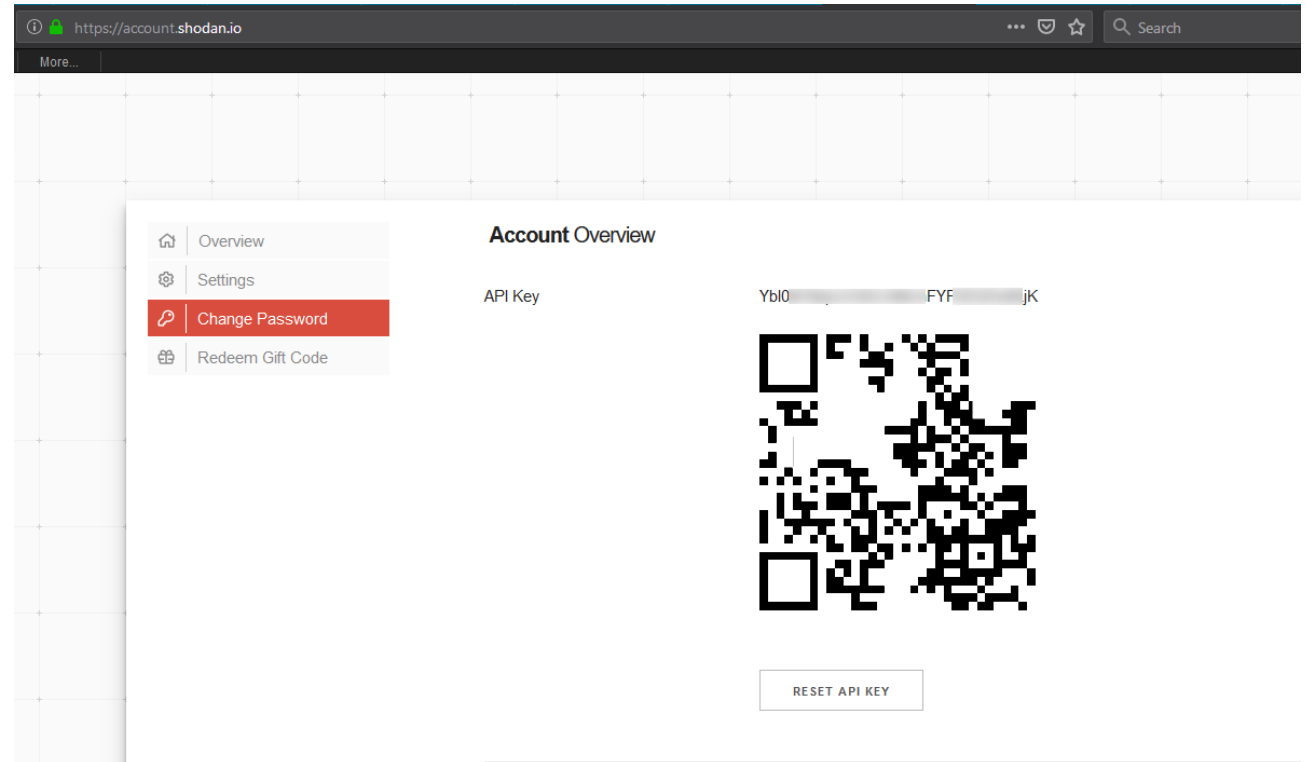


# API Keys

A lot of tools require API Keys

([https://en.wikipedia.org/wiki/Application\\_programming\\_interface\\_key](https://en.wikipedia.org/wiki/Application_programming_interface_key))

These often require you to signup, some require subscriptions/fees. If you need to maintain OpSec, use a burner mail account!



# Notes from the field

Tools are great, they let you collect large volumes of data and can help sort through noise to get to useful intel, however you need time to contextualise, read and understand this data.

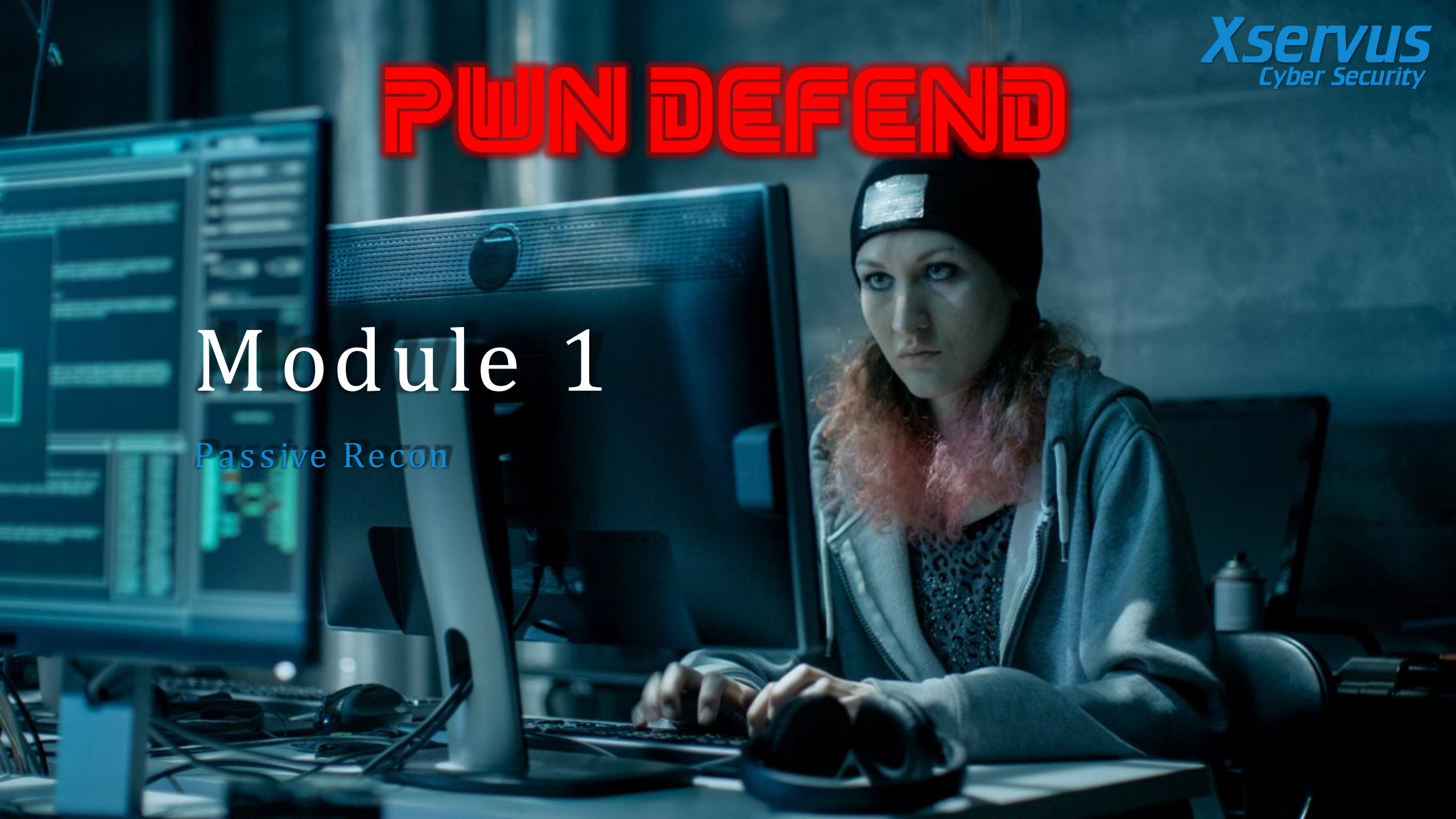
Using a web browser and doing some intel gathering will help you understand your target's business, people and customers better than any tool output will.

The key here is to manage your time wisely and combine manual and tool based research to build a picture in a timely manner.

# PWN DEFEND

## Module 1

Passive Recon



# Covering your tracks

Before we start delving into the web we need to think about privacy and precautions we may want to take! **Make sure you understand the legal implications of investigations before you start going out wild on the internet! Do not break the law!**

Some tools which can help with anonymous internet access are below:

<https://tails.boum.org/>

<https://www.torproject.org/projects/torbrowser.html.en>

<https://github.com/susmithHCK/torghost>

# whois

The whois tool looks up domain registrar details and can be used either for forward lookups (domain name) or reverse lookup (ip address). Due to GDPR the usefulness of whois lookups is dramatically reduced at the time of writing due to data protection laws.

```
root@kali2019:~# whois pwdefend.com
No match for domain "PWDEFEND.COM".
>>> Last update of whois database: 2019-02-21T20:41:13Z <<<

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability. VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
root@kali2019:~# █
```

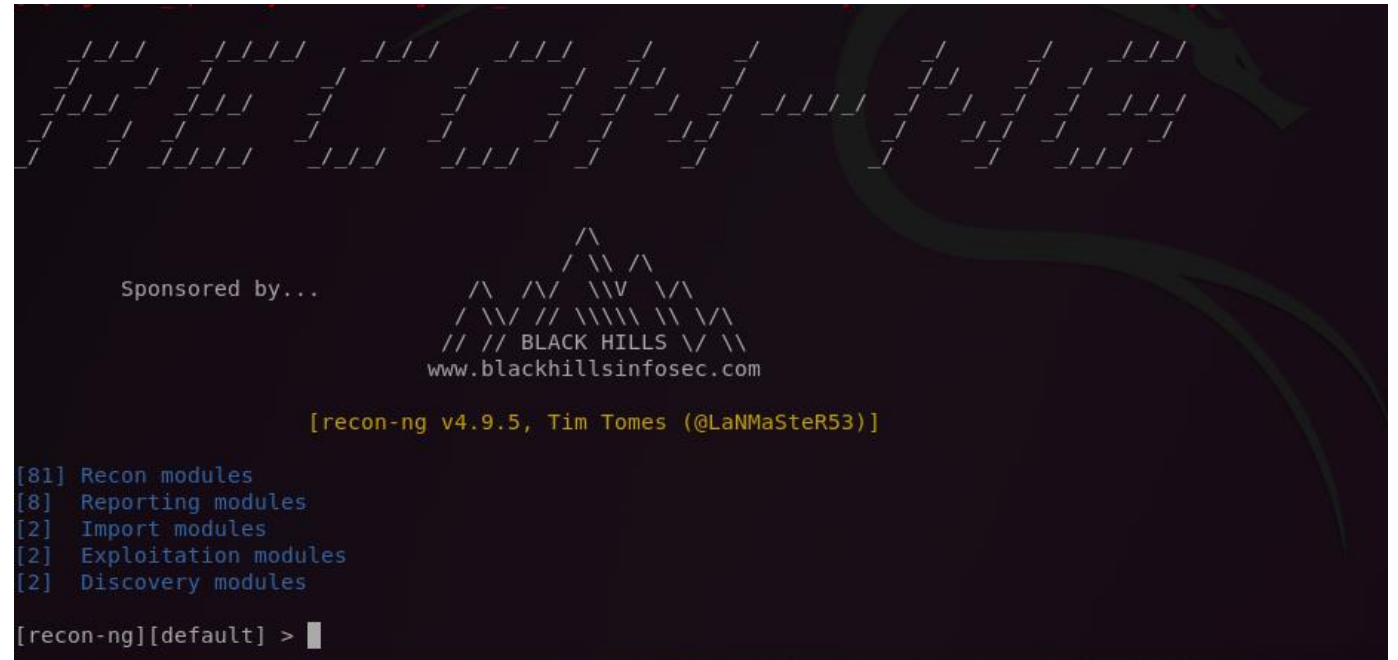


# Recon-ng

Recon-ng is an open source recon framework.

To get the most out of recon-ng API keys should be configured for services such as:

- Twitter
- HavelBeenPwned
- Google
- Jigsaw
- Shodan

A screenshot of a terminal window showing the Recon-ng framework's startup sequence. At the top, the word 'RECONNG' is displayed in a large, stylized font made of small dashes. Below it, the text 'Sponsored by...' is followed by a logo for 'BLACK HILLS' and the website 'www.blackhillsinfosec.com'. The version and author information '[recon-ng v4.9.5, Tim Tomes (@LaNMaSteR53)]' is shown in yellow. A list of modules is displayed in blue: '[81] Recon modules', '[8] Reporting modules', '[2] Import modules', '[2] Exploitation modules', and '[2] Discovery modules'. The prompt '[recon-ng][default] >' is at the bottom with a cursor.

```
RECONNG

Sponsored by...
// // BLACK HILLS // //
www.blackhillsinfosec.com

[recon-ng v4.9.5, Tim Tomes (@LaNMaSteR53)]

[81] Recon modules
[8]  Reporting modules
[2]  Import modules
[2]  Exploitation modules
[2]  Discovery modules

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

The syntax for recon-ng is similar to the Metasploit framework

# Google Dorks

Most people just use regular string searches in google, however for conducting recon we can do a whole lot more!

In google you can use dorks, which are query parameter searches which have the following syntax:

intitle:

inurl:

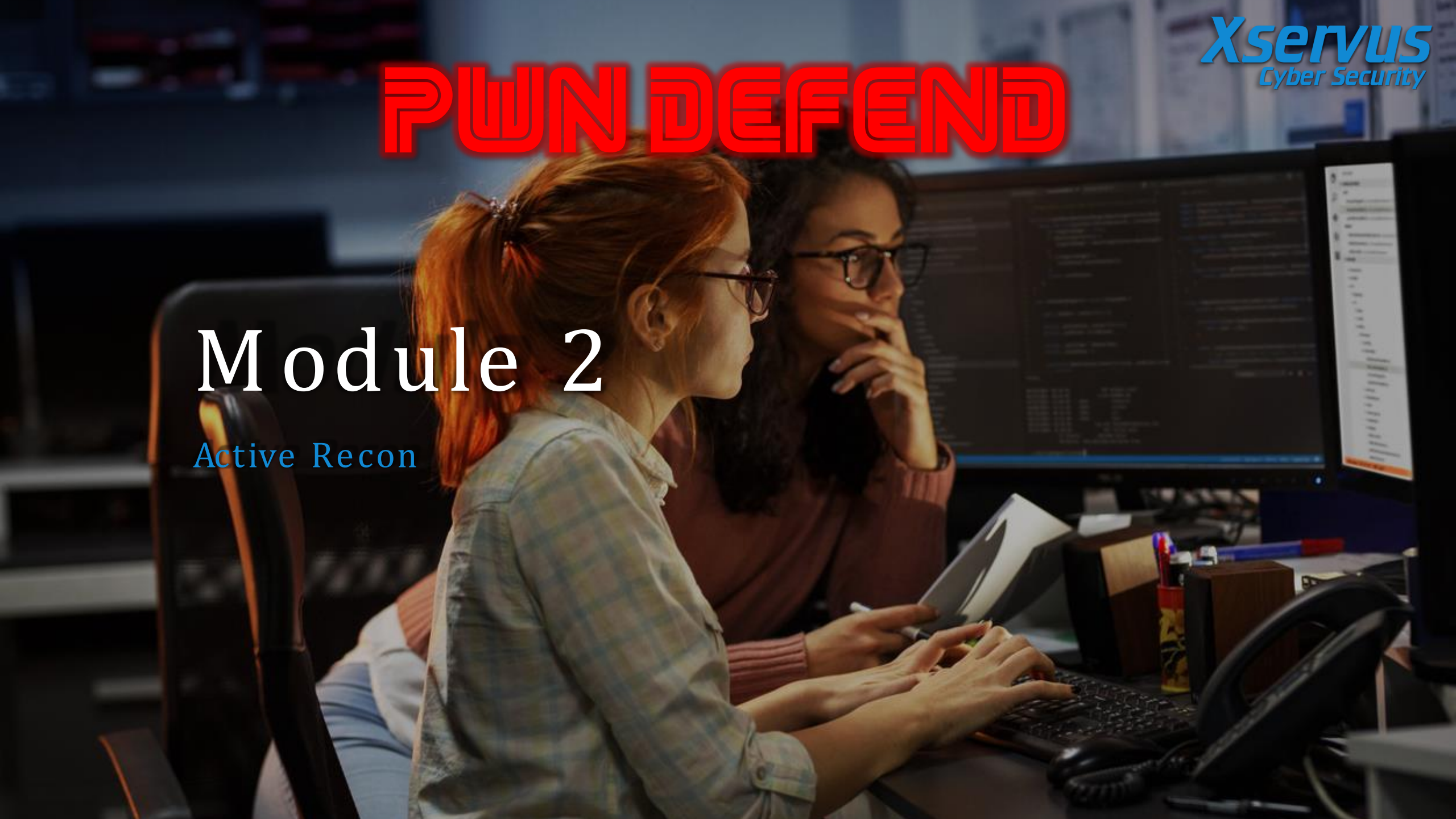
site:

filetype:

# PWN DEFEND

## Module 2

Active Recon





# Nslookup

On Windows, GNU/LINUX and OS X you will likely find this tool. Whilst the syntax can vary slightly nslookup lets you send DNS requests to a target. This is useful as the traffic will blend in with normal requests. We can target a specific server and record type e.g.

server 8.8.8.8

set type=MX

pwndefend.com

```
root@kali2019:/pentest# nslookup
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> set type=mx
> pwndefend.com
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
pwndefend.com mail exchanger = 0 pwndefend-com.mail.protection.outlook.com.

Authoritative answers can be found from:
> █
```

# DMitry

DMitry (Deepmagic Information Gathering Tool) is a UNIX/(GNU)Linux Command Line. This is a great tool which can get a lot of intel on a target.

<https://tools.kali.org/information-gathering/dmitry>

```
root@kali2019:~# dmitry pwndefend.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:213.171.195.105
HostName:pwndefend.com

Gathered Inet-whois information for 213.171.195.105
-----

inetnum:          213.171.192.0 - 213.171.195.255
netname:          FASTHOSTS-UK-NETWORK
org:              ORG-FHL1-RIPE
descr:            Shared Hosting
country:          GB
admin-c:          FHUK-RIPE
tech-c:           FHUK-RIPE
status:           ASSIGNED PA
mnt-by:           AS15418-MNT
mnt-by:           AS8560-MNT
remarks:          INFRA-AW
created:          2011-03-23T17:34:05Z
last-modified:    2019-01-24T10:41:55Z
source:           RIPE

organisation:     ORG-FHL1-RIPE
org-name:         Fasthosts Internet Limited
org-type:         LIR
address:          Discovery House 154 Southgate Street
address:          GL1 2EX
address:          Gloucester
address:          UNITED KINGDOM
phone:            +448445830777
fax-no:           +441452541633
mnt-ref:          AS15418-MNT
mnt-ref:          RIPE-NCC-HM-MNT
mnt-by:           RIPE-NCC-HM-MNT
mnt-by:           AS15418-MNT
admin-c:          FHUK-RIPE
tech-c:           FHUK-RIPE
abuse-c:          FH4126-RIPE
created:          2004-04-17T12:14:35Z
last-modified:    2019-02-15T10:21:18Z
source:           RIPE # Filtered

role:             Fasthosts Networks UK
address:          Fasthosts Internet Limited
address:          Discovery House
address:          154 Southgate Street
address:          Gloucester, GL1 2EX
phone:            +44 1452 553077
```

# Host

- Host is a dns lookup tool

```
root@kali2019:~# host pwndefend.com
pwndefend.com has address 213.171.195.105
pwndefend.com mail is handled by 0 pwndefend-com.mail.protection.outlook.com.
root@kali2019:~# █
```

# DNSRecon

DNS Recon is a great tool (alongside DIG) for DNS enumeration

The following example shows dnsrecon being used to enumerate pwndefend.com and attempt a subdomain enumeration and save the results in pwndefend.xml

```
dnsrecon -d pwndefend.com -D /usr/share/wordlists/dnsmap.txt -t std -  
-xml pwndefend.xml
```

<https://tools.kali.org/information-gathering/dnsrecon>

# Subdomain enumeration using Sublist3r

Subdomain enumeration can be achieved using a range of methods. Sublist3r is a great tool for doing this.

<https://github.com/about3l3/Sublist3r>

```
root@kali2019:/pentest/Sublist3r# ./sublist3r.py -d pwndefend.com

  SUBLIST3R

# Coded By Ahmed Aboul-Ela - @about3l3

[-] Enumerating subdomains now for pwndefend.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Total Unique Subdomains Found: 1
ctf01.ctf.pwndefend.com
root@kali2019:/pentest/Sublist3r#
```

# dnsenum

dnsenum is a tool included in kali. An example of the output is from the following command:

*dnsenum pwndefend.com*

<https://tools.kali.org/information-gathering/dnsenum>

```
root@kali2019:/pentest# dnsenum pwndefend.com
Smartmatch is experimental at /usr/bin/dnsenum line 698.
Smartmatch is experimental at /usr/bin/dnsenum line 698.
dnsenum VERSION:1.2.4

----- pwndefend.com -----

Host's addresses:
-----
pwndefend.com.                600      IN      A       213.171.195.105

Name Servers:
-----
ns1.livedns.co.uk.           600      IN      A       217.160.81.244
ns2.livedns.co.uk.           600      IN      A       217.160.82.244
ns3.livedns.co.uk.           600      IN      A       217.160.83.244

Mail (MX) Servers:
-----
pwndefend-com.mail.protection.outlook.com. 10      IN      A       104.47.0.36
pwndefend-com.mail.protection.outlook.com. 10      IN      A       104.47.2.36

Trying Zone Transfers and getting Bind Versions:
-----

Trying Zone Transfer for pwndefend.com on ns3.livedns.co.uk ...
AXFR record query failed: NOTAUTH

Trying Zone Transfer for pwndefend.com on ns1.livedns.co.uk ...
AXFR record query failed: NOTAUTH

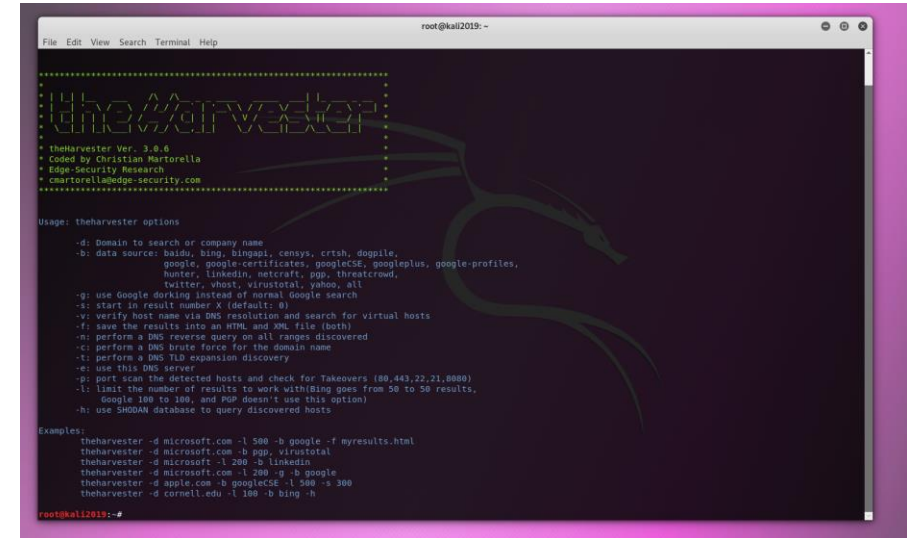
Trying Zone Transfer for pwndefend.com on ns2.livedns.co.uk ...
AXFR record query failed: NOTAUTH

brute force file not specified, bay.
root@kali2019:/pentest#
```

# The Harvester

The harvester is a tool which is going to scour the internet to get you data on the target domain. Again you will need to configure API keys for best results:

```
theharvester -d  
pwndefend.com -l 500 -b all -f  
pwndefend-c2.html
```



```
root@kali2019: ~
File Edit View Search Terminal Help

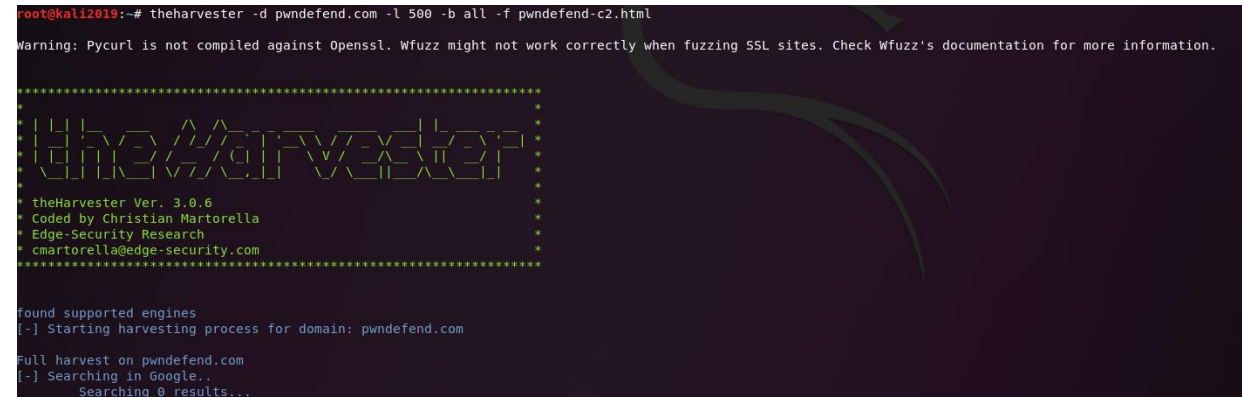
theHarvester

theHarvester Ver. 3.0.6
Coded by Christian Martorella
Edge-Security Research
cmartorella@edge-security.com

Usage: theharvester options
-d: Domain to search or company name
-b: data source: baidu, bing, bingapi, censys, crtsh, doppile,
    google, google-certificates, googleCSE, googleplus, google-profiles,
    hunter, linkedin, netcraft, pgg, threatcrowd,
    twitter, whois, virustotal, yahoo, all
-s: start in result number X (default: 0)
-v: verify host name via DNS resolution and search for virtual hosts
-f: save the results into an HTML and XML file (both)
-n: perform a DNS reverse query on all ranges discovered
-c: perform a DNS brute force for the domain name
-t: perform a DNS TLD expansion discovery
-e: use this DNS server
-l: port scan the detected hosts and check for Takeovers (80,443,22,21,8080)
    -l: limit the number of results to work with(fuzz goes from 50 to 50 results,
    Google 100 to 100, and PGP doesn't use this option)
-h: use SHODAN database to query discovered hosts

Examples:
theharvester -d microsoft.com -l 500 -b google -f myresults.html
theharvester -d microsoft.com -b pgg, virustotal
theharvester -d microsoft.com -l 200 -b linkedin
theharvester -d microsoft.com -l 200 -g -b google
theharvester -d apple.com -b googleCSE -l 500 -s 300
theharvester -d cornell.edu -l 100 -b bing -h

root@kali2019:~#
```



```
root@kali2019:~# theharvester -d pwndefend.com -l 500 -b all -f pwndefend-c2.html
Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.

theHarvester

theHarvester Ver. 3.0.6
Coded by Christian Martorella
Edge-Security Research
cmartorella@edge-security.com

found supported engines
[-] Starting harvesting process for domain: pwndefend.com

Full harvest on pwndefend.com
[-] Searching in Google..
    Searching 0 results...
```

# Web Based Tools

There's a lot of tools you can use for recon! Way more than I can realistically go into in a short course, and as you may have noticed there is a lot of overlap! What we are going to do is look at some key areas of recon and leave the main exploring experience for you! However let's look at some tools that are used on real engagements:

- <https://dnsdumpster.com/>
- <https://securitytrails.com/>

Both of these sites have API access



# PWN DEFEND

## Module 3

Visualisation Toolsets

# Maltego

- Maltego is a great tool for obtaining and visualising data on a target. There is a community version included in Kali, however for large targets you will need a subscription.
- Fire it up and see what intel you can locate on a target. Also look at the extension modules (you will often need an API key) e.g. Shodan



# Spiderfoot

My friend Jason (thanks dude!) introduced me to Spider foot. Spiderfoot is a fantastic tool, once again you will need API keys configured to get the most out of this. You will also want to plan sensibly with time management. I often will run this days before I start an engagement so that it's collecting data over the days and nights before I want to review the data.

<https://www.spiderfoot.net/>



# Spiderfoot HX

Whilst writing this episode I wanted to quickly touch on SpiderFoot HX (Currently in private beta)

This brings the SpiderFoot to the Cloud era! So far I'm really liking the experience

<https://www.spiderfoot.net/hx/>





# PWN DEFEND

## Module 4

Specialised Search Engines

# Search Engines

## Shodan

Shodan is probably the most well known internet device search engine

Website: <https://account.shodan.io/login>

## Censys

<https://censys.io/>

Both have their own syntax but you can do some cool recon with these!

# Shodan

- Shodan is branded as the search engine for the internet of things! It's incredibly popular and is a great source of data.

The screenshot displays the Shodan search engine interface. At the top, the Shodan logo is on the left, followed by a search bar containing 'pwnDefend'. To the right of the search bar are navigation links: 'Explore', 'Downloads', 'Reports', 'Developer Pricing', and 'Enterprise Access'. Below the search bar is a secondary navigation bar with buttons for 'Exploits', 'Maps', 'Share Search', 'Download Results', and 'Create Report'.

The main content area is divided into several sections:

- TOTAL RESULTS:** Shows a count of 2 results.
- TOP COUNTRIES:** Includes a world map with red markers indicating the locations of the search results. Below the map, a table lists the top countries: United States (1) and Netherlands (1).
- TOP ORGANIZATIONS:** A table listing the top organizations: Microsoft Azure (2).

On the right side, two search results are displayed:

- 13.81.11.233:** Identified as Microsoft Azure, added on 2019-02-17 07:18:00 GMT, located in the Netherlands, Amsterdam. A 'cloud' icon is present. The associated text includes: '220 pwnDefend CTF01 FTP - Not in Scope however http://ctf01.ctf.pwndefend.com/ is ;)', '530 Login incorrect.', '530 Please login with USER and PASS.', '211-Features: EPRT, EPSV, MDTM, PASV, REST STREAM, SIZE, TVFS', and '211 End'.
- 40.83.165.35:** Identified as Microsoft Azure, added on 2019-02-18 11:15:08 GMT, located in the United States, San Jose. A 'cloud' icon is present. The associated text includes: '220 pwnDefend CTF02 FTP - In Scope however don't bother using brute ;)', '230 Login successful.', '214-The following commands are recognized. ABOR ACCT ALLO APPE CDUP CWD DELE EPRT EPSV FEAT HELP LIST MDTM MKD MODE NLST NOOP OPTS PASS PASV PORT PWD QUIT REIN REST RETR RMD RNFR RNT0 SITE SIZE SM...', and '214 End'.

At the bottom right, a copyright notice reads: '© 2013-2019, All Rights Reserved - Shodan®'.

# Censys

- The following example shows a Censys search result for pwnDefend

The screenshot shows the Censys search interface. At the top, the Censys logo is on the left, and a search bar contains 'IPv4 Hosts' and 'pwnDefend'. To the right of the search bar are links for 'Register' and 'Sign In'. Below the search bar, a navigation bar includes links for 'Results', 'Map', 'Metadata', 'Report', and 'Docs'. The main content area is divided into two columns. The left column, titled 'Quick Filters', contains sections for 'Autonomous System' (listing 2 results for MICROSOFT-CORP-MSN-AS-BLOCK), 'Protocol' (listing 2 results for 21/ftp, 22/ssh, 80/http), and 'Tag' (listing 2 results for ftp, http, ssh). The right column, titled 'IPv4 Hosts', shows two results. The first result is for IP 13.81.11.233, located in Amsterdam, North Holland, Netherlands, with details about the host being a MICROSOFT-CORP-MSN-AS-BLOCK, running Ubuntu, and having ports 21/ftp, 22/ssh, 80/http open. The second result is for IP 40.83.165.35, located in San Jose, California, United States, with details about the host being a MICROSOFT-CORP-MSN-AS-BLOCK, running Ubuntu, and having ports 21/ftp, 22/ssh, 80/http open. Both results show a search for '80.http.get.body: <? // error\_reporting(E\_ALL); // ini\_set("display\_errors", 1); ?> <html lang = "en"> <he'.

**Quick Filters**  
For all fields, see [Data Definitions](#)

**Autonomous System:**

- 2 MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation

**Protocol:**

- 2 21/ftp
- 2 22/ssh
- 2 80/http

**Tag:**

- 2 ftp
- 2 http
- 2 ssh

**IPv4 Hosts**  
Page: 1/1 Results: 2 Time: 31ms

[13.81.11.233](#)

- MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation (8075) Amsterdam, North Holland, Netherlands
- Ubuntu 21/ftp, 22/ssh, 80/http
- #pwnDefend CTF Challenge 01
- 80.http.get.body: <? // error\_reporting(E\_ALL); // ini\_set("display\_errors", 1); ?> <html lang = "en"> <he

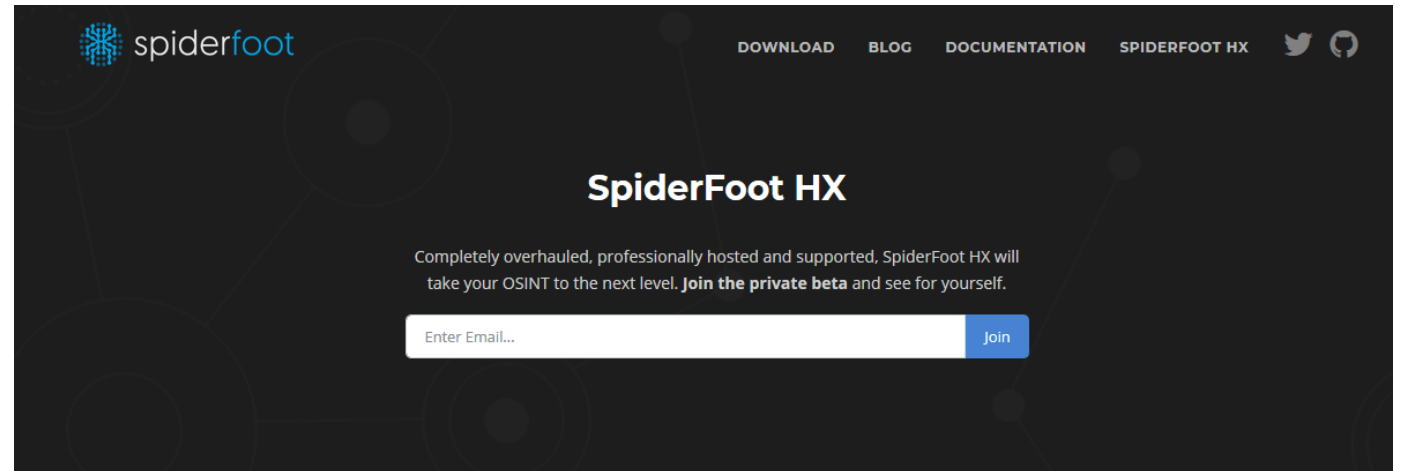
[40.83.165.35](#)

- MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation (8075) San Jose, California, United States
- Ubuntu 21/ftp, 22/ssh, 80/http
- 403 Forbidden
- 21.ftp.banner.banner: 220 pwnDefend CTF02 FTP - In



# Spiderfoot HX

There is also a hosted version of SpiderFoot in the form of SpiderFoot HX which is currently in private beta!



## SPIDERFOOT HX FEATURES

SpiderFoot HX builds upon the module base of the open source version and a completely overhauled architecture for scalability, speed and much more functionality.



### Cloud Hosted

Accessible any time, anywhere requiring no management or setup costs. Always be running the latest version.



### Scheduled Scanning

Automatically scan targets according to a daily, weekly or monthly schedule, without having to manually perform the scan. This is most useful for continuous perimeter monitoring.



### Scale & Speed

Get results 5-10x faster than the open source version and handle over one million data elements easily, thanks to a completely overhauled and distributed architecture.



### Change Detection

Be notified about the changes detected between scheduled scans, enabling the identification of potential risks quickly. You can also pick any two scans and compare them to identify differences.



### API

Further automate your OSINT by integrating with the fully documented RESTful API, including examples to get you up-and-running quickly.



### Team Collaboration

Define different access levels to team members using SpiderFoot HX and add annotations to data elements and identified changes.



### Multi-target Scanning

Got multiple entities which are in reality part of the same target? With SpiderFoot HX you can specify multiple targets in the one scan to easily see all the inter-relationships.



### Reporting & Drill-down

Automatically identify risky data items, break down data based on the source, category or module, drill down into individual data points to see their inter-relations and history.

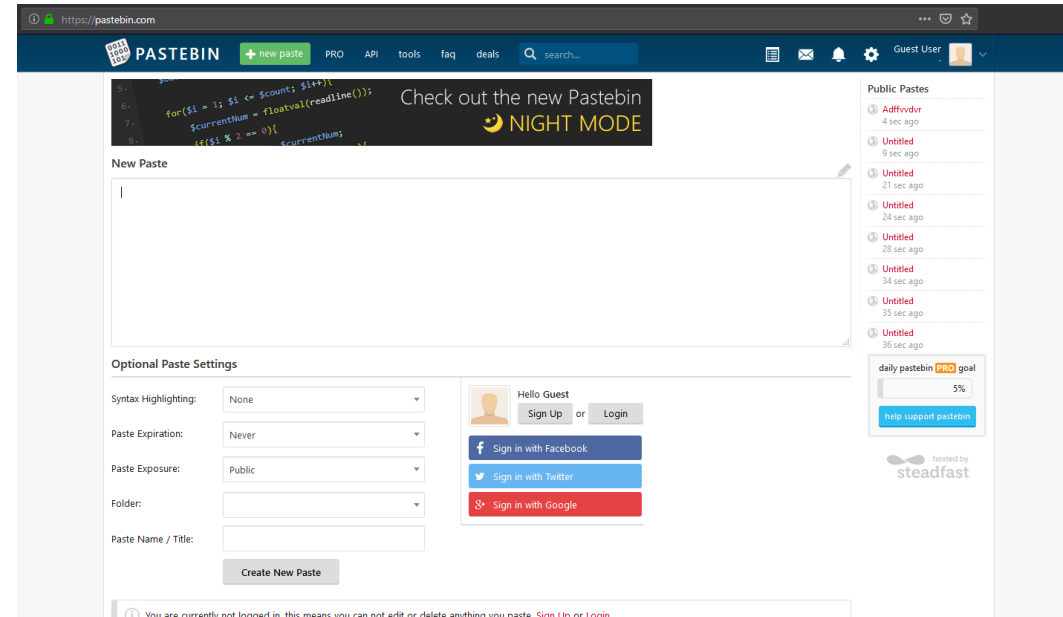


### Support

E-mail support around the clock to help you get the most value out of SpiderFoot HX and address any issues you might encounter.

# Pastebin

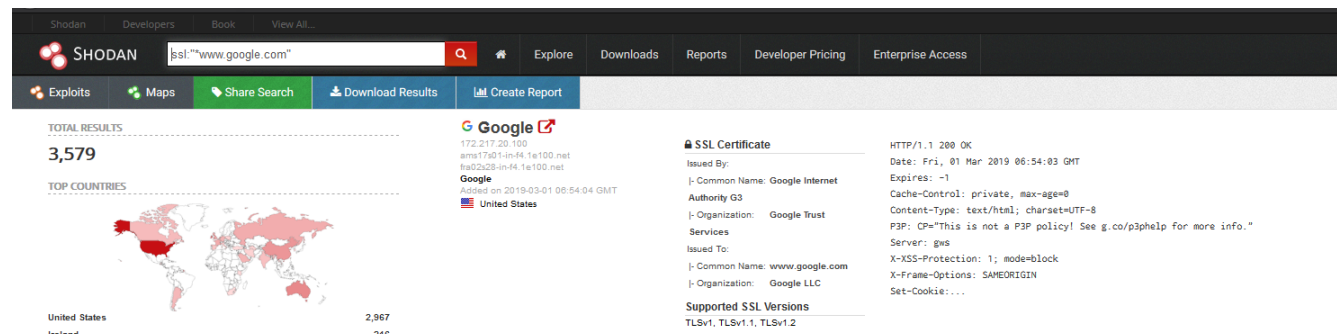
- Pastebin is a text only paste site! It's very commonly used by people to dump data quickly... it can contain a wealth of information



# Pro Tip

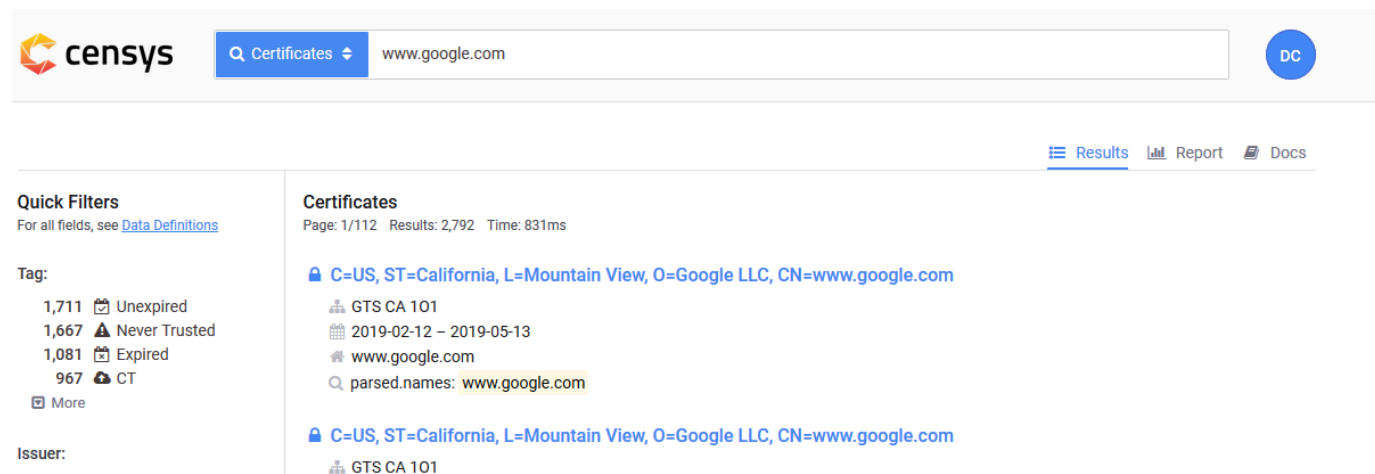
I've not called out tool syntax in this episode on purpose. However I want to showcase something cool that I use on ops!

Sometimes you will be hunting a target that has tried to be obscure, searching certificate data can be a quick way to find your targets (and sometimes leaks internal server/domain names and IPs etc.)



SHODAN search results for the query `ssl:"www.google.com"`. The interface shows a top navigation bar with links like Shodan, Developers, Book, and View All. Below the search bar, there are tabs for Exploits, Maps, Share Search, Download Results, and Create Report. The main content area displays the following information:

- TOTAL RESULTS:** 3,579
- TOP COUNTRIES:** A world map with red markers indicating the locations of the results. The United States has 2,967 results, Ireland has 216, and Australia has 115.
- Google** (IP: 172.217.20.100):
  - Common Name: Google Internet Authority G3
  - Organization: Google Trust Services
  - Issued To: www.google.com
  - Organization: Google LLC
  - Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2
- SSL Certificate:**
  - Issued By: Google
  - Issued To: www.google.com
  - Organization: Google LLC
  - Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2
- HTTP/1.1 200 OK:**
  - Date: Fri, 01 Mar 2019 06:54:03 GMT
  - Expires: -1
  - Cache-Control: private, max-age=0
  - Content-Type: text/html; charset=UTF-8
  - P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
  - Server: gws
  - X-XSS-Protection: 1; mode=block
  - X-Frame-Options: SAMEORIGIN
  - Set-Cookie: ...



Censys search results for the query `www.google.com`. The interface shows a top navigation bar with the Censys logo and a search bar. Below the search bar, there are tabs for Results, Report, and Docs. The main content area displays the following information:

- Quick Filters:** For all fields, see [Data Definitions](#).
- Tag:**
  - 1,711 Unexpired
  - 1,667 Never Trusted
  - 1,081 Expired
  - 967 CT
  - [More](#)
- Issuer:** GTCS CA 101
- Certificates:** Page: 1/112 Results: 2,792 Time: 831ms
  - [C=US, ST=California, L=Mountain View, O=Google LLC, CN=www.google.com](#)
  - GTCS CA 101
  - 2019-02-12 – 2019-05-13
  - www.google.com
  - parsed.names: www.google.com
  - [C=US, ST=California, L=Mountain View, O=Google LLC, CN=www.google.com](#)
  - GTCS CA 101

# PWN DEFEND

## Hacking 101

Course 2 Review

# Exercises

## Exercise A – Passive Recon

1. Practise passive recon against a chosen domain (feel free to use [pwndefend.com](https://pwndefend.com) however you may find targets with richer datasets)
2. Look at the differences between active and passive tools

# Exercises

## Exercise B – Active Recon

1. Practise active recon against a domain (feel free to use [pwndefend.com](https://pwndefend.com)) and lab server targets

***Make sure you know what your tools are doing before blindly using them on the internet! It's a good idea to setup lab servers and use active scan against these. You can use a cloud service provider such as Azure or Amazon AWS/EC2 to get real life experience in a safe way! Check applicable laws before doing active recon on a target you don't own!***

# Exercises

## Exercise C – Data Visualisation Tools

1. Practise using Maltego to map a target domain
2. Look at adding manually discovered data into the dataset
3. Use 3<sup>rd</sup> party extensions such as Shodan to enriched the dataset

# Exercises

## Exercise D – Specialist Search Engines

1. Practise using Shodan and Censys to identify target intel
2. Hunt for the pwnDefend flag hidden on pastebin!



# Review

In this short course we covered:

- Ensuring our actions are lawful
- Active and Passive Internet Reconnaissance
- Tools and techniques to perform recon using command line and web based tools
- Reviewed data capture and visualization toolsets (Maltego)
- Used general purpose and specialised search engines

# PWN DEFEND

## Hacking 101

Course 2 Review

# Course 2 Complete

We hope this short course content was useful and gave a decent insight into web recon with common tools. The subject is huge and this is just a taster. You really need to get your hands on with this and get active with the tools and techniques! Get lab time in, it will pay dividends down the road!

Go and read all the things and practise in safe environments. Remember just because you find it on the internet, even if its exposed to the public doesn't mean you should be poking into it! Remember to operate within your local laws! Use hacking as a force for good! #hack4good

I truly hope this was useful for you, please send comments/feedback/suggestions back to UK\_Daniel\_Card on twitter!

# PWN DEFEND

Created by

***Xservus***  
***Cyber Security***

<https://www.xservus.com>

Thank you!

#pwnDefend