



# Scanning & Footprinting

Nmap, Netdiscover, Netcat, Masscan  
WHOIS, Web Archive, OSINT

By Deano

B00091839@student.itb.ie



# **!!! WARNING !!!**

I and the Hacker Soc will not be responsible for your mistakes or actions with the information you will learn from this or any talks or workshops you participate

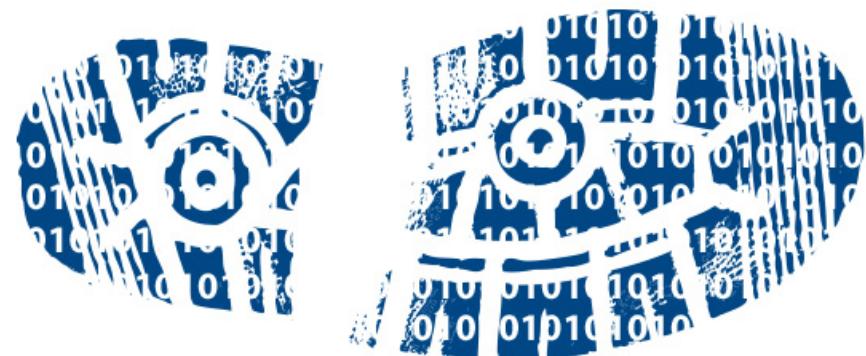


# Footprinting

AKA Reconnaissance

Simply “gathering of information before the attack”

This could be from a WHO.is or DNS record, historic information from web.archive.org or OSINT from public posts.



# Google Hacking - DORK

## Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

Any Category

Search

SEARCH

| Date       | Title   | Category                       |
|------------|---|--------------------------------|
| 2018-07-03 | filetype:xls   xlsx intext:software license site:.gov                         | Files Containing Juicy Info    |
| 2018-07-03 | filetype:xls   xlsx intext:cisco .cisco.com site:.gov                         | Files Containing Juicy Info    |
| 2018-07-03 | intext:vmware virtual site:.gov filetype:xls   xlsx   doc   pdf               | Files Containing Juicy Info    |
| 2018-07-03 | (intitle:"plexpy - home" OR "intitle:tautulli - home") AND intext:"libraries" | Various Online Devices         |
| 2018-07-02 | intext:define(AUTH_KEY, 'wp-config.php filetype:txt                           | Files Containing Passwords     |
| 2018-06-27 | "Powered by 2Moons"   | Advisories and Vulnerabilities |
| 2018-06-26 | intitle:"UltraDNS Client Redirection Service"                                 | Various Online Devices         |
| 2018-06-26 | "Powered by Planet eStream"   | Pages Containing Login Portals |
| 2018-06-25 | intitle:"This is pdfTeX. Version"   | Files Containing Juicy Info    |
| 2018-06-25 | inurl:wp-config-backup.txt  | Files Containing Passwords     |

### Footholds (74)

Examples of queries that can help an attacker gain a foothold into a web server

### Sensitive Directories (166)

Google's collection of web sites sharing sensitive directories. The files contained in here will vary from sensitive to über-secret!

### Vulnerable Files (62)

HUNDREDS of vulnerable files that Google can find on websites.

### Vulnerable Servers (94)

These searches reveal servers with specific vulnerabilities. These are found in a different way than the searches found in the "Vulnerable Files" section.

### Error Messages (100)

Really verbose error messages that say WAY too much!

### Network or Vulnerability Data (84)

These pages contain such things as firewall logs, honeypot logs, network information, IDS logs... All sorts of fun stuff!

### Various Online Devices (386)

This category contains things like printers, video cameras, and all sorts of cool things found on the web with Google.

### Web Server Detection (101)

These links demonstrate Google's awesome ability to profile web servers.

### Files Containing Usernames (21)

These files contain usernames, but no passwords... Still, Google finding usernames on a web site.

### NEW Files Containing Passwords (263)

PASSWORDS!!! Google found PASSWORDS!

### Sensitive Online Shopping Info (11)

Examples of queries that can reveal online shopping information like customer data, suppliers, orders, credit card numbers, credit card info, etc

### NEW Files Containing Juicy Info (523)

No usernames or passwords, but interesting stuff none the less.

### Pages Containing Login Portals (486)

These are login pages for various services. Consider them the front door of a website more sensitive functions.

### Advisories and Vulnerabilities (2017)

These searches locate vulnerable servers. These searches are often generated from various security advisory posts, and in many cases are product or version-specific.

### Advanced

### What you can do with it

### Google this

**site:** search only within a specific site

**site:**www.stanford.edu

**filetype:** find a type of file: PDF, DOC, TXT ...

**filetype:**PDF

**define:** find definitions for a word

**define:**audacity

**intitle:** find words in the title of the webpage

**intitle:**inspirational

**..** get ranges of numbers, dates, or prices

presidents 1800 ..1900

**word \* word** find other combinations of words between words

creative \* writing

**-word** search for homer, but NOT simpson

homer -simpson

**"word"** find exact words—no synonyms or plurals

"peace" "freedom"

**"set of words"** search for exact set of words, quotes or phrases

"I have a dream"



index: index.of (mp4) p90x



All Videos Images News Shopping More Settings Tools

About 137,000 results (0.36 seconds)

### Index of /public/P90x

www.spodi.com/public/P90x/?C=D;O=A ▾

Index of /public/P90x ... [VID].P90x-Ab Ripper.mp4, 2013-12-13 18:55, 405M. [VID].P90x-Back and ... P90x-Chest and Back.mp4, 2013-12-13 18:56, 1.7G. [VID] ...

### Index of /misc/P90X

netsleds.com/misc/P90X/ ▾

Index of /misc/P90X. Name Last modified Size Description · Parent Directory - AB RIPPER.avi 09-Mar-2010 20:21 207M BACK BICEPS.mp4 09-Mar-2010 ...

### Index of /P90X/AVI - Parent Directory - vcci.org

media.vcci.org/P90X/AVI/ ▾

Index of /P90X/AVI. Parent Directory - AB Ripper.X.avi · Back & Biceps.avi · Cardio X.avi · Chest & Back.avi · Chest, Shoulders, & Triceps.avi · Core Synergistics.

### Index of /p90x3 - Borealis Media

www.borealismedia.com/p90x3/ ▾

P90X.DISC.12.Ab.Ripper.mov, 14-Sep-2012 10:07, 255M. [], P90X3 - Accelerator.mp4, 10-Oct-2014 20:26, 650M. [], P90X3 - Agility X.mp4, 10-Oct-2014 20:30 ...

### Index of /P90X

## Index of /public/P90x

| Name  | Last modified    | Size | Description |
|---|------------------|------|-------------|
|  Parent Directory        | -                | -    | -           |
|  P90x-Ab Ripper.mp4      | 2013-12-13 18:55 | 405M |             |
|  P90x-Back and Biceps.>  | 2013-12-13 18:55 | 1.7G |             |
|  P90x-Cardio X.mp4       | 2013-12-13 18:56 | 1.0G |             |
|  P90x-Chest Shoulders.>  | 2013-12-13 18:57 | 1.8G |             |
|  P90x-Chest and Back.mp4 | 2013-12-13 18:56 | 1.7G |             |
|  P90x-Core Synergisti..> | 2013-12-13 18:55 | 1.4G |             |
|  P90x-Kenpo X.mp4        | 2013-12-13 18:58 | 1.5G |             |
|  P90x-Legs and Back.mp4  | 2013-12-13 18:59 | 1.9G |             |
|  P90x-Patience Yoga.mp4  | 2013-12-13 18:59 | 943M |             |
|  P90x-Plyometrics.mp4    | 2013-12-13 19:00 | 1.5G |             |
|  P90x-Shoulders and A..> | 2013-12-13 18:58 | 1.9G |             |
|  P90x-X Stretch.mp4      | 2013-12-13 19:00 | 1.4G |             |
|  P90x-Yoga X.mp4         | 2013-12-13 19:01 | 2.2G |             |

Apache Server at www.spodi.com Port 80

## Index of /admin/report/stats - Balbriggan Community College

[www.balbriggancommunitycollege.com/admin/report/stats/](http://www.balbriggancommunitycollege.com/admin/report/stats/) ▾

Index of /admin/report/stats. Name · Last modified · Size · Description · Parent Directory, -. settings.php, 2010-07-14 00:01, 242.

## Index of password txt facebook login - Northeast Smart Energy

[nesmartenergy.com/annq/zdo.php?uw=index-of-password-txt-facebook-login](http://nesmartenergy.com/annq/zdo.php?uw=index-of-password-txt-facebook-login) ▾

Index of password txt facebook login [Randy Dave] Collection of comics cartoon porn. .... matter. index of/parent directory filetype:htpasswd etc File download Password. ... Password. php last modified on 21/09/17 at 9:07 010010 Jan 2006 An ...

## Index of /OnLineHelp/Utilities/BCD536-SD-CARD-STUFF - Scancat

[www.scancat.com/OnLineHelp/Utilities/BCD536-SD-CARD-STUFF/](http://www.scancat.com/OnLineHelp/Utilities/BCD536-SD-CARD-STUFF/) ▾

Index of /OnLineHelp/Utilities/BCD536-SD-CARD-STUFF. Icon Name Last modified Size Description. [DIR] Parent Directory - [ ] BCD436-536HPOM\_EN\_10.



**PROTIP:** links with ip addresses in them are often your best bet for finding cams.

## EVERYONE:

- 1: copy links into google to watch unprotected security cameras
- 2: post interesting ones
- 3: ????
- 4: PROFIT!

```
# inurl:/view.shtml
# intitle:"Live View / - AXIS" | inurl:view/view.shtml^
# inurl:ViewerFrame?Mode=
# inurl:ViewerFrame?Mode=Refresh
# inurl:axis-cgi/jpg
# inurl:view/index.shtml
# inurl:view/view.shtml
# liveapplet
# intitle:"live view" intitle:axis
# intitle:liveapplet
# allintitle:"Network Camera NetworkCamera"
# intitle:axis intitle:"video server"
# intitle:liveapplet inurl:LvAppl
# intitle:"EvoCam" inurl:"webcam.html"
# intitle:"Live NetSnap Cam-Server feed"
# intitle:"Live View / - AXIS 206M"
# intitle:"Live View / - AXIS 206W"
# intitle:"Live View / - AXIS 210?
# inurl:indexFrame.shtml Axis
# intitle:start inurl:cgistart
# intitle:"WJ-NT104 Main Page"
# intitle:snc-z20 inurl:home/
# intitle:snc-cs3 inurl:home/
# intitle:snc-rz30 inurl:home/
# intitle:"sony network camera snc-p1?
# viewnetcam.com
# intitle:"Toshiba Network Camera" user login
# intitle:"i-Catcher Console - Web Monitor"
```

# SHODAN

Main      Exploits      Research      Videos      Anniversary Promotion      Settings      Logout      Buy      ?

**SHODAN**  **Search**

Home      Search Directory      Data Analytics/ Exports      Developer Center      Labs

Dashboard      History

**Dashboard**

**Recently Shared Search Queries**

- tunisie 3
- Gas stations 2
- Dedicated Micros camera 2

[www.shodanhq.com/browse](http://www.shodanhq.com/browse)

**Your Recent Searches**

- scada port:137
- scada
- "cisco-ios" "last-modified"
- scada

0 Credits

 CONTACT ME  
STAY UP TO DATE  
[FOLLOW ME ON TWITTER](#)

For direct inquiries:

12:40 PM  
6/19/2013

**Popular Searches** 

| Date      | Search Query                         | Count |
|-----------|--------------------------------------|-------|
| 15 MAR 10 | Webcam                               | 1285  |
|           | best ip cam search I have found yet. |       |
| 13 JAN 12 | Netcam                               | 369   |
|           | Netcam                               |       |
| 13 AUG 10 | dreambox                             | 234   |
|           | dreambox                             |       |
| 6 FEB 12  | Cams                                 | 227   |
|           | admin admin                          |       |
| 14 JAN 10 | default password                     | 204   |

**Order By**

- » Popularity
- » Recently Added

**Popular Tags**

| Tag      | Count |
|----------|-------|
| scada    | 44    |
| http     | 33    |
| webcam   | 30    |
| cisco    | 24    |
| router   | 24    |
| login    | 23    |
| ftp      | 23    |
| telnet   | 21    |
| dreambox | 20    |
| voip     | 19    |

# Web Archive

## Information Gatherable

### Emails, Phone Numbers, Locations, Names, Project Names

INTERNET ARCHIVE  
http://www.itb.ie/80/  
426 captures  
4 Mar 2000 - 8 Mar 2018

FEB MAR JUN  
04 1999 2000 2001

Institute of Technology  
Blanchardstown

Institiúid Teicneolaíochta  
Baile Bhlaínsír



- Full Time Prospectus
- Continuing Education Programme
- Employment Opportunities
- Staff
- Location
- Contact Us
- Future Plans
- Disclaimer

Continuing Education Prospectus now available. E-mail your request by [Clicking here](#)

Number of visitors to this site this millennium  
0 0 0 1

Institute of Technology Blanchardstown, Blanchardstown Road North, Blanchardstown, Dublin 15. Tel. (01) 885 1000 Fax. (01) 8851001

Developed by Zilcom Limited  
Copyright © 1997 [Zilcom Limited]. All rights reserved.  
Revised: January 20, 2000.

#### Courses on offer in 2000

Until the new purpose-built campus is available for use, the Institute is limited in the number and range of courses it can offer. The following six courses will be offered from September 2000.

In choosing the courses on offer, emphasis has been placed on courses that provide skills and job opportunities in key areas of the technology sector, including electronics, computing and information technology and languages.

[National Certificate in Engineering - Electronics and Computer Engineering](#)

[National Certificate in Computing - Information Technology](#)

[National Certificate in Business Studies](#)

[National Diploma in Business Studies - Business Studies, Information Technology and French](#)

[National Diploma in Business Studies - Business Studies, Information Technology and German](#)

[National Diploma in Business Studies - Business Studies, Information Technology and Spanish](#)

[ thefacebook ]  
login register about

Welcome to Thefacebook!

[ Welcome to Thefacebook ]

Thefacebook is an online directory that connects people through social networks at colleges.

We have opened up Thefacebook for popular consumption at **Harvard University**.

You can use Thefacebook to:

- Search for people at your school
- Find out who are in your classes
- Look up your friends' friends
- See a visualization of your social network

To get started, click below to register. If you have already registered, you can log in.

[Register](#) [Login](#)

about contact faq terms privacy  
a Mark Zuckerberg production  
Thefacebook © 2004

# Who.is

The screenshot shows the Who.is website interface. At the top, there's a search bar with placeholder text "Search for domains or IP addresses..." and a magnifying glass icon. Below the search bar are navigation links for "Premium Domains", "Transfer", and "Features". A secondary navigation bar below the search bar includes "Whois", "History", "DNS Records", and "Diagnostics". The main content area is titled "whois information". Under this, there's a "Registrar Info" section with details like Name (Omnis Network, LLC), Whois Server (whois.omnis.com), and Status (ok https://icann.org/epp#ok). There's also an "Important Dates" section showing Expires On (2022-08-05), Registered On (2011-07-26), and Updated On. The "Name Servers" section lists several nameservers with their corresponding IP addresses, many of which are redacted. The "Similar Domains" section is partially visible, followed by a "Registrar Data" section which includes "Registrant Contact Information" and "Administrative Contact Information". The registrant contact information includes fields for Name, Organization, Address, City, State / Province, Postal Code, Country, Phone, and Email, all of which are redacted. The administrative contact information is similarly redacted.

## Information Gatherable

DNS Information

Names

Address

Country

Email Address

Domain Information

Phone Numbers

Server IP Address

Since 2018 is now slightly  
useless

DAMN GDPR

# OSINT

Onsite Deskside Engineer - Dublin

Apply Now

**Job Description**

- Minimum 6 yrs hands on experience as deskside/Onsite support/local IT engineer
- Experience in Providing Hands & feet Support for Network and Datacenter Equipment/Devices
- Strong Microsoft Operating System installation (Win 7 & Win10) and troubleshooting skills
- Strong experience in troubleshooting MS office (Outlook, Word, Excel, PowerPoint etc.)
- Strong desktop support knowledge including hardware, software, and networking concepts
- Strong skills in Desktops, Workstations, Notebooks and Printers and Handhelds
- Basic understanding of Audio/Video equipment and conference room setup
- User account creation for Active Directory, Exchange Mailboxes, Distribution lists
- Remote desktop connectivity applications like SMS, Bomgar, WebEx, Live Meeting, and Windows Native tools tool Escalations
- Troubleshoot and assist end users with mobile device setup, activations and performance issues.
- Handheld – Blackberry, Android & IOS support knowledge
- Strong Customer service skills
- Strong written and verbal communication skills
- Good Understanding of ITIL processes
- Hands on Experience on ITSM tools like Service Now

**Certifications**

- A+ Certified or Equivalent Certified
- CCNA - Cisco Certified Network Associate
- A+ CompTIA
- MCTS Microsoft Certified Technology Specialist

**Soft Skills**

- Excellent communication and conversation skills (Verbal and Written)
- Good in local and English language
- Good documentation skills
- Good working knowledge of MS OFFICE (Including MS Project and Visio)
- Should have a great customer handling skills
- Able to handle unforeseen situations
- High level of acceptance

**Job Type:** Contract

**Experience:**

- Deskside Engineer: 4 years (Required)

**Education:**

- Bachelor's (Required)

**Location:** Dublin

**Equipment:** Cisco, Datacentre hardware

**OS:** Windows 7 & Windows 10

**Hardware:** Desktops, Workstations, Notebooks, Printers and Handhelds

**Protocol:** Active Directory, Microsoft Exchange, Remote Desktop SMS, Bomgar, WebEx, Live Meetings.

**Handheld:** Android, Blackberry & IOS

**Experience:** 4 years + Degree



# Dumpster Diving

What it says on the tin...

Physically sifting through the trash of a company

Things That Can Be Found

Internal Email address - Used for Phishing  
Internal Phone Numbers – Used for Phishing  
Contact Names – Used for Phishing  
Old ID Cards – A lot of companies don't shred these  
USB Sticks – A lot get thrown out by accident  
HardDrives – Rare but sometimes contains info on prototype technology  
Pages with passwords – Happens a lot



How to Stop ---- **SHRED AND BURN EVERYTHING**

# Shoulder Surfing

The act of looking over someone's shoulder  
**!! SUPER HIGH TECH !!**

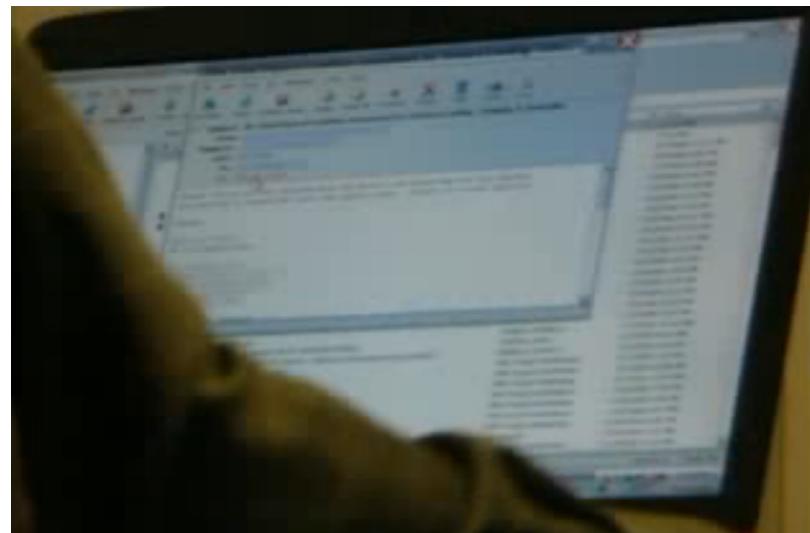
During an attack on a company doing this on a targeted individual such as a system administrator, you can get info such as

Passwords

Password structure – for making wordlists

Habits – can be used for Phishing

Check their minesweeper score



# Social Engineering

This is using peoples emotions and general need to be helpful against themselves

For example calling a call line with a baby crying saying you need to transfer onto your wife who just passed away account to pay the power bill – check motherboard for similar attack on YouTube

Kevin Mitnick the Godfather of Social Engineers

- Stole top prototype technology from bell labs by asking for it

**FREE KEVIN**



How to stop it....

Really good staff training



# NMAP

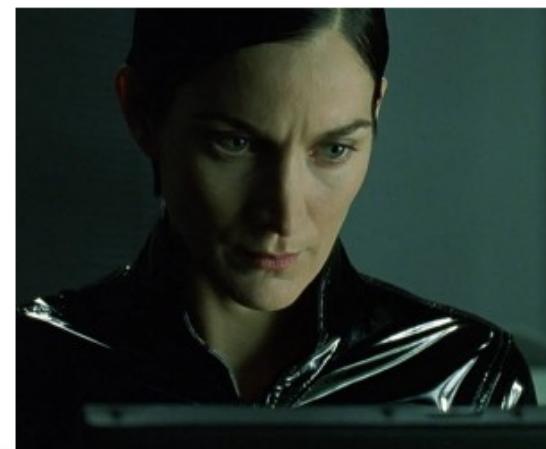


# What is Nmap?

# NMAP

Nmap is the world's leading port scanner, and a popular part of the pen tester's tool kit. Nmap is a port scanner that has the ability to scan your perimeter network devices and servers from an external perspective, i.e. outside your firewall. It allows you to scan 1 IP or a range of IP addresses.

The tool has many options, some are advanced, but for the sake of introducing y'all to it we'll stick with basics that are needed to begin using it and we'll develop from that as we need in future workshops.



```
80/tcp      open     http  
81/tcp      open     hosts-2.nse  
10  [mobile]  
11  nmap -v -SS -O 10.2.2.2  
11  
13 Starting nmap V. 2.54BETA25  
13 Insufficient responses for TCP sequencing (3). OS detection  
13 accurate  
14 Interesting ports on 10.2.2.2:  
14 (The 1539 ports scanned but not shown below are in state: cl  
51 Port      State       Service  
51 22/tcp    open        ssh  
50  
68 No exact OS matches for host  
68  
24 Nmap run completed -- 1 IP address (1 host up) scanned  
50  B Sshnuke 10.2.2.2 -rootpw="Z10H0101"  
50  Connecting to 10.2.2.2:ssh ... successful.  
Re  Attempting to exploit SSHv1 CRC32 ... successful.  
IP  Resetting root password to "Z10H0101".  
System open: Access Level <9>  
Hn  B ssh 10.2.2.2 -l root  
root@10.2.2.2's password: █  
RTF CONTROL  
ACCESS GRANTED
```

# A Quick Glossary

| Statement         | Meaning  |
|-------------------|--|
| Open Port         | Actively accepting TCP connections                 |
| Closed Port       | Can probe but No application listening on the port |
| Filtered Port     | Unavailable can not say its Open or Closed         |
| Unfiltered Port   | Available but unable to say Open or Closed         |
| Open   Filtered   | Can not say if port is open or filtered            |
| Closed   Filtered | Can not say if port is closed or filtered          |
| Passive Scanning  | Non Aggressive Scan to hide scan                   |
| Verbose           | Display all outputs to terminal                    |

Above is a list of replies you will see from nmap that may be confusing

Running the nmap command in the console should output something like this.

root@kali:~# nmap

nmap -h

man nmap

```
Nmap 7.70 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
      -iL <inputfilename>; Input from list of hosts/networks
      -iR <num hosts>; Choose random targets
      --exclude <host1[,host2][,host3],...>; Exclude hosts/networks
      --excludefile <exclude_file>; Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>; Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>; Customize TCP scan flags
  -sI <zombie host[:probeport]>; Idle scan
  -sV/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>; FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>; Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
        --exclude-ports <port ranges>; Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>; Scan <number> most common ports
  --port-ratio <ratio>; Scan ports more common than <ratio>
```

As a start, the following command will run a port scan on 192.168.1.10, the **-sV** option makes nmap determine service & version information automatically, the command looks like:

**nmap -sV 192.168.1.10**

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-20 12:54 BST
Nmap scan report for 192.168.1.10
Host is up (1.0s latency).
Not shown: 993 closed ports
PORT      STATE    SERVICE          VERSION
135/tcp    open     msrpc           Microsoft Windows RPC
139/tcp    open     netbios-ssn     Microsoft Windows netbios-ssn
445/tcp    open     microsoft-ds?
514/tcp    filtered shell
902/tcp    open     ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp    open     vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
5357/tcp   open     http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.59 seconds
```

From this simple scan, we can determine it is running a Windows Operating System and has a list of open ports, including 1 filtered. Nmap scanned 1000 ports, with the possibility of scanning ports 1 to 65535, and found 993 closed ports.

# Let's say we want to scan for individual ports

nmap -sV -p 80 192.168.1.10

-p is the option in nmap for ports,  
80 being the port number

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-20 13:29 BST
Nmap scan report for 192.168.1.10
Host is up (0.00061s latency).

PORT      STATE      SERVICE VERSION
80/tcp     filtered  http

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.59 seconds
```

## We can also say scan for open ports online

nmap -sV --open -p- 192.168.1.10

We can use the --open option in nmap to scan for open ports, notice the -p- option which tells nmap to scan all 65k+ ports and list what's open.

```
Nmap scan report for 192.168.1.10
Host is up (1.0s latency).
Not shown: 65108 closed ports, 409 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE      SERVICE      VERSION
135/tcp    open       msrpc        Microsoft Windows RPC
139/tcp    open       netbios-ssn   Microsoft Windows netbios-ssn
445/tcp    open       microsoft-ds?
902/tcp    open       ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp    open       vmware-auth   VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
5040/tcp   open       unknown
5357/tcp   open       http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10801/tcp  open       http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp  open       msrpc        Microsoft Windows RPC
49665/tcp  open       msrpc        Microsoft Windows RPC
49666/tcp  open       msrpc        Microsoft Windows RPC
49667/tcp  open       msrpc        Microsoft Windows RPC
49695/tcp  open       msrpc        Microsoft Windows RPC
49733/tcp  open       msrpc        Microsoft Windows RPC
51000/tcp  open       unknown
53213/tcp  open       tcpwrapped
54247/tcp  open       tcpwrapped
62086/tcp  open       tcpwrapped

1 service unrecognized despite returning data. If you know the service/version, please
submit a service/version update via https://nmap.org/submit/ .
```

# Lets Say there is a Firewall

To scan ports Passively as not to be caught by a possible IDS or Firewall

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-20 14:09 BST
Nmap scan report for 192.168.1.10
Host is up (1.0s latency).

PORT      STATE SERVICE VERSION
80/tcp    closed  http

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.35 seconds
```

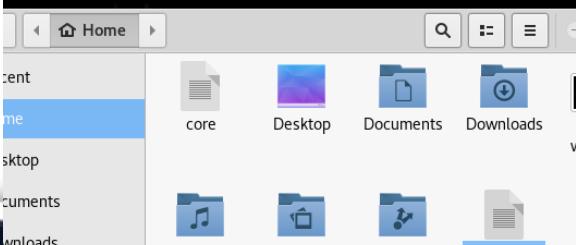
nmap -sV -Pn -p 80 192.168.1.10    -Pn treats all hosts as online

We can also save a copy of it for later reporting using -oX option

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-20 14:22 BST
Nmap scan report for 192.168.1.10
Host is up (1.0s latency).

PORT      STATE SERVICE VERSION
80/tcp    closed  http

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.34 seconds
root@OPS:~# 
```



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE nmaprun>
<?xml-stylesheet href="file:///usr/bin/../share/nmap/nmap.xsl" type="text/xsl"?>
<!-- Nmap 7.70 scan initiated Fri Apr 20 14:22:12 2018 as: nmap -sV -Pn -oX report1.txt -p 80
192.168.1.10 -->
<nmaprun scanner="nmap" args="nmap -sV -Pn -oX report1.txt -p 80 192.168.1.10" start="1524230532"
startstr="Fri Apr 20 14:22:12 2018" version="7.70" xmloutputversion="1.04">
<scaninfo type="syn" protocol="tcp" numservices="1" services="80"/>
<verbose level="0"/>
<debugging level="0"/>
<host starttime="1524230534" endtime="1524230535"><status state="up" reason="user-set"
reason_ttl="0"/>
<address addr="192.168.1.10" addrtype="ipv4"/>
</host>
</hosts>
<ports><port protocol="tcp" portid="80"><state state="closed" reason="reset" reason_ttl="128"/>
<service name="http" method="table" conf="3"/></port>
</ports>
<times srtt="1001165" rttvar="1001165" to="5005825"/>
</host>
<runstats><finished time="1524230535" timestr="Fri Apr 20 14:22:15 2018" elapsed="3.34"
summary="Nmap done at Fri Apr 20 14:22:15 2018; 1 IP address (1 host up) scanned in 3.34 seconds"
exit="success"/><hosts up="1" down="0" total="1"/>
</runstats>
</nmaprun>
```

# Nmap Scripts

Nmap has some powerful scripts that can be viewed with: **ls /usr/share/nmap/scripts**

```
acarsd-info.nse          ip-forwarding.nse
address-info.nse         ip-geolocation-geoplugin.nse
afp-brute.nse           ip-geolocation-ipinfodb.nse
afp-ls.nse               ip-geolocation-map-bing.nse
afp-path-vuln.nse       ip-geolocation-map-google.nse
afp-serverinfo.nse      ip-geolocation-map-kml.nse
afp-showmount.nse        ip-geolocation-maxmind.nse
ajp-auth.nse             ip-https-discover.nse
ajp-brute.nse            ipidseq.nse
ajp-headers.nse          ipmi-brute.nse
ajp-methods.nse          ipmi-cipher-zero.nse
ajp-request.nse          ipmi-version.nse
```

We can use these scripts for many tasks, such as vulnerability scanning or brute forcing, let's check for an old Netapi SMB vulnerability:

**nmap --script smb-vuln-ms08-067 192.168.1.10 -n**

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-20 14:38 BST
Nmap scan report for 192.168.1.10
Host is up (1.0s latency).
Not shown: 993 closed ports
PORT      STATE    SERVICE
135/tcp    open     msrpc
139/tcp    open     netbios-ssn
445/tcp    open     microsoft-ds
514/tcp    filtered shell
902/tcp    open     iss-realsecure
912/tcp    open     apex-mesh
5357/tcp   open     wsddapi

Nmap done: 1 IP address (1 host up) scanned in 8.66 seconds
```

# Most Common Nmap Options

| Option                     | Command                |
|----------------------------|------------------------|
| Service and Version        | -sV                    |
| Search by port             | -p / -p 80 / -p 80-100 |
| Search by Open / Closed    | -open / -closed        |
| Output as XML for Report   | -oX                    |
| To use a script            | --script               |
| Passive Scan               | -Pn                    |
| Verbose                    | -vv                    |
| Identify Operating System  | -o                     |
| Standard Service detection | -A                     |

There is lots more that can be found in help or on the man page.  
There is also a GUI version called Zenmap.

# NetDiscover

The Netdiscover tool does active/passive scanning by only leveraging the ARP protocol to discover live hosts on the network, this is more useful than ICMP based scanning, since pings can be blocked by firewalls and hosts, but ARP cannot be blocked. They are meant not to be blocked, but the tool simply can't do port scanning since it operates in Layer 2 of the OSI model.

## netdiscover --help

```
Netdiscover 0.3-pre-beta7 [Active/passive arp reconnaissance tool]
Written by: Jaime Penalba <jpenalbae@gmail.com>

Usage: netdiscover [-i device] [-r range | -l file | -p] [-m file] [-s time] [-n node] [-c count]
[-f] [-d] [-S] [-P] [-c]
-i device: your network device
-r range: scan a given range instead of auto scan. 192.168.6.0/24,/16,/8
-l file: scan the list of ranges contained into the given file
-p passive mode: do not send anything, only sniff
-m file: scan the list of known MACs and host names
-F filter: Customize pcap filter expression (default: "arp")
-s time: time to sleep between each arp request (milliseconds)
-n node: last ip octet used for scanning (from 2 to 253)
-c count: number of times to send each arp request (for nets with packet loss)
-f enable fastmode scan, saves a lot of time, recommended for auto
-d ignore home config files for autoscan and fast mode
-S enable sleep time suppression between each request (hardcore mode)
-P print results in a format suitable for parsing by another program
-N Do not print header. Only valid when -P is enabled.
-L in parsable output mode (-P), continue listening after the active scan is completed

If -r, -l or -p are not enabled, netdiscover will scan for common lan addresses.
```

Typing **netdiscover** without arguments will simply tell the tool to do an active ARP scan ( send ARP packets and sniff for replies ) on all private IPv4 networks ( 192.168..0.0/16, 172.16.0.0/12, 10.0.0.0/8 ) and output something like the following. It also has a passive mode similar to nmap.

### **netdiscover -p**

```
Currently scanning: (passive) | Screen View: Unique Hosts  
0 Captured ARP Req/Rep packets, from 0 hosts. Total size: 0
```

| IP | At MAC Address | Count | Len | MAC Vendor / Hostname |
|----|----------------|-------|-----|-----------------------|
| -  | -              | -     | -   | -                     |

If I let the scan continue it would list the IP addresses that were available with the given options. This type of scan will take long and we're not sure we discovered all hosts on that network, since we are only listening for ARP requests/replies.

If needed, you can do a net discover within a range by using the **-r** option.



# Netcat

Netcat (nc), also known as the TCP/IP swiss army knife, is a feature rich network utility which can be used to read and write data to network connections using TCP or UDP. But you are here to learn how to use netcat as a port scanner.

The tool acts as a quick port scanner when you're in a hurry or you are in the middle of a pentest and don't want to upload/install heavy tools like nmap as it comes pre-installed with most linux distributions, netcat has other functions useful to pen-testing we will explore in later workshops.

## netcat -h

```
[v1.10-41.1]
connect to somewhere: nc [-options] hostname port[s] [ports] ...
listen for inbound: nc -l -p port [-options] [hostname] [port]
options:
  -c shell commands      as '-e'; use /bin/sh to exec [dangerous!]
  -e filename            program to exec after connect [dangerous!]
  -b                   allow broadcasts
  -g gateway             source-routing hop point[s], up to 8
  -G num                source-routing pointer: 4, 8, 12, ...
  -h                   this cruft
  -i secs               delay interval for lines sent, ports scanned
  -k                   set keepalive option on socket
  -l                   listen mode, for inbound connects
  -n                   numeric-only IP addresses, no DNS
  -o file              hex dump of traffic
  -p port              local port number
  -r                   randomize local and remote ports
  -q secs              quit after EOF on stdin and delay of secs
  -s addr              local source address
  -T tos               set Type Of Service
  -t                   answer TELNET negotiation
  -U                   UDP mode
  -v                   verbose [use twice to be more verbose]
  -w secs              timeout for connects and final net reads
  -c                  Send CRLF as line-ending
  -z                  zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\-\data').
```

## netcat -w 1 -n 10.0.1.21 -z 1-1000 -v

```
(UNKNOWN) [192.168.1.10] 1000 (?) : Connection timed out
(UNKNOWN) [192.168.1.10] 999 (?) : Connection timed out
(UNKNOWN) [192.168.1.10] 998 (?) : Connection timed out
(UNKNOWN) [192.168.1.10] 997 (?) : Connection timed out
(UNKNOWN) [192.168.1.10] 996 (?) : Connection timed out
(UNKNOWN) [192.168.1.10] 995 (pop3s) : Connection timed out
(UNKNOWN) [192.168.1.10] 994 (?) : Connection timed out
(UNKNOWN) [192.168.1.10] 993 (imaps) : Connection timed out
(UNKNOWN) [192.168.1.10] 992 (telnets) : Connection timed out
(UNKNOWN) [192.168.1.10] 991 (?) : Connection timed out
(UNKNOWN) [192.168.1.10] 990 (ftps) : Connection timed out
(UNKNOWN) [192.168.1.10] 988 (?) : Connection timed out
```

-z : port scanning mode

-v : verbose and show port responses

-n : No hostname resolving

-w : timeout value if port doesn't respond



This is the fastest Internet port scanner. It can scan the entire Internet in under 6 minutes, transmitting 10 million packets per second.

It produces results similar to nmap, the most famous port scanner. It uses asynchronous transmission, The major difference is that it's faster than these other scanners. In addition, it's more flexible, allowing arbitrary address ranges and port ranges.

### masscan -h

```
usage:  
masscan -p80,8000-8100 10.0.0.0/8 --rate=10000  
scan some web ports on 10.x.x.x at 10kpps  
masscan --nmap  
list those options that are compatible with nmap  
masscan -p80 10.0.0.0/8 --banners -oB <filename>  
save results of scan in binary format to <filename>  
masscan --open --banners --readscan <filename> -oX <savefile>  
read binary scan results in <filename> and save them as xml in <savefile>
```

**-p [low-high][p1,p2...]** : Port range or a list of ports  
**-i <int>** : Use a specified interface, e.g. wlan0 / eth0  
**-n** : No hostname resolution.  
**-Pn** : No ping/host discovery before port scan.  
**--rate <number>**: Packet amount, default is 100/s

### masscan -p80,22,21,23,8080,10000 192.168.1.10 -i eth0 --rate 1000

```
Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2018-04-20 14:38:27 GMT  
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth  
Initiating SYN Stealth Scan  
Scanning 1 hosts [6 ports/host]  
rate: 0.00-kpps, 100.00% done, waiting -46-secs, found=0  
rate: 0.00-kpps, 100.00% done, waiting -47-secs, found=0  
^Zte: 0.00-kpps, 100.00% done, waiting -94-secs, found=0
```

# DNSrecon

What is DNS – “Domain Name Service”  
Translates domain names to IP addresses.

A lot of companies tend to run their own DNS server, attacking this can give info such as the number of servers or transfer addresses or if there are multiple IP addresses.  
DNS traffic is, 90% of the time, not logged or checked.

```
root@sanctuary:~# dnsrecon -d 10101brew.com
[*] Performing General Enumeration of Domain: 10101brew.com
[-] DNSSEC is not configured for 10101brew.com
[*] SOA dns1.registrar-servers.com 216.87.155.33
[*] NS dns4.registrar-servers.com 216.87.152.33
[*] NS dns1.registrar-servers.com 216.87.155.33
[*] NS dns3.registrar-servers.com 216.87.155.33
[*] NS dns5.registrar-servers.com 216.87.155.33
[*] NS dns2.registrar-servers.com 216.87.152.33
[*] MX eforward3.registrar-servers.com 38.101.213.206
[*] MX eforward5.registrar-servers.com 38.101.213.202
[*] MX eforward2.registrar-servers.com 209.188.18.54
[*] MX eforward1.registrar-servers.com 38.101.213.200
[*] MX eforward4.registrar-servers.com 69.160.33.74
[*] A 10101brew.com 192.64.119.111
[*] TXT 10101brew.com v=spf1 include:spf.efwd.registrar-servers.com ~all
[*] Enumerating SRV Records
[-] No SRV Records Found for 10101brew.com
[*] 0 Records Found
```

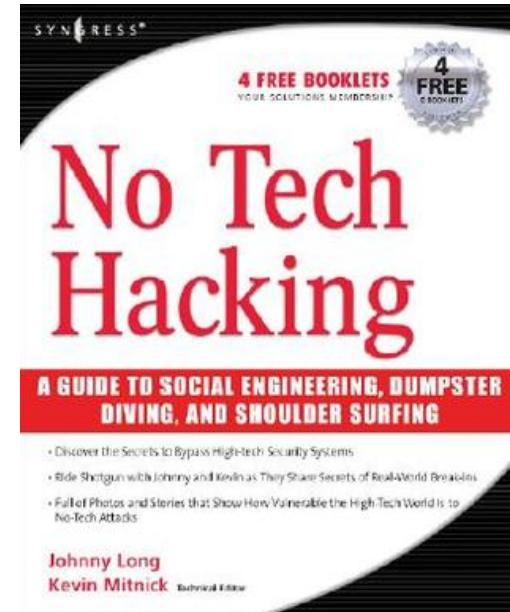
The tool to use in Kali for DNS attacks is dnsrecon.

Help command: **dnsrecon -h**

Usage: **dnsrecon -d [URL]**

# Further Reading

- No Tech Hacking by Johnny Long & Kevin Mitnick
- Anything by Kevin Mitnick
- Look into 4chan “pol” V.S. HWNDU #3
- DefCon 15 - T112 - No-Tech Hacking  
by Johnny Long



# Questions?