
HACK
LANCASTER UNIVERSITY
ETHICAL HACKING GROUP


LANCASTER UNIVERSITY
HACK
ETHICAL HACKING GROUP

Recon

Reconnaissance

LANCASTER UNIVERSITY
HACK
ETHICAL HACKING GROUP

What is Reconnaissance?

- Gathering of information on targets to allow development of attacks.
- Can be passive or active.

Passive Recon

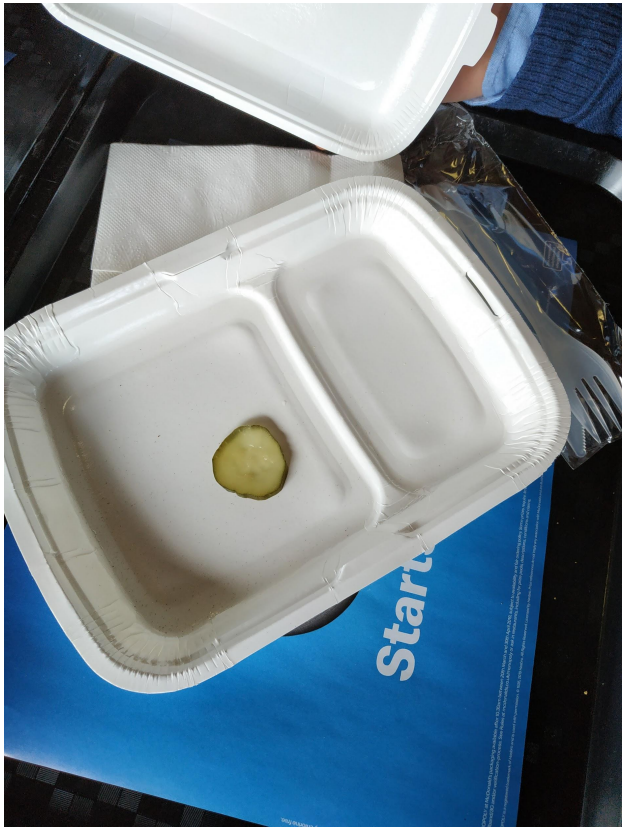
Trying to gain information on a target system without ever actually engaging directly with that system. Includes:

Finding IP's and Subdomains
Identifying people related to target
Identifying potential attack vectors
Identifying possible interesting information to access
Looking for utilized technologies

It can be scarily easy to find things...

Let’s do some passive recon on this image

By the way, this is what happens when you order a cheeseburger with everything removed but the pickle.



LANCASTER UNIVERSITY
HACK
ETHICAL HACKING GROUP

Scenario: A target has put this image on the web

So now we know the device the person is using

We can now assume what the OS is and some default software that might be running on this device.

We now have some potential attack vectors.

Camera

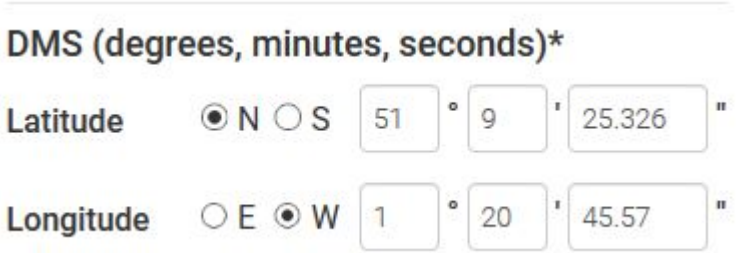
Make	Xiaomi
Model	MI MAX 3
Exposure	1/215
Aperture	1.9
Focal Length	3.9 mm
ISO Speed	200
Flash	Off, Did not fire

LANCASTER UNIVERSITY HACK ETHICAL HACKING GROUP

We also get a location...

Well, now we know exactly where this image was taken.

Most phones have locational data turned on by default.



McDonald's, RoadChef Sutton Scotney Services, Test Valley SO21 3JY, United Kingdom
Latitude: 51.157035 | **Longitude:** -1.345992

LANCASTER UNIVERSITY
HACK
ETHICAL HACKING GROUP

Oh dear...

We now know:

The target's device
The OS running on that device
The default apps on the device
Information on a target's locational behaviour
They like McDonald's
They are willing to spend 99p on a pickle slice

Active Reconnaissance

Trying to gain information on a target system while directly interacting with this system. Includes:

Port and service scanning
Actively investigating a physical site
Actively interacting with a human target
Phishing emails

A quick intro to servers, services, and IP addresses

- IP addresses: identifiers assigned to systems (hosts) that are connected to a network.
- Two main forms, IPv4 (aaa.bbb.ccc.ddd) and IPV6 (aaaa:bbbb:cccc:dddd:eeee:ffff:gggg:hhhh). IPv6 is not very common.
- Some ip addresses with certain prefixes are ‘local’:
  - 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 are intended for local networks and will not appear as routable addresses on the internet.
  - 127.0.0.0/8 intended as loopback, the current host.
- Networked hosts communicate using IP packets composed of source and destination IPs, and a message body.

Network protocols

- Built on top of IP are many layer 4 protocols, though the vast majority of internet traffic is Transmission Control Protocol and User Datagram Protocol.
- Both TCP and UDP introduce the concept of source and destination ports, numbers between 1 and 65535 that act to disambiguate packets being sent between two computers.
- UPD: Message based protocol, really just a thin wrapper over IP.
- TCP: Stream protocol, provides a way to transfer a sequence of bytes that will be reliably received by the destination in the same order as the sender sent them.

Services

- Operating system implementations of TCP and UDP support the action of ‘listening’ on a port, in which an application ‘opens’ a port on a network interface.
- Clients can then initiate connections to open ports, the listening application will then be notified of the new connection, and can begin transmitting/receiving data from it.

Scanning - Let’s have a look at Nmap

The most popular tool for network enumeration is called Nmap

This tool is packaged with most Linux distributions

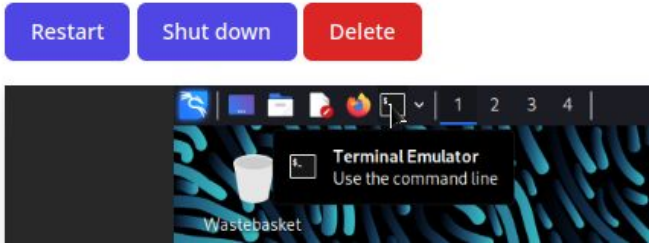
There are a number of different scan types available - we will run through these shortly

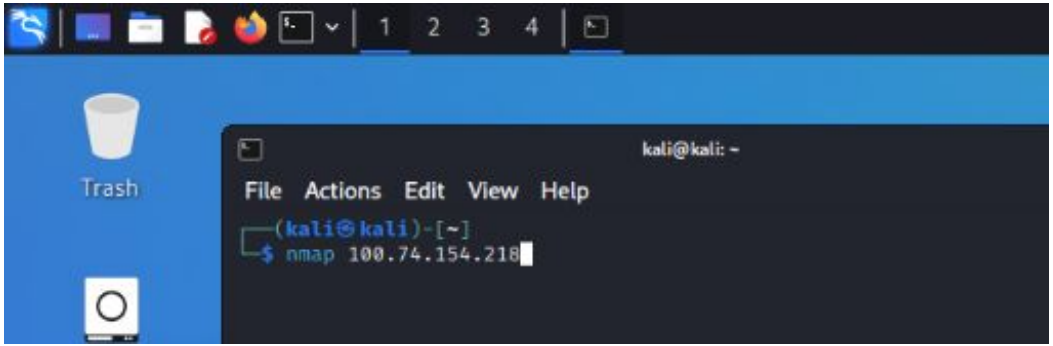
Nmap has a robust scripting engine, this allows us to use some very useful scripts to assist with recon

Read the manual, it’s very well written: https://linux.die.net/man/1/nmap

Using nmap, and a quick intro to terminals

- Nmap is a command line based program, if this is your first time using one, it's this icon on our kali VMs.
- Now type `nmap <ip>` into the terminal and hit enter.

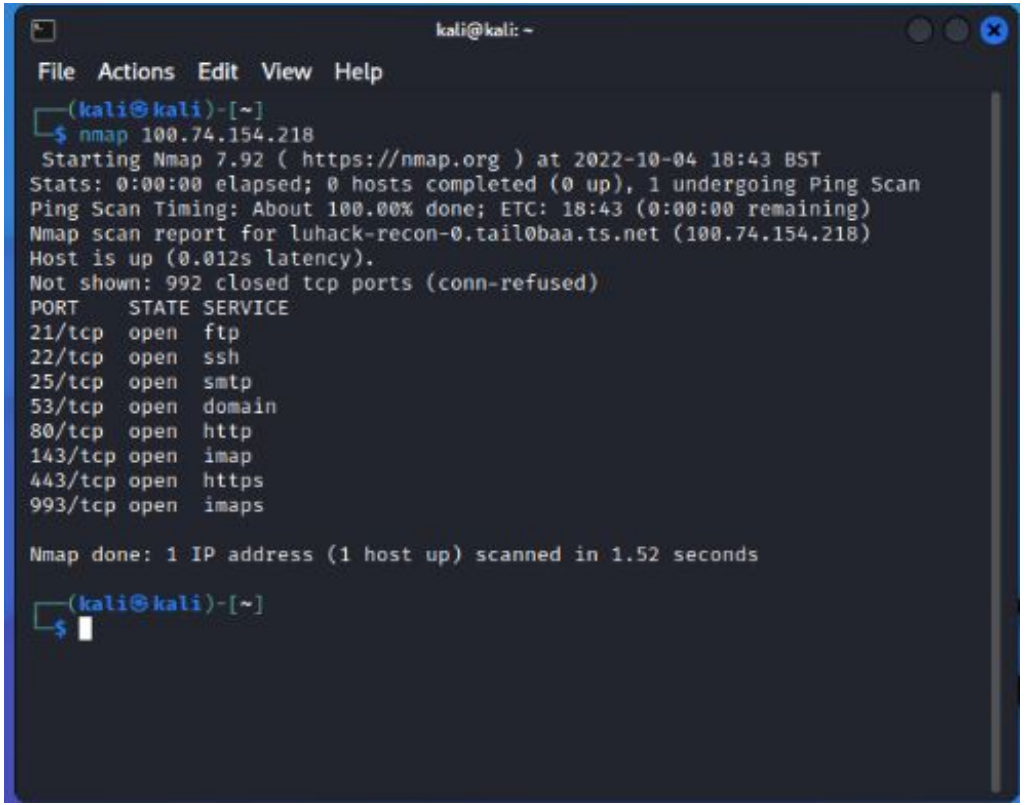




LANCASTER UNIVERSITY HACK ETHICAL HACKING GROUP

Using nmap, and a quick intro to terminals

-



LANCASTER UNIVERSITY HACK ETHICAL HACKING GROUP

Nmap Parameters

TCP SYN scans - nmap -sS ...
TCP Connect scans - nmap -sT ...
UDP scan - nmap -sU ...

Detect OS and services (very useful) - nmap -A ...
Detect services - nmap -sV ...
Target a single port - nmap -p 22 ...
Target a port range - nmap -p 1-100 ...
Scan all ports (really slow) - nmap -p- ...

Connect vs Syn

You will probably have noticed two types of TCP scan.

TCP Connect
TCP Syn

Both of these scans are very different, and you will want to use them both for different scenarios.

TCP SYN - The stealthy boi

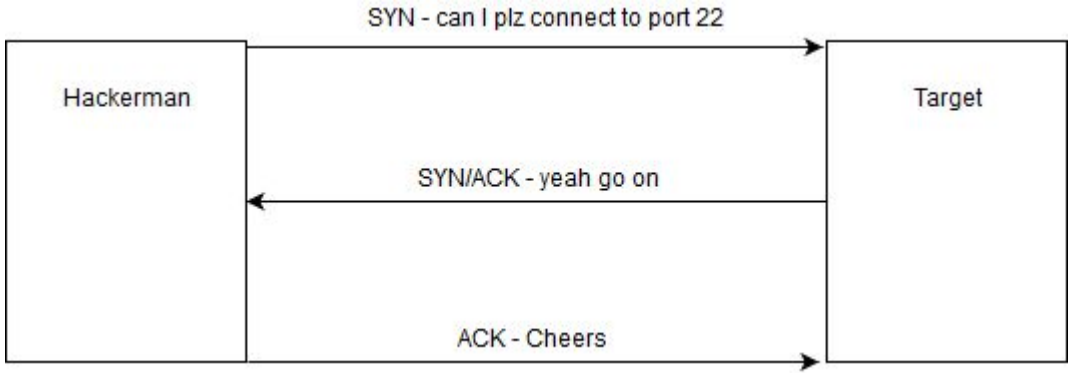
The SYN scan is the default scan Nmap will perform if no options are specified. It is fast, stealthy and often ignored by firewalls

The reason SYN is so stealthy is because it never fully completes a TCP Connection to the target machine.

To understand this, we must understand how TCP connections are handled.

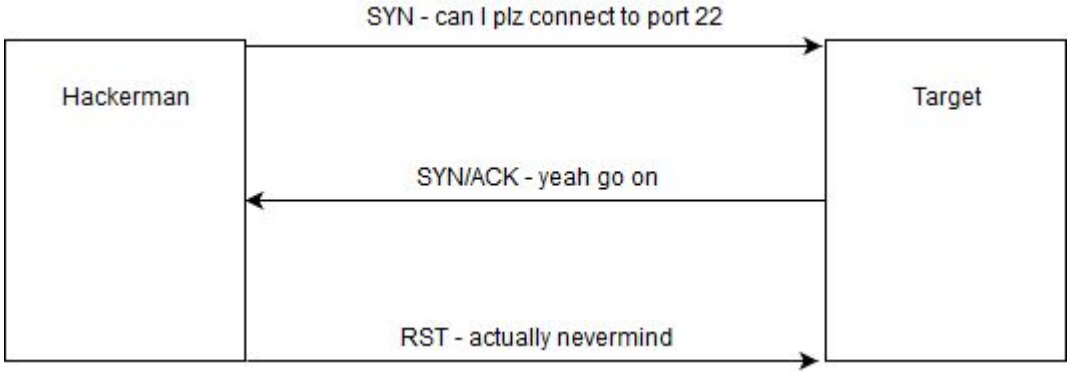
How does TCP actually work?

TCP Connections are established with a Three-Way Handshake
To make a connection, all three of these packets must be sent and received by the correct hosts.
See diagram.



TCP SYN revisited

Now we know how connections are made, let's look at SYN again.
SYN scans allow us to be stealthy as they don’t allow the Three-Way Handshake to complete, but we still get a response from the target.
To achieve this, we introduce a RST packet.



LANCASTER UNIVERSITY HACK ETHICAL HACKING GROUP

TCP Connect

As you probably have guessed, TCP Connect makes a TCP connection with the target.

We normally do not want this.

This has a high overhead performance and time wise, as making full connections takes a **long** time in comparison to sending a SYN and an RST packet.

Also, we leave a lot of evidence. Most Firewalls will log TCP connections.

Nmap OS Detection

Nmap has the ability to take an educated guess at the OS of the target machine.

Now, this one is a little less clear cut in how it works, as computers don't just hand out this information to anyone who asks.

To achieve this, Nmap sends a series of TCP and UDP packets to the host. It then analyses these responses bit by bit, and compares them to a database of known OS fingerprints.

This is why we get a percentage guess at an OS, rather than a definitive answer

Nmap Service Detection

Probably the most useful tool in the Nmap arsenal.

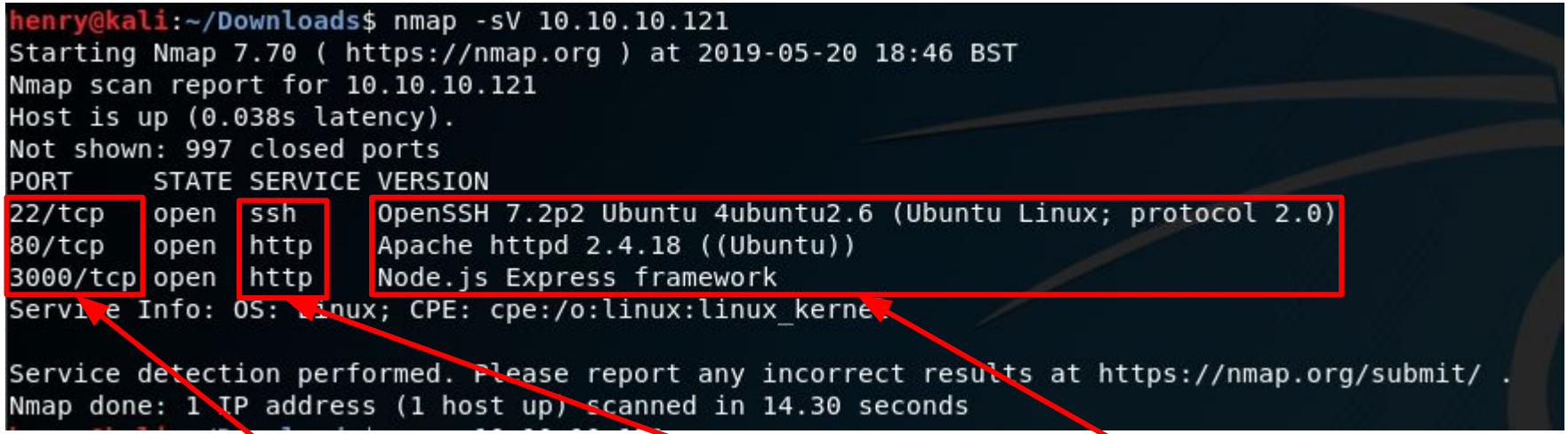
Tells us what service is running on a specific port.

Often includes details like version numbers.

Basically gives us an initial search term to start looking for footholds.

Add “exploit” at the end of a service name and version number and you’ll be off to a good start eg. “VSFTPD v2.3.4 exploit”

Interpreting Nmap Output



Port No. & Transport Protocol, Service Running, Version of Service

LANCASTER UNIVERSITY HACK ETHICAL HACKING GROUP

Useful Links

https://nmap.org/book/man.html

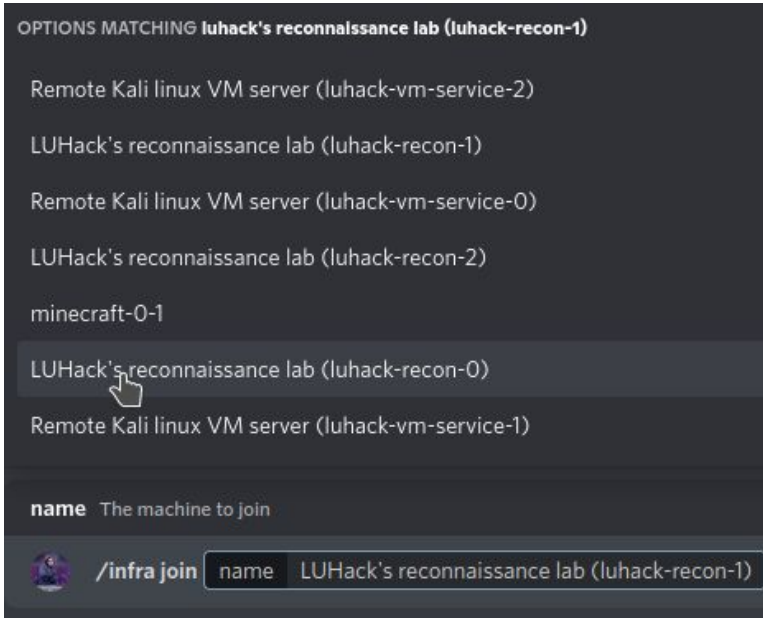
https://www.inetdaemon.com/tutorials/internet/tcp/3-way_handshake.shtml

http://metapicz.com/#landing

Practical

Today's practical is on the `luhack-recon` labs.
Use the /infra join command or click one of the buttons we'll shortly be posting in the chat.

Try and solve the challenges located at https://scc-luhack.lancs.ac.uk/challenges/tag/session1



LANCASTER UNIVERSITY HACK ETHICAL HACKING GROUP