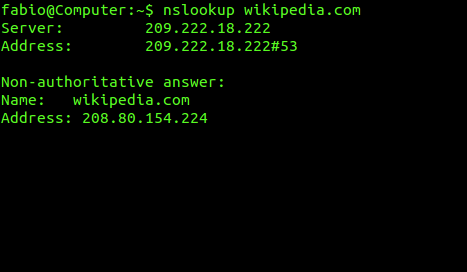
NSLOOKUP

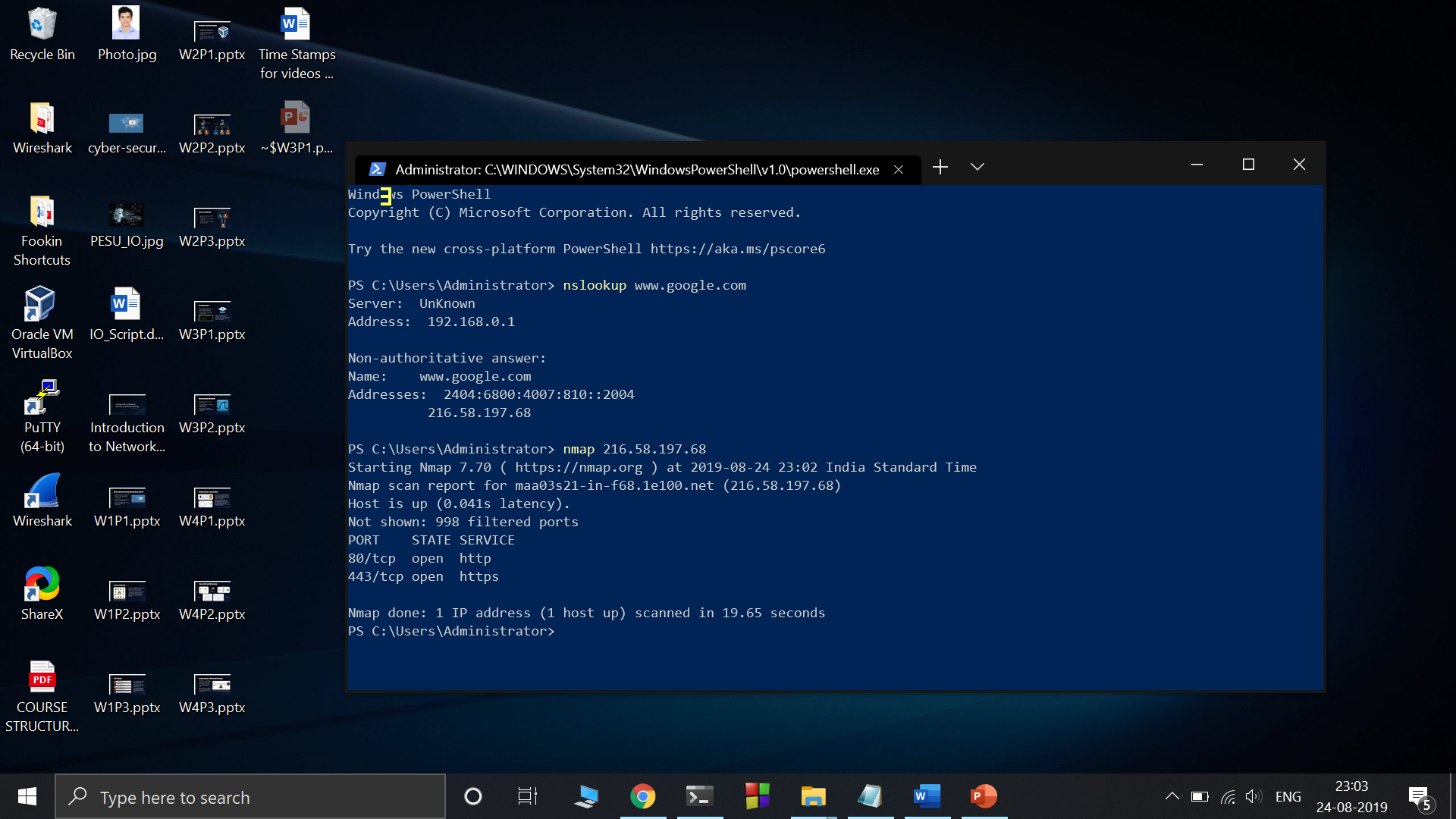
NSLOOKUP is used with the basic syntax: **nslookup [target]**



Recon with NMAP

The basic syntax for an NMAP scan is **nmap [target]**

Example: **nmap 10.0.2.5**



# Difference between UDP and TCP

UDP is a connection-less protocol that does not assure the delivery of packets at the other end. However, that does not mean it is an unreliable protocol; higher-level applications must take care to verify that data has been received at the other end. This practice has its own uses, like with live audio/video transfers, where real-time delivery is a must.

TCP is a connection-oriented protocol, which assures delivery of packets. ICMP packets are used to convey error messages, if any. The TCP three-way handshake is used to establish and reset connections, and this concept is key to understanding various NMAP scan types. In the TCP three-way handshake:

1. A “client” initiates communication with a SYN (Synchronise) packet with a randomly generated number, X.
2. The server acknowledges with a SYN-ACK (Acknowledgement), X+1 and a randomly generated number, Y.
3. The client again sends an ACK, followed by Y+1, thus completing the handshake. Now the client and server can start data transfer

# NMAP Scan Types:

## SYN SCAN [-sS]

This is the default scan and is good for most purposes. It is quieter than a TCP Connect scan, that is, it won’t show up on most simple logs. It works by sending a single TCP SYN packet to each possible port. If it gets a SYN ACK packet back, then Nmap knows there is a service running there. If it doesn’t get a response, it assumes the port is closed. The SYN scan does not complete the TCP handshake by sending an ACK back to the machine; as far as the scanee is concerned, it never sees a valid connection. However, the remote system will hold this “half socket” open until it times out from not receiving a response.

## TCP Connect [-sT]

This works much like the SYN scan, except it completes the full TCP handshake and makes a full connection. This scan is not only noisy but also puts more load on the machines being scanned and the network. However, if stealth or bandwidth is not an issue, a Connect scan is sometimes more accurate than the SYN scan. Also, if you don’t have administrator or root privileges on the Nmap machine, you won’t be able to run anything other than a Connect scan because the specially crafted packets for other scans require low-level OS access.

## Ping Sweep [-sP]

This does a simple ping of all the addresses to see which ones are answering to ICMP. If you don’t really care about what services are running and you just want to know which IP addresses are up, this is a lot faster than a full port scan. However, some machines may be configured not to respond to a ping (for example, machines running the new XP firewall) but still have services running on them, so a ping sweep is not as accurate as a full port scan.

## UDP Scan [-sU]

This scan checks to see if there are any UDP ports listening. Since UDP does not respond with a positive acknowledgment like TCP and only responds to an incoming UDP packet when the port is closed, this type of scan can sometimes show false positives. However, it can also reveal Trojan horses running on high UDP ports and hidden RPC services. It may be quite slow, since some machines intentionally slow down responses to this kind of traffic to avoid being overwhelmed. Machines running Windows OS, however, do not implement this slowdown feature, so you should be able to use UDP to scan Windows hosts normally.

## FIN Scan [-sF]

This is a stealthy scan, like the SYN scan, but sends a TCP FIN packet instead. Most but not all computers will send a RST packet back if they get this input, so the FIN scan can show false positives and negatives, but it may get under the radar of some IDS programs and other countermeasures.

## NULL Scan [-sN]

Another very stealthy scan that sets all the TCP header flags to off or null. This is not normally a valid packet and some hosts will not know what to do with this. Windows operating systems are in this group, and scanning them with NULL scans will produce unreliable results. However, for non-Windows servers protected by a firewall, this can be a way to get through.

## XMAS Scan [-sX]

Similar to the NULL scan except all the flags in the TCP header are set to on. Windows machines won’t respond to this due to the way their TCP stack is implemented. Xmas scans derive their name from the set of flags that are turned on within a packet. These scans are designed to manipulate the PSH, URG and FIN flags of the TCP header.

## RPC Scan [-sR]

This special type of scan looks for machines answering to RPC (Remote Procedure Call) services. RPC, which allows remote commands to be run on the machine under certain conditions, can be a dangerous service. Since RPC services can run on many different ports, it is hard to tell from a normal scan which ones might be running RPC. This scan will probe the ports found open on a machine with commands to show the program name and version if RPC is running. It’s not a bad idea to run one of these scans every so often just to find out if and where you have these services running.

## Windows Scan [-sW]

This scan relies on an anomaly in the responses to ACK packets in some operating systems to reveal ports that are supposed to be filtered. Operating systems that are known to be vulnerable to this kind of scan include some versions of AIX, Amiga, BeOS, BSDI, Cray, DG/UX, Digital UNIX, FreeBSD, HP/UX, IRIX, MacOS, NetBSD, OpenBSD, OpenStep, OpenVMS, OS/2, QNX, Rhapsody, SunOS 4.X, Tru64 UNIX, Ultrix, VAX, and VxWorks.

## Idle Scan [-sI]

This type of scan is a new feature for Nmap version 3.0. It is a super stealthy method whereby the scan packets are bounced off an external host. You don’t need to have control over the other host but it does have to setup and meet certain requirements. You must input the IP address of our “zombie” host and what port number to use.It is one of the more controversial options in Nmap since it really only has a use for malicious attacks.

# NMAP CHEAT SHEET

* **nmap -sP 10.0.0.0/24**

Ping scans the network, listing machines that respond to ping.

* **nmap -p 1–65535 -sV -sS -T4 [target]**

Full TCP port scan using with service version detection — usually my first scan, I find T4 more accurate than T5 and still “pretty quick”.

* **nmap -v -sS -A -T4 [target]**

Prints verbose output, runs stealth syn scan, T4 timing, OS and version detection + traceroute and scripts against target services.

* **nmap -v -sS -A -T5 [target]**

Prints verbose output, runs stealth syn scan, T5 timing, OS and version detection + traceroute and scripts against target services.

* **nmap -v -sV -O -sS -T5 [target]**

Prints verbose output, runs stealth syn scan, T5 timing, OS and version detection.

* **nmap -v -p 1–65535 -sV -O -sS -T4 [target]**

Prints verbose output, runs stealth syn scan, T4 timing, OS and version detection + full port range scan.

* **nmap -v -p 1–65535 -sV -O -sS -T5 [target]**

Prints verbose output, runs stealth syn scan, T5 timing, OS and version detection + full port range scan.

* **nmap -iL ip-addresses.txt**

Scans a list of IP addresses from the file ip-addresses.txt, you can add options before / after.