# Lab 7 Transport Layer: Well Known Ports and Servers

To access common services, the client needs to know that the server is listening on a certain port number. In our lab with hubs and switches we used a ncat listener (server) and client to chat between computers; the person running the server had to tell the client which port to connect to. For common services, the servers listen on “well known” port numbers so that the clients do not have to ask for the port number. Web HTTP servers usually listen on TCP port 80, HTTPS servers on TCP port 443, Microsoft file sharing on TCP port 445, etc. Well known ports fall in the range 0 to 1023. You can find a list of well known ports here: <https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers>.

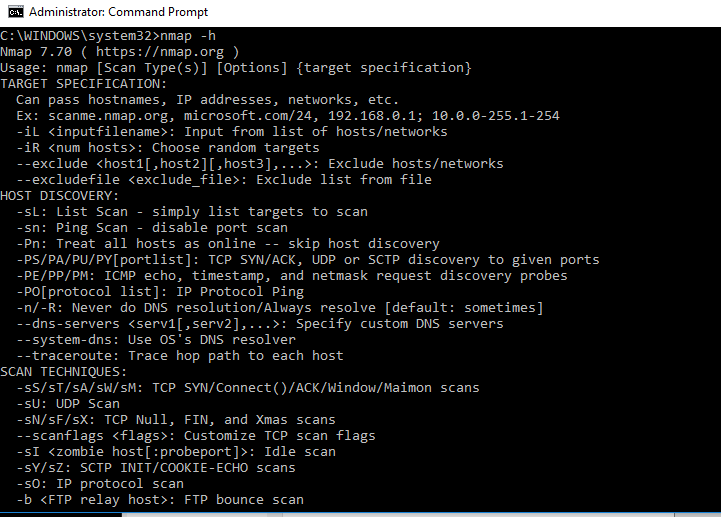
The transport layer allows a computer to associate software processes with port numbers so that the computer knows which process should receive incoming data. The combination of an IP address and a port number is called a socket and should be unique. For example, if 192.168.1.1 is running a web server on the well-known port 80, the complete address is 192.168.1.1:80.

## <Warning!!> This lab will use nmap to scan for listening ports on a specified classroom server, but nmap can also be used to scan an entire network. You have permission to scan the specified server, and nothing else. Attackers will often scan a network in search of targets, so network administrators consider network scans to be hostile acts. Also, it is possible that a scan could cause a server to crash; even if the server crashed because it was poorly configured or written, the crash will be your fault. Do not scan any network unless you have written permission from the network owner. </Warning!!>

Note: This warning \*mostly\* applies to scanning done within an organization, such as your school. Computers directly connected to the Internet are being scanned continuously by attackers and researchers. You can \*usually\* run small scans on the Internet without getting into trouble, but you should be careful and use common sense.

# A Brief Look at Nmap

Zenmap is just a GUI frontend for nmap, so it is worthwhile to look at nmap. Open a command prompt and type nmap -h. You will see that nmap is a complicated application with many options. You should be able to understand many of the options based on what you’ve learned in networking. Scan through the options.

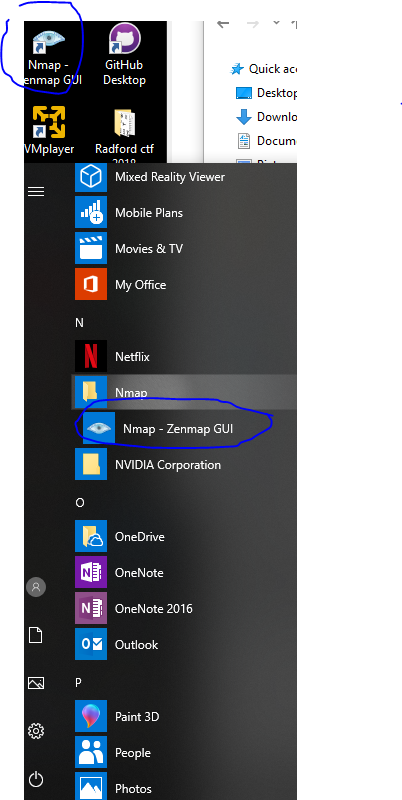


# Port Scanning with Zenmap

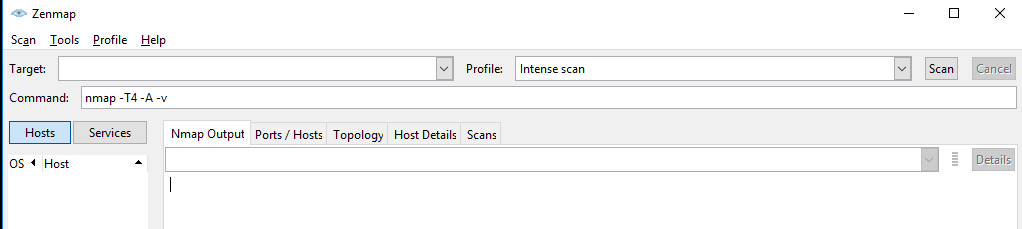
Zenmap is the GUI frontend for the nmap scanner, which normally uses a command line interface (CLI). We will scan one IP address looking for open, or listening, ports. Zenmap will send test traffic to the IP address on many ports and label the ports according to the response it receives. If the TCP port is “closed” (not listening) the host usually responds with a TCP Reset (RST), meaning “Go away!” If there is a firewall blocking the traffic (it may be the firewall on the host) there will be no response and Zenmap will label the port “filtered.” If the TCP port is listening, the IP address will respond with the TCP handshake (SYN/ACK) and Zenmap will label the port as “open.” Sending test packets to multiple ports on an IP address is known as a port scan.

In the Intense Scan, nmap will send specially crafted packets to the IP address in an attempt to determine the operating system (OS) and service versions. It will also capture the responses that traffic to specific port numbers generate and use them to determine the service that is running on that port.

Scanning using the default scan settings is very noisy, in that it generates a lot of traffic. If the network has good security monitoring installed, noisy scans should be easily detected. Judicious and patient use of nmap can be more difficult to detect. We will use the noisy (sloppy) options in this lab, but just know that scanning can be done much more carefully.

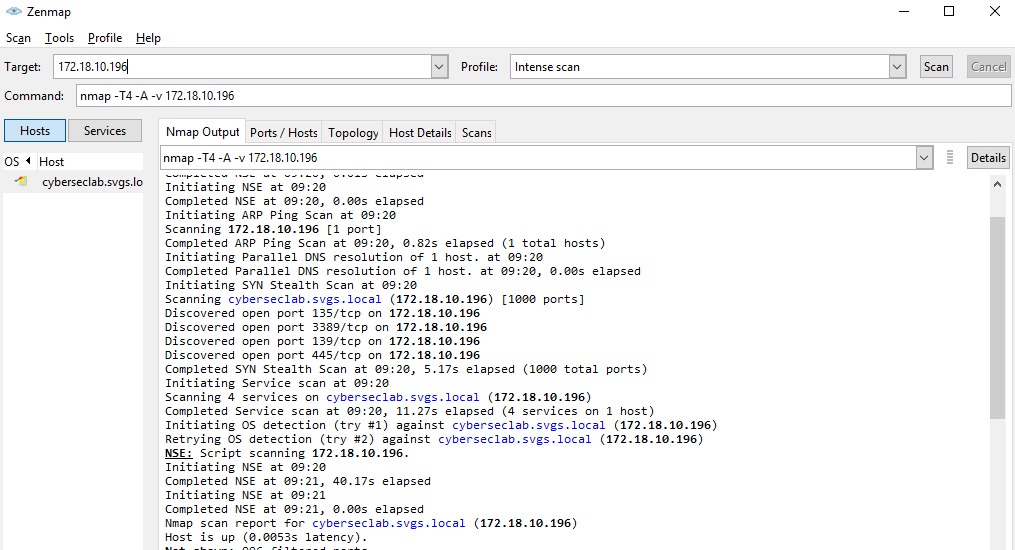
Zenmap should already be installed on your computer, so you just need to open it. Zenmap is found under Nmap in your application menu, or there may be a Zenmap icon on your desktop. 

The Zenmap window has a field for Target, which is the IP address you wish to scan. Enter the IP address that the instructor gives you into this block. The Profile field allows you to select the type of scan.



The Intense Scan throws most of what nmap has at the target. Besides looking for open ports, it tries to identify the Operating System of the target and identify any services it finds on open ports. It also runs some nmap scripts to further identify the target. It only scans the 1,000 most common TCP ports by default, however. You can scan all ports (0 to 65,535) but that takes a long time.

The Command field shows the nmap command that will be executed. Select different profiles, and you will see the Command change accordingly.

Run an Intense scan on the IP address the instructor gives you. The address may be different than the example shown below, so don’t use that by mistake.  


# Hand in

1. What OS does nmap think the target is running?
2. Make a list of the open ports and services. Look up three of them using your favorite search engine. Explain what they are used for and if they are secure services (a couple of the services on the target are obviously insecure.)
3. Some services use simple text-based protocols that can be easily manipulated. Use ncat to connect to open ports on the target until you find one that replies with text or responds to text entries from you. If you connect to a service that does not appear to respond, it does not mean the connection failed; more likely, the service is waiting for specific data (often binary) from you. Paste a screenshot of your result. The syntax to use ncat is the same as we used in the hub and switch lab: ncat [IP address] [port number]
4. If there is time, use the Profile that scans all TCP ports and rescan the target. Do you find anything interesting?