

**Lab 7: *Network Security***

Please make sure you take screenshots for any part that we asked you to "write up the results". I want to match your answers with what you got from scanning.

**Overview:**

In this lab we’ll looking at foot-printing, scanning and enumeration. We will be scanning one machine, to discover what services it is running, then the IFS Lab to discover what machines and the services they are running. To do this will be using a tool called ***Nmap***, the “world’s most popular network security scanner”. Finally, you will look at the traffic generated by Nmap to get a sense of how much network communication is involved in a scan.

## Read and Study

**The Network Security Test Lab, Chapter 4:  
 Detecting Live Systems and Analyzing Results**

**Warning:**

**Do not use Nmap to scan ANY network unless you have explicit permission to scan that network.**

**If you ignore this warning, you might become familiar with the operations of the** [**ITCU of the RCMP**](http://www.rcmp-grc.gc.ca/on/prog-serv/support-soutien/itcu-gict-eng.htm)**, because it could be considered "unauthorized access to a computer system", and some scans can lead to a** [**DoS**](http://www.cert.org/tech_tips/denial_of_service.html) **on poorly configured systems.** You might be able to argue against this successfully, but it might require the services of a lawyer, and your equipment might be confiscated while the argument takes place. Even without police involvement, you might end up losing the services of your ISP.  
  
**Consider yourself warned.  
  
You have permission to scan:**

* **The server at IP Address 172.16.11.65 in the IFS lab**
* **The internal network in the IFS lab labeled “SCAN” on the white board.**

**You do not have permission to scan any other networks at Seneca.**

**Objective:**

1. Demonstrate how to foot print a company.
2. Scanning of a single server.
3. Scanning and enumeration a network.
4. Understanding the cost of a scan.

NOTE: The sections highlighted in:

* Green: does not require IFS Lab or VM Workstation Pro & Window’s 7
* Yellow: does require VM Workstation Pro & Window’s 7
* Red: does require the IFS Lab

**The Lab Activities**

### Part 1: Foot-printing

Foot-printing involves determining the following:

* The scope of the footprint – an organization, a subnet or a machine.
* Searching public web sites and databases for organization and network information that may be useful to plan an attack against known vulnerabilities.
* Network reconnaissance—determining network topology, access points and DNS record information.

**Foot-Printing Seneca:**

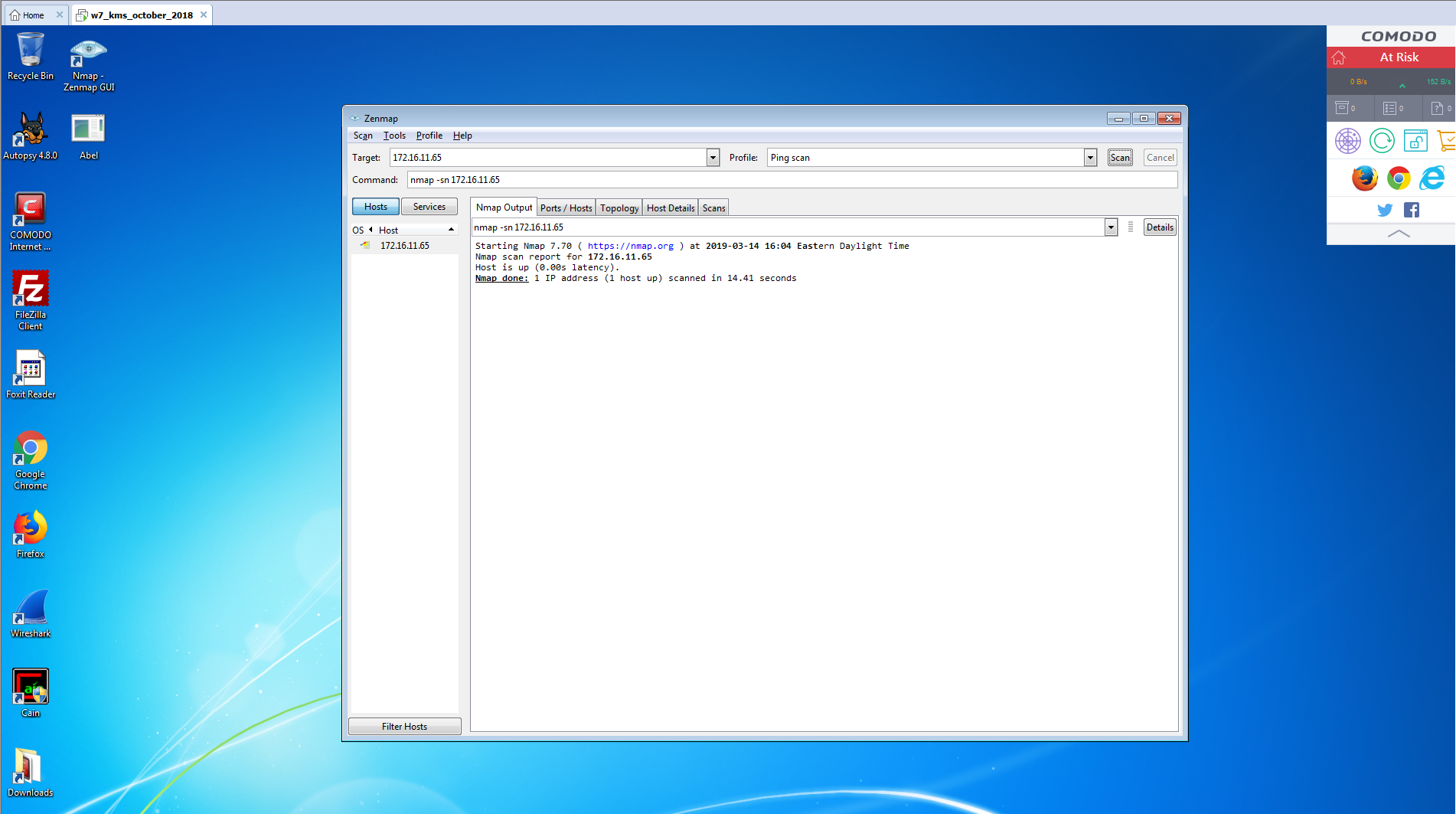
1. In Foot-Printing is an organization that deals with a systems search to logging to the Seneca’s website page. In the past, many other programs were a major loophole in the patches that were created in these sites, so it contained more information and less potential information for the amount of students.

2. The search bar, was a basic information system for seneca. As it was used for simple things like phone numbers, addresses, domain ids, registrations numbers etc.

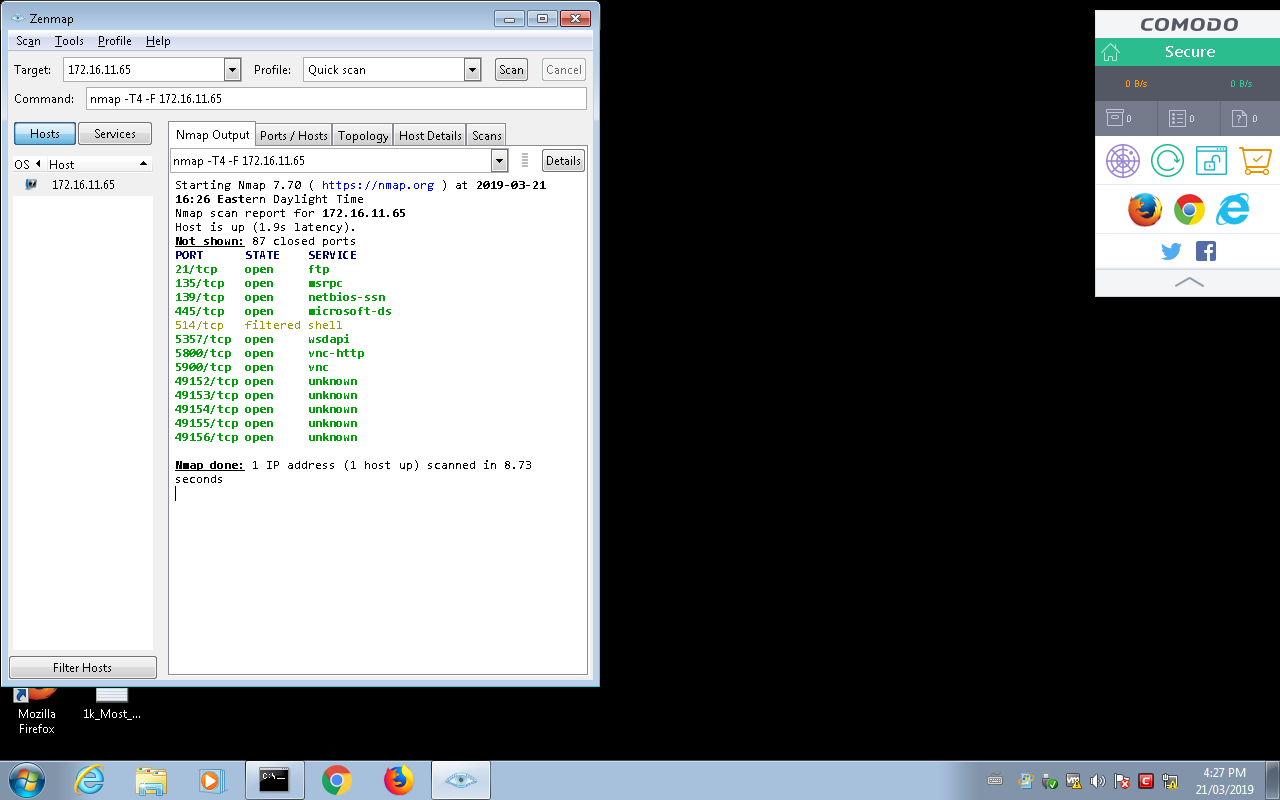
**NMAP and the 172.16.11.65 server:**

1. Ping Scan

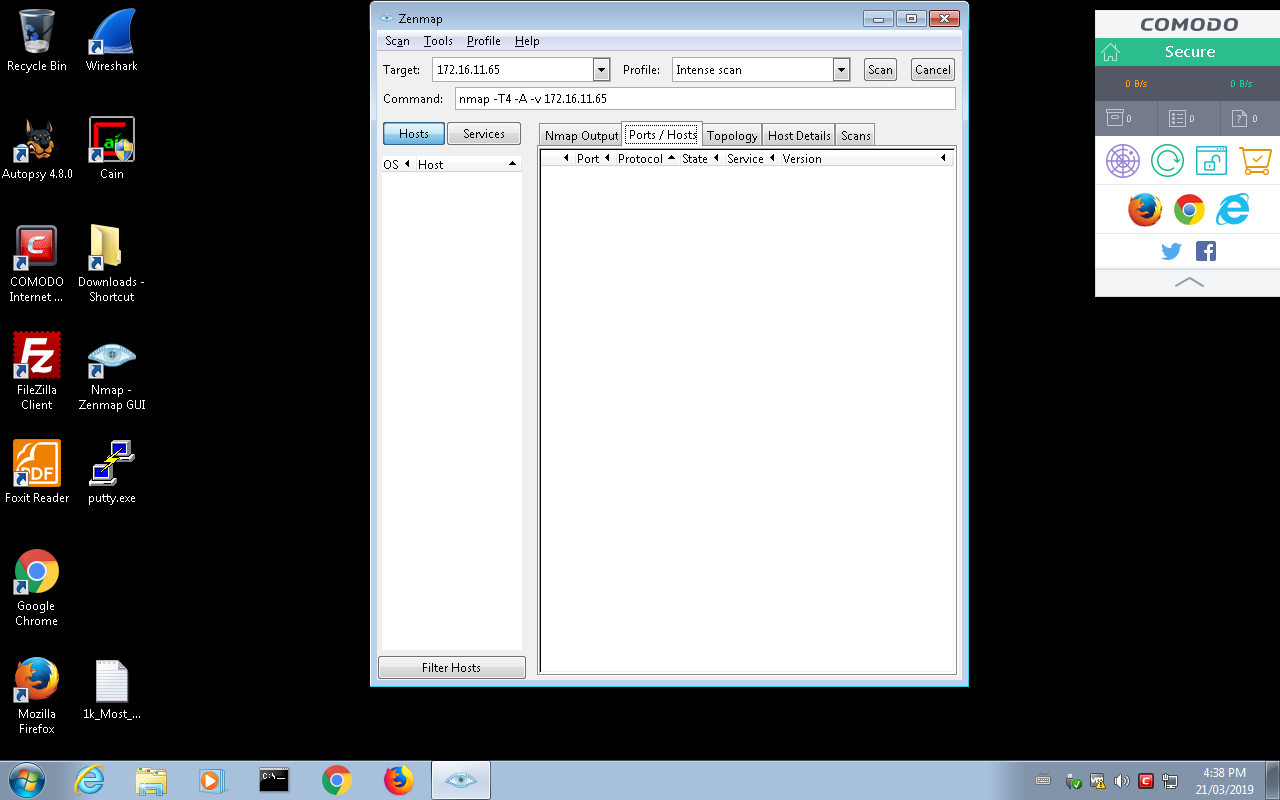
Quick Scan, This scan shows all ports and there states compared to ping scan.



1. Intense Scan



4. The intense scan Ports/Hosts shows all the open and filtered ports and what services they are. The regular nmap output shows more detail about each port with all IPs, traceroutes, etc.



### Part 3: Scanning and Enumeration of a Network

If we are to learn about what is happening on our network, rather than just one computer, we should be familiar with the basic protocols, and service identification.

You should understand the significance of port numbers, so you should know which port numbers are associated with these commonly used services:

* HTTP & HTTPS
* DNS
* DHCP (bootp)
* SSH
* TELNET
* FTP
* SMTP
* NetBIOS
* Microsoft-DS

Look up any port numbers that show up on your Nmap scans, this will give you an idea of what they do.

Before you use Nmap, read and understand [the nmap man page](http://nmap.org/book/man.html). If you do not take the time to understand the output of Nmap, you will end up wasting lots of time.

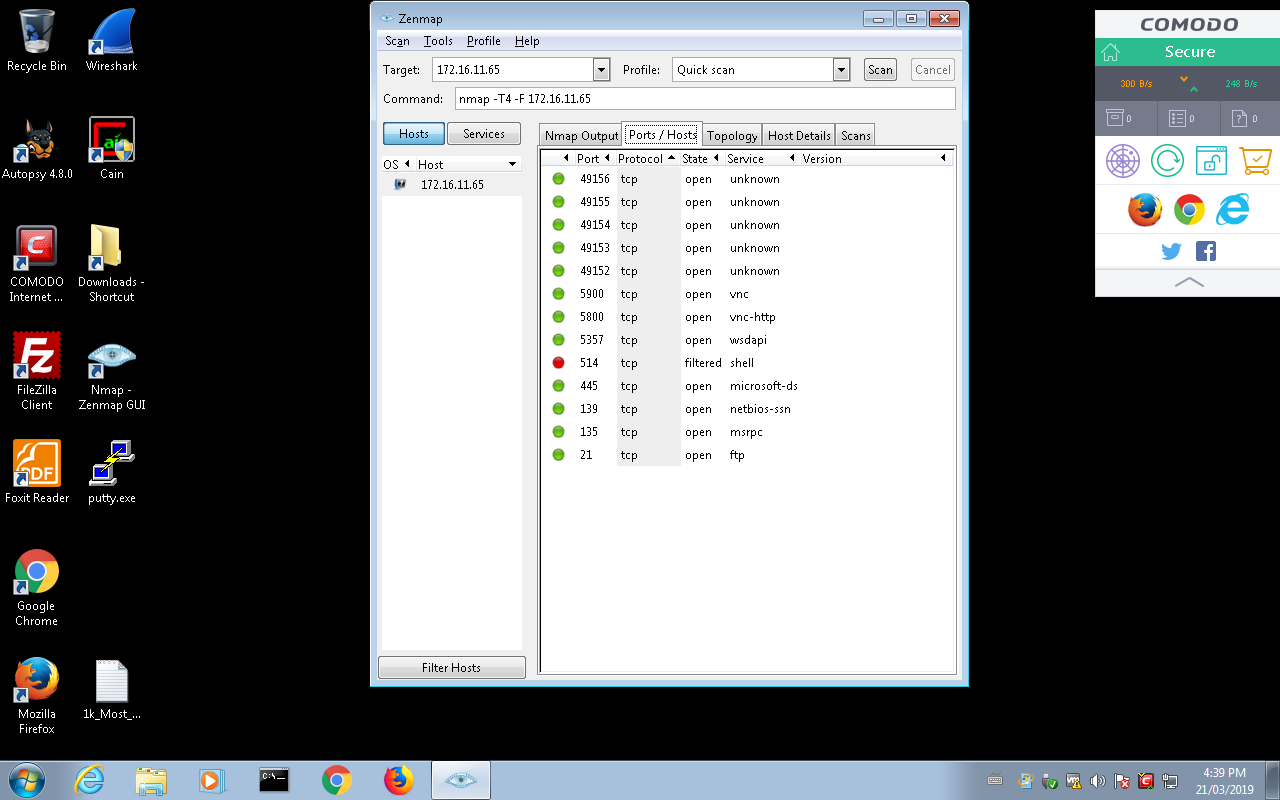
* [*A Short History of Nmap*](file:///E:\SEC625\nmap)
* [*Zenmap*](https://nmap.org/zenmap/)
* [*Zenmap User’s Guide*](https://nmap.org/book/zenmap.html)
* [*30 Useful Nmap Commands*](http://www.cyberciti.biz/networking/nmap-command-examples-tutorials/)

Using Nmap, scan the ***IFS Lab network given on IFS Lab website under SEC625*** (i.e. you need to be on the IFS Lab network to do this) and discover hosts that are listening. You need a quick and simple scan to discover hosts, and more complex scans to find out information of each host discovered.

Look over the resources mentioned at the start of the lab. Decide on some other interesting scans to try on the servers you have discovered.

***Questions:***

1. There were 625 services on 42 hosts, on the network 172.16.11.0/26



1. 27 hosts are running on this service. The IPs are all start with (172.16.11.x)

MySQL:11 hosts are running on this service.

FTP**:** 21 hosts are running on this service. The IPs are all start with (172.16.11.x)

3. I got this information by clicking the “Services” button underneath “Command”

4.Operating systems on network:

* 28 Windows
* 4 Linux
* 1 MAC OS

### Part 4: Determining the cost of a scan

Doing a scan of a network and host on the network might seem the obvious and easiest thing to do. Such scans generate traffic. Let’s capture that traffic and see how much there is.

NB:

* There is only general guidance given for this part of the lab. You are expected to do research etc. to find out any information you don’t know.
* You need to get Kali VM from the IFS Lab server. Once you have it, you do not require the IFS Lab for the remainder of this part of the exercise.

**Steps**

1. Install Kali as a VM on you VM Workstation Pro (Kali Linux is available from the IFS Lab website).
2. Start Wireshark on your *Window’s* 7 VM, and begin Capture
3. Using the **command-line** on Kali, use Nmap to do *an intense scan* of your *Window’s* 7 VM
4. Stop your Wireshark capture on *Window’s* 7 VM once the Nmap scan is complete
5. Review your Wireshark capture to see the volume of traffic an ‘uncontrolled’ scan can generate.
6. Based on how things have been done in previous labs. Under a heading “**Scan Costs”** in your report, **create screenshots** and insert them under the appropriate sub-headings that show the following:

