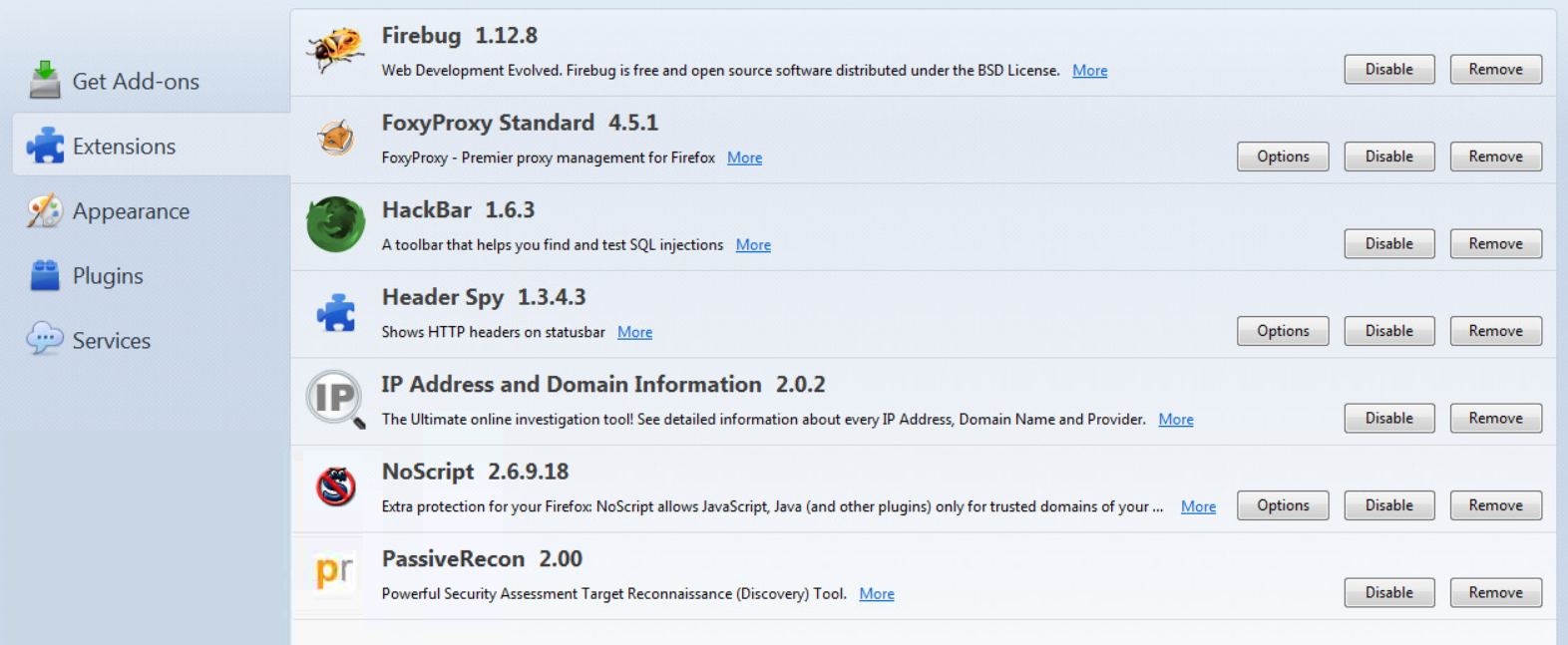
# Documentation

**Information Gathering**

**3.1 Passive Reconnaissance**

**Tools/Add-ons**



**I clicked on “More” link for each Firefox extension to see how it might be useful during a Pen Test but didn’t find showIP 2.0. And couldn’t install it from online either because of no internet connections**

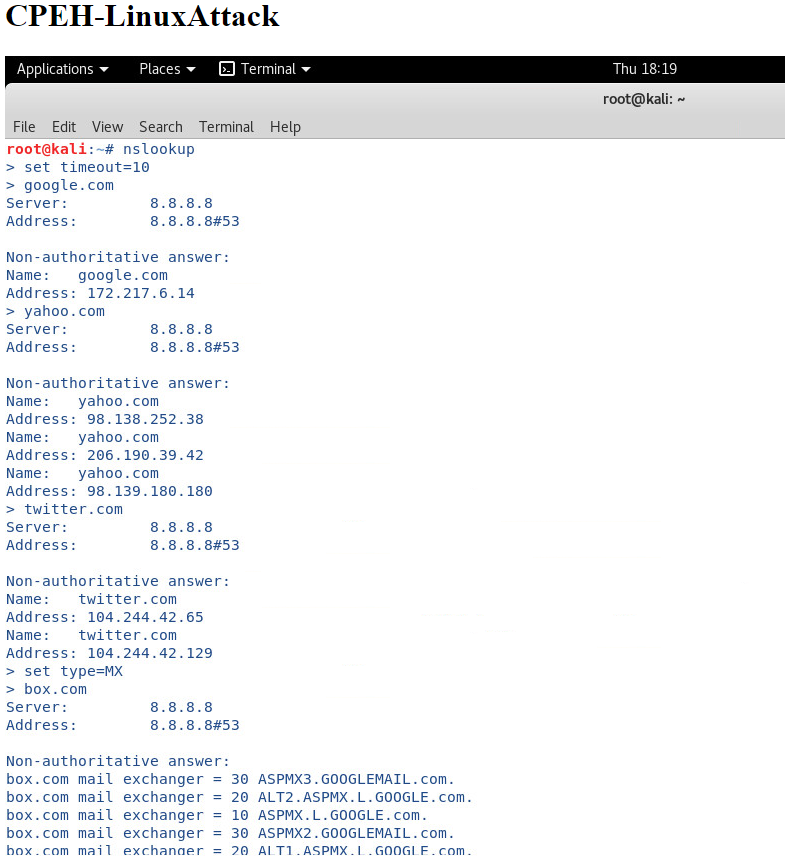
**At some point after looking at the add-ons, I have disable the Hackbar toolbar.**

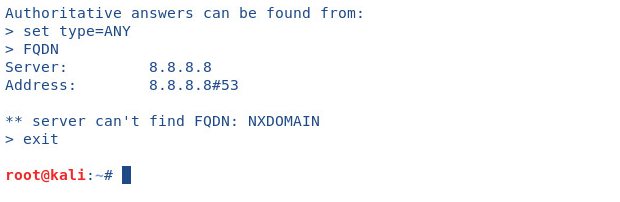


**2. From *my own computer,* I visited to this URL** <http://online-­domain-­tools.com> **to see some of the fee tools available to gather information on my targets.**



**3. Using Nslookup**





**3.2 Google Queries**

**1. Gather information from Aegon**

**I.** Members of the Executive Board of AEGON N.V. and AEGON USA

**Alexander R. Wynaendts**

CEO and Chairman of the Executive and Management Board

Alex joined Aegon in 1997 and was appointed as a member of Aegon´s Executive Board in 2003

**Matthew J. Rider**

CFO and member of the Executive Board

Was appointed on May 19, 2017.

[**https://www.aegon.com/en/Home/Investors/News-releases/2016/aegon-to-appoint-matthew-rider-as-cfo/**](https://www.aegon.com/en/Home/Investors/News-releases/2016/aegon-to-appoint-matthew-rider-as-cfo/)

**II.** Educational Background of the CEO

* **Ecole Superieure D'electricite** Graduated, 1984
* **Paris - Sorbonne University** Graduated, Economics, 1983

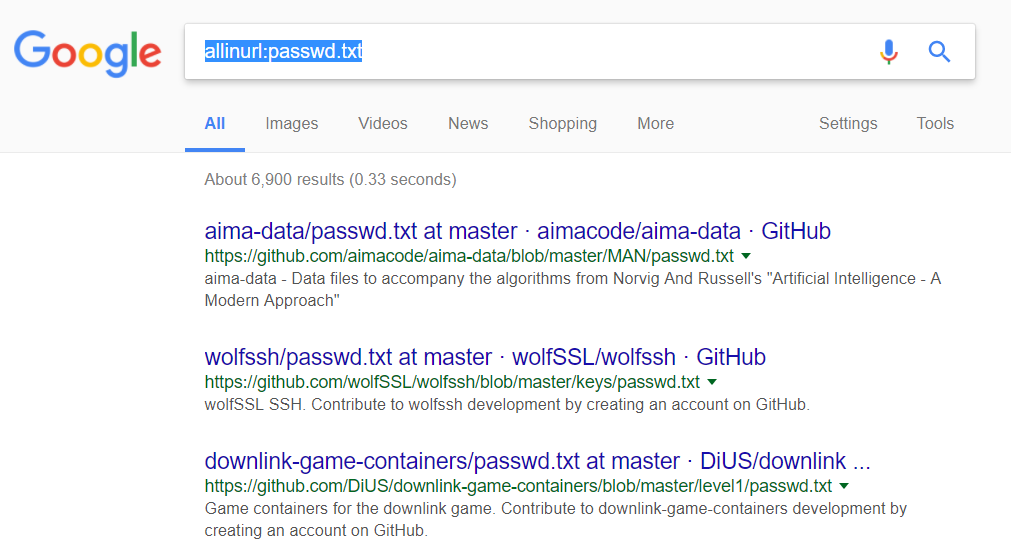
**III.** Find out the office location, telephone and name of the CEO.

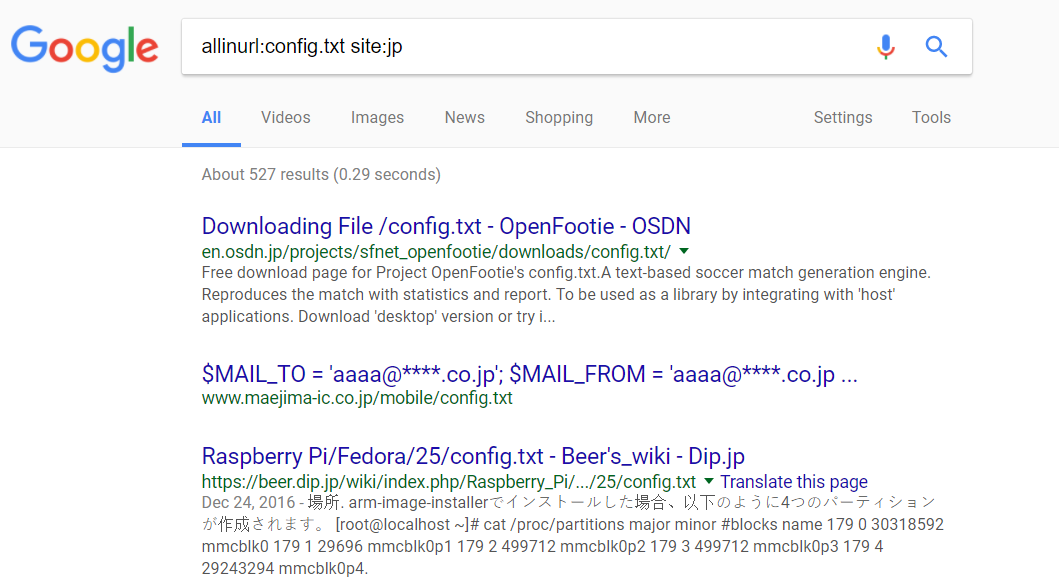
Alexander R. Wynaendts, CEO



**2. Practice utilizing the following Google Queries (screenshots are shown below)**

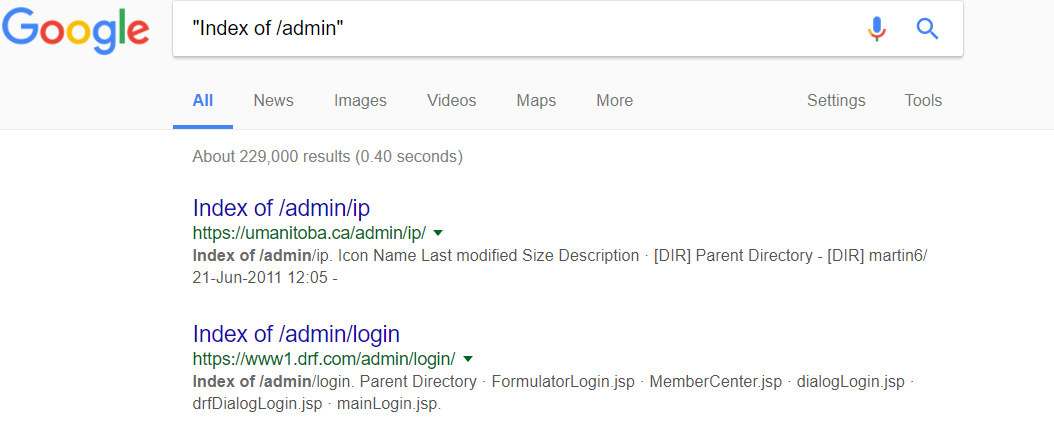


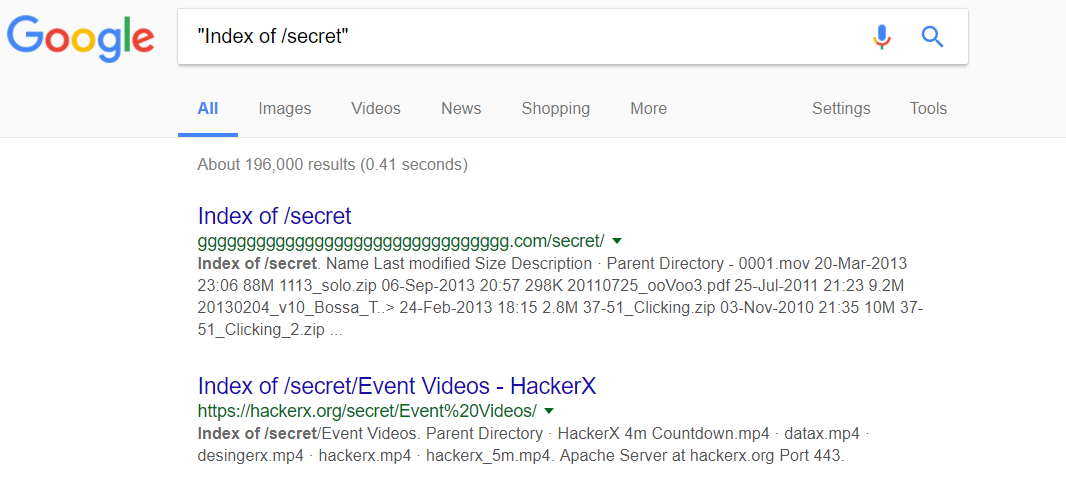


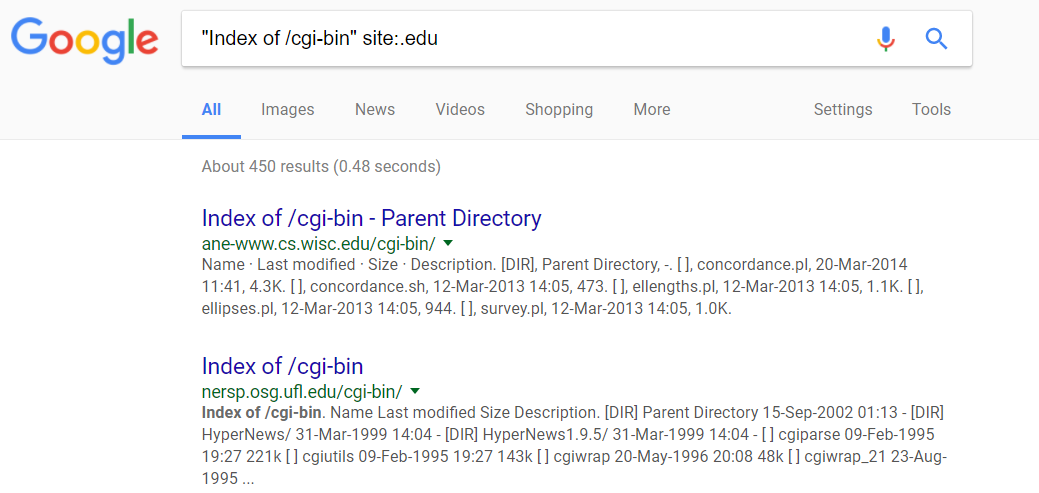


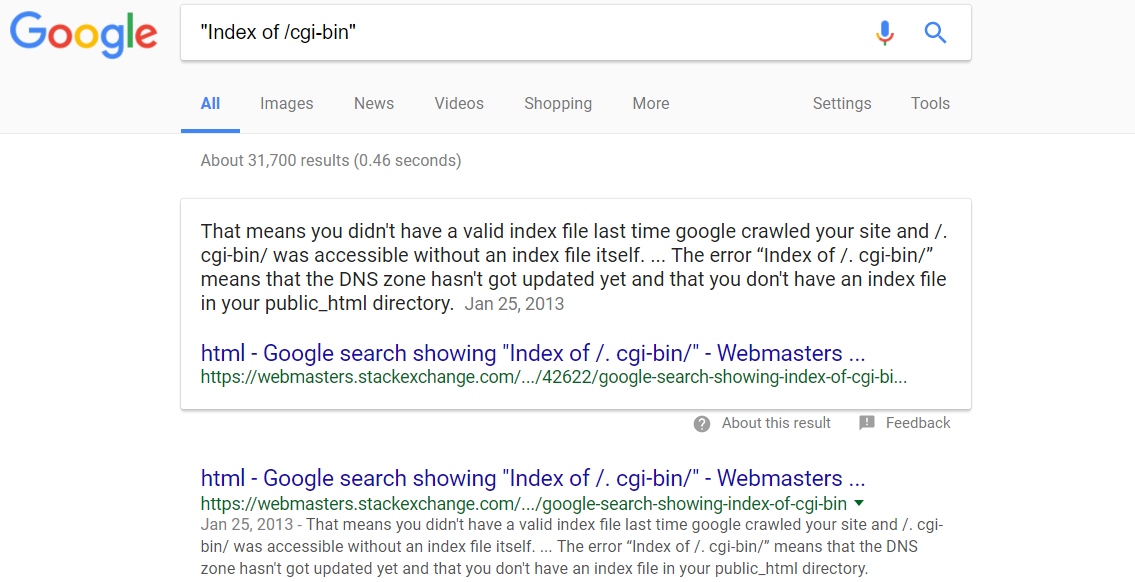


**3. Practicing index browsing enabled directories (Screenshots are below)**

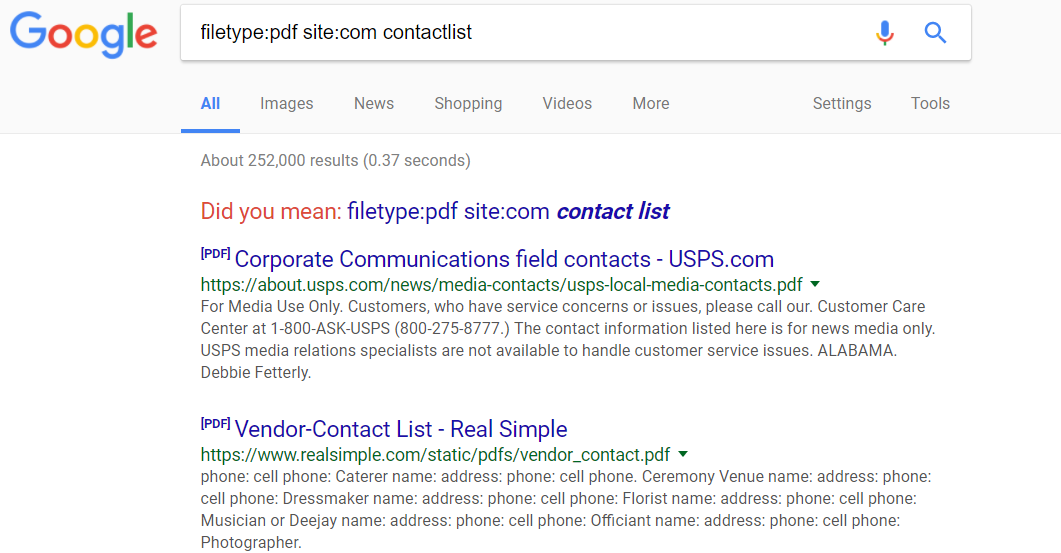


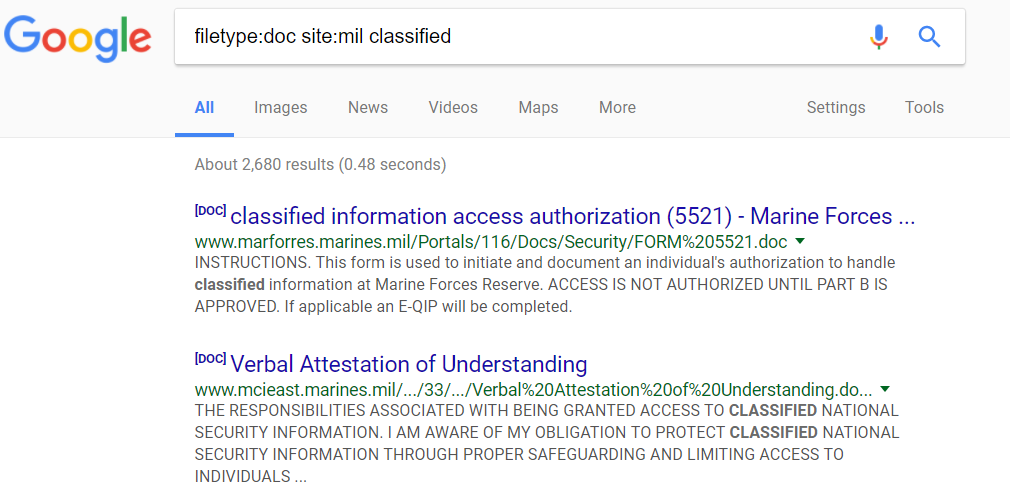






**4. Searching for particular file types**

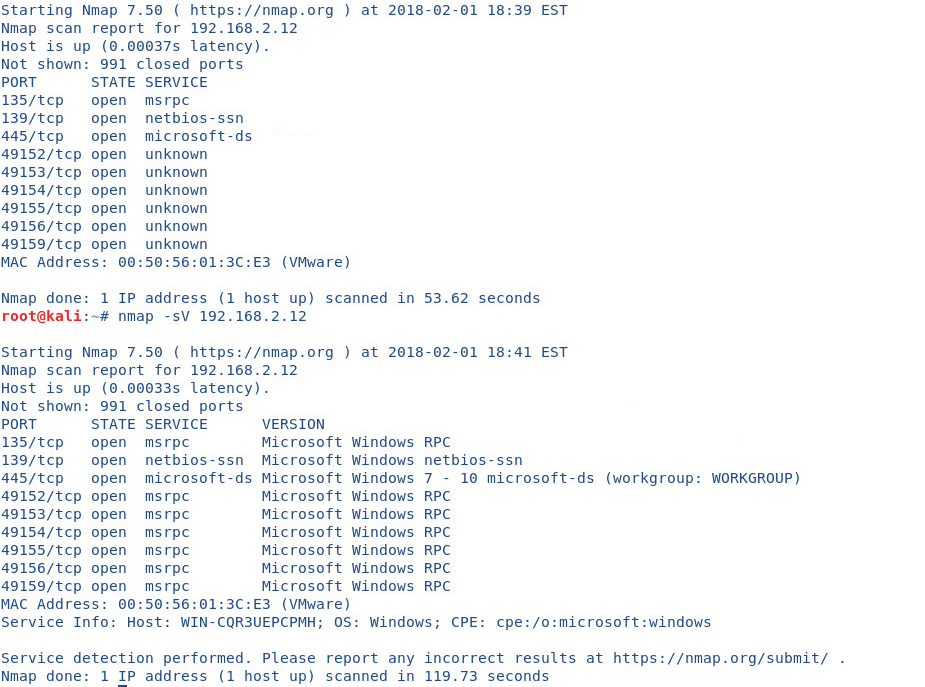


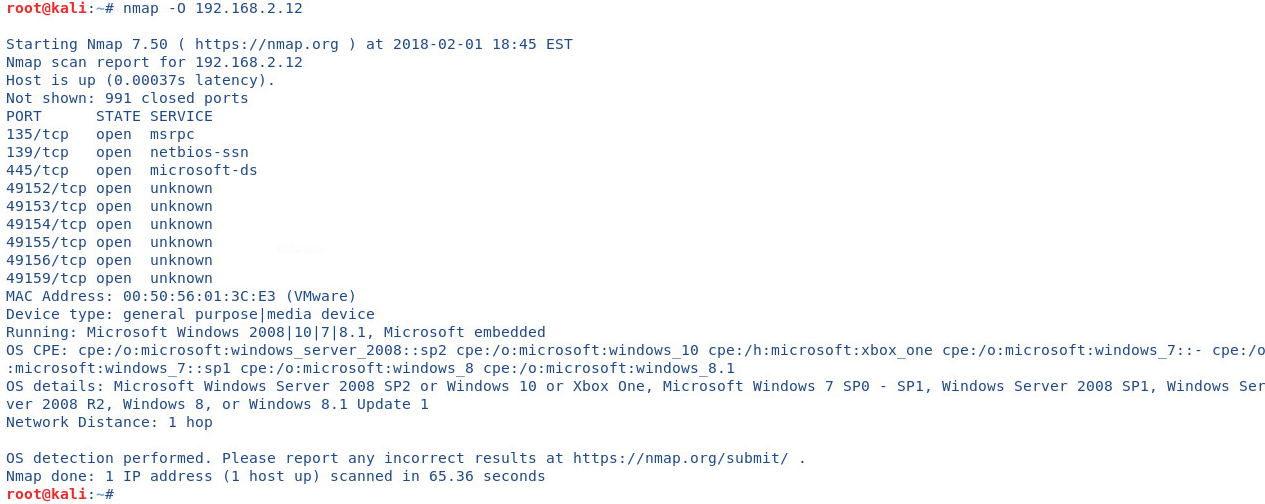


**3.3 Active Reconnaissance**

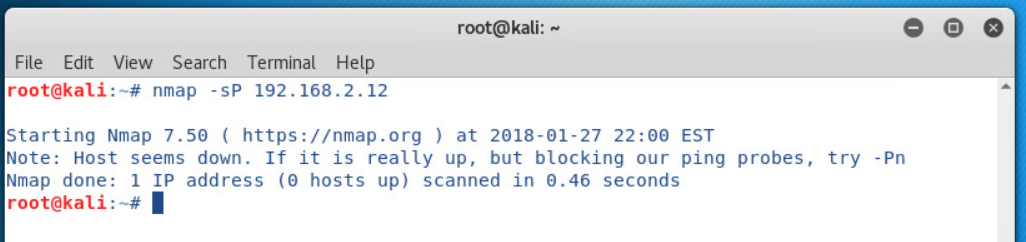
**1. Open  a  bash  shell  and  run  the  different  commands  against  one  of  your  Windows  VMs**

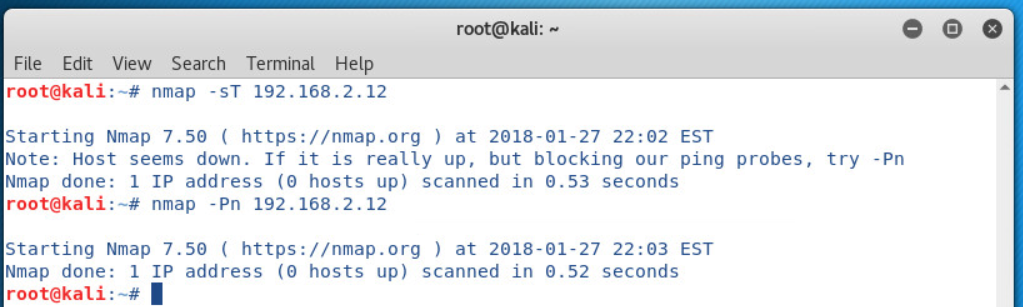


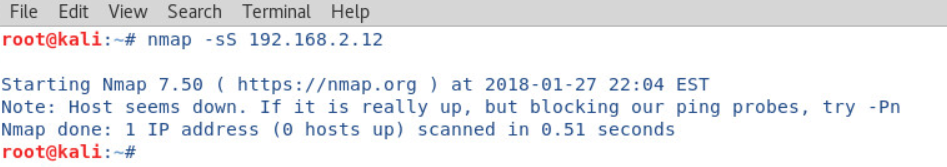


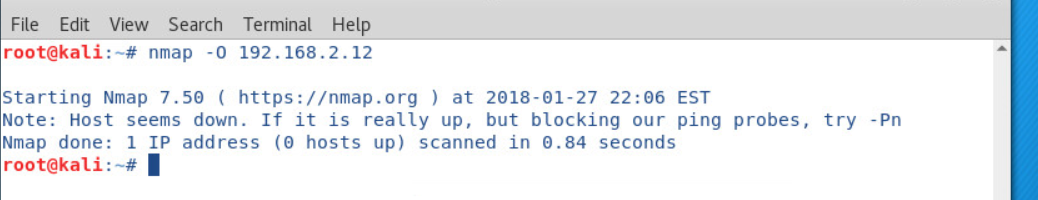


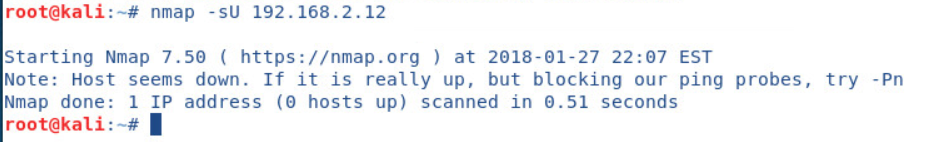
**---------------**

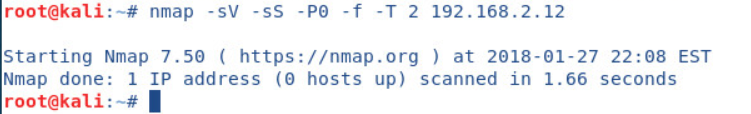


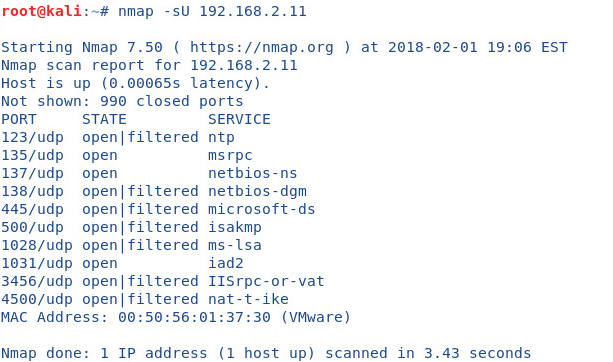




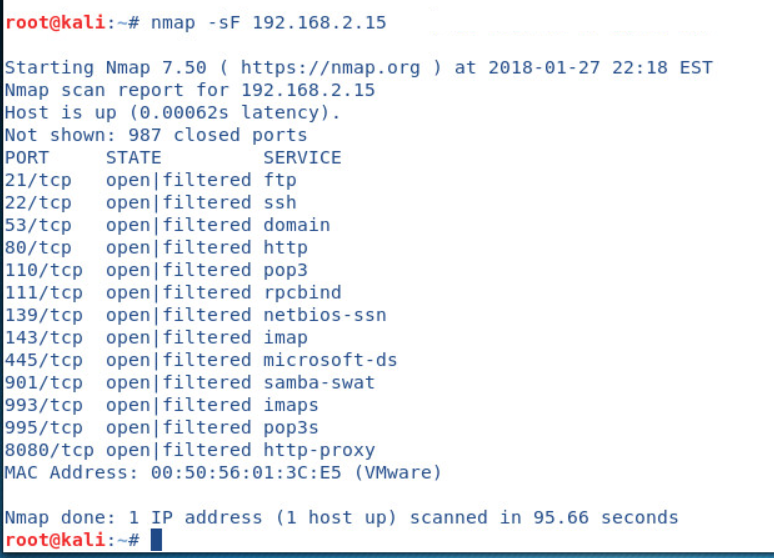


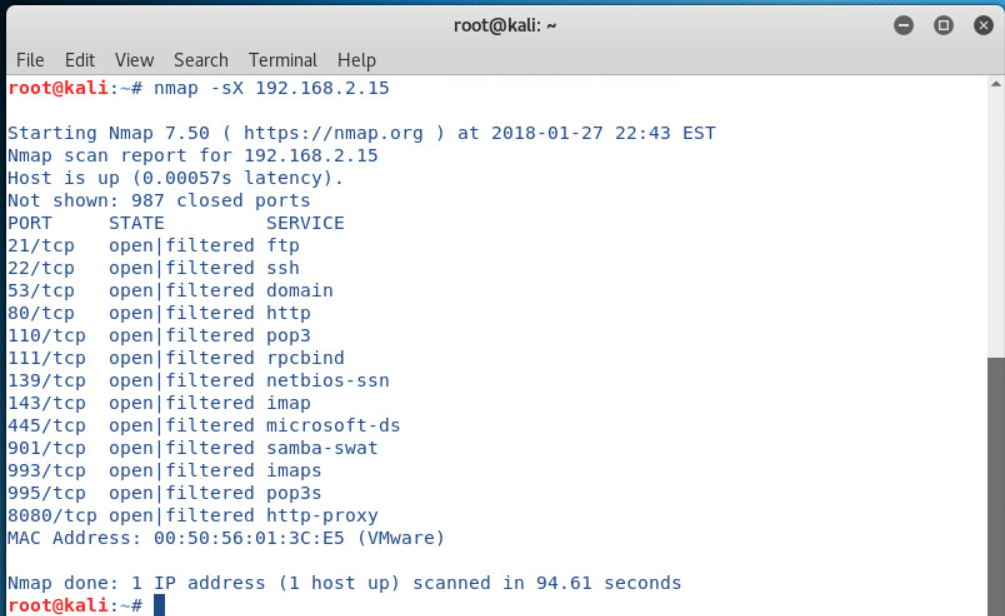


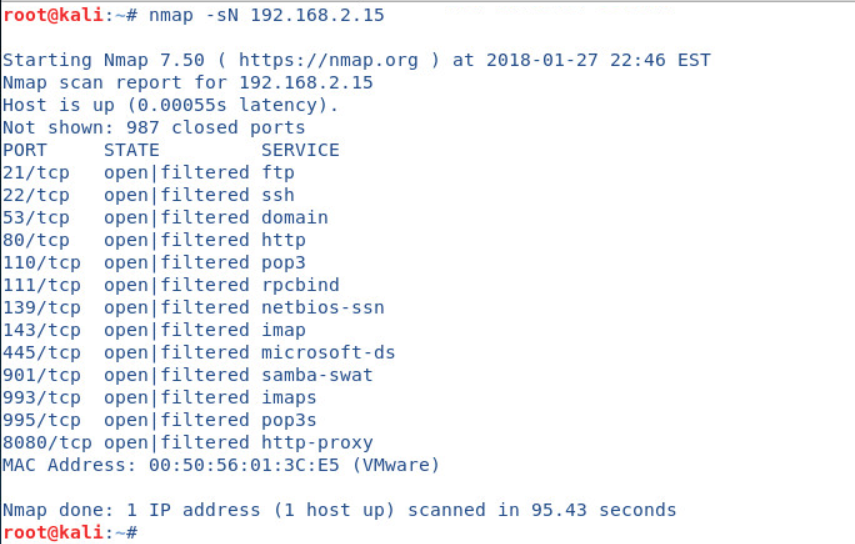




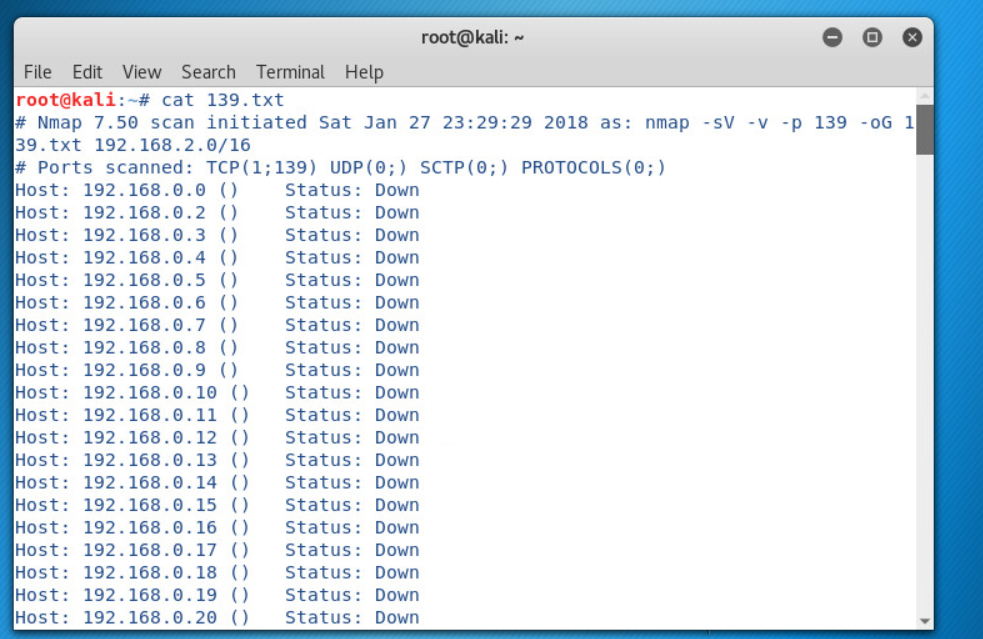
**b.** For the following scans, you will need to attack a UNIX box that has been setup by your instructor. Please record the IP address of the UNIX box here. 1. \_192.168.2.15\_

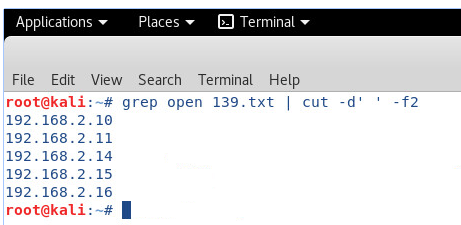




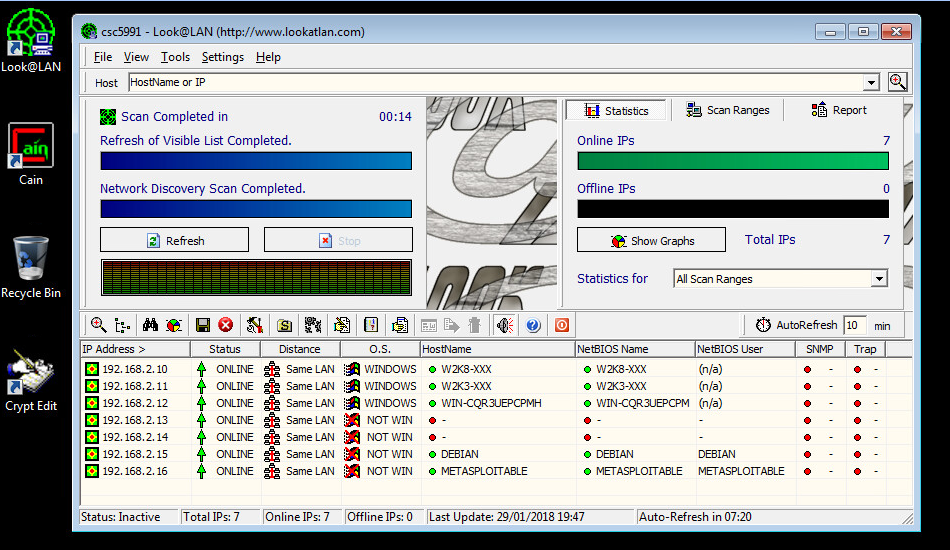






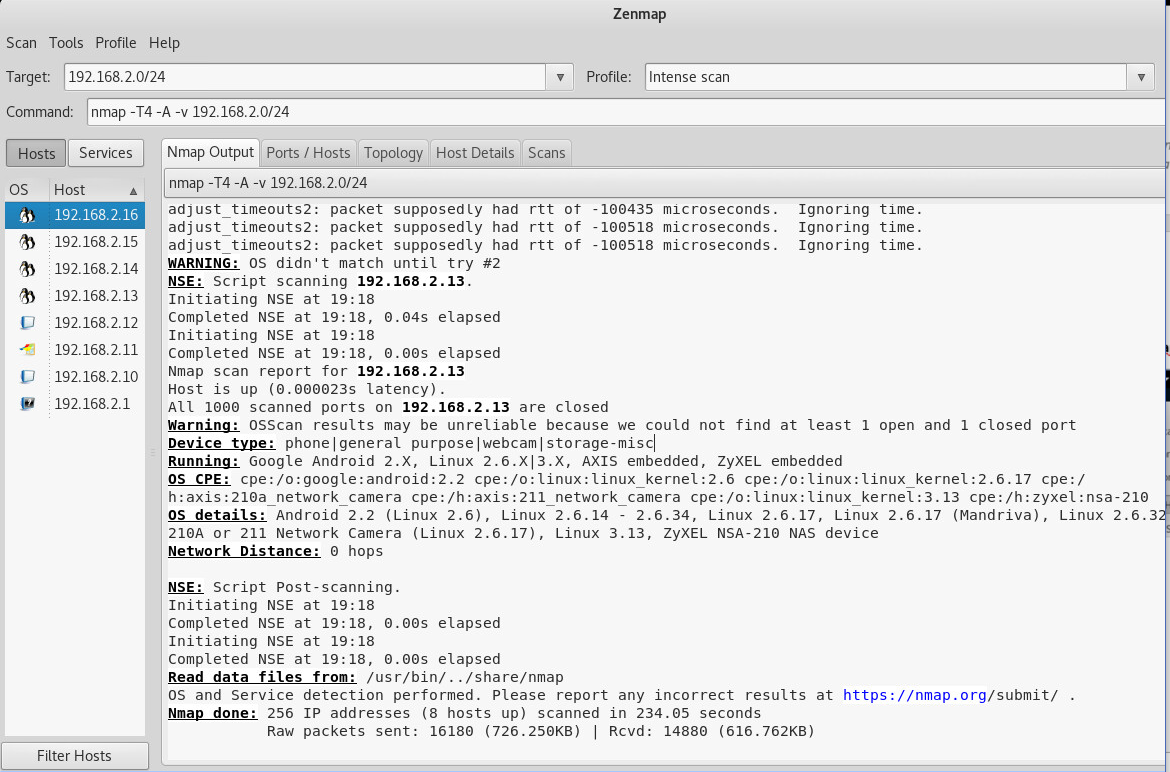


**3.5 Look@LAN**





**3.6 Zenmap**



**3.7 Hping3**

1. Take note of the following options: -c, -S, -p, -2 and -F

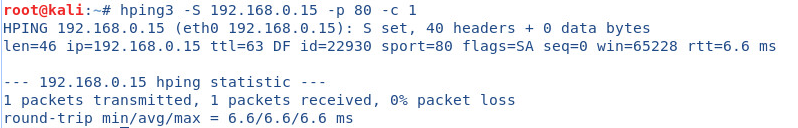
-c 🡪 –count packet count

-S 🡪 –baseport base source port

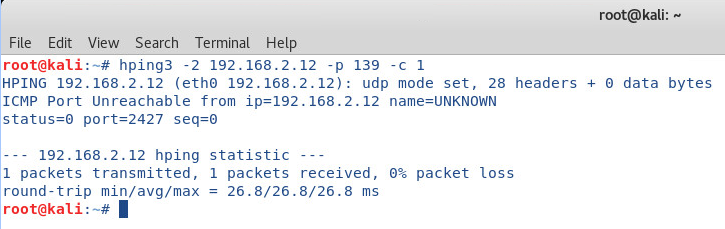
-p 🡪 –destport [+][+] <port> destination port (default 0) ctrl+z inc/dec

-2 🡪 –udp UDP mode

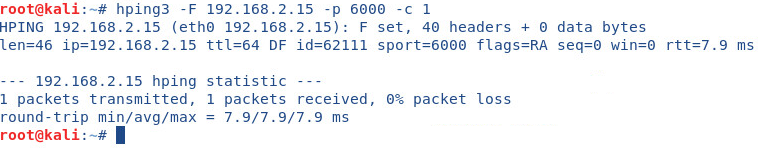
-F 🡪 –fin Set FIN flag

b. Half-open SYN Scan

c. UDP Scan (target windows computer)



d. FIN Scan (used against Debian)



# Vulnerabilities

No vulnerabilities discovered in this lab.