Week 9-Lab:

**Ifconfig:**

* Run ifconfig and determine the name/id of your primary network interface: **10.0.2.15**
* What is your primary interface's IP address? Is it different from your public IP? Why or why not?: **10.0.2.15. Yes it is different than the public ip which is 172.126.4.118.**

**A public IP address is the address that is assigned to a computing device to allow direct access over the Internet. It is globally unique, and can only be assigned to a unique device. A private IP address is the address space allocated by InterNIC to allow organizations to create their own private network. The primary address on an interface is the address that is used by default as the local address for broadcast and multicast packets sourced locally and sent out the interface. (Ref: http://www.juniper.net/documentation/en\_US/junos12.3/topics/usage-guidelines/interfaces-configuring-default-primary-and-preferred-addresses-and-interfaces.html)**

* What is the MAC address of your primary interface?: **08:00:27:a1:b6:e6**
* Identify and understand your [loopback interface](http://askubuntu.com/questions/247625/what-is-the-loopback-device-and-how-do-i-use-it):

**o: flags=73<UP,LOOPBACK,RUNNING> mtu 65536**

**inet 127.0.0.1 netmask 255.0.0.0**

**inet6 ::1 prefixlen 128 scopeid 0x10<host>**

**loop txqueuelen 1 (Local Loopback)**

**RX packets 8574 bytes 361677 (353.2 KiB)**

**RX errors 0 dropped 0 overruns 0 frame 0**

**TX packets 8574 bytes 361677 (353.2 KiB)**

**TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0**

**Ping:**

* What is the IP address of codepath.com?: **198.58.125.217**
* What is the IP address of google.com?: **172.217.4.238**
* Why would the IP address of google.com change between runs or from different locations?: **Because google uses different servers based on the locations.**

**Nslookup:**

* Using the IP for codepath.com from the previous, pass it to nslookup: **nslookup 198.58.125.217**
* Does the domain returned from nslookup match? If not, why not?

**Server: 192.168.1.254**

**Address: 192.168.1.254#53**

nslookup shows the host name and IP address of the DNS server that is configured for the local system.

**Traceroute:**

* Compare the traceroutes for codepath.com and google.com

**google.com: 16 hops**

**Codepath.com: 13 hops**

* How many of the hops are the same? What accounts for this?: **7 hops**
* Which has more hops? What accounts for the difference?: **google**

**telnet:**

* What's one thing that makes telnet insecure?: **telnet does not encrypt communication between the client and server. Everything is sent in plain text, even passwords.**
* Can you telnet to codepath.com? What port is open and why?
  + **Port 80 is open. Because codepath server is running in this port.**

**Curl and wget:**

* Identify some differences between the two: **wget supports recursive download while curl dies not**
* Which would you be more likely to use for interacting with a RESTful API from the command line?
* Which support recursive downloading?: **wget**
* Which are you more likely to find pre-installed on a Linux OS?: **wget**
* What is the syntax for each for downloading a file to the current directory?
  + wget <http://www.linode.com/docs/assets/695-wget-example.txt>
  + curl –O <http://www.linode.com/docs/assets/695-wget-example.txt>

**Ssh and scp:**

* Why is key authentication preferred to passwords?: **Keys don't get transmitted to the remote system but passwords need to be.**
* What is the syntax for copying a file from a local folder to a remote one?:
  + **scp -r user@your.server.example.com:/path/to/foo /home/user/Desktop/**

**Milestone 1: Security-Flavored Net Tools**

**Challenge 1:** Run nmap against your localhost IP to see all open ports

* See how many of the ports you can match to services
  + nmap -v localhost
* Hint: try shutting down Docker or Virtualbox and re-running nmap

**PORT STATE SERVICE**

**135/tcp open msrpc**

**445/tcp open microsoft-ds**

**843/tcp open unknown**

**2200/tcp open ici**

**2222/tcp open EtherNetIP-1**

**3306/tcp open mysql**

**4004/tcp open pxc-roid**

**49152/tcp open unknown**

**49153/tcp open unknown**

**49154/tcp open unknown**

**49155/tcp open unknown**

**49156/tcp open unknown**

**49157/tcp open unknown**

**49160/tcp open unknown**

**Milestone 2: Grabbing Packets with tcpdump**

**Challenge 1:** Determine the IP address for codepath.com and use tcpdump to display packets with that IP as the destination. Then open [http://www.codepath.com](http://www.codepath.com/) in the browser and check the output. Notice the output displays the HTTP requests in addition to the packets.

* How many requests to load the main codepath.com page?: **3**
* What type of resource accounts for most of the requests?: **S (start connection), P (push data), F (finish connection)**
* Now try the same exercise with [https://security.codepath.com](https://security.codepath.com/). What differences do you see in the output? What accounts for those differences? **It has many S, P, F requests as the page refreshes frequently.**

**Challenge 2:** You can also monitor DNS queries on port 53 with tcpdump. Use this to determine the IP of your primary DNS:

* Listen for DNS queries on port 53**: sudo tcpdump -vvv -s 0 -l -n port 53**
* Think of a domain name that probably exists (common word or phrase + .com) but that you've never visited before (suggestion: zombo.com) and open it in a browser
* Look at the tcpdump output for the UDP packets trying to resolve the domain. The destination IP should be the DNS

**192.168.1.254.53 > 10.0.2.15.60030: [udp sum ok] 32899 q: AAAA? zombo.com. 0/1/0 ns: zombo.com. [1h] SOA ns.liquidweb.com. root.ns.liquidweb.com. 2003081204 3600 3600 3600 3600 (81)**

**Milestone 3: Hello, Wireshark**

* Look at the source and destination IPs; how much of the traffic is inbound vs. outboud?
* Try nslookup on a couple of IPs that aren't in your network. See if you can figure out who those IPs belong to

**Server: 192.168.1.254**

**Address: 192.168.1.254#53**

**Non-authoritative answer:**

**232.109.55.157.in-addr.arpa name = msnbot-157-55-109-232.search.msn.com.**

**nslookup 192.168.1.254 -v**

**\*\*\* Invalid option: v**

**Server: 192.168.1.254**

**Address: 192.168.1.254#53**

**254.1.168.192.in-addr.arpa name = homeportal.**

**254.1.168.192.in-addr.arpa name = attlocal.net.**

**254.1.168.192.in-addr.arpa name = igateway.**

**254.1.168.192.in-addr.arpa name = gateway.**

**254.1.168.192.in-addr.arpa name = api.home.**

**254.1.168.192.in-addr.arpa name = dsldevice.**

* Try to identify traffic associated with at least one process on your host that's either part of the OS itself or is auto-launched at startup

**nslookup 192.168.1.69**

**Server: 192.168.1.254**

**Address: 192.168.1.254#53**

**69.1.168.192.in-addr.arpa name = Zakia.**

**nslookup 65.52.108.74**

**Server: 192.168.1.254**

**Address: 192.168.1.254#53**

**\*\* server can't find 74.108.52.65.in-addr.arpa: NXDOMAIN**

* See if you can spot any [ARP](https://en.wikipedia.org/wiki/Address_Resolution_Protocol) packets used to resolve IPs to MAC addresses:

**3 1.024022 ArrisGro\_4f:f1:a1 Broadcast ARP 60 Who has 192.168.1.69? Tell 192.168.1.254**

**4 1.024042 IntelCor\_77:e9:08 ArrisGro\_4f:f1:a1 ARP 42 192.168.1.69 is at 30:3a:64:77:e9:08**