Network Reconnaissance and Discovery Tools

1. What are reasons to use a command line tool as opposed to a graphical user interface, or GUI-based software tool?

2. Match the following command line tools with their function

A. tracert/traceroute

B. nslookup/dig

C. ipconfig/ifconfig

D. nmap

E. ping

F. arp

G. route

H. curl

\_\_\_ Displays the network configuration information for the machine

\_\_\_ Determines the route taken over a network to reach a target host

\_\_\_ Port scanner and network mapper tool

\_\_\_ Shows the table that stores the MAC addresses associated with IP Addresses

\_\_\_ Transfers data from one server to another

\_\_\_ Tests the connectivity of machines using ICMP traffic

\_\_\_ Query DNS information available from a name server

\_\_\_ Can view the route table and alter the route network traffic is taking

3. Match the following applications with their function

A. the harvester

B. Sn1per

C. scanless

D. dnsenum

E. Nessus

F. Cuckoo

\_\_\_ Combines command line tools (whois, ping, etc…) to gather intelligence against a system

\_\_\_ Gathers intelligence without ever giving away your own IP Address

\_\_\_ Sandboxes environment to test files before trying on actual system/server

\_\_\_ Similar to nmap, scans the ports for vulnerabilities as well

\_\_\_ Finds DNS records and all the servers and DNS entries for an organization

\_\_\_Gathers public facing information about a company or domain

4. What’s the difference between the nslookup and dig commands?

5. How is pathping similar to traceroute? What’s the difference between the two?

6. What is the difference between netcat and netstat?

7. Why might someone use the hping command?

8. What’s the difference between sn1per and scanless?

9. What services/data sources does theHarvester use to gather information?