Cybersecurity Guided Notes (ANSWER KEY)

# Lesson 4.1.1 - 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?

   Answers will vary, here are some common answers:

   Automation of tool execution and information

   Most servers only use CLI to conserve system resources

   The command line is also powerful because of the ability to string commands together and make tools interact with one another in ways specific to the task

2. Match the following command line tools with their function

| | |
|---|---|
| A. tracert/traceroute | __C__ Displays the network configuration information for the machine |
| B. nslookup/dig | __A__ Determines the route taken over a network to reach a target host |
| C. ipconfig/ifconfig | __D__ Port scanner and network mapper tool |
| D. nmap | __F__ Shows the table that stores the MAC addresses associated with IP Addresses |
| E. ping | __H__ Transfers data from one server to another |
| F. arp | __E__ Tests the connectivity of machines using ICMP traffic |
| G. route | __B__ Query DNS information available from a name server |
| H. curl | __G__ 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__ | Combines command line tools (whois, ping, etc…) to gather intelligence against a system |
| B. Sn1per | __C__ | Gathers intelligence without ever giving away your own IP Address |
| C. scanless | __F__ | Sandboxes environment to test files before trying on actual system/server |
| D. dnsenum | __E__ | Similar to nmap, scans the ports for vulnerabilities as well |
| E. Nessus | __D__ | Finds DNS records and all the servers and DNS entries for an organization |
| F. Cuckoo | __A__ | Gathers public facing information about a company or domain |

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

   Nslookup shows the user the IP Addresses associated with a domain name while dig command can provide more information about the domain address.

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

   They both show the path between two hosts, however pathping also uses ping to locate spots where traffic is slow. Thus, trying to find where delays might exist.

6. What is the difference between netcat and netstat?

   netcat is a tool that allows a user to read and write directly to a network interface while the netstat command is a network statistics tools that displays current network activity.

7. Why might someone use the hping command?

   Allows the person to create their own packets to test the security of a network against firewalls, open ports, etc.

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

   sn1per can be traced back to the user who ran the scan while scanless cannot be traced back to the user

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

   Answers will vary, some answers might include:

   Twitter

   Google

   Yahoo

   Bing

   LinkedIn