CSCD 330 - Computer Networks

Lab 1, Tool scavenger hunt

Instructions:

The command line tool `man` is your friend. Use `man` and the Internet to answer the following questions. **Do not** copy the explanation of `man` for your answers, but use it as a guide to run the tool and find out what it's doing.

Questions:

1. What does `ping` do, how do you know?

   Ping send ICMP packets to the target host. If you ping google.com if returns an echo reply with the TTL and the time it took to reach the target host and back.

2. How could `ping` be useful?

   Checking the network connectivity of a device for capabilities, latency and packet loss.

3. What does `dig` do?

   Queries DNS servers, performs DNS lookup and displays the answers returned. IP addresses, domain name and query time.

4. What does `nslookup` do?

   Also queries DNS servers and displays IP addresses affiliated with the target host.
   Can also perform reverse DNS search to recover the domain name.

5. Do `dig` and `nslookup` tell you any of the same information? If so, what?

   Yes, they tell you similar information based on the flag provided. Perform reverse DNS, IP addresses, domain name.

6. What is a domain name?

   A text-based alternative to access a target host rather than using IP addresses, which can be complex to remember. google.com vs 142.250.217.110

7. What is a DNS server?

   Ensures that internet traffic is routed to the correct server by translating the domain name into an IP address allowing you to access the target host.

8. What DNS server does your machine use?

   10.201.16.11

9. How would you change this DNS server from the command line on a Linux machine?

   sudo resolvectl dns enp0s3 8.8.8.8 1.1.1.1, this will change the DNS server until system reboot or the network is restarted.

10. What is `wireshark`?

    A network protocol analysis tool used to view live traffic or PCAP files.

11. What is `traceroute`?

    A tool to trace the path of data packets from your device to the target host, identifying the different hops along the way.

12. What is the difference between running `traceroute` with `-T` vs `-I`?

    Traceroute with -T uses TCP packets to send along the route to a specific port number, while traceroute with -I sends ICMP packets and behaves like the ping command.

13. What is `whois`?

    A query protocol runs over TCP port 43 to ask databases maintained by domain registries and registrars for technical information regarding these domains such as company, contact information, DNS servers, etc.....

14. What is RFC 3912?

    The official specification/standard that defines the WHOIS protocol.

15. On the topic of RFCs, what is an RFC?

    A technical document published by the Internet Engineering Task Force that documents standards, Protocols, procedures and practices such as how email and web data is transferred.

16. Use `nslookup` and `dig` on the same domain (e.g., google.com). Do they return the same IP address? What happens when you put the IP address(es) in the address bar of your browser?

    Yes they return the same IP address. And whether you use the domain's name or IP address in your browser, it will take you to the same domain.

17. Explain the output of the command `ip a`?

    Displays the network interfaces on your Linux machine, along with their IP address configuration and status.

18. What is `tcpdump`?

    A command line network packet analyzer that captures and displays network traffic, just like Wireshark.

19. Is there anything specific you want to learn about networks? If so, what? If not, what do you hope to get out of this class?

    I don't have any specific learning outcomes for this class except to learn whatever this class has to offer to further enhance my cybersecurity experience.

20. Tell me something about yourself.

    If I added one or 2 more animals to my household, I feel like I could start charging people admittance to my zoo. I have 3 dogs, 2 frogs, 1 Ball python, carnivorous plants and several aquariums hosting: axolotls, eels, pike, lesser siren. I breed axolotls as well.

21. Do you have any prior experience with Linux, the terminal, or Python? If so, how much?

    I have previous experience with Linux and the terminal through participation in the cybersecurity club and cyber related events in the last year: NCAE, NCL, Spokane Cyber Cup. However, I do not have much experience with python.