

Computer Security Fundamentals – Spring 2023

Introduction, Networking and Security Basics

Total: 10 points

Q1. The color of their (hackers) hats (1.5 pts)

Tell me how they look like? For,

- 1) Black hat hackers (0.5 pt)
- 2) White hat hackers (0.5 pt)
- 3) , and Gray hat hackers (0.5 pt)

Q2. What is the meaning of “Footprinting” in the process of hacking? (0.5 pt)

(Just give me 3~4 lines, at most)

Q3. In our slides, I put 3 traditional styles of password hacking. Among these 3 styles, (1 pt)

- 1) Which one is more efficient? (0.5 pt)
- 2) In what kind of special use case? (0.5 pt)

Q4. DHCP (1 pt)

Briefly talk about the high level idea of DHCP.

Hint: There is a process of the setup of DHCP between ISP and online / offline devices

Q5. The role of the router (1 pt)

Choose an answer to best describe the role of a router. (Or what we can do in a router?)

- A) We can install firewall onto the router
- B) The router is doing a job called NAT, so the packet is sending out from the private network can be correctly delivered to the device in the internet.

Similarly, the machine in the private network can be benefited from the NAT to get the packets delivering from the internet.

- C) We can have the router use the public IP, but the rest of the PCs or mobiles phones inside of the private network can use private IP addresses. That means, they can share one public IP address. This can help to alleviate the issue of the draining resource of IPv4 public IP address.
- D) All of them above

Q6. CIDR in IPv4 (1 pt)

If I put a CIDR like this: 192.168.1.12/24, tell me what is the range of this subnet.

Q7. IPv6 (1 pt)

As we know, the IPv6 has an option to compress its IP address string.

Tell me the following IPv6 string, “after” the compression, how it looks like?

2001:edb8:0000:0000:abff:0000:0000:0234

Q8. Normal V.S. Promiscuous mode (1 pt)

When we are using the “sniffer” software, the software will change the setting in our Ethernet card. What are the differences between these 2 different modes?

Q9. SSID and BSSID (1 pt)

What’s the difference between SSID and BSSID? Can you give me an example of that?

Q10. OSINT (1 pt)

OSINT is a kind of technology that can allow us to do the queries against several online databases.

Tell me the benefit to use such kind of technology instead of “doing everything by ourselves”