Week 4

Key knowledge/skills: network security & attacks

Q1. Where is the information about ports and device Layer 2 addresses kept in a switch? And where is the information about IP address kept in a router?

Sample answer: MAC address table; Routing table.

Q2. Which type of query is sent from a DNS resolver to a DNS server?

Sample answer: Recursive

Q3. How many host IPv4 addresses are possible in a /24 network?

Sample answer: 254

Q4. How do UDP scans work?

Sample answer: UDP scans have to rely on ICMP "port unreachable" messages to determine whether a port is open. When the scanner sends a UDP packet and the port is not open on the victim's system, that system will respond with an ICMP "port unreachable" message.

Q5. What is a phishing attack?

Sample answer: This is a type of attack where the attacker presents a link that looks like a valid, trusted resource to a user. When the user clicks it, he is prompted to disclose confidential information such as his username and password.

Q6. How do you describe a traditional IPS?

Sample answer: A network security appliance or software technology that inspects network traffic to detect and prevent security threats and exploits.