NAME: PRATIBA.S

DATE:15.09.25 ROLL NO.:241901080

# EXERCISE 7

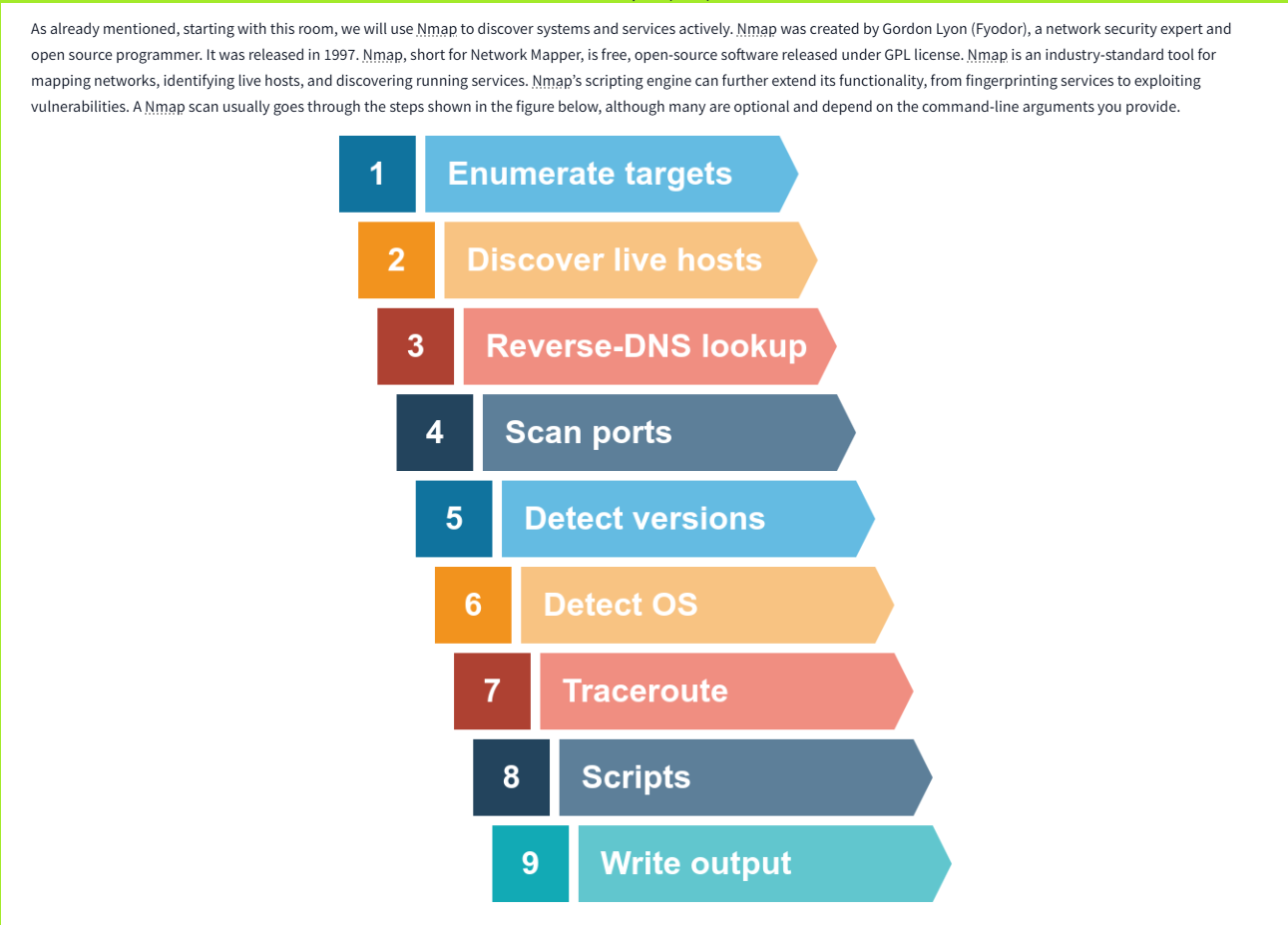
**NMAP TO DISCOVER LIVE HOSTS USING ARP SCAN, ICMP SCAN, AND TCP/UDP**

**PING IN TRY HACK ME PLATFORM**

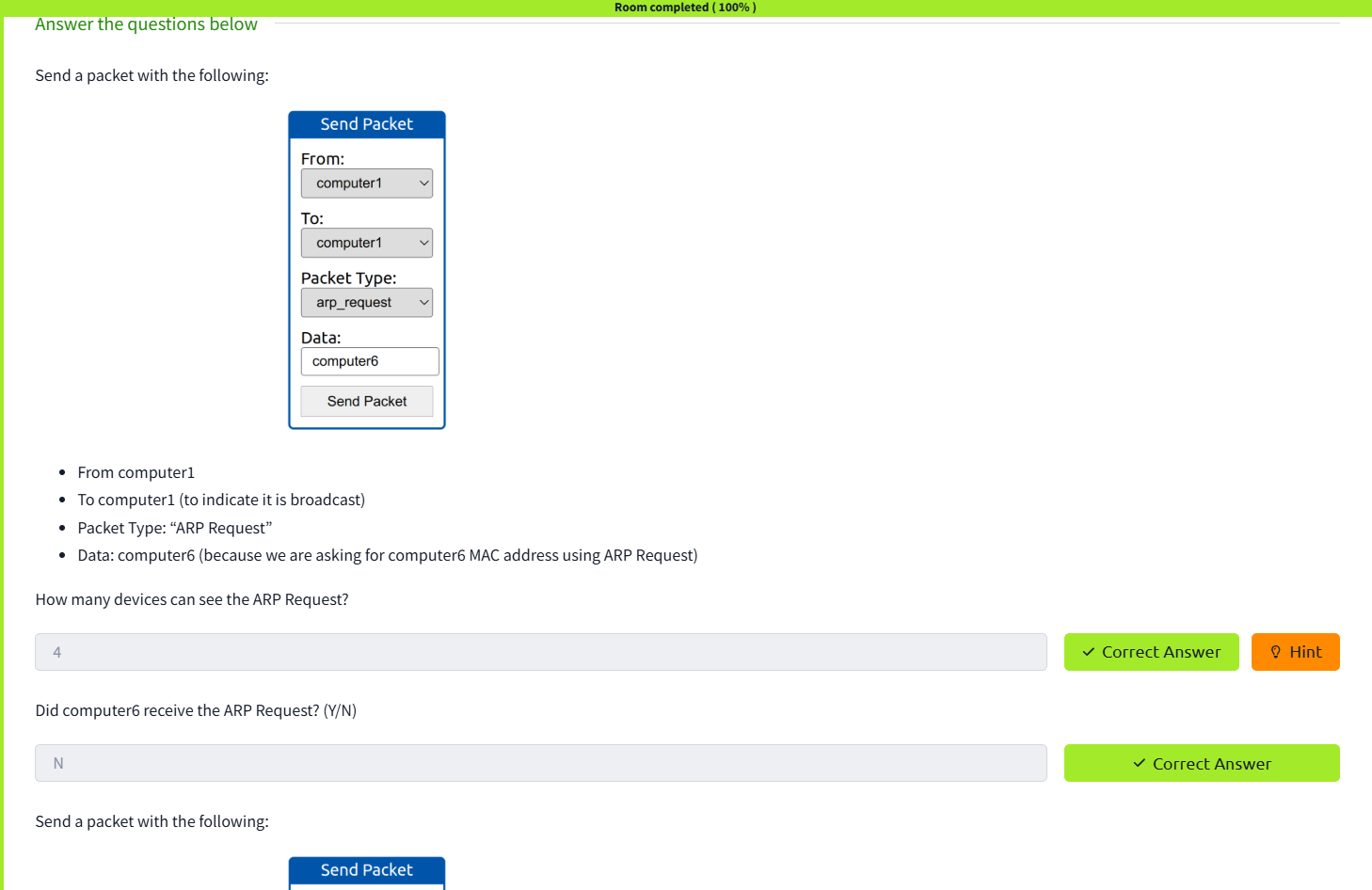
**AIM:**

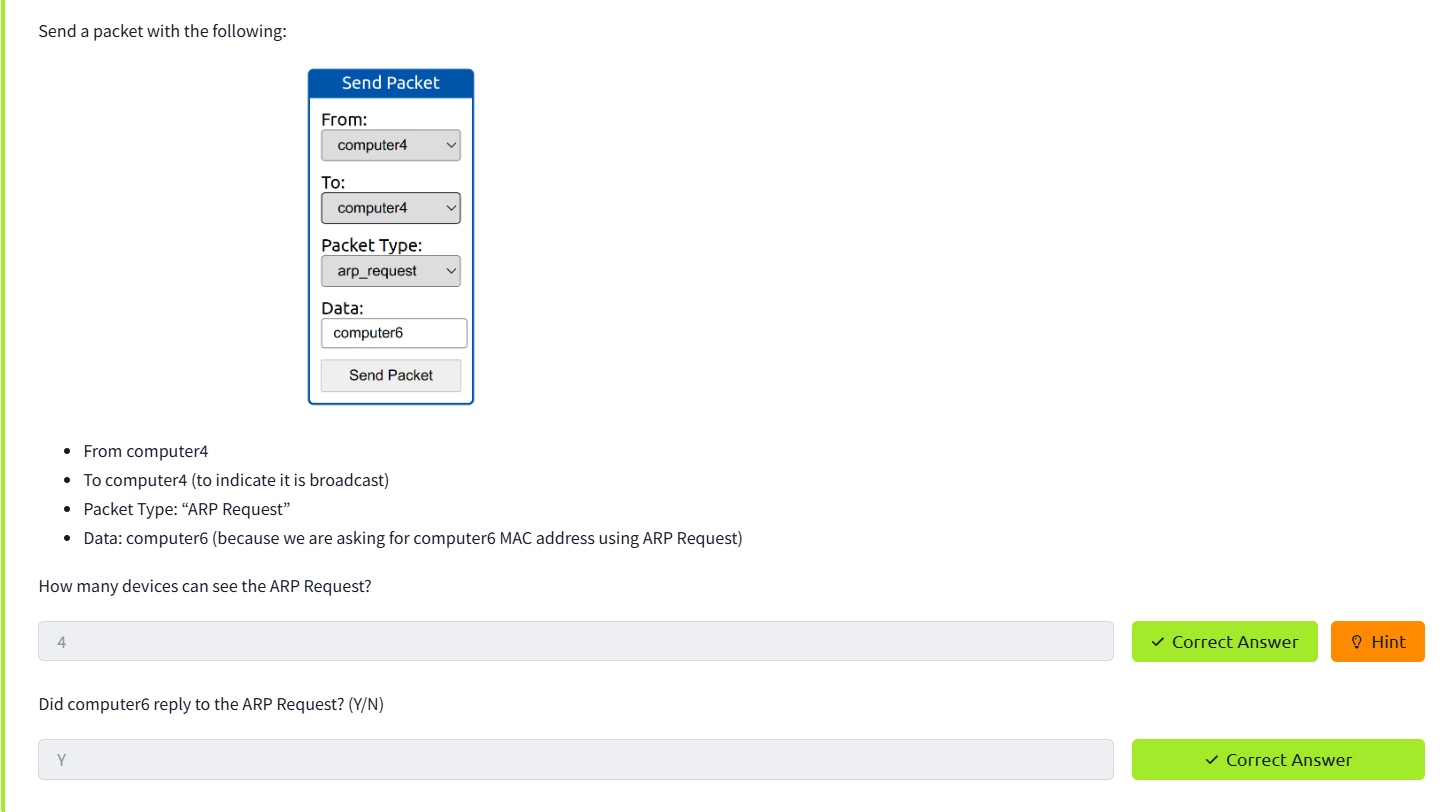
In this module, we focus on discussing live hosts on a network using Nmap. Finding which systems are online is crucial before scanning ports or services to save time and avoid unnecessary network traffic. This forms the foundation for effective network mapping and security auditing.

**TASK 1**: **INTRODUCTION**

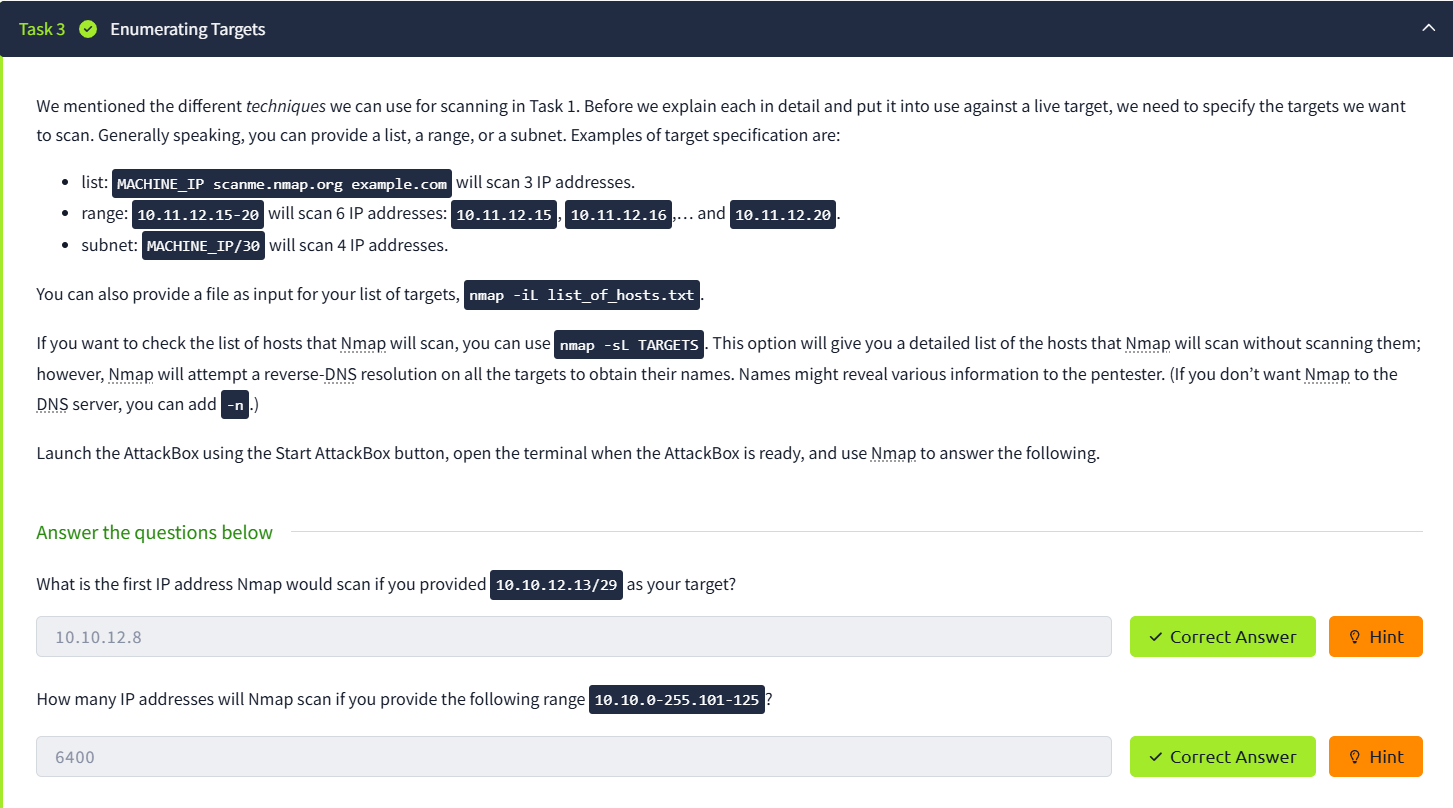


**TASK 2: SUBNETWORKS**

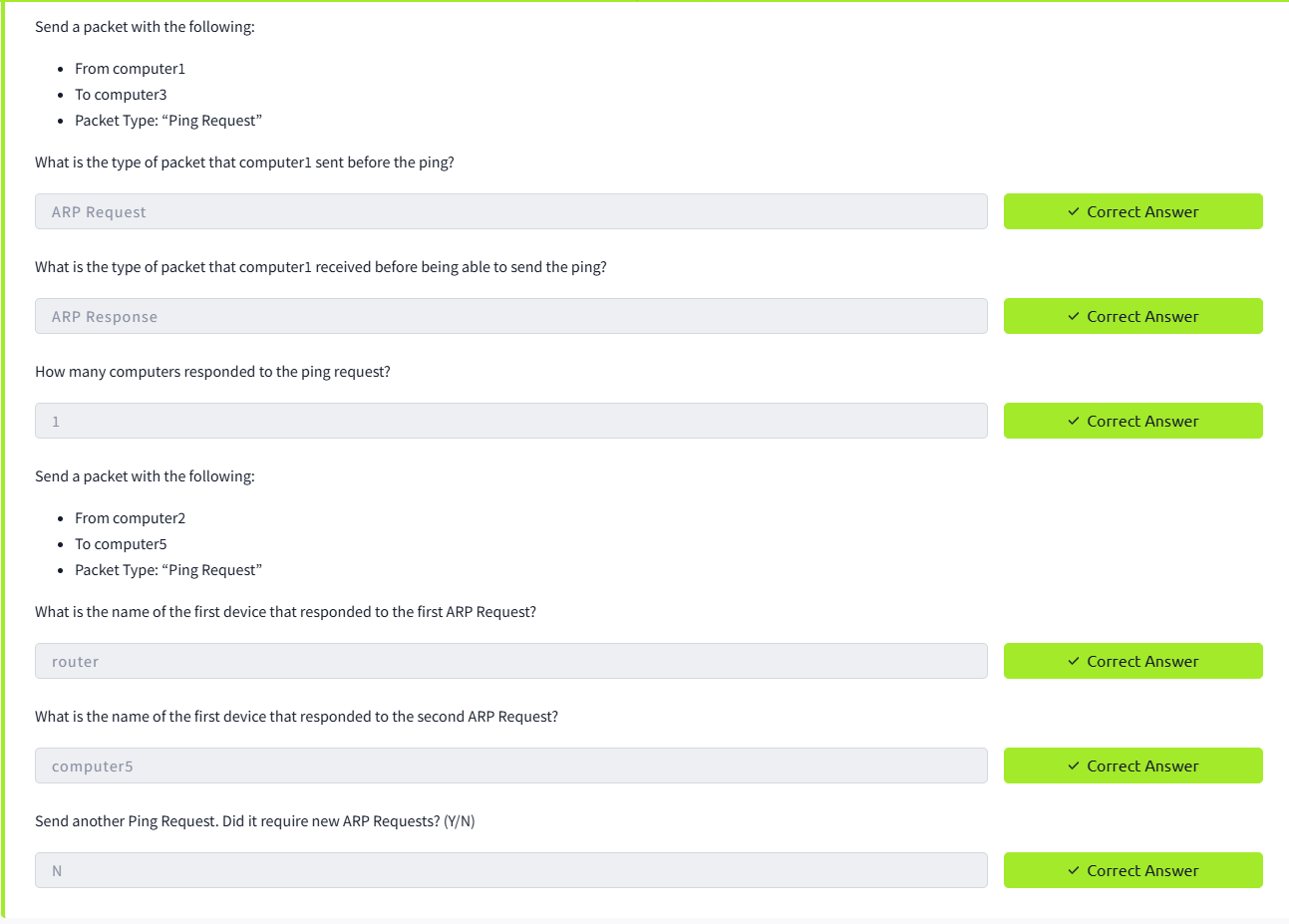
****

****

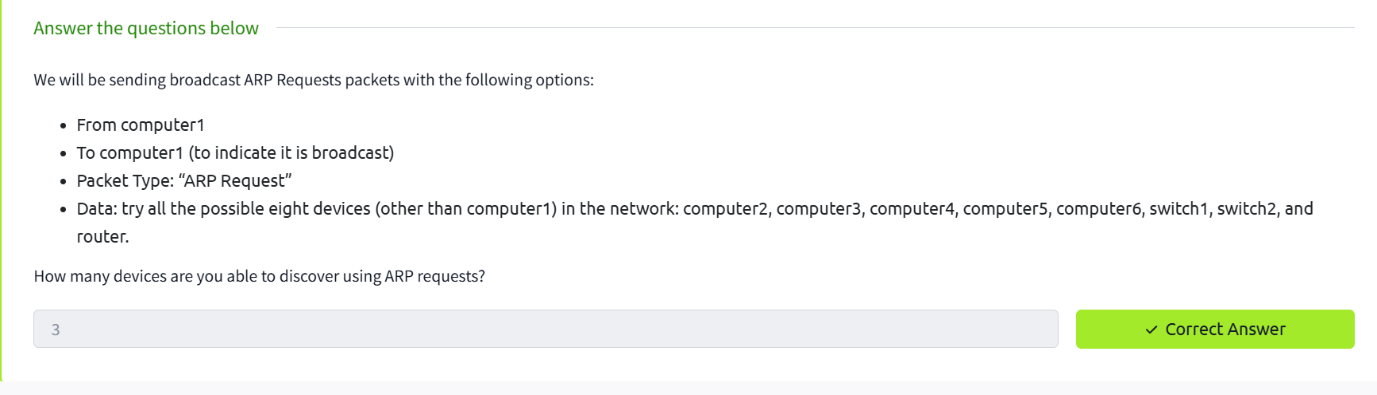
**TASK 3: ENUMERATING TARGETS**

****

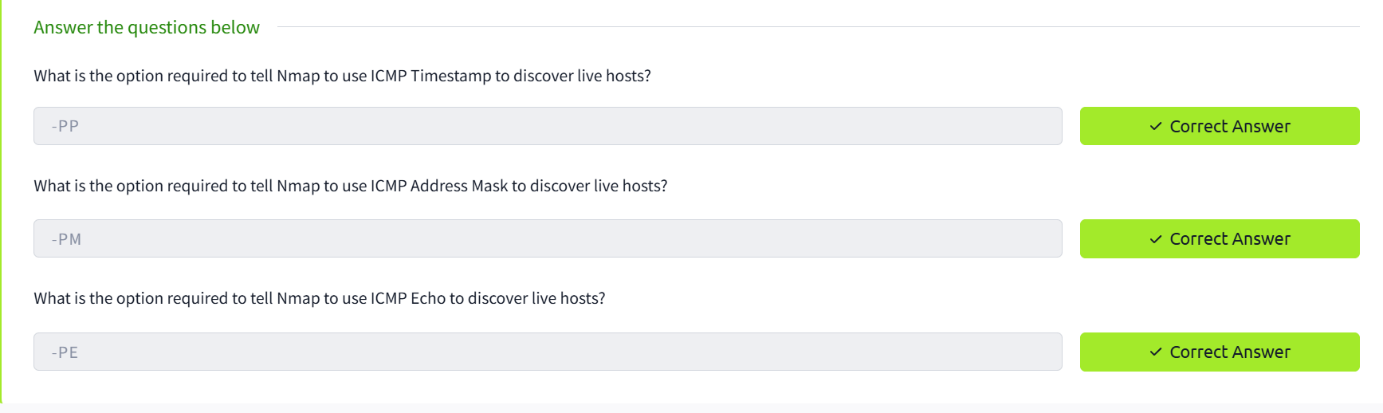
**TASK 4: DISCOVERING LIVE HOSTS**

****

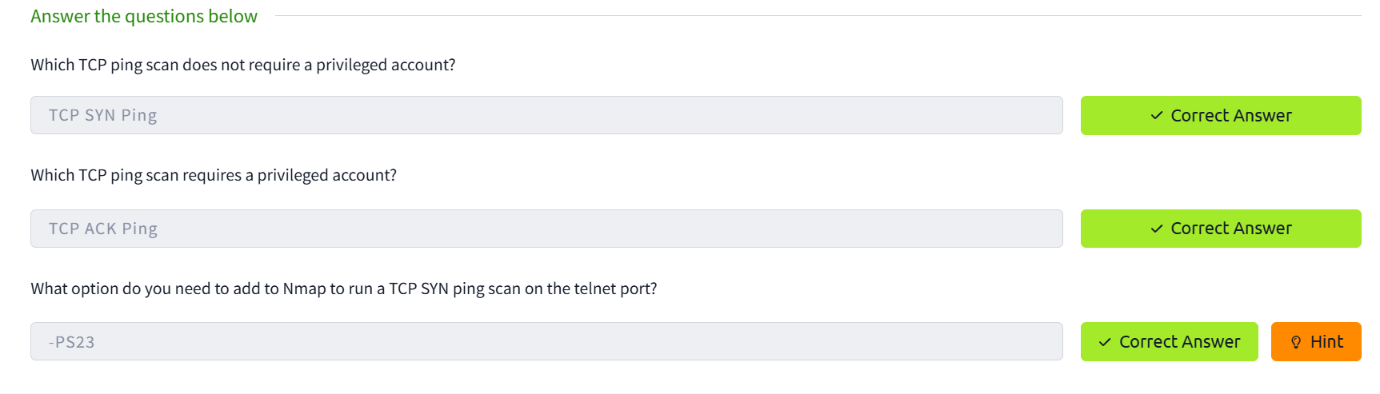
**TASK 5: NMAP HOST DISCOVERY USING ARP**

****

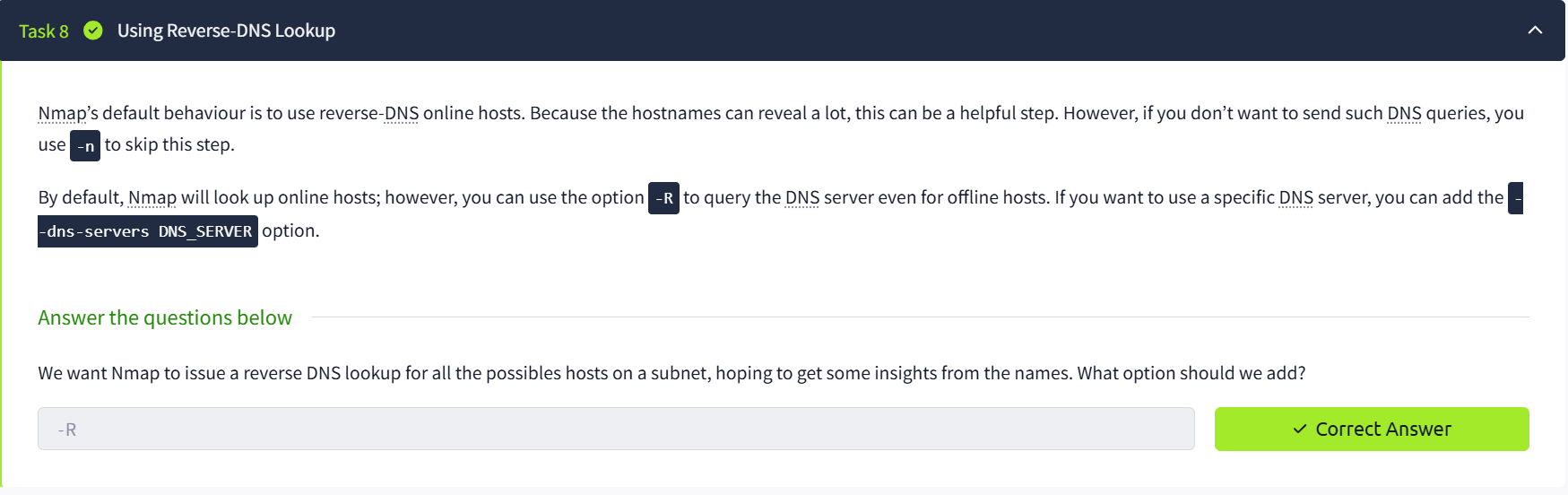
**TASK 6: NMAP HOST DISCOVERY USING ICMP**

****

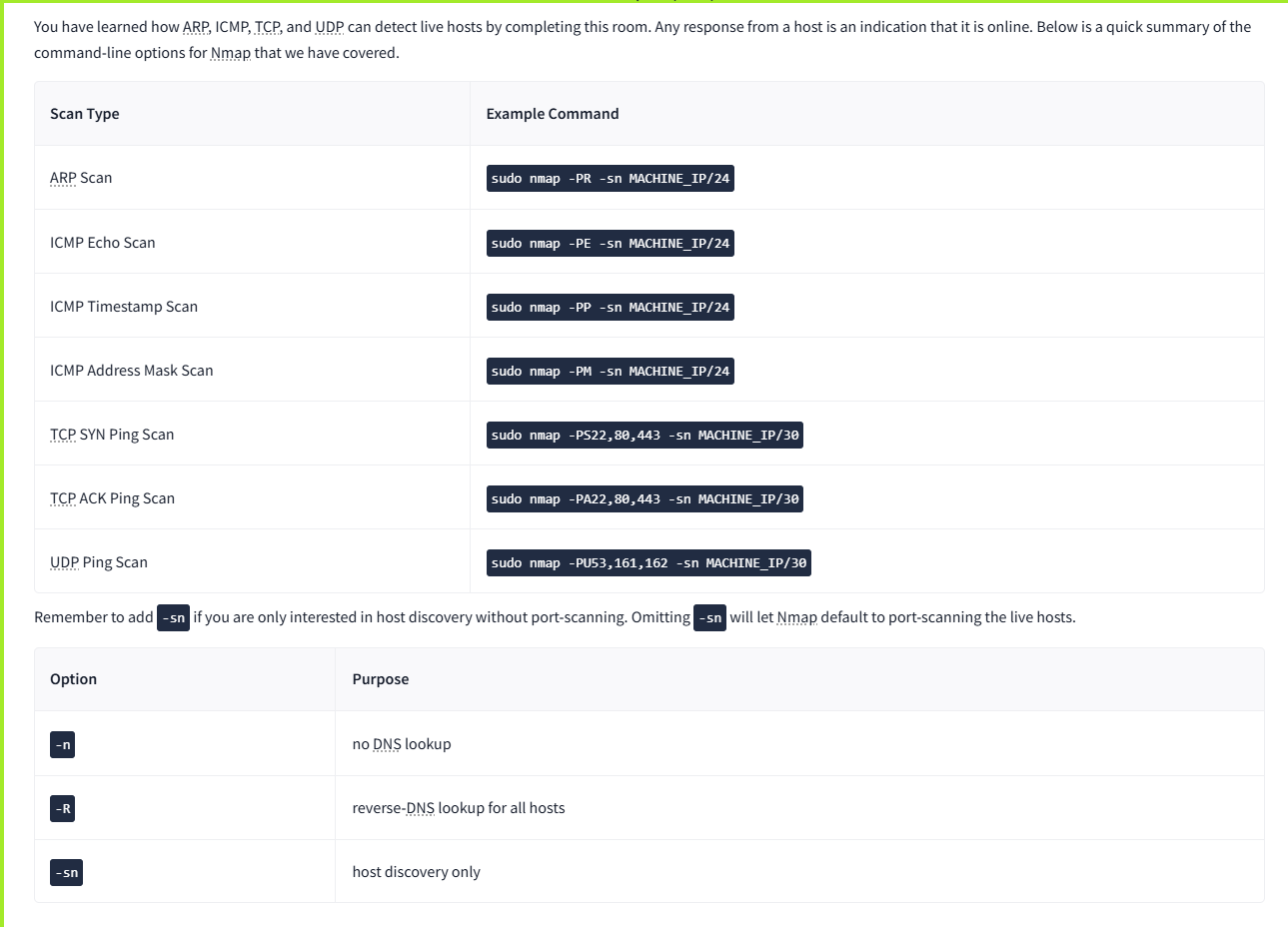
**TASK 7: NMAP HOST DISCOVERY USING TCP AND UDP**

****

**TASK 8: USING REVERSE DNS LOOKUP**

****

**TASK 9: SUMMARY**

****

**RESULT:**

Nmap detects live hosts using ARP, ICMP, TCP SYN/ACK, and UDP. DNS lookups are run by default, but the -n, -R, and --dns-servers options control resolution.