Task 1: Firstly, you need to find the IP address of the vulnerable server.

Output :
```
ping cyberrange.threatguardians.com
PING cyberrange.threatguardians.com (4.240.113.112): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
```

Task 2: Second, you must find the vulnerable server's open ports.

Output:
```
sudo nmap -PN -sV cyberrange.threatguardians.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-10 20:08 IST
Nmap scan report for cyberrange.threatguardians.com (4.240.113.112)
Host is up (0.019s latency).
Not shown: 928 filtered tcp ports (no-response), 70 filtered tcp ports (admin-prohibited)
PORT   STATE SERVICE    VERSION
22/tcp open  tcpwrapped
80/tcp open  tcpwrapped
```

Task 3: Third, you must find the operating system running on the host where service is running.

Output:
```
└─ nmap -sV cyberrange.threatguardians.com
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Task 4: Find the port number used by telnet service.

Output:
```
23/tcp   open  telnet      Linux telnetd
(└─ nmap -sV cyberrange.threatguardians.com
)
```

Task 5: Find the port number used by irc service.

Output:

```
6667/tcp open  irc         UnrealIRCd
(└─ nmap -sV
cyberrange.threatguardians.com
┘
)
```