Q1)

1. I would place my self as the other pcs connected to the switch, so that the other devices register me as a normal device. Then i can attack the network and get the data.
2. The ARP-Request is a broadcast request, so it will go to all the other devices. These devices will the respond and deliver the MAC-Address of the gateway to the PC1.   
   My role as the „man in the middle“, is to pretend that I am the default gateway, so that the data traffic from and to the internet is send to me. So i give the other devices my MAC-Adress, which is the same as the gateway and they will write that down in their ARP table. From then on the data traffic to the internet is send to my device.
3. As the „man in the middle“ i send an ARP-request to the other devices in the network. After that I will get the ARP-Reply of the other devices and with that the MAC-Adress of the gateway. Then I respond with an ARP-Reply. In this reply, I send my MAC-Address which is the same as the gateway. The other devices update their ARP-table and write down my MAC-Address. From now on all traffic that is send to the gateway is send to me as well. So I am able to read their data.   
     
   1. ARP-Request from the Attacker to the other devices

2. ARP-Reply from the other devices

3. ARP-Reply of the attacker with the wrong MAC-Address

4. The other devices update their ARP-table

5. The data of the other devices to the router can be listened to from now on.

Q2)

Part 1)

1. *What is significant about the contents of the destination address field?*

Significant is, that the destination address is 12 byte long. In this example the address is the broadcast address, so its 12 times the f (ff:ff:ff:ff:ff:ff)

1. *Why does the PC send out a broadcast ARP prior to sending the first ping request?*  
   The PC needs to know the gateway. Fort hat he needs to send an ARP-Request, that he gets the MAC-Address of the gateway.
2. *What is the Vendor ID (OUI) of the Source’s NIC?*

The Vendor ID is: f4:8c:50

1. *What portion of the MAC address is the OUI?*

It is the half oft he MAC address

1. *What is the Source’s NIC serial number?*

The serial number is: 62:62:6d

Part 2)

* 1. H3-eth0 : IP Address: 10.0.0.13 MAC-Address: e6:94:a8:4a29:6b
  2. *What is the IP address of the default gateway for the host H3?*

10.0.0.1

* 1. *What is the MAC address of the PC’s NIC?  
     e6:94:a8*

*What is the default gateway’s MAC address?*

*d2:04:6f:15:a9:33*

* 1. *What type of frame is displayed?*IPv4
  2. *What is the source IP address?*

10.0.0.13

What is the destination IP address?

10.0.0.1

* 1. Source: e6:94:a8:4a:29:6b

Destination: d2:04:2f:15:a9:33

* 1. Source: 10.0.0.13

Destination: 172.16.0.40

* 1. Because it is the MAC-Address of the gateway, where the request leaves the local network
  2. It is not displayed in Wireshark because it’s handled by the hardware (the network card) and never passed up to the software.

Q3)

Part 1)

1. What is Nmap?

Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

1. What is nmap used for?

While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

1. What is the nmap command used?

to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

1. What does the switch -A do?

Enable OS detection, version detection, script scanning, and traceroute

1. What does the switch -T4 do?

Set timing template (higher is faster)

1. Which ports and services are opened?

21/tcp open

22/tcp open

23/tcp open

1. For each of the open ports, record the software that is providing the services.  
   ftp, ssh, telnet
2. Which network does your VM belong to?

/24 -> 10.0.2 network

1. How many hosts are up?  
   1 host
2. What is the purpose of this site?  
   To learn more about nmap and to be able to scan the site
3. Which ports and services are opened?

Port 22 tcpwrapped

Port 80 http

Port 9929 nping-echo Nping echo

Port 31337 tcpwrapped

1. Which ports and services are filtered?

None but in the example:

135/tcp filtered msrpc

139/tcp filtered netbios-ssn

445/tcp filtered microsoft-ds

593/tcp filtered http-rpc-epmap

4444/tcp filtered krb524

1. What is the IP address of the server?   
   45.33.32.156
2. What is the operating system?

Service Info: OS: Linux;

1. Nmap is a powerful tool for network exploration and management. How can Nmap help with network security?

How can Nmap be used by a threat actor as a nefarious tool?

Nmap helps with network security by identifying active hosts, open ports, and potential vulnerabilities, allowing administrators to secure their systems.  
However, threat actors can use Nmap to scan networks, gather information, and find weaknesses to exploit in attacks.