1. Blocking FTP is a good idea because FTP is an insecure protocol. Credentials are sent over the wire in the clear(evident in the pcap file), thus allowing an attacker to easily compromise the machine. If FTP is needed, FTPS is a better option since its traffic is encrypted with SSL.

2. This question is a bit tricky. A machine on a virtual subnet will report x.x.x.1 (with x.x.x being the CIDR block of the specific subnet) as the DNS server. However, on any VMWare subnet, x.x.x.1 is reserved for the VMware host machine. All VMWare does is forward DNS queries from VMs to the host's DNS servers. In this case, while a VM will report x.x.x.1 as the DNS servers, they're actually using the UDel DNS servers.

3. The port scan will tell us which ports are open. From this we can tell if the firewall is configured properly (extraneous open ports increase attack surface and it's best practice to close unused ports.) Specifically, this scan tells us that the firewall is configured correctly and will only allow Web traffic and DNS packets out.

4. pfSense is configured by default not to reply to pings or port scans from the WAN. This is done as a security measure and to make an attacker's job harder. Ping is disabled to prevent a DDoS attack and to prevent a would-be attacker from learning about the installation. pfSense will also not reply to port scans for the same reason; nmap scans can give an attacker valuable information about a target.