CNSP Fall Hackathon- NOV 2016

The Challenge:
A network trace with attack data is provided. (Note that the IP address of the victim has been changed to hide the true location.) Analyze and answer the following questions:

1. Which systems (i.e. IP addresses) are involved? (2pts)
2. What can you find out about the attacking host (e.g., where is it located)? (2pts)
3. How many TCP sessions are contained in the dump file? (2pts)
4. How long did it take to perform the attack? (2pts)
5. Which operating system was targeted by the attack? And which service? Which vulnerability? (6pts)
6. Can you sketch an overview of the general actions performed by the attacker? (6pts)
7. What specific vulnerability was attacked? (2pts)
8. What actions does the shellcode perform? Pls list the shellcode. (8pts)
9. Do you think a Honeypot was used to pose as a vulnerable victim? Why? (6pts)
10. Was there malware involved? Whats the name of the malware? (We are not looking for a detailed malware analysis for this challenge) (2pts)
11. Do you think this is a manual or an automated attack? Why? (2pts)