PV204 – FIREWALLS ASSIGNMENT [10 POINTS]

Write a set of rules for your Linux personal firewall on your laptop. Assume that you have just one Ethernet interface named eth0 and the firewall will use just default table "filter". The firewall should have the following functionality:

1. Default policy set to DROP.
2. Allowed access to loopback interface.
3. Allowed ICMP messages that are really necessary for fully working of ping and traceroute from/to laptop.
4. Allowed Web traffic (including DNS requests and https).
5. Opened ports for FTP and Samba.
6. Allowed a SSH connection to laptop, but just from your university server IP (let's say 147.251.48.155).
7. Logged incoming access from all reserved addresses (spoofing alerting).

Note 1: The assignment requires a little bit of searching what exactly you need to allow and/or block.

Note 2: Put to the IS just the shell script with appropriate iptables commands (and comments).