04. Network Security Hardening

Part 1: Select up to three hardening tools and methods to implement
1) Port Filtering: This method allows in and out traffic to be controlled. This is one of the most effective ways to disrupt and block unwanted traffic going inside the network and potentially causing damage and infiltration. Prepared By: Burak Kılıç 2) Disabling Unused Ports: Unused ports are gateways of hackers to get inside the network. Any unused ports should be shutdown. 3) Penetration Test: This test is done to foresee the potential vulnerabilities in the security system and address them before they are exploited.

Part 2: Explain your recommendations
1- Port Filtering is one of the main security measures to stop attackers from getting inside. In this case, firewall is used to block certain ports and only specific traffic from specific ports are allowed. 2- If unused ports in Routers, Switches, Servers are not shut down, it will be a huge vulnerability for the security. These ports invite hackers unless they are blocked. 3- Penetration testing is one of the best ways to understand whether there is a potential security breach that could be exploited by hackers in future. It is arguably the best way to detect vulnerabilities and incoming potential attacks.