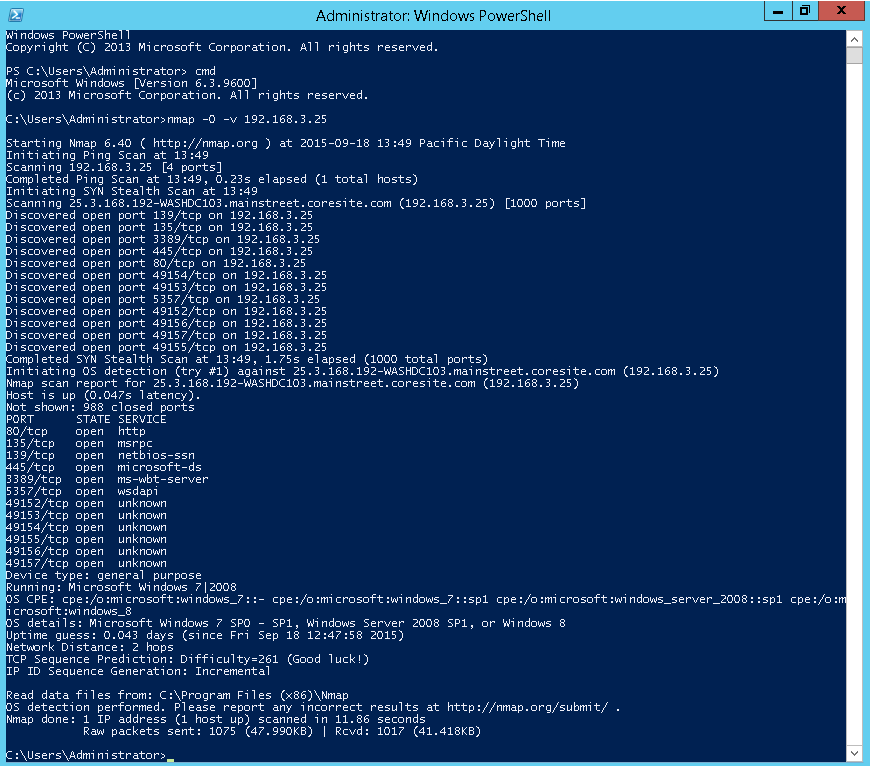
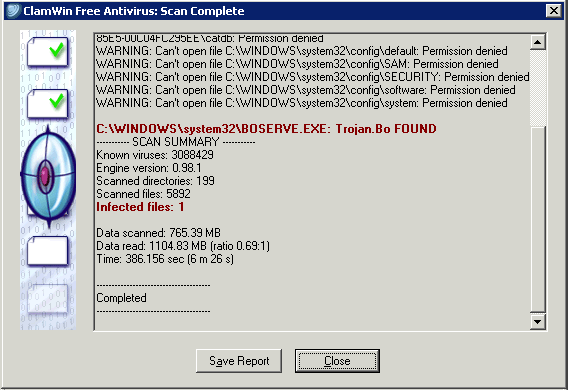
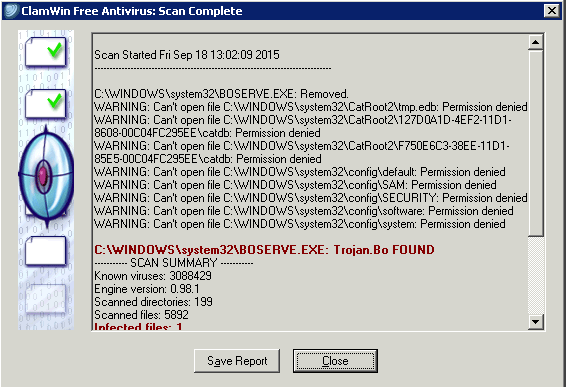
**Lab Report**

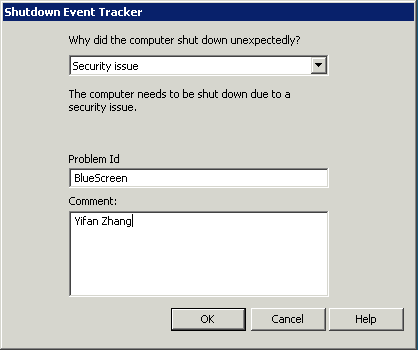
# Nmap –O –v 192.168.3.25



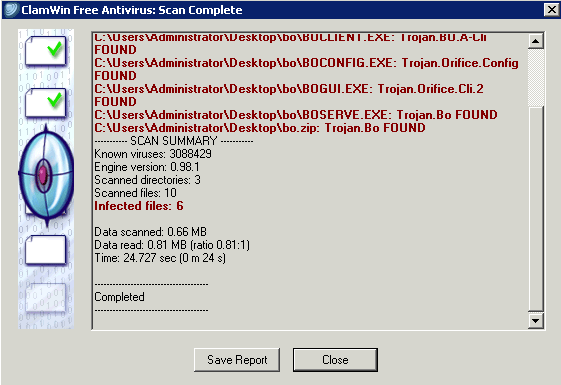
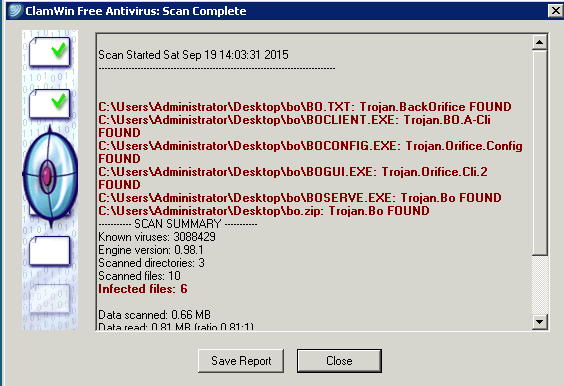
# ClamWin system32 folder scan result



# Shutdown Event Tracker



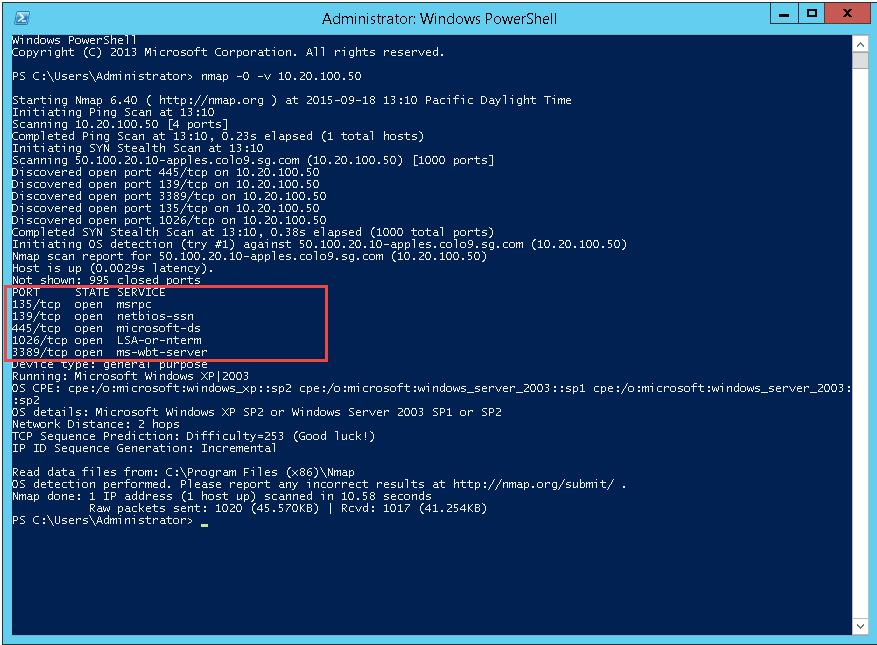
# ClamWin desktop folder scan result



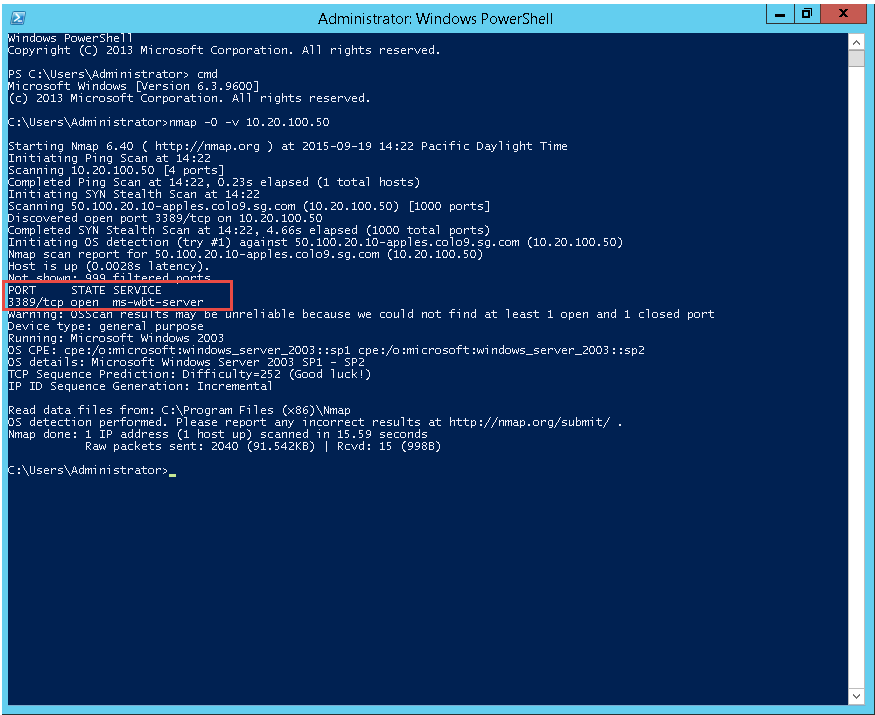
# Nmap scan results and the reduced attack surface

1. **Nmap –O –v 10.20.100.50**

Before applying Firewall



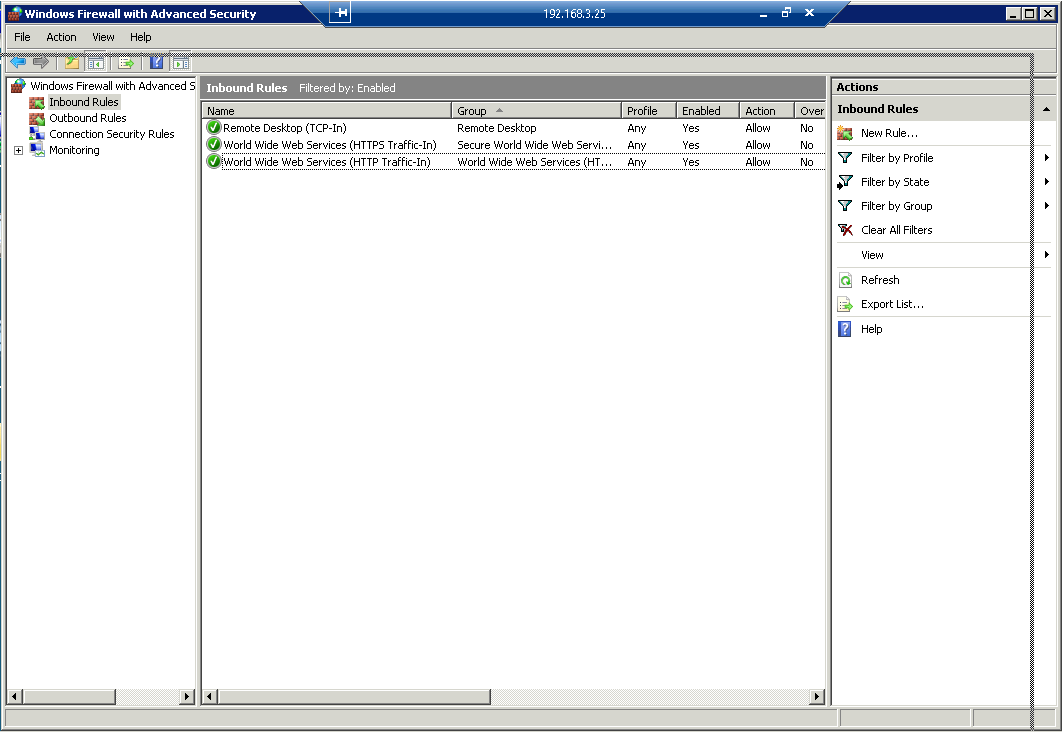
After applying Firewall



**Explanation:**

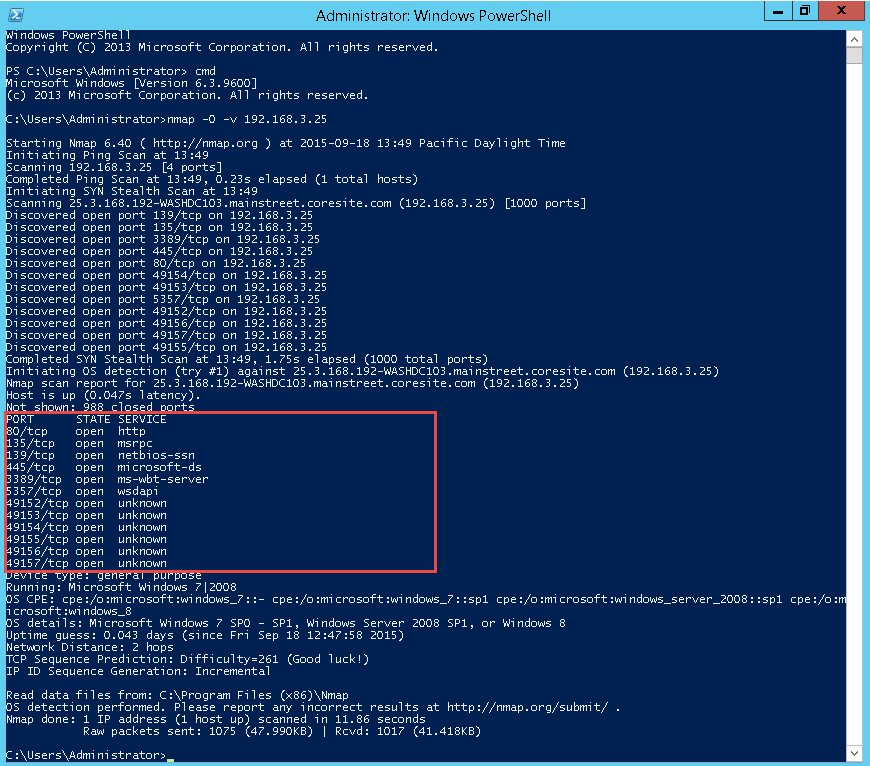
Before we apply the firewall, we could see that there are 5 ports are open for services on machine IP 10.20.100.50. And, after there are only 1 port left. The more ports open for services, the more risky a server is. The reason is that attackers could use these ports to communicate between their local machine and target server. The most common exploit is to send tremendous data through these open channels.

1. **Enabled Inbound Rules**

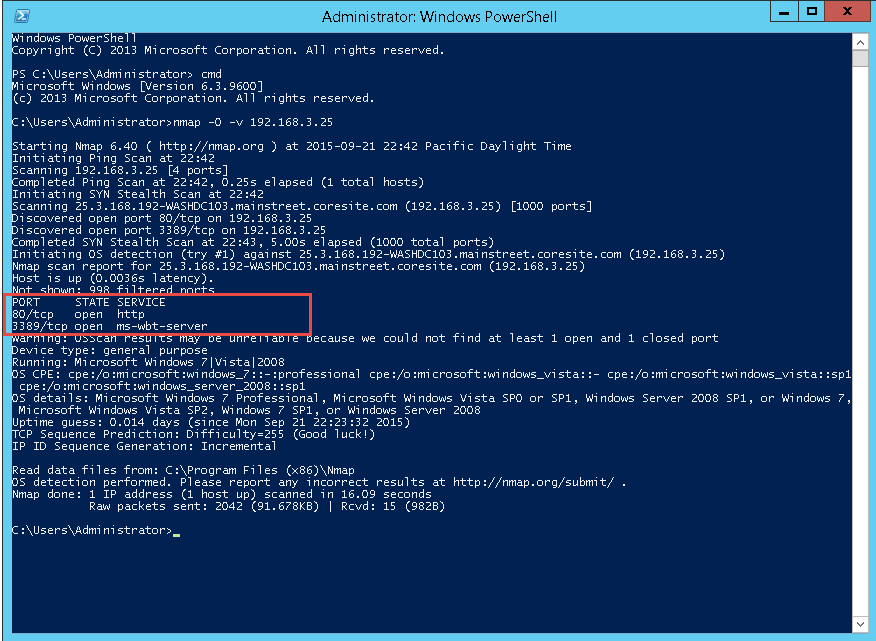


1. **Nmap –O –v 192.168.3.25**

Before applying firewall



After applying Firewall



**Explanation:**

Same as the previous analysis in section 5.1, the firewall blocked the majority ports existing on machine IP 192.168.3.25. And, this action could reduce a lot of the hacking risks because hackers could utilize these open ports to implement an attack to targets. For example, some hackers could use DDos or DoS technique to attack these ports, which makes the services are not available to end user. However, using this way to harden system has an obvious side-effect that when service ports are blocked, both normal user and hackers could not use it any more. Thus, a more wise way to do that is to refine the filtering rules instead of disable them all.