Challenge Lab 2 Report

Question Description:

Nmap command could probe a firewalled network in a stealthy manner. Explain how the command works.

Answer:

Nmap tools provide numerous switches to detect and investigate the overall network environment. In this challenge part, we want to scan 172.30.0.0/24 stealthily which means that there will be no records of the scan left in target system.

After some research, I found that there are several switches related to stealthy scanning and the first switch is –sS. So, therefore we use the command Nmap –sS 172.30.0.0/24. With the –sS option, Nmap will not create a session and will not leave records in application logs. And, for this switch, we can get information without completing TCP handshake process.

However, sometimes although –sS option doesn’t need complete TCP handshake process, it will be filtered by firewall. In order to bypass firewall or avoid firewall’s detection, we can use –sF option which may help us bypass firewall’s IDS and IPS scans.

Reference:

infosecinstitute. (2012, 7 18). *Nmap from Beginner to Advanced*. Retrieved 9 24, 2015, from infosecinstitute.com: http://resources.infosecinstitute.com/nmap/