STM

Practical Assignments

Q.1. Install pfSense, Squid proxy and Squidguard proxy. Configure web filtering as below.

Create a sales user. Allow this user to access all social networking sites, gmail and live email sites. Block all other sites.

Create a developer user. Allow this user access to RedHat, Microsoft, Google, Oracle, IBM, AWS cloud sites. Block all other sites.

For all other users allow only banking sites, google and government sites. Block all other sites.

Also block searches for following words for all users

Torrent, movies, cricket, football, sports, hacking

Q.2. Install pfSense. Install snort on it. Configure it as an inline IPS. Block following activities.

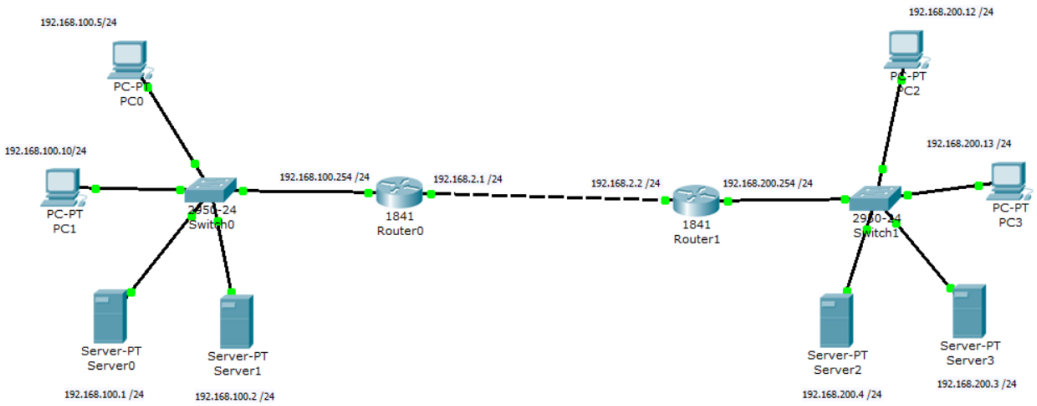
A. If kali linux site is accessed.
B. If metasploit is accessed
C. If SSH to AWS cloud is detected
D. If remote desktop to remote Windows machine is detected

Q.3. Install and configure OpenVPN server on pfSense and allow sam and Tina to remotely access the network.

Q.4. Configure following in the Firewalld on a VM with 2 network cards.

A. Open tcp ports - 80, 110, 25 and 3389 in internal zone.
B. Shift second interface to internal zone.

Q.5. Configure access list for following network.



A. Entire 192.168.100.0 network should be able access the website on Server2.
B. Only PC1 should be able to access the website on Server3
C. PC0 should be able to ping to any PC/Server in 192.168.200.0 network.
D. PC2 should be able to access website on Server0.
E. PC3 should be able to access website on Server1.
F. PC3 should be able to ping to any PC/SERVER in 192.168.100.0 network.