Name: Hemant Jain

Lab Progress Report Due Date: 2/22/2021

Current Week Since Start Date: Week 5 (2/23/2021– 2/29/2021)

Reporting Week: From Feb 18, 2021 to Feb 22, 2021

Summary about the TestOut Module-5 Learning:

From the TestOut LabSim, I learnt about the Security Zone Facts and how the portions of the network or system that have specific security concerns. Security Zone Networks types namely includes wireless, guest, honeynet and ad hoc. The common zones are likely Intranet, Internet, Extranet, Wireless and Demilitarized zones(DMZ). Interesting I came across the Proxy Servers which is a type of firewall that stands in between clients requesting resources from other servers. The Internet content filter had two types of configurations: Allow All or Block All. Parental controls which are likely used by parents at home to monitor their child activities on Internet.

Network Access Control (NAC) controls the access into the network by not allowing the computers from unknown sources to connect-over. DMZ is a buffer network that is located between a private network and untrusted network, such as the Internet. Others are like Bastion, Screening routers , Dual-homes gateway, Screened host gateway, Screened Subnet. Reading about the Firewall Facts, Functions and what key role firewall plays out in the VPN and private internal connection networks. Learning about the different firewall types likely Packet-Filtering(Stateless) makes decisions about which network traffic to allow by examining information in the IP Header, such as source and destination addresses etc. Stateful firewalls makes the decision based on virtual circuits or sessions stored.

Application firewall layer also called Application-level gateway makes security decision based on information contained within the data portion of a packet. Common features offered by firewalls were Blocking ping to WAN, Stealth mode, TCP Flood, UDP flood, ICMP Notification, Fragmented Packets, SYN Flood Detect Rate, Echo Storm Detect Rate, ICMP Flood Detect Rate. Learning about Web Threats and Protection methodologies available to prevent it was great.

Web filters are the content filter that prevents out the users from visiting the restricted websites. Web threat filters out the preventing users from visiting the websites with known

malicious contents. Spam and Spam filters are widely in MNC's to avoid the spamming of the employees. And to resist or prevent it we have software that scans content to identify and dispose of the phishing contents using the Anti-Phishing Software. Web threat protects both the hardware and software using one of the protection mechanisms namely: Website/URL content filtering, Web threat filtering, Gateway email spam filters, Virus scanners, Anti-Phishing software, Data loss prevention, Encryption, and Proxies.

Learnt how to identify the passive attack from an active attack. What areas of your networks you should be focusing around to prevent the Network threats and how segmenting helps in increasing your network security? Network segmentation is the main component of secure network-architecture. Logic behind it is a system or systems were compromised, the damage would be limited to that network segment only. It makes it much easier to identify the suspicious network traffic since the traffic is broken into manageable chunks. Threat focus points includes the Entry points, Inherent vulnerabilities, documentation, and network baselines.

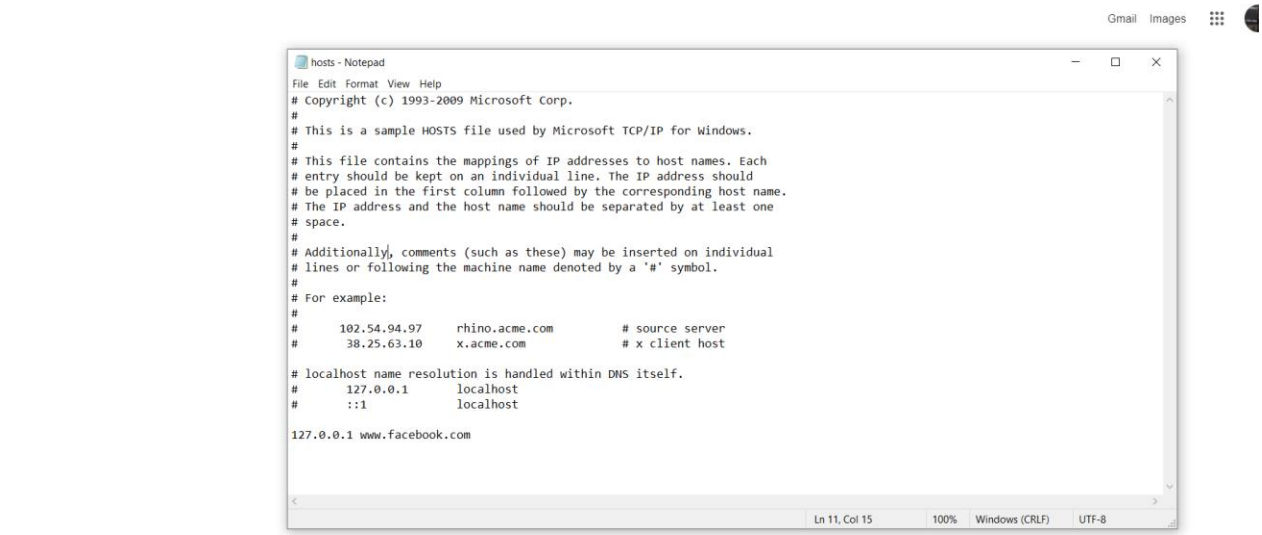
In the end modules it summarized the network flow and packet flow of the packets in the intern-network connected domains across routers and switches. Defining the VLAN (Virtual LAN) network which is the collection of devices that belong together and act as if they are connected to the same wire or physical switch.

Discussing about both the aspects of VLAN Advantages and disadvantages was nice learning giving users the complete share-view about the VLAN before proceeding with it ahead. Creating VLAN with switch offers benefits like easy administration, less expensive and higher performances. Router Security includes discussion about Change factory results, use secure protocols, implementing physical security, Securing the configuration files, Update firmware and use anti-spoofing rules.

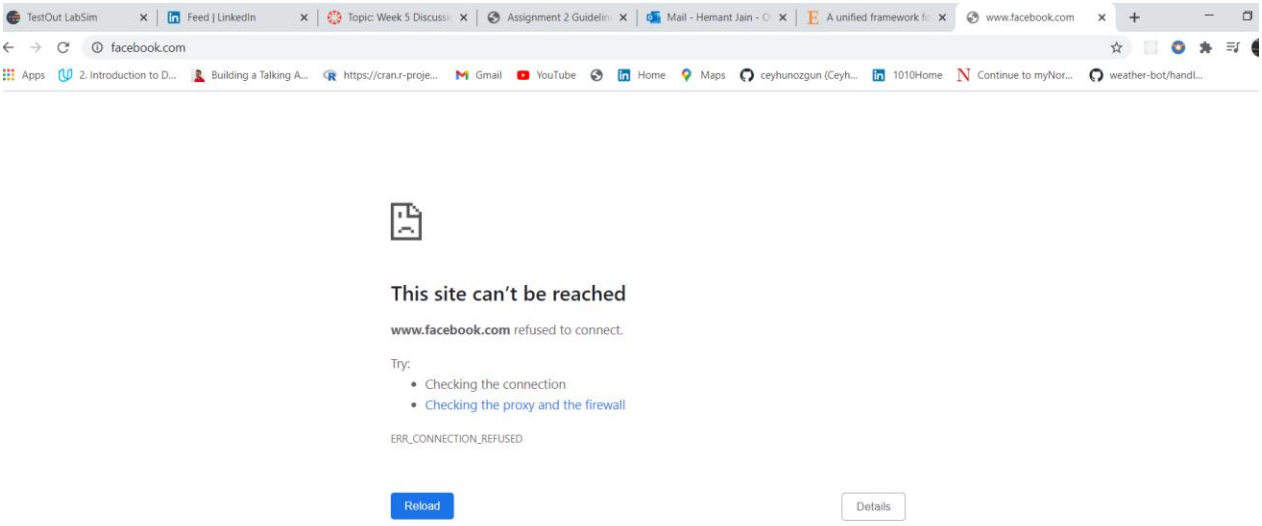
In-class Lab Homework:

SMAC Lab Screenshots:

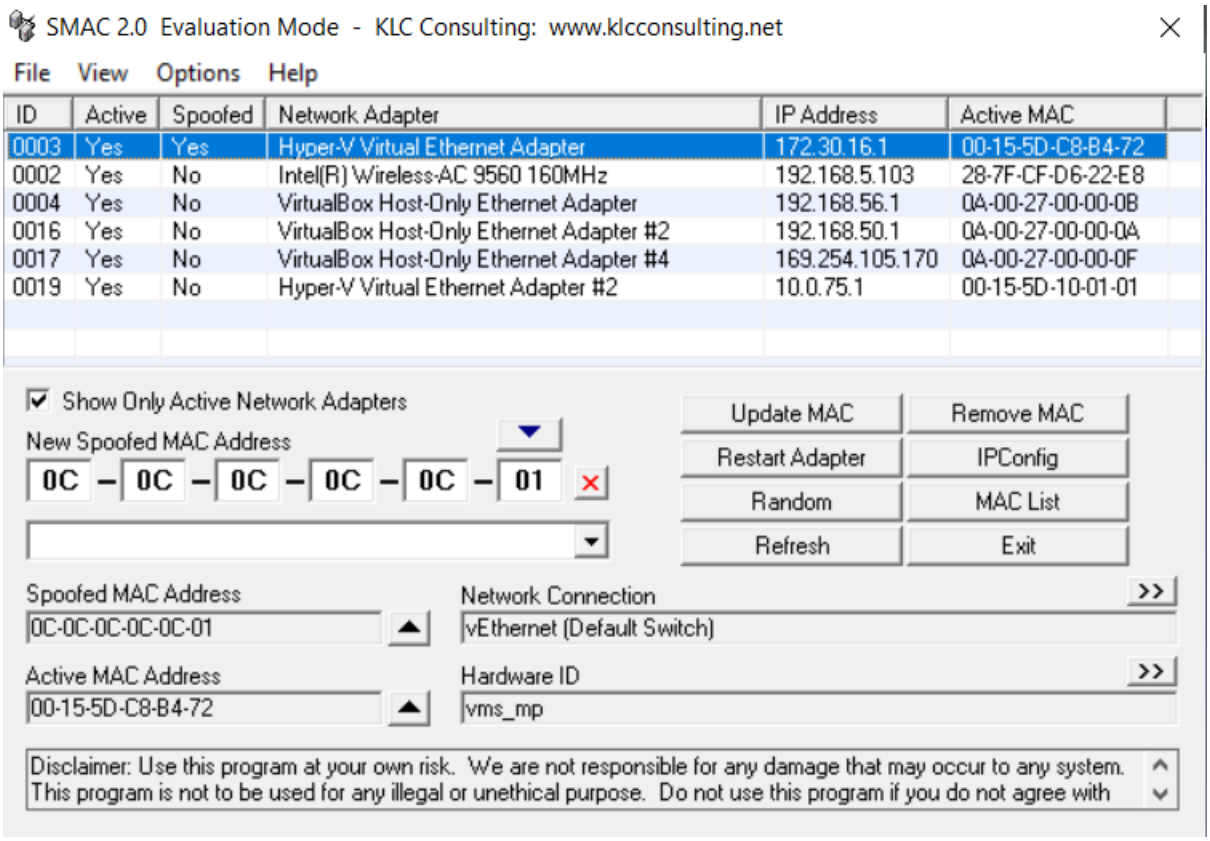
1. /hosts file – Edited out with the block connection for www.facebook.com URL from localhost



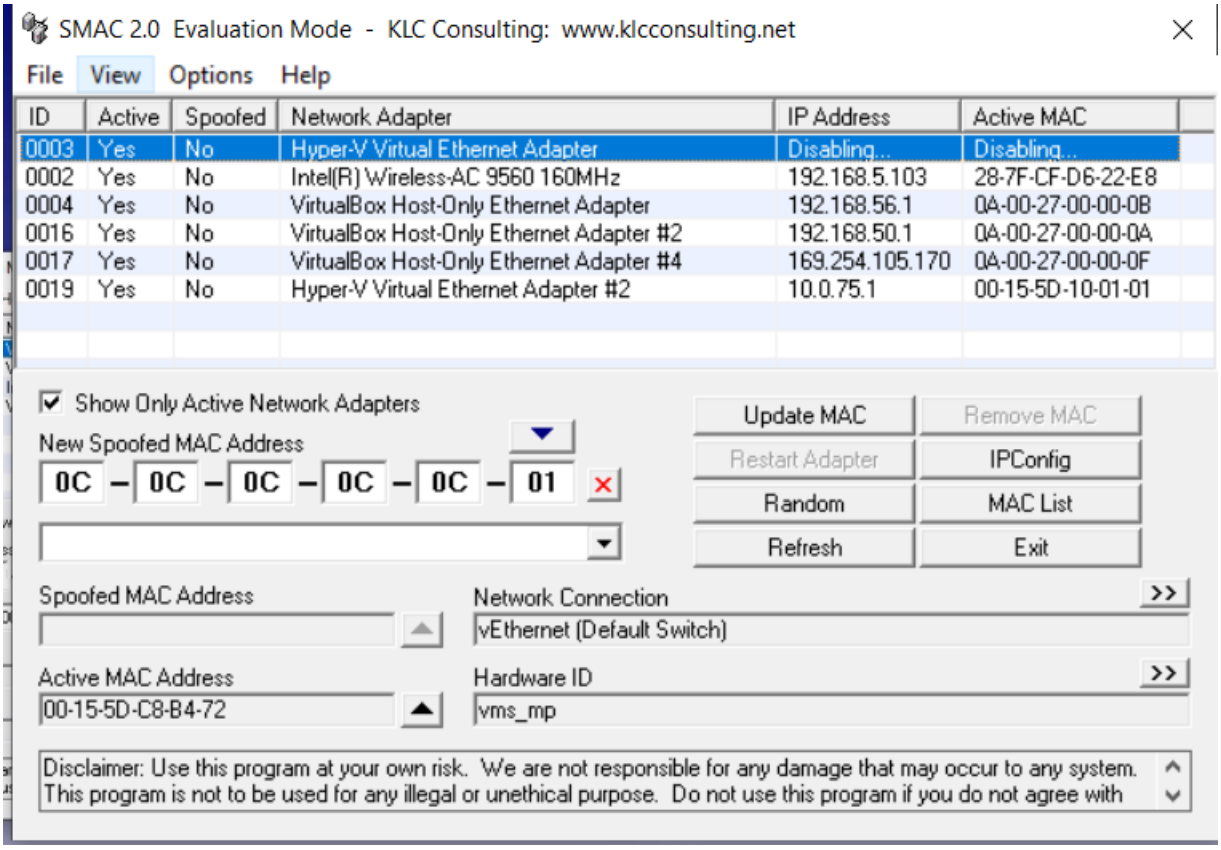
2. www.facebook.com URL was unreachable as it was blocked in the above hosts file



3. SMAC Tool with the SMAC Spoofing of the MAC URL with dummy Network MAC.



4. Disabling the dummy Spoofed MAC URL to the original MAC address of the computer.



Progress Embedded Image of Progress Report from LabSim:

4.2.9 Section Quiz	59 seconds	100% (2/15/2021 5:33…	100% (2/15/2021 5:33…
4.3.5 Configure NTFS…	7 minutes 10 seconds	100% (2/15/2021 5:46…	100% (2/15/2021 5:46…
4.3.6 Disable Inherita…	2 minutes 12 seconds	100% (2/15/2021 5:48…	100% (2/15/2021 5:48…
4.3.7 Section Quiz	1 minute 8 seconds	100% (2/15/2021 5:35…	100% (2/15/2021 5:35…
4.4.6 Section Quiz	1 minute 32 seconds	100% (2/15/2021 5:37…	100% (2/15/2021 5:37…
5.1.7 Configure a Sec…	12 minutes 10 seconds	100% (2/21/2021 8:15…	100% (2/21/2021 8:15…
5.1.8 Configure Netw…	4 minutes 42 seconds	100% (2/21/2021 8:22…	100% (2/21/2021 8:22…
5.1.10 Configure QoS	14 minutes 42 seconds	100% (2/21/2021 8:39…	100% (2/21/2021 8:39…
5.1.13 Section Quiz	11 minutes 36 seconds	100% (2/21/2021 10:5…	100% (2/21/2021 10:5…
5.2.3 Configure a DMZ	5 minutes 2 seconds	100% (2/21/2021 8:45…	100% (2/21/2021 8:45…
5.2.5 Section Quiz	1 minute 49 seconds	100% (2/21/2021 11:0…	100% (2/21/2021 11:0…
5.3.5 Configure a Peri…	7 minutes 55 seconds	100% (2/21/2021 8:54…	100% (2/21/2021 8:54…
5.3.6 Section Quiz	2 minutes 38 seconds	100% (2/22/2021 12:2…	100% (2/22/2021 12:2…
5.4.3 Configure NAT	4 minutes 37 seconds	100% (2/21/2021 9:00…	100% (2/21/2021 9:00…
5.4.5 Section Quiz	59 seconds	100% (2/21/2021 10:1…	100% (2/21/2021 10:1…
5.5.4 Configure a Re…	11 minutes 36 seconds	100% (2/21/2021 9:13…	100% (2/21/2021 9:13…
5.5.5 Configure a VP…	6 minutes 14 seconds	100% (2/21/2021 9:20…	100% (2/21/2021 9:20…
5.5.8 Section Quiz	7 minutes 10 seconds	90% (2/20/2021 8:24 …	90% (2/20/2021 8:24 …

Resource	Time In Resource	Newest Score	Highest Score
5.6.3 Configure URL …	11 minutes 42 seconds	60% (2/22/2021 11:30…	60% (2/21/2021 9:25 …
5.6.5 Section Quiz	1 minute 8 seconds	100% (2/21/2021 10:1…	100% (2/21/2021 10:1…
5.7.3 Section Quiz	1 minute 44 seconds	100% (2/21/2021 10:4…	100% (2/21/2021 10:4…
5.8.3 Section Quiz	2 minutes 14 seconds	100% (2/21/2021 10:3…	100% (2/21/2021 10:3…
5.9.6 Secure a Switch	2 minutes 37 seconds	100% (2/21/2021 9:33…	100% (2/21/2021 9:33…
5.9.7 Section Quiz	1 minute 18 seconds	100% (2/21/2021 10:3…	100% (2/21/2021 10:3…
5.10.4 Section Quiz	4 minutes 24 seconds	90% (2/21/2021 10:23…	90% (2/21/2021 10:23…
5.11.6 Spoof MAC Ad…	6 minutes 13 seconds	100% (2/21/2021 9:40…	100% (2/21/2021 9:40…
5.11.9 Harden a Switch	6 minutes 44 seconds	100% (2/21/2021 9:47…	100% (2/21/2021 9:47…
5.11.10 Secure Acces…	9 minutes 10 seconds	100% (2/22/2021 11:3…	100% (2/22/2021 11:3…
5.11.11 Secure Acces…	5 minutes 13 seconds	100% (2/22/2021 11:4…	100% (2/22/2021 11:4…
5.11.12 Section Quiz	3 minutes 13 seconds	100% (2/21/2021 10:1…	100% (2/21/2021 10:1…
5.12.4 Explore VLANs	30 minutes 43 seconds	100% (2/22/2021 4:00…	100% (2/22/2021 4:00…
5.12.5 Section Quiz	1 minute 29 seconds	100% (2/21/2021 10:1…	100% (2/21/2021 10:1…
5.13.5 Restrict Telnet …	2 minutes 30 seconds	100% (2/22/2021 12:1…	100% (2/22/2021 12:1…
5.13.6 Permit Traffic	42 seconds	100% (2/22/2021 12:1…	100% (2/22/2021 12:1…
5.13.7 Block Source …	1 minute 54 seconds	100% (2/22/2021 12:2…	100% (2/22/2021 12:2…
5.13.8 Section Quiz	2 minutes 43 seconds	100% (2/22/2021 3:46…	100% (2/22/2021 3:46…