Project A – OS and Networking

By: Malcolm Brown

Executive Summary

- Upgrading a client's IT system by installing:
 - New firewall, CEO PC, Webserver, DNS server,
 - and some Linux machines for monitoring and conducting cybersecurity related tasks.

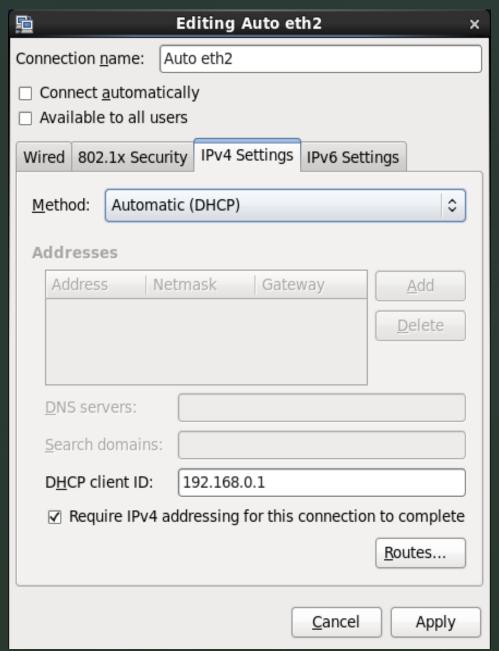
Execution: What I Created

- Created and configured virtual machines with new network.
- Creating a new user account on the web server.
- Verified trusted network can't be pinged by untrusted network.
- Designed security baseline for the server.
- This reduced cost and met client's operational needs.

Problems Identified and Their Resolution

Problem	Solution
 Initally couldn't connect to internet on CEO's PC 	Manually configured the correct IP and DNS Server address
- IPv4 settings misconfigured.	 Fixed network inconnection problem Able to visit "www.seclab.net" with firefox afterwards.

Problems Identified and Their Resolution – Cont'd



Problems Identified and Their Resolution – Cont'd

Problem	Solution
Unable perform port scans on DNS, webserver in Kali Linux.	 Utilized "sudo su" command. Perform port scans on the DNS, Web servers.

Problems Identified and Their Resolution – Cont'd

```
kali@kali: ~
                                                                  _ _ X
File Actions Edit View Help
       valid_lft forever preferred_lft forever
kali@kali:~$ nmap -s0 10.200.0.11
You requested a scan type which requires root privileges.
OUITTING!
kali@kali:~$ nmap -sS 10.200.0.11 -0
You requested a scan type which requires root privileges.
QUITTING!
kali@kali:~$ sudo -s
[sudo] password for kali:
root@kali:/home/kali# nmap -sS 10.200.0.11 -0
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-01 19:17 EST
Nmap scan report for ns1.seclab.net (10.200.0.11)
Host is up (0.00071s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 2 hops
OS detection performed. Please report any incorrect results at https:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds
root@kali:/home/kali#
```

Recommendations

- Update Firewall software periodically.
- Use secured passwords.
- Company wide password resets every 6 months.

Thanks!! Any Questions!