**Cape Coral Technical Cyber Lab**

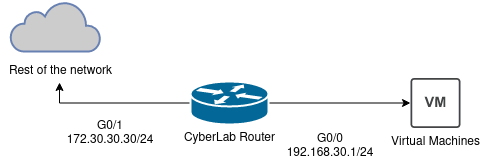


**Author: Jaden Dossous**

**Overview**

The cyberlab here at CCTC is a place for aspiring Cybersecurity profressionals to practice their RedTeam and BlueTeam skills. With mutiple vunerable machines and a SIEM to detect attacks, it is perfect platform to build both skillssets.

The way the CyberLab stands now is that the CyberLab router is connected to *Frenchie* through G0/1 and connected to the *ESXi server* through G0/0.



**Security Onion**

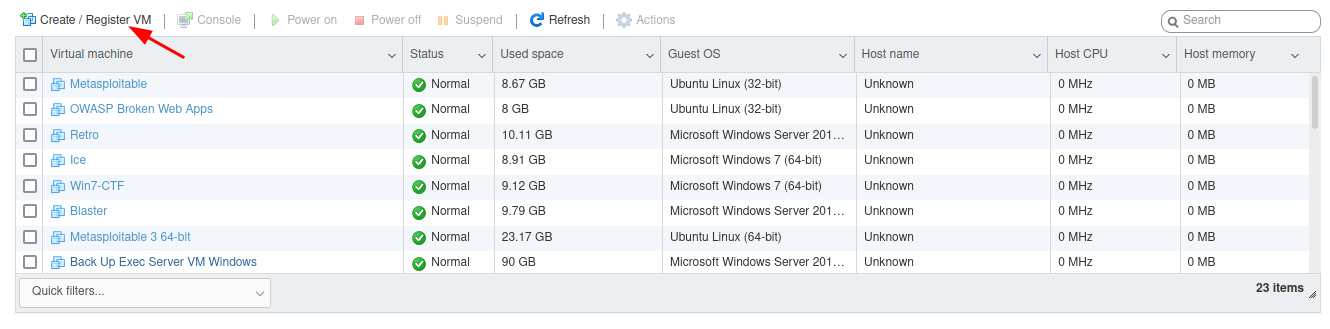
Security Onion is the SIEM option used in the CyberLab it has two NICs one for mananment and the other for capturing traffic mirrored to from Frenchie on port G0/20. The **mananment IP is 192.168.30.10**

**Configuration**

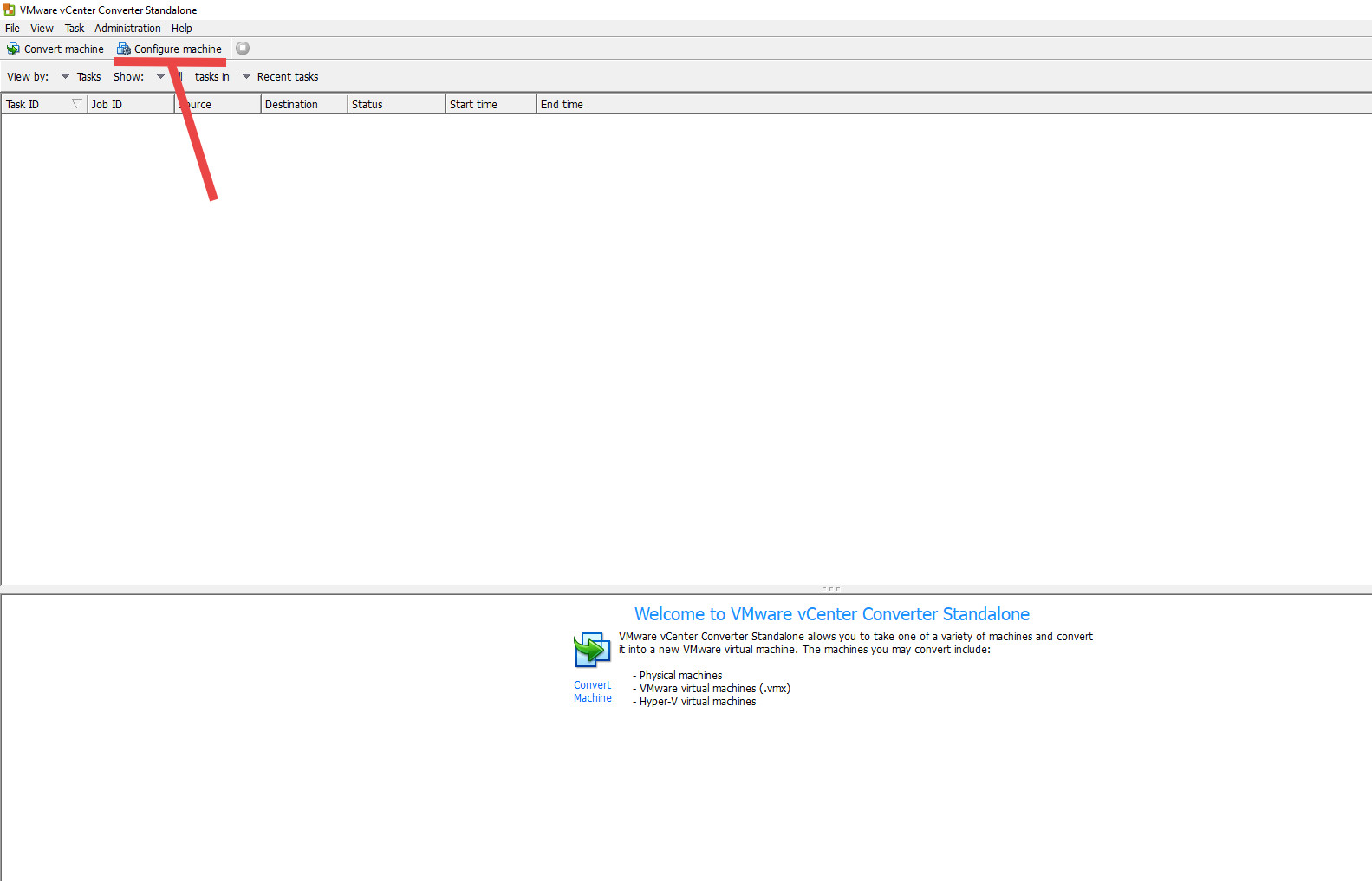
There are multiple parts to lab, thankfully the vital componets should aleady be configured for you. ESXi and the Router don’t need much mainting beyon updates and slight tweaks to fit what is desired. The routers entire config is saved at the end of this file and would only need to transfered to the router.

**Adding Virtual Machines**

Adding virtual machines can be relativly easy depending on the file format.If its a .ova or .iso it can be uploaded and configured within ESXi.



Follow the wizard to add the virtual machine

Now for .vmx/.vmhd to add the virtual machine you must convert it using vCenter Converter. This program is windows only so you have to use the windows machine in the phone lab. 

Once the menu opens change the source location to the second option *vmware workstation or other virtual machine.* Browse to the source and follow the rest of the wizard.

**Router Config**

Building configuration...

Current configuration : 1570 bytes

!

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname CyberLabRouter

!

boot-start-marker

boot-end-marker

!

!

no aaa new-model

!

!

ip cef

no ip dhcp use vrf connected

ip dhcp excluded-address 192.168.30.1

ip dhcp excluded-address 192.168.30.2

ip dhcp excluded-address 192.168.30.3

ip dhcp excluded-address 192.168.30.3 192.168.30.30

!

ip dhcp pool CyberLab

network 192.168.30.0 255.255.255.0

default-router 192.168.30.1

!

!

no ip domain lookup

ip domain name Netlab.local

ip auth-proxy max-nodata-conns 3

ip admission max-nodata-conns 3

!

multilink bundle-name authenticated

!

!

voice-card 0

no dspfarm

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

username admin privilege 15 secret 5 $1$g1ex$lqXTAQlEoTepp4nyGa0T8/

archive

log config

hidekeys

!

!

!

!

!

!

!

interface GigabitEthernet0/0

description Path to CyberLab

ip address 192.168.30.1 255.255.255.0

duplex auto

speed auto

!

interface GigabitEthernet0/1

description Port to Frenchie

ip address 172.30.30.30 255.255.0.0

duplex auto

speed auto

!

ip forward-protocol nd

ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1

ip route 10.0.0.0 255.255.255.0 GigabitEthernet0/1

ip route 172.30.0.0 255.255.0.0 172.30.30.1

!

!

ip http server

no ip http secure-server

!

!

!

!

!

!

!

control-plane

!

!

!

!

!

!

!

!

!

!

line con 0

logging synchronous

line aux 0

line vty 0 4

login local

transport input ssh

line vty 5 15

login local

transport input ssh

!

scheduler allocate 20000 1000

!

end

**CyberLab network Map**

METASPLOITABLE

Nmap scan report for 192.168.30.2

DVWA

Nmap scan report for 192.168.30.49

IGNITE

Nmap scan report for 192.168.30.32

WIN7-CTF

Nmap scan report for 192.168.30.38

ICE

Nmap scan report for 192.168.30.39

Downloads

\*\*https://github.com/digininja/DVWA.git\*\*

\*\*https://darkstar7471.com/resources.html\*\*