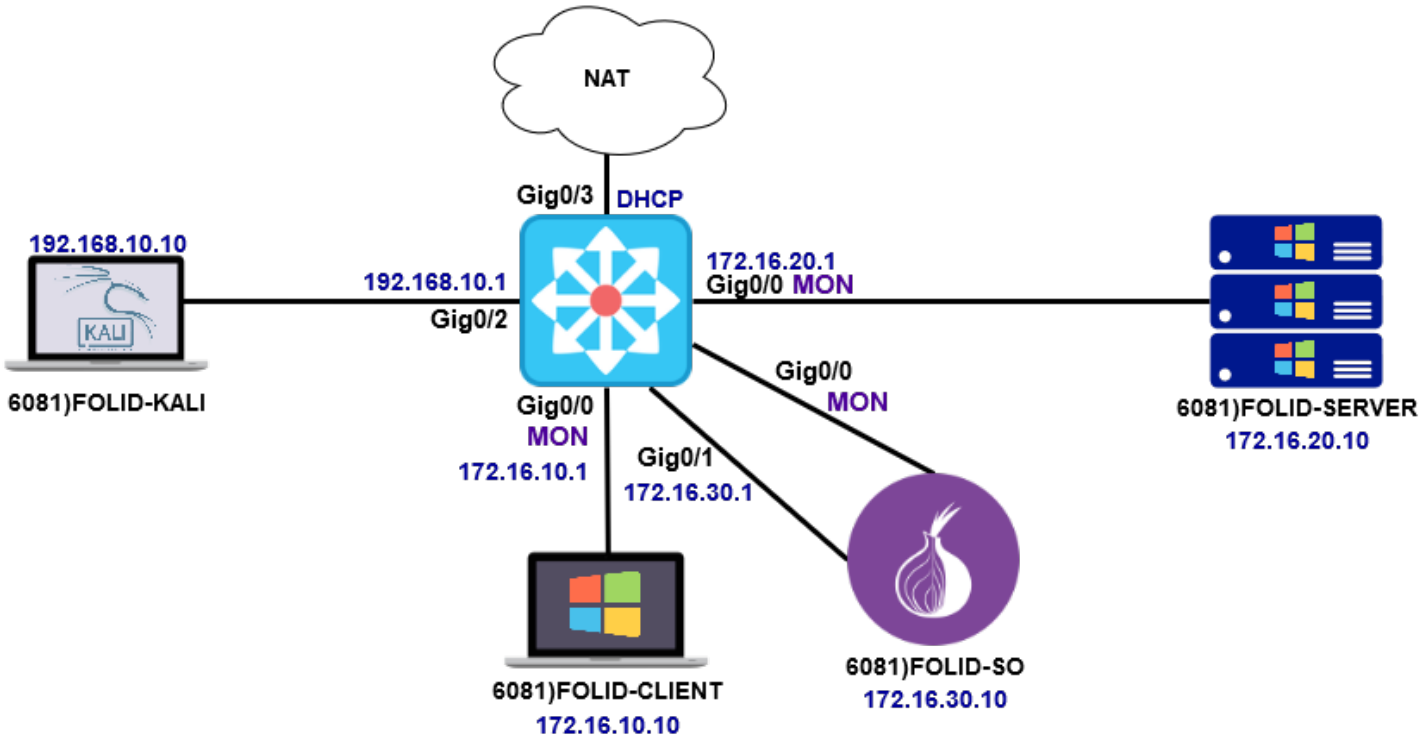
Lab 1 – Lab Environment Setup

Lab Topology and Learning Goals



In this lab you will setup your lab environment to simulate and monitor networks attacks

Required Resources

- **VMware Workstation 15**
- **VM Templates:**
  - **_Kali2020.1b**
  - **_SecurityOnion16.04.6.5**
  - **_Server2016(1607)GUI**
- **VM:**
  - **6081) Router**

Submission Instructions

Submit your completed lab to the appropriate lab quiz on FOL

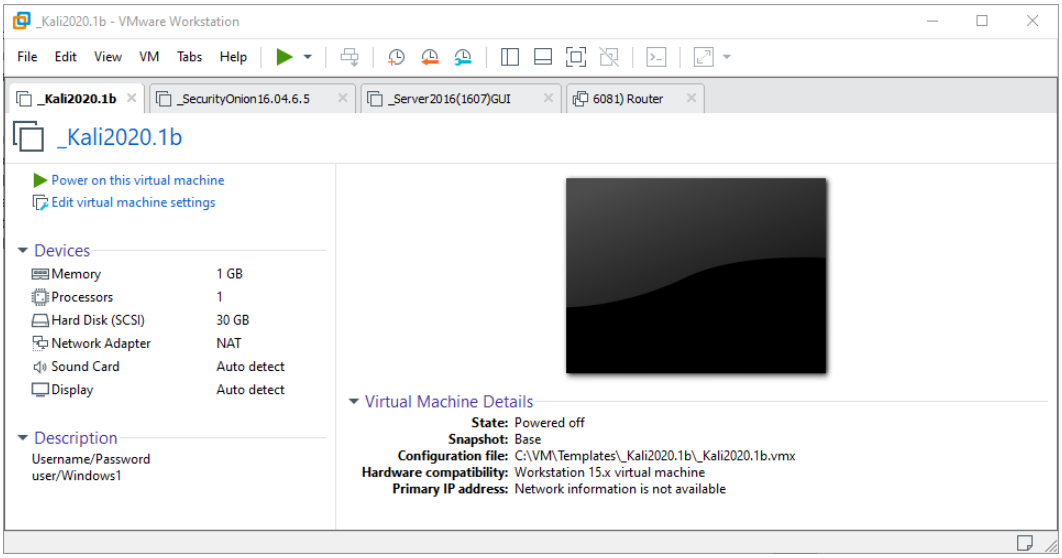
- You can attempt the quiz multiple time, but only the last attempt will be graded
- Submissions are accepted until 11:59 PM of the same day
- Submissions by email will not be accepted
- All screenshots must include you FOLID (where FOLID is your FOL username)

Lab 1 – Lab Environment Setup

Download and Import VM Templates

Download and extract the VM templates **_Kali2020.1b**, **_SecurityOnion16.04.6.5**, **_Server2016(1607)GUI**, and the VM **6081) Router**.

It is recommended that you store these files in a central location (like C:\VM). **Please ensure that they are stored on SSD storage**.

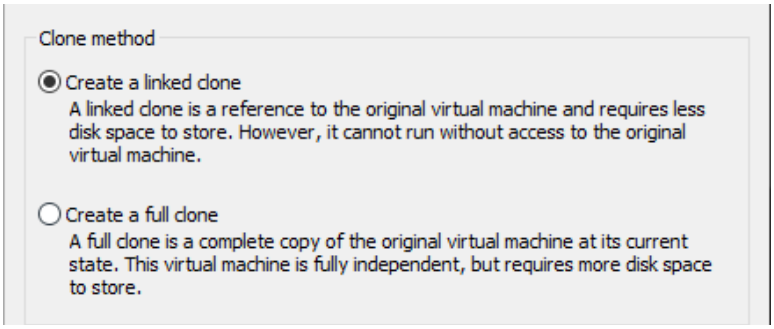


Import the templates into VMware Workstation, but do not power them on. The VM templates (identified by an _ before the name) are only for cloning and should never be powered on.

Lab 1 – Lab Environment Setup

Create Linked VM Clones

Using linked VM clones, we can use our template file in combination with linked clones to reduce the storage space that our lab setup requires.



Bring the **_Kali2020.1b** VM template to the foreground; from the **VM** menu, select **Manage**, then **Clone**. Move through the wizard and create a linked clone, with the following Virtual Machine Name: **6081)FOLID-KALI** *(where FOLID represents your FOL username)*

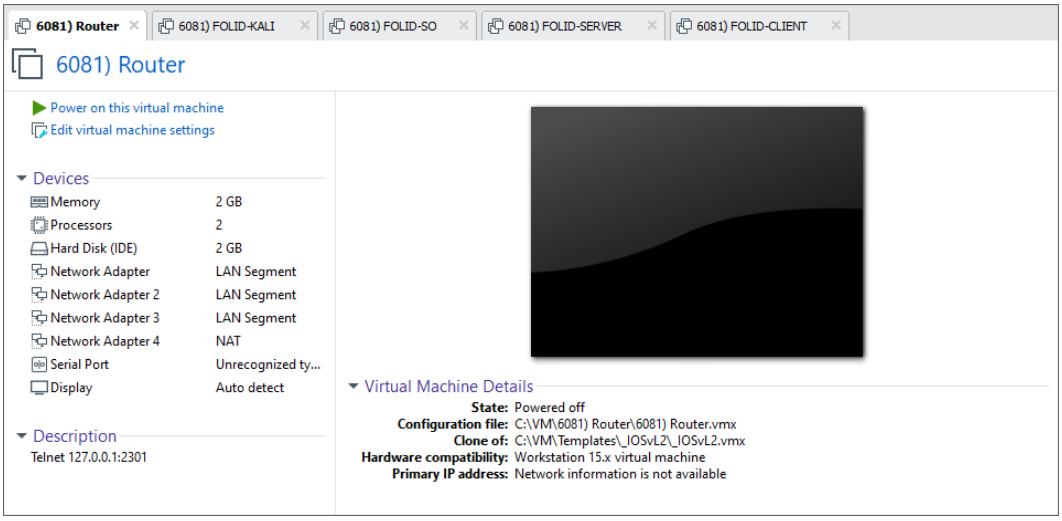
You can now close the template **_Kali2020.1b.**

Create the following linked clones from the other templates:

- **_SecurityOnion16.04.6.5**
  - 6081)FOLID-SO

* Modify the **6081)FOLID-SO** VM to have 6 GB of RAM.

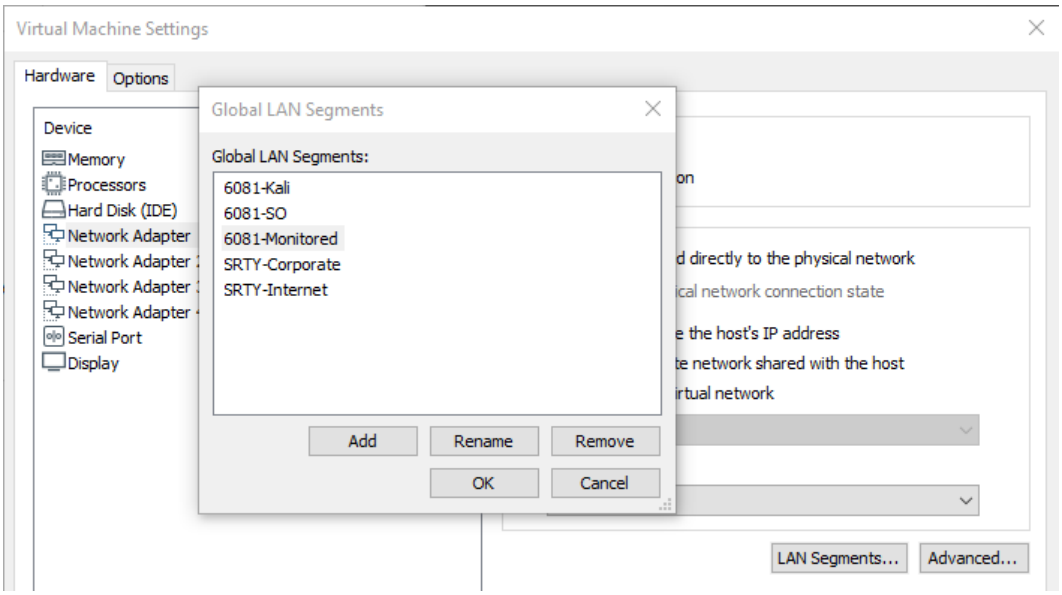
- **_Server2016(1607)GUI**
  - 6081)FOLID-SERVER
  - 6081)FOLID-CLIENT



Add a screenshot of your VMware Workstation windows that shows the name of each cloned VM to the Lab 1 quiz. Ensure that your FOLID is visible in all tabs.

Create LAN Segments

We will be using LAN segments to simulate and separate networks. Note, the logical topology provided at the start of the lab will differ from the physical topology of the environment. This removes the need to duplicate traffic on the router.



Open the VM settings for **6081)Router** and click on the first network adapter (**Network Adapter**). Click the **LAN Segments** button to edit the Global LAN Segments.

Create the LAN segments: **6081-Kali**, **6081-SO**, and **6081-Monitored**

Assign the following interface to their appropriate LAN segments:

- **6081)Router**
  - Network Adapter – **NAT** (*not a LAN segment*)
  - Network Adapter 2 – **6081-Monitored**
  - Network Adapter 3 – **6081-SO**
  - Network Adapter 4 – **6081-Kali**
- **6081)FOLID-Kali**
  - Network Adapter – **6081-Kali**
- **6081)FOLID-SO**
  - Network Adapter – **6081-SO**
  - Network Adapter 2 – **6081-Monitored**
- **6081)FOLID-SERVER**
  - Network Adapter – **6081-Monitored**
- **6081)FOLID-CLIENT**
  - Network Adapter – **6081-Monitored**

Lab 1 – Lab Environment Setup

Configure Hostnames and IP Settings

Power on the Windows hosts, complete the setup, configuring the password as **Windows1**

Configure the **IP setting** (all networks are /24, use 172.16.20.10 as the DNS server), and the hostnames as **XXX-FOLID-CLIENT** and **XXX-FOLID-Server** (where XXX represents the semester code [Summer 2020 would be S20] and FOLID represents your FOL username)

Add a screenshot of the Windows client displaying both the configured address information and hostname to the Lab 1 quiz

Add a screenshot of the Windows server displaying both the configured address information and hostname to the Lab 1 quiz

Power on the Kali host, configure the **IP addresses** (use 1.1.1.1 as the DNS server), and the hostnames as **XXX-FOLID-Attacker** (where XXX represents the semester code [Summer 2020 would be S20] and FOLID represents your FOL username)

Add a screenshot of the Kali host displaying both the configured address information and hostname to the Lab 1 quiz

Shutdown the hosts and take a snapshot called **Lab 1 complete**

Submit your **Lab 1** quiz

References

- Security Onion Solutions. (2020). Security Onion: Security Onion Documentation. Evans, GA: Author.
- Timashenka, A. (n.d.). 'Flat and simple part 1 - free' by Alex Timashenka. Retrieved May 5, 2020, from https://www.iconfinder.com/iconsets/flat-and-simple-part-1-free