Updated: Feb 26, 2023

Assessment Prep Assignment

Several systems in your current environment will be removed the day before the assessment, first thing in the morning. These include:

- rw01
- fw01
- web01

> 💣 This means that all outstanding labs/homework that depends on your existing environment must be completed the day before the assessment.

Between now and then you should rehearse, backup any relevant configurations you might need and organize your notes (perhaps build a playbook), and labs that will assist you during the assessment.

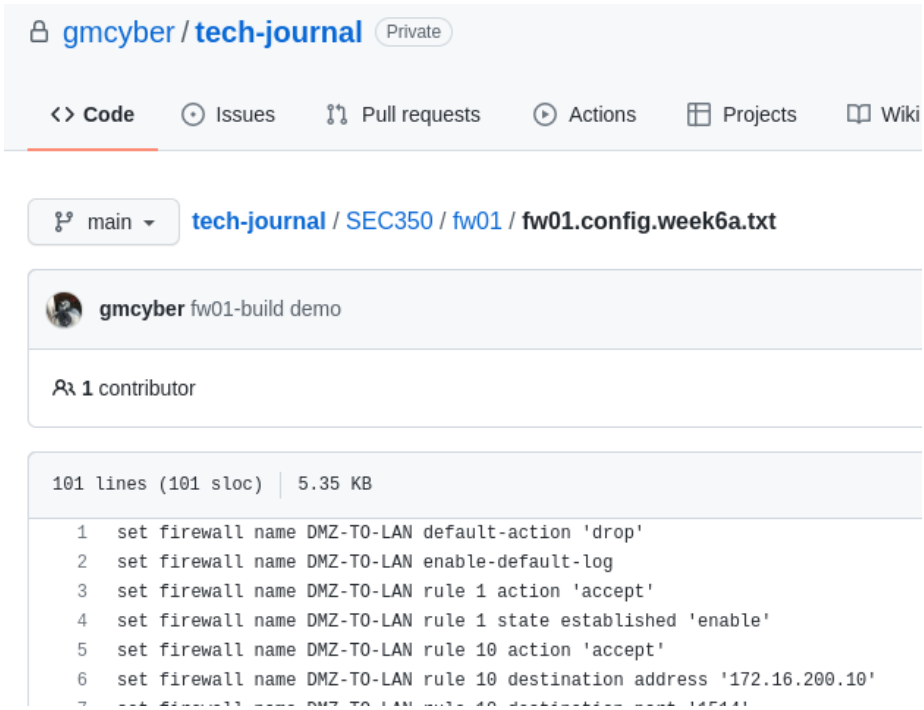
- You are on your own for the assessment ... open notes and internet, just no open neighbor. This is really a test of your notes.
- You will be getting new VM's.
- Don't be late, as you will likely need the full time.

fw01 configuration Backup

Spend some time referring to your fw01 configuration prior to the assessment. edge01 (the new firewall will be very close in configuration requirements). You might also consult your instructor's week 4 configuration

```
Deliverable 1.  Backup your current fw01 configuration github, provide a screenshot of the raw commands necessary to reconstitute your firewall.  Remember, there may be some adjustments in IP addresses and rules for your internal systems.
```

Updated: Feb 26, 2023



Assessment Description

For the assessment, you will be given a 3 zone network to configure that consists of:

1) **traveler**. A WAN based road warrior user running Windows 10. (this replaces the linux rw01)
2) **edge01**. A vyOS Firewall with three interfaces (WAN, DMZ, LAN). You will need to add an interface using vCenter. (this replaces fw01)
3) **nginx01**. A DMZ based nginx web server running Ubuntu (this replaces web01 and apache)
4) **dhcp01**. A LAN based dhcp server running Ubuntu

Requirements

- All systems should have an accurate hostname.
- All Linux systems should have a named sudo or administrator user.
- The two new ubuntu systems do not have a host firewall enabled, this is ok (for now)
- wks1, mgmt01 should be able to surf the internet.
- wks1, mgmt01 should be able to navigate to nginx01
- mgmt01 should be able to ssh to nginx01
- nginx01 and dhcp01 should have wazuh agents installed and be able to connect to wazuh
- nginx01 should have a custom web page (practice this on jump)

Updated: Feb 26, 2023

- traveler should be able to get to nginx01's custom test page by navigating to edge01's WAN IP address.
- traveler should be able to perform ssh keybased authentication with jump. Traveler is a Windows box, but ssh on powershell is nearly exactly the same as linux to include key generation. You will need to add a new public key to authorized_keys.
- dhcp01 should serve a pool of dhcp addresses to the LAN from .100 to .150.
- WKS1 should use dhcp addressing

Hints

- You do not need to work serially through this assessment, it is the end result that matters. If you are waiting for a reboot on traveler, then start configuring your other servers.
- Get all communications working BEFORE creating zones and locking down the firewalls. It's terribly difficult to debug both services and network firewalls at the same time.
- Make sure to link your firewalls to the appropriate From and To zones.
- Make sure you have the correct netmask on all Linux systems.
- Restart any service if you touch a configuration file (network, nginx, rsyslog, etc…).
- Make sure you include the appropriate vsphere label on all deliverables where your name is not obvious in the console.
- Check every VM's network settings to make sure they are on the correct segment.
- Don't forget to look at /var/log/messages to debug firewall issues.
- Do not try to use the default gateway address 10.0.17.2 as your WAN interface IP address as this will cause problems for other students and might be embarrassing.

Updated: Feb 26, 2023

Nginx Web Server

Practice this on jump (it is an ubuntu box). Poweroff first and grab a snapshot so you can revert.

`Deliverable 2. Provide a screenshot of your new web server on jump or practice, you can navigate to it from mgmt01`

Ubuntu DHCP Server

You can also practice this on jump, just move it to LAN, change the IP to something else and see if you can get wks01 to use dhcp services for IP, Netmask, Gateway and DNS settings. Make sure to reset wks01 to static.

`There is no deliverable associated with this, but it is recommended that you practice this too. If using jump, take a snapshot of jump before you do this so you can revert it back to the correct network and configuration.`

Traveler is a Windows System

You should research how to create a keypair using powershell or putty and make sure you can adjust jumps authorized_keys file to use your new windows public key.

`Deliverable 3. Practice this on either mgmt02 or wks01. Figure out how to create a keypair using either powershell or PuTTY, transfer the public portion to one of your linux systems and demonstrate a passwordless login from windows to a linux system.`

Clearing the firewall configuration

You should rehearse vyos commands by clearing your current configuration. The following commands will do that. Note, this configuration will likely have the vyos/vyos password combination because that is what it ships with.

```
configure
load /opt/vyatta/etc/config.boot.default
commit
Save
```

```
# to save and load a backup config file
Save backup_1
Load /config/backup_1
```

Updated: Feb 26, 2023

💣Preparation or lack thereof will be evident in the assessment results. Please dedicate class time and at least an equal time before assessment on preparing your notes and researching requirements you aren't clear on.