CCNP ROUTING AND SWITCHING

TACACS+ FOR WINDOWS VM AAA

Brennen Tse
10/9/2022

Windows: AAA TACACS+

Table of Contents:

Purpose:

In this lab, students are to recognize the uses of AAA and configure the two main AAA protocols, open-source RADIUS and Cisco proprietary TACACS+. Students are to set up a VM server with either Windows or Linux Ubuntu OS's. With either RADIUS or TACACS+ installed on the server, a Router should be able to establish remote authentication on the router to confirm user credentials with the server. Users should use SSH to secure login for administrative access into the router, and be prompted to enter login details which can be verified by the AAA server. In this report, I will be configuring TACACS+ on the Windows VM.

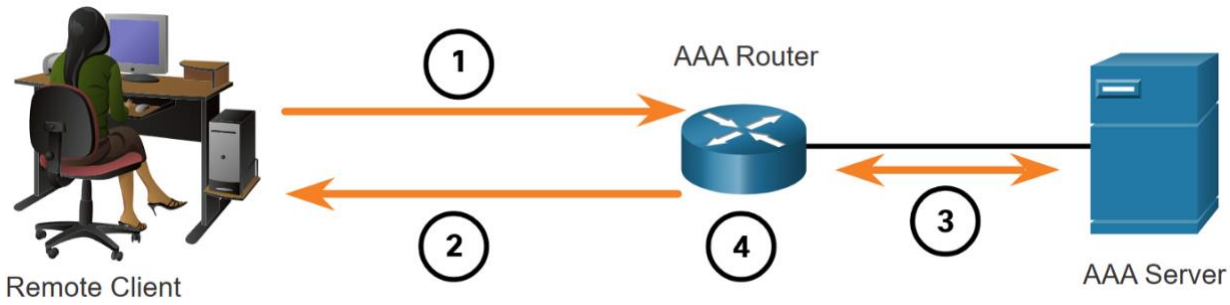
Background Information:

AAA is the acronym for the security framework of Authentication, Authorization and Accounting for validating user login. This framework is usually used when users are accessing network infrastructure or resources remotely and to ensure added security. Levels of privilege and access can be assigned as well. Through authentication, you can control who is permitted to access certain resources. This is accomplished from comparing a user credentials with a database of valid users.

The advantages of using RADIUS or TACACS+ to remotely store user profiles is that since the user profiles are not stored locally, if someone was to gain unauthorized access to the router, the network security would not be compromised. Authorization dictates what network resources authenticated users can use, usually through privilege levels or access to certain commands. Finally, accounting is used to monitor and capture activity to use in monitoring network performance and user logins.

AAA clients can be a variety of several devices, mainly routers, switches and firewalls. In this lab we will focus on the router. These devices are known as a NAS, or Network Access Server, that serve as the device that users locally get AAA from, and the device in direct contact with the AAA server. Communication between the AAA server and the NAS is conducted through the authentication protocol, namely RADIUS and TACACS+.

AAA Communication Process:



1. Remote client tries to login to router using PPP. In our case we use Putty.
2. AAA Router requests username and password.
3. Once username and password are given, AAA router sends these to AAA authentication server through either RADIUS or TACACS+ to check validity and authorization of user.
4. Once receiving this information, router either grants user access or denies access.

RADIUS vs TACACS:
Terminal Access Controller Access Control System Plus (TACACS+) is used to communicate between the client and NAS server and is Cisco proprietary. Remote Access Dial-In User Service (RADIUS) is a protocol that is open standard used for the same purpose as TACACS+ but uses port 1812 and 1813. Both were designed for slightly different purposes can be used for the same roles, as RADIUS would ideally be used to authenticate and log remote users while TACACS+ is used for admin access to network devices like the router in this lab. TACACS+ is more reliable using TCP port 49 instead of RADIUS's UPD ports 1812 and 1813, and also provides more control of authorization of commands. TACACS+ is more secure as all packets in are encrypted while only passwords are in RADIUS. However, RADIUS is open standard meaning it can be used on devices other than Cisco ones. The authentication processes are the same between both protocols.

Differences:
TACACS+ separates each component of AAA, Authentication, Authorization and Accounting while RADIUS combines Authentication and Authorization, using port 1812 for them and 1813 for accounting. TACACS+ offers multiprotocol support and is used for device administration, while RADIUS is used for network access.

TACACS vs TACACS+
So what's the difference between TACACS and TACACS+?
-TACACS is the older version of TACACS+
-TACACS is open standard vs TACACS+
However, using TACACS is not recommended as TACAS does not:
-prompt for password change
-use of dynamic tokens
-support Kerberos secret key authentication
While TACACS+ has dynamic passwords, TFA, and audit functions. Both use TCP and Port 49.

TACACS+ and its protocols:

There are three different TACACS+ messages during the authentication process. Start (client -> server), Reply (server -> client) and Continue (client -> server).

1. When the TACACS+ client is connected to by a user using SSH or Telnet, a Start message is sent to the server with an authentication request.
2. The TACACS+ server sends a Reply message back with a prompt asking for a username.
3. Once a username is entered, the TACACS+ client sends a Continue message to the server.
4. The TACACS+ server send another Reply message back asking for a password.
5. Once a password is entered, the TACACS+ client sends another Continue message to the server.
6. The TACACS+ server will check the username against the password in its databases and once it's either authenticated or rejected, one of four different reply messages can be sent: Either
   a. Accept: Authentication is successful, authorization stage reached.
   b. Reject: Authentication is unsuccessful.
   c. Error: Authentication failed.
   d. Continue: More information (MFA) is required to proceed and authenticate.

Lab Summary:

A router which serves as the authentication client and NAS is connected to a PC hosting the VM with the TACACS+ server. Although these devices are physically connected through a single link, they logically represent separate devices. To confirm that the authentication protocols are working, a new user profile should be added to the authentication database and confirmed that it works. Incorrect logins should also be checked to make sure that the authentication isn't set to allow all. For the TACACS+ VM server we used Window's 2019 server and a download of the TACACS+ software.

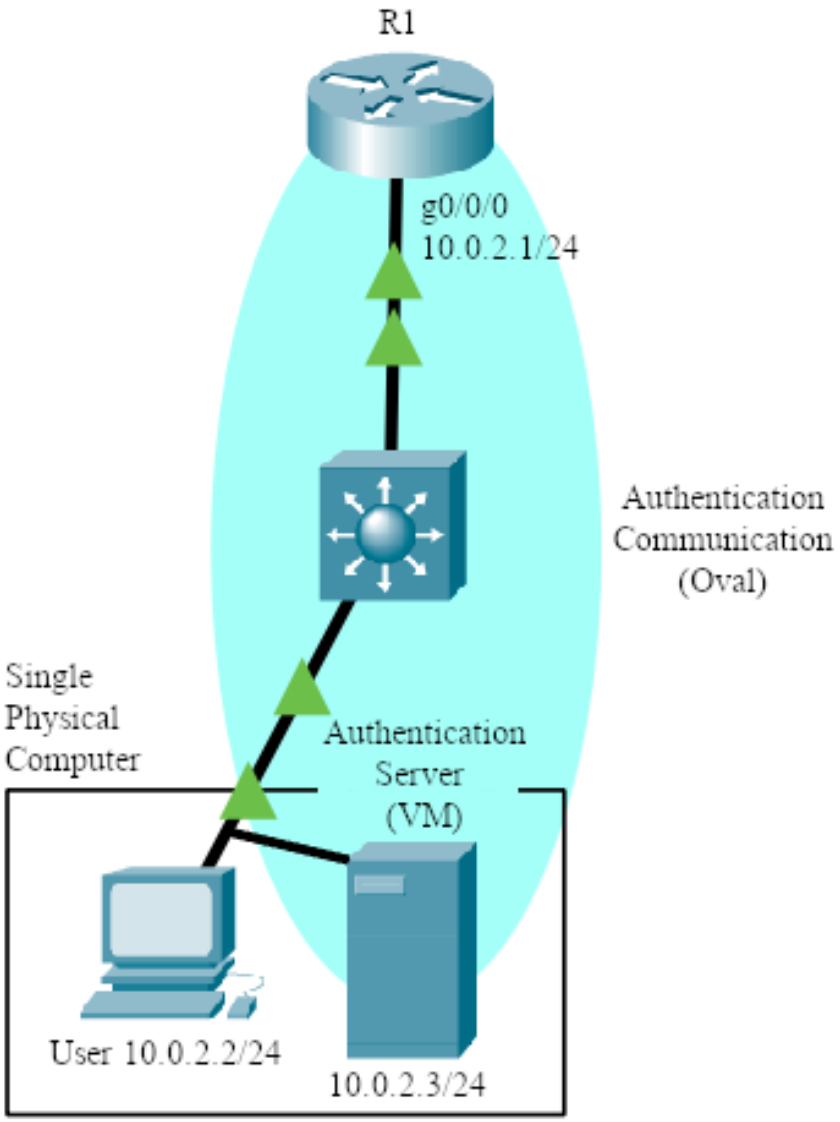
For TACACS+, the server ran on the user computer itself rather than on a separate VM host, making the user device the both the remote client and TACACS+ host. The startup exe file was installed from the official TACACS website. Of the files downloaded after the wizard installation, "authentication," "clients," and "authorization" were edited for the goal of this lab. These files can be directly edited through a text editor, like Notepad++. User templates have already been made and by removing the comment tags, the text is rendered as

readable code. There is also a pre-existing template for the clients. The corresponding information was filled in for all the files. This included IP addresses, usernames, passwords, and enable passwords.

From the installation wizard, a couple other useful features were installed. TacVerify looks for errors in the configuration, and admin command prompt can run TacTests that attempt to login with information without ever contacting the NAS. Restarting the service is also done on the command prompt.

Changes of configuration afterwards are documented as evidence of functionality. After all elements of configuration, the protocols are operational and AAA is in use.

Network Diagram



Router Commands:

Below are the minimum required commands to enable TACACS+ on whatever router you use, in our case it was a 4321. These should be executed in privilege exec:

```
aaa new-model
aaa authentication login default group tacacs+
aaa authentication enable default group tacacs+
tacacs server <Arbitrary Name>
 address ipv4 <IP>
 key <Server Key>
```

// TACACS+ Lab Commands Defined:

Router(config)# **aaa authentication *login default group tacacs+***

- Make the router verify login credentials with a tacacs server

Router(config)# **aaa authentication *enable default group tacacs+***

- Make the router verify privilege exec mode credentials with a tacacs server

Defining a TACACS Server

Router(config)# **tacacs server [*name*]**

- Define a tacacs server

The router will use the ip of the tacacs server to verify credentials. You can only type this command after aaa new-model *has been declared.*

Router(config-server-tacacs)# **address ipv4 [*ip*]**

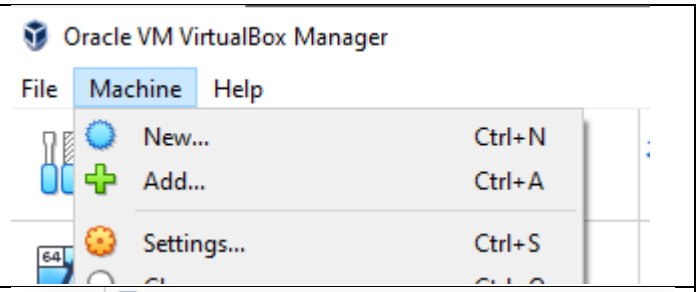
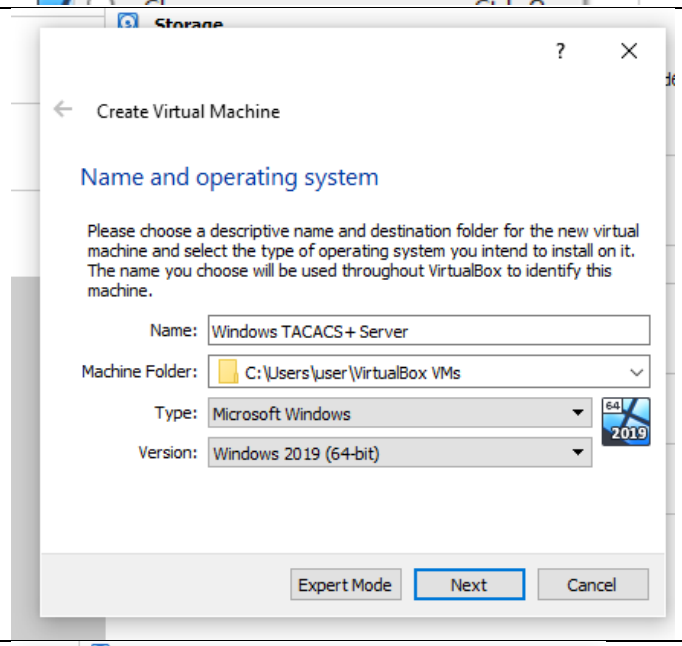
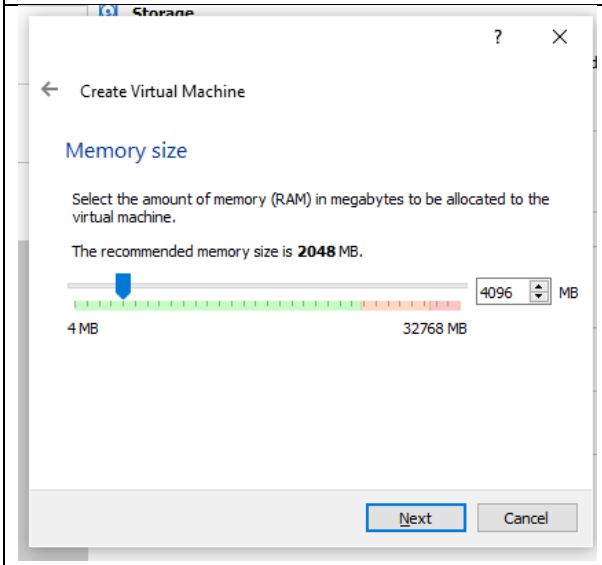
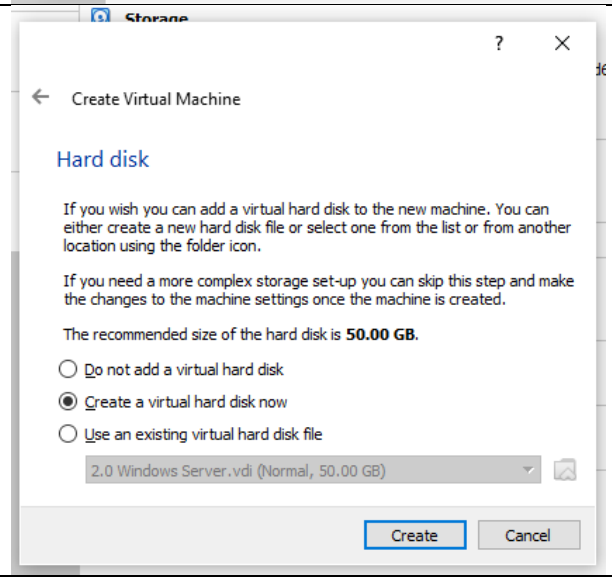
- Defines the *ip address* of the tacacs server

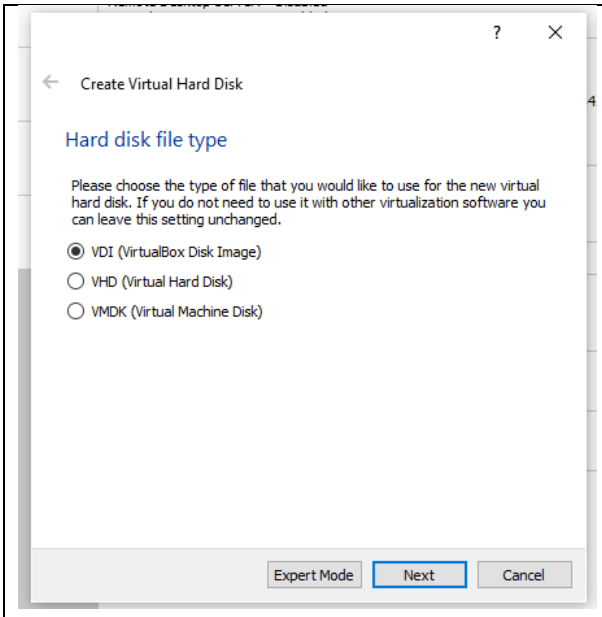
Router(config-server-tacacs)# **key [*key*]**

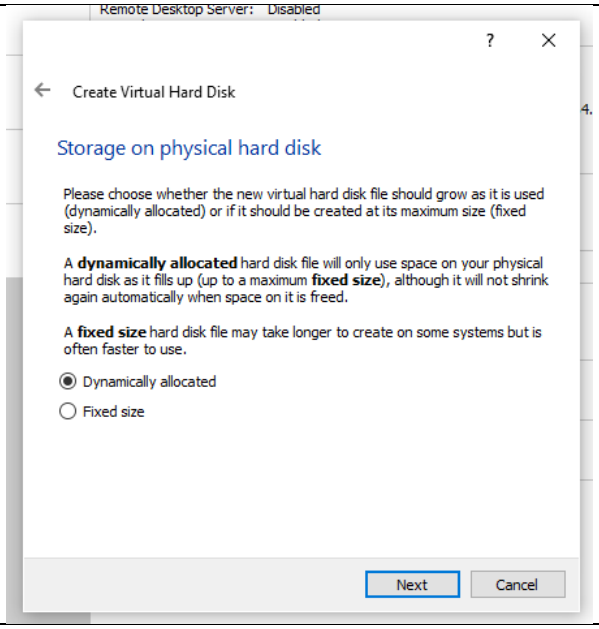
- Define the *key* of the tacacs server

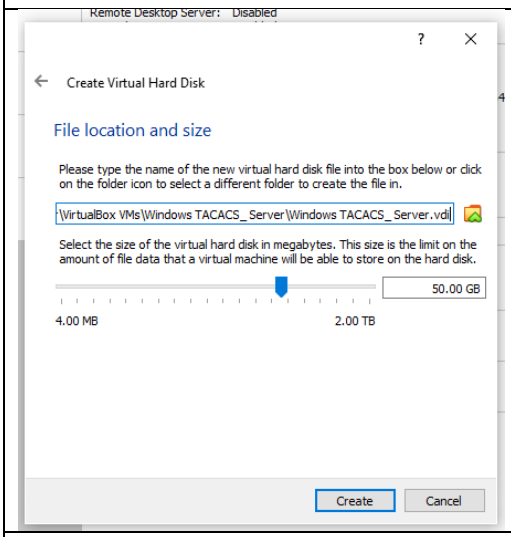
The key on the router should match the key in the tacacs+ server's configuration files.

TACACS+ Configuration with Windows Server:

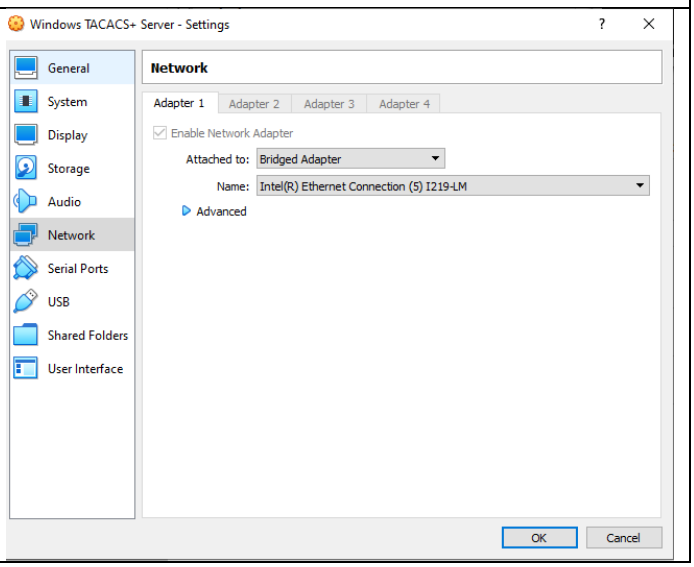
Install and open VirtualBox. In Machine>New create a new machine.	
Name and select the version that matches the windows machine image you should have downloaded. In my case I used Windows 2019.	
	



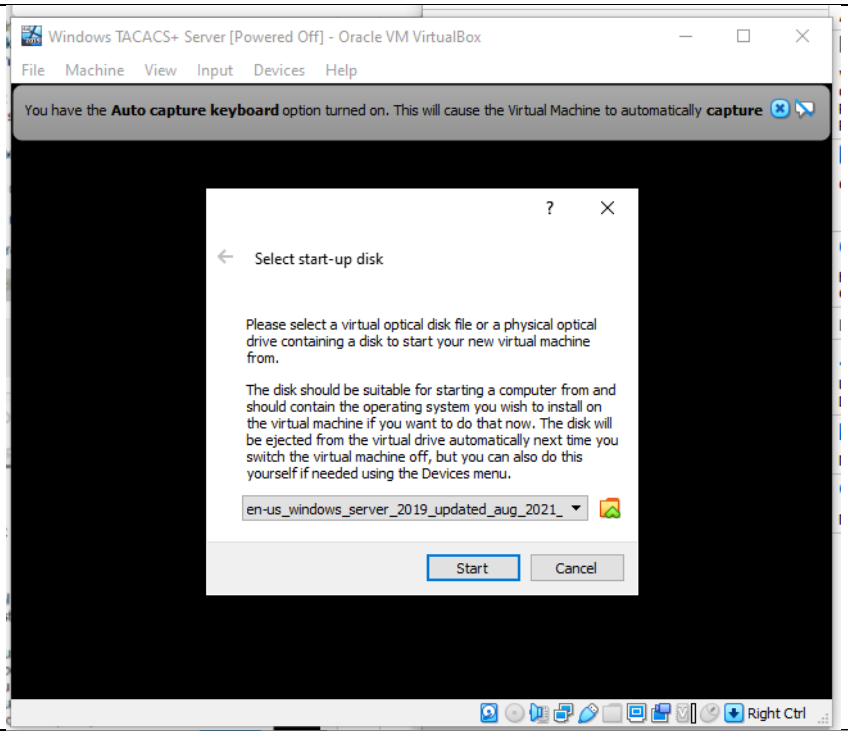




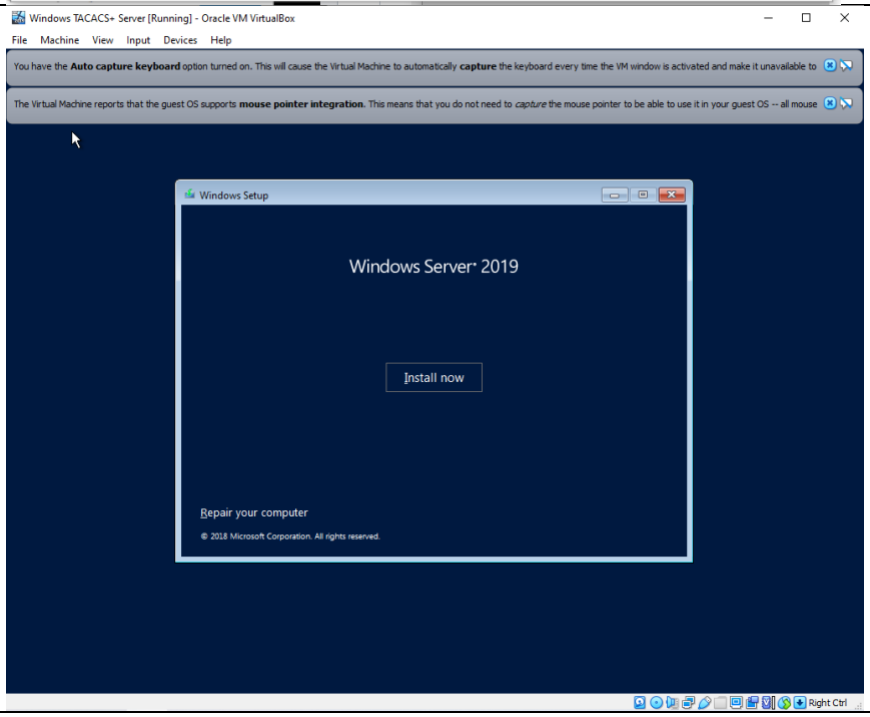
In the Virtual Machine go to settings>network>adapter 1 and change the NAT to Bridge Adapter (Ethernet).

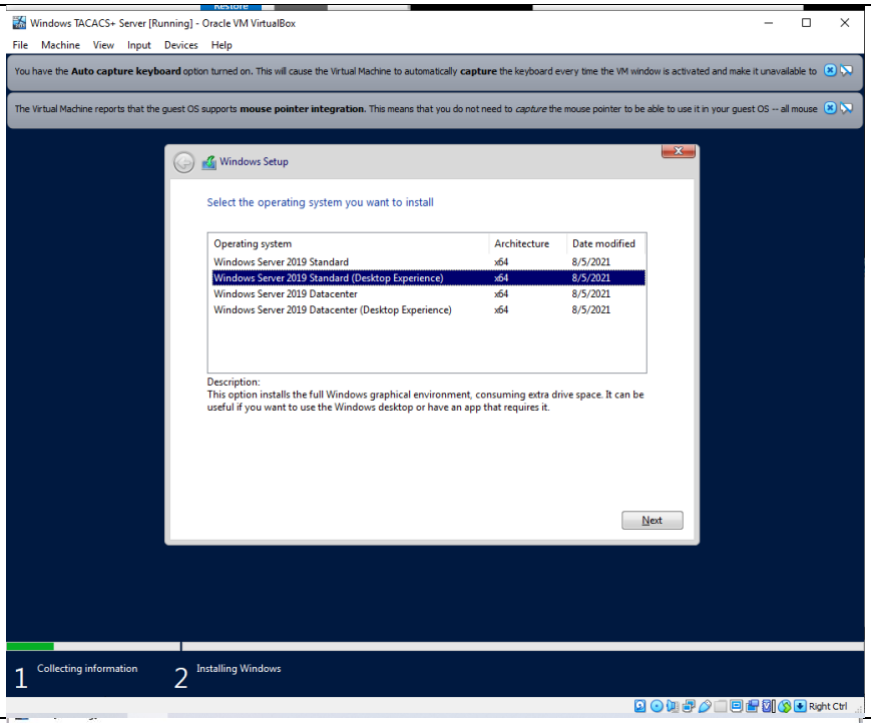
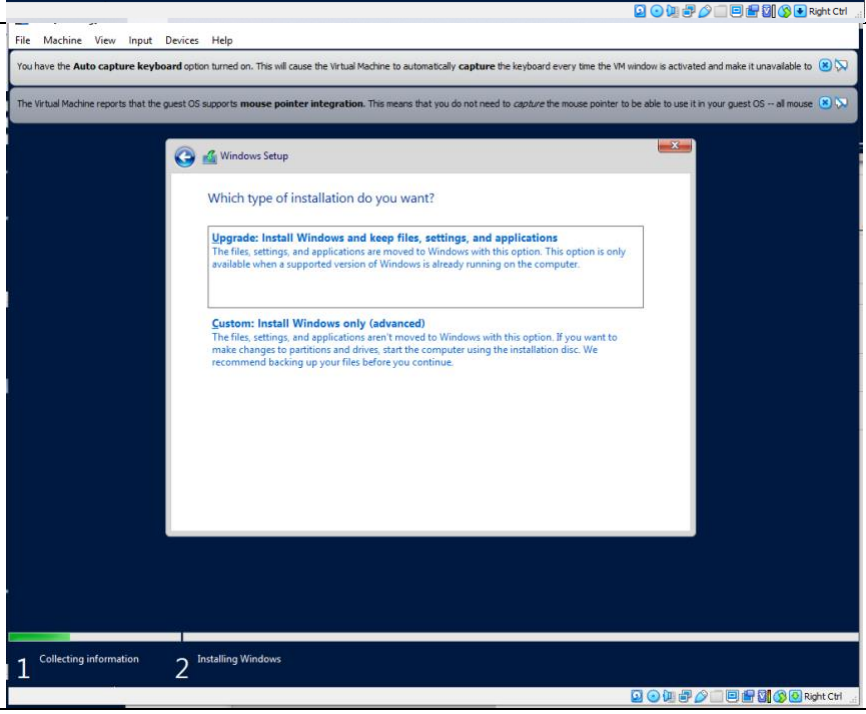


After the disk is created, launch the VM after clicking the green start arrow. Select the correct windows server image from the start-up disk.

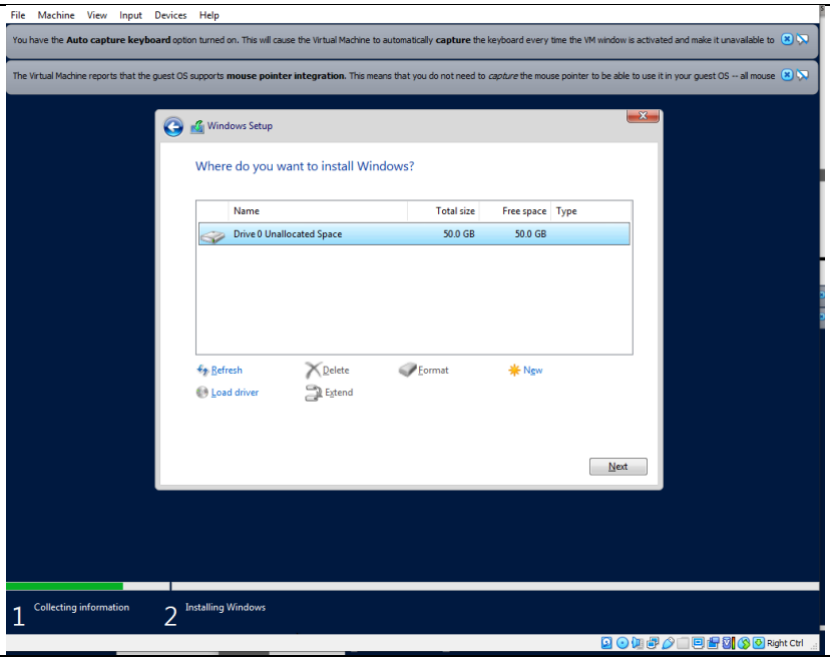


Click Install Now and navigate the language preferences.



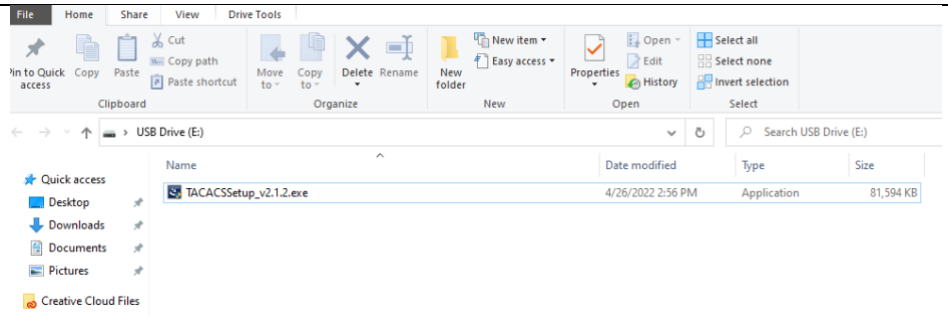
Choose either of the Standard versions. I chose the Desktop Experience.	
Click the Custom option, install Windows only. We only want an empty windows server for our TACACS+ VM.	

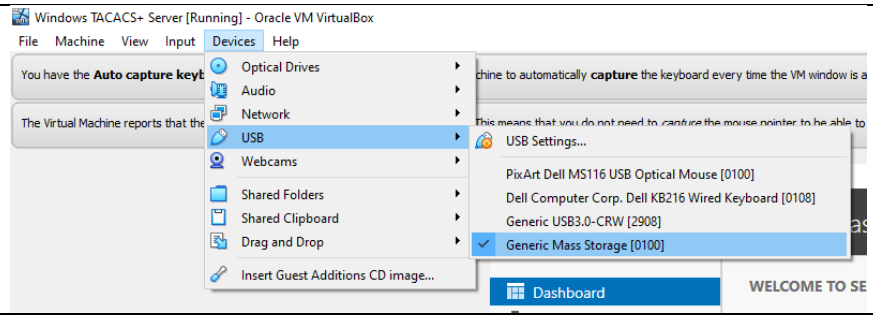
Select the available drive and complete the install.

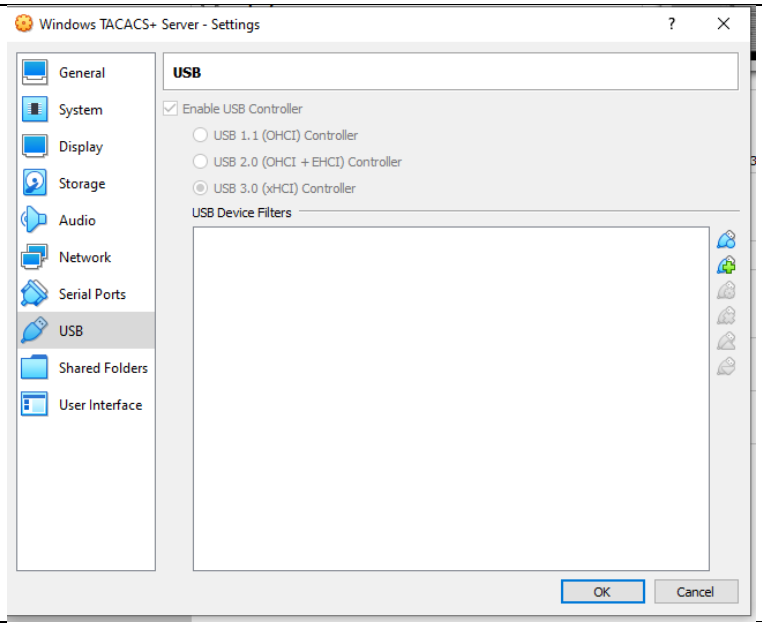
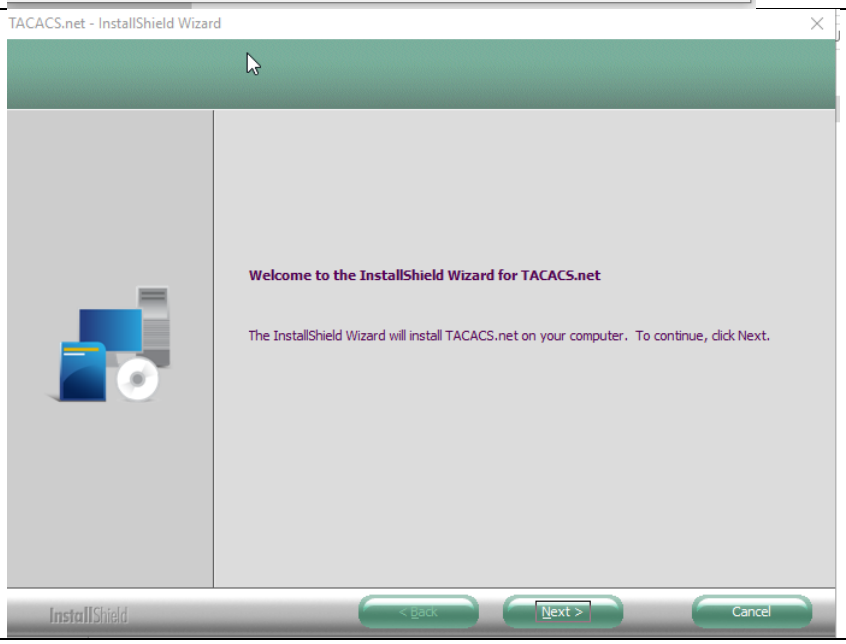


DOWNLOADING and INSTALLING TACACS+

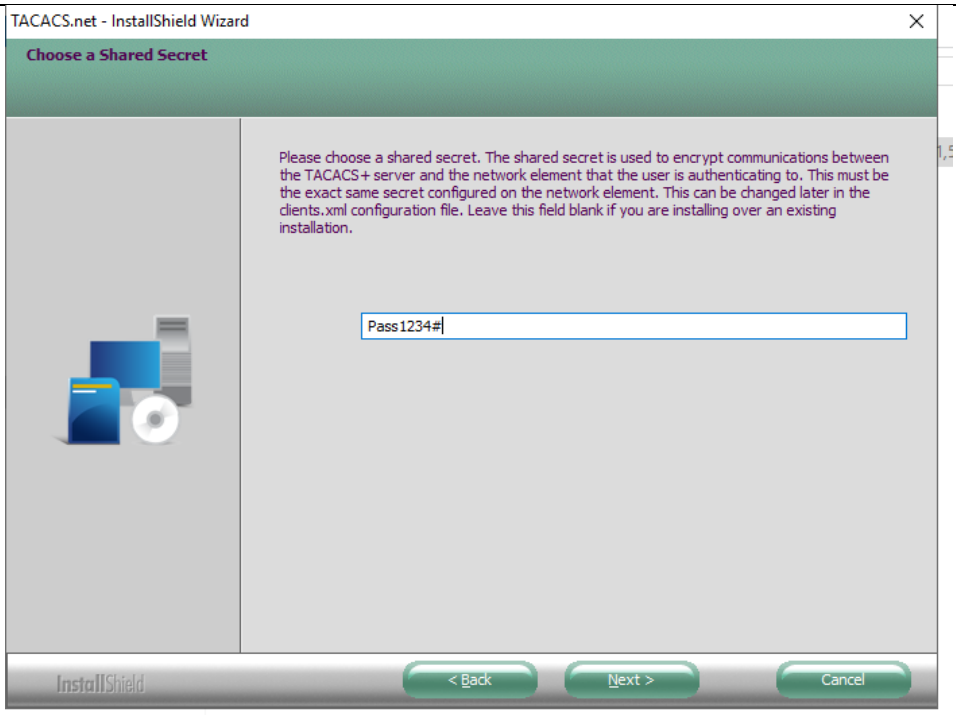
Download the TACACS+ service from TACACS.net. In my case I put it on a USB and will download it from there.



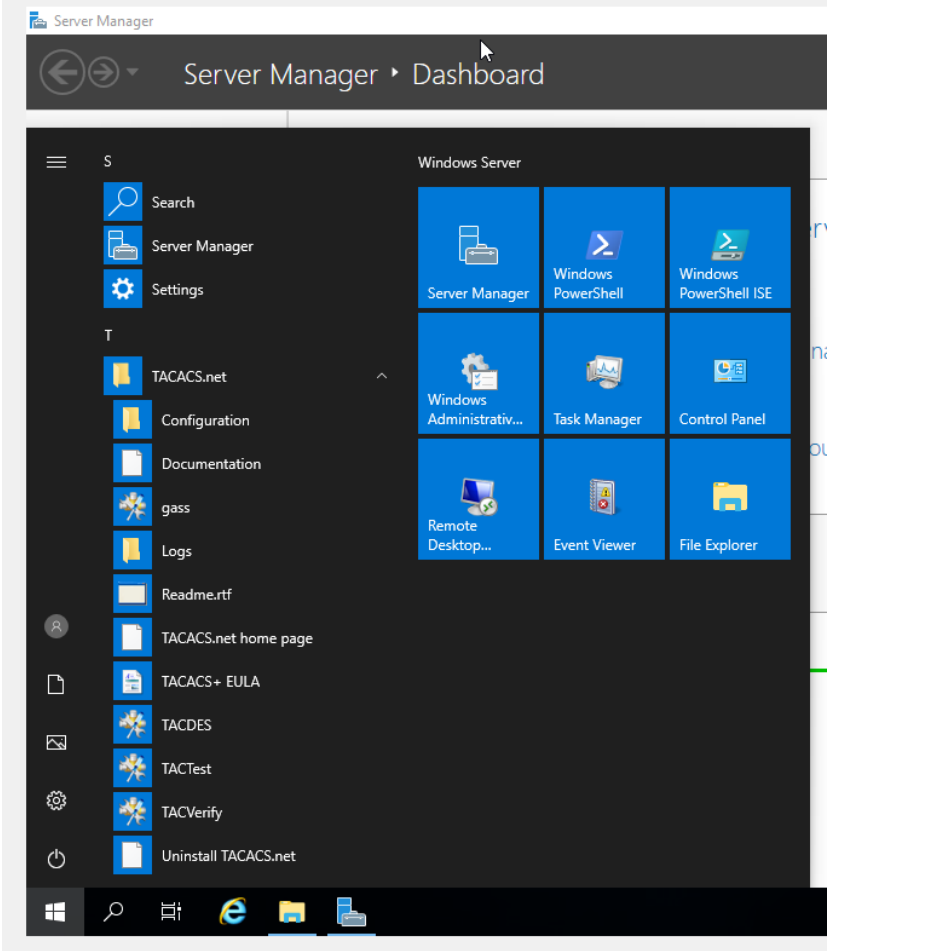


Troubleshooting: If you are installing from a USB drive, go into the VM settings>USB and change the USB to version 3.0 instead of the default 1.1.	
When the VM runs TACACS+, you will be given this prompt, click next.	

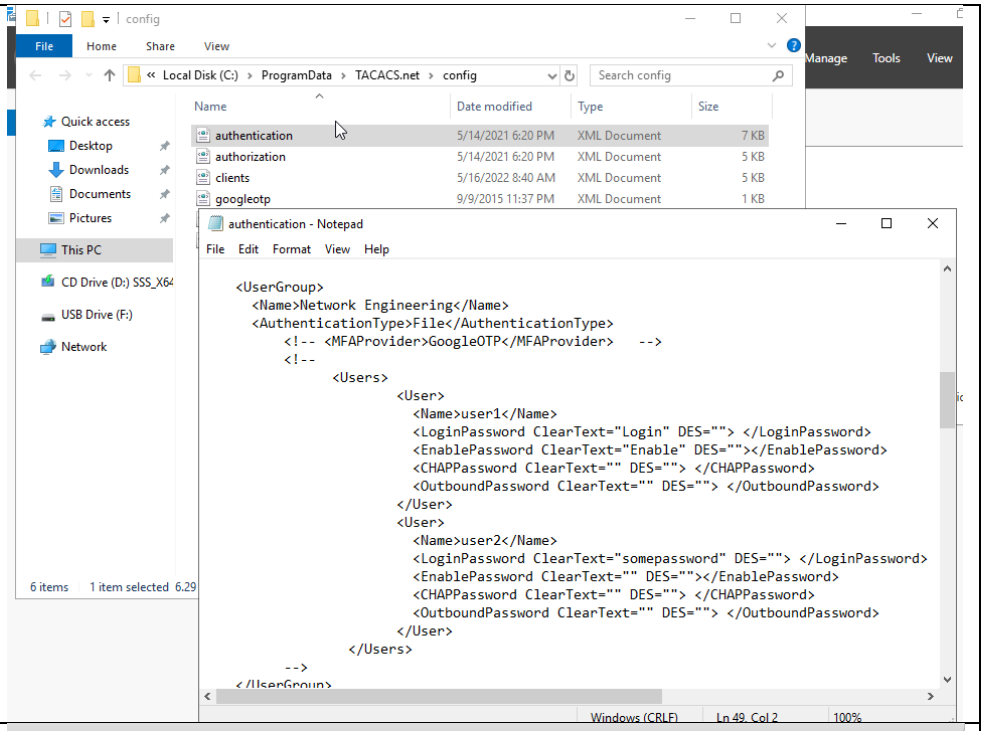
Enter a key of your choosing and remember it. It will be important later.



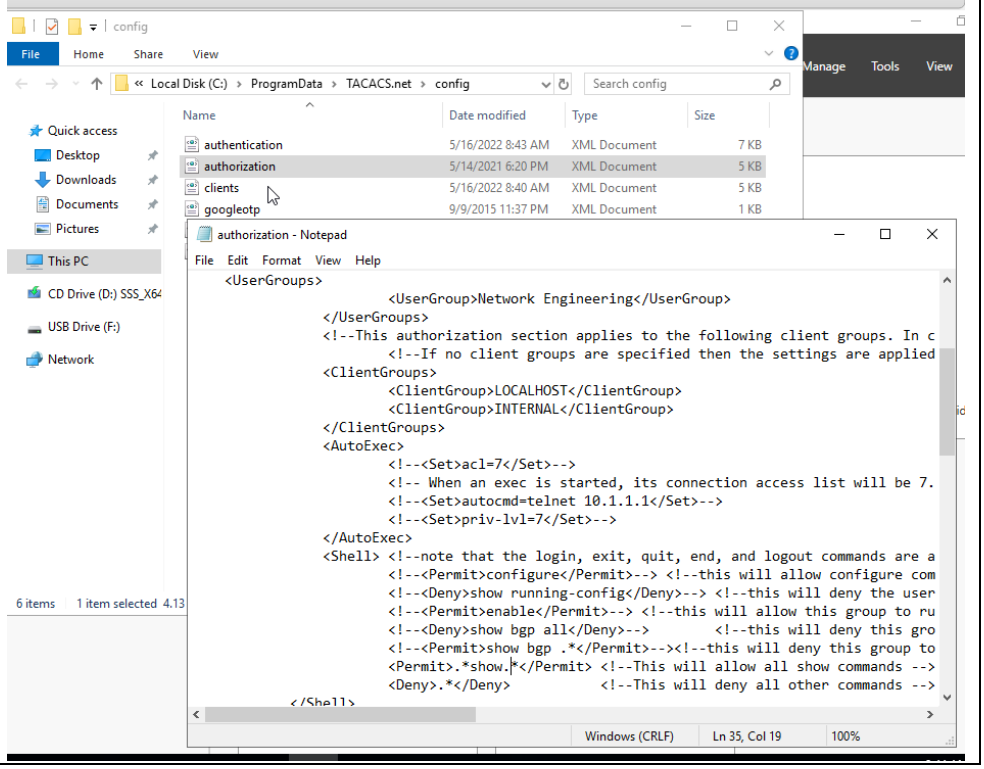
Navigate to the TACACS.net folder and open Configuration.



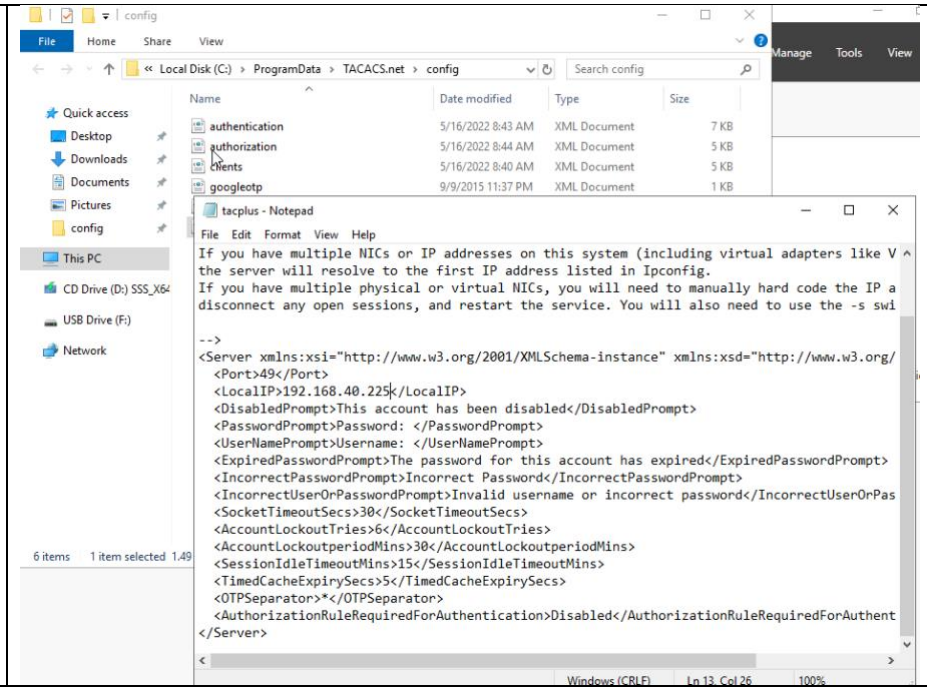
Open the authentication xml document with Notepad and scroll down to the UserGroup section. Note: to enable the users remove the <!-- --!> from the section. Those were used to comment out certain parts. Changes the User Profiles as you see fit.



By default the permit will only allow *show.* commands, however you should remove the show command and leave it blank to allow all commands.



Change the local IP from the default.



This IP Should match the ip address of the vm host machine.

```
C:\Users\Administrator>sc stop TACACS.net

SERVICE_NAME: TACACS.net
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 3  STOP_PENDING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\Users\Administrator>sc start TACACS.net

SERVICE_NAME: TACACS.net
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 2  START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 664
        FLAGS              :

C:\Users\Administrator>
```

```
C:\Users\Administrator>tacverify

All files have the correct syntax. Validating configuration...

No errors were found in the configuration.
```

Remember to disable the firewall in this production environment.

More Show Commands:

```
-----------------

SUMMARY STATISTICS

-----------------

Total Commands  .....................  1
Successes  ..........................  1
Failures  ...........................  0
No Results  .........................  0
Time Taken for commands  ............  0.064 secs
Avg Possible Transactions/Second  ...  15
Network Time per command  ...........  0.029 secs
Total Network time  .................  0.029 secs
Sent Transactions/Second  ...........  7.1

C:\Users\Administrator>
```

```
C:\Users\Administrator>tactest -s 192.168.40.225 -k Pass1234# -u CLASS -p CISCO
Performing LoginASCII with CLASS,CISCO,False
Trying to open connection to 192.168.40.225:49

Sending:
 MajorVersion=12
MinorVersion=0
Type=Authentication
SeqNum=1
IsEncrypted=True
IsSingleConnect=True
SessionID=1684496624
DataLength=8
 **Authentication Start**:
Action=Login
priv-lvl=1
Type=Ascii
Service=Login
User=
Port=
RemAddr=
Data=*******[Hidden for security]

Received Header:
 MajorVersion=12
MinorVersion=0
Type=Authentication
SeqNum=2
IsEncrypted=True
```

Confirmation of Successful Authentication.

Verification of Connection

```
R1#show run | include tacacs
aaa authentication login default group tacacs+ enable
aaa authentication enable default group tacacs+ enable
tacacs server MAIN

R1#show run | include aaa
aaa new-model
aaa authentication login default group tacacs+ enable
aaa authentication enable default group tacacs+ enable
aaa session-id common
```

ROUTER TACACS+ SHOW RUN:

```
version 16.7
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
!
aaa new-model
```

```
!
aaa authentication login default group tacacs+
aaa authentication enable default group tacacs+
!
aaa session-id common
!
subscriber templating
vtp domain cisco
vtp mode transparent
!
multilink bundle-name authenticated
!
license udi pid ISR4321/K9 sn FDO220523GF
no license smart enable
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
redundancy
 mode none
!
interface GigabitEthernet0/0/0
 ip address 192.168.40.226 255.255.255.0
 negotiation auto
!
interface GigabitEthernet0/0/1
 no ip address
 shutdown
 negotiation auto
!
interface Serial0/1/0
 no ip address
 shutdown
!
interface Serial0/1/1
 no ip address
 shutdown
!
interface GigabitEthernet0/2/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/2/1
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
```

```
ip tftp source-interface GigabitEthernet0
!
tacacs server <MAIN>
 address ipv4 192.168.40.225
 key Pass1234#
!
control-plane
!
line con 0
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
!
wsma agent exec
!
wsma agent config
!
wsma agent filesys
!
wsma agent notify
!
!
end
```

Problems for RADIUS and TACACS+

There were, expectedly, many problems during configuration, testing, and troubleshooting, especially those stemming from the inexperience of the new interfaces and outdated software. The one that would end up causing the greatest confusion is the necessity to restart the protocol service after making major changes, such as changing the shared secret key or an IP address. This caused many understanding conflicts as configurations do not update and apply instantaneously, making certain changes and configurations not display properly from a user device perspective. This interfered with expectations of certain commands and confused the general understanding of whether a command functioned or not. Ultimately, the "service FreeRadius restart" command for RADIUS and the "sc start/stop TACACS.net" for TACACS+ became go-to commands after any edit.

For FreeRadius v3 and Oracle VirtualBox, there were relatively small issues in regard to downloading the proper bootstrap version for USB integration. This was done to download operating disk images and .exe files for the virtual machine. The problem mainly stemmed from the inability to access files from the USB with TACACS+ and transfer it to the VM. After some troubleshooting, I discovered that VirtualBox as a default supports USB 2.0, instead of USB 3.0, which was needed to file share with the latest USB's. After an extension pack was found, the problem was resolved. All versions and options are found on the Oracle VirtualBox website. Version 6.0 was used for this lab. An important configuration directed towards VirtualBox is the necessity to change the network adapter to a *bridged adapter*. This allows the virtual machine to share and connect their information via ethernet, where it would otherwise be isolated. This was the key solution to more than a couple pinging problems.

Other quicker issues relating to TACACS+ included the lack of permission to run TacTest commands, which could be fixed by using the *admin* command prompt, done by right-clicking the

command prompt application. When TACACS+ needed to be restarted but the start command says that it is already running, stop the TACACS before trying to restart it. The wording for the commands must be very accurate, and even a slight mistype can lead to later bugs, as in some cases the interface will accept the incorrect command without notifying you. This led to a problem with my TACACS+ software in that the router was not connecting to the VM because the proper interface was still in its shutdown mode. With TACACS+ especially you needed to ensure that the right brackets were deleted to get the proper parts of the software working on the Windows Machine.

Conclusion

This revealing lab was indisputably valuable in the new interfaces to be familiar with. As my first useful application with Linux and VirtualBox, I learned and navigated a wide array of commands, specifically those of Ubuntu Linux, Oracle VirtualBox, and Notepad++. In the foreign environment, it was an achievement to be able to understand and execute the protocols fully and functionally. AAA and other security protocol and frameworks like CIA are essential parts of today's cybersecurity architecture, and continuing to improve and expand their use will lead to a more secure and safe world for all Internet users.