Lab 6-2FA with Google Authenticator

Dawn M Inman

CSC-432 Computer and Network Security

Professor Nick Merante

April 17, 2020

Abstract

This lab sets up google authentication, which is a two-factor authentication, on the CentOS 7 routerVM. This lab goes through the process of setting it up via SSH. Logging into Proxmox was not altered because if there are any issues it needs to be able to be accessed by both the student and professor. Two-factor authentication (2FA) is explored as well as Google Authentication methods and reasonings. Screen shots are provided as proof of authentication login success.

Keywords: CentOS 7, Kali Xfce, Proxmox, QEMU, PuTTY, SSH, Google Authentication, two-factor authentication, 2FA

Lab 6-2FA with Google Authenticator

Two-factor authentication means having a second protection layer for an account or system. This is a two-step process requiring two different types of information to work properly. Examples could be passwords, pins, email, an ATM card, fingerprint, or key. Since it is two-factor, the process might require a password and a key, or a pin and an ATM card, etc. The two-factor system was designed to reduce the instances of unauthorized persons from gaining access to accounts with only stolen passwords. Some users feel this is inconvenient when logging into other devices as the user will need their normal password as well as a multi-digit code that comes through on a trusted device. This prevents theft from other users. Google does a great job with their authentication system and it was applied to the student's router VM during this lab. (Kenton, 2019)

Google Authenticator is an app that takes away the risk of receiving a text to use as authorization. Because they take away the possibility of being hacked via phone number and password, it is a more secure two-factor verification. Once the app is installed it sends a six-digit code that is refreshed every 30 seconds. When Google Authenticator is installed onto a device like the router, it produces a QR code that can be scanned with the app, as well as options if the app isn't working like a secret key, verification codes and scratch codes that are saved for a later date in case access to the account is blocked or passwords are forgotten. (Chin, 2018) To complete the set-up, some files need to be altered so that the authentication is a requirement before login in allowed. Once finished, double checking to make sure the authentication is working properly while still logged in is an excellent idea so that one is never locked out of a system on accident.

This lab uses the virtual router on the student network, a CentOS 7 router. CentOS 7 is so named because it stands for Community ENTerprise Operating System. It is based on the Linux kernel, free and has been available since 2004. Red Hat Enterprise Linux is the origination of CentOS 7 so it is a compatible option when requiring Linux software. It is very popular with almost 30% of Linux web servers using it in 2011 and has been one of the most popular in hosting history. (CentOS Blog, 2020)

Kali Xfce is a newer Kali release. It is on the same line of Kali environments that have been created for Penetration Testing. There is a new feature called "Kali Undercover" which can make the display of Kali look like Windows 10. This can happen quickly so it is a type of stealth feature meant for blending in when in public areas. (Abrams, 2019) Other new features include KaliNetHunter KeX for Android which can install a full Kali desktop via Android, upgrading the kernel, Git powered documentation and adding PowerShell. (Elwood, 2019)

Proxmox is also being used by the systems and is used extensively in this lab. Proxmox VE hypervisor is based on GNU/Linux (Debian) and is open source. It has a central web-based management that does not require more installation. (Cheng, 2014) Version 5.4 is built specifically on Debian 9.8 with a "specially modified Linux Kernel 4.15". (Proxmox, 2019) Proxmox is capable of two types of virtualization: OpenVZ and KVM. OpenVZ needs a patched Linux kernel so Linux guests are the only operating system type that can be created. In OpenVZ, the guests are called containers because they share the same architecture and kernel as the host operating system. (Cheng, 2014) KVM (Kernel-based Virtual Machine) is a modified Linux kernel built with the KVM module so that it can give hardware-assisted virtualization. Virtualization is performed by a software-based emulator (QEMU) which simulates the virtualized environment while KVM only exposes the /dev/kvm interface. (Cheng, 2014) "This converts Linux into a Type 1 (bare-metal) hypervisor." (What is KVM?, 2020) Then QEMU or the software-based emulator will create the virtual machines on top of KVM. (What is KVM? 2020) Proxmox VE is relatively simple to start working with but can be very in depth as Simon M.C. Cheng has authored a book called Proxmox High Availability which goes into more detail when setting up a high availability virtual cluster. (Cheng, 2014)

PuTTY is used several times during the lab. PuTTY is an SSH client for Windows, Mac, and Linux. It has a terminal window for access to the server used in this lab, the GNU/Linux server named router. (How to use PuTTY on Windows, 2020) SSH is a software package and means Secure Shell. It secures system administration and file transfers even though the networks are insecure. Tatu Ylonen is the inventor of SSH and OpenSSH which is an open source SSH program is based off of his free versions. (SSH(Secure Shell), 2020)

Objective

This labs purpose is to apply two-factor authorization via Google Authenticator to the SSH pathways that go to the router. This is accomplished through the installation of both epel-release and Google Authenticator. Files are changed so the authentication is required at login and screenshots are given to show successful login via SSH with authentication.

The computer that is being used is a 2011 HP Pavillion dv7, i7 quad core processor and 16GB RAM with Windows10Pro operating system. Google Chrome is the internet browser being used for connecting to Proxmox. KaliVM is on Proxmox. The KaliVM then runs Fire Fox internet browser, PuTTY as the SSH connection. The router is a CentOS 7 system with Google Authenticator installed.

Results and Analysis[1]

To use Google Authenticator it must be on the device one wants to authenticate. On the CentOS 7 router, the following command was typed in to see if the program package was on the machine:

```
yum install epel-release
```

This was already loaded onto the machine. Following the lab directions, google authenticator was tried:

```
google-authenticator
```

however, it came up with an error that said command not found. After looking online, some directions said to install the authenticator with this:

```
yum install google-authenticator
```

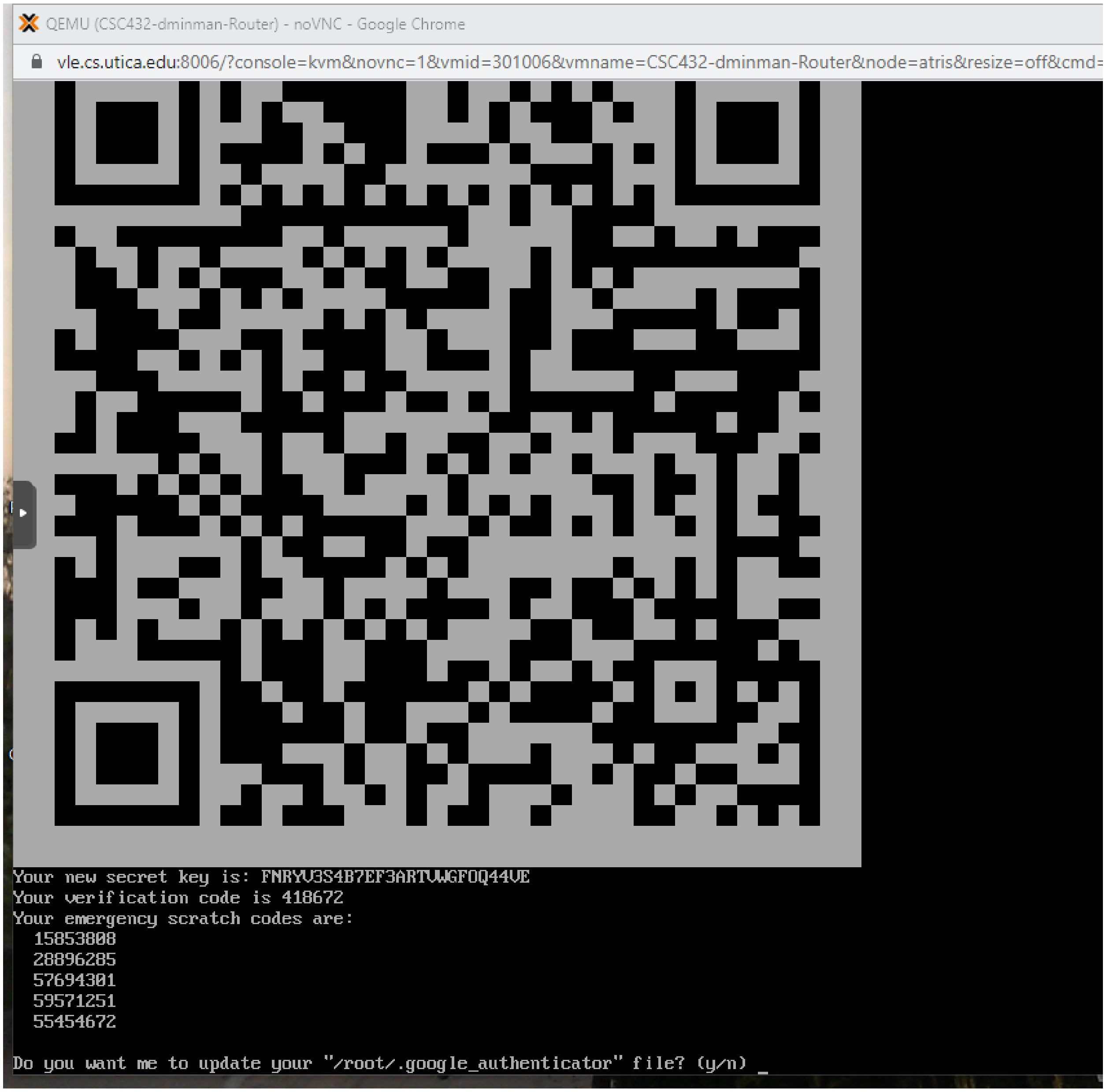
This worked perfectly and the installation was a success.

To run the authenticator, type in:

```
google-authenticator
```

When asked if the tokens should be time based, yes was chosen.

This produced a scannable QR code, a secret key, a verification code, and five emergency scratch codes which were saved in a couple different ways before any more steps were taken. Scanning the QR code with the Google Authenticator app was very easy and set up the account quickly.


QEMU (CSC432-dminman-Router) - noVNC - Google Chrome
vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=301006&vmname=CSC432-dminman-Router&node=atris&resize=off&cmd=

```
Your new secret key is: FNRYV3S4B7EF3ARTVWGFOQ44VE
Your verification code is 418672
Your emergency scratch codes are:
  15853808
  28896285
  57694301
  59571251
  55454672

Do you want me to update your "/root/.google_authenticator" file? (y/n) _
```

Figure 1google authentication codes

Next the router is updated by choosing yes to updating the google authentication file.

More questions followed, much longer than written, but these are the general topics of the questions: (answers are per the lab instructions)

Disallowing multiple users? y

Time-skew compensation? n

Enable rate-limiting? n

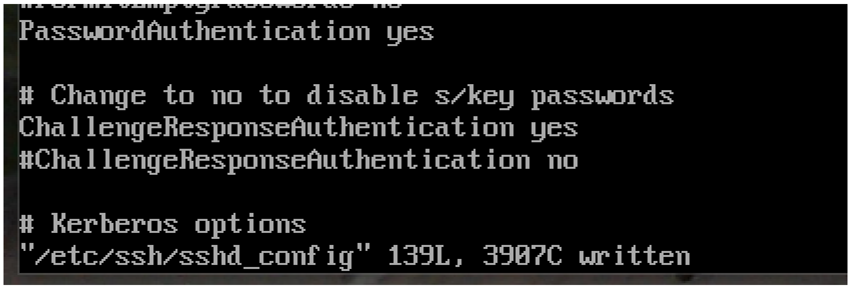
Now at the prompt again, the next step is to configure the operating system to require google authentication at SSH login. Editing the file /etc/pam.d/sshd with vi text editor, add this line to the bottom of the file:

auth required pam_google_authenticator.so

Next edit another file with vi, /etc/ssh/sshd.config, by commenting out (#) the no line and uncommenting (removing #) from the yes line.

ChallengeResponseAuthenticaton yes

#ChallengeResponseAuthentication no



```
PasswordAuthentication yes

# Change to no to disable s/key passwords
ChallengeResponseAuthentication yes
#ChallengeResponseAuthentication no

# Kerberos options
"/etc/ssh/sshd_config" 139L, 3907C written
```

Figure 2 Challenge Response Authentication set up

Save, close, and restart sshd service by typing in:

Systemctl restart sshd.service

The last step is to sign in while still logged in. This is to prevent being locked out if something goes wrong.

Type into the command line

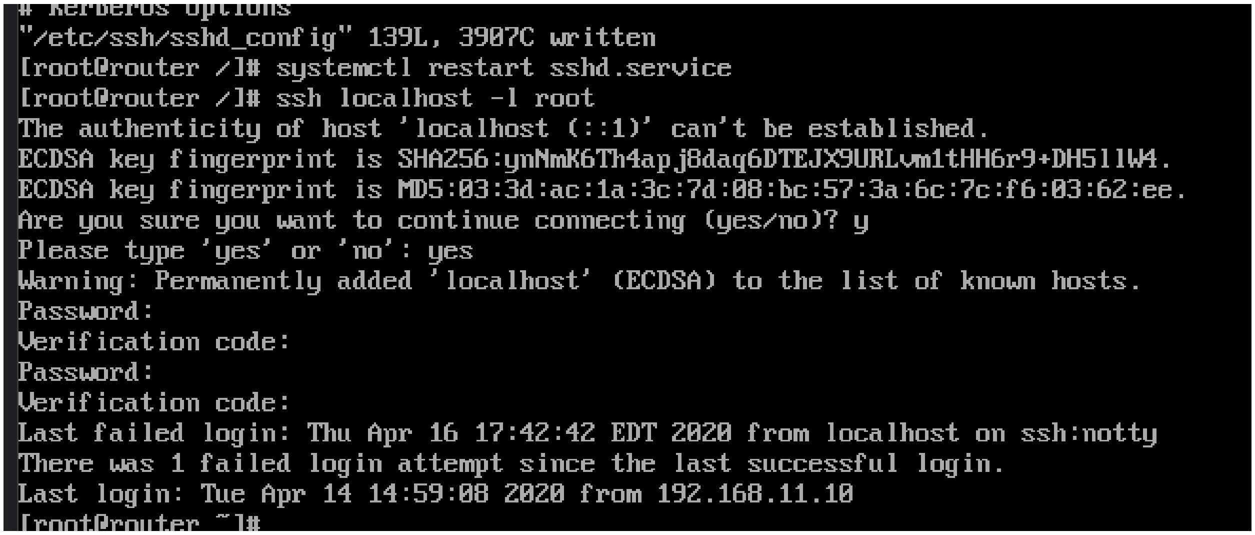
ssh localhost -l root

Are you sure: yes

Password: (router password)

Verification code: (google authentication code from phone app)

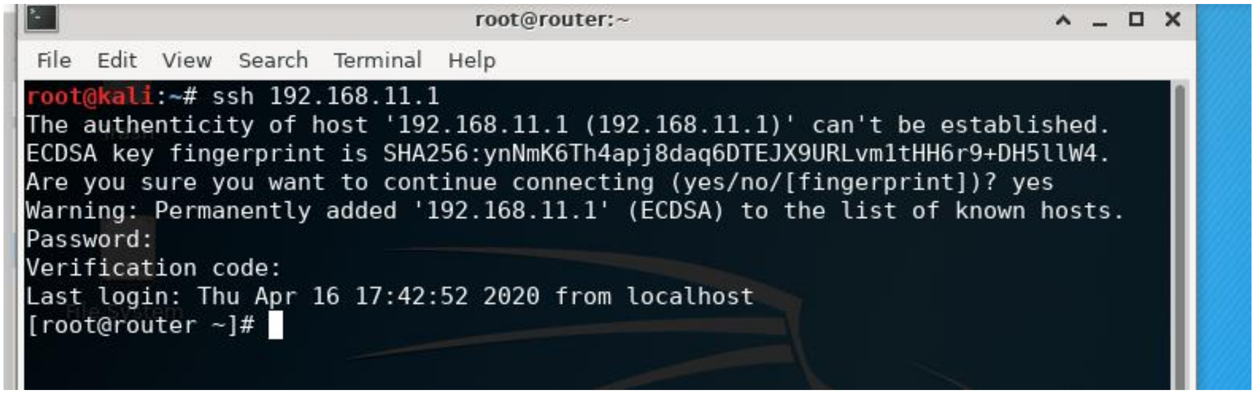
Note that the password and Google Authentication code to not show up when typed in for added security measures.



```
# Kerberos options
"/etc/ssh/sshd_config" 139L, 3907C written
[root@router /]# systemctl restart sshd.service
[root@router /]# ssh localhost -l root
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:ynNmK6Th4apj8daq6DTEJX9URLvm1tHH6r9+DH5llW4.
ECDSA key fingerprint is MD5:03:3d:ac:1a:3c:7d:08:bc:57:3a:6c:7c:f6:03:62:ee.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
Password:
Verification code:
Password:
Verification code:
Last failed login: Thu Apr 16 17:42:42 EDT 2020 from localhost on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Tue Apr 14 14:59:08 2020 from 192.168.11.10
[root@router ~]#
```

Figure 3 Logging into router with google authentication

For the last proof of good authentication, the router was entered via SSH from the KaliVM.



```
root@kali:~# ssh 192.168.11.1
The authenticity of host '192.168.11.1 (192.168.11.1)' can't be established.
ECDSA key fingerprint is SHA256:ynNmK6Th4apj8daq6DTEJX9URLvm1tHH6r9+DH5llW4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.11.1' (ECDSA) to the list of known hosts.
Password:
Verification code:
Last login: Thu Apr 16 17:42:52 2020 from localhost
[root@router ~]#
```

Conclusion.

This lab was successful at teaching how to set up google authentication on the CentOS 7 router. This process was familiar as the student has been using two-factor authentication from google for a few years, but this is the first time Google Authenticator was installed on the students' phone and used as the tool for verification. The process for this was very easy to understand and user friendly. This is an important part of two-factor authorization as if the process is not simple enough, users will not use the service, making themselves more vulnerable in exchange for convenience. This service seemed like a great fit, convenient and with a lot of added security for the time it takes to complete the short authorizations. Overall this lab was an excellent learning experience and a great source for future router and network authentication administration.

References

Abrams, Lawrence. (November 29, 2019). *Kali Linux adds 'undercover' mode to impersonate* Windows 10. BleepingComputer. Retrieved from https://www.bleepingcomputer.com/news/security/kali-linux-adds-undercover-mode-to-impersonate-windows-10/

Centos Blog (2020). *What is Centos?* Retrieved from https://www.centosblog.com/what-is-centos/

Cheng, Simon M.C. (October 27, 2014). *Basic concept of ProxMox Virtual Environment.* Packt. Retrieved from https://hub.packtpub.com/basic-concepts-proxmox-virtual-environment/

Chin, Casey. (July, 22, 2018). *How to secure your accounts with better two-factor authentication.* Retreived from https://www.wired.com/story/two-factor-authentication-apps-authy-google-authenticator/

Elwood. (November 26, 2019). *Kali Linux 2019.4 release*. Kali Linux News. Retrieved from https://www.kali.org/news/kali-linux-2019-4-release/

Kenton, Will. (May 9, 2019). *Two-factor authentication (2FA).* Retreived from https://www.investopedia.com/terms/t/twofactor-authentication-2fa.asp

ProxMox. (April 11, 2019). ProxMox.com Retrieved from https://www.proxmox.com/en/news/press-releases/proxmox-ve-5-4

SSH(Secure Shell). (2020). SSH.com. Retrieved from https://www.ssh.com/ssh

What is KVM? (2020) RedHat.com Retrieved from https://www.redhat.com/en/topics/virtualization/what-is-KVM

Lab Network Topology

Kali2020VM--VMWare ethernet adapter--Student HP----(internal –router—external)

192.168.22.136 192.168.22.1 10.0.0.17 10.0.0.1 192.168.104.161

/

/

WWW

|

Gateway 10.42.0.1

|

chewy 10.42.0.31/16

|

darknet 172.16.0.3/16

|

External 172.16.242.32

router

Internal 192.168.11.1

/ \

Kali VM 192.168.11.10 WebServerVM 192.168.11.15