

Lab #10: System Monitoring
CSC432 – Computer Information and Security
Franklin Nuth
5 April 2019

Abstract

In this lab, I will be working on setting up system monitoring software on my web server. I will Cacti, a system monitoring software for Cent OS 7 that will allow me to see information about the devices on my network. I will configure the MySQL databases and configuration files for the Cacti installation so it can work for me when I enter my web server from my Kali machine.

Introduction

Even on fully secure networks, system monitoring is an important aspect that most admins must acknowledge and utilize to maintain a high standard of security. System monitoring can be used to observe the amount of resources being used on any device on a network, from processing power to hard drive capacity. It will be easier to upgrade and replace devices when they are not running. Because information given to the Cacti software is detailed and real-time, admins have no excuse to delay on making fixes for both present and future attacks. I will be installing Cacti and observing how it will help me as an administrator of my virtual network.

Processes & Screenshots

There a number of things I needed to do before installing Cacti. First of all, I need to clean out the standard yum repository with “yum install epel-release” on my web server.

```
QEMU (CSC432-fsnuth-Web) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432050&vmname=CSC432-fsnuth-Web&node=atris

[root@web ~]# yum install epel-release
Loaded plugins: fastestmirror
Reposdata is over 2 weeks old. Install yum-cron? Or run: yum makecache fast
base                               | 3.6 kB  00:00:00
extras                             | 3.4 kB  00:00:00
updates                             | 3.4 kB  00:00:00
(1/2): extras/7/x86_64/primary_db   | 187 kB  00:00:00
(2/2): updates/7/x86_64/primary_db | 3.4 MB  00:00:00
Determining fastest mirrors
 * base: mirrors.rit.edu
 * extras: mirrors.rit.edu
 * updates: mirrors.rit.edu
Resolving Dependencies
--> Running transaction check
--> Package epel-release.noarch 0:7-11 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package                        Arch      Version      Repository      Size
=====
Installing:
epel-release                   noarch    7-11         extras           15 k

Transaction Summary
=====
Install 1 Package

Total download size: 15 k
Installed size: 24 k
Is this ok [y/d/N]: y
Downloading packages:
epel-release-7-11.noarch.rpm      | 15 kB  00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : epel-release-7-11.noarch                                1/1
  Verifying  : epel-release-7-11.noarch                                1/1

Installed:
  epel-release.noarch 0:7-11

Complete!
[root@web ~]# _
```

(The result of typing “yum install epel-release” on my web server. Everything is now ready for installing Cacti.)

After cleaning out the repositories, we now install Cacti with “yum install mariadb cacti”.

```
QEMU (CSC432-fsnuth-Web) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432050&vmname=CSC432-fsnuth-Web&node=atris

=====
Install 1 Package (+7 Dependent packages)

Total download size: 12 M
Installed size: 62 M
Is this ok [y/d/N]: y
Downloading packages:
(1/8): perl-Compress-Raw-Bzip2-2.061-3.el7.x86_64.rpm | 32 kB 00:00:00
(2/8): perl-Compress-Raw-Zlib-2.061-4.el7.x86_64.rpm | 57 kB 00:00:00
(3/8): perl-DBD-MySQL-4.023-6.el7.x86_64.rpm | 140 kB 00:00:00
(4/8): perl-IO-Compress-2.061-2.el7.noarch.rpm | 260 kB 00:00:00
(5/8): perl-DBI-1.627-4.el7.x86_64.rpm | 802 kB 00:00:00
(6/8): perl-Net-Daemon-0.48-5.el7.noarch.rpm | 51 kB 00:00:00
(7/8): perl-PIRPC-0.2020-14.el7.noarch.rpm | 36 kB 00:00:00
(8/8): mariadb-server-5.5.60-1.el7_5.x86_64.rpm | 11 MB 00:00:03
-----
Total 3.5 MB/s | 12 MB 00:00:03
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : perl-Compress-Raw-Bzip2-2.061-3.el7.x86_64 1/8
  Installing : 1:perl-Compress-Raw-Zlib-2.061-4.el7.x86_64 2/8
  Installing : perl-IO-Compress-2.061-2.el7.noarch 3/8
  Installing : perl-Net-Daemon-0.48-5.el7.noarch 4/8
  Installing : perl-PIRPC-0.2020-14.el7.noarch 5/8
  Installing : perl-DBI-1.627-4.el7.x86_64 6/8
  Installing : perl-DBD-MySQL-4.023-6.el7.x86_64 7/8
  Installing : 1:mariadb-server-5.5.60-1.el7_5.x86_64 8/8
  Verifying : 1:mariadb-server-5.5.60-1.el7_5.x86_64 1/8
  Verifying : perl-Net-Daemon-0.48-5.el7.noarch 2/8
  Verifying : perl-DBD-MySQL-4.023-6.el7.x86_64 3/8
  Verifying : perl-IO-Compress-2.061-2.el7.noarch 4/8
  Verifying : 1:perl-Compress-Raw-Zlib-2.061-4.el7.x86_64 5/8
  Verifying : perl-DBI-1.627-4.el7.x86_64 6/8
  Verifying : perl-Compress-Raw-Bzip2-2.061-3.el7.x86_64 7/8
  Verifying : perl-PIRPC-0.2020-14.el7.noarch 8/8

Installed:
  mariadb-server.x86_64 1:5.5.60-1.el7_5

Dependency Installed:
  perl-Compress-Raw-Bzip2.x86_64 0:2.061-3.el7 perl-Compress-Raw-Zlib.x86_64 1:2.061-4.el7 perl-DBD-MySQL.x86_64 0:4.023-6.el7
  perl-DBI.x86_64 0:1.627-4.el7 perl-IO-Compress.noarch 0:2.061-2.el7 perl-Net-Daemon.noarch 0:0.48-5.el7
  perl-PIRPC.noarch 0:0.2020-14.el7

Complete!
[root@web ~]#
```

(Installing everything needed to run Cacti with “yum install mariadb-server cacti”. We will be working very closely with MySQL very soon.)

```
QEMU (CSC432-fsnuth-Web) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432050&vmname=CSC432-fsnuth-Web&node=atris

[root@web ~]# service mariadb status
Redirecting to /bin/systemctl status mariadb.service
mariadb.service - MariaDB database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled)
   Active: active (running) since Mon 2019-04-01 10:11:39 EDT; 54s ago
     Process: 2915 ExecStartPost=/usr/libexec/mariadb-wait-ready $MAINPID (code=exited, status=0/SUCCESS)
     Process: 2884 ExecStartPre=/usr/libexec/mariadb-prepare-db-dir %n (code=exited, status=0/SUCCESS)
    Main PID: 2914 (mysqld_safe)
      CGroup: /system.slice/mariadb.service
              └─2914 /bin/sh /usr/bin/mysqld_safe --basedir=/usr
                └─3077 /usr/libexec/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql/plugin --log-erro...

Apr 01 10:11:37 web.localdomain systemd[1]: Starting MariaDB database server...
Apr 01 10:11:37 web.localdomain mariadb-prepare-db-dir[2884]: Database MariaDB is probably initialized in /var/lib/mysql ...one.
Apr 01 10:11:37 web.localdomain mariadb-prepare-db-dir[2884]: If this is not the case, make sure the /var/lib/mysql is em...dir.
Apr 01 10:11:37 web.localdomain mysqld_safe[2914]: 190401 10:11:37 mysqld_safe Logging to '/var/log/mariadb/mariadb.log'.
Apr 01 10:11:37 web.localdomain mysqld_safe[2914]: 190401 10:11:37 mysqld_safe Starting mysqld daemon with databases fro...mysql
Apr 01 10:11:39 web.localdomain systemd[1]: Started MariaDB database server.
Hint: Some lines were ellipsized, use -l to show in full.
[root@web ~]# _
```

(Double checking with “service mariadb status” to make sure that my MariaDB is running.)

After that, we use “mysql -u root -p” to access the database server. Because I do not have a password, I just have to enter and I’m in.

```
QEMU (CSC432-fsnuth-Web) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432050&vmname=CSC432-fsnuth-Web&node=atris

[root@web ~]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 3
Server version: 5.5.60-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database cacti;
Query OK, 1 row affected (0.00 sec)

MariaDB [(none)]> grant all privileges on cacti.* to cacti@localhost identified by 'cacti';
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> quit;
Bye
root@web ~]#
```

(Making it into the MariaDB server. This is where I can do MySQL commands for my database.)

```
QEMU (CSC432-fsnuth-Web) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432050&vmname=CSC432-fsnuth-Web&node=atris

glibc-common-2.17      libXau-1.0.8          python-pyudev-0.15
glib-networking-2.40.0 libXdamage-1.1.4      python-setuptools-0.9.8
gmp-6.0.0              libXext-1.3.3         python-slip-0.4.0
gnupg-2.0.22           libXfixes-5.0.3       python-slip-dbus-0.4.0
gnutls-3.3.8           libXft-2.3.2          python-urlgrabber-3.10
gobject-introspection-1.36.0 libxml2-2.9.1         pyxattr-0.5.1
gpgme-1.3.2            libXpm-3.5.12         qrencode-libs-3.4.1
graphite2-1.3.10       libXrender-0.9.10     readline-6.2
grep-2.20              libxslt-1.1.28        redhat-release
groff-base-1.22.2      libXxf86vm-1.1.4      rpm-4.11.1
grub2-2.02             libzip-0.10.1         rsyslog-7.4.7
grub2-tools-2.02       linux-firmware-20140911 sed-4.2.2
grubby-8.28            logrotate-3.8.6       setup-2.8.71
gsettings-desktop-schemas-3.8.2 lua-5.1.4             shadow-utils-4.1.5.1
gzip-1.5               lvm2-2.02.115         shared-mime-info-1.1
harfbuzz-1.7.5         lzo-2.06              slang-2.2.4
hostname-3.13          mailcap-2.1.41        snappy-1.1.0
httpd-2.4.6            make-3.82             sqlite-3.7.17
httpd-tools-2.4.6      man-db-2.6.3          sudo-1.8.6p7
hwdata-0.252           mariadb-5.5.60        systemd
info-5.1               mariadb-libs-5.5.60  sysvinit-tools-2.88
itscripts-9.49.24      microcode_ctl         t1lib-5.1.2
route-3.10.0           mozjs17-17.0.0        tar-1.26
rutils-2.4.3           ncurses-5.9           tcp_wrappers-libs-7.6
iptables-1.4.21        ncurses-base-5.9      teamd-1.15
iputils-20121221       net-snmp-5.7.2        trousers-0.3.11.2
irqbalance-1.0.7       net-snmp-libs-5.7.2   tuned-2.4.1
iotw-firmware-20080701 nettle-2.7.1          tzdata-2015g
iwl1000-firmware-39.31.5.1 net-tools-2.0         ustr-1.0.4
iwl100-firmware-39.31.5.1 NetworkManager        util-linux-2.23.2
iwl105-firmware-18.168.6.1 NetworkManager-1.0.0  virt-what-1.13
iwl135-firmware-18.168.6.1 neut-0.52.15          which-2.20
iwl2000-firmware-18.168.6.1 neut-python-0.52.15  wpa_supplicant-2.0
iwl2030-firmware-18.168.6.1 nss_compat_oss1-0.9.6 xfsprogs-3.2.1
iwl13160-firmware-22.0.7.0 openldap-2.4.39        xz-5.1.2
iwl13945-firmware-15.32.2.9 openssh-6.6.1p1        xz-libs-5.1.2
iwl4965-firmware-228.61.2.24 openssl-1.0.2k         yum-3.4.3
iwl5000-firmware-8.83.5.1_1 os-prober-1.58         yum-metadata-parser-1.1.4
iwl15150-firmware-8.24.2.2 p11-kit-0.20.7         yum-plugin-fastestmirror-1.1.31
iwl6000-firmware-9.221.4.1 pam-1.1.8              zlib-1.2.7
iwl6000g2a-firmware-17.168.5.3 pango-1.42.4
iwl6000g2b-firmware-17.168.5.2 parted-3.1

[root@web doc]# mysql -u cacti -p -D cacti < /usr/share/doc/cacti-1.2.2/cacti.sql
Enter password:
[root@web doc]# mysql -u cacti -p -D cacti < /usr/share/doc/cacti-1.2.2/cacti.sql
Enter password:
ERROR 1050 (42S01) at line 12: Table 'aggregate_graph_templates' already exists
[root@web doc]#
```

(Afterwards, we initialize the SQL database with the source file by typing in “mysql -u cacti -p -D cacti < /usr/share/doc/cacti-1.2.2/cacti.sql”.)

```
QEMU (CSC432-fsnuth-Web) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432050&vmname=CSC432-fsnuth-Web&node=atris

<?php
/**
 *-----*
 * | Copyright (C) 2004-2019 The Cacti Group |
 * | |
 * | This program is free software; you can redistribute it and/or |
 * | modify it under the terms of the GNU General Public License |
 * | as published by the Free Software Foundation; either version 2 |
 * | of the License, or (at your option) any later version. |
 * | |
 * | This program is distributed in the hope that it will be useful, |
 * | but WITHOUT ANY WARRANTY; without even the implied warranty of |
 * | MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the |
 * | GNU General Public License for more details. |
 * |-----*
 * | Cacti: The Complete RRDtool-based Graphing Solution |
 * |-----*
 * | This code is designed, written, and maintained by the Cacti Group. See |
 * | about.php and/or the AUTHORS file for specific developer information. |
 * |-----*
 * | http://www.cacti.net/ |
 * |-----*
 */

/*
 * Make sure these values reflect your actual database/host/user/password
 */

$database_type      = 'mysql';
$database_default   = 'cacti';
$database_hostname   = 'localhost';
$database_username   = 'cacti';
$database_password   = 'cacti';
$database_port       = '3306';
$database_ssl        = false;
$database_ssl_key     = '';
$database_ssl_cert    = '';
$database_ssl_ca      = '';

/*
 * When the cacti server is a remote poller, then these entries point to
 * the main cacti server. Otherwise, these variables have no use and
 * must remain commented out.
 */

#$database_type      = 'mysql';
#$database_default   = 'cacti';
-- INSERT --
```

(Configuring my database information to work in the “db.php” file.)


```
QEMU (CSC432-fsnuth-Web) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432050&vmname=CSC432-fsnuth-Web&node=atris

#
# Cacti: An rrd based graphing tool
#
# For security reasons, the Cacti web interface is accessible only to
# localhost in the default configuration. If you want to allow other clients
# to access your Cacti installation, change the httpd ACLs below.
# For example:
# On httpd 2.4, change "Require host localhost" to "Require all granted".
# On httpd 2.2, change "Allow from localhost" to "Allow from all".

Alias /cacti /usr/share/cacti

<Directory /usr/share/cacti/>
    <IfModule mod_authz_core.c>
        # httpd 2.4
        Require all granted
    </IfModule>
    <IfModule !mod_authz_core.c>
        # httpd 2.2
        Order deny,allow
        Deny from all
        Allow from 192.168.0.1
    </IfModule>
</Directory>

<Directory /usr/share/cacti/install>
    # mod_security overrides.
    # Uncomment these if you use mod_security.
    # allow POST of application/x-www-form-urlencoded during install
    #SecRuleRemoveById 960010
    # permit the specification of the rrdtool paths during install
    #SecRuleRemoveById 900011
</Directory>

# These sections marked "Require all denied" (or "Deny from all")
# should not be modified.
# These are in place in order to harden Cacti.
<Directory /usr/share/cacti/log>
    <IfModule mod_authz_core.c>
        Require all denied
    </IfModule>
    <IfModule !mod_authz_core.c>
        Order deny,allow
        Deny from all
    </IfModule>
</Directory>

"cacti.conf" 57L, 1504C
```

(The configuration of my “cacti.conf” file. We configure the httpd service here so that cacti works properly.)

```
QEMU (CSC432-fsnuth-Web) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432050&vmname=CSC432-fsnuth-Web&node=atris

... or under UNIX:
extension=mysqli.so

... or with a path:
extension=/path/to/extension/mysqli.so

If you only provide the name of the extension, PHP will look for it in its
default extension directory.

;;;
; Note: packaged extension modules are now loaded via the .ini files
; found in the directory /etc/php.d; these are loaded by default.
;;;

; Module Settings ;

[CLI Server]
; Whether the CLI web server uses ANSI color coding in its terminal output.
cli_server.color = On

[Date]
; Defines the default timezone used by the date functions
; http://php.net/date.timezone
date.timezone = America/New_York

; http://php.net/date.default-latitude
date.default_latitude = 31.7667

; http://php.net/date.default-longitude
date.default_longitude = 35.2333

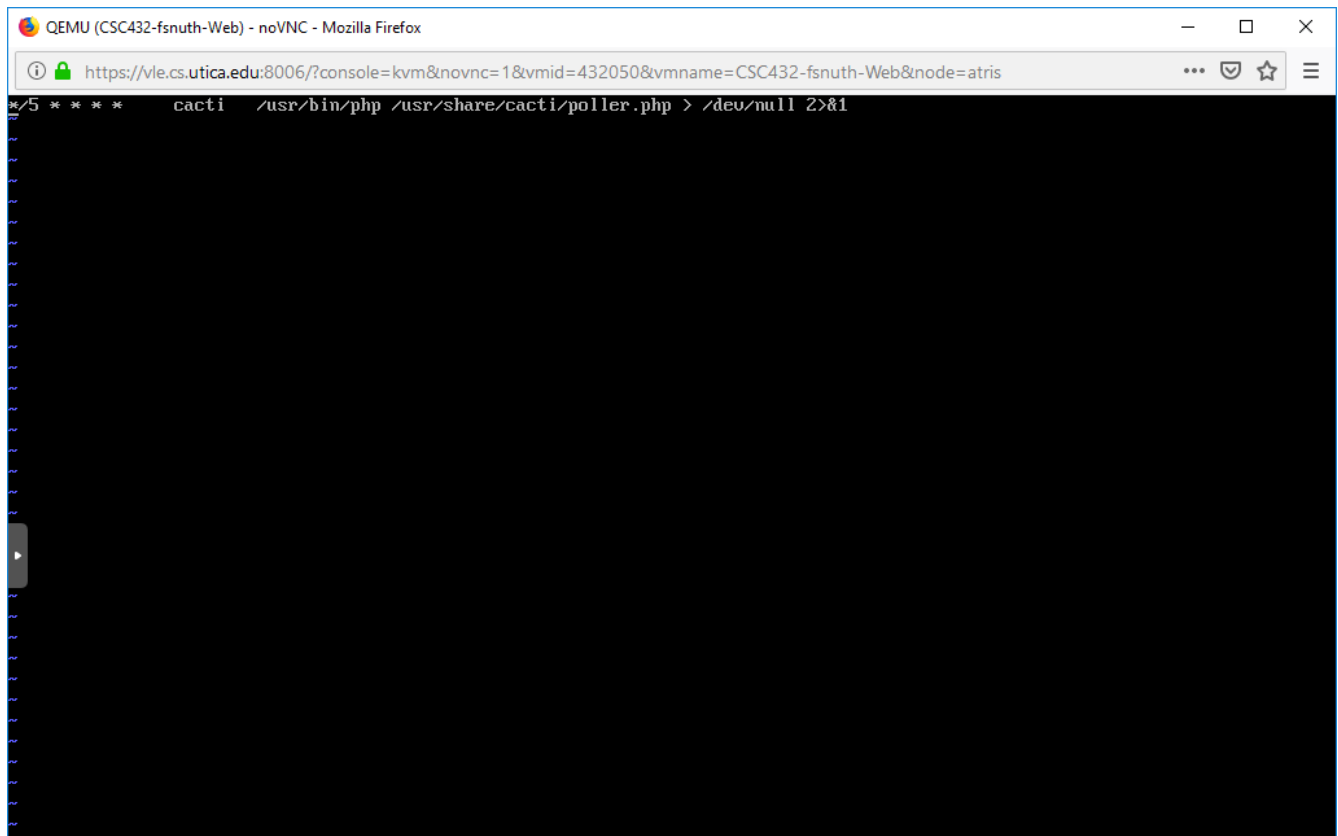
; http://php.net/date.sunrise-zenith
date.sunrise_zenith = 90.583333

; http://php.net/date.sunset-zenith
date.sunset_zenith = 90.583333

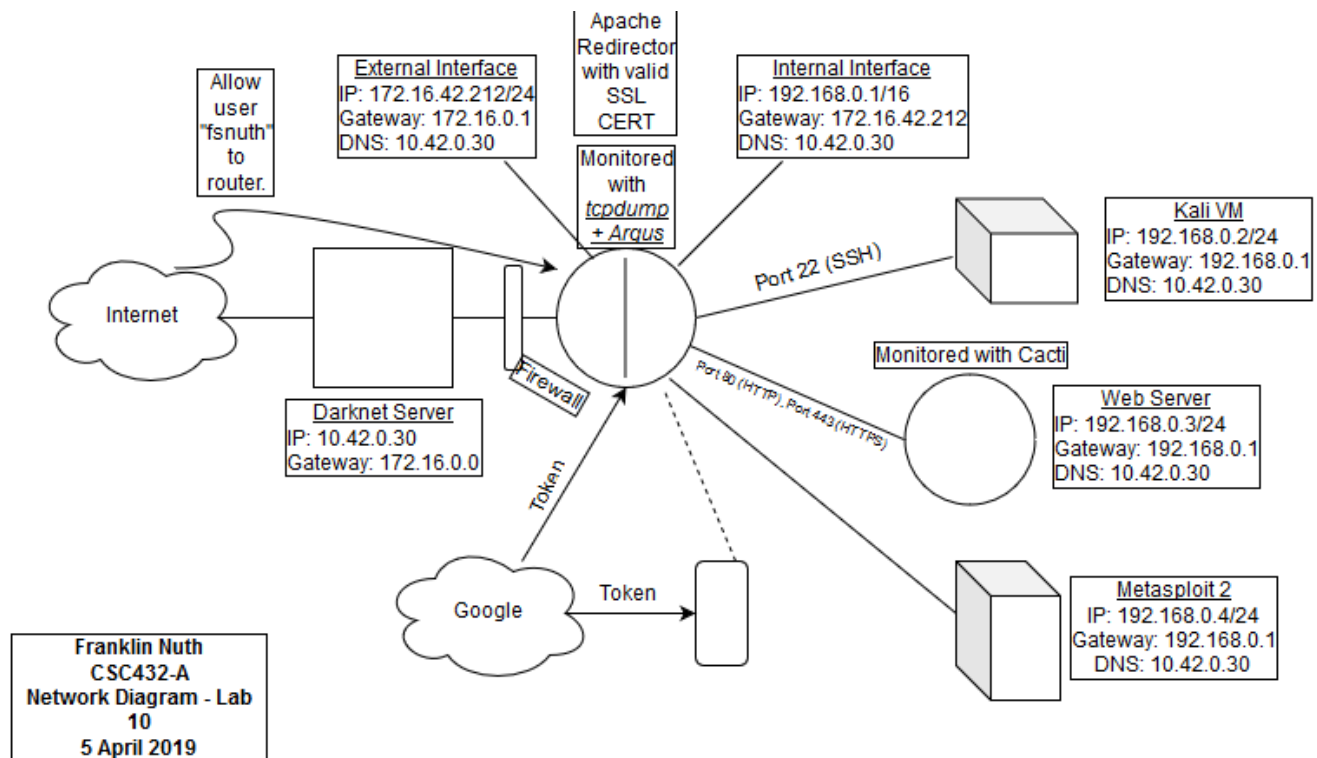
[filter]
; http://php.net/filter.default
filter.default = unsafe_raw

; http://php.net/filter.default-flags
filter.default_flags =
```

(Changing the time zone to “America/New_York”. This will let the service know my time zone and adjust to me accordingly.)



(Uncommenting the line so that the user named “cacti” will have access to the resources on the web server.)



Issues & Resolutions

The first issues that I ran into was getting denied from my own Cacti server. I think this might be a problem in either the configuration of my files, my MySQL queries, the absence of some packages, or just a bug in my Apache software. I'll get back to this part when I resolved the issue.

Conclusion

In this lab, I have attempted to install Cacti on my web server. I have used MySQL to do queries in the database to try and allow the user named 'cacti' access to the web server. I was not successful in installing Cacti, but I have learned a great deal about installing monitoring software and MySQL.

References

- Dominguez, Alberto. 5 April 2019. *The importance of having a good monitoring system*. Retrieved from: <https://blog.pandorafms.org/why-you-need-a-monitoring-system/>
- The Apache Software Foundation. 1 January 2019. *Upgrading to 2.4 from 2.2*. Retrieved from: <https://httpd.apache.org/docs/2.4/upgrading.html>