Proxy Filtering Project

Setup

For this assignment, you will need to minimally use your ubuntu vm instance to install the proxy programs and some vm instance that has a browser to test if the proxy is working correctly.

- Your squid should listen on 3128, e2guardian on 8282(change the `filterport` in the e2guardian.conf file). Squid and e2guardian should be on the same machine.
- **YOU MUST DISABLE THE FIREWALL ON YOUR UBUNTU MACHINE, by doing a `sudo ufw disable` or `sudo ufw stop`** (It may already be disabled)
- Edit your browser config to make requests through your proxy. Using something like foxproxy can make your changes easier. You should visit some websites and make sure that things work. You should be able to view access logs in `/var/log/squid/access.log`. If you connect to port 3128, only the squid rules will be processed. If you connect to 8282, e2guardian will process its' rules first and then will forward onto squid.
- Whenever you make changes to the squid configuration file you will have to do a `sudo service squid3 restart` to make them take effect.

You can see some screenshots as to how to begin this assignment here.

Tasks

Remember to make sure that you are TASTEFUL. We need not experiment with any questionable sites to test our rules.

- Use Squid to do the following
  - Restrict people using an Mozilla browser from accessing any sites on Thursdays and Fridays from 8am to 5pm (might have to install a mozilla browser to test it).
  - Restrict anyone from accessing any .utahtech.edu site.
  - Restrict anyone from accessing any URL that has the word 'corn' in it.
  - Restrict the HTTP POST method from anyone.
- Use e2guardian to do the following:
  - Block access to the site: msn.com
  - Block a site if both the words 'evil' and 'computer' appear on the same page
  - Block downloading of all pdf files
  - Research 2 other e2guardian lists that you want to and do it.

- Install squidguard and a blacklist as described below:

  - `sudo apt-get install squidguard`
  - Grab blacklists from here

  - I untarred mine in the `/etc/squid/blacklists/`

  - edit `/etc/squidguard/squidGuard.conf` (to contain only this)

```
dbhome /var/lib/squidguard/db
logdir /var/log/squidguard
dest bad{
   domainlist /etc/squid/blacklists/bad/domains
}
acl {
   default {
      pass !bad all
      redirect http://localhost/blocked.html
    }
}
```

  - Change the word `localhost` above, to the ip of your squid machine... (Really, it just needs to be pointed to any web server that has the blocked message you want).. I installed apache2 on my squid server and created `/var/www/html/blocked.html` with some content in it, and reloaded squid.

  - Note that it is looking for the `bad/domains` file. (I created this, but you could point it to any of those that are in your blacklists directory. You could look in any of those blacklist directories to see how they are structured).

- Add an entry at the end of squid.conf

  url_rewrite_program /usr/bin/squidGuard -c /etc/squidguard/squidGuard.conf

- spacing and indentation is critical in the squidGuard.conf file, look at tail -f /var/log/squid/squidGuard.log to make sure it is working correctly. That file, blocked.html must exist in correct dir
- Obviously test it to see if your sites are being blocked.
- Make sure that squid has loaded correctly.

To pass off

- Copy the relevant squid rules to a file.
- Take a screenshot of the other stuff in action

NOTE

Proxies are VERY exploitable from malicious do-badders on the internet. Make sure that you are listening at the port above. When I have marked off your assignment score, please disable your proxy.