Assignment 1 - Discovery

Instructions:

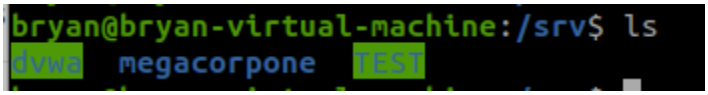
With the trend of social media and gaining a network being a common priority these days, many organizations expose too much information to the public. This abundance of information helps attackers organize their attacks. You will step into the shoes of an attacker and see how attackers collect information before an attack.

You are to use your OSINT skills to answer the following questions by performing reconnaissance on a site you set up. Each question will be worth the specified number of points. The assignment will be worth a total of 40 points with 32 points being from answers to the questions, and 8 points for overall report quality (spelling, grammar, use of complete sentences, formatting, etc.). Your submission to each question must provide a walkthrough of how you obtained the solution, accompanied by screenshots. Your walkthroughs must be detailed enough so that they can be replicated by someone with basic technical skills.

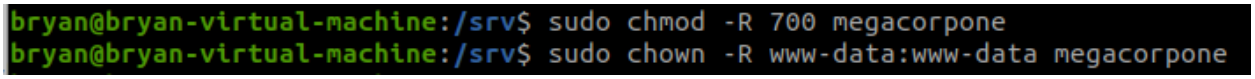
Before you start:

You are to first set up the megacorpone website (zip file provided on BrightSpace) on a Ubuntu machine. **All requests and active reconnaissance must be performed on your site, and no other target, unless the question specifically mentions it.** Follow the directions below to install your megacorpone site (assuming you have Apache installed on your machine).

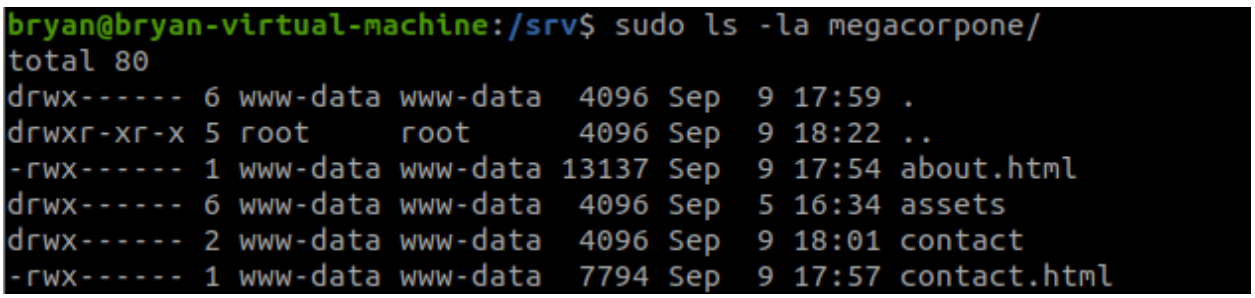
- Extract the megacorpone.zip file and place it in your /srv folder



- Change the permissions and ownership



- Verify that the permissions are similar to what is below



- Now modify your /etc/apache2/apache.conf file to include the following data, changing the Directory value and the AllowOverride value

```
  GNU nano 6.2                    /etc/apache2/apache2.conf *
# your system is serving content from a sub-directory in /srv you must a
# access here, or in any related virtual host.
<Directory />
        Options FollowSymLinks
        AllowOverride None
        Require all denied
</Directory>

<Directory /usr/share>
        AllowOverride None
        Require all granted
</Directory>

<Directory /srv/megacorpone>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
</Directory>
```

- Now modify /etc/apache2/sites-enabled/000-default.conf to have the following information

```
 GNU nano 6.2        /etc/apache2/sites-enabled/000-default.conf *
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and po
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header
        # match this virtual host. For the default virtual host (this file)
        # value is not decisive as it is used as a last resort host regardl
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /srv/megacorpone
```

- Run `sudo systemctl start apache2` to start your web server

- Run `ip a` and show your results at the beginning of your assignment submission. All requests you make to the site in your assignment submissions should match your ens33 or eth0 IP address.

```
bryan@bryan-virtual-machine:/srv$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:55:01:47 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.42.80/24 brd 192.168.42.255 scope global dynamic noprefixroute
ens33
       valid_lft 253525sec preferred_lft 253525sec
    inet6 fe80::8b25:7f6c:74f2:f0bc/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN
 group default qlen 1000
    link/ether 52:54:00:a1:08:d5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
       valid_lft forever preferred_lft forever
```

Assignment:

You can now visit your site from the browser on your host or Kali machine. It is recommended to clear your browser's cache before starting the assignment.

1. Who is the VP of legal and what is their Email address? (4 points)

2. During class, we conducted a DNS zone transfer on MegaCorpOne's name server. Given the list of subdomains we found, what subdomains look like good targets for an attack and why? Pickl 3 subdomains. (4 points)

3. What email address does the contact-us form go to? (4 points)

4. When was the site last updated? (4 points)

5. Can you find the secret message and what does it say? (4 points)

6. Plan out a social engineering attack against a target of your choosing. You may use any number of attacks (email phishing, vishing, etc.) in an attempt to gain initial access into MegaCorpOne's environment (credentials, workstation access, M365, VPN, etc.). You must explain each step of the attack including what you would say to the target, who you are pretending to be (if applicable), why you chose the target, and list potential replies to your social engineering. (12 points)