Exercise: Mr Robot - Defending with Firewall Rate Limiting

Steps

This is the third MrRobot exercise. If you haven't done the others yet, please use the attack path from the first to secure `root` access on this system. If you don't have time for that, use the Getting SSH Access on the MrRobot Virtual Machine instructions to do this.

We'd like to break the `wfuzz` run in a different way than using OSSEC. There's no reason for legitimate users to need to make quite so many authentication attempts.

In the first exercise, we used `wfuzz` to guess usernames at a tremendously fast rate. We needed speed to be effective there as attackers.

Let's configure `iptables` to stop anyone from starting quite so many new connections in a specific time window. This isn't anywhere as surgical as OSSEC, but it doesn't require adding any programs to a system.

1. First, let's login to the MrRobot VM as `robot`, `sudo su -` to `root`, and deactivate OSSEC:

   ```
   ssh robot@mrrobot
   abcdefghijklmnopqrstuvwxyz
   sudo su -
   /var/ossec/bin/ossec-control stop
   ```

2. Now, on the Kali terminal, try running that `wfuzz` to make sure it works:

   ```
   wfuzz -c -z file,wordlist.txt --hs "Invalid username" -d "log=FUZZ&pwd=unlikelypass" ht
   ```

3. Now, point your browser at the MrRobot login page, so you can see that things are working fine:

   http://mrrobot/wp-login.php

4. Next, back in the MrRobot terminal, let's use `ufw` (Ubuntu's uncomplicated firewall) to create a rate limiting rule that we'll then investigate with `iptables`. First, find the current port `80/http` rule number:

```
ufw status numbered
```

5. Find the rule that has `80/tcp` on it and note the rule number - use that in the next command in place of `$CHANGEME`:

   ```
   ufw delete $CHANGEME
   ```

6. Now, add a rule that allows port `80`, but limits it:

   ```
   ufw limit 80/tcp
   ```

7. Take a look at the iptables rule that `ufw` put in place, so you can see how rate limiting works in `iptables`:

   ```
   iptables-save | grep 80 | grep seconds
   ```

8. Now, point your browser at the MrRobot login page, so you can see that things are working fine:

   http://mrrobot/wp-login.php

9. Now, on the Kali terminal, try running that `wfuzz` command - you should see it fail, as it starts by opening too many connections at once to MrRobot for our new rate-limiting rule:

   ```
   wfuzz -c -z file,wordlist.txt --hs "Invalid username" -d "log=FUZZ&pwd=unlikelypass" ht
   ```

10. Change your Slack status to `:thumbsup:`.

11. Suspend the virtual machines:

    ```
    sudo /scripts/suspend-all-vms.sh
    ```