PenTest Lab Exercise Ex100 – Responder

Goal

Use Responder to capture credentials.

Tasks

1. Log in to the ndg box and schedule an exercise Ex100 lab.
2. Use information you gained from previous activities to get root access to `devbox.artstailor.com`. Don't worry. Nothing's changed in that department since your last excursion.
3. You will find, if you look around, that, as with most machines on the planet, this linux system does not have Responder installed. Copy the responder directory `/usr/share/responder` from `Kali`.
4. Check to see if `Responder` will be able to capture credentials. In particular capture network traffic (`tcpdump` is still in `ssl-extras` on `Kali`) that shows that spoofing the `wpad` host might bear fruit. Show this in your report.
5. If you run `Responder` with appropriate flags on, you may be able to capture credentials. You may want to take a look at Trelis's 2018 Blog Post to get a better idea of how to do this. I know that post is several years old, but Windows is still installed with `LLMNR` fallback by default.
6. When you run `Responder`, you may see some error messages about ports it could not open services on. You should kill any services that cause a conflict. You can see which executable has a port ### open by using

   ```
   sudo netstat -tnlp | grep ###
   ```

   If the executable doesn't have the same name as the service, it is usually relatively similar. You can get a list of services with

   ```
   sudo service --status-all
   ```

and you can kill the service named *service-name* with

`sudo service` *service-name* `stop`

7. As usual, feel free to store any relevant information you may find on `plunder.pr0b3.com` for later reference.

8. And, of course, write a partial penetration test report with your findings. Include an attack narrative if the information in your findings would not be sufficient for Hank to know you understand what you did and how it worked.