EDR Project By Maor Sofer

In the ReadMe.txt file you can read about the software (What the software do, What the server side do and what client side do, How to prepare the server to use and how to edit the website black list).
Here screenshot of the file:

```
 GNU nano 5.2                                                    ReadMe.txt
#### Endpoint Detection and Response (EDR) ####
The purpose of the software is to monitor the network traffic in the clients,
if something suspicious happens the client sends an alert to the server that something is happening.
It scan if MiTM attack happends, if the computer enters an unauthorized site and all the online client send heart beat every 30 seconds to show that they are online.
There is an apache2 server on the server side where the WebsiteBlackList.txt file exists which contains all the sites that have decided not to be accessed.

#### Clients ####
All The work happands in the clients side, the clients read all the traffic and send logs to the server
When the client is online he send heart beat to the server every 30 seconds to show that they are online.
Every minute the client scan the arp table and scan for duplicate mac, if he found a duplicate mac it send alert on MiTM to the server.
The client side always if the computer enter an unauthorized site and if he found he send alert on unauthorized site to the server.
Every hour the client scan if there any changes have been made to the WebsiteBlackList.txt file and that's how he knows if it is OK or if it needs to update its file.

#### Server ####
The server always listen for incoming connection to recevie logs from the clients.
When the server gets a log, he analyzes it and writes it in the right place.
   If the server get log about MiTM attack, he update it in the "MiTMDetect.log" file.
   If the server get log about unauthorized site, he update it in the "BlackListDetect.log" file.
   If the server get heart beat from client, he update it in the "AlivePCs.log" file.
The server also write all the logs in the "EDR.log" file.
The server also checks when the clients sent heart beat for the last time, if it is more than two minutes he deletes it from the "AlivePCs.log" file and writes it in the "EDR.log" file.

#### Prepare the server to use ####
First place the folder where you want it to be.
After this run the "ServerInstall.py" file, for install and configure all the necessary stuff for the server side of the EDR.
Before completing the installation, the "ChangeWebsiteBlackList.py" file will open and you can add urls to the black list.
After it finishes the installation is complete.
The installation install apache2 pn the server and it create a folder with the "WebsiteBlackList.txt" file in there,
it also create for you a "Logs" folder in the software location with four log files: "EDR.log", "AlivePCs.log", "MiTMDetect.log", "BlackListDetect.log".
When the installation is complete you can run the "EDR-Server.py" file to run the server or reboot your OS to run it automatically using crontab.

#### Edit the website black list ####
If you want to edit the website black list all you just need to do it run the "ChangeWebsiteBlackList.py" file and follow the instructions.
```

The EDR.log file should look like this:

```
 GNU nano 5.2                                                    EDR.log
1 2020/10/12 | 02:11:42 - [!] MiTM attack happend on 10.0.3.24
2 2020/10/12 | 02:12:12 - [+] Detect HeartBeat from 10.0.3.24
3 2020/10/12 | 02:12:34 - [!] 10.0.3.24 log in site 2 (facebook.com) from black list
4 2020/10/12 | 02:12:42 - [!] MiTM attack happend on 10.0.3.24
5 2020/10/12 | 02:12:42 - [+] Detect HeartBeat from 10.0.3.24
6 2020/10/12 | 02:12:42 - [!] MiTM attack happend on 10.0.3.24
7 2020/10/12 | 02:13:12 - [+] Detect HeartBeat from 10.0.3.24
8 2020/10/12 | 02:16:00 - [-] 10.0.3.24 are not alive
9
```

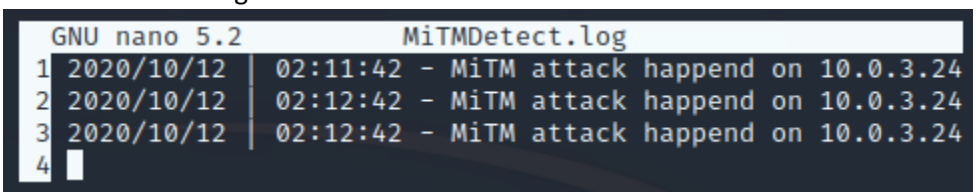
1+4+6 lines: The server find MiTM attack on one of the clients.
2+5+7 lines: The server find HeartBeat from one of the clients.
Third line: The server find that one of the clients log in to website that in the black list.
Eighth line: The server find that one of the client are not alive.

The BlackListDetect.log file should look like this:

```
 GNU nano 5.2                                            BlackListDetect.log
1 2020/10/12 | 02:12:34 - 10.0.3.24 log in site 2 (facebook.com) from black list
2
```

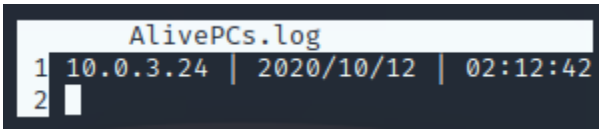
In here we see that the server find that one of the clients log in to website that in the black list.

The MiTMDetect.log file should look like this:



In here we see that the server find a MiTM attack (or three attacks) on one of the clients.

The AlivePCs.log file should look like this:



In here we see that the server find that one of the client are alive (online).