Capt Alamri, 2d Lt Hayden, 2d Lt Mireles

Project Tasks 3 & 4

22 January 2019

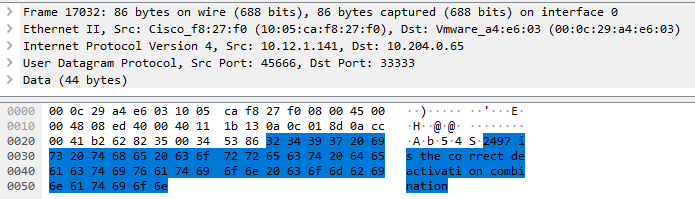
1. ***Mission Impossible***

Your mission, if you choose to accept it, is to craft a packet that will elicit the deactivation code for the deadly object called “The Rabbit’s Foot” from the highly-secure MI server on UDP port 2600.

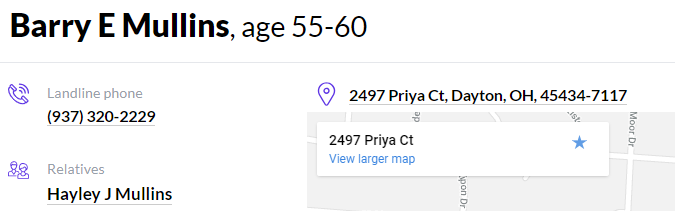
* 1. The request packet must conform to the following:
     + Payload is “**Ethan Hunt**” followed by a space followed by a string containing a number between **0000-9999** without leading zeroes. This number is the deactivation code.
       - Example: “**Ethan Hunt 1234**”
       - Example: “**Ethan Hunt 543**”
       - Example: “**Ethan Hunt 8860**”
     + Source port of request must be 3, 33, 333, 3333 or 33333
     + The response from the server will not contain the string “**ERROR**” if it receives the correct combination.
     + What is the deactivation code? Provide a screenshot showing the successful deactivation code; be sure your source IP is in the screenshot. What is the significance of this code number relative to Dr. Mullins?
  2. This target is named **mi#.m4i.local**, where # is your team number. For example, team 5 will interact with **mi5.m4i.local**.

**Solution:**

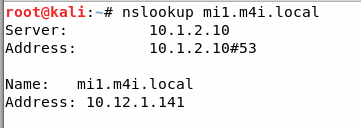
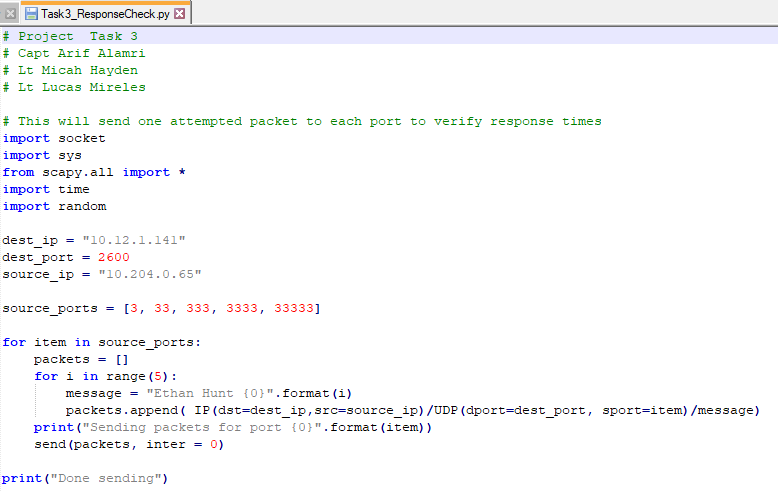
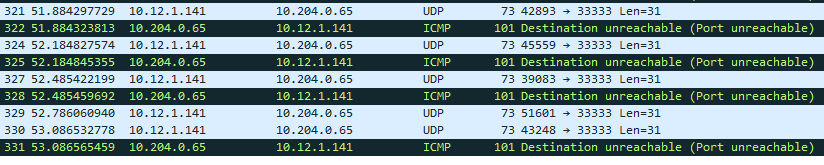
* Deactivation code is “Ethan Hunt 2497”.

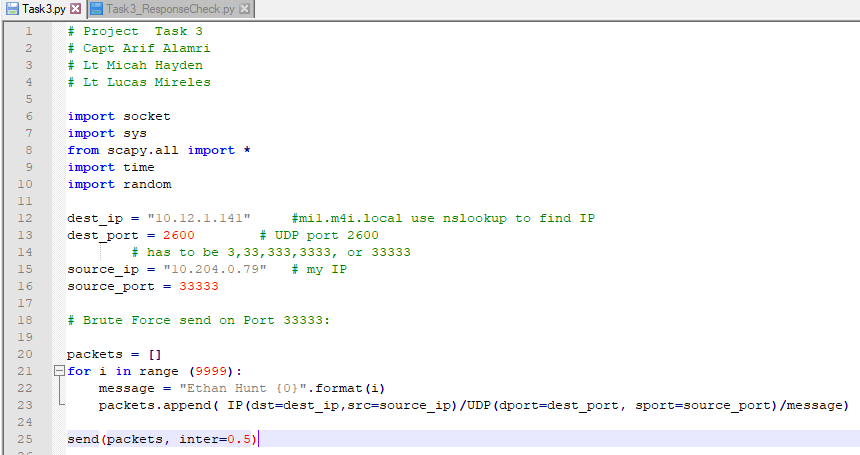


* The reply from the mi1.m4i.local server (10.12.1.141) sent the reply “2497 is the correct deactivation combination” to my IP of 10.204.0.65 and my port 33333.
* 2497 is Dr. Mullins’ street number, found by google searching “Barry Mullins 2497”, and going to the first link at https://nuwber.com/person/563a38b898f8a849c12d44ef

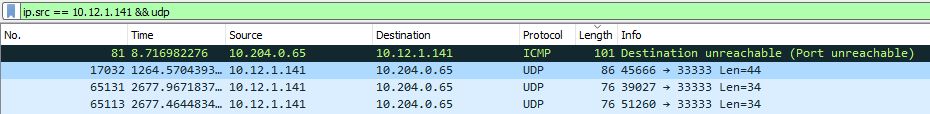


**Steps:**

* Ran nslookup mi1.m4i.local to find IP address of target machine:
* Sent one packet from each source port 3, 33, 333, 3333, and 33333 to determine which port would be the fastest to send all needed packets to determine correct combination. This was executed by executing “python Task3\_ResponseCheck.py” from Linux terminal.
* Compared how long it took to receive all 5 replies to each port: port 33333 received all 5 replies the fastest, with a time of approximately 1.2 seconds.
* Sent packets containing the payload “Ethan Hunt X” where X contained all integers from 0 to 9999 by executing the below command:

Task3.py file:

* Sorted resulting Wireshark capture by packet size, and packet type of UDP to find packet containing the successful deactivation, packet contents shown in Solution above.



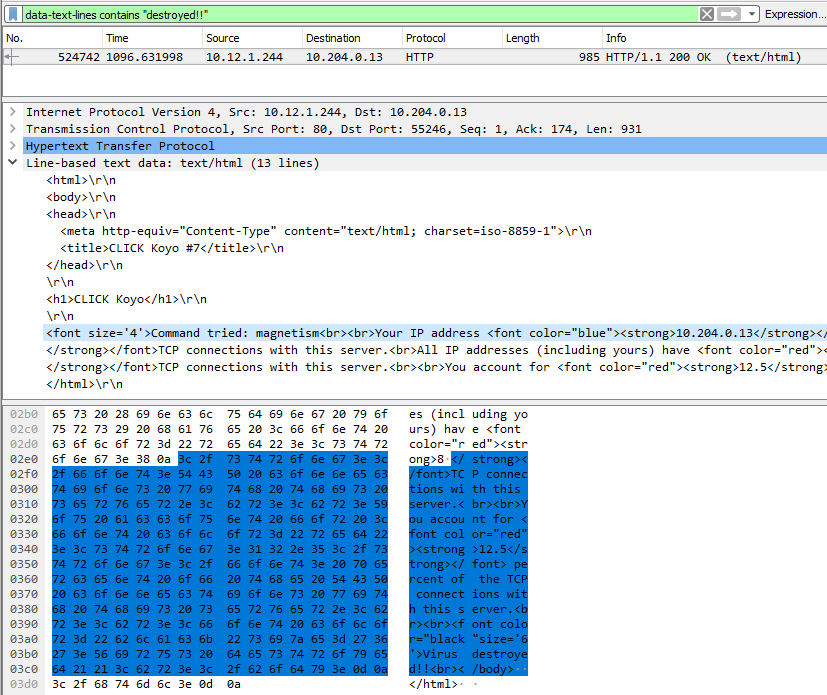
1. ***Live Free Or Die Hard***

Your assignment is to render a SCADA virus inert in order to avert the dumping of toxic levels of chlorine into the water supply. Similar to most SCADA devices, this device uses a web interface, and the virus has inserted a server-side script listening on the web interface. You must send the correct trigger word to **scada.m4i.local** in order to destroy the virus.

* + - The response from the virus will contain the string “**destroyed!!**” if it receives the correct trigger word.
    - Be mindful of the number of TCP connections you are creating. Recall that TCP connections on a server are limited and can take on the order of 30 seconds to finish the TIME WAIT state.
    - What is the trigger word? Provide a screenshot showing the successful trigger word.

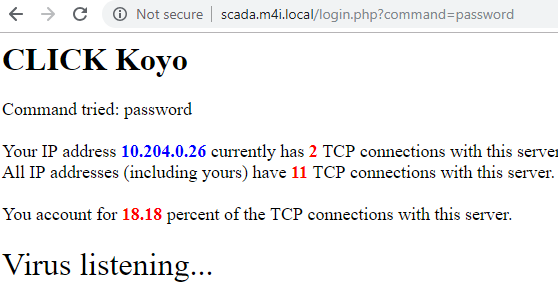
**Solution:**

* The correct trigger word is “magnetism”

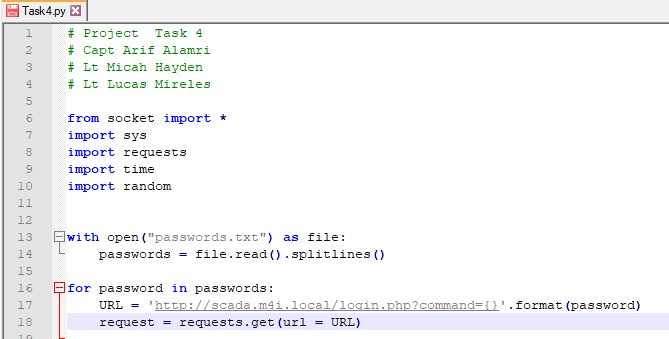


**Steps:**

* Determined the target utilized a web server based on Task 4 prompt.
* Went to <http://scada.m4i.local> and submitted a password to get the format of the URL with associated password - password:



* Created Python script to brute force send passwords to the webserver until the correct password was attempted using the given passwords text file:



* Executed Task4.py (above) to send all password combinations:



* Went through Wireshark capture to find successful deactivation, shown in **Solution** above.

**General Observations**

How long did it take you to complete this project? If possible, please indicate the time required for each of the four tasks.

* Task 1 – 1 hour
* Task 2 – 1 hour
* Task 3 – 3 hours
* Task 4 – 2 hours

Was it an appropriate length project?

* It was an appropriate length project because it was split into two turn-ins.

What corrections and or improvements do you suggest for this project? Please be very specific, and if you add new material, provide the exact wording and instructions you would give to future students in the new lab handout. You may cross out and edit text on previous pages to make minor corrections/suggestions.

* Reference Task 1 & 2 submission for updates to those tasks
* Add passwords.txt file to Task 4 prompt
* It was slightly redundant having 2 tasks that could be solved using brute force approaches in a short amount of time (Tasks 3 and 4)