Progress report (Iteration III)

Daria Vaskovskaya (d.vaskovskaya@innopolis.ru)

March 2020

Intro

- **Student Name**: Daria Vaskovskaya
- **Topic**: Man In The Middle Attacks: Execution and Detection
- **Supervisor**: Rasheed Hussain
- **Iteration number**: 3

Initial plan

Done during third iteration

- `task` Test and experiment with detection tool based on "The Security Impact of HTTPS Interception" paper - mitmengine [1]
- `hours spent` 12 hours
- `status` Done
- `results` will be available below

Current issues

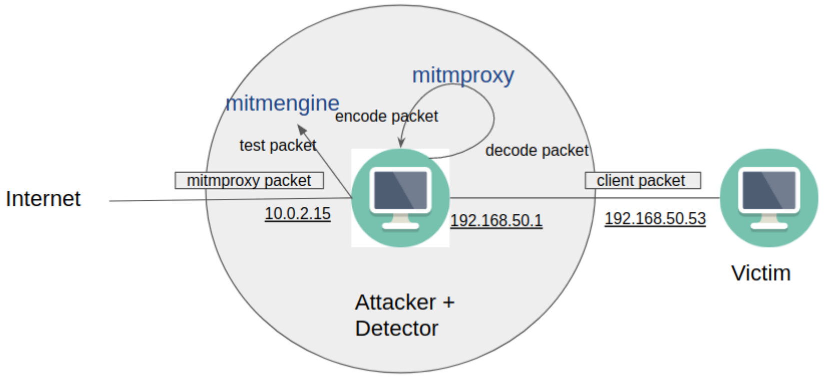
- I made some tests and mitmproxy appears to be undetectable by mitmengine. This can happen because of mitmproxy is very smart already or my tests fell in the subset of situations where mitmengine is not that good or I wrongly understand how mitmengine works. Nevertheless, I need more time to determine what happens exactly.

Results

Change of setup

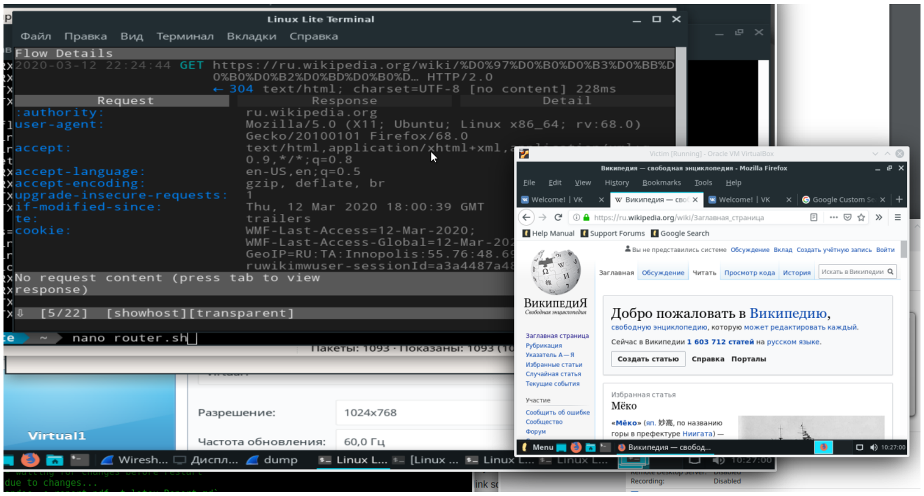
I decided to stay with VirtualBox for now, because it is easier for me and I wanted to test whether mitmengine can detect mitmproxy or not as fast as possible. Moreover, the “The Security Impact of HTTPS Interception” is based on major browsers’ TLS handshakes, that means that I need proper emulation of a browser on a machine. Of course, there are tools like Puppeteer which can do some kind of a simulation, however maybe they do not simulate browsers at 100% and this can ruin the full experiment.

I created two virtual machines: one for the victim functions and another one for the attacker+detector functions. I set up attacker machine as a router as I did during the first iteration (using the same script), then I connected virtual machines. The idea of a set up is the following:



Mitmproxy detection

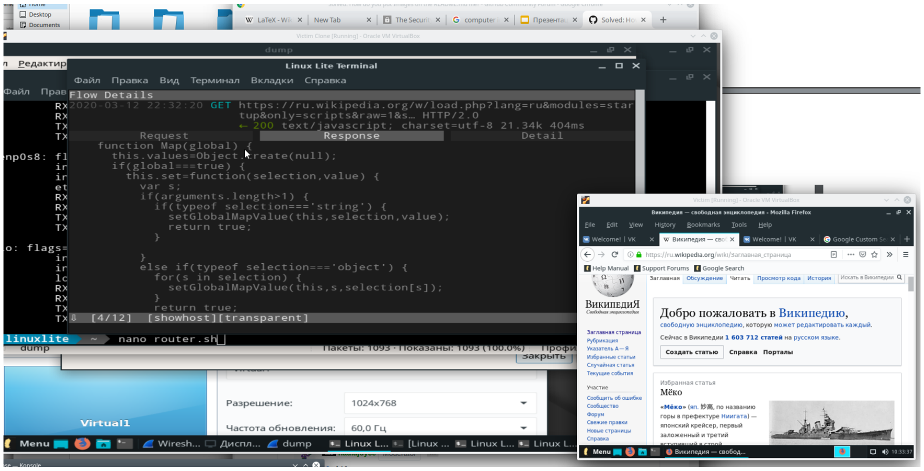
I successfully installed and ran mitmproxy via “./mitmproxy –mode transparent –showhost”. After addition of mitmproxy keys to the victim machine it became possible to see https traffic. Then packets became encrypted with mitmproxy and sent to the internet. Proof of concept:



Linux Lite Terminal
Файл Правка Вид Терминал Вкладки Справка
Википедия — свободная энциклопедия - Mozilla Firefox
Добро пожаловать в Википедию,
Разрешение: 1024x768
Частота обновления: 60,0 Гц
Virtual1

```
Flow Details
2020-03-12 22:24:44 GET https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D0%BB%D
                        0%B0%D0%B2%D0%BD%D0%B0%D… HTTP/2.0
                     ← 304 text/html; charset=UTF-8 [no content] 228ms
             Request                    Response                    Detail
:authority:                    ru.wikipedia.org
user-agent:                    Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:68.0)
                               Gecko/20100101 Firefox/68.0
accept:                        text/html,application/xhtml+xml,a
                               0.9,*/*;q=0.8
accept-language:               en-US,en;q=0.5
accept-encoding:               gzip, deflate, br
upgrade-insecure-requests:     1
if-modified-since:             Thu, 12 Mar 2020 18:00:39 GMT
te:                            trailers
cookie:                        WMF-Last-Access=12-Mar-2020;
                               WMF-Last-Access-Global=12-Mar-202
                               GeoIP=RU:TA:Innopolis:55.76:48.69
                               ruwikimwuser-sessionId=a3a4487a48
No request content (press tab to view
response)

⇩  [5/22]  [showhost][transparent]
~  nano router.sh
```

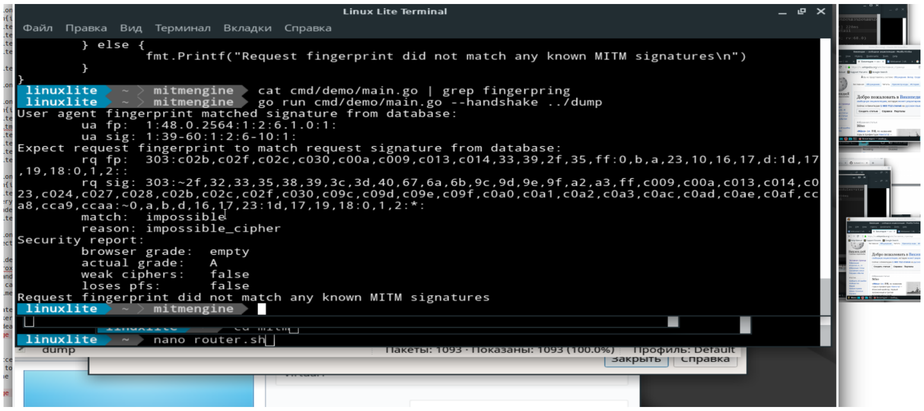


Linux Lite Terminal
Файл Правка Вид Терминал Вкладки Справка
Victim Clone [Running] - Oracle VM VirtualBox
dump
Википедия — свободная энциклопедия - Mozilla Firefox
Добро пожаловать в Википедию,
Разрешение: 1024x768
Частота обновления: 60,0 Гц
Virtual1

```
Flow Details
2020-03-12 22:32:20 GET https://ru.wikipedia.org/w/load.php?lang=ru&modules=star
                        tup&only=scripts&raw=1&s… HTTP/2.0
                     ← 200 text/javascript; charset=utf-8 21.34k 404ms
             Request                    Response                    Detail
    function Map(global) {
      this.values=Object.create(null);
      if(global===true) {
        this.set=function(selection,value) {
          var s;
          if(arguments.length>1) {
            if(typeof selection==='string') {
              setGlobalMapValue(this,selection,value);
              return true;
            }

          }
          else if(typeof selection==='object') {
            for(s in selection) {
              setGlobalMapValue(this,s,selection[s]);
            }
            return true;
⇩  [4/12]  [showhost][transparent]
linuxlite  ~  nano router.sh
```

Then I downloaded mitmengine repository. There is demo code in it which can determine if there is mitm having file with traffic as an input. So, I recorded dump file with requests from the victim via tcpdump, installed all mitmengine dependencies and ran this code with my dump as an input. Mitmengine did not detect any proxy:



```
        } else {
                fmt.Printf("Request fingerprint did not match any known MITM signatures\n")
        }
}
linuxlite  ~  mitmengine  cat cmd/demo/main.go | grep fingerpring
linuxlite  ~  mitmengine  go run cmd/demo/main.go --handshake ../dump
User agent fingerprint matched signature from database:
        ua fp:  1:48.0.2564:1:2:6.1.0:1:
        ua sig: 1:39-60:1:2:6-10:1:
Expect request fingerprint to match request signature from database:
        rq fp:  303:c02b,c02f,c02c,c030,c00a,c009,c013,c014,33,39,2f,35,ff:0,b,a,23,10,16,17,d:1d,17
,19,18:0,1,2::
        rq sig: 303:~2f,32,33,35,38,39,3c,3d,40,67,6a,6b,9c,9d,9e,9f,a2,a3,ff,c009,c00a,c013,c014,c0
23,c024,c027,c028,c02b,c02c,c02f,c030,c09c,c09d,c09e,c09f,c0a0,c0a1,c0a2,c0a3,c0ac,c0ad,c0ae,c0af,cc
a8,cca9,ccaa:~0,a,b,d,16,17,23:1d,17,19,18:0,1,2:*:
        match:  impossible
        reason: impossible_cipher
Security report:
        browser grade:  empty
        actual grade:   A
        weak ciphers:   false
        loses pfs:      false
Request fingerprint did not match any known MITM signatures
linuxlite  ~  mitmengine  
linuxlite  ~  nano router.sh
```

Future plans

Dig into the code of mitmproxy and mitmengine in order to determine why mitmproxy is not detected.

Hours: 12

[1] Mitmproxy: https://mitmproxy.org/

[2] Mitmengine: https://github.com/cloudflare/mitmengine