Android Malware Analysis Lab

Dilver Huertas Guerrero, Department of Systems and Industrial Engineering, Universidad Nacional de Colombia, Bogotá, Colombia e-mail: djhuertasg@unal.edu.co

UNSECURELAB

Objective

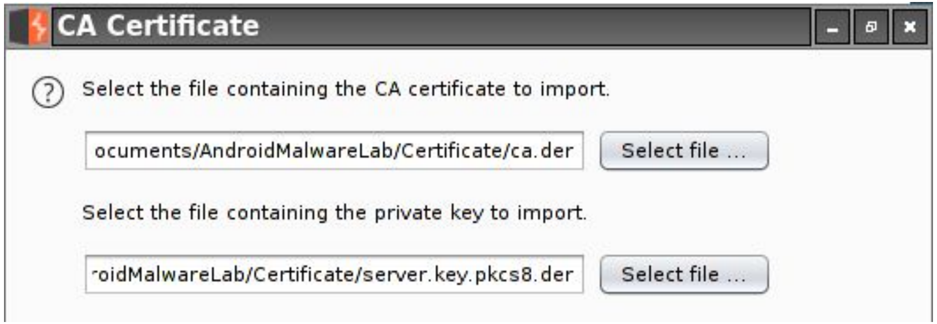
Objective

Show how to configure a malware analysis lab for Android using a virtual machine, that could be deployed over QEMU or VirtualBox. The tool Burp Suite to establish a proxy as a certified authority and Frida to do pentesting.

Setting up the lab

Virtualizing Android

Proxy Network

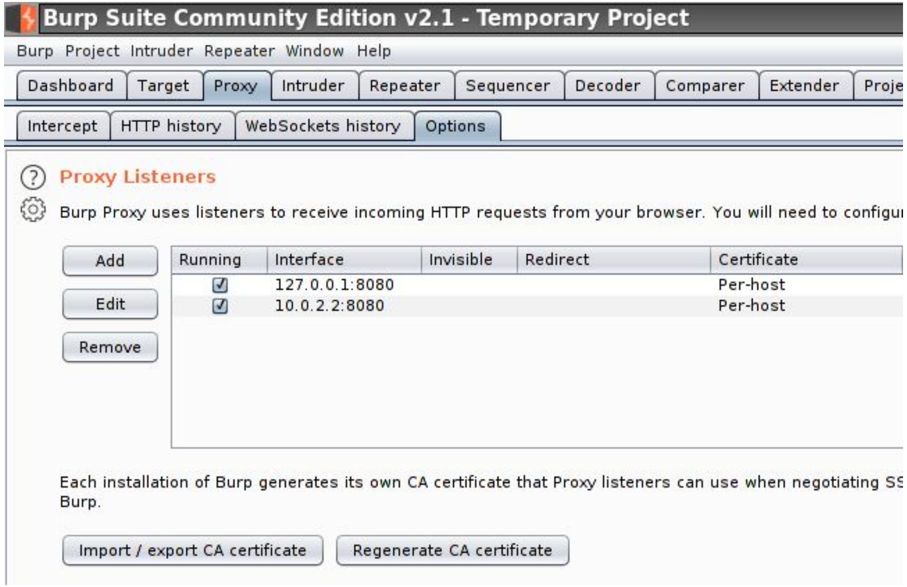


Select the file containing the CA certificate to import.

ocuments/AndroidMalwareLab/Certificate/ca.der

Select the file containing the private key to import.

roidMalwareLab/Certificate/server.key.pkcs8.der



Burp Suite Community Edition v2.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Proje
Intercept HTTP history WebSockets history Options

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configu

Running	Interface	Invisible	Redirect	Certificate
☑	127.0.0.1:8080			Per-host
☑	10.0.2.2:8080			Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SS
Burp.

Import / export CA certificate
Regenerate CA certificate

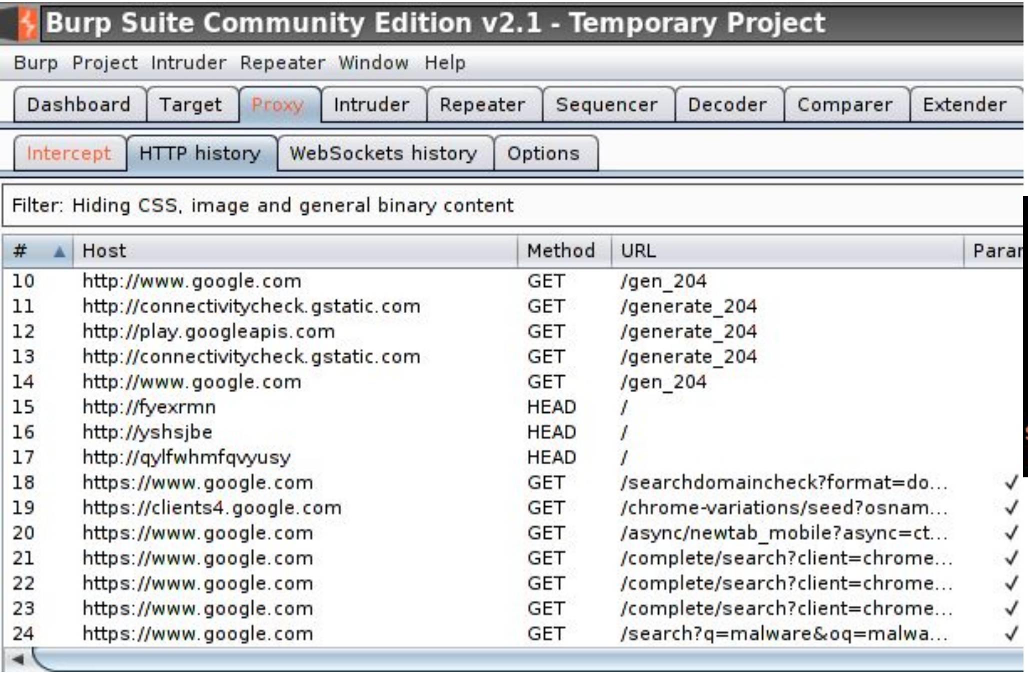
UNSECURELAB

Pentesting

FЯIDA

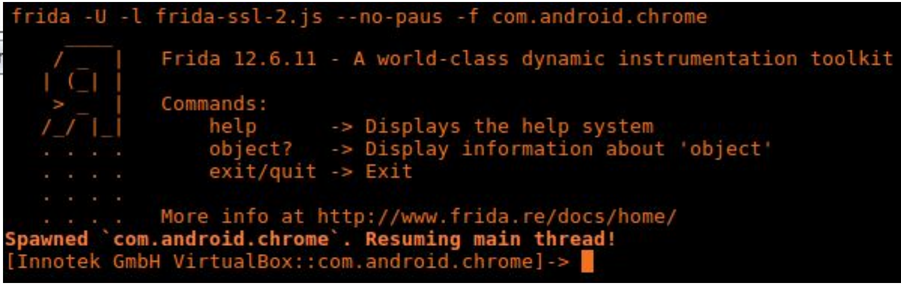
Testing the lab

Testing com.android.chrome


Burp Suite Community Edition v2.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender
Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

# ▲	Host	Method	URL	Parar
10	http://www.google.com	GET	/gen_204	
11	http://connectivitycheck.gstatic.com	GET	/generate_204	
12	http://play.googleapis.com	GET	/generate_204	
13	http://connectivitycheck.gstatic.com	GET	/generate_204	
14	http://www.google.com	GET	/gen_204	
15	http://fyexrmn	HEAD	/	
16	http://yshsjbe	HEAD	/	
17	http://qylfwhmfqvyusy	HEAD	/	
18	https://www.google.com	GET	/searchdomaincheck?format=do...	✓
19	https://clients4.google.com	GET	/chrome-variations/seed?osnam...	✓
20	https://www.google.com	GET	/async/newtab_mobile?async=ct...	✓
21	https://www.google.com	GET	/complete/search?client=chrome...	✓
22	https://www.google.com	GET	/complete/search?client=chrome...	✓
23	https://www.google.com	GET	/complete/search?client=chrome...	✓
24	https://www.google.com	GET	/search?q=malware&oq=malwa...	✓



```
frida -U -l frida-ssl-2.js --no-paus -f com.android.chrome
     ____
    / _  |   Frida 12.6.11 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at http://www.frida.re/docs/home/
Spawned `com.android.chrome`. Resuming main thread!
[Innotek GmbH VirtualBox::com.android.chrome]-> █
```

Conclusions and further work

- QEMU vs VirtualBox
- Burp Suite only as proxy network (Squid)
- Test with actual malware

Thank you!

Questions?