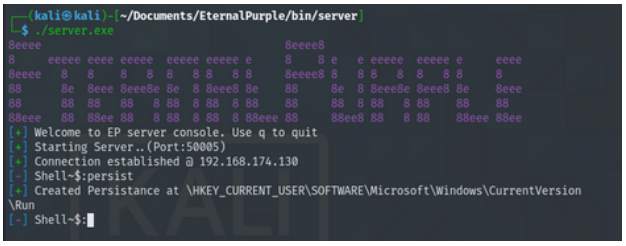
POL GALVEZ

INFORMATICS ENGENEERING AT UNIVERSITAT POLITECNICA DE CATALUNYA

+34 635824169
polgalvezsoriano@gmail.com
github.com/polgs

EPURPLE BACKDOOR github.com/PolGs/Persistent-Backdoor



What?

- Developed a W10 remote access tool (**RAT**) for red teaming with **persistence** on reboot and self **replication** functionalities.

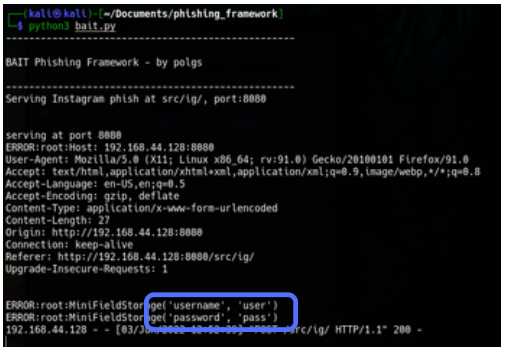
How?

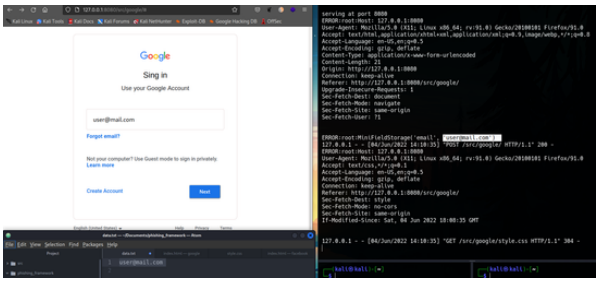
- Used **C**, **sockets** and **windows.h** module to code server and client executables. I also used nircmd to add **spyware** functionalities and UPX for **obfuscating** payload.

Result

- The executable gives total remote control of the victim's machine and at the time was not detected by many AV (Microsoft and Avast).

BAITER - PHISHING TOOLKIT github.com/PolGs/BAIT_Phishing_Framework





What?

- Developed a phishing script for credential harvesting on popular sites like Instagram or Google

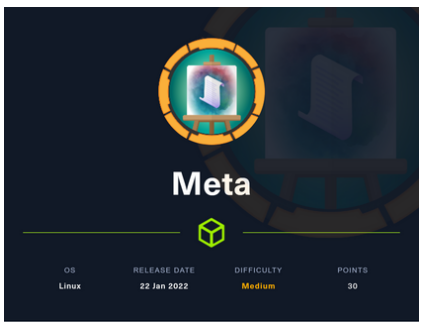
How?

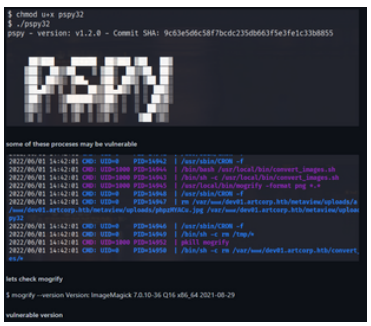
- Used python to host a web server and process POST requests sent with the corresponding credentials

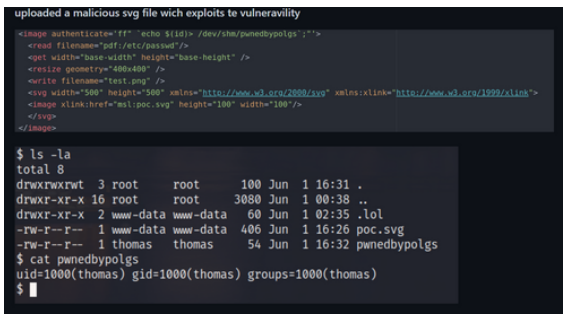
Result

- The script hosts fake login forms and stores credentials. Very powerful tool combined with DNS poisoning

HTB META github.com/PolGs/htb-meta







What?

- Solved Meta machine from HackTheBox.

How?

- Used python script to generate malicious jpg file and gain user access.
- Exploited ImageMagick and NeoFetch vulnerability to escalate privileges

Result

- Successfully exploited CVE-2021-22204 and 2016-3714.