专注APT攻击与防御

https://micropoor.blogspot.com/

前言：

在团体渗透测试的项目中，如红蓝对抗，团队渗透测试比赛等，最重要的是过程与结果实时共享于团队，例如：A同学nmap目标站，B同学也nmap目标站，这在对抗比赛中是极其浪费时间也是非常容易引起防火墙，日志服务器或其他设备的警觉。所以打算写一系列关于未来团队渗透的对抗。争取做到过程与结果，团队实时共享。把曾经的团队作战经验形成一个适应对抗，比赛等的参考。

popy简介：

Pupy是一个开源，跨平台（Windows，Linux，OSX，Android），多功能RAT（远程管理工具）和主要用python编写的后期开发工具。它具有全内存读取操作，进程注入等。Pupy可以使用各种传输进行通信，迁移到进程（注入），从内存加载远程Python代码。

项目地址：https://github.com/n1nj4sec/pupy

root@John:~/Desktop# git clone https://github.com/n1nj4sec/pupy.git

root@John:~/Desktop/pupy/pupy# pip install rpyc

root@John:~/Desktop/pupy/pupy# git submodule update

root@John:~/Desktop/pupy/pupy# cd .. root@John:~/Desktop/pupy# pip install -r pupy/requirements.txt

root@John:~/Desktop/pupy/# wget https://github.com/n1nj4sec/pupy/releases/download/latest/payload\_templates.txz

root@John:~/Desktop/pupy# tar xvf payload\_templates.txz && mv payload\_templates/\* pupy/payload\_templates/ && rm payload\_templates.txz &&

rm -r payload\_templates

root@John:~/Desktop/pupy/pupy# apt-get install python-xlib

附录：

Collecting pyautogui

Using cached PyAutoGUI-0.9.36.tar.gz

Complete output from command python setup.py egg\_info: Traceback (most recent call last):

File "<string>", line 1, in <module>

File "/tmp/pip-build-a90ODY/pyautogui/setup.py", line 6, in <module>

version=\_\_import\_\_('pyautogui').\_\_version\_\_,

File "pyautogui/\_\_init\_\_.py", line 115, in <module>

from . import \_pyautogui\_x11 as platformModule

File "pyautogui/\_pyautogui\_x11.py", line 160, in <module>

\_display = Display(os.environ['DISPLAY'])

File "/usr/lib/python2.7/UserDict.py", line 40, in \_\_getitem\_\_

raise KeyError(key) KeyError: 'DISPLAY'

must install on local server with GUI

Micropoor