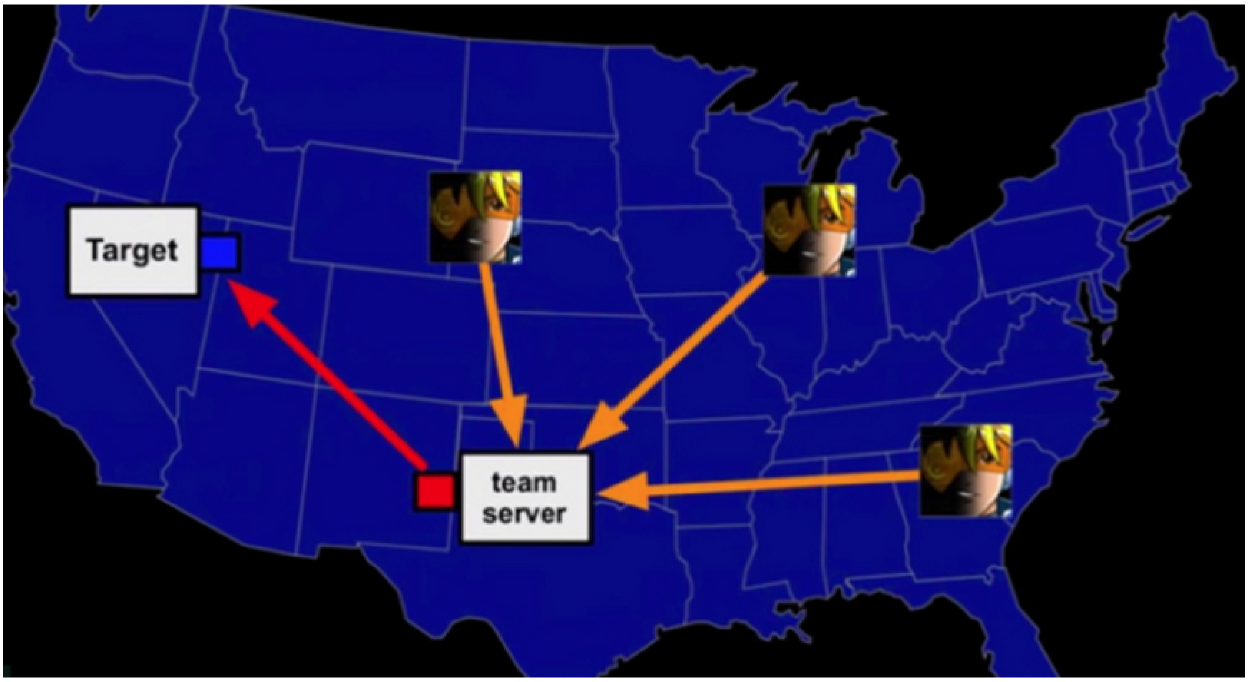
专注APT攻击与防御
https://micropoor.blogspot.com/

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。

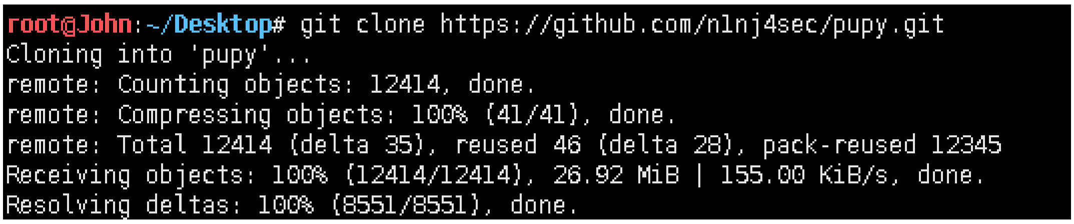


popy简介：

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。

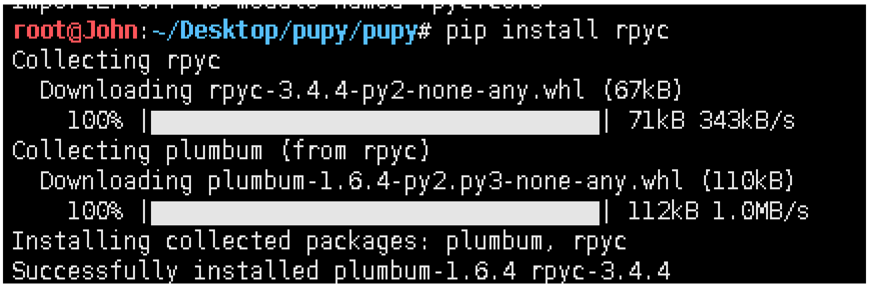
项目地址：https://github.com/n1nj4sec/pupy

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



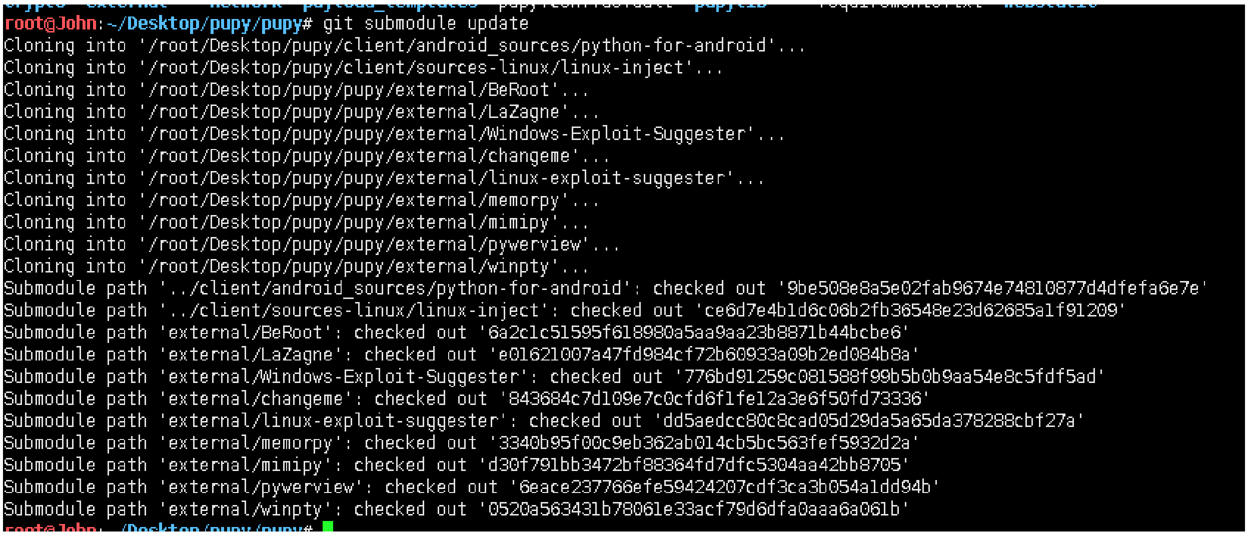
```
root@John:~/Desktop# git clone https://github.com/n1nj4sec/pupy.git
Cloning into 'pupy'...
remote: Counting objects: 12414, done.
remote: Compressing objects: 100% (41/41), done.
remote: Total 12414 (delta 35), reused 46 (delta 28), pack-reused 12345
Receiving objects: 100% (12414/12414), 26.92 MiB | 155.00 KiB/s, done.
Resolving deltas: 100% (8551/8551), done.
```

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



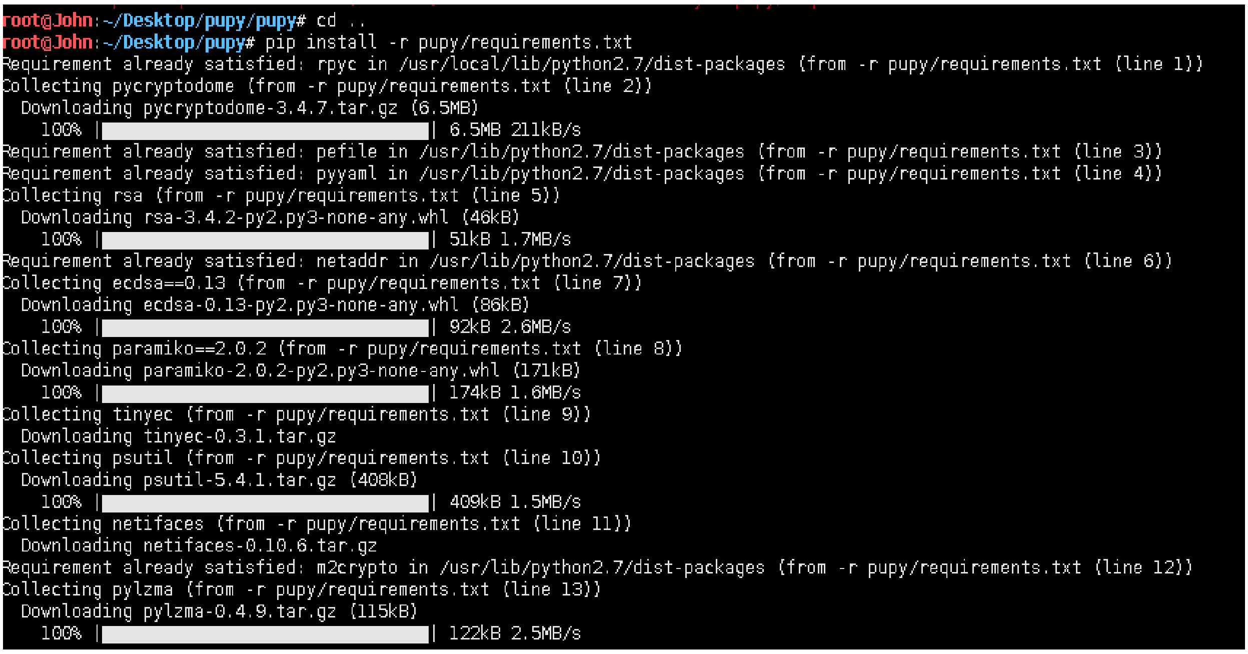
```
root@John:~/Desktop/pupy/pupy# pip install rpyc
Collecting rpyc
  Downloading rpyc-3.4.4-py2-none-any.whl (67kB)
    100% |████████████████████████████████| 71kB 343kB/s
Collecting plumbum (from rpyc)
  Downloading plumbum-1.6.4-py2.py3-none-any.whl (110kB)
    100% |████████████████████████████████| 112kB 1.0MB/s
Installing collected packages: plumbum, rpyc
Successfully installed plumbum-1.6.4 rpyc-3.4.4
```

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



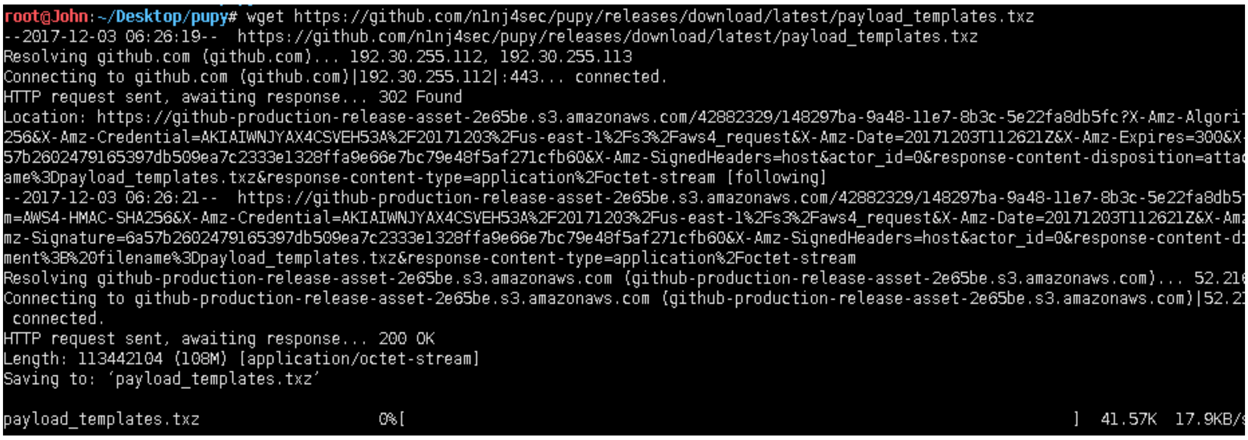
```
root@John:~/Desktop/pupy/pupy# git submodule update
Cloning into '/root/Desktop/pupy/client/android_sources/python-for-android'...
Cloning into '/root/Desktop/pupy/client/sources-linux/linux-inject'...
Cloning into '/root/Desktop/pupy/pupy/external/BeRoot'...
Cloning into '/root/Desktop/pupy/pupy/external/LaZagne'...
Cloning into '/root/Desktop/pupy/pupy/external/Windows-Exploit-Suggester'...
Cloning into '/root/Desktop/pupy/pupy/external/changeme'...
Cloning into '/root/Desktop/pupy/pupy/external/linux-exploit-suggester'...
Cloning into '/root/Desktop/pupy/pupy/external/memorpy'...
Cloning into '/root/Desktop/pupy/pupy/external/mimipy'...
Cloning into '/root/Desktop/pupy/pupy/external/pywerview'...
Cloning into '/root/Desktop/pupy/pupy/external/winpty'...
Submodule path '../client/android_sources/python-for-android': checked out '9be508e8a5e02fab9674e74810877d4dfefa6e7e'
Submodule path '../client/sources-linux/linux-inject': checked out 'ce6d7e4b1d6c06b2fb36548e23d62685a1f91209'
Submodule path 'external/BeRoot': checked out '6a2c1c51595f618980a5aa9aa23b8871b44bcbe6'
Submodule path 'external/LaZagne': checked out 'e01621007a47fd984cf72b60933a09b2ed084b8a'
Submodule path 'external/Windows-Exploit-Suggester': checked out '776bd91259c081588f99b5b0b9aa54e8c5fdf5ad'
Submodule path 'external/changeme': checked out '843684c7d109e7c0cfd6f1fe12a3e6f50fd73336'
Submodule path 'external/linux-exploit-suggester': checked out 'dd5aedcc80c8cad05d29da5a65da378288cbf27a'
Submodule path 'external/memorpy': checked out '3340b95f00c9eb362ab014cb5bc563fef5932d2a'
Submodule path 'external/mimipy': checked out 'd30f791bb3472bf88364fd7dfc5304aa42bb8705'
Submodule path 'external/pywerview': checked out '6eace237766efe59424207cdf3ca3b054a1dd94b'
Submodule path 'external/winpty': checked out '0520a563431b78061e33acf79d6dfa0aaa6a061b'
```

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



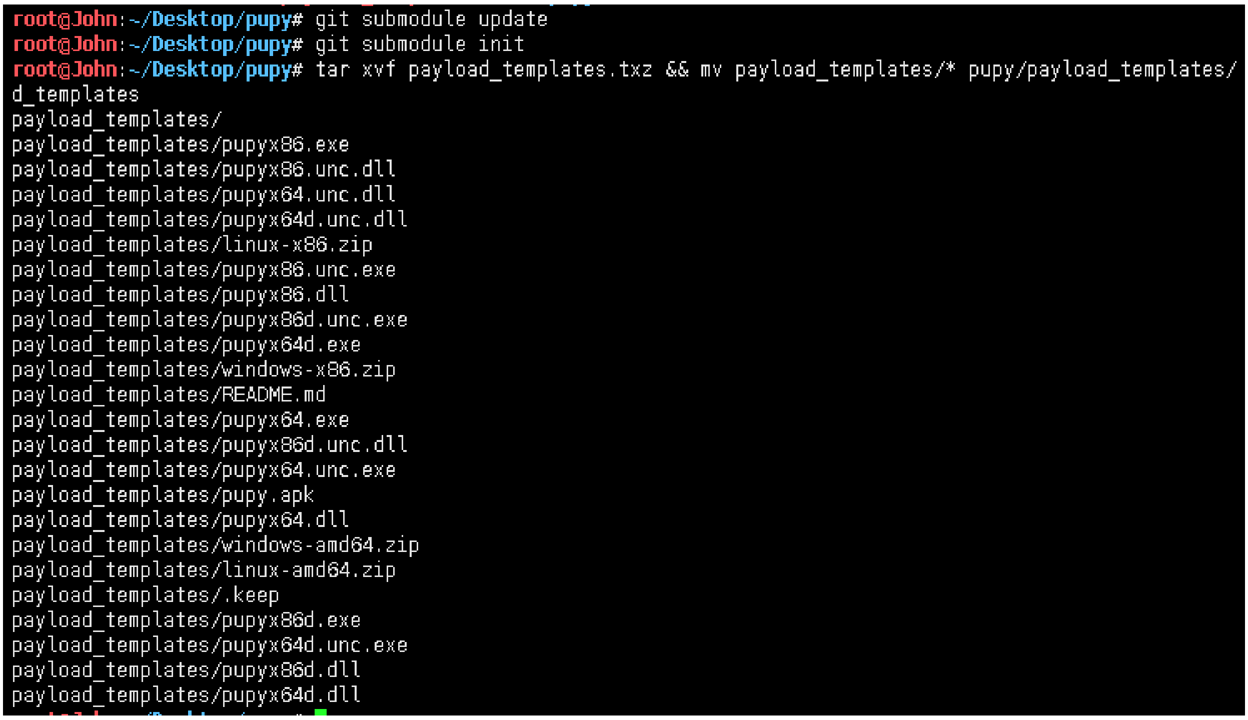
```
root@John:~/Desktop/pupy/pupy# cd ..
root@John:~/Desktop/pupy# pip install -r pupy/requirements.txt
Requirement already satisfied: rpyc in /usr/local/lib/python2.7/dist-packages (from -r pupy/requirements.txt (line 1))
Collecting pycryptodome (from -r pupy/requirements.txt (line 2))
  Downloading pycryptodome-3.4.7.tar.gz (6.5MB)
    100% |████████████████████████████████| 6.5MB 211kB/s
Requirement already satisfied: pefile in /usr/lib/python2.7/dist-packages (from -r pupy/requirements.txt (line 3))
Requirement already satisfied: pyyaml in /usr/lib/python2.7/dist-packages (from -r pupy/requirements.txt (line 4))
Collecting rsa (from -r pupy/requirements.txt (line 5))
  Downloading rsa-3.4.2-py2.py3-none-any.whl (46kB)
    100% |████████████████████████████████| 51kB 1.7MB/s
Requirement already satisfied: netaddr in /usr/lib/python2.7/dist-packages (from -r pupy/requirements.txt (line 6))
Collecting ecdsa==0.13 (from -r pupy/requirements.txt (line 7))
  Downloading ecdsa-0.13-py2.py3-none-any.whl (86kB)
    100% |████████████████████████████████| 92kB 2.6MB/s
Collecting paramiko==2.0.2 (from -r pupy/requirements.txt (line 8))
  Downloading paramiko-2.0.2-py2.py3-none-any.whl (171kB)
    100% |████████████████████████████████| 174kB 1.6MB/s
Collecting tinyec (from -r pupy/requirements.txt (line 9))
  Downloading tinyec-0.3.1.tar.gz
Collecting psutil (from -r pupy/requirements.txt (line 10))
  Downloading psutil-5.4.1.tar.gz (408kB)
    100% |████████████████████████████████| 409kB 1.5MB/s
Collecting netifaces (from -r pupy/requirements.txt (line 11))
  Downloading netifaces-0.10.6.tar.gz
Requirement already satisfied: m2crypto in /usr/lib/python2.7/dist-packages (from -r pupy/requirements.txt (line 12))
Collecting pylzma (from -r pupy/requirements.txt (line 13))
  Downloading pylzma-0.4.9.tar.gz (115kB)
    100% |████████████████████████████████| 122kB 2.5MB/s
```

```
root@John:~/Desktop/pupy/# wget https://github.com/n1nj4sec/pupy/releases/download/latest/payload_templates.txz
```



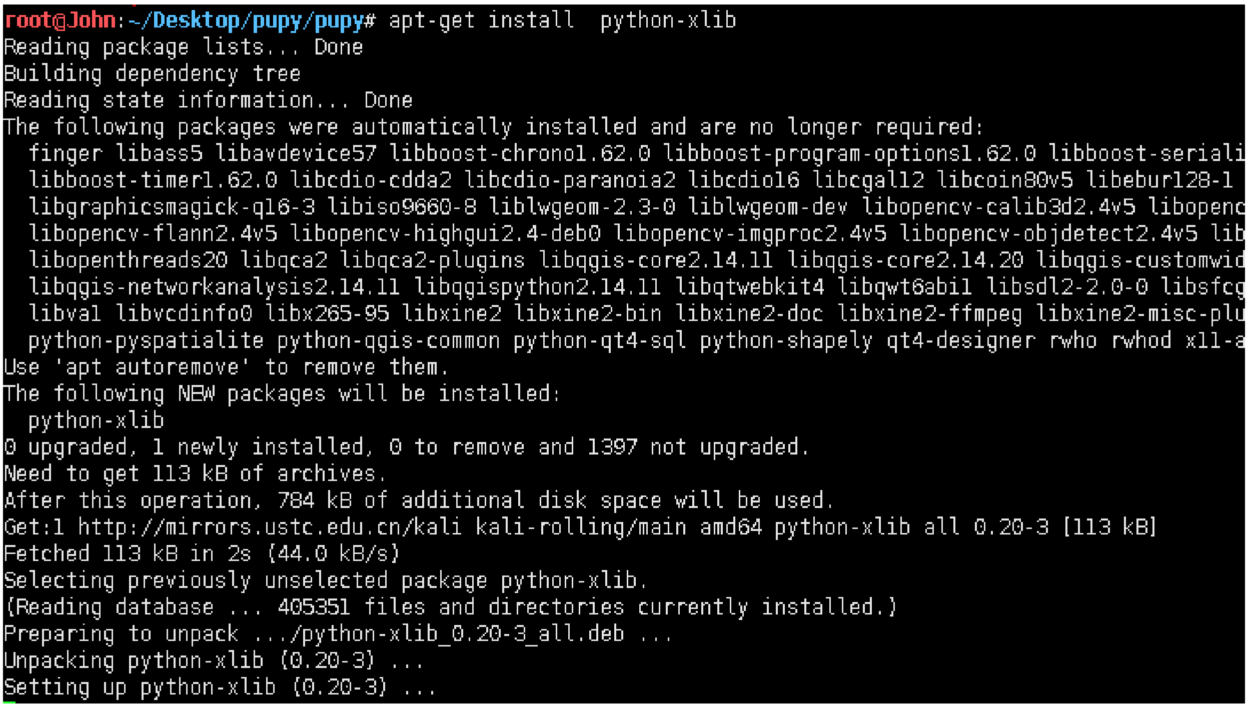
```
root@John:~/Desktop/pupy# wget https://github.com/n1nj4sec/pupy/releases/download/latest/payload_templates.txz
--2017-12-03 06:26:19--  https://github.com/n1nj4sec/pupy/releases/download/latest/payload_templates.txz
Resolving github.com (github.com)... 192.30.255.112, 192.30.255.113
Connecting to github.com (github.com)|192.30.255.112|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://github-production-release-asset-2e65be.s3.amazonaws.com/42882329/148297ba-9a48-11e7-8b3c-5e22fa8db5fc?X-Amz-Algori
256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20171203%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20171203T112621Z&X-Amz-Expires=300&X-
57b2602479165397db509ea7c2333e1328ffa9e66e7bc79e48f5af271cfb60&X-Amz-SignedHeaders=host&actor_id=0&response-content-disposition=attac
ame%3Dpayload_templates.txz&response-content-type=application%2Foctet-stream [following]
--2017-12-03 06:26:21--  https://github-production-release-asset-2e65be.s3.amazonaws.com/42882329/148297ba-9a48-11e7-8b3c-5e22fa8db5
m=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20171203%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20171203T112621Z&X-Am
mz-Signature=6a57b2602479165397db509ea7c2333e1328ffa9e66e7bc79e48f5af271cfb60&X-Amz-SignedHeaders=host&actor_id=0&response-content-di
ment%3B%20filename%3Dpayload_templates.txz&response-content-type=application%2Foctet-stream
Resolving github-production-release-asset-2e65be.s3.amazonaws.com (github-production-release-asset-2e65be.s3.amazonaws.com)... 52.21
Connecting to github-production-release-asset-2e65be.s3.amazonaws.com (github-production-release-asset-2e65be.s3.amazonaws.com)|52.2
 connected.
HTTP request sent, awaiting response... 200 OK
Length: 113442104 (108M) [application/octet-stream]
Saving to: ‘payload_templates.txz’

payload_templates.txz               0%[                                                                       ]  41.57K  17.9KB/
```

```
root@John:~/Desktop/pupy# tar xvf payload_templates.txz && mv payload_templates/* pupy/payload_templates/ && rm payload_templates.txz && rm -r payload_templates
```

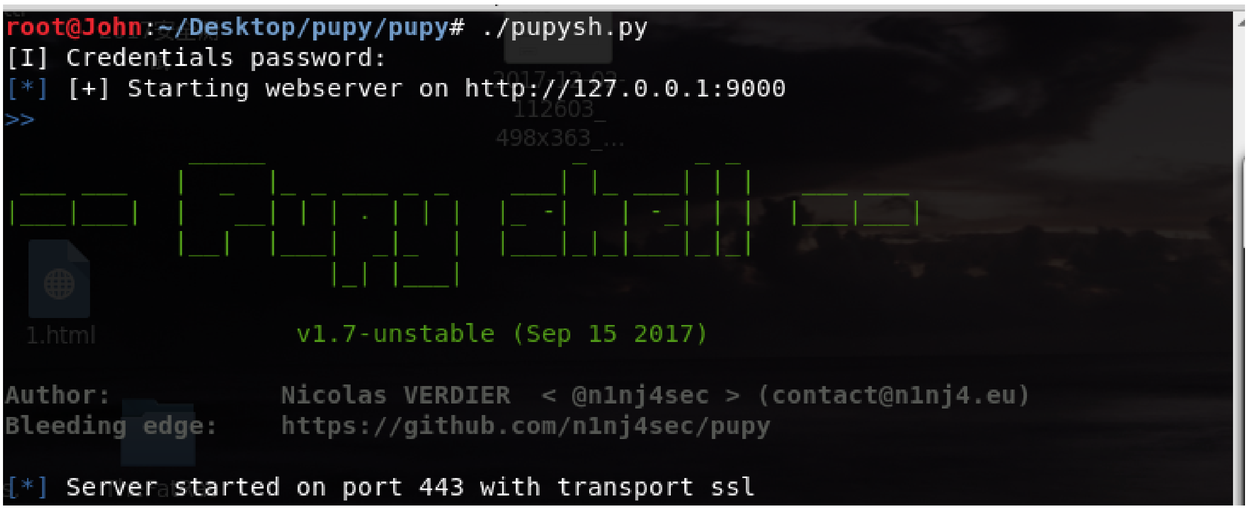


```
root@John:~/Desktop/pupy# git submodule update
root@John:~/Desktop/pupy# git submodule init
root@John:~/Desktop/pupy# tar xvf payload_templates.txz && mv payload_templates/* pupy/payload_templates/
d_templates
payload_templates/
payload_templates/pupyx86.exe
payload_templates/pupyx86.unc.dll
payload_templates/pupyx64.unc.dll
payload_templates/pupyx64d.unc.dll
payload_templates/linux-x86.zip
payload_templates/pupyx86.unc.exe
payload_templates/pupyx86.dll
payload_templates/pupyx86d.unc.exe
payload_templates/pupyx64d.exe
payload_templates/windows-x86.zip
payload_templates/README.md
payload_templates/pupyx64.exe
payload_templates/pupyx86d.unc.dll
payload_templates/pupyx64.unc.exe
payload_templates/pupy.apk
payload_templates/pupyx64.dll
payload_templates/windows-amd64.zip
payload_templates/linux-amd64.zip
payload_templates/.keep
payload_templates/pupyx86d.exe
payload_templates/pupyx64d.unc.exe
payload_templates/pupyx86d.dll
payload_templates/pupyx64d.dll
```

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



```
root@John:~/Desktop/pupy/pupy# apt-get install  python-xlib
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  finger libass5 libavdevice57 libboost-chrono1.62.0 libboost-program-options1.62.0 libboost-seriali
  libboost-timer1.62.0 libcdio-cdda2 libcdio-paranoia2 libcdio16 libcgal12 libcoin80v5 libebur128-1
  libgraphicsmagick-q16-3 libiso9660-8 liblwgeom-2.3-0 liblwgeom-dev libopencv-calib3d2.4v5 libopenc
  libopencv-flann2.4v5 libopencv-highgui2.4-deb0 libopencv-imgproc2.4v5 libopencv-objdetect2.4v5 lib
  libopenthreads20 libqca2 libqca2-plugins libqgis-core2.14.11 libqgis-core2.14.20 libqgis-customwid
  libqgis-networkanalysis2.14.11 libqgispython2.14.11 libqtwebkit4 libqwt6abi1 libsdl2-2.0-0 libsfcg
  libval libvcdinfo0 libx265-95 libxine2 libxine2-bin libxine2-doc libxine2-ffmpeg libxine2-misc-plu
  python-pyspatialite python-qgis-common python-qt4-sql python-shapely qt4-designer rwho rwhod x11-a
Use 'apt autoremove' to remove them.
The following NEW packages will be installed:
  python-xlib
0 upgraded, 1 newly installed, 0 to remove and 1397 not upgraded.
Need to get 113 kB of archives.
After this operation, 784 kB of additional disk space will be used.
Get:1 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 python-xlib all 0.20-3 [113 kB]
Fetched 113 kB in 2s (44.0 kB/s)
Selecting previously unselected package python-xlib.
(Reading database ... 405351 files and directories currently installed.)
Preparing to unpack .../python-xlib_0.20-3_all.deb ...
Unpacking python-xlib (0.20-3) ...
Setting up python-xlib (0.20-3) ...
```



```
root@John:~/Desktop/pupy/pupy# ./pupysh.py
[I] Credentials password:
[*] [+] Starting webserver on http://127.0.0.1:9000
>>
             _____                    _       _ _
 ___ ___    |  _  |_ _ ___ _ _    ___| |_ ___| | |    ___ ___
|___|___|   |   __| | | . | | |  |_ -|   | -_| | |   |___|___|
            |__|  |___|  _|_  |  |___|_|_|___|_|_|
                      |_| |___|

                   v1.7-unstable (Sep 15 2017)

Author:             Nicolas VERDIER  < @n1nj4sec > (contact@n1nj4.eu)
Bleeding edge:      https://github.com/n1nj4sec/pupy

[*] Server started on port 443 with transport ssl
```

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