

# Printer Hacking

1984001 강민석

# ➤ 목차

- 동기
- 실습 1 – PRET 툴 사용
- 실습 2 – PUTTY 사용
- 실습 3 – Python3 으로 툴 만들기
- 배운 점

# 동기

프린터기의 IP주소를 보고  
해킹 시도를 하게 되었다.



# 실습 1

PRET 툴 사용

# 실습 1

먼저 PRET 라는 Printer hacking tool  
을 사용해서 실습해봤다.

Git clone 을 사용하여 툴을  
다운받아준다.

```
root@kali:~# cd Desktop/  
root@kali:~/Desktop# git clone https://github.com/RUB-NDS/PRET.git  
Cloning into 'PRET'...  
remote: Enumerating objects: 357, done.  
remote: Total 357 (delta 0), reused 0 (delta 0), pack-reused 357  
Receiving objects: 100% (357/357), 1.74 MiB | 1.66 MiB/s, done.  
Resolving deltas: 100% (183/183), done.  
root@kali:~/Desktop# ls -al  
total 31004  
drwxr-xr-x  3 root root    4096 Jun 20 21:24 .  
drwxr-xr-x 17 root root    4096 Jun 20 20:52 ..  
-rwxr--r--  1 root root    8620 Jun 20 20:44 download.jpg  
-rwxr--r--  1 root root 31722939 Jun  4 20:42 ngrok  
drwxr-xr-x 10 root root    4096 Jun 20 21:24 PRET  
root@kali:~/Desktop#
```

# 실습 1

다음으로 pret.py 실행파일을  
실행시켜 주변 프린터기를  
확인한다.

```
root@kali:~/Desktop# ls
download.jpg  init_sat  ngrok  PRET
root@kali:~/Desktop# cd PRET/
root@kali:~/Desktop/PRET# ls
capabilities.py  discovery.py  LICENSE.md  pcl.py  README.md
codebook.py    fonts        lpd         pjl.py  testpages
console.py     fuzzer.py   mibs       postscript.py
db             helper.py   operators.py  pret.py
DISCLAIMER.md  img        overlays    printer.py
root@kali:~/Desktop/PRET# ./pret.py
No target given, discovering local printers
```

address	device	uptime	status
192.168.180.15	SINDOH A601_A606 451444LM1...	1 day	0xeca480ebb9842eec84a0...
192.168.180.127	SINDOH A603_A608 451444HH1...	5 days	0xeca480ebb9842eec84a0...

```
usage: pret.py [-h] [-s] [-q] [-d] [-i file] [-o file] target {ps,pjl,pcl}
pret.py: error: too few arguments

root@kali:~/Desktop/PRET#
```

# 실습 1

./pret.py (대상ip) (printer jop language) 로  
Printer shell 에 접속한다.

```
root@kali:~/Desktop/PRET# ./pret.py 192.168.180.15 pjl

  _ _ _ _ _
 / _ _ _ _ \
|   _   _   |
|  _/_ _ _  |
| _/_ _ _ _ |
|  _/_ _ _  |
|   _   _   |
 \ _ _ _ _ /
  _ _ _ _ _

PRET | Printer Exploitation Toolkit v0.40
    | by Jens Mueller <jens.a.mueller@rub.de>

    | ' pentesting tool that made
    | dumpster diving obsolete.. '

(ASCII art by
Jan Foerster)

Connection to 192.168.180.15 established
Device: SINDOH A601 A606

Welcome to the pret shell. Type help or ? to list commands.
192.168.180.15:/> |
```

# 실습 1

Print 명령어 사용후  
"hello" 텍스트를 입력한다.

(경로지정시 경로에 있는  
파일도 프린트 가능)

```
root@kali:~/Desktop/PRET# ./pret.py 192.168.180.15 pjl

  /-----/
 /-----/ /
|===|----| |
|    |    | |
|    |    | |
|  /.'---.| |
|-||/____\|-|
|_||=L==H==|_|_|/

PRET | Printer Exploitation Toolkit v0.40
    | by Jens Mueller <jens.a.mueller@rub.de>

    | ' pentesting tool that made
    | dumpster diving obsolete.. '

(ASCII art by
Jan Foerster)

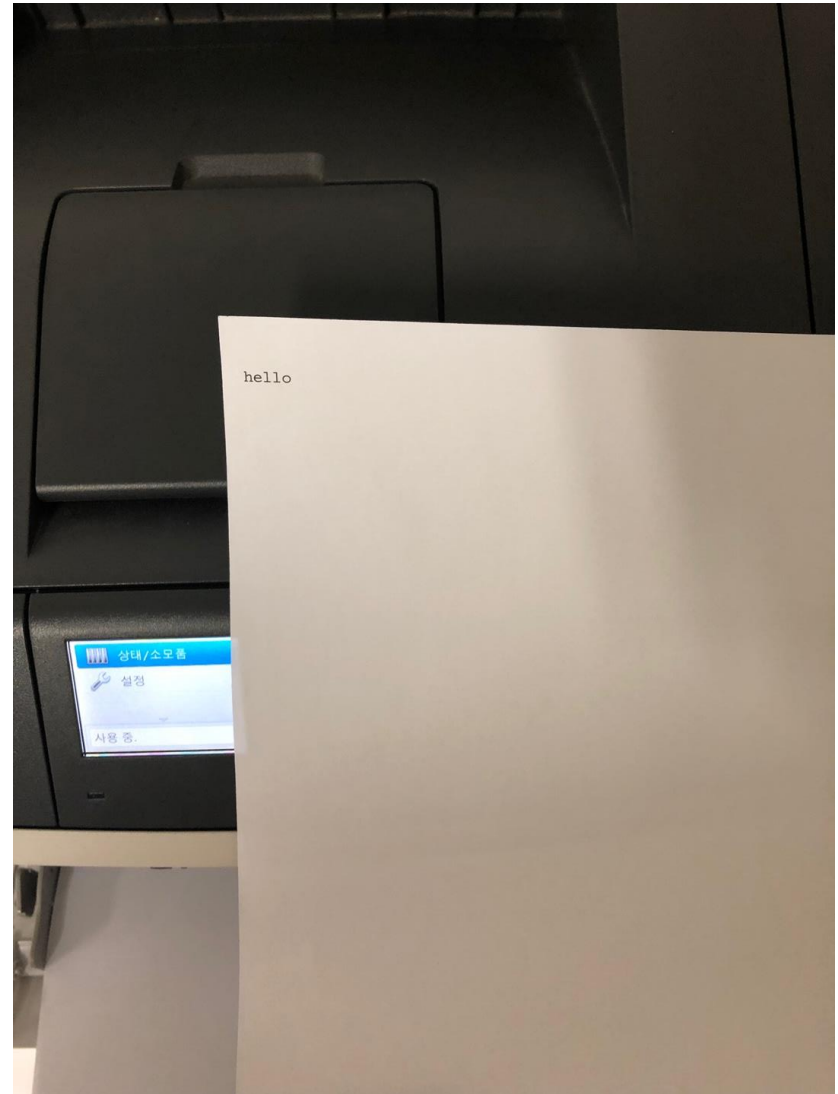
Connection to 192.168.180.15 established
Device: SINDOH A601 A606

Welcome to the pret shell. Type help or ? to list commands.
192.168.180.15:/> print
File or "text": "hello"
192.168.180.15:/> █
```



# 실습 1

오른쪽과 같이 "hello"가 프린트 된  
것을 볼 수 있다.



# 실습 2

Putty 사용

# 실습 2

두번째 실습이다.

포트스캔 툴 Nmap 을 사용하여  
열린 포트들을 알 수 있었다.

(-sS 옵션을 줘서 syn scan을 사용  
하였다.)



```
root@kali:~# nmap -sS 192.168.180.15
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-22 18:07 KST
Nmap scan report for 192.168.180.15
Host is up (0.0018s latency).
Not shown: 985 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
79/tcp    open  finger
80/tcp    open  http
443/tcp   open  https
515/tcp   open  printer
631/tcp   open  ipp
4000/tcp  open  remoteanything
5000/tcp  open  upnp
5001/tcp  open  complex-link
6100/tcp  open  synchronet-db
8000/tcp  open  http-alt
9100/tcp  open  jetdirect
9200/tcp  open  wap-wsp
9500/tcp  open  ismserver
10000/tcp filtered snet-sensor-mgmt
MAC Address: 00:21:B7:41:1E:96 (Lexmark International)

Nmap done: 1 IP address (1 host up) scanned in 1.68 seconds
root@kali:~#
```

Syn scan 은 공격자가 해당IP로 syn 패킷을 보낸다. 이때 열려 있는 port 에서 syn, ack 이 온다면 공격자는 ack 대신 rst를 보내 강제종료 시킨다.  
위방법을 통해 열려 있는 port를 확인하는 공격이다.

# 실습 2

앞에서 본 9100/TCP jetdirect port가  
인쇄서버 포트임을 알게 되었다.

HP Jetdirect 인쇄 서버 - TCP/IP(UDP) 연결을 위한 HP Jetdirect 포트 ...

<https://support.hp.com/kr-ko/document/c02842501> ▸

Jetdirect의 포트 활성화에 대한 자세한 내용은 특정 인쇄 서버에 대한 설명서를 참조하십시오(대부분은 hp.com에 있음). 특히, Telnet 사용에 대한 섹션을 참조 ...

HP Jetdirect Print Servers - HP Jetdirect Port Numbers for TCP/IP ...

<https://support.hp.com/us-en/document/c02480766> ▸ 이 페이지 번역하기

These ports can be use to FTP files directly to Jetdirect print servers. HP Jetdirect listens on TCP port 20 for FTP connection requests. Port 21 is the control port, ...

JetDirect - Wikipedia

<https://en.wikipedia.org/wiki/JetDirect> ▸ 이 페이지 번역하기

HP Jetdirect is the name of a technology sold by Hewlett-Packard that allows computer printers to be directly attached to a Local Area Network. The "Jetdirect" designation covers a range of models from the external 1 and 3 port parallel print servers known as the 300x and 500x, ...

History · External print servers · Internal print servers · Other Jetdirect products

Port 9100 printing - Hacking Printers

[hacking-printers.net/wiki/index.php/Port\\_9100\\_printing](https://hacking-printers.net/wiki/index.php/Port_9100_printing) ▸ 이 페이지 번역하기

2017. 3. 24. - Raw port 9100 printing, also referred to as JetDirect, AppSocket or PDL-datastream actually is not a printing protocol by itself. Instead all data ...

Default printer ports? - Hewlett Packard Enterprise Community

<https://community.hpe.com/t5/Networking/...ports/t5-p/5658643> ▸ 이 페이지 번역하기

답변 3개

2012. 5. 15. - For hp-ux default models like rmodel /dumb it needs to listen on the port 515/tcp, if it is jetdirect printer model and using 'HP Jetdirect software' ...

printing - AppSocket/HP JetDirect - how to find host and port ...

<https://askubuntu.com/.../appsocket-hp-jetdirect-how-to-find-host...> ▸ 이 페이지 번역하기

답변 1개

2016. 3. 13. - The host is the printer itself. You have to configure the JetDirect card in the printer to a proper IP address. Is the printer use autoconfigure ...

Integrating Linux and Windows - 152페이지 - Google 도서 검색결과

<https://books.google.co.kr/books?isbn=0130306703> - 이 페이지 번역하기

Mike McCune - 2001 - Computers

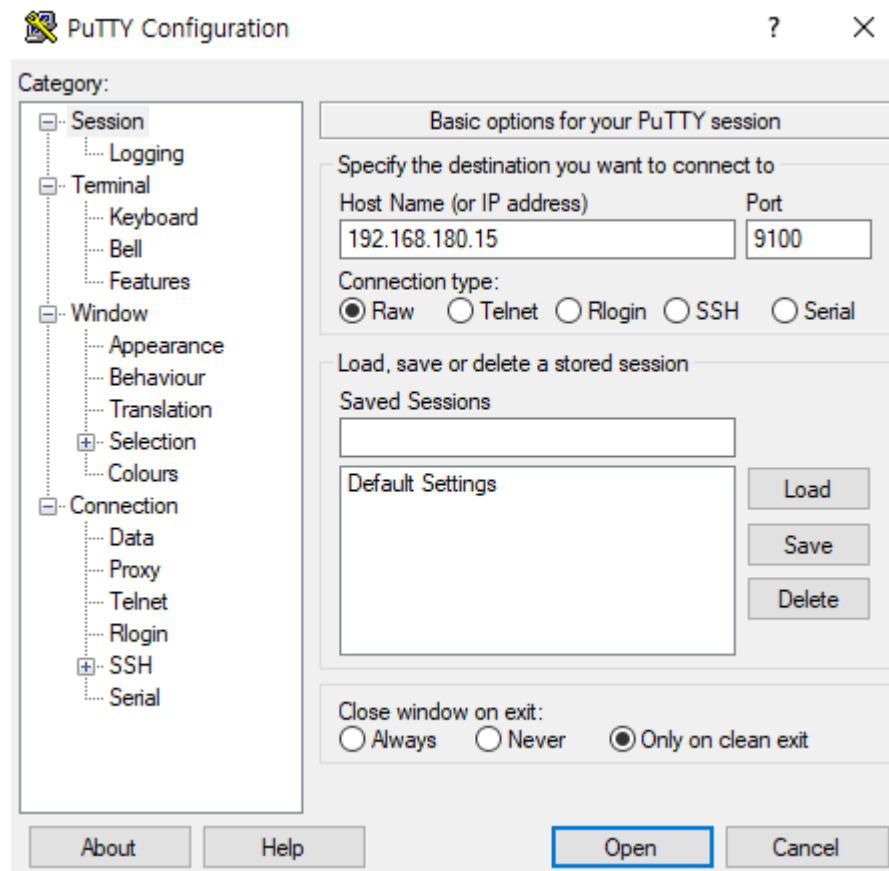
Hewlett Packard (HP) JetDirect printers need to send non-text output as raw on the queue option, which is set on the JetDirect port. A JetDirect printer is an HP ...

Using Network Printers - CUPS.org

<https://www.cups.org/doc/network.html> ▸ 이 페이지 번역하기

# 실습 2

Putty 를 사용하여  
인쇄 서버에 접속해준다.



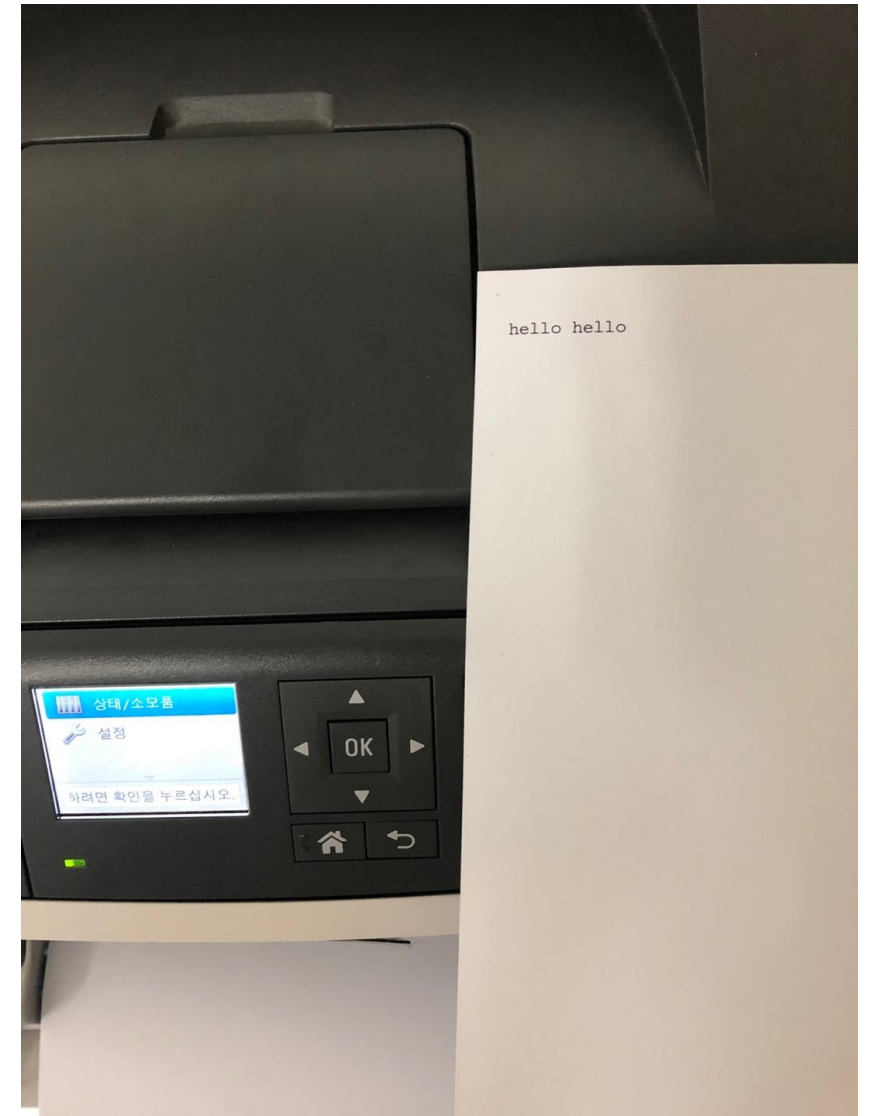
# 실습 2

입력하고 싶은 말을  
입력해주고 세션을 종료한다.



# 실습 2

Hello hello 가 프린트 된 것을 확인 할 수 있다.



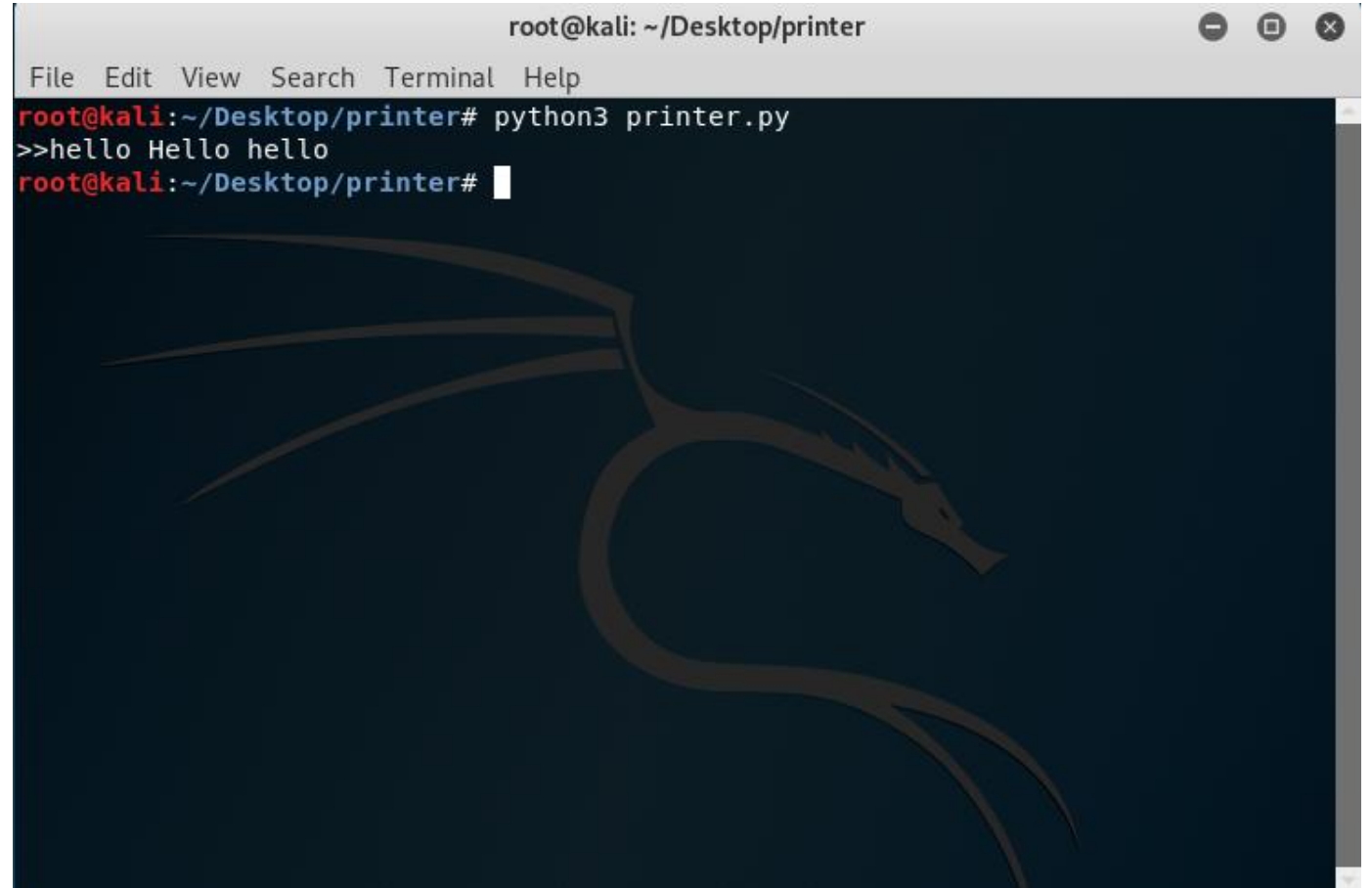
# 실습 3

Python3 로 툴 만들기



# 실습 3

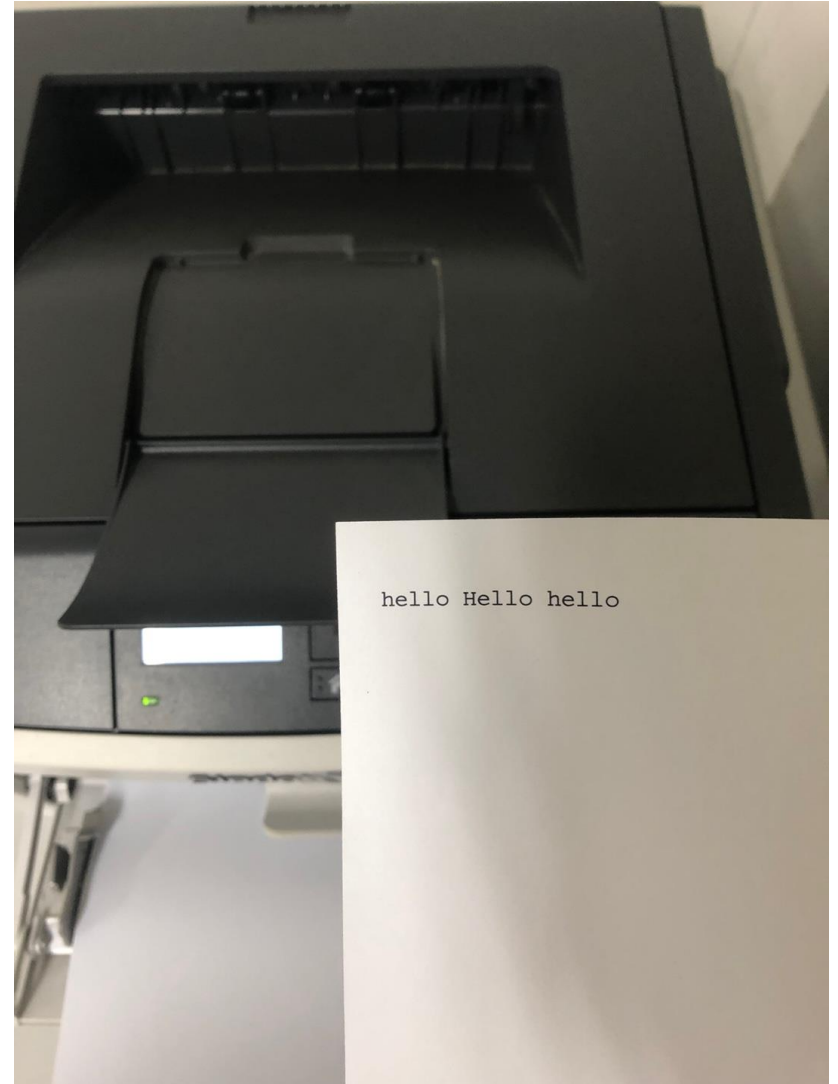
Python3 printer.py 로 툴을  
실행시킨다

A screenshot of a terminal window titled 'root@kali: ~/Desktop/printer'. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal shows the command 'python3 printer.py' being executed, which outputs '>>hello Hello hello'. The prompt 'root@kali:~/Desktop/printer#' is visible, followed by a cursor. A large, faint dragon logo is visible in the background of the terminal window.

```
root@kali: ~/Desktop/printer
File Edit View Search Terminal Help
root@kali:~/Desktop/printer# python3 printer.py
>>hello Hello hello
root@kali:~/Desktop/printer#
```

# 실습 3

hello Hello hello 가  
프린트 된 것을 확인 할 수 있다.



# 실습 3에 사용된 틀

While 문 사용시 강력한  
자원 소모 공격 가능

[illegible]

# 배운 점

(프린터 인쇄 서버 취약점)

[프린터의 9100번 포트는 인쇄 서버 포트이며 인쇄포트에 쉽게 접근 할 수 있다]  
위 프린터 해킹 실습을 통하여 network printer 는 해킹이 가능

스텔스 스캔(nmap -sS)

[대상 IP 에 공격자가 syn 패킷을 보내고 열려 있는 포트에게서 syn, ack 을 받는다.  
이후 공격자는 ack 을 보내지않고 rst (강제종료) 패킷을 보낸다.

이렇게 열려 있는 포트를 스캔 할 수 있다]

클라이언트에서 서버로 데이터를 보내는 소켓프로그래밍