Kioptrix-Vulnhub Level 2 Written by Macha

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

2379 Captured ARP Req/Rep packets, from 7 hosts.   Total size: 142740

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.1     c8:d3:a3:de:53:20    994   59640  D-Link International
192.168.1.27    54:48:10:e2:00:39    144    8640  Dell Inc.
192.168.1.32    00:0c:29:3d:69:f7    148    8880  VMware, Inc.
192.168.1.23    50:9a:4c:b9:a5:1c      1      60  Dell Inc.
192.168.1.25    54:e1:ad:0e:4b:03   1090   65400  LCFC(HeFei) Electronics Technology co., ltd
192.168.1.26    d4:81:d7:f6:a0:b8      1      60  Dell Inc.
192.168.1.28    54:bf:64:20:8e:f7      1      60  Dell Inc.
```

Figure 1: Firstly i using netdiscover to identify the vmware i setup for kioptrix machine

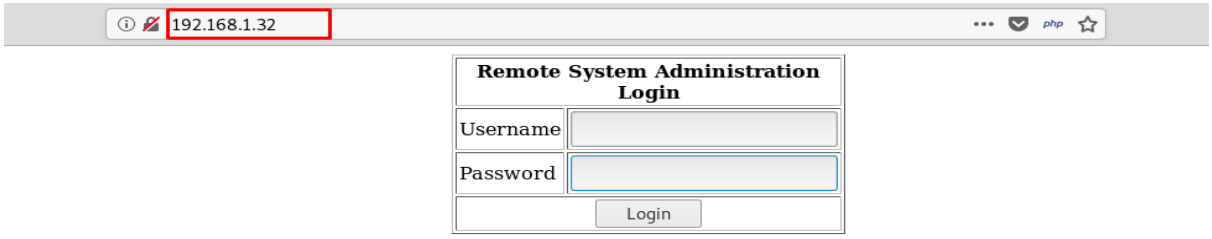

Figure 2:Yeah this is my victim to enumerate more

```
tarting Nmap 7.70 ( https://nmap.org ) at 2019-04-18 02:44 EDT
map scan report for 192.168.1.32
ost is up (0.0022s latency).
ot shown: 65528 closed ports
ORT     STATE SERVICE    VERSION
2/tcp   open  ssh        OpenSSH 3.9p1 (protocol 1.99)
0/tcp   open  http       Apache httpd 2.0.52 ((CentOS))
11/tcp  open  rpcbind    2 (RPC #100000)
43/tcp  open  ssl/https?
18/tcp  open  status     1 (RPC #100024)
31/tcp  open  ipp        CUPS 1.1
306/tcp open  mysql      MySQL (unauthorized)
AC Address: 00:0C:29:3D:69:F7 (VMware)
```

Figure 3: I starting using nmap to know what services is running in kioptrix machine

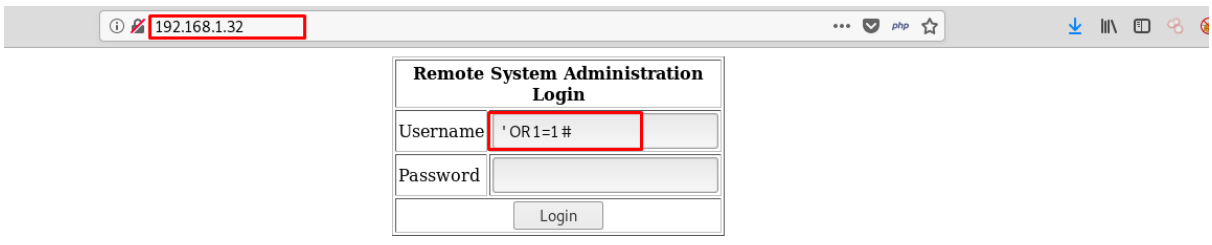

Figure 4:The web application is vulnerable to sql injection

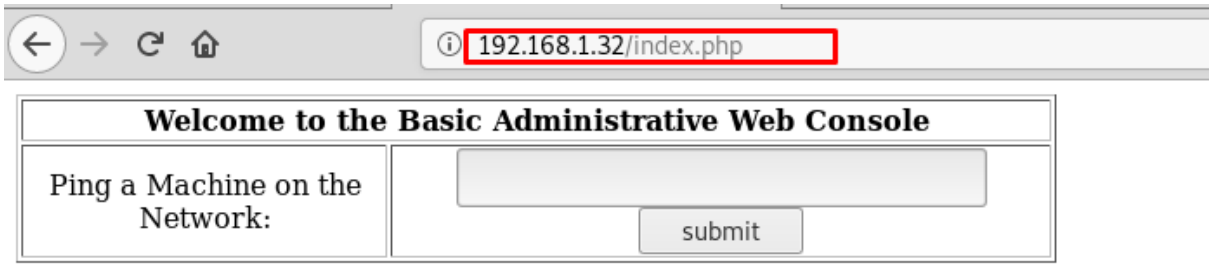

Figure 5:After i using sql injection query i found administrative web console

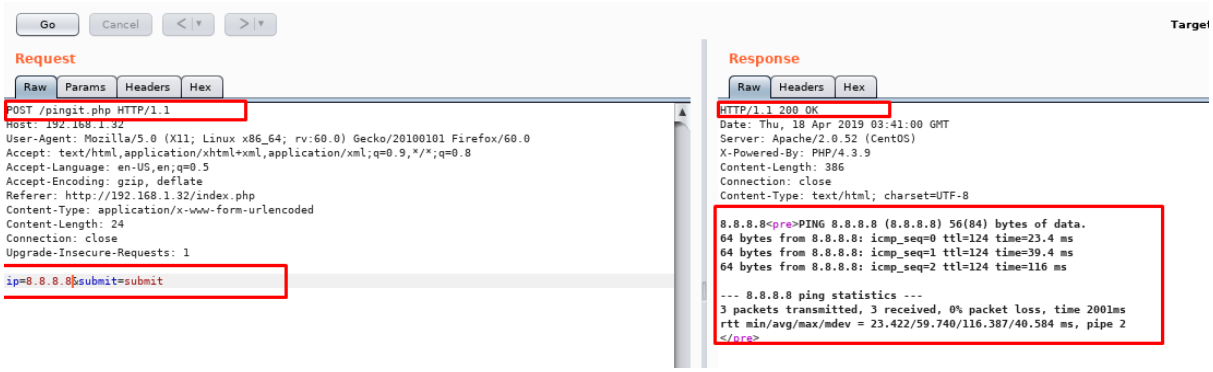

Figure 6:From here we able ping 8.8.8.8 it's look like command injection in web application

Figure 7:I try to get bash reverse shell from pentest monkey to perform reverse shell

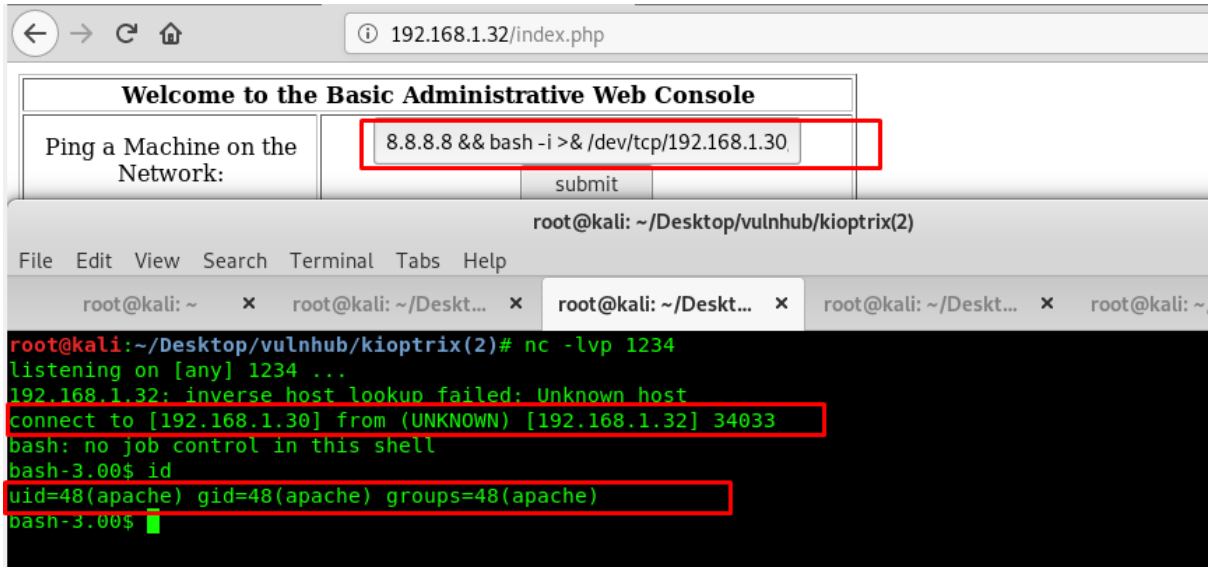

Figure 8:From here i using reverse shell to bind shell to my kali box and finally i got shell and my shell is low privilege

Privilege Escalation

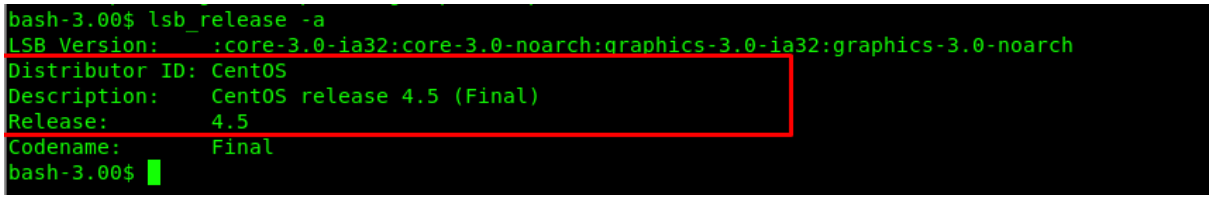

Figure 9:From here kioptrix machine using os centos and kernel version is 4.5.

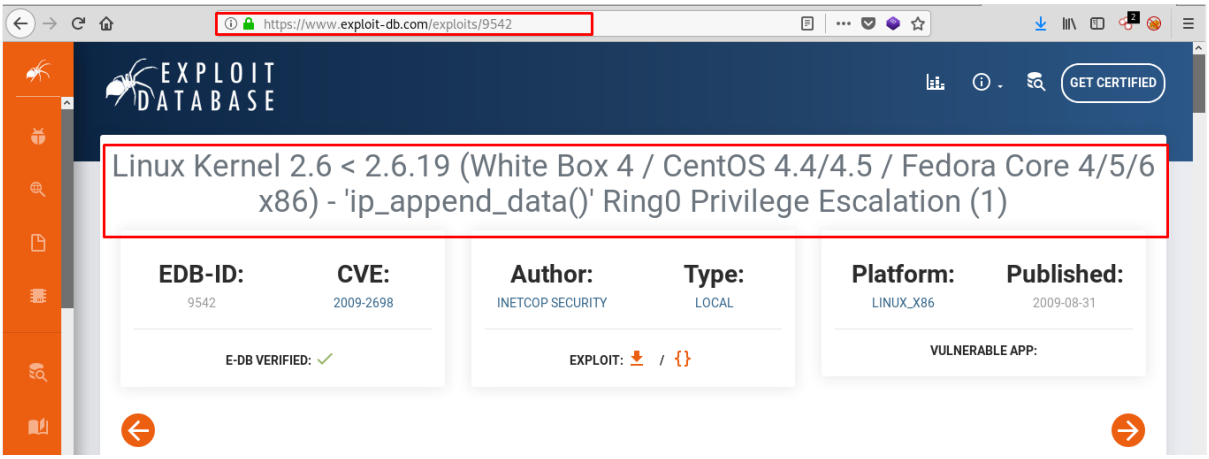

Figure 10:I just search in google the centos kernel version some exploit able to perform privilege escalation

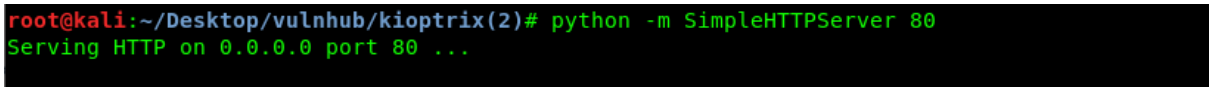

Figure 11:After i download the exploit file i want to transfer the exploit to victim machine this method I using for transfer file.

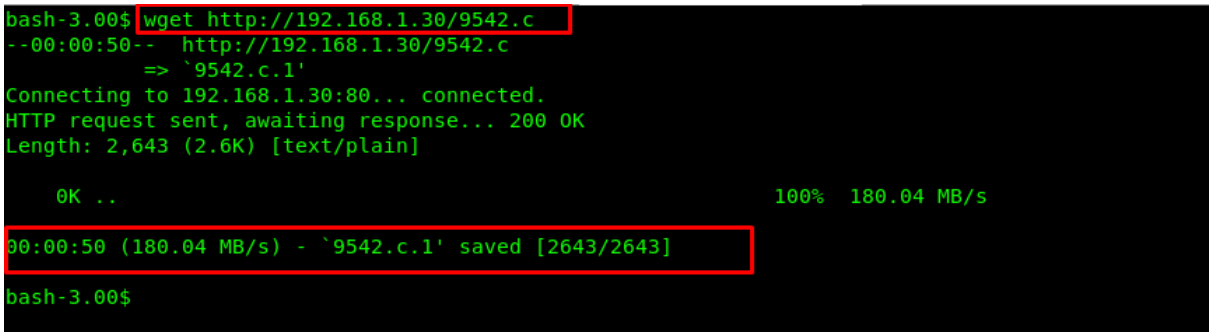

Figure 12:In victim machine i just wget the file

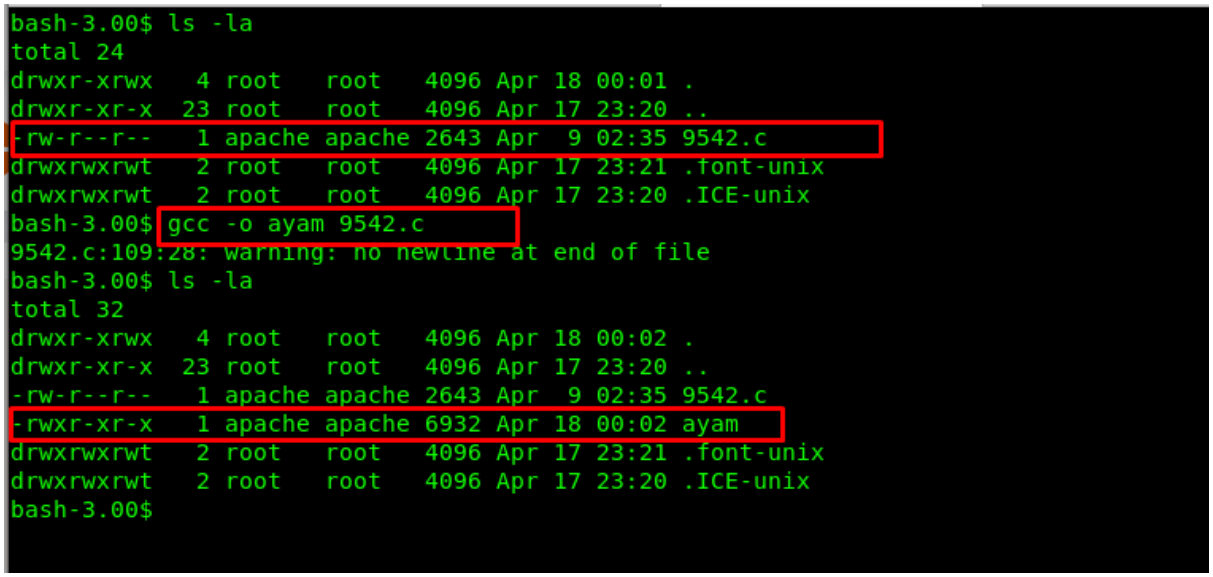

Figure 13:After the file successfully transfer i want compile the exploit file to ayam. ayam will be my exploit file

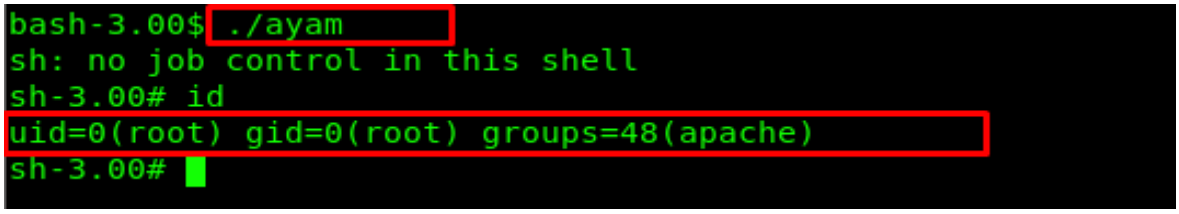

Figure 14:booyah finally i able run the exploit it's give me the root privilege in kioptrix machine