AUBURN

UNIVERSITY

Project 3

Blake Moore

12/1/2023

1 Executive Summary

This report documents my investigation of a Windows 10 registry. I was tasked to investigate this registry to find multiple different pieces of information. This includes: the users and groups associated with the system, the names of the users, the last login time and date of the user “aubie”, the automatically started applications and the time the autostart was last run, the private IP address of the system, and the most recently executed Windows Run commands. To recover this information from the provided Windows registry I primarily used the Registry Ripper tool and its associated plugins, which we discussed in class. All the information recovered is discussed in this report.

Table of Contents

2 Problem Description

For this assignment I was given a 7zip file containing a Windows 10 registry. I was tasked with investigating this registry to find different pieces of information, using any of the tools we discussed in class. To find the information to answer the questions provided, I used the Registry Ripper tool.

3 Analysis Techniques

In order to answer the first few questions for this investigation, I needed to pull information from the Security Accounts Manager, also known as the SAM file. To examine this file, I made a command that uses the Registry Ripper tool alongside a plugin. This command was “regripper -r SAM -p sampare”. Note that my personal install of the Registry Ripper tool is different due to being installed into Ubuntu on a Windows machine, so “regripper” replaces what would normally be “rip.pl”. To see this command run, see Figure 1. There were five users identified: Administrator, Guest, DefaultAccount, WDAGUtilityAccount, and aubie. See Figures 2-6 for these results. This also told me that the “aubie” user last logged in on October 23rd, 2020, at 00:01:01. This can be seen in Figure 6. There were 19 different groups identified, but only five of these contained any users. To see these five groups, see Figures 7-11.

After gaining the information about the users and groups associated with this registry from the SAM file, I continued on to investigating the system settings. To see the automatically run programs, I used the command “regripper -r software -p run”. This showed three different automatically ran applications: VMWare VM3DService Process, VMWare User Process, and Security Health. The last time the autostart was run was October 23rd, 2020, at 00:01:09. To see this, see Figure 12.

I then needed to find the private IP associated with the registry. To do this, I ran the Registry Ripper command “regripper -r system -p ips”. This showed the private IP associated with the registry, 192.168.48.141. To see this, see Figure 13.

The last step in the investigation was to find out what the most recently executed commands in the Windows Run window were. To find this information, I needed to use Registry Ripper to find the RunMRU key in the NTUSER.DAT file. I navigated to the aubie folder within the Users folder and ran “regripper -r NTUSER.DAT -p runmru”. This showed me three recently ran commands: cmd\1, "C:\Program Files\Windows Mail\wab.exe"\1, and "C:\Program Files\internet explorer\iexplore.exe"\1. To see this, see Figure 14.

4 Tables and Screenshots

All screenshots referenced are shown here.

```
blakemo@DESKTOP-GDG7PM8:/mnt/c/Users/bamaw/Downloads/foreProj3/unZip$ regripper -r SAM -p samparse
Launching samparse v.20200825
samparse v.20200825
(SAM) Parse SAM file for user & group mbrshp info


User Information
------------------------
Username        : Administrator [500]
Full Name       :
User Comment    : Built-in account for administering the computer/domain
Account Type    :
Account Created : 2020-09-08 05:56:00Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0
Embedded RID    : 500
  --> Password does not expire
  --> Account Disabled
  --> Normal user account
```

Figure 1: Registry Ripper command to examine SAM.

```
User Information
------------------------
Username         : Administrator [500]
Full Name        :
User Comment     : Built-in account for administering the computer/domain
Account Type     :
Account Created : 2020-09-08 05:56:00Z
Name             :
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count      : 0
Embedded RID     : 500
  --> Normal user account
  --> Password does not expire
  --> Account Disabled
```

Figure 2: Administrator user information.

```
Username         : Guest [501]
Full Name        :
User Comment     : Built-in account for guest access to the computer/domain
Account Type     :
Account Created : 2020-09-08 05:56:00Z
Name             :
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count      : 0
Embedded RID     : 501
  --> Password not required
  --> Normal user account
  --> Password does not expire
  --> Account Disabled
```

Figure 3: Guest user information.

```
Username         : DefaultAccount [503]
Full Name        :
User Comment     : A user account managed by the system.
Account Type     :
Account Created  : 2020-09-08 05:56:00Z
Name             :
Last Login Date  : Never
Pwd Reset Date   : Never
Pwd Fail Date    : Never
Login Count      : 0
Embedded RID     : 503
  --> Password not required
  --> Normal user account
  --> Password does not expire
  --> Account Disabled
```

Figure 4: DefaultAccount user information.

```
Username         : WDAGUtilityAccount [504]
Full Name        :
User Comment     : A user account managed and used by the system for Windows Defender Application Guard scenarios.
Account Type     :
Account Created  : 2020-09-08 05:56:00Z
Name             :
Last Login Date  : Never
Pwd Reset Date   : 2020-09-08 07:51:58Z
Pwd Fail Date    : Never
Login Count      : 0
Embedded RID     : 504
  --> Normal user account
  --> Account Disabled
```

Figure 5: WDAGUtilityAccount user information.

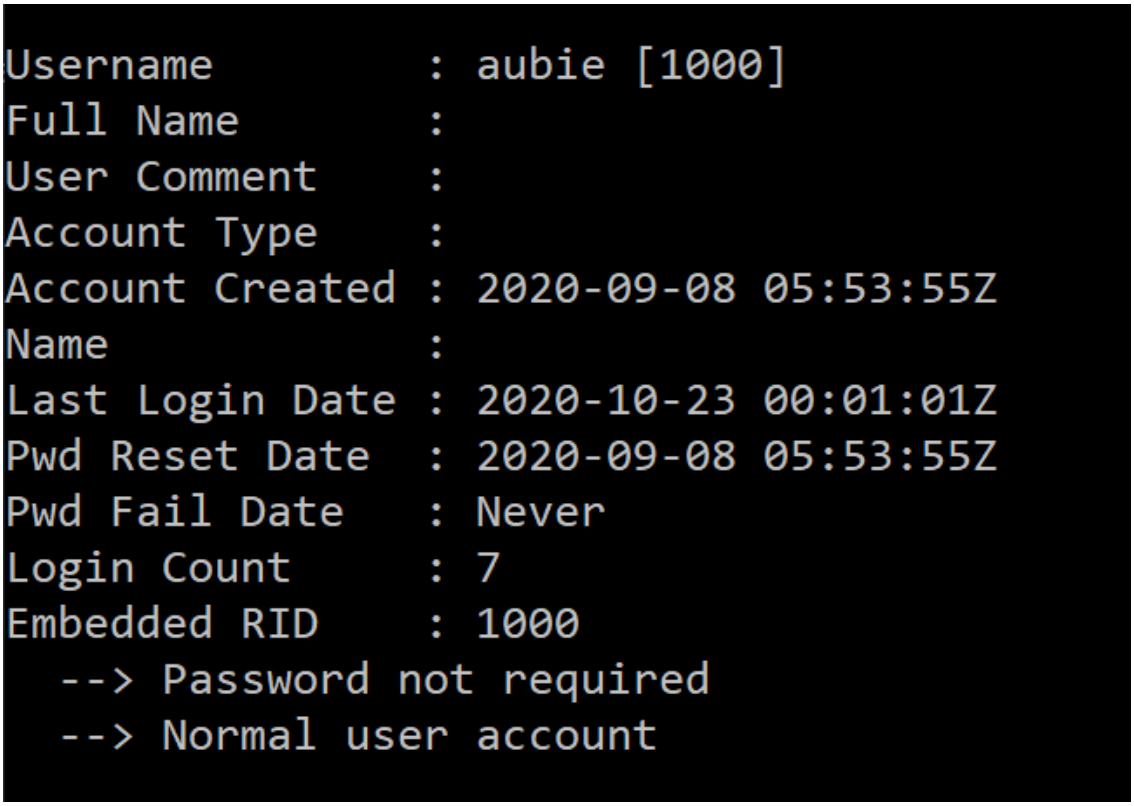

Figure 6: aubie user information.

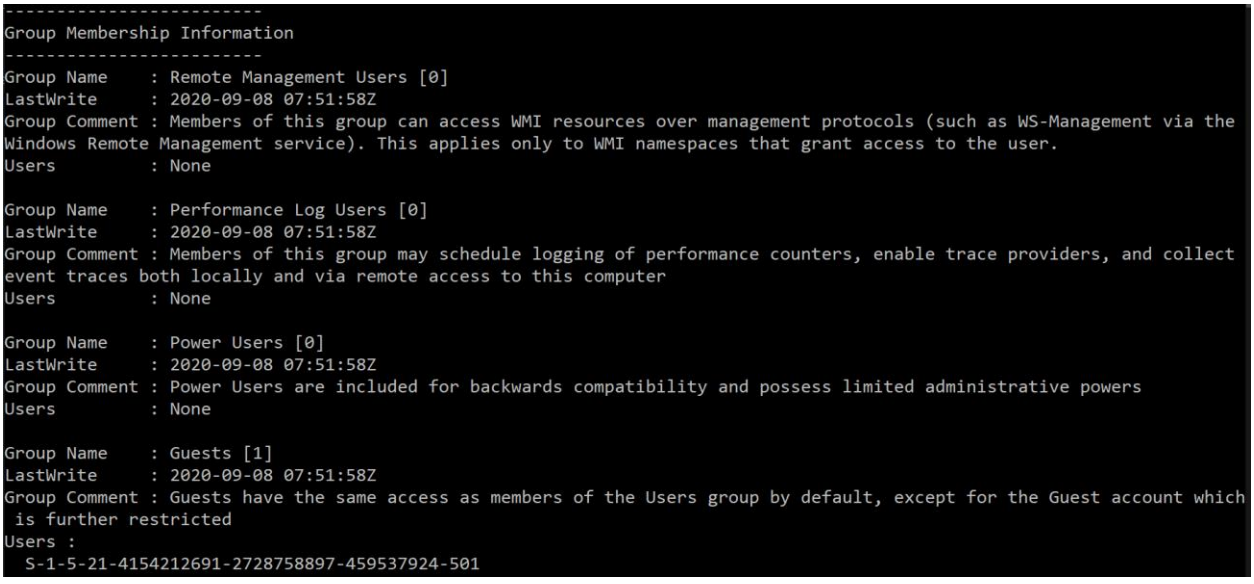

Figure 7: Example of groups with no users, and Guests [1] the first of the five groups with users.

```
Group Name    : IIS_IUSRS [1]
LastWrite     : 2020-09-08 07:51:58Z
Group Comment : Built-in group used by Internet Information Services.
Users :
  S-1-5-17
```

Figure 8: IIS_IURS [1], the second of the five groups with users.

```
Group Name    : Administrators [2]
LastWrite     : 2020-09-08 05:53:55Z
Group Comment : Administrators have complete and unrestricted access to the computer/domain
Users :
  S-1-5-21-4154212691-2728758897-459537924-1000
  S-1-5-21-4154212691-2728758897-459537924-500
```

Figure 9: Administrators [2], the third of the five groups with users.

```
Group Name    : Users [3]
LastWrite     : 2020-09-08 05:53:55Z
Group Comment : Users are prevented from making accidental or intentional system-wide changes and can run most applicati
ons
Users :
  S-1-5-4
  S-1-5-21-4154212691-2728758897-459537924-1000
  S-1-5-11
```

Figure 10: Users [3], the fourth of the five groups with users.

```
Group Name    : System Managed Accounts Group [1]
LastWrite     : 2020-09-08 07:51:58Z
Group Comment : Members of this group are managed by the system.
Users :
  S-1-5-21-4154212691-2728758897-459537924-503
```

Figure 11: System Managed Accounts Group [1], the last of the five groups with users.

```
blakemo@DESKTOP-GDG7PM8:/mnt/c/Users/bamaw/Downloads/foreProj3/unZip$ regripper -r software -p run
Launching run v.20200511
run v.20200511
(Software, NTUSER.DAT) [Autostart] Get autostart key contents from Software hive

Microsoft\Windows\CurrentVersion\Run
LastWrite Time 2020-10-23 00:01:09Z
  VMware User Process - "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
  SecurityHealth - %windir%\system32\SecurityHealthSystray.exe
  VMware VM3DService Process - "C:\Windows\system32\vm3dservice.exe" -u

Microsoft\Windows\CurrentVersion\Run has no subkeys.
```

Figure 12: Software run, showing automatically started applications and the last time the autostart was run.

```
blakemo@DESKTOP-GDG7PM8:/mnt/c/Users/bamaw/Downloads/foreProj3/unZip$ regripper -r system -p ips
Launching ips v.20200518
ips v.20200518
(System) Get IP Addresses and domains (DHCP,static)

IPAddress            Domain
192.168.48.141       localdomain                    Hint:
```

Figure 13: Registry ripper command being run to find the IP address associated with the registry.

```
blakemo@DESKTOP-GDG7PM8:/mnt/c/Users/bamaw/Downloads/foreProj3/unZip/Users/aubie$ regripper -r NTUSER.DAT -p runmru
Launching runmru v.20200525
runmru v.20200525
(NTUSER.DAT) Gets contents of user's RunMRU key

RunMru
Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
LastWrite Time 2020-10-21 13:38:13Z
MRUList = cba
a   cmd\1
b   "C:\Program Files\Windows Mail\wab.exe"\1
c   "C:\Program Files\internet explorer\iexplore.exe"\1
```

Figure 14: Results of examining NTUSER.DAT file.

5 Conclusions and Recommendations

I was given a 7zip file containing a Windows 10 registry and tasked with retrieving various information from it. I knew from class a few different tools that I could use to complete this task, but decided to use Registry Ripper since I am used to command line tools and its wide variety of plugins. With this tool and my knowledge from class I was able to recover all of the required information associated with the registry.