AUBURN

UNIVERSITY

Registry Forensics

Mary Mitchell, Vicki McLendon, and Adia Foster

3 December 2022

Table of Contents

Executive Summary

This report details our team's investigation of the Win10Reg.7z registry we were provided with. During this investigation, we discovered the users and groups associated with the system, general data regarding these users, information on the programs the system ran on startup, the system's IP address, and the recently used Windows Run commands. This information is detailed in the report and can also be seen in the table below. The primary tool we used to collect this information was Registry Ripper. Along with the plugin commands provided to us in the class demo notes, we were able to determine the proper commands to collect the information we were looking for.

Users	Groups	Autostart Programs	IP Address	Run Commands
Administrator	19 identified	VMware VM3DService Process	192.169.48.141	cmd\1
Guest	5 with users	SecurityHealth		"C:\Program Files\Windows Mail\wab.exe"\1
DefaultAccount		VMware User Process		"C:\Program Files\internet explorer\iexplore.exe"\1
WDAGUtilityAccount				
aubie				

Problem Description

For this project, we were given a forensically collected copy of a Windows 10 registry named Win10Reg.7z. Our team was tasked with investigating this registry and collecting certain pieces of information about the system it was pulled from as well as information on its users. This involved using the Registry Ripper tool we acquired in class to pull information from the registry.

Description of Analysis

To begin our investigation, we needed to find information in the Security Accounts Manager regarding the users and groups associated with the system. We determined how to get this information from the description of Registry Ripper plugin commands provided to us in our class demo notes. Once we had consulted the notes, we used the command ‘rip.pl -r SAM -p samparse’ which gave us descriptions of the users and groups on the system (Figure 1). Five users were identified in the output: Administrator, Guest, DefaultAccount, WDAGUtilityAccount, and aubie (Figures 2-6). Additionally, the user information gave us the last login time of the user aubie, which was on October 23, 2020, at 00:01:01 (Figure 6). The command then identified nineteen total groups, however, only five of these groups contained any users (Figures 7-11).

Once we obtained the information regarding the users and groups on the system, we investigated some of the system settings. We first took a look at the autostart programs that are run on login. This information was found in the software file using the command ‘rip.pl -r software -p run’ (Figure 12). It showed the following three autostart programs: VMWare VM3DService Process, VMWare User Process, and SecurityHealth, which were last run on October 23, 2020 at 00:01:09. Next we looked at the system file to obtain the IP address of the system which was 192.168.48.141 (Figure 13). Our last step was to find the most recently executed commands from the Windows Run command window. To do this, we needed to find

the RunMRU key in the NTUSER.DAT file. We used the command ‘rip.pl -r NTUSER.DAT -p runmru’, which gave us the commands: cmd\1, “C:\Program Files\Windows Mail\wab.exe”\1, and “C:\Program Files\internet explorer\iexplore.exe”\1 (Figure 14).

Conclusion

When we started this project we began by trying FTK Imager and Registry Explorer to conduct the investigation, but we were unable to consistently find the requested information on all of our machines. The interfaces proved to be confusing and did not provide a clear way to obtain information from the registry. Additionally, the applications behaved differently for each member of the team. This led us to continue searching for a tool that would produce clear and consistent results for everyone. In the end, that tool was Registry Ripper. We were hesitant to use Registry Ripper because of the lack of a GUI, however, it proved to be the most helpful tool and we are glad we used it. With the text document containing plugin commands, we quickly got the hang of using Registry Ripper. If we were to start this project again, we would definitely begin by using Registry Ripper. Using this tool sooner could have sped up our work on the assignment and improved our overall efficiency.

List of Figures


```
$ rip.pl -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
```



```
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
  --> Password does not expire
  --> Account Disabled
  --> Normal user account
```

Figure 4: DefaultAccount 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
  --> Password does not expire
  --> Account Disabled
  --> Normal user account
```

Figure 5: WDAGUtilityAccount 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
  --> Account Disabled
  --> Normal user account
```

Figure 6: aubie User Information

```
Username        : aubie [1000]
Full Name       :
User Comment    :
Account Type    :
Account Created : 2020-09-08 05:53:55Z
Name            :
Last Login Date : 2020-10-23 00:01:01Z
Pwd Reset Date  : 2020-09-08 05:53:55Z
Pwd Fail Date   : Never
Login Count     : 7
Embedded RID    : 1000
  --> Password not required
  --> Normal user account
```

Figure 7: IIS_IUSRS Group Information

```
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: Guest Group Information

```
Group Name    : Guests [1]
LastWrite     : 2020-09-08 07:51:58Z
Group Comment : Guests have the same access as members of the Users group by default, except for the Guest account which is further re
stricted
Users :
  S-1-5-21-4154212691-2728758897-459537924-501
```

Figure 9: Administrators Group Information

```
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-1-5-21-4154212691-2728758897-459537924-500
  S-1-5-21-4154212691-2728758897-459537924-1000
```

Figure 10: Users Group Information

```
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 applications
Users :
  S-1-5-11
  S-1-5-21-4154212691-2728758897-459537924-1000
  S-1-5-4
```

Figure 11: System Managed Accounts Group Information

```
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 12: Command to get Autostart Key Contents from Software Hive

```
$ rip.pl -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 VM3DService Process - "C:\Windows\system32\vm3dservice.exe" -u
  SecurityHealth - %windir%\system32\SecurityHealthSystray.exe
  VMware User Process - "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
```

Figure 13: Command to get IP Addresses and Domains

```
$ rip.pl -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 14: Command to get Contents of User's RunMRU Key

```
$ rip.pl -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
```