



AUBURN

---

UNIVERSITY

Project 3 Report

Laura Wilson

5 November 2023

## Executive Summary

In this report is our investigation of the Win10Reg.7z that was provided to us. The primary tool that was used to collect this information was Registry Ripper in addition to the plugin commands that were provided to us in the class notes. The groups and users that were associated with this system and the data regarding these users such as information on programs that ran during startup, the system's IP address, and Windows Run commands that were recently used on the system. This information is found in the table below.

Users	Groups	Autostart Programs	IP Address	Run Commands
Administrator	19 identified	VMware WM3DService Process	192.169.48.141	cmd\1
Guest	5 with users	SecurityHealth	none	"C:\Program Files\Windows Mail\wab.exe"\1
DefaultAccount	none	VMware User Process	none	"C:\Program Files\internet explorer\iexplore.exe"\1
WDAGUtilityAccount	none	none	none	none
aubie	none	none	none	none

## Problem Description

In this project we were given a forensically collected copy of the Windows 10 registry that was named Win10Reg.7z. We were tasked with investigating it and collecting specific information about the system that it was pulled from as well as its users. In order to do this we used the Registry Ripper tool to pull this information from the registry.

## Description of Analysis

In our investigation we started with finding information in the Security Accounts Manager regarding the system's users and groups. We used the command 'rip.pl -r SAM p samparse' which gave us descriptions of the system's users and groups (Figure 1-6). The five users that were identified in the output: Administrator, Guest, DefaultAccount, WDAGUtilityAccount, and aubie. In addition, the user information gave us that the last login time of the user aubie, which happened to be October 23, 2020, at 00:01:01. The command we used identified a total of nineteen groups but only five contains users.

After gaining information about the users and groups on the stem we gathered information about the systems settings. First, we looked at the autostart programs that ran during login. Using the command 'rip.pl -r software -p run' (Figure 7) was used to find the software file. This showed that there were three autostart programs: VMWare VM3DService Proces, VMWare User Process, and SecurityHealth, which ran on October 23, 2020, at 00:01:09. Next was looking at the system file to obtain the IP address of the system which was 192.168.48.141 (Figure 8). The last step was to find the most recently executed commands from the Windows Run command window. To do this we needed to run the RunMRU key in the NTUSER.DAT file. Using the command 'rip.pl -r NTUSER.DAT -p runmru' that gave us the three commands: cmd\1, "C:\Program Files\Windows Mail\wab.exe"\1, and "C:\Program Files\internet explorer\iexplore.exe"\1 (Figure 9).

## **Conclusion**

When starting the project we looked through class demo notes to find out that use the tool Registry Ripper would be the tool best used for this project. If we were to start this project again we would have definitely started planned to start earlier as this project didn't take as long as previously thought.

## List of Figures

Figure 1: a copy of the document from entering 'rip.pl -r SAM p samparse'

samparse v.20220921

(SAM) Parse SAM file for user & group mbrshp info

### User Information

-----

Username : Administrator [500]

SID : S-1-5-21-4154212691-2728758897-459537924-500

Full Name :

User Comment : Built-in account for administering the computer/domain

Account Type :

Account Created : Tue Sep 8 05:56:00 2020 Z

Name :

Last Login Date : Never

Pwd Reset Date : Never

Pwd Fail Date : Never

Login Count : 0

--> Normal user account

--> Account Disabled

--> Password does not expire

Username : Guest [501]

SID : S-1-5-21-4154212691-2728758897-459537924-501

Full Name :

User Comment : Built-in account for guest access to the computer/domain

Account Type :

Account Created : Tue Sep 8 05:56:00 2020 Z

Name :

Last Login Date : Never

Pwd Reset Date : Never

Pwd Fail Date : Never

Login Count : 0

--> Password not required

--> Normal user account

--> Account Disabled

--> Password does not expire

Username : DefaultAccount [503]

SID : S-1-5-21-4154212691-2728758897-459537924-503

Full Name :

User Comment : A user account managed by the system.

Account Type :

Account Created : Tue Sep 8 05:56:00 2020 Z

Name :

Last Login Date : Never

Pwd Reset Date : Never

Pwd Fail Date : Never

Login Count : 0

--> Password not required

--> Normal user account

--> Account Disabled

--> Password does not expire

Username : WDAGUtilityAccount [504]

SID : S-1-5-21-4154212691-2728758897-459537924-504

Full Name :

User Comment : A user account managed and used by the system for Windows Defender Application

Guard scenarios.

Account Type :

Account Created : Tue Sep 8 05:56:00 2020 Z

Name :

Last Login Date : Never

Pwd Reset Date : Tue Sep 8 07:51:58 2020 Z

Pwd Fail Date : Never

Login Count : 0

--> Normal user account

--> Account Disabled

Username : aubie [1000]

SID : S-1-5-21-4154212691-2728758897-459537924-1000

Full Name :

User Comment :

Account Type :

Account Created : Tue Sep 8 05:53:55 2020 Z



Name :

Last Login Date : Fri Oct 23 00:01:01 2020 Z

Pwd Reset Date : Tue Sep 8 05:53:55 2020 Z

Pwd Fail Date : Never

Login Count : 7

--> Password not required

--> Normal user account

-----

#### Group Membership Information

-----

Group Name : Cryptographic Operators [0]

LastWrite : Tue Sep 8 07:51:58 2020 Z

Group Comment : Members are authorized to perform cryptographic operations.

Users : None

Group Name : Performance Log Users [0]

LastWrite : Tue Sep 8 07:51:58 2020 Z

Group Comment : Members of this group may schedule logging of performance counters, enable trace providers, and collect event traces both locally and via remote access to this computer

Users : None

Group Name : Performance Monitor Users [0]

LastWrite : Tue Sep 8 07:51:58 2020 Z

Group Comment : Members of this group can access performance counter data locally and remotely

Users : None

Group Name : Users [3]

LastWrite : Tue Sep 8 05:53:55 2020 Z

Group Comment : Users are prevented from making accidental or intentional system-wide changes and can run most applications

Users :

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

S-1-5-4

S-1-5-11

Group Name : Distributed COM Users [0]

LastWrite : Tue Sep 8 07:51:58 2020 Z

Group Comment : Members are allowed to launch, activate and use Distributed COM objects on this machine.

Users : None

Group Name : Administrators [2]

LastWrite : Tue Sep 8 05:53:55 2020 Z

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

Group Name : Network Configuration Operators [0]

LastWrite : Tue Sep 8 07:51:58 2020 Z

Group Comment : Members in this group can have some administrative privileges to manage configuration of networking features

Users : None

Group Name : Remote Management Users [0]

LastWrite : Tue Sep 8 07:51:58 2020 Z

Group Comment : Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management service). This applies only to WMI namespaces that grant access to the user.

Users : None

Group Name : Replicator [0]

LastWrite : Tue Sep 8 07:51:58 2020 Z

Group Comment : Supports file replication in a domain

Users : None

Group Name : Hyper-V Administrators [0]

LastWrite : Tue Sep 8 07:51:58 2020 Z

Group Comment : Members of this group have complete and unrestricted access to all features of Hyper-V.

Users : None

Group Name : Device Owners [0]

LastWrite : Tue Sep 8 07:51:58 2020 Z

Group Comment : Members of this group can change system-wide settings.

Users : None

Group Name : Access Control Assistance Operators [0]

LastWrite : Tue Sep 8 07:51:58 2020 Z

Group Comment : Members of this group can remotely query authorization attributes and permissions for resources on this computer.

Users : None

Group Name : IIS\_IUSRS [1]

LastWrite : Tue Sep 8 07:51:58 2020 Z

Group Comment : Built-in group used by Internet Information Services.

Users :

S-1-5-17

Group Name : Event Log Readers [0]

LastWrite : Tue Sep 8 07:51:58 2020 Z

Group Comment : Members of this group can read event logs from local machine

Users : None

Group Name : Remote Desktop Users [0]

LastWrite : Tue Sep 8 07:51:58 2020 Z

Group Comment : Members in this group are granted the right to logon remotely

Users : None

Group Name : System Managed Accounts Group [1]

LastWrite : Tue Sep 8 07:51:58 2020 Z

Group Comment : Members of this group are managed by the system.

Users :

S-1-5-21-4154212691-2728758897-459537924-503

Group Name : Power Users [0]

LastWrite : Tue Sep 8 07:51:58 2020 Z

Group Comment : Power Users are included for backwards compatibility and possess limited administrative powers

Users : None

Group Name : Backup Operators [0]

LastWrite : Tue Sep 8 07:51:58 2020 Z

Group Comment : Backup Operators can override security restrictions for the sole purpose of backing up or restoring files

Users : None

Group Name : Guests [1]

LastWrite : Tue Sep 8 07:51:58 2020 Z

Group Comment : Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted

Users :

S-1-5-21-4154212691-2728758897-459537924-501

Analysis Tips:

- For well-known SIDs, see <http://support.microsoft.com/kb/243330>

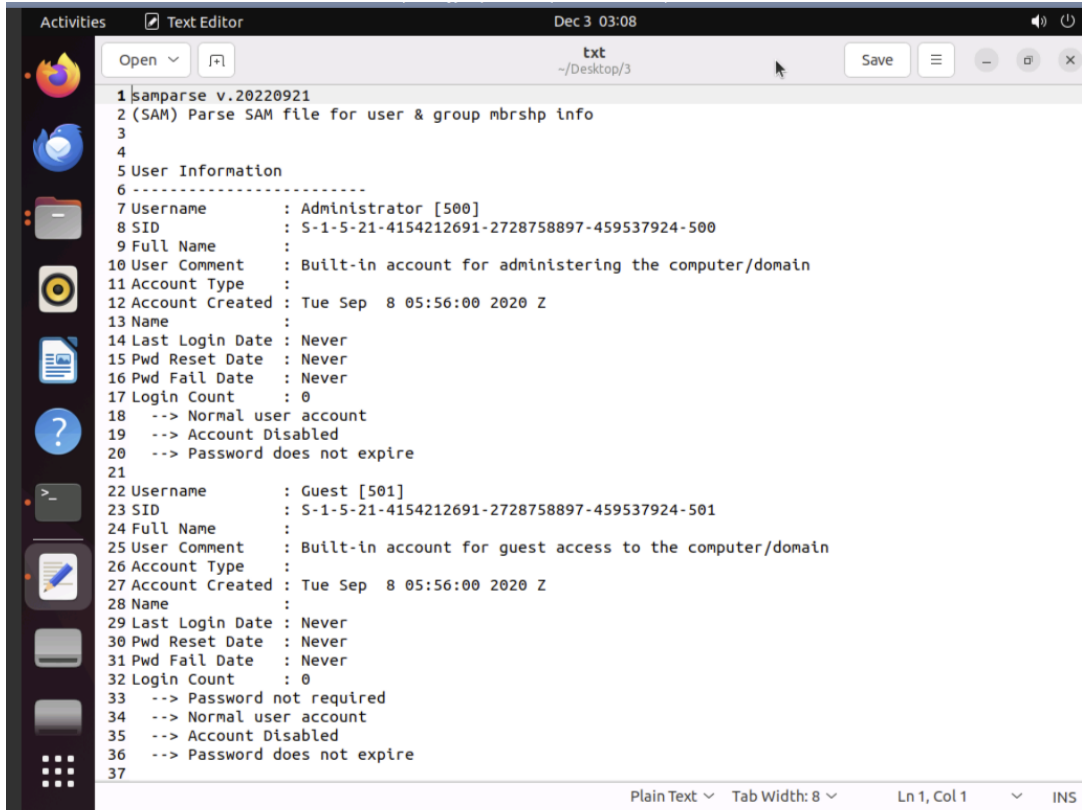
- S-1-5-4 = Interactive

- S-1-5-11 = Authenticated Users

- Correlate the user SIDs to the output of the ProfileList plugin

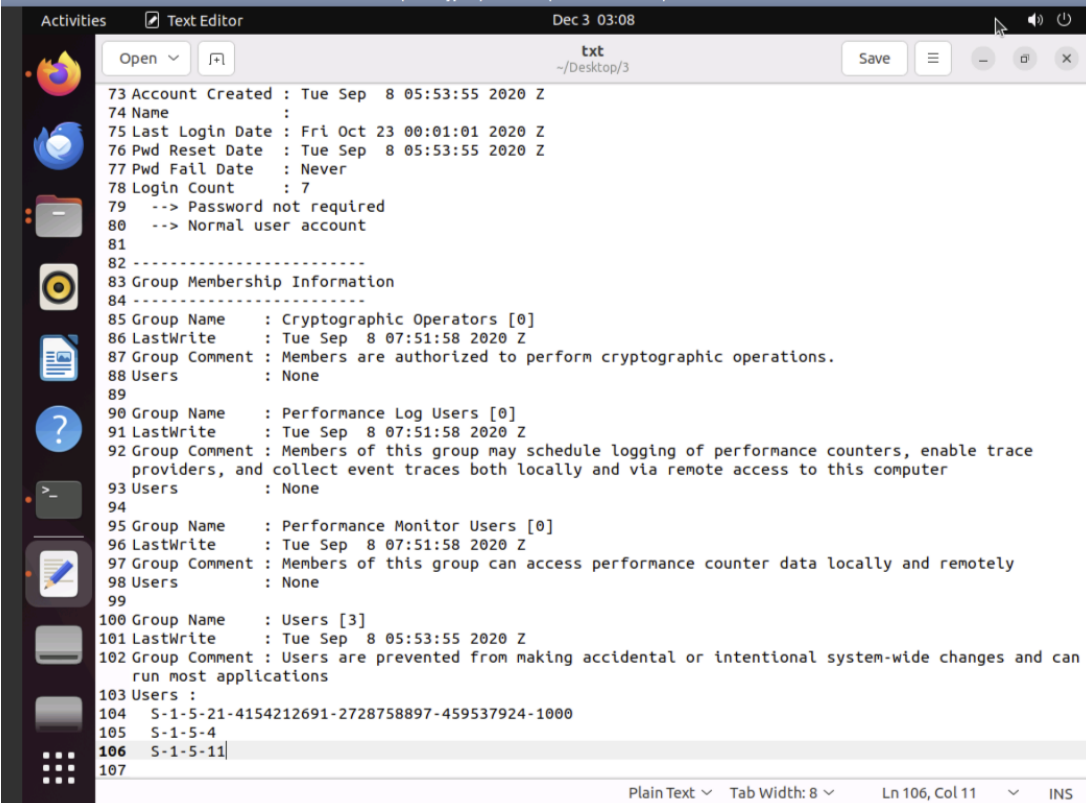
Figure 2-6: evidence from 'rip.pl -r SAM p samparse' command on the machine

Figure 2: start of groups and users on system



```
1 | samparse v.20220921
2 (SAM) Parse SAM file for user & group mbrshp info
3
4
5 User Information
6 -----
7 Username      : Administrator [500]
8 SID           : S-1-5-21-4154212691-2728758897-459537924-500
9 Full Name     :
10 User Comment  : Built-in account for administering the computer/domain
11 Account Type  :
12 Account Created : Tue Sep  8 05:56:00 2020 Z
13 Name         :
14 Last Login Date : Never
15 Pwd Reset Date : Never
16 Pwd Fail Date  : Never
17 Login Count   : 0
18 --> Normal user account
19 --> Account Disabled
20 --> Password does not expire
21
22 Username      : Guest [501]
23 SID           : S-1-5-21-4154212691-2728758897-459537924-501
24 Full Name     :
25 User Comment  : Built-in account for guest access to the computer/domain
26 Account Type  :
27 Account Created : Tue Sep  8 05:56:00 2020 Z
28 Name         :
29 Last Login Date : Never
30 Pwd Reset Date : Never
31 Pwd Fail Date  : Never
32 Login Count   : 0
33 --> Password not required
34 --> Normal user account
35 --> Account Disabled
36 --> Password does not expire
37
```





The screenshot shows a Linux desktop environment. On the left is a vertical dock with icons for Firefox, a mail client, a file manager, a terminal, and a help icon. The top panel displays 'Activities', 'Text Editor', and the date 'Dec 3 03:08'. The text editor window, titled 'txt' and located at '~/Desktop/3', contains the following text:

```
73 Account Created : Tue Sep 8 05:53:55 2020 Z
74 Name :
75 Last Login Date : Fri Oct 23 00:01:01 2020 Z
76 Pwd Reset Date : Tue Sep 8 05:53:55 2020 Z
77 Pwd Fail Date : Never
78 Login Count : 7
79 --> Password not required
80 --> Normal user account
81
82 -----
83 Group Membership Information
84 -----
85 Group Name : Cryptographic Operators [0]
86 LastWrite : Tue Sep 8 07:51:58 2020 Z
87 Group Comment : Members are authorized to perform cryptographic operations.
88 Users : None
89
90 Group Name : Performance Log Users [0]
91 LastWrite : Tue Sep 8 07:51:58 2020 Z
92 Group Comment : Members of this group may schedule logging of performance counters, enable trace
providers, and collect event traces both locally and via remote access to this computer
93 Users : None
94
95 Group Name : Performance Monitor Users [0]
96 LastWrite : Tue Sep 8 07:51:58 2020 Z
97 Group Comment : Members of this group can access performance counter data locally and remotely
98 Users : None
99
100 Group Name : Users [3]
101 LastWrite : Tue Sep 8 05:53:55 2020 Z
102 Group Comment : Users are prevented from making accidental or intentional system-wide changes and can
run most applications
103 Users :
104 S-1-5-21-4154212691-2728758897-459537924-1000
105 S-1-5-4
106 S-1-5-11|
107
```

The status bar at the bottom of the text editor shows 'Plain Text', 'Tab Width: 8', 'Ln 106, Col 11', and 'INS'.

Figure 3:

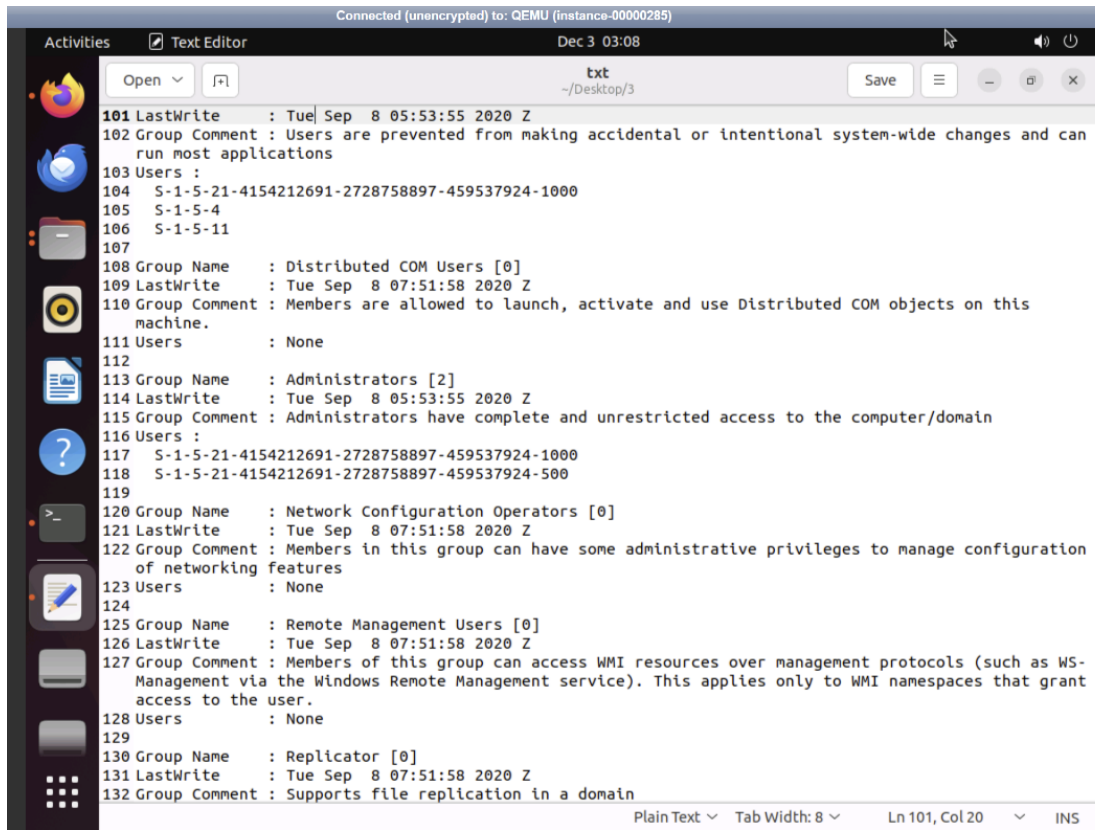


Figure 4

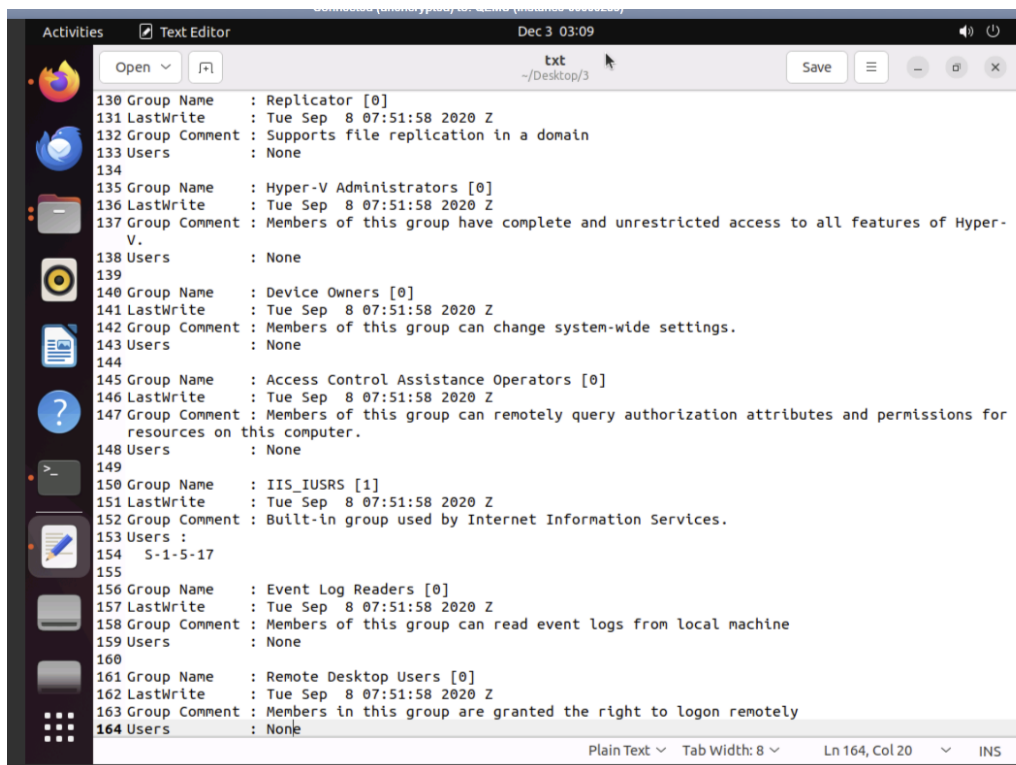
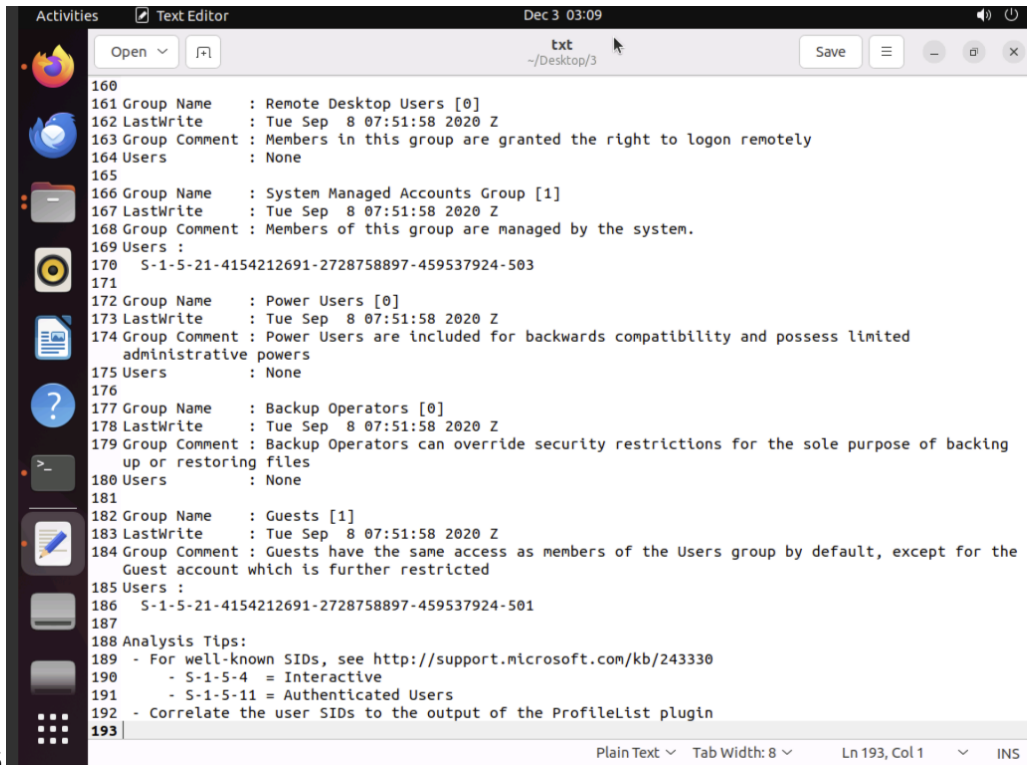


Figure 5

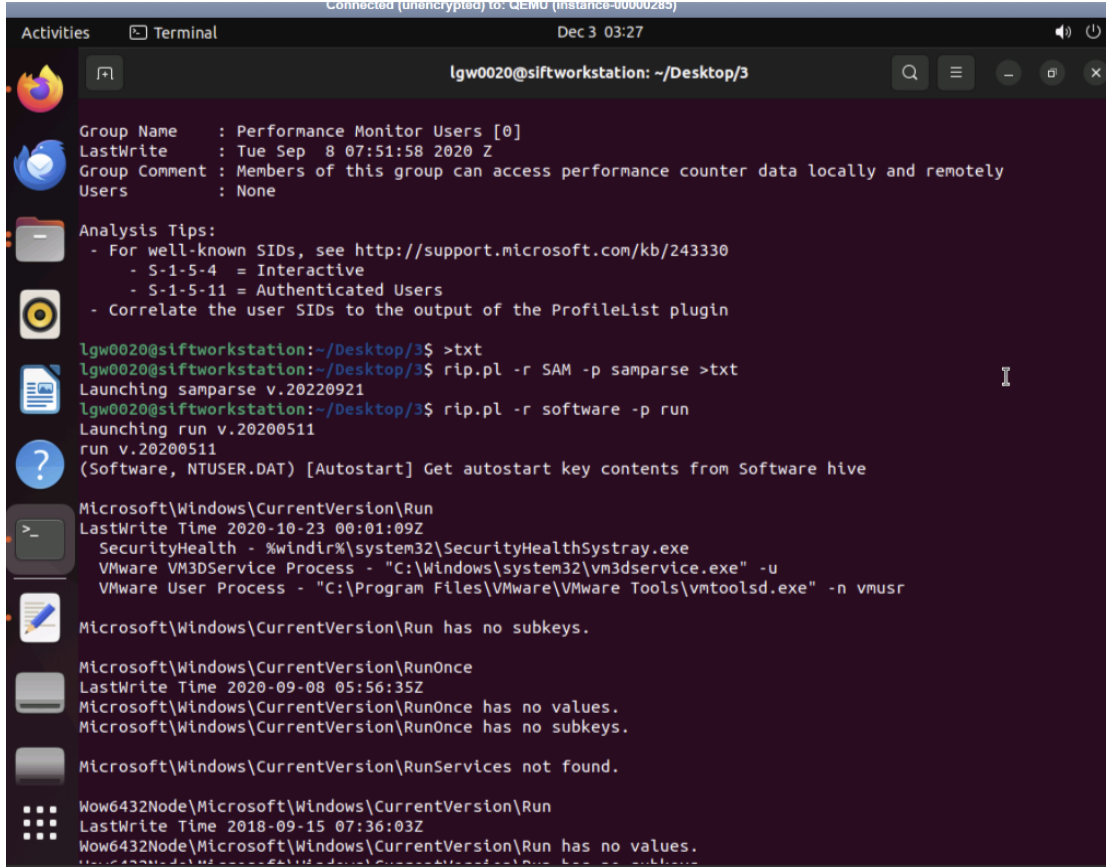


The screenshot shows a Linux desktop with a dark theme. On the left is a vertical dock with icons for Firefox, a mail client, a file manager, a terminal, and a text editor. The top panel displays 'Activities', 'Text Editor', and the date 'Dec 3 03:09'. The text editor window, titled 'txt' at '~/Desktop/3', contains a list of system groups and their details. The status bar at the bottom indicates 'Plain Text', 'Tab Width: 8', 'Ln 193, Col 1', and 'INS'.

```
160
161 Group Name : Remote Desktop Users [0]
162 LastWrite : Tue Sep 8 07:51:58 2020 Z
163 Group Comment : Members in this group are granted the right to logon remotely
164 Users : None
165
166 Group Name : System Managed Accounts Group [1]
167 LastWrite : Tue Sep 8 07:51:58 2020 Z
168 Group Comment : Members of this group are managed by the system.
169 Users :
170 S-1-5-21-4154212691-2728758897-459537924-503
171
172 Group Name : Power Users [0]
173 LastWrite : Tue Sep 8 07:51:58 2020 Z
174 Group Comment : Power Users are included for backwards compatibility and possess limited
administrative powers
175 Users : None
176
177 Group Name : Backup Operators [0]
178 LastWrite : Tue Sep 8 07:51:58 2020 Z
179 Group Comment : Backup Operators can override security restrictions for the sole purpose of backing
up or restoring files
180 Users : None
181
182 Group Name : Guests [1]
183 LastWrite : Tue Sep 8 07:51:58 2020 Z
184 Group Comment : Guests have the same access as members of the Users group by default, except for the
Guest account which is further restricted
185 Users :
186 S-1-5-21-4154212691-2728758897-459537924-501
187
188 Analysis Tips:
189 - For well-known SIDs, see http://support.microsoft.com/kb/243330
190 - S-1-5-4 = Interactive
191 - S-1-5-11 = Authenticated Users
192 - Correlate the user SIDs to the output of the ProfileList plugin
193
```

Figure 6

Figure 7: Autostart key Content from Software hive



A terminal window titled "Connected (unattended) to: DEMO (instance:00000285)" with a timestamp of "Dec 3 03:27". The terminal shows the user "lgw0020@siftworkstation" in the directory "~/Desktop/3". The output includes group information for "Performance Monitor Users", analysis tips for SIDs, and the execution of "rip.pl" to query the registry. The registry output shows the "Run" key under "Microsoft\Windows\CurrentVersion\" for various users, with some keys having values and others being empty or not found.

```
lgw0020@siftworkstation: ~/Desktop/3
Group Name      : Performance Monitor Users [0]
LastWrite      : Tue Sep  8 07:51:58 2020 Z
Group Comment   : Members of this group can access performance counter data locally and remotely
Users          : None

Analysis Tips:
- For well-known SIDs, see http://support.microsoft.com/kb/243330
- S-1-5-4 = Interactive
- S-1-5-11 = Authenticated Users
- Correlate the user SIDs to the output of the ProfileList plugin

lgw0020@siftworkstation:~/Desktop/3$ >txt
lgw0020@siftworkstation:~/Desktop/3$ rip.pl -r SAM -p samparse >txt
Launching samparse v.20220921
lgw0020@siftworkstation:~/Desktop/3$ 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
SecurityHealth - %windir%\system32\SecurityHealthSystray.exe
VMware VM3DServ Process - "C:\Windows\system32\vm3dservice.exe" -u
VMware User Process - "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr

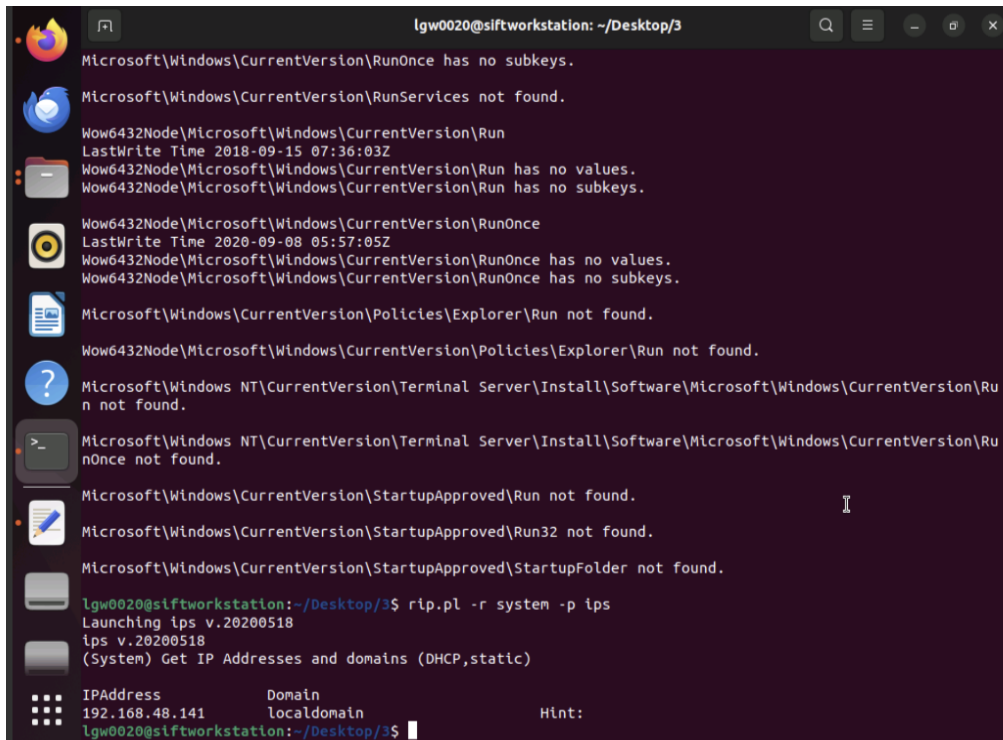
Microsoft\Windows\CurrentVersion\Run has no subkeys.

Microsoft\Windows\CurrentVersion\RunOnce
LastWrite Time 2020-09-08 05:56:35Z
Microsoft\Windows\CurrentVersion\RunOnce has no values.
Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.

Microsoft\Windows\CurrentVersion\RunServices not found.

Wow6432Node\Microsoft\Windows\CurrentVersion\Run
LastWrite Time 2018-09-15 07:36:03Z
Wow6432Node\Microsoft\Windows\CurrentVersion\Run has no values.
Wow6432Node\Wow6432Node\Microsoft\Windows\CurrentVersion\Run has no subkeys.
```

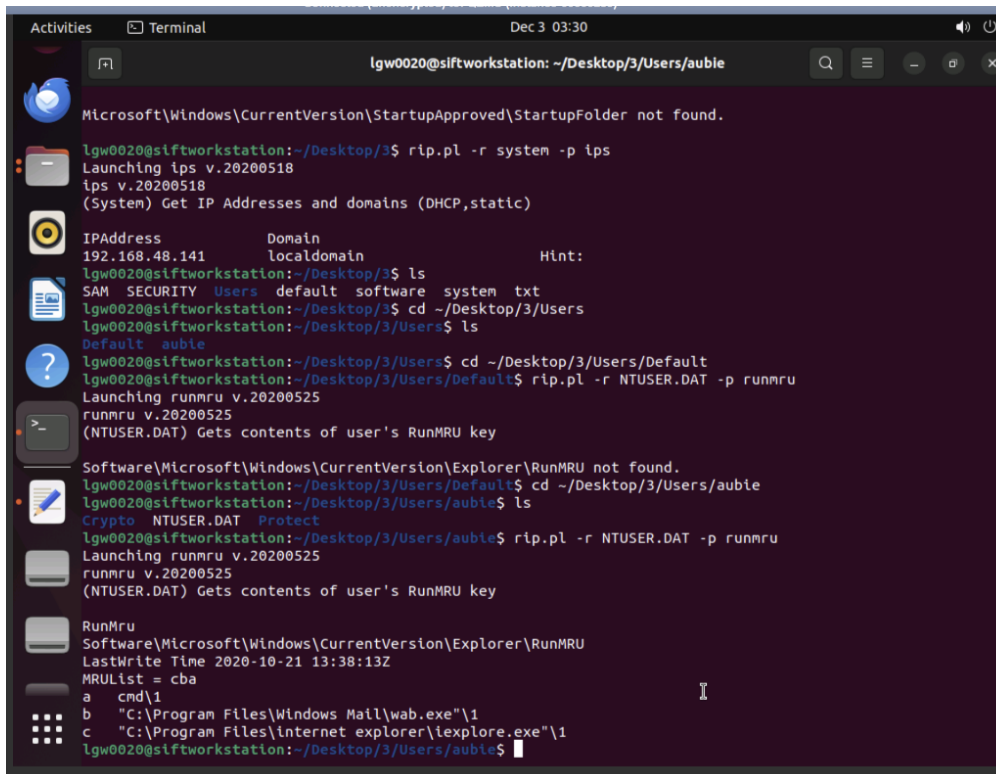
Figure 8: Command for IP address



```
lgw0020@siftworkstation: ~/Desktop/3
Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.
Microsoft\Windows\CurrentVersion\RunServices not found.
Wow6432Node\Microsoft\Windows\CurrentVersion\Run
LastWrite Time 2018-09-15 07:36:03Z
Wow6432Node\Microsoft\Windows\CurrentVersion\Run has no values.
Wow6432Node\Microsoft\Windows\CurrentVersion\Run has no subkeys.
Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce
LastWrite Time 2020-09-08 05:57:05Z
Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no values.
Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.
Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.
Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.
Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run
n not found.
Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run
Once not found.
Microsoft\Windows\CurrentVersion\StartupApproved\Run not found.
Microsoft\Windows\CurrentVersion\StartupApproved\Run32 not found.
Microsoft\Windows\CurrentVersion\StartupApproved\StartupFolder not found.
lgw0020@siftworkstation:~/Desktop/3$ rip.pl -r system -p ips
Launching ips v.20200518
ips v.20200518
(System) Get IP Addresses and domains (DHCP,static)

IPAddress      Domain      Hint:
192.168.48.141  localdomain
```

Figure 9: RunMRU key



The terminal window shows a series of commands and outputs for extracting the RunMRU key. It starts with a failed attempt to find the StartupFolder, followed by running 'rip.pl' to get IP addresses. Then, it navigates through the file system to find the NTUSER.DAT file. Finally, it uses 'rip.pl' again to extract the RunMRU key, displaying its contents.

```
Microsoft\Windows\CurrentVersion\StartupApproved\StartupFolder not found.
lgw0020@siftworkstation: ~/Desktop/3$ rip.pl -r system -p ips
Launching ips v.20200518
ips v.20200518
(System) Get IP Addresses and domains (DHCP,static)

IPAddress          Domain              Hint:
192.168.48.141      localdomain
lgw0020@siftworkstation: ~/Desktop/3$ ls
SAM SECURITY Users default software system txt
lgw0020@siftworkstation: ~/Desktop/3$ cd ~/Desktop/3/Users
lgw0020@siftworkstation: ~/Desktop/3/Users$ ls
Default auble
lgw0020@siftworkstation: ~/Desktop/3/Users$ cd ~/Desktop/3/Users/Default
lgw0020@siftworkstation: ~/Desktop/3/Users/Default$ rip.pl -r NTUSER.DAT -p runmru
Launching runmru v.20200525
runmru v.20200525
(NTUSER.DAT) Gets contents of user's RunMRU key

Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU not found.
lgw0020@siftworkstation: ~/Desktop/3/Users/Default$ cd ~/Desktop/3/Users/auble
lgw0020@siftworkstation: ~/Desktop/3/Users/auble$ ls
Crypto NTUSER.DAT Protect
lgw0020@siftworkstation: ~/Desktop/3/Users/auble$ 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 cnd\1
b "C:\Program Files\Windows Mail\wab.exe"\1
c "C:\Program Files\Internet explorer\iexplore.exe"\1
lgw0020@siftworkstation: ~/Desktop/3/Users/auble$
```