Studienprogramm Sachbearbeiter:in Digitale Forensik Praktikum Betriebssysteme Dozent: Leander Hossfeld hossfeld@hs-mittweida.de Stand: 20.04.2023



Betriebssysteme

Praktikum 5 (Teil 2)

In diesem Praktikum lernen Sie die Nutzung der LDAP Lightweight Services zum Einlesen einer AD Datenbank eines DC auf einem Client PC, kennen.

Vorbereitung

Nutzen Sie bitte für die Bearbeitung die bereitgestellte Windows VM:

<u>https://download.hs-</u>

mittweida.de/intranet/lehre/CB/Bodach/BKA%20Studiengang/Betriebssysteme/Praktikum%20Blockwochen/Wind ows/Windows10-Pwnd.ova

Zusätzlich finden Sie hier die für das Praktikum zu nutzende ISO-Datei **PRBlock2.iso**:

https://download.hs-

mittweida.de/intranet/lehre/CB/Bodach/BKA%20Studiengang/Betriebssysteme/Praktikum%20Blockwochen/Wind ows/PRBlock2.iso

Allgemeine Hinweise

Kopieren Sie bitte die **Windows10-BS-Pwnd.ova** Datei und die ISO Datei **PRBlock2.iso** auf ihre lokale Festplatte in ein separates Verzeichnis, auf das Sie Zugriff haben, bestenfalls Laufwerk D:.

Sachverhalt

Von einem Actice Directory Domain Controller Server sollen die Datenbank Eintragungen überprüft und der Nutzer mit der SID -1771 ermittelt werden.

Um was für einen Windows Server handelt es sich, von dem die lokalen Kopien der NTDS.dit Datenbank stammen?

Inhaltsverzeichnis

Vorb	ereitung	0
Allge	meine Hinweise	0
Sach	verhalt	0
1.	Aufgabenstellung vorbereiten	2
2.	Aufgabenstellung Durchführung	4
2.1	Datenbank Datei vorbereiten	4
2.2	Installation der LDAP-Tools von den Windows Features	4
2.3	Datenbank mit DSAMAIN als LDAP-Server verfügbar machen	5
2.4	Abruf via ADSI-Editor	7
2.5	Abruf via PowerShell Kommandos	7
2.6	Suchen Sie den Mitarbeiter mit der SID -1771 am Ende	9
2.7	Windows Server feststellen	10
2./	Windows Sciver resistenen	

1. Aufgabenstellung vorbereiten

Öffnen Sie Virtualbox.

Importieren Sie zuerst die OVA-Datei.

Wählen dann die VM Windows-10-BS-Pwnd aus. Gehen Sie auf **Ändern** (nicht Doppelklicken auf die VM, das würde diese Starten).



> Wählen Sie den Massenspeicher aus

😔 v	/indows10-Pwnd - Ein	stellungen		-		×	
	Allgemein	Massenspeicher					
	System	Massenspeicher	Attribute				
	Anzeige	🖕 Controller: SATA	Optisches Laufwerk:	SATA-Port 1		Q	
		🙆 Windows 10-Pwnd-disk002.v		Live-CD/DVD		Virtuelles optisches Medium auswählen/erzeugen	
	Massenspeicher	🦾 💽 leer	- e	<u>H</u> otplug-fähig		Abbild auswahlen	
•	Audio		Informationen			PR2.iso	
5	Netzwerk		Größe:			Windows 10_x64.iso	
	Serielle Schnittstellen		Ort:			😪 Entfernt das virtuelle Medium aus dem Laufwerk	
	USB		angeschossen an.				
	Gemeinsame Ordner						
:	Benutzerschnittstelle						
		💠 🔶 📑 🙀					
	Ungi	iltige Einstellungen erkannt 🗖	ОК	Abbrechen	Hilfe		



> Binden Sie bei der CD die heruntergeladene Abbilddatei PRBlock2.iso ein



2. Aufgabenstellung Durchführung

2.1 Datenbank Datei vorbereiten

Aufgabe soll es sein eine gesicherte Active Directory Datenbank von einem Domänen Controller auf einem Client PC einzulesen und Zugriff auf die Datenbank zu erhalten.

Die zu nutzende Datenbank ntds.dit befindet sich auf der CD im Verzeichnis ntds.

Bitte kopieren Sie diese Datenbank auf den Desktop von Nutzer 1.

2.2 Installation der LDAP-Tools von den Windows Features

Einstellungen	- 🗆 X
Startseite Einstellung suchen	Apps und Features Ruellen für das Abrufen von Apps auswählen
Apps	Wenn Sie ausschließlich Apps aus dem Microsoft Store installieren, tragen Sie zum Schutz Ihres Geräts bei.
IΞ Apps und Features	Überall \checkmark
I≕ Standard-Apps	Apps und Features
띠실 Offline-Karten	Optionale Features
Apps für Websites	Aliase für die App-Ausführung
□ Videowiedergabe	Sie können nach Laufwerken suchen, sortieren und filtern. Wenn Sie eine App deinstallieren oder verschieben möchten, wählen Sie sie aus
→ Autostart	der Liste aus. Diese Liste durchsuchen

Rufen Sie über Rechtsklick auf den Start Button Apps & Features auf.

Wählen Sie Optionale Features aus.

← Einstellungen		_		×
ଜ Optionale Features				
Windows Hello-Gesichtserkennung	95,8 MB			
Windows Media Player	77,9 MB			
Windows PowerShell Integrated Scrip	oting 6,82 MB			
envioliment	07.12.2019			
Windows-Fax und -Scan	17,8 MB			
🛟 WordPad	6,25 MB			
Verwandte Einstellungen Mehr Windows-Funktionen				
Re Hilfe anfordern				

Scrollen Sie nach unten, dort befindet sich der Punkt Mehr Windows-Funktionen.



Aktivieren Sie Active Directory Lightweight Directory Services.

Überprüfen Sie, ob die Anwendung dsamain.exe verfügbar ist. Öffnen Sie dazu mit Rechtsklick auf Start eine Windows PowerShell Admin Konsole und starten Sie dsamain.exe.



2.3 Datenbank mit DSAMAIN als LDAP-Server verfügbar machen

Nutzen Sie das PowerShell Administrator Fenster um die Datenbank als LDAP-Server zu starten:



Achten Sie darauf, dass die VM-Netzwerkzugriff aktiviert hat.



Bestätigen Sie die Firewall Ausnahme!

Der LDAP-Server ist jetzt unter 127.0.0.1:50005 erreichbar. Überprüfen Sie die Zugriffsmöglichkeit in einem zweiten PowerShell Fenster, **ohne das vorherige zu schließen**!

```
ldp.exe 127.0.0.1:50005
```



2.4 Abruf via ADSI-Editor

É	Ihor Start S	Windows	Varwaltungenrogra	mmo hat man	dia Möglichkait	don ADSI-Editor 71	ıöffnan
C		vvii100vv3	ver waltungsprogra	initie nat man	ule moglici keit	uen ADDI-Luitor Zt	i onnen.

📝 ADSI-Editor	3	- 🗆 X
Datei Aktion Ansicht ?		
Z ADSI-Editor		Aktionen
	Verbindungseinstellungen X	ADSI-Editor
	Name: Praktikum AD	Weitere Aktionen
	L Pfad: LDAP://127.0.0.1:50005/Standardmäßiger Namenskontext	
	L Verbindungspunkt	
	D Definierten Namen oder Namenskontext auswählen oder eingeben:	
	×	
	Bekannten Namenskontext auswählen:	
	Standardmäßiger Namenskontext	
	Computer	
	Domäne oder Server auswählen oder eingeben: (Server Domäne [:port])	
	127.0.0.1:50005 🗸	
	O Standard (Domäne oder Server, an der/dem Sie angemeldet sind)	
	SSL-basierte Verschlüsselung verwenden	
	Erweitert OK Abbrechen	

Wenn man sich hier mit dem Server über 127.0.0.1:50005 unter Computer verbindet kann man ebenfalls auf die Einstellungen zugreifen.

Datei Aktion Ansicht ?
Image: Second
CN=LostAndFound CN=Managed Service Accounts CN=MINDS Queter U=Tier 1
CN=Managed Service Accounts Attribut-Editor Sicherheit U=Tier 1
CN-NTDS Quistas
Attribute:
V CONTRACTOR OF
CN=ADOLFO_PATRICK Attribut Wert
> OU=AWS desktopProfile <nicht festgelegt=""></nicht>
OU=AZR destinationIndicator <nicht festgelegt=""></nicht>
CN=BART_POOLE displayName DARRYL_MATTHEWS
OU=BDE displayNamePrintable <nicht festgelegt=""></nicht>
CN=DARRYL_MATTHEWS distinguishedName CN=DARRYL_MATTHEWS,OU=People,DC
OU=Deprovisioned division <nicht festgelegt=""></nicht>
OU=ESM dSASignature <nicht festgelegt=""></nicht>
OU=FIN ds.CorePropagationU
OU=FSR dynamic_LDArServer <nicht resignergt=""></nicht>
CN=GEOFFREY_WYNN employeerD < rule issgeegt.>
CN=HAROLD_ALLEN extensionName (inclut festigled)
OU=HRE facsimileTelephoneN
OU=ITS <
OU=OGC
CN=PATRICIA_SHEPHERD Bearbeiten Filter
OU=SEC
CN=THEODORE_ENGLAND
OU=TST OK Abbrechen Übernehmen Hilfe
OU=Unassociated
CN-Program Data

2.5 Abruf via PowerShell Kommandos

Führen Sie jetzt den ersten Teil des PowerShell Skriptes für den Abruf der Domänen-Informationen aus

		4)
PS	C:\Users\Nutzer1>	ldp.exe 127.0.0.1:50005
PS	C:\Users\Nutzer1>	<pre>\$DN = ([adsi]"LDAP://localhost:50005").distinguishedName;</pre>
PS	C:\Users\Nutzer1>	<pre>\$DomainObj = New-Object System.DirectoryServices.DirectoryEntry("LDAP://localhost:50005/\$DN");</pre>
PS	C:\Users\Nutzer1>	<pre>\$objSearcher = New-Object System.DirectoryServices.DirectorySearcher -ArgumentList \$DomainObj;</pre>
PS	C:\Users\Nutzer1>	<pre>\$0bjSearcher.PageSize = \$PageSize; \$objSearcher.SizeLimit = 100000;</pre>
PS	C:\Users\Nutzer1>	<pre>\$0bjSearcher.Filter = '(objectCategory=user)'</pre>
PS	C:\Users\Nutzer1>	<pre>\$Users = \$ObjSearcher.FindAll();</pre>
PS	C:\Users\Nutzer1>	<pre>\$0bjSearcher.Filter = '(objectCategory=group)'</pre>
PS	C:\Users\Nutzer1>	<pre>\$Groups = \$ObjSearcher.FindAll();</pre>
PS	C:\Users\Nutzer1>	<pre>\$0bjSearcher.Filter = '(objectCategory=computers)'</pre>
PS	C:\Users\Nutzer1>	<pre>\$Computers = \$0bjSearcher.FindAll();</pre>
PS	C:\Users\Nutzer1>	<pre>\$0bjSearcher.dispose();</pre>
PS	C:\Users\Nutzer1>	

Jetzt kann man Skript basiert oder manuell darauf zugreifen:

Name	Value
distinguishedname	{CN=Gast, CN=Users, DC=testlab, DC=local}
countrycode	{0}
samaccountname	{Gast}
objectsid	
adspath	{LDAP://localnost:50005/CN=Gast,CN=Users,DC=testlab,DC=local}
samaccounttype	{805306368}
primarygroupid	{514}
cn	{Gast}
objectguid	{184 248 23 136 211 203 1/6 65 154 211 134 205 224 1/9 49 60}
objectcategory	{CN=Person, CN=Schema, CN=Configuration, DC=Testian, DC=Iocal}
description	{Vordefiniertes Konto fur Gastzugriff auf den Computer bzw. die Domane}
objectclass	{top, person, organizationalPerson, user}
codepage	
name	{Gast}
PS C:\Users\Nutzer1> \$Gro	ups.properties[0]
Name	Value
objectcategory	///
uspchanged	
distinguishedneme	(Horady) /CN-Administratoren CN-Ruiltin DC-testlab DC-local)
grouptype	
whencreated	[*2147403043] [42] 46 2020 11:46:401
samaccountname	
description	(Administratoren haben uneingeschränkten Vollzugriff auf den Computer hzw. die Domäne 3
instancetype	Aumanistratoren naben uneingesen ankten voirzagirri aur den compater bzw. die bomane.;
adenath	ut; //DAD://localbost:50005/CN=Administratoren_CN=Builtin_DC=testlab_DC=locall
samaccounttype	[204 7/ 10201050:00007 CN-Administrator engen-builten,be-cestub,be-10201] /53870013
objectsid	
whenchanged	{03 06 2022 08:21:413
objectguid	/3 106 19 04 03 207 85 78 153 216 25 23 174 138 64 218\
member	(STEETED STEED) STEETED STEED
cn	{Administratoren}
usnereated	(Administration chi) /81001
admincount	
iscriticalsystemobiect	{True}
objectclass	{tong group}
systemflags	{-1946157056}
	{03,06,2022,08:20:29,03,06,2022,08:20:27,03,06,2022,08:20:27,03,06,2022,08:20:26,}
dscorepropagationdata	
dscorepropagationdata	{Administratoren}



2.6 Suchen Sie den Mitarbeiter mit der SID -1771 am Ende

Der einfachste Weg ist die Anwendung ldp.exe. Diese verfügt über eine SID-Suchfunktion unter Hilfsprogramme. Was man dafür allerdings benötigt, ist die komplette SID. Hier bietet es sich an diese von einem der Accounts zu nehmen und die letzte SID-Kennung auszutauschen.



2.7 Windows Server feststellen

Für die Feststellung des Servers hilft uns auch die Anwendung ldp.exe weiter. Nach dem Verbinden werden diese Daten angezeigt.

🔐 Idap://Praktikum	1:50005/DC=testl	lab,DC=local	N	_		\times
Verbindung Durchs	uchen Ansicht	Optionen	Hilfsprogramme ?			
Verbindung Durchs	uchen Ansicht boal A e.com,DC=1 C=testlab,DC C=testlab,DC C=testlab,DC C=testlab,CC C=testlab,CC C=testlab,DC DORE_ATKII distlist1,OL ecurityPrinc Groups,DC= ture,DC=tes ture,DC=tes C=testlab,D Service Acc otas,DC=tes C=testlab,D	Optionen 03.00 NEW instance ¹ isCriticalS lastLogor lastLogor localPolic logonCou msDFSR- Globi msDS-Ge msDS-Su name: DC objectCal objectCal objectCal objectSid operating operating operating operating sAMAcc sAMAcc serverRe serverRe	Hilfsprogramme ? 2022 10:20:27 Mitteleuropäische Somm; 03.06.2022 10:20:26 Mitteleuropäische Somm; 0x1 = (1 SD), 0x1 = (NEW_SD), 0x1 = (NEW_SD); yei: 0x4 = (WRIE); yei: 0x4 = (WRIE); 27.06.2022 10:44:20 Mitteleuropäische Somm; Timestamp: 23.06.2022 18:44:20 Mitteleuropäische Somm; Flags: 0; ti 172; ComputerReferenceBL: CN=DC1,CN=Topology,CN=Domain System Volume,CN=DFSR- ISettings, CN=System,DC=testiab,DC=local; herationki: 4:40; Binary blob 8 bytess; popriedEncryptionTypes: 0x1C = (RC4_HMAC_MD5 AES128_CT5_HMAC_SHA1_96 AES256_1; gory: CN=Computer,CN=Schema,CN=Configuration,DC=testiab,DC=local; is (5): top; person; organizationalPerson; user; computer; D: e5513dee_2022_416_4880_53940b52897. System: Windows Server 2019 Standard; System: Windows Server 2019 Standard; System: Windows Server 2019 Standard; System: Windows Server 2019 ControlLERS); bet: 02.06.2022 13:50:44 Mitteleuropäische Somm; rences: CN=RD Set(CN=DC1,OU=Domain Controllers,DC=testiab,DC=local; untName: DC15; untName: DC15; untName: DC15; untName: DC15; untName: DC15; UntSides204/DC1 testiab,DC=local; LC1=C01,CN=Servers,CN=Default=First-Site-Name,CN=Sites,CN=Cnfiguration,DC=testiab,DC=local; untName: DC15; UntSides204/DC1 testiab,Iocal; Idap/DC1 testiab,Iocal; C1.testiab,Iocal/ForestDnsZones.testiab,Iocal; Idap/DC1 testiab,Iocal/DomainDnsZones.testiab,Iocal; C1.testiab,Iocal/ForestDnsZones.testiab,Iocal; Idap/DC1 testiab,Iocal/DomainDnsZones.testiab,Iocal; Idap/DC1 testiab,Iocal/DomainDnsZones.testiab,Iocal; Idap/DC1 testiab,Iocal/DomainDnsZones.testiab,Iocal/DomainDnsZones.testiab,Iocal/SorestDnsZones.testiab,Iocal; Idap/DC1 testiab,Iocal/DomainDnsZones.testiab,Iocal; Idap/DC1 testiab,Iocal/Doma	EW_SD), 0> CTS_HMAC_ tlab,DC=loca cal; TERMSR	x1 = (_SHA1_96 al; XV/DC1;);
CN=Program OU=Quaranti	Data,DC=te ne,DC=testli ↓	Rest	эмило плекаар лисар ракурст пекаар осал, GC/DC-1 restablic/carrestablio/Carrestablio/Carrestablio/Carrestablio (ctedKrbHost/DC1; RPC/9223eff7-0f11-4e11-83bb-ce8549ffb94b_msdcs.testlablioca); HOST/DC /DC1 restablioca/TEST1 AB: HOST/DC1 + BOST/DC1 testlablioca); HOST/DC1 testlablioca/Restablioca/	1/TESTLAB; local:	au.iocai;	
<	>	E351	1235-4B06-11D1-AB04-00C04FC2DCD2/9223eff7-0f11-4e11-83bb-ce8549ffb94b/testlab.local;	Jap/DC1/TES	TLAB;	~
Fertig					NUM	

Auch PowerShell kann uns diese Informationen liefern.

Name	Value
 ridsetreferences	 {(N=RID Set.CN=DC1.0U=Domain Controllers.DC=testlab.DC=local}
logoncount	{172}
codepage	(0)
objectcategory	{CN=Computer.CN=Schema.CN=Configuration.DC=testlab.DC=local}
msdfsr-computerreferencebl	<pre>{CN=DC1.CN=Topology.CN=Domain System Volume.CN=DFSR-GlobalSettings.CN=System.DC=testlab.DC=local}</pre>
iscriticalsvstemobiect	(Teas)
operatingsvstem	{Windows Server 2019 Standard}
usnchanged	18/1401
instancetype	4
name	{DC1}
badpasswordtime	(0)
pwdlastset	132986442446587104}
serviceprincipalname	<pre>{Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/DC1.testlab.local. ldap/DC1.testlab.local/ForestDnsZones.testlab</pre>
obiectclass	{top, person, organizationalPerson, user}
badpwdcount	{0}
samaccounttype	{805306369}
lastlogontimestamp	{133004762601526128}
usncreated	{12293}
msds-generationid	{54 145 198 1 83 51 22 94}
objectguid	{238 61 81 233 146 32 253 74 136 157 83 157 10 82 137 183}
localpolicyflags	(0)
whencreated	{02.06.2022 11:50:18}
adspath	{LDAP://localhost:50005/CN=DC1.0U=Domain Controllers.DC=testlab.DC=local}
useraccountcontrol	{532480}
cn	{DC1}
countrycode	{0}
primarveroupid	(516)
whenchanged	{23.06.2022 16:44:20}
operatingsystemversion	{10.0 (17763)}
dnshostname	{DC1.testlab.local}
dscorepropagationdata	{03.06.2022 08:20:29. 03.06.2022 08:20:27. 03.06.2022 08:20:27. 03.06.2022 08:20:26}
lastlogon	{133007930601526406}
distinguishedname	{CN=DC1.OU=Domain Controllers.DC=testlab.DC=local}
msds-supportedencryptiontypes	{28}
samaccountname	{DC1\$}
obiectsid	{1 5 0 0 0 0 5 21 0 0 207 193 126 18 129 212 50 55 186 108 112 232 232 3 0 0}
lastlogoff	{0}
serverreferencebl	{CN=DC1.CN=Servers.CN=Default-First-Site-Name.CN=Sites.CN=Configuration.DC=testlab.DC=local}
	(0)))))))))))))))))))))))))))))))))))))