

Дампим домен и смотрим артефакты / Хабр

habr.com/ru/articles/828292

artrone

July 11, 2024

114	3.971175006	192.168.1.3	192.168.1.1	LDAP	1177	searchRequest(18)	"CN=Schema,CN=Configuration,DC=test,DC=local" wholeSubtree
115	3.979010967	192.168.1.1	192.168.1.3	LDAP	18389	searchResEntry(18)	"CN=ms-DS-Computer-AuthN-Policy-BL,CN=Schema,CN=Configuration,DC=test,DC=local" wholeSubtree
116	3.979042734	192.168.1.3	192.168.1.1	TCP	66	40885 → 389 [ACK]	Seq=17563 Ack=582970 Win=988800 Len=0 TSval=348311
117	3.983193795	192.168.1.3	192.168.1.1	LDAP	1177	searchRequest(19)	"CN=Schema,CN=Configuration,DC=test,DC=local" wholeSubtree
118	3.989145201	192.168.1.1	192.168.1.3	LDAP	18823	searchResEntry(19)	"CN=Domain-Wide-Policy,CN=Schema,CN=Configuration,DC=test,DC=local" wholeSubtree
119	3.989181546	192.168.1.3	192.168.1.1	TCP	66	40885 → 389 [ACK]	Seq=18674 Ack=601727 Win=1026304 Len=0 TSval=348311
120	3.993552496	192.168.1.3	192.168.1.1	LDAP	1177	searchRequest(20)	"CN=Schema,CN=Configuration,DC=test,DC=local" wholeSubtree
121	3.997912933	192.168.1.1	192.168.1.3	LDAP	18071	searchResEntry(20)	"CN=ms-WMI-ChangeDate,CN=Schema,CN=Configuration,DC=test,DC=local" wholeSubtree
122	3.997942267	192.168.1.3	192.168.1.1	TCP	66	40885 → 389 [ACK]	Seq=19785 Ack=619732 Win=1062400 Len=0 TSval=348311
123	4.002591197	192.168.1.3	192.168.1.1	LDAP	1177	searchRequest(21)	"CN=Schema,CN=Configuration,DC=test,DC=local" wholeSubtree
124	4.005658451	192.168.1.1	192.168.1.3	LDAP	12175	searchResEntry(21)	"CN=msSFU-30-Netgroup-Host-At-Domain,CN=Schema,CN=Configuration,DC=test,DC=local" wholeSubtree
125	4.005691248	192.168.1.3	192.168.1.1	TCP	66	40885 → 389 [ACK]	Seq=20896 Ack=631841 Win=1086592 Len=0 TSval=348311
126	4.009266613	192.168.1.3	192.168.1.1	LDAP	206	searchRequest(22)	"DC=test,DC=local" wholeSubtree
127	4.012427510	192.168.1.1	192.168.1.3	LDAP	6614	searchResEntry(22)	"DC=test,DC=local" searchResRef(22) searchRequest(23)
128	4.012458388	192.168.1.3	192.168.1.1	TCP	66	40885 → 389 [ACK]	Seq=21036 Ack=638389 Win=1099648 Len=0 TSval=348311
129	4.014134042	192.168.1.3	192.168.1.1	LDAP	219	searchRequest(23)	"CN=Partitions,CN=Configuration,DC=test,DC=local" wholeSubtree
130	4.014953556	192.168.1.1	192.168.1.3	LDAP	246	searchResEntry(23)	"CN=TEST,CN=Partitions,CN=Configuration,DC=test,DC=local" wholeSubtree
131	4.016228439	192.168.1.3	192.168.1.1	LDAP	244	searchRequest(24)	"CN=Partitions,CN=Configuration,DC=test,DC=local" wholeSubtree
132	4.017175698	192.168.1.1	192.168.1.3	LDAP	1282	searchResEntry(24)	"CN=Enterprise Configuration,CN=Partitions,CN=Configuration,DC=test,DC=local" wholeSubtree
133	4.019139396	192.168.1.3	192.168.1.1	LDAP	671	searchRequest(25)	"DC=test,DC=local" wholeSubtree
134	4.023359076	192.168.1.1	192.168.1.3	LDAP	7309	searchResEntry(25)	"CN=DC_TEST,OU=Domain Controllers,DC=test,DC=local" wholeSubtree
135	4.023390715	192.168.1.3	192.168.1.1	TCP	66	40885 → 389 [ACK]	Seq=21972 Ack=647028 Win=1117056 Len=0 TSval=348311
137	4.070410506	192.168.1.3	192.168.1.1	LDAP	735	searchRequest(26)	"DC=test,DC=local" wholeSubtree
138	4.074128044	192.168.1.1	192.168.1.3	LDAP	19032	searchResEntry(26)	"CN=Администратор,CN=Users,DC=test,DC=local" searchRequest(27)
139	4.074162252	192.168.1.3	192.168.1.1	TCP	66	40885 → 389 [ACK]	Seq=22641 Ack=665994 Win=1154494 Len=0 TSval=348311
197	4.312648160	192.168.1.3	192.168.1.1	LDAP	335	searchRequest(34)	"DC=test,DC=local" wholeSubtree
199	4.321362648	192.168.1.1	192.168.1.3	LDAP	63778	searchResEntry(34)	"CN=Администраторы,CN=Builtin,DC=test,DC=local" searchRequest(35)
200	4.321403205	192.168.1.3	192.168.1.1	TCP	66	40885 → 389 [ACK]	Seq=22910 Ack=729706 Win=1282432 Len=0 TSval=348311
201	4.321551312	192.168.1.1	192.168.1.3	LDAP	29026	searchResEntry(34)	"CN=Администраторы домена,CN=Users,DC=test,DC=local" wholeSubtree
202	4.321551854	192.168.1.3	192.168.1.1	TCP	66	40885 → 389 [ACK]	Seq=22910 Ack=758666 Win=1320576 Len=0 TSval=348311
203	4.321585870	192.168.1.1	192.168.1.3	LDAP	21253	searchResEntry(34)	"CN=Контроллеры домена - только чтение,CN=Users,DC=test,DC=local" wholeSubtree
204	4.321724578	192.168.1.3	192.168.1.1	TCP	66	40885 → 389 [ACK]	Seq=22910 Ack=779853 Win=1303168 Len=0 TSval=348311
224	4.382520630	192.168.1.3	192.168.1.1	LDAP	278	searchRequest(44)	"DC=test,DC=local" wholeSubtree
225	4.385122802	192.168.1.1	192.168.1.3	LDAP	1396	searchResEntry(44)	"CN=DC_TEST,OU=Domain Controllers,DC=test,DC=local" wholeSubtree
226	4.424327992	192.168.1.3	192.168.1.1	TCP	66	40885 → 389 [ACK]	Seq=23122 Ack=781183 Win=1323520 Len=0 TSval=348311
228	4.502540867	192.168.1.3	192.168.1.1	LDAP	336	searchRequest(45)	"DC=test,DC=local" wholeSubtree
229	4.504418465	192.168.1.1	192.168.1.3	LDAP	4032	searchResEntry(45)	"CN=(31B2F340-016D-11D2-945F-00C04FB984F9),CN=Policy,DC=test,DC=local" wholeSubtree
230	4.504453762	192.168.1.3	192.168.1.1	TCP	66	40885 → 389 [ACK]	Seq=23392 Ack=785149 Win=1331456 Len=0 TSval=348311
231	4.543702584	192.168.1.3	192.168.1.1	LDAP	323	searchRequest(46)	"DC=test,DC=local" wholeSubtree
232	4.544877133	192.168.1.1	192.168.1.3	LDAP	6337	searchResEntry(46)	"OU=Domain Controllers,DC=test,DC=local" searchRequest(47)
233	4.544899512	192.168.1.3	192.168.1.1	TCP	66	40885 → 389 [ACK]	Seq=23649 Ack=791420 Win=1344000 Len=0 TSval=348311
241	4.588976984	192.168.1.3	192.168.1.1	LDAP	378	searchRequest(50)	"DC=test,DC=local" wholeSubtree
243	4.633355450	192.168.1.1	192.168.1.3	LDAP	63778	searchResEntry(50)	"CN=Users,DC=test,DC=local" searchResEntry(50)
244	4.633510345	192.168.1.1	192.168.1.3	LDAP	29026	searchResEntry(50)	"CN=10b3ad2a-6883-4fa7-90fc-6377cbddc1b26,CN=Operational,DC=test,DC=local" wholeSubtree
245	4.633568288	192.168.1.3	192.168.1.1	TCP	66	40885 → 389 [ACK]	Seq=23961 Ack=884092 Win=1320576 Len=0 TSval=348311
246	4.633607706	192.168.1.1	192.168.1.3	LDAP	29026	searchResEntry(50)	"CN=10b3ad2a-6883-4fa7-90fc-6377cbddc1b26,CN=Operational,DC=test,DC=local" wholeSubtree

🔥 Атака Domain Dump позволяет злоумышленнику сдампить домен для получения информации о пользователях и группах, а также для последующего построения пути компрометации домена.

Теория

**данная статья будет рассмотрена на примере утилиты bloodhound **

Стадии работы на примере **bloodhound**:

1. Аутентификация через указанный протокол
2. Сбор информации о количестве лесов, доменов и хостов
3. Сбор информации о пользователях, группах, политиках и т. д.
4. Попытки обращений к компьютерам домена
5. Проверка активных пользователей

Процесс удаленного дампа может быть осуществлен с помощью Kerberos или NTLM аутентификации. В случае, если был выбран Kerberos и произошла ошибка получения TGT, метод авторизации будет автоматически изменен на NTLM.

Трафик проведенной атаки выглядит следующим образом:

No.	Time	Source	Destination	Protocol	Length	Info
114	3.971175006	192.168.1.1	192.168.1.1	LDAP	1177	searchRequest(18) "CN=Schema,CN=Configuration,DC=test,DC=local" whole
115	3.979040967	192.168.1.1	192.168.1.1	LDAP	18389	searchResEntry(18) "CN=ms-DS-Computer-AuthN-Policy-BL,CN=Schema,CN=Co
116	3.979042734	192.168.1.1	192.168.1.1	TCP	66	40885 → 389 [ACK] Seq=17563 Ack=582970 Win=988800 Len=0 TSval=348319
117	3.983193795	192.168.1.1	192.168.1.1	LDAP	1177	searchRequest(19) "CN=Schema,CN=Configuration,DC=test,DC=local" whole
118	3.989145201	192.168.1.1	192.168.1.1	LDAP	18823	searchResEntry(19) "CN=Domain-Wide-Policy,CN=Schema,CN=Configuration,
119	3.989181546	192.168.1.1	192.168.1.1	TCP	66	40885 → 389 [ACK] Seq=18674 Ack=601727 Win=1026304 Len=0 TSval=348311
120	3.993562496	192.168.1.1	192.168.1.1	LDAP	1177	searchRequest(20) "CN=Schema,CN=Configuration,DC=test,DC=local" whole
121	3.997912933	192.168.1.1	192.168.1.1	LDAP	18071	searchResEntry(20) "CN=ms-WMI-ChangeDate,CN=Schema,CN=Configuration,DC=
122	3.997942267	192.168.1.1	192.168.1.1	TCP	66	40885 → 389 [ACK] Seq=19785 Ack=619732 Win=1062400 Len=0 TSval=348311
123	4.002591197	192.168.1.1	192.168.1.1	LDAP	1177	searchRequest(21) "CN=Schema,CN=Configuration,DC=test,DC=local" whole
124	4.005658451	192.168.1.1	192.168.1.1	LDAP	12175	searchResEntry(21) "CN=msSFU-30-Netgroup-Host-At-Domain,CN=Schema,CN=
125	4.005691248	192.168.1.1	192.168.1.1	TCP	66	40885 → 389 [ACK] Seq=20896 Ack=631841 Win=1086592 Len=0 TSval=348311
126	4.009266613	192.168.1.1	192.168.1.1	LDAP	206	searchRequest(22) "DC=test,DC=local" wholeSubtree
127	4.012427510	192.168.1.1	192.168.1.1	LDAP	6614	searchResEntry(22) "DC=test,DC=local" searchResRef(22) searchR
128	4.012458388	192.168.1.1	192.168.1.1	TCP	66	40885 → 389 [ACK] Seq=21036 Ack=638389 Win=1099648 Len=0 TSval=348311
129	4.014134042	192.168.1.1	192.168.1.1	LDAP	219	searchRequest(23) "CN=Partitions,CN=Configuration,DC=test,DC=local"
130	4.01953556	192.168.1.1	192.168.1.1	LDAP	246	searchResEntry(23) "CN=TEST,CN=Partitions,CN=Configuration,DC=test,D
131	4.016228439	192.168.1.1	192.168.1.1	LDAP	244	searchRequest(24) "CN=Partitions,CN=Configuration,DC=test,DC=local"
132	4.017175698	192.168.1.1	192.168.1.1	LDAP	1282	searchResEntry(24) "CN=Enterprise Configuration,CN=Partitions,CN=Conf
133	4.019139396	192.168.1.1	192.168.1.1	LDAP	671	searchRequest(25) "DC=test,DC=local" wholeSubtree
134	4.023359076	192.168.1.1	192.168.1.1	LDAP	7309	searchResEntry(25) "CN=DC_TEST,OU=Domain Controllers,DC=test,DC=loca
135	4.023390715	192.168.1.1	192.168.1.1	TCP	66	40885 → 389 [ACK] Seq=21972 Ack=647028 Win=1117056 Len=0 TSval=348311
137	4.070410506	192.168.1.1	192.168.1.1	LDAP	735	searchRequest(26) "DC=test,DC=local" wholeSubtree
138	4.074128044	192.168.1.1	192.168.1.1	LDAP	19032	searchResEntry(26) "CN=Администратор,CN=Users,DC=test,DC=local" s
139	4.074162252	192.168.1.1	192.168.1.1	TCP	66	40885 → 389 [ACK] Seq=22641 Ack=665994 Win=1154944 Len=0 TSval=348311
197	4.312648160	192.168.1.1	192.168.1.1	LDAP	335	searchRequest(34) "DC=test,DC=local" wholeSubtree
199	4.321362648	192.168.1.1	192.168.1.1	LDAP	63778	searchResEntry(34) "CN=Администраторы,CN=Builtin,DC=test,DC=local"
200	4.321403205	192.168.1.1	192.168.1.1	TCP	66	40885 → 389 [ACK] Seq=22910 Ack=729706 Win=1282432 Len=0 TSval=348311
201	4.321521312	192.168.1.1	192.168.1.1	LDAP	29026	searchResEntry(34) "CN=Администраторы домена,CN=Users,DC=test,DC=loca
202	4.321531854	192.168.1.1	192.168.1.1	TCP	66	40885 → 389 [ACK] Seq=22910 Ack=758666 Win=1320576 Len=0 TSval=348311
203	4.321585870	192.168.1.1	192.168.1.1	LDAP	21253	searchResEntry(34) "CN=Контроллеры домена - только чтение,CN=Users,D
204	4.321724578	192.168.1.1	192.168.1.1	TCP	66	40885 → 389 [ACK] Seq=22910 Ack=779853 Win=1303168 Len=0 TSval=348311
224	4.382520630	192.168.1.1	192.168.1.1	LDAP	278	searchRequest(44) "DC=test,DC=local" wholeSubtree
225	4.385122802	192.168.1.1	192.168.1.1	LDAP	1396	searchResEntry(44) "CN=DC_TEST,OU=Domain Controllers,DC=test,DC=loca
226	4.424327992	192.168.1.1	192.168.1.1	TCP	66	40885 → 389 [ACK] Seq=23122 Ack=781183 Win=1323520 Len=0 TSval=348311
228	4.502540867	192.168.1.1	192.168.1.1	LDAP	336	searchRequest(45) "DC=test,DC=local" wholeSubtree
229	4.504418465	192.168.1.1	192.168.1.1	LDAP	4032	searchResEntry(45) "CN=(31B2F340-816D-11D2-94F5-00C04FB984F9),CN=Pol-
230	4.504453762	192.168.1.1	192.168.1.1	TCP	66	40885 → 389 [ACK] Seq=23392 Ack=785149 Win=1331456 Len=0 TSval=348311
231	4.543702584	192.168.1.1	192.168.1.1	LDAP	323	searchRequest(46) "DC=test,DC=local" wholeSubtree
232	4.544877133	192.168.1.1	192.168.1.1	LDAP	6337	searchResEntry(46) "OU=Domain Controllers,DC=test,DC=local" searcl
233	4.544899512	192.168.1.1	192.168.1.1	TCP	66	40885 → 389 [ACK] Seq=23649 Ack=791420 Win=1344000 Len=0 TSval=348311
241	4.588976984	192.168.1.1	192.168.1.1	LDAP	378	searchRequest(50) "DC=test,DC=local" wholeSubtree
243	4.633355450	192.168.1.1	192.168.1.1	LDAP	63778	searchResEntry(50) "CN=Users,DC=test,DC=local" searchResEntry(50)
244	4.633510345	192.168.1.1	192.168.1.1	LDAP	29026	searchResEntry(50) "CN=10b3ad2a-6883-4fa7-90fc-6377cbdc1b26,CN=Operat
245	4.633568288	192.168.1.1	192.168.1.1	TCP	66	40885 → 389 [ACK] Seq=23961 Ack=884092 Win=1320576 Len=0 TSval=348311
246	4.633610726	192.168.1.1	192.168.1.1	LDAP	2400	searchResEntry(50) "CN=10b3ad2a-6883-4fa7-90fc-6377cbdc1b26,CN=Operat

No.	Time	Source	Destination	Protocol	Length	Info
134	4.023359076	192.168.1.1	192.168.1.1	LDAP	7309	searchResEntry(25) "CN=DC_TEST,OU=Domain Controllers,DC=test,DC=loca
135	4.023390715	192.168.1.1	192.168.1.1	TCP	66	40885 → 389 [ACK] Seq=21972 Ack=647028 Win=1117056 Len=0 TSval=348311
137	4.070410506	192.168.1.1	192.168.1.1	LDAP	735	searchRequest(26) "DC=test,DC=local" wholeSubtree
138	4.074128044	192.168.1.1	192.168.1.1	LDAP	19032	searchResEntry(26) "CN=Администратор,CN=Users,DC=test,DC=local" s
139	4.074162252	192.168.1.1	192.168.1.1	TCP	66	40885 → 389 [ACK] Seq=22641 Ack=665994 Win=1154944 Len=0 TSval=348311
<p>Frame 138: 19032 bytes on wire (152256 bits), 19032 bytes captured (152256 bits) on interface eth0, id 0</p> <p>Ethernet II, Src: 08:00:27:bf:6f:d2 (08:00:27:bf:6f:d2), Dst: 08:00:27:41:84:96 (08:00:27:41:84:96)</p> <p>Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.3</p> <p>Transmission Control Protocol, Src Port: 389, Dst Port: 40885, Seq: 647028, Ack: 22641, Len: 18966</p> <p>Lightweight Directory Access Protocol</p> <p>LDAPMessage searchResEntry(26) "CN=Администратор,CN=Users,DC=test,DC=local" [1968 results]</p> <p>messageID: 26</p> <p>protocolOp: searchResEntry (4)</p> <p>searchResEntry</p> <p>objectName: CN=Администратор,CN=Users,DC=test,DC=local</p> <p>attributes: 14 items</p> <ul style="list-style-type: none"> PartialAttributeList item objectClass PartialAttributeList item description PartialAttributeList item distinguishedName PartialAttributeList item whenCreated PartialAttributeList item nTSecurityDescriptor PartialAttributeList item userAccountControl PartialAttributeList item lastLogon PartialAttributeList item pwdLastSet PartialAttributeList item primaryGroupID PartialAttributeList item objectSid PartialAttributeList item adminCount PartialAttributeList item sAMAccountName PartialAttributeList item sAMAccountType PartialAttributeList item lastLogonTimestamp <p>[Response To: 137]</p> <p>[Time: 0.003717538 seconds]</p> <p>Lightweight Directory Access Protocol</p> <p>Lightweight Directory Access Protocol</p> <p>Lightweight Directory Access Protocol</p> <p>Lightweight Directory Access Protocol</p> <p>Lightweight Directory Access Protocol</p> <p>Lightweight Directory Access Protocol</p> <p>Lightweight Directory Access Protocol</p> <p>Lightweight Directory Access Protocol</p> <p>Lightweight Directory Access Protocol</p> <p>LDAPMessage searchResRef(19)</p> <p>messageID: 26</p> <p>protocolOp: searchResRef (19)</p> <p>searchResRef: 1 item</p> <p>[Response To: 137]</p> <p>[Time: 0.003717538 seconds]</p> <p>Lightweight Directory Access Protocol</p> <p>LDAPMessage searchResRef(26)</p> <p>messageID: 26</p> <p>protocolOp: searchResRef (19)</p> <p>searchResRef: 1 item</p>						

```

> Frame 138: 19032 bytes on wire (152256 bits), 19032 bytes captured (152256 bits) on interface eth0, id 0
> Ethernet II, Src: 08:00:27:bf:6f:d2 (08:00:27:bf:6f:d2), Dst: 08:00:27:41:84:96 (08:00:27:41:84:96)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.3
> Transmission Control Protocol, Src Port: 389, Dst Port: 40885, Seq: 647028, Ack: 22641, Len: 18966
> Lightweight Directory Access Protocol
  > LDAPMessage searchResEntry(26) "CN=Администратор,CN=Users,DC=test,DC=local" [1968 results]
    messageID: 26
    > protocolOp: searchResEntry (4)
      > searchResEntry
        objectName: CN=Администратор,CN=Users,DC=test,DC=local
        > attributes: 14 items
          > PartialAttributeList item objectClass
            type: objectClass
            > vals: 4 items
              AttributeValue: top
              AttributeValue: person
              AttributeValue: organizationalPerson
              AttributeValue: user
          > PartialAttributeList item description
            type: description
            > vals: 1 item
              AttributeValue: d092d18d182d180d0bed0b5d0bdd0b0d18f20d183d187d0b5d182d0bed0b0d18f20...
          > PartialAttributeList item distinguishedName
            type: distinguishedName
            > vals: 1 item
              AttributeValue: 434e3dd090d0b4d0bcd0b8d0bdd0b8d181d182d180d0b0d182d0bed1802c434e3d557365...
          > PartialAttributeList item whenCreated
            type: whenCreated
            > vals: 1 item
              AttributeValue: 20240627141856.0Z
          > PartialAttributeList item nTSecurityDescriptor
            type: nTSecurityDescriptor
            > vals: 1 item
              > NT Security Descriptor
                Revision: 1
                > Type: 0x9c04, Self Relative, DACL Protected, SACL Auto Inherited, DACL Auto Inherited, DACL Present
                Offset to owner SID: 1160
                Offset to group SID: 0
                Offset to SACL: 0
                Offset to DACL: 20
                > Owner: S-1-5-21-3271603407-350436319-1246551825-512 (Domain SID-Domain Admins)
                > NT User (DACL) ACL
          > PartialAttributeList item userAccountControl
            type: userAccountControl
            > vals: 1 item
              AttributeValue: 512

```

Таким образом, от сервера нам прилетает вся информация, в данном случае, о пользователе «Администратор», которая представлена в виде обычного текста и HEX формата.

Практика

Дамп через Kerberos аутентификацию

```
python bloodhound.py -u ldapdump-user -p Bloodhound? -ns 192.168.1.1 -d test.local -c ALL --zip --auth-method kerberos -k
```

```

(root@kali)-[~/BloodHound.py]
# python bloodhound.py -u ldapdump-user -p Bloodhound? -ns 192.168.1.1 -d test.local -c ALL --zip --auth-method kerberos -k
INFO: Found AD domain: test.local
INFO: Getting TGT for user
INFO: Connecting to LDAP server: DC_TEST.test.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 2 computers
INFO: Connecting to LDAP server: DC_TEST.test.local
INFO: Found 9 users
INFO: Found 55 groups
INFO: Found 3 gpos
INFO: Found 3 ous
INFO: Found 22 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: PC1.test.local
INFO: Querying computer: DC_TEST.test.local
INFO: User Администратор is logged in on DC_TEST.test.local from fe80::6d42:a03:9f11:169e
INFO: Done in 00M 04S
INFO: Compressing output into 20240707011718_bloodhound.zip

```

Как видно, 2 строка вывода программы проинформировала нас о получении TGT, что свидетельствует о том, что аутентификация через Kerberos была успешно выполнена.

Трафик атаки

Как обычно, начинаем с Kerberos аутентификации. Поскольку дальше идет работа с LDAP, то и в TGS_REQ SNameString будет содержать ldap

13	0.008513134	192.168.1.3	192.168.1.1	TCP	66 56504 → 88 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3493419065 TSecr=
14	0.008644642	192.168.1.3	192.168.1.1	KRB5	252 AS-REQ
15	0.009862435	192.168.1.1	192.168.1.3	KRB5	1569 AS-REP
16	0.009890613	192.168.1.3	192.168.1.1	TCP	66 56504 → 88 [ACK] Seq=187 Ack=1504 Win=31872 Len=0 TSval=3493419067 TS
17	0.010597905	192.168.1.3	192.168.1.1	TCP	66 56504 → 88 [FIN, ACK] Seq=187 Ack=1504 Win=31872 Len=0 TSval=34934190
18	0.011155054	192.168.1.1	192.168.1.3	TCP	66 88 → 56504 [ACK] Seq=1504 Ack=188 Win=532736 Len=0 TSval=2601006 TSec
19	0.011155182	192.168.1.1	192.168.1.3	TCP	60 88 → 56504 [RST, ACK] Seq=1504 Ack=188 Win=0 Len=0
20	0.175337001	192.168.1.3	192.168.1.1	DNS	78 Standard query 0x50f6 A DC.TEST.test.local
21	0.176124896	192.168.1.1	192.168.1.3	DNS	94 Standard query response 0x50f6 A DC.TEST.test.local A 192.168.1.1
22	0.178750461	192.168.1.3	192.168.1.1	DNS	78 Standard query 0xb85c A DC.TEST.test.local
23	0.179031341	192.168.1.3	192.168.1.1	DNS	78 Standard query 0x2c53 AAAA DC.TEST.test.local
24	0.179525448	192.168.1.1	192.168.1.3	DNS	94 Standard query response 0xb85c A DC.TEST.test.local A 192.168.1.1
25	0.180989301	192.168.1.1	192.168.1.3	DNS	125 Standard query response 0x2c53 AAAA DC.TEST.test.local SOA DC.TEST.t
26	0.181282100	192.168.1.3	192.168.1.1	TCP	74 56508 → 88 [SYN] Seq=0 Win=32128 Len=0 MSS=1460 SACK_PERM TSval=3493
27	0.181932897	192.168.1.1	192.168.1.3	TCP	74 88 → 56508 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK
28	0.181950918	192.168.1.3	192.168.1.1	TCP	66 56508 → 88 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3493419239 TSecr=
29	0.182073124	192.168.1.3	192.168.1.1	KRB5	1461 TGS-REQ
30	0.183356782	192.168.1.1	192.168.1.3	KRB5	1534 TGS-REP
31	0.183371705	192.168.1.3	192.168.1.1	TCP	66 56508 → 88 [ACK] Seq=1396 Ack=1469 Win=31872 Len=0 TSval=3493419240
32	0.183766908	192.168.1.3	192.168.1.1	TCP	66 56508 → 88 [FIN, ACK] Seq=1396 Ack=1469 Win=31872 Len=0 TSval=349341
33	0.184313152	192.168.1.1	192.168.1.3	TCP	66 88 → 56508 [ACK] Seq=1469 Ack=1397 Win=66560 Len=0 TSval=2601180 TSec
34	0.184313323	192.168.1.1	192.168.1.3	TCP	60 88 → 56508 [RST, ACK] Seq=1469 Ack=1397 Win=0 Len=0
35	0.189111117	192.168.1.3	192.168.1.1	TCP	74 59381 → 389 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3493
36	0.189727847	192.168.1.1	192.168.1.3	TCP	74 389 → 59381 [SYN, ACK] Seq=1 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SA
37	0.189750022	192.168.1.3	192.168.1.1	TCP	66 59381 → 389 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3493419247 TSecr=
38	0.190168215	192.168.1.3	192.168.1.1	LDAP	1406 bindRequest(1) "<ROOT>" sasl
39	0.191956872	192.168.1.1	192.168.1.3	LDAP	132 bindResponse(1) success [BoundErrorUnreassembled Packet]
40	0.191975801	192.168.1.3	192.168.1.1	TCP	66 59381 → 389 [ACK] Seq=1341 Ack=67 Win=32128 Len=0 TSval=3493419249 TS
41	0.193592809	192.168.1.3	192.168.1.1	LDAP	317 searchRequest(2) "<ROOT>" baseObject
42	0.194436850	192.168.1.1	192.168.1.3	TCP	3149 searchResEntry(2) "<ROOT>" searchResDone(2) success [1967 result
43	0.194525307	192.168.1.3	192.168.1.1	TCP	66 59381 → 389 [ACK] Seq=1592 Ack=3141 Win=31872 Len=0 TSval=3493419251
44	0.195757180	192.168.1.3	192.168.1.1	LDAP	343 searchRequest(3) "CN=Aggregate,CN=Schema,CN=Configuration,DC=test,DC=
45	0.198588278	192.168.1.1	192.168.1.3	TCP	17442 389 → 59381 [ACK] Seq=3141 Ack=1869 Win=66048 Len=17376 TSval=2601189
46	0.198620289	192.168.1.3	192.168.1.1	TCP	66 59381 → 389 [ACK] Seq=1869 Ack=20517 Win=31872 Len=0 TSval=3493419250
47	0.199306255	192.168.1.3	192.168.1.1	TCP	23234 389 → 59381 [ACK] Seq=20517 Ack=1869 Win=66048 Len=23168 TSval=260118
48	0.199320861	192.168.1.3	192.168.1.1	TCP	66 59381 → 389 [ACK] Seq=1869 Ack=43685 Win=31872 Len=0 TSval=3493419250
49	0.199934588	192.168.1.1	192.168.1.3	TCP	29026 389 → 59381 [ACK] Seq=43685 Ack=1869 Win=66048 Len=28900 TSval=260118
50	0.199949030	192.168.1.3	192.168.1.1	TCP	66 59381 → 389 [ACK] Seq=1869 Ack=72645 Win=31872 Len=0 TSval=349341925
51	0.200689085	192.168.1.1	192.168.1.3	TCP	31922 389 → 59381 [ACK] Seq=72645 Ack=1869 Win=66048 Len=31856 TSval=260118
52	0.200703278	192.168.1.3	192.168.1.1	TCP	66 59381 → 389 [ACK] Seq=1869 Ack=104501 Win=95616 Len=0 TSval=34934192
53	0.201393023	192.168.1.1	192.168.1.3	TCP	37714 389 → 59381 [ACK] Seq=104501 Ack=1869 Win=66048 Len=37648 TSval=2601
54	0.201407653	192.168.1.3	192.168.1.1	TCP	66 59381 → 389 [ACK] Seq=1869 Ack=142149 Win=170880 Len=0 TSval=3493419
55	0.201824361	192.168.1.1	192.168.1.3	TCP	18890 389 → 59381 [ACK] Seq=142149 Ack=1869 Win=66048 Len=18824 TSval=2601
56	0.201833720	192.168.1.3	192.168.1.1	TCP	66 59381 → 389 [ACK] Seq=1869 Ack=160973 Win=208512 Len=0 TSval=3493419
57	0.202528925	192.168.1.1	192.168.1.3	TCP	24682 389 → 59381 [ACK] Seq=160973 Ack=1869 Win=66048 Len=24616 TSval=2601
58	0.202542662	192.168.1.3	192.168.1.1	TCP	66 59381 → 389 [ACK] Seq=1869 Ack=185589 Win=257792 Len=0 TSval=3493419
59	0.202655944	192.168.1.1	192.168.1.3	TCP	24682 389 → 59381 [ACK] Seq=185589 Ack=1869 Win=66048 Len=24616 TSval=2601
60	0.202666381	192.168.1.3	192.168.1.1	TCP	66 59381 → 389 [ACK] Seq=1869 Ack=210205 Win=307072 Len=0 TSval=3493419
61	0.203128214	192.168.1.1	192.168.1.3	TCP	60882 389 → 59381 [ACK] Seq=210205 Ack=1869 Win=66048 Len=60816 TSval=2601
62	0.203145453	192.168.1.3	192.168.1.1	TCP	66 59381 → 389 [ACK] Seq=1869 Ack=271021 Win=391680 Len=0 TSval=3493419
63	0.203717475	192.168.1.1	192.168.1.3	LDAP	38010 searchResEntry(3) "CN=Aggregate,CN=Schema,CN=Configuration,DC=test,DC=

▼ Kerberos
▶ Record Mark: 1391 bytes
▼ tgs-req
pvno: 5
msg-type: krb-tgs-req (12)
padata: 1 item
▼ PA-DATA pA-TGS-REQ
▼ padata-type: pA-TGS-REQ (1)
▶ padata-value: 6e8204d3308204cfa003020105a10302010ea2070305000000000a38204426182043e30...
▼ req-body
Padding: 0
▶ kdc-options: 40810010
realm: TEST.LOCAL
▼ sname
name-type: KRB5-NT-SRV-INST (2)
▼ sname-string: 2 items
SNameString: ldap
SNameString: DC.TEST.test.local
till: Jul 13, 2024 00:52:52.000000000 +10

После этого, идет аналогичный запрос TGS_REQ, но уже для обращения к SMB — SNameString: cifs

317	0.966957238	192.168.1.3	192.168.1.1	TCP	66 56524 → 88 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3493420024 TSecr=
318	0.967328126	192.168.1.3	192.168.1.1	KRB5	1461 TGS-REQ
319	0.968884624	192.168.1.1	192.168.1.3	KRB5	1534 TGS-REP
320	0.968831445	192.168.1.3	192.168.1.1	TCP	66 56524 → 88 [ACK] Seq=1396 Ack=1469 Win=31872 Len=0 TSval=3493420026
321	0.969899567	192.168.1.3	192.168.1.1	TCP	66 56524 → 88 [FIN, ACK] Seq=1396 Ack=1469 Win=31872 Len=0 TSval=349342
322	0.970464905	192.168.1.1	192.168.1.3	TCP	66 88 → 56524 [ACK] Seq=1469 Ack=1397 Win=532736 Len=0 TSval=2601966 TS
323	0.970465032	192.168.1.1	192.168.1.3	TCP	60 88 → 56524 [RST, ACK] Seq=1469 Ack=1397 Win=0 Len=0
324	0.972690790	192.168.1.3	192.168.1.1	TCP	74 33874 → 445 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=349
325	0.973326442	192.168.1.1	192.168.1.3	TCP	74 445 → 33874 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SA
326	0.973453530	192.168.1.3	192.168.1.1	TCP	66 33874 → 445 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3493420030 TSecr
327	0.974649692	192.168.1.3	192.168.1.1	SMB	139 Negotiate Protocol Request
328	0.975659597	192.168.1.1	192.168.1.3	SMB2	318 Negotiate Protocol Response
329	0.975730617	192.168.1.3	192.168.1.1	TCP	66 33874 → 445 [ACK] Seq=74 Ack=253 Win=32000 Len=0 TSval=3493420033 TS
330	0.981696916	192.168.1.3	192.168.1.1	SMB2	176 Negotiate Protocol Request
331	0.982763775	192.168.1.1	192.168.1.3	SMB2	318 Negotiate Protocol Response
332	0.986071826	192.168.1.3	192.168.1.1	SMB2	1482 Session Setup Request
333	0.987564821	192.168.1.1	192.168.1.3	SMB2	164 Session Setup Response
334	0.989851882	192.168.1.3	192.168.1.1	SMB2	230 Encrypted SMB3
335	0.990556580	192.168.1.1	192.168.1.3	SMB2	202 Encrypted SMB3
336	0.991916192	192.168.1.3	192.168.1.1	SMB2	254 Encrypted SMB3
337	0.992719725	192.168.1.1	192.168.1.3	SMB2	274 Encrypted SMB3
338	0.995136484	192.168.1.3	192.168.1.1	SMB2	306 Encrypted SMB3
339	0.995934566	192.168.1.1	192.168.1.3	SMB2	202 Encrypted SMB3
340	0.996652848	192.168.1.3	192.168.1.1	TCP	66 46629 → 389 [ACK] Seq=14574 Ack=341840 Win=205312 Len=0 TSval=349342
341	0.996921595	192.168.1.3	192.168.1.1	TCP	66 59381 → 389 [ACK] Seq=24153 Ack=1018185 Win=489472 Len=0 TSval=34934
342	0.998018509	192.168.1.3	192.168.1.1	SMB2	235 Encrypted SMB3
343	0.998884051	192.168.1.1	192.168.1.3	SMB2	270 Encrypted SMB3
344	1.001955656	192.168.1.3	192.168.1.1	SMB2	318 Encrypted SMB3
345	1.002710897	192.168.1.1	192.168.1.3	SMB2	202 Encrypted SMB3
346	1.003952295	192.168.1.3	192.168.1.1	SMB2	235 Encrypted SMB3
347	1.004794453	192.168.1.1	192.168.1.3	SMB2	362 Encrypted SMB3
348	1.007709066	192.168.1.3	192.168.1.1	SMB2	190 Encrypted SMB3
349	1.009092046	192.168.1.1	192.168.1.3	SMB2	190 Encrypted SMB3
350	1.010726570	192.168.1.3	192.168.1.1	SMB2	230 Encrypted SMB3
351	1.011528358	192.168.1.1	192.168.1.3	SMB2	202 Encrypted SMB3
352	1.013136544	192.168.1.3	192.168.1.1	SMB2	250 Encrypted SMB3
353	1.013866140	192.168.1.1	192.168.1.3	SMB2	274 Encrypted SMB3
354	1.015476233	192.168.1.3	192.168.1.1	SMB2	306 Encrypted SMB3
355	1.016282365	192.168.1.1	192.168.1.3	SMB2	202 Encrypted SMB3
356	1.017647037	192.168.1.3	192.168.1.1	SMB2	235 Encrypted SMB3
357	1.018308924	192.168.1.1	192.168.1.3	SMB2	270 Encrypted SMB3
358	1.021182915	192.168.1.3	192.168.1.1	SMB2	270 Encrypted SMB3
359	1.022181648	192.168.1.1	192.168.1.3	SMB2	202 Encrypted SMB3
360	1.023373287	192.168.1.3	192.168.1.1	SMB2	235 Encrypted SMB3
361	1.024102191	192.168.1.1	192.168.1.3	SMB2	250 Encrypted SMB3
362	1.026315182	192.168.1.3	192.168.1.1	SMB2	312 Encrypted SMB3
363	1.027181629	192.168.1.1	192.168.1.3	SMB2	202 Encrypted SMB3
364	1.028288225	192.168.1.3	192.168.1.1	SMB2	235 Encrypted SMB3

```

Kerberos
  Record Mark: 1391 bytes
  tgs-req
    pvno: 5
    msg-type: krb-tgs-req (12)
    padata: 1 item
      PA-DATA pA-TGS-REQ
        padata-type: pA-TGS-REQ (1)
          padata-value: 6e8204d3308204cfa003020105a10302010ea20703050000000000a38204426182043e30...
    req-body
      Padding: 0
      kdc-options: 40810010
      realm: TEST.LOCAL
      sname
        name-type: KRB5-NT-SRV-INST (2)
        sname-string: 2 items
          SNameString: cifs
          SNameString: DC_TEST.test.local

```

Дамп через NTLM аутентификацию

```
python bloodhound.py -u ldapdump-user -p Bloodhound? -ns 192.168.1.1 -d test.local -c ALL --zip --auth-method ntlm
```

```

(root@kali)-[~/BloodHound.py]
# python bloodhound.py -u ldapdump-user -p Bloodhound? -ns 192.168.1.1 -d test.local -c ALL
--zip --auth-method ntlm
INFO: Found AD domain: test.local
INFO: Connecting to LDAP server: DC_TEST.test.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 2 computers
INFO: Connecting to LDAP server: DC_TEST.test.local
INFO: Found 9 users
INFO: Found 55 groups
INFO: Found 3 gpos
INFO: Found 3 ous
INFO: Found 22 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: PC1.test.local
INFO: Querying computer: DC_TEST.test.local
INFO: User Администратор is logged in on DC_TEST.test.local from fe80::6d42:a03:9f11:169e
INFO: Done in 00M 04S
INFO: Compressing output into 20240707012439_bloodhound.zip

```

Трафик атаки

Сначала идет NTLM аутентификация, сразу после которой идут LDAP запросы.

13	0.009205556	192.168.1.1	192.168.1.3	LDAP	92 bindResponse(1) success
14	0.009280668	192.168.1.3	192.168.1.1	TCP	66 35867 → 389 [ACK] Seq=15 Ack=27 Win=32128 Len=0 TSval=3493044578 TSecr=3493044583
15	0.009764598	192.168.1.3	192.168.1.1	LDAP	116 bindRequest(2) "NTLM", NTLMSSP_NEGOTIATE
16	0.010499255	192.168.1.1	192.168.1.3	LDAP	288 bindResponse(2) success, NTLMSSP_CHALLENGE
17	0.011167183	192.168.1.3	192.168.1.1	LDAP	410 bindRequest(3) "<ROOT>", NTLMSSP_AUTH, User: test.local\ldapdump-user
18	0.012789213	192.168.1.1	192.168.1.3	LDAP	88 bindResponse(3) success
19	0.013687213	192.168.1.3	192.168.1.1	LDAP	317 searchRequest(4) "<ROOT>" baseObject
20	0.014437538	192.168.1.1	192.168.1.3	LDAP	3140 searchResEntry(4) "<ROOT>" searchResDone(4) success [1967 results]
21	0.014519998	192.168.1.3	192.168.1.1	TCP	66 35867 → 389 [ACK] Seq=660 Ack=3345 Win=31872 Len=0 TSval=3493044583 TSecr=3493044588
22	0.015650049	192.168.1.3	192.168.1.1	LDAP	343 searchRequest(5) "CN=Aggregate,CN=Schema,CN=Configuration,DC=test,DC=local"
23	0.018574292	192.168.1.3	192.168.1.1	TCP	17442 389 → 35867 [ACK] Seq=3345 Ack=937 Win=531968 Len=17376 TSval=2226334 TSecr=3493044588
24	0.018601950	192.168.1.3	192.168.1.1	TCP	66 35867 → 389 [ACK] Seq=937 Ack=20721 Win=31872 Len=0 TSval=3493044587 TSecr=3493044588
25	0.019171537	192.168.1.3	192.168.1.1	TCP	23234 389 → 35867 [ACK] Seq=20721 Ack=937 Win=531968 Len=23168 TSval=2226334 TSecr=3493044588
26	0.019182173	192.168.1.3	192.168.1.1	TCP	66 35867 → 389 [ACK] Seq=937 Ack=43889 Win=31872 Len=0 TSval=3493044588 TSecr=3493044588
27	0.019798825	192.168.1.1	192.168.1.3	TCP	29026 389 → 35867 [ACK] Seq=43889 Ack=937 Win=531968 Len=28960 TSval=2226334 TSecr=3493044588
28	0.019815467	192.168.1.3	192.168.1.1	TCP	66 35867 → 389 [ACK] Seq=937 Ack=72849 Win=31872 Len=0 TSval=3493044588 TSecr=3493044588
29	0.020539046	192.168.1.1	192.168.1.3	TCP	31922 389 → 35867 [ACK] Seq=72849 Ack=937 Win=531968 Len=31856 TSval=2226334 TSecr=3493044588
30	0.020555327	192.168.1.3	192.168.1.1	TCP	66 35867 → 389 [ACK] Seq=937 Ack=104705 Win=95616 Len=0 TSval=3493044588 TSecr=3493044588
31	0.021198914	192.168.1.1	192.168.1.3	TCP	37714 389 → 35867 [ACK] Seq=104705 Ack=937 Win=531968 Len=37648 TSval=2226334 TSecr=3493044588
32	0.021216483	192.168.1.3	192.168.1.1	TCP	66 35867 → 389 [ACK] Seq=937 Ack=142353 Win=170880 Len=0 TSval=3493044588 TSecr=3493044588
33	0.021922624	192.168.1.1	192.168.1.3	TCP	43596 389 → 35867 [ACK] Seq=142353 Ack=937 Win=531968 Len=43440 TSval=2226334 TSecr=3493044588
34	0.021939284	192.168.1.3	192.168.1.1	TCP	66 35867 → 389 [ACK] Seq=937 Ack=185793 Win=257792 Len=0 TSval=3493044588 TSecr=3493044588
35	0.022649661	192.168.1.1	192.168.1.3	TCP	49298 389 → 35867 [ACK] Seq=185793 Ack=937 Win=531968 Len=49232 TSval=2226334 TSecr=3493044588
36	0.022663531	192.168.1.3	192.168.1.1	TCP	66 35867 → 389 [ACK] Seq=937 Ack=235025 Win=356224 Len=0 TSval=3493044588 TSecr=3493044588
37	0.023431920	192.168.1.1	192.168.1.3	TCP	55090 389 → 35867 [ACK] Seq=235025 Ack=937 Win=531968 Len=55024 TSval=2226334 TSecr=3493044588
38	0.023499332	192.168.1.3	192.168.1.1	TCP	66 35867 → 389 [ACK] Seq=937 Ack=290049 Win=466304 Len=0 TSval=3493044588 TSecr=3493044588
39	0.023842614	192.168.1.1	192.168.1.3	TCP	11650 389 → 35867 [ACK] Seq=290049 Ack=937 Win=531968 Len=11584 TSval=2226334 TSecr=3493044588
40	0.023852911	192.168.1.3	192.168.1.1	TCP	66 35867 → 389 [ACK] Seq=937 Ack=301633 Win=489472 Len=0 TSval=3493044588 TSecr=3493044588
41	0.024881408	192.168.1.1	192.168.1.3	LDAP	7602 searchResEntry(5) "CN=Aggregate,CN=Schema,CN=Configuration,DC=test,DC=local"
42	0.024959818	192.168.1.3	192.168.1.1	TCP	66 35867 → 389 [ACK] Seq=937 Ack=309169 Win=504576 Len=0 TSval=3493044588 TSecr=3493044588
43	0.024971262	192.168.1.3	192.168.1.1	LDAP	206 searchRequest(6) "CN=Schema,CN=Configuration,DC=test,DC=local" wholetype="*" searchResEntry(6) "CN=Schema,CN=Configuration,DC=test,DC=local" searchResDone(6) success [1 results]
44	0.024982591	192.168.1.1	192.168.1.3	LDAP	17947 searchRequest(7) "CN=Schema,CN=Configuration,DC=test,DC=local" wholetype="*" searchResEntry(7) "CN=Schema,CN=Configuration,DC=test,DC=local" searchResDone(7) success [1 results]
45	0.023169811	192.168.1.3	192.168.1.1	TCP	66 35867 → 389 [ACK] Seq=1077 Ack=327050 Win=540288 Len=0 TSval=3493044588 TSecr=3493044588
46	0.027599186	192.168.1.3	192.168.1.1	LDAP	1177 searchRequest(8) "CN=Schema,CN=Configuration,DC=test,DC=local" wholetype="*" searchResEntry(8) "CN=Schema,CN=Configuration,DC=test,DC=local" searchResDone(8) success [1 results]
47	0.027990942	192.168.1.1	192.168.1.3	LDAP	18251 searchResEntry(8) "CN=Schema,CN=Configuration,DC=test,DC=local" wholetype="*" searchResDone(8) success [1 results]
48	0.028100561	192.168.1.3	192.168.1.1	TCP	66 35867 → 389 [ACK] Seq=2188 Ack=345235 Win=565888 Len=0 TSval=3493044588 TSecr=3493044588
49	0.028620328	192.168.1.1	192.168.1.3	LDAP	1177 searchRequest(9) "CN=Schema,CN=Configuration,DC=test,DC=local" wholetype="*" searchResEntry(9) "CN=Schema,CN=Configuration,DC=test,DC=local" searchResDone(9) success [1 results]
50	0.028673998	192.168.1.3	192.168.1.1	LDAP	18703 searchResEntry(9) "CN=Schema,CN=Configuration,DC=test,DC=local" wholetype="*" searchResDone(9) success [1 results]
51	0.028696944	192.168.1.3	192.168.1.1	TCP	66 35867 → 389 [ACK] Seq=3299 Ack=363872 Win=565888 Len=0 TSval=3493044588 TSecr=3493044588
52	0.103396886	192.168.1.3	192.168.1.1	TCP	1177 searchRequest(9) "CN=Schema,CN=Configuration,DC=test,DC=local" wholetype="*" searchResEntry(9) "CN=Schema,CN=Configuration,DC=test,DC=local" searchResDone(9) success [1 results]
53	0.105351358	192.168.1.1	192.168.1.3	LDAP	18427 searchResEntry(9) "CN=Schema,CN=Configuration,DC=test,DC=local" wholetype="*" searchResDone(9) success [1 results]
54	0.105373523	192.168.1.3	192.168.1.1	TCP	66 35867 → 389 [ACK] Seq=363872 Ack=937 Win=565888 Len=0 TSval=3493044588 TSecr=3493044588

Осуществление еще одной NTLM аутентификации для взаимодействия с SMB.

279	0.775106044	192.168.1.1	192.168.1.3	SMB2	318 Negotiate Protocol Response
280	0.776971941	192.168.1.3	192.168.1.1	SMB2	224 Session Setup Request, NTLMSSP_NEGOTIATE
281	0.777375986	192.168.1.1	192.168.1.3	TCP	66 59407 → 389 [ACK] Seq=13642 Ack=342044 Win=499968 Len=0 TSval=3493044588 TSecr=3493044588
282	0.777945728	192.168.1.3	192.168.1.1	SMB2	371 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_AUTH, User: test.local\ldapdump-user
283	0.780473356	192.168.1.3	192.168.1.1	SMB2	534 Session Setup Request, NTLMSSP_AUTH, User: test.local\ldapdump-user
284	0.782021581	192.168.1.1	192.168.1.3	SMB2	151 Session Setup Response
285	0.784239164	192.168.1.3	192.168.1.1	SMB2	230 Encrypted SMB3
286	0.784816935	192.168.1.1	192.168.1.3	SMB2	202 Encrypted SMB3
287	0.785273004	192.168.1.3	192.168.1.1	TCP	66 35867 → 389 [ACK] Seq=23221 Ack=1018389 Win=579584 Len=0 TSval=3493044588 TSecr=3493044588
288	0.786569273	192.168.1.3	192.168.1.1	SMB2	254 Encrypted SMB3
289	0.787309890	192.168.1.1	192.168.1.3	SMB2	274 Encrypted SMB3
290	0.789326588	192.168.1.3	192.168.1.1	SMB2	306 Encrypted SMB3
291	0.790135893	192.168.1.1	192.168.1.3	SMB2	202 Encrypted SMB3
292	0.791846336	192.168.1.3	192.168.1.1	SMB2	235 Encrypted SMB3
293	0.792590122	192.168.1.1	192.168.1.3	SMB2	270 Encrypted SMB3
294	0.796505437	192.168.1.3	192.168.1.1	SMB2	318 Encrypted SMB3
295	0.797367630	192.168.1.1	192.168.1.3	SMB2	202 Encrypted SMB3
296	0.798747364	192.168.1.3	192.168.1.1	SMB2	235 Encrypted SMB3
297	0.799607746	192.168.1.1	192.168.1.3	SMB2	362 Encrypted SMB3
298	0.801814175	192.168.1.3	192.168.1.1	SMB2	190 Encrypted SMB3
299	0.802554633	192.168.1.1	192.168.1.3	SMB2	190 Encrypted SMB3
300	0.803967581	192.168.1.3	192.168.1.1	SMB2	230 Encrypted SMB3
301	0.804590751	192.168.1.1	192.168.1.3	SMB2	202 Encrypted SMB3
302	0.806137626	192.168.1.3	192.168.1.1	SMB2	250 Encrypted SMB3
303	0.807204682	192.168.1.1	192.168.1.3	SMB2	274 Encrypted SMB3
304	0.809858867	192.168.1.3	192.168.1.1	SMB2	306 Encrypted SMB3
305	0.810629373	192.168.1.1	192.168.1.3	SMB2	202 Encrypted SMB3
306	0.812665321	192.168.1.3	192.168.1.1	SMB2	235 Encrypted SMB3
307	0.813450365	192.168.1.1	192.168.1.3	SMB2	270 Encrypted SMB3
308	0.815745040	192.168.1.3	192.168.1.1	SMB2	270 Encrypted SMB3
309	0.816413917	192.168.1.1	192.168.1.3	SMB2	202 Encrypted SMB3
310	0.817638638	192.168.1.3	192.168.1.1	SMB2	235 Encrypted SMB3
311	0.818365703	192.168.1.1	192.168.1.3	SMB2	250 Encrypted SMB3
312	0.820453817	192.168.1.3	192.168.1.1	SMB2	312 Encrypted SMB3
313	0.821059173	192.168.1.1	192.168.1.3	SMB2	202 Encrypted SMB3
314	0.822305384	192.168.1.3	192.168.1.1	SMB2	235 Encrypted SMB3
315	0.822973458	192.168.1.1	192.168.1.3	SMB2	234 Encrypted SMB3
316	0.825387705	192.168.1.3	192.168.1.1	SMB2	286 Encrypted SMB3
317	0.826396862	192.168.1.1	192.168.1.3	SMB2	202 Encrypted SMB3
318	0.827982263	192.168.1.3	192.168.1.1	SMB2	235 Encrypted SMB3
319	0.828968001	192.168.1.1	192.168.1.3	SMB2	326 Encrypted SMB3
320	0.830370426	192.168.1.3	192.168.1.1	SMB2	306 Encrypted SMB3

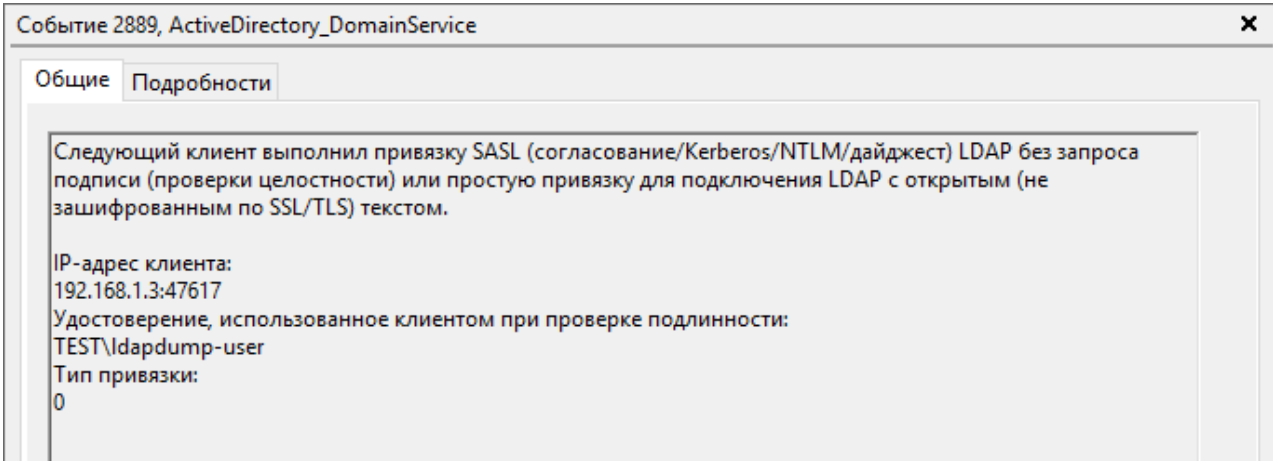
Локальный дамп

Также, если есть необходимость выявить всех пользователей домена и информацию о них, можно выполнить локальный дамп с помощью PoSH `Get-ADUser -Filter * -Properties DisplayName, EmailAddress, Enabled, LastLogonDate | Format-Table -AutoSize`

PS C:\Users\Администратор.WIN-8Q40H33CDSA> Get-ADUser -Filter * -Properties DisplayName, EmailAddress, Enabled, LastLogonDate Format-Table -AutoSize							
DisplayName	DistinguishedName	EmailAddress	Enabled	GivenName	LastLogonDate	Name	
	CN=Администратор,CN=Users,DC=test,DC=local		True		28.06.2024 0:25:26	Администратор	
	CN=Гость,CN=Users,DC=test,DC=local		False			Гость	
	CN=DefaultAccount,CN=Users,DC=test,DC=local		False			DefaultAcc...	
	CN=krbtgt,CN=Users,DC=test,DC=local		False			krbtgt	
Admin Demo	CN=Admin Demo,OU=Admins,DC=test,DC=local		True	Admin	28.06.2024 0:36:04	Admin Demo	
PTHuser	CN=PTHuser,CN=Users,DC=test,DC=local		True	PTHuser	01.07.2024 5:35:36	PTHuser	
AsREP User	CN=AsREP User,CN=Users,DC=test,DC=local		True	AsREP	05.07.2024 7:43:39	AsREP User	
LDAP Dump	CN=LDAP Dump,CN=Users,DC=test,DC=local		True	LDAP	05.07.2024 7:48:19	LDAP Dump	

Артефакты

















Как правило, при проведении данной атаки, основным фактором является наличие множества событий MSGID 1644 (Выполнен LDAP запрос), а также MSGID 2889 (Незащищенные привязки LDAP), которые подкрепляются событиями из разделов ниже



Дамп через Kerberos аутентификацию

	Аудит успеха	07.07.2024 1:18:32	Microsoft Win...	4634	Выход из системы
	Аудит успеха	07.07.2024 1:18:32	Microsoft Win...	4634	Выход из системы
	Аудит успеха	07.07.2024 1:18:29	Microsoft Win...	4634	Выход из системы
	Аудит успеха	07.07.2024 1:18:29	Microsoft Win...	5140	Общий файловый ресурс
	Аудит успеха	07.07.2024 1:18:29	Microsoft Win...	5140	Общий файловый ресурс
	Аудит успеха	07.07.2024 1:18:29	Microsoft Win...	5140	Общий файловый ресурс
	Аудит успеха	07.07.2024 1:18:29	Microsoft Win...	5140	Общий файловый ресурс
	Аудит успеха	07.07.2024 1:18:29	Microsoft Win...	5140	Общий файловый ресурс
	Аудит успеха	07.07.2024 1:18:29	Microsoft Win...	5140	Общий файловый ресурс
	Аудит успеха	07.07.2024 1:18:29	Microsoft Win...	4624	Вход в систему
	Аудит успеха	07.07.2024 1:18:29	Microsoft Win...	4769	Операции с билетами службы Kerbe...
	Аудит успеха	07.07.2024 1:18:29	Microsoft Win...	4769	Операции с билетами службы Kerbe...
	Аудит успеха	07.07.2024 1:18:28	Microsoft Win...	4624	Вход в систему
	Аудит успеха	07.07.2024 1:18:28	Microsoft Win...	4769	Операции с билетами службы Kerbe...
	Аудит успеха	07.07.2024 1:18:28	Microsoft Win...	4624	Вход в систему
	Аудит успеха	07.07.2024 1:18:28	Microsoft Win...	4769	Операции с билетами службы Kerbe...
	Аудит успеха	07.07.2024 1:18:28	Microsoft Win...	4768	Служба проверки подлинности Kerb...

Дамп через NTLM аутентификацию

	Аудит успеха	07.07.2024 1:24:24	Microsoft Win...	4634	Выход из системы
	Аудит успеха	07.07.2024 1:24:24	Microsoft Win...	4634	Выход из системы
	Аудит успеха	07.07.2024 1:24:21	Microsoft Win...	4634	Выход из системы
	Аудит успеха	07.07.2024 1:24:21	Microsoft Win...	5140	Общий файловый ресурс
	Аудит успеха	07.07.2024 1:24:21	Microsoft Win...	5140	Общий файловый ресурс
	Аудит успеха	07.07.2024 1:24:21	Microsoft Win...	5140	Общий файловый ресурс
	Аудит успеха	07.07.2024 1:24:21	Microsoft Win...	5140	Общий файловый ресурс
	Аудит успеха	07.07.2024 1:24:20	Microsoft Win...	5140	Общий файловый ресурс
	Аудит успеха	07.07.2024 1:24:20	Microsoft Win...	4776	Проверка учетных данных
	Аудит успеха	07.07.2024 1:24:20	Microsoft Win...	5140	Общий файловый ресурс
	Аудит успеха	07.07.2024 1:24:20	Microsoft Win...	4624	Вход в систему
	Аудит успеха	07.07.2024 1:24:20	Microsoft Win...	4776	Проверка учетных данных
	Аудит успеха	07.07.2024 1:24:20	Microsoft Win...	4624	Вход в систему
	Аудит успеха	07.07.2024 1:24:20	Microsoft Win...	4776	Проверка учетных данных
	Аудит успеха	07.07.2024 1:24:20	Microsoft Win...	4624	Вход в систему
	Аудит успеха	07.07.2024 1:24:20	Microsoft Win...	4776	Проверка учетных данных

Вывод

Как видно, основной последовательностью событий в журнале безопасности Windows при разных протоколах аутентификации служат:

1. Вход в систему (как правило, несколько раз подряд)
2. Обращения к службам:
 1. Для Kerberos в TGS_REQ: ldap и cifs в SNameString
 2. Для NTLM: ldap и smb
3. Обращения к шару *\IPC\$ с маской 0x1 (чтение данных или перечисление каталогов)
4. Выход из системы (количество эквивалентно входам)

Профит

Получаем визуализацию полученных данных и ищем доступные пути компрометации домена

