

Tangled Heist

Description :

The survivors' group has meticulously planned the mission 'Tangled Heist' for months. In the desolate wasteland, what appears to be an abandoned facility is, in reality, the headquarters of a rebel faction. This faction guards valuable data that could be useful in reaching the vault. Kaila, acting as an undercover agent, successfully infiltrates the facility using a rebel faction member's account and gains access to a critical asset containing invaluable information. This data holds the key to both understanding the rebel faction's organization and advancing the survivors' mission to reach the vault. To get the flag, spawn the docker instance and answer the questions!

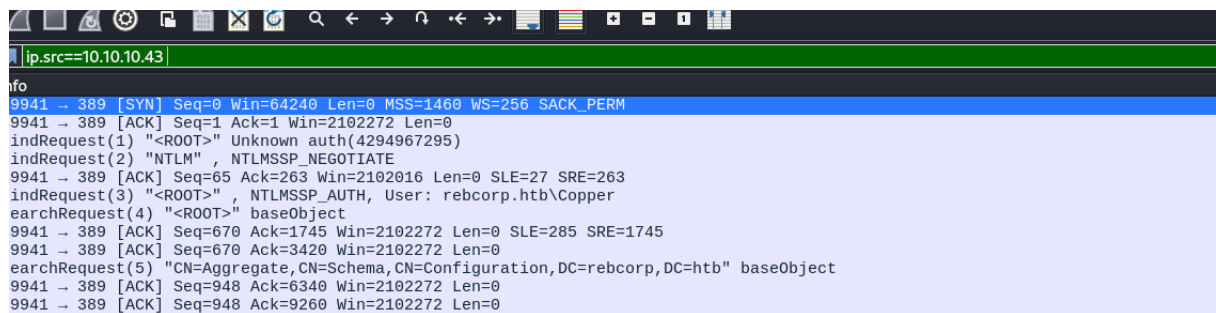
We have a .pcap file , let's analyze it with wireshark .

It look like there is only two Ip address in the conversation : 10.10.10.43—10.10.10.100

Let's answer the question:

Which is the username of the compromised user used to conduct the attack?

The only address is 10.10.10.43, and it's assigned to the copper user



What is the Distinguished Name (DN) of the Domain Controller? Don't put spaces between commas. (for example: CN=...,CN=...,DC=...,DC=...)

The structure of the DN of the the domain controller is :

CN=<DomainControllerName>,OU=Domain Controllers,DC=<Domain>,DC=<TopLevelDomain>

I used strings command to search for OU=Domain Controller : strings capture.pcap | grep "Domain"

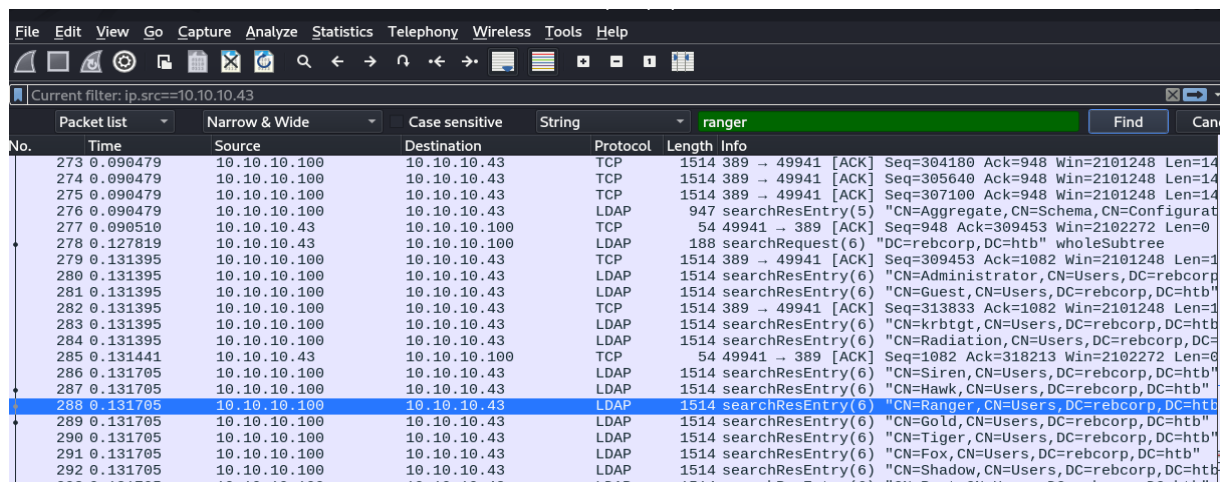
Its CN=SRV195,OU=Domain Controllers,DC=rebcorp,DC=htb

Which is the Domain managed by the Domain Controller?

Rebcorp.htb

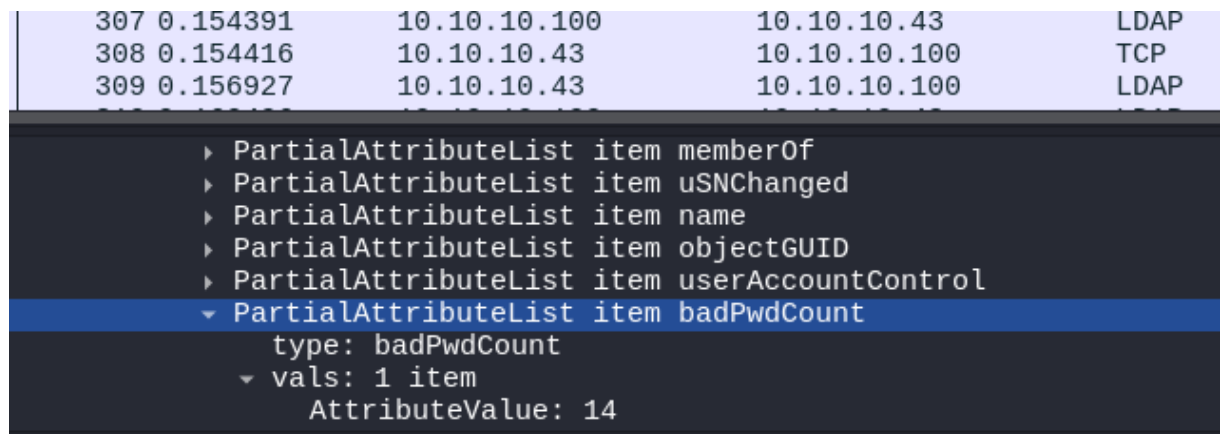
How many failed login attempts are recorded on the user account named 'Ranger'? (for example: 6)

I searched for ranger in the search barre.



No.	Time	Source	Destination	Protocol	Length	Info
273	0.090479	10.10.10.100	10.10.10.43	TCP	1514	389 → 49941 [ACK] Seq=304180 Ack=948 Win=2101248 Len=14
274	0.090479	10.10.10.100	10.10.10.43	TCP	1514	389 → 49941 [ACK] Seq=305640 Ack=948 Win=2101248 Len=14
275	0.090479	10.10.10.100	10.10.10.43	TCP	1514	389 → 49941 [ACK] Seq=307100 Ack=948 Win=2101248 Len=14
276	0.090479	10.10.10.100	10.10.10.43	LDAP	947	searchResEntry(5) "CN=Aggregate,CN=Schema,CN=Configurat
277	0.090510	10.10.10.43	10.10.10.100	TCP	54	49941 → 389 [ACK] Seq=948 Ack=309453 Win=2102272 Len=0
278	0.127819	10.10.10.43	10.10.10.100	LDAP	188	searchRequest(6) "DC=rebcorp,DC=htb" wholeSubtree
279	0.131395	10.10.10.100	10.10.10.43	TCP	1514	389 → 49941 [ACK] Seq=309453 Ack=1082 Win=2101248 Len=1
280	0.131395	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=Administrator,CN=Users,DC=rebcorp,DC=htb"
281	0.131395	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=Guest,CN=Users,DC=rebcorp,DC=htb"
282	0.131395	10.10.10.100	10.10.10.43	TCP	1514	389 → 49941 [ACK] Seq=313833 Ack=1082 Win=2101248 Len=1
283	0.131395	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=krbtgt,CN=Users,DC=rebcorp,DC=htb"
284	0.131395	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=Radiation,CN=Users,DC=rebcorp,DC=htb"
285	0.131441	10.10.10.43	10.10.10.100	TCP	54	49941 → 389 [ACK] Seq=1082 Ack=318213 Win=2102272 Len=0
286	0.131705	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=Siren,CN=Users,DC=rebcorp,DC=htb"
287	0.131705	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=Hawk,CN=Users,DC=rebcorp,DC=htb"
288	0.131705	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=Ranger,CN=Users,DC=rebcorp,DC=htb"
289	0.131705	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=Gold,CN=Users,DC=rebcorp,DC=htb"
290	0.131705	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=Tiger,CN=Users,DC=rebcorp,DC=htb"
291	0.131705	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=Fox,CN=Users,DC=rebcorp,DC=htb"
292	0.131705	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=Shadow,CN=Users,DC=rebcorp,DC=htb"

Then I checked the ldap (lightweight directory access protocol) and searched for Badpwdcount .



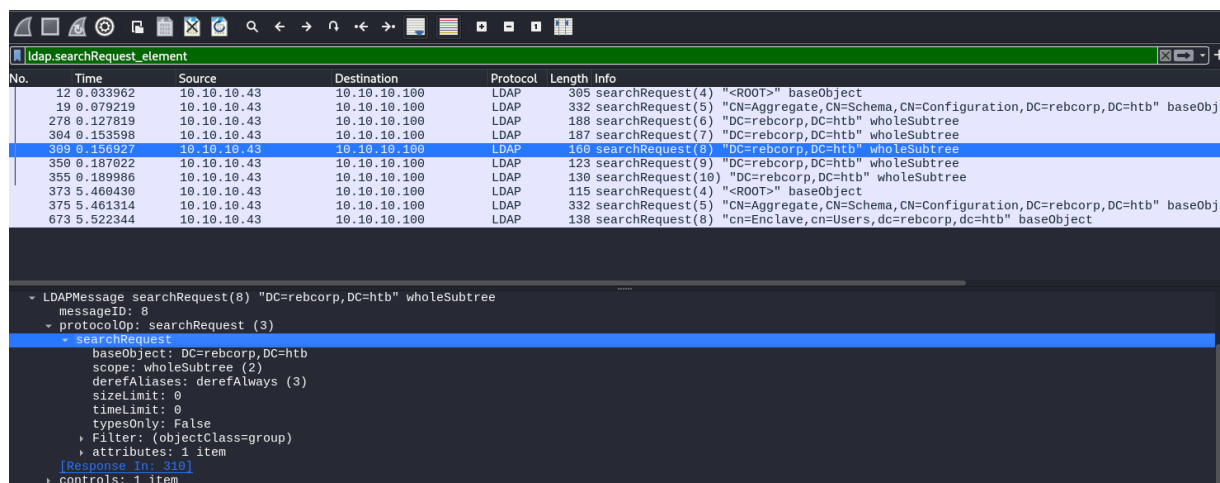
No.	Time	Source	Destination	Protocol	Length	Info
307	0.154391	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=Gold,CN=Users,DC=rebcorp,DC=htb"
308	0.154416	10.10.10.43	10.10.10.100	TCP	54	49941 → 389 [ACK] Seq=1082 Ack=318213 Win=2102272 Len=0
309	0.156927	10.10.10.43	10.10.10.100	LDAP	1514	searchResEntry(6) "CN=Shadow,CN=Users,DC=rebcorp,DC=htb"

```
PartialAttributeList item memberOf
PartialAttributeList item uSNChanged
PartialAttributeList item name
PartialAttributeList item objectGUID
PartialAttributeList item userAccountControl
PartialAttributeList item badPwdCount
  type: badPwdCount
  vals: 1 item
    AttributeValue: 14
```

Its 14

Which LDAP query was executed to find all groups?

At first, I didn't understand this question, but after conducting some research on Google, I got it. Here are the steps to follow: Search for the search request packets (ldap.searchRequest_element), then look for the Filter field and search for (objectclass=group)."



No.	Time	Source	Destination	Protocol	Length	Info
12	0.033962	10.10.10.43	10.10.10.100	LDAP	305	searchRequest(4) "<ROOT>" baseObject
19	0.079219	10.10.10.43	10.10.10.100	LDAP	332	searchRequest(5) "CN=Aggregate,CN=Schema,CN=Configuration,DC=rebcorp,DC=htb" baseObj
278	0.127819	10.10.10.43	10.10.10.100	LDAP	188	searchRequest(6) "DC=rebcorp,DC=htb" wholeSubtree
304	0.153598	10.10.10.43	10.10.10.100	LDAP	187	searchRequest(7) "DC=rebcorp,DC=htb" wholeSubtree
309	0.156927	10.10.10.43	10.10.10.100	LDAP	160	searchRequest(8) "DC=rebcorp,DC=htb" wholeSubtree
350	0.187022	10.10.10.43	10.10.10.100	LDAP	123	searchRequest(9) "DC=rebcorp,DC=htb" wholeSubtree
355	0.189986	10.10.10.43	10.10.10.100	LDAP	130	searchRequest(10) "DC=rebcorp,DC=htb" wholeSubtree
373	5.460430	10.10.10.43	10.10.10.100	LDAP	115	searchRequest(4) "<ROOT>" baseObject
375	5.461314	10.10.10.43	10.10.10.100	LDAP	332	searchRequest(5) "CN=Aggregate,CN=Schema,CN=Configuration,DC=rebcorp,DC=htb" baseObj
673	5.522344	10.10.10.43	10.10.10.100	LDAP	138	searchRequest(8) "cn=Enclave,cn=Users,dc=rebcorp,dc=htb" baseObject

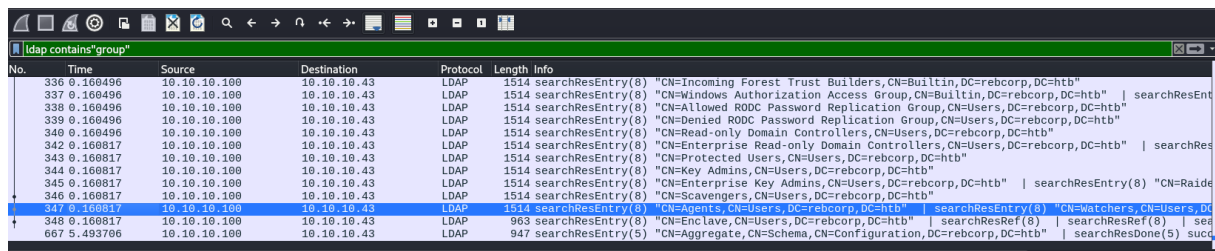
```
LDAPMessage searchRequest(8) "DC=rebcorp,DC=htb" wholeSubtree
  messageID: 8
  protocolOp: searchRequest (3)
  searchRequest
    baseObject: DC=rebcorp,DC=htb
    scope: wholeSubtree (2)
    derefAliases: derefAlways (3)
    sizeLimit: 0
    timeLimit: 0
    typesOnly: False
    Filter: (objectClass=group)
    attributes: 1 item
      [Response In: 310]
    controls: 1 item
```

The answer : (objectClass=group)

How many non-standard groups exist?

5

I searched for 'group' and looked for the packets that are different from the others. I found four packets at the end that are non-standard. However, be careful with the packet in line 347; it contains two groups: 'Agents' and 'Watchers'."

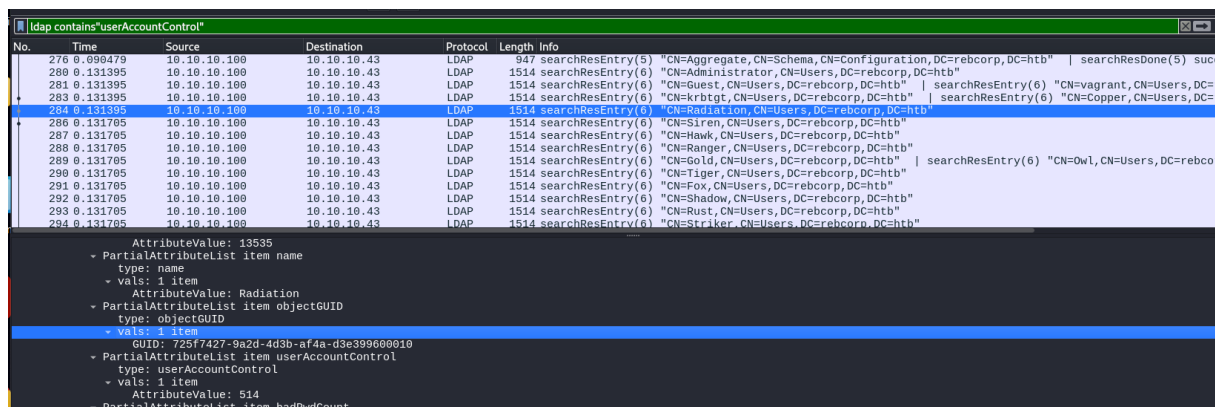


Wireshark packet capture showing LDAP search results for 'group'. The table lists packets with columns: No., Time, Source, Destination, Protocol, Length, and Info. The search results include various groups like 'CN=Incoming Forest Trust Builders', 'CN=Windows Authorization Access Group', 'CN=Allowed RODC Password Replication Group', 'CN=Denied RODC Password Replication Group', 'CN=Read-only Domain Controllers', 'CN=Enterprise Read-only Domain Controllers', 'CN=Protected Users', 'CN=Key Admins', 'CN=Enterprise Key Admins', 'CN=Scavengers', 'CN=Agents', and 'CN=Watchers'.

No.	Time	Source	Destination	Protocol	Length	Info
336	0.160496	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(8) "CN=Incoming Forest Trust Builders,CN=Builtin,DC=rebcorp,DC=htb"
337	0.160496	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(8) "CN=Windows Authorization Access Group,CN=Builtin,DC=rebcorp,DC=htb" searchResEntry(8)
338	0.160496	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(8) "CN=Allowed RODC Password Replication Group,CN=Users,DC=rebcorp,DC=htb"
339	0.160496	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(8) "CN=Denied RODC Password Replication Group,CN=Users,DC=rebcorp,DC=htb"
340	0.160496	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(8) "CN=Read-only Domain Controllers,CN=Users,DC=rebcorp,DC=htb"
342	0.160817	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(8) "CN=Enterprise Read-only Domain Controllers,CN=Users,DC=rebcorp,DC=htb" searchResEntry(8)
343	0.160817	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(8) "CN=Protected Users,CN=Users,DC=rebcorp,DC=htb"
344	0.160817	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(8) "CN=Key Admins,CN=Users,DC=rebcorp,DC=htb"
345	0.160817	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(8) "CN=Enterprise Key Admins,CN=Users,DC=rebcorp,DC=htb" searchResEntry(8) "CN=Raide"
346	0.160817	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(8) "CN=Scavengers,CN=Users,DC=rebcorp,DC=htb"
347	0.160817	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(8) "CN=Agents,CN=Users,DC=rebcorp,DC=htb" searchResEntry(8) "CN=Watchers,CN=Users,DC=htb"
348	0.160817	10.10.10.100	10.10.10.43	LDAP	963	searchResEntry(8) "CN=Enclave,CN=Users,DC=rebcorp,DC=htb" searchResRef(8) searchResRef(8) searchResEntry(8)
667	5.493706	10.10.10.100	10.10.10.43	LDAP	947	searchResEntry(5) "CN=Aggregate,CN=Schema,CN=Configuration,DC=rebcorp,DC=htb" searchResDone(5) succ

One of the non-standard users is flagged as 'disabled', which is it?

To find disabled users in Wireshark, you'll need to look for LDAP searchRequest or searchResEntry packets containing the "userAccountControl" attribute and check its value. The presence of a specific bit in this value (such as 514 or 0x0202) will indicate that the account is disabled.



Wireshark packet capture showing LDAP search results for 'userAccountControl'. The table lists packets with columns: No., Time, Source, Destination, Protocol, Length, and Info. The search results include various users like 'CN=Aggregate', 'CN=Administrator', 'CN=Quest', 'CN=kbrtgt', 'CN=Radiation', 'CN=Siren', 'CN=Hawk', 'CN=Ranger', 'CN=Gold', 'CN=Tiger', 'CN=Fox', 'CN=Shadow', 'CN=Enclave', and 'CN=Striker'. The packet at line 284 shows the 'userAccountControl' attribute with a value of 514, indicating a disabled account.

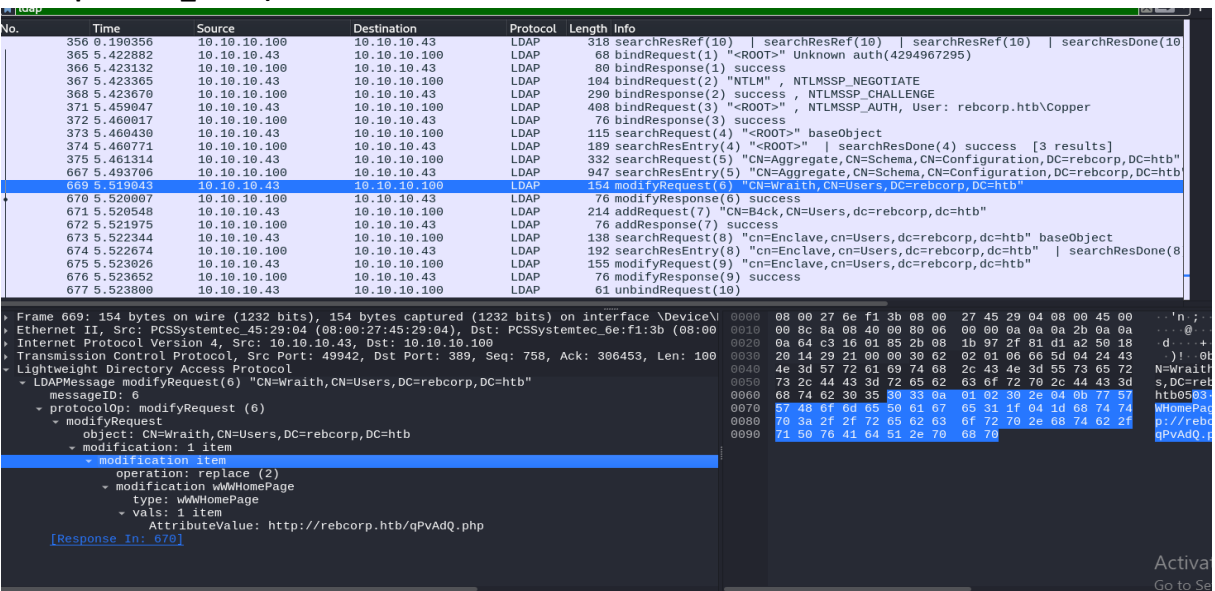
No.	Time	Source	Destination	Protocol	Length	Info
276	0.090479	10.10.10.100	10.10.10.43	LDAP	947	searchResEntry(5) "CN=Aggregate,CN=Schema,CN=Configuration,DC=rebcorp,DC=htb" searchResDone(5) succ
280	0.131395	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=Administrator,CN=Users,DC=rebcorp,DC=htb"
281	0.131395	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=Quest,CN=Users,DC=rebcorp,DC=htb" searchResEntry(6) "CN=vagrant,CN=Users,DC=r
283	0.131395	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=kbrtgt,CN=Users,DC=rebcorp,DC=htb" searchResEntry(6) "CN=Copper,CN=Users,DC=r
284	0.131395	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=Radiation,CN=Users,DC=rebcorp,DC=htb"
286	0.131705	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=Siren,CN=Users,DC=rebcorp,DC=htb"
287	0.131705	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=Hawk,CN=Users,DC=rebcorp,DC=htb"
288	0.131705	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=Ranger,CN=Users,DC=rebcorp,DC=htb"
289	0.131705	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=Gold,CN=Users,DC=rebcorp,DC=htb" searchResEntry(6) "CN=Owl,CN=Users,DC=rebcor
290	0.131705	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=Tiger,CN=Users,DC=rebcorp,DC=htb"
291	0.131705	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=Fox,CN=Users,DC=rebcorp,DC=htb"
292	0.131705	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=Shadow,CN=Users,DC=rebcorp,DC=htb"
293	0.131705	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=Enclave,CN=Users,DC=rebcorp,DC=htb"
294	0.131705	10.10.10.100	10.10.10.43	LDAP	1514	searchResEntry(6) "CN=Striker,CN=Users,DC=rebcorp,DC=htb"

AttributeValues: 13535
- PartialAttributeList item name
type: name
- vals: 1 item
AttributeValue: Radiation
- PartialAttributeList item objectGUID
type: objectGUID
- vals: 1 item
GUID: 725f7427-9a2d-4d3b-af4a-d3e399600b10
- PartialAttributeList item userAccountControl
type: userAccountControl
- vals: 1 item
AttributeValue: 514
- PartialAttributeList item badPwdCount

AttributeValue : 514

Answer : Radiation

The attacker targeted one user writing some data inside a specific field. Which is the field name? (for example: field_name)



Wireshark packet capture showing LDAP modifyRequest for 'CN=Wraith'. The table lists packets with columns: No., Time, Source, Destination, Protocol, Length, and Info. The packet at line 669 shows a modifyRequest for 'CN=Wraith' with a modification of 'wWWHomePage'.

No.	Time	Source	Destination	Protocol	Length	Info
356	0.190356	10.10.10.100	10.10.10.43	LDAP	318	searchResRef(10) searchResRef(10) searchResRef(10) searchResDone(10)
365	5.422882	10.10.10.43	10.10.10.100	LDAP	68	bindRequest(1) "c=ROOT" Unknown auth(4294967295)
366	5.423132	10.10.10.100	10.10.10.43	LDAP	80	bindResponse(1) success
367	5.423305	10.10.10.43	10.10.10.100	LDAP	104	bindRequest(2) "NTLM", NTLMSSP_NEGOTIATE
368	5.423670	10.10.10.100	10.10.10.43	LDAP	290	bindResponse(2) success, NTLMSSP_CHALLENGE
371	5.459047	10.10.10.43	10.10.10.100	LDAP	408	bindRequest(3) "c=ROOT", NTLMSSP_AUTH, User: rebcorp.htbCopper
372	5.460017	10.10.10.100	10.10.10.43	LDAP	76	bindResponse(3) success
373	5.460430	10.10.10.43	10.10.10.100	LDAP	115	searchRequest(4) "c=ROOT" baseObject
374	5.460771	10.10.10.100	10.10.10.43	LDAP	189	searchResEntry(4) "c=ROOT" searchResDone(4) success [3 results]
375	5.461314	10.10.10.43	10.10.10.100	LDAP	332	searchRequest(5) "CN=Aggregate,CN=Schema,CN=Configuration,DC=rebcorp,DC=htb"
667	5.493706	10.10.10.100	10.10.10.43	LDAP	947	searchResEntry(5) "CN=Aggregate,CN=Schema,CN=Configuration,DC=rebcorp,DC=htb"
669	5.519043	10.10.10.43	10.10.10.100	LDAP	154	modifyRequest(6) "CN=Wraith,CN=Users,DC=rebcorp,DC=htb"
670	5.520007	10.10.10.100	10.10.10.43	LDAP	76	modifyResponse(6) success
671	5.520548	10.10.10.43	10.10.10.100	LDAP	214	addRequest(7) "CN=B4ck,CN=Users,dc=rebcorp,dc=htb"
672	5.521975	10.10.10.100	10.10.10.43	LDAP	76	addResponse(7) success
673	5.522344	10.10.10.43	10.10.10.100	LDAP	138	searchRequest(8) "cn=Enclave,cn=Users,dc=rebcorp,dc=htb" baseObject
674	5.522674	10.10.10.100	10.10.10.43	LDAP	192	searchResEntry(8) "cn=Enclave,cn=Users,dc=rebcorp,dc=htb" searchResDone(8)
675	5.523026	10.10.10.43	10.10.10.100	LDAP	155	modifyRequest(9) "cn=Enclave,cn=Users,dc=rebcorp,dc=htb"
676	5.523652	10.10.10.100	10.10.10.43	LDAP	76	modifyResponse(9) success
677	5.523800	10.10.10.43	10.10.10.100	LDAP	61	unbindRequest(10)

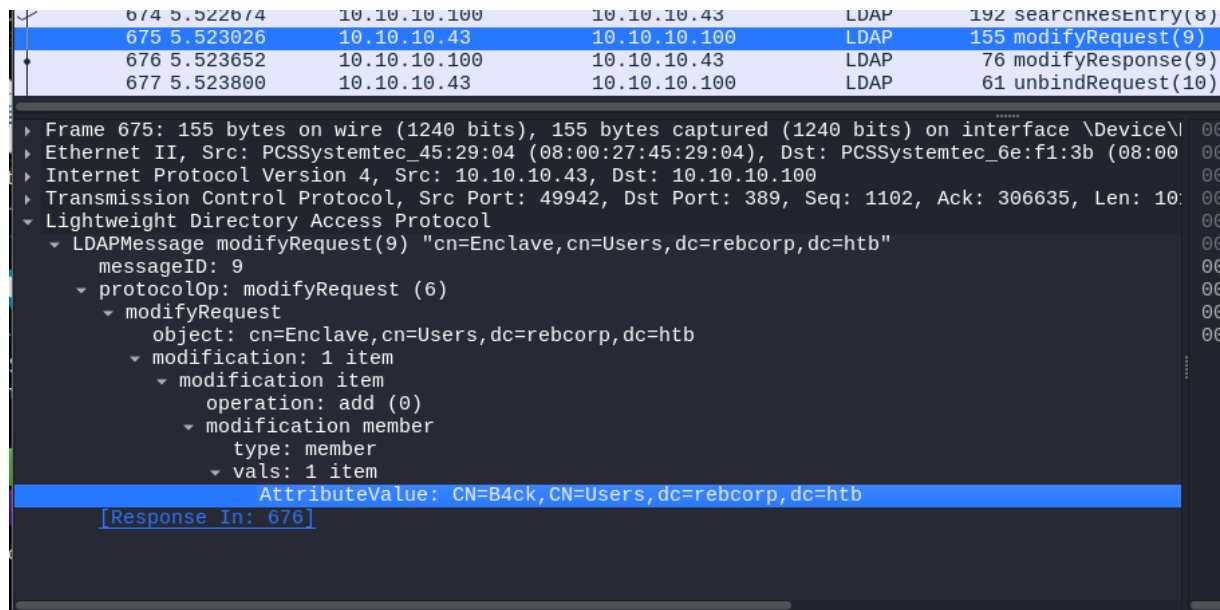
Frame 669: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface DeviceN
Ethernet II, Src: PCSSystemtec 45:29:04 (08:00:27:45:29:04), Dst: PCSSystemtec 6e:f1:3b (08:00:00:00:00:00)
Internet Protocol Version 4, Src: 10.10.10.43, Dst: 10.10.10.100
Transmission Control Protocol, Src Port: 49942, Dst Port: 389, Seq: 758, Ack: 306453, Len: 100
Lightweight Directory Access Protocol
- LDAPMessage modifyRequest(6) "CN=Wraith,CN=Users,DC=rebcorp,DC=htb"
messageID: 6
- protocolOp: modifyRequest (6)
- modifyRequest
object: CN=Wraith,CN=Users,DC=rebcorp,DC=htb
- modification: 1 item
- modification item
operation: replace (2)
- modification wWWHomePage
type: wWWHomePage
- vals: 1 item
AttributeValue: http://rebcorp.htb/qPvAdQ.php
[Response In: 670]

Just check the modify request and you'll find a modification on **wWWHomePage** .

[9/11] Which is the new value written in it? (for example: value123):

<http://rebcorp.htb/qPvAdQ.php>

[10/11] The attacker created a new user for persistence. Which is the username and the assigned group? Don't put spaces in the answer (for example: username,group) :



B4ck,Enclave

The attacker obtained an hash for the user 'Hurricane' that has the UF_DONT_REQUIRE_PREAUTH flag set. Which is the correspondent plaintext for that hash? (for example: plaintext_password)

After a quick search for UF_DONT_REQUIRE_PREAUTH, I found that I should extract the Kerberos ticket and decrypt it to obtain the plaintext.

Here are the steps to follow:

- 1) Extract the pcap traffics and save them into a pdml file : `tshark -r capture.pcap -T pdml > file.pdml`
- 2) Extract the Kerberos ticket from the traffics and generate a john hash for it : `kerb2john file.pdml >hash`
- 3) `john --wordlist=rockyou.txt hash`

```
$ john --wordlist=rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA256 AES 128/128 SSE2 4x])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
april18 (?)
1g 0:00:00:00 DONE (2024-08-19 23:47) 33.33g/s 204800p/s 204800c/s 204800C/s allison1..iheartyou
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Answer : april18

I recommend to read for john