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 asnwer the questions!

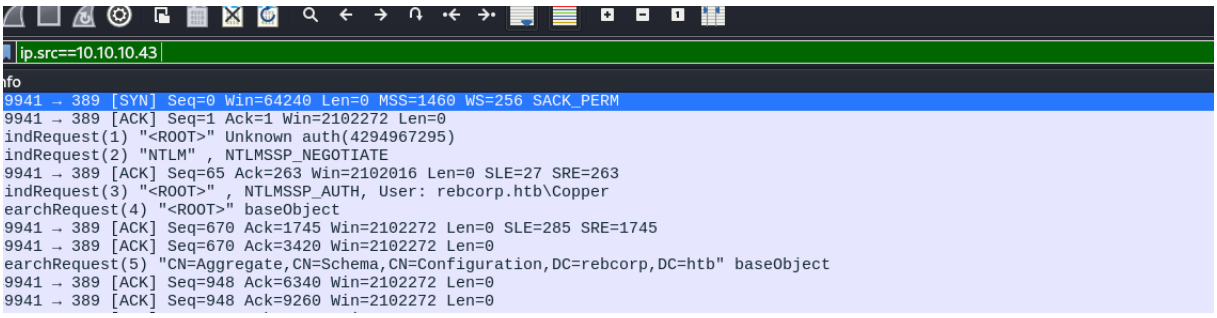
We have a .pcap file , let’s analyze it with wireshark .

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”

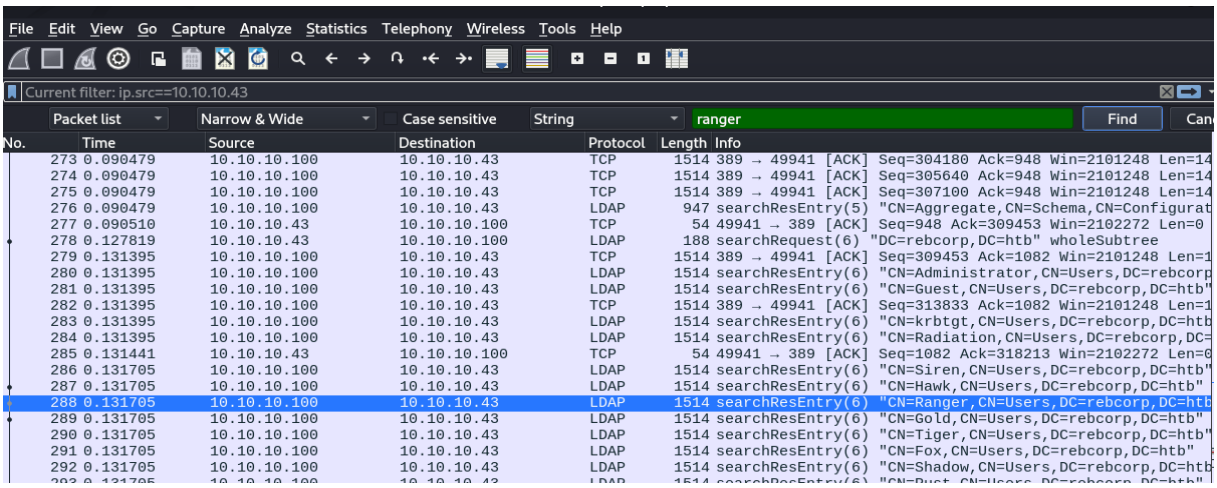
Its CN=SRV195,OU=Domain Controllers,DC=rebcorp,DC=htb

Which is the Domain managed by the Domain Controller?

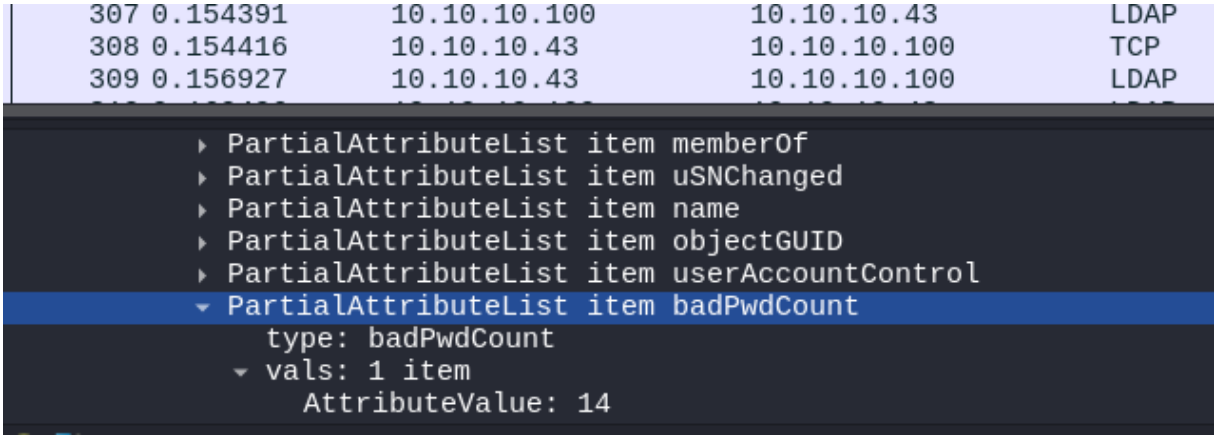
Rebcorp.htb

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

I searched for ranger in the search barre.



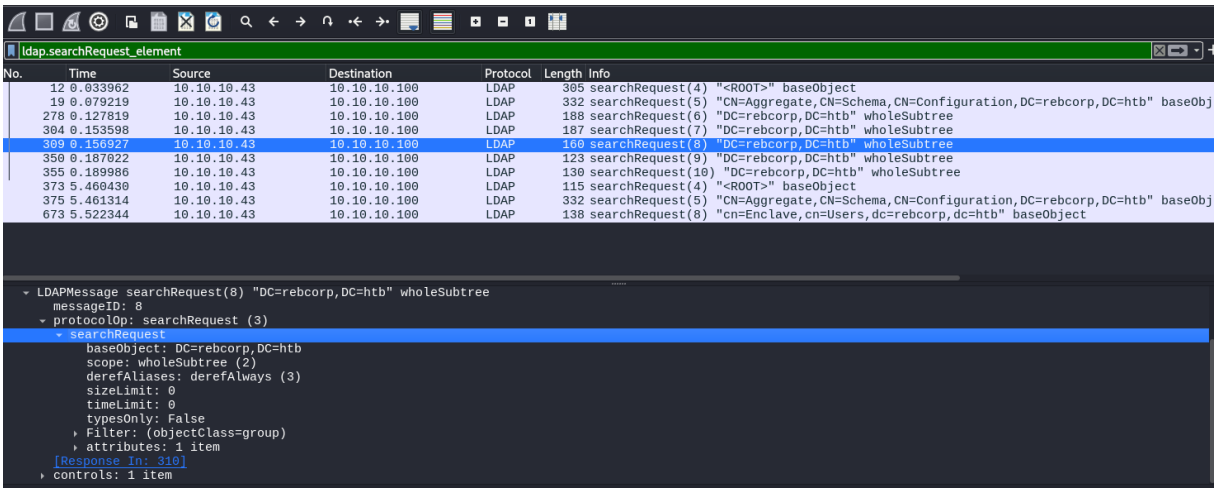
Then I checked the ldap (lightweight directory access protocol) and searched for Badpwdcount .



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)."

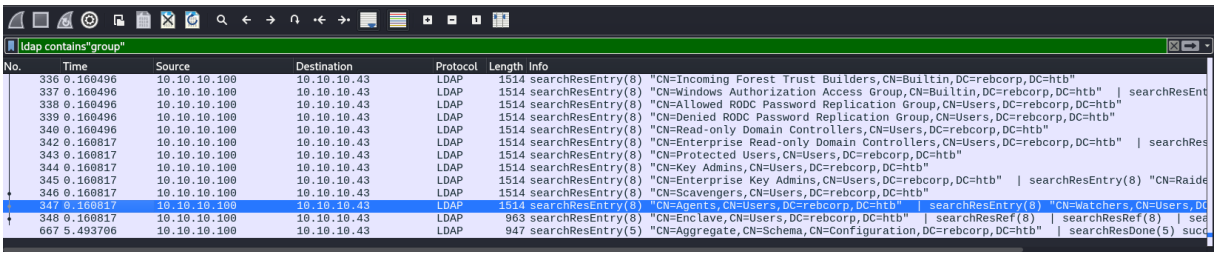


The answer : (objectClass=group)

How many non-standard groups exist?

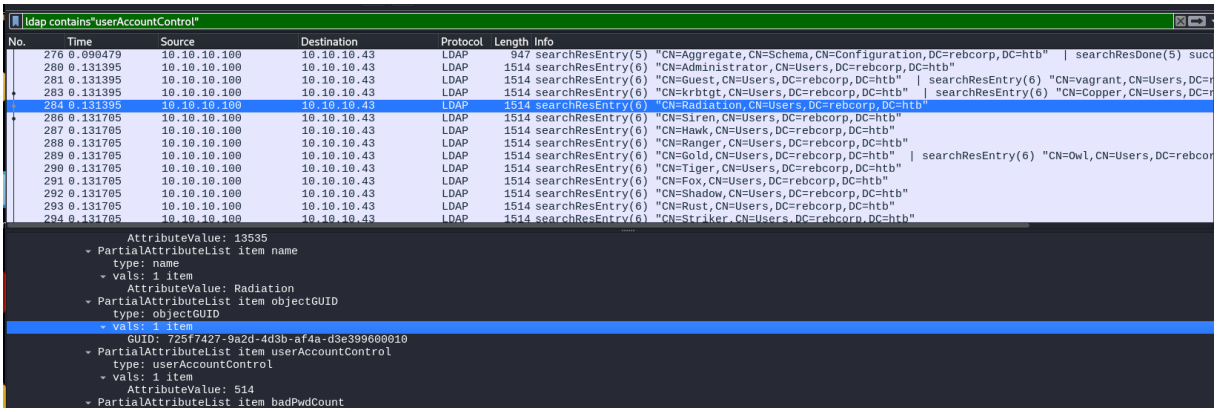
5

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'."



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

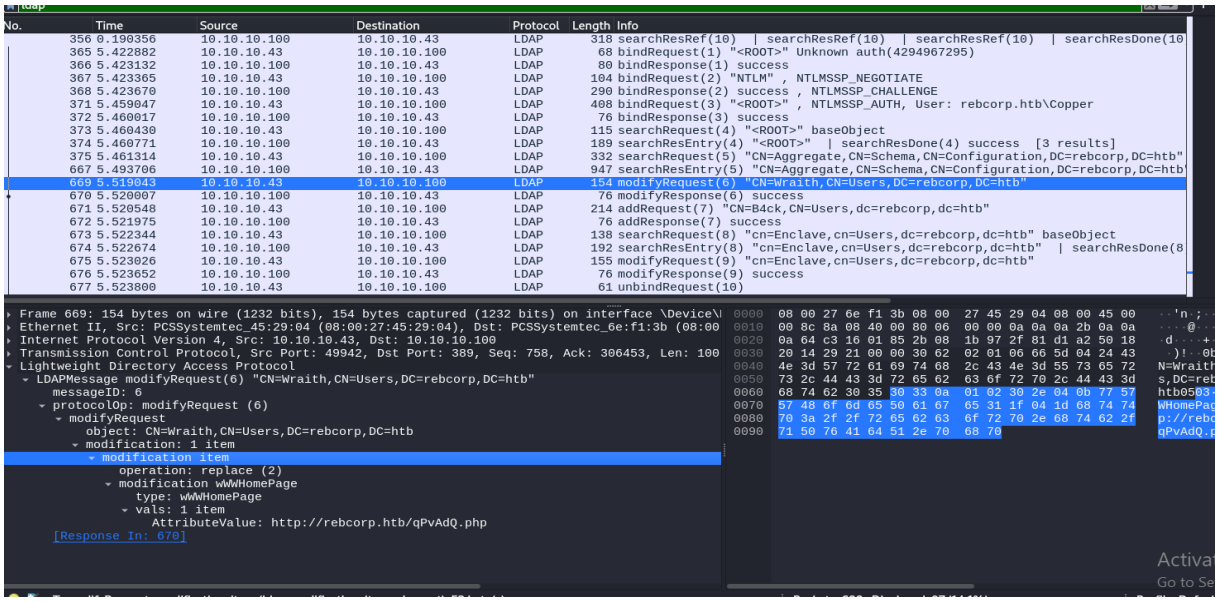
To find disabled users in Wireshark, you'll need to look for LDAP searchRequest or searchResEntry packets containing the “userAccountControl” attribute and check its value. The presence of a specific bit in this value (such as 514 or 0x0202) will indicate that the account is disabled.



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)

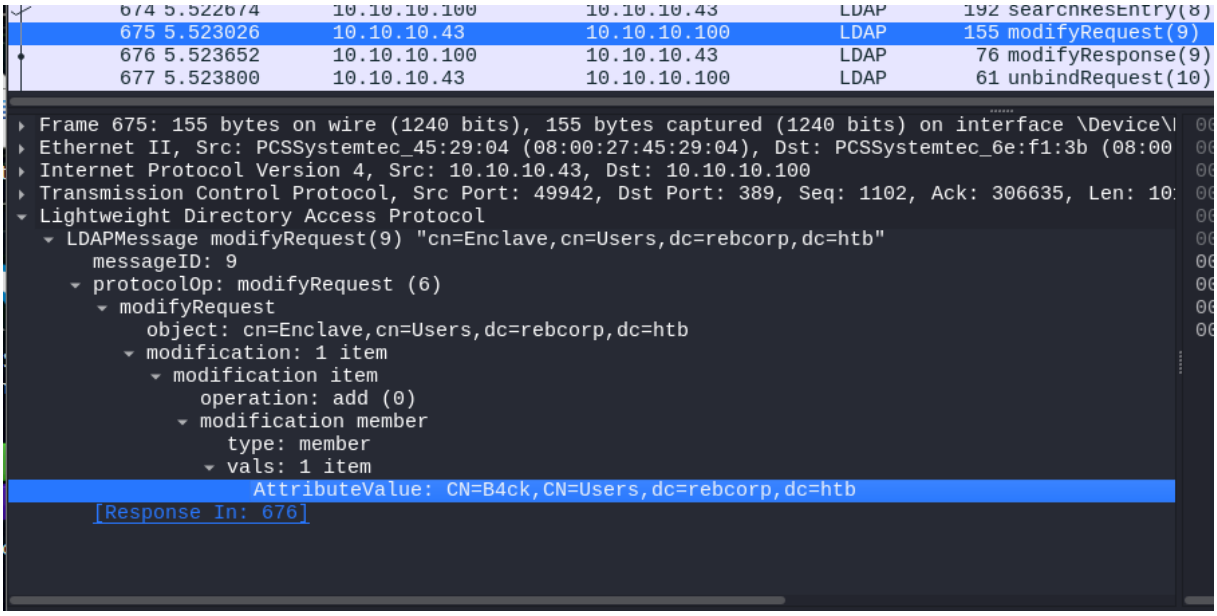


Just check the modify request and you'll find a modification on **wWWHomePage .**

[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-SH
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