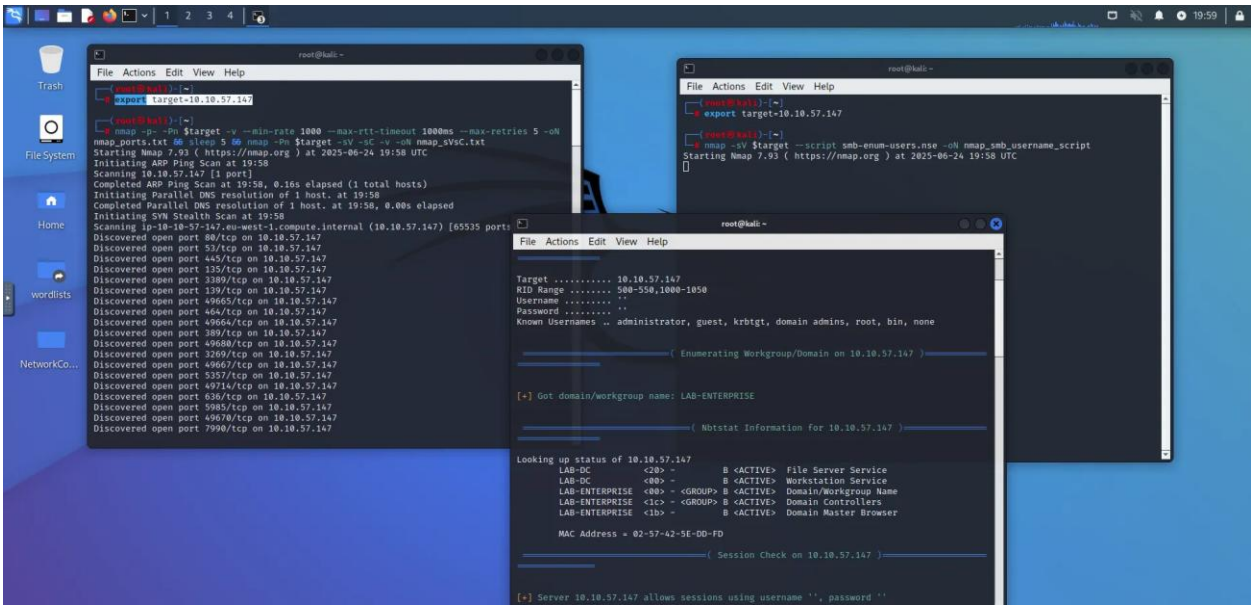
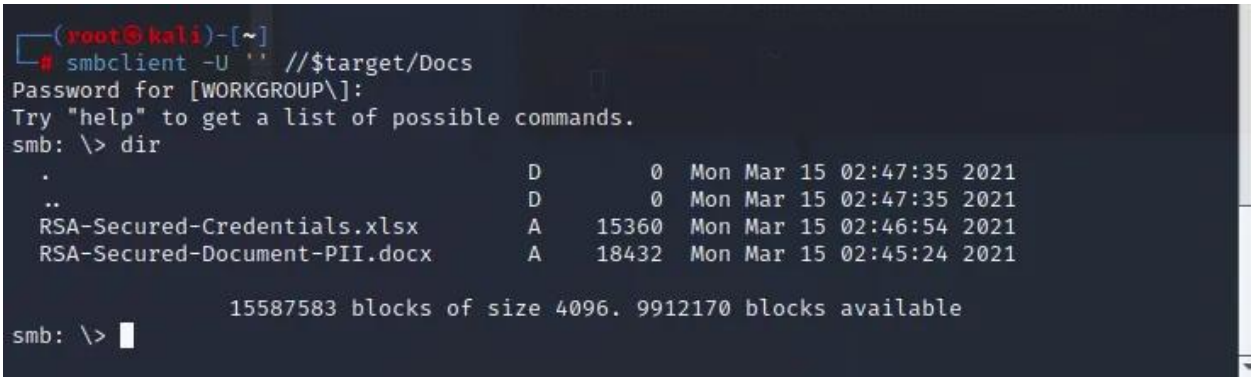
Try Hack Me room: Enterprise summed up, mainly for the OSCP practice. I was able to get the root user, but the payload didn’t work in the environment. Most likely a user error. But after getting in, it wasn’t as bad.

Step one: Enumeration



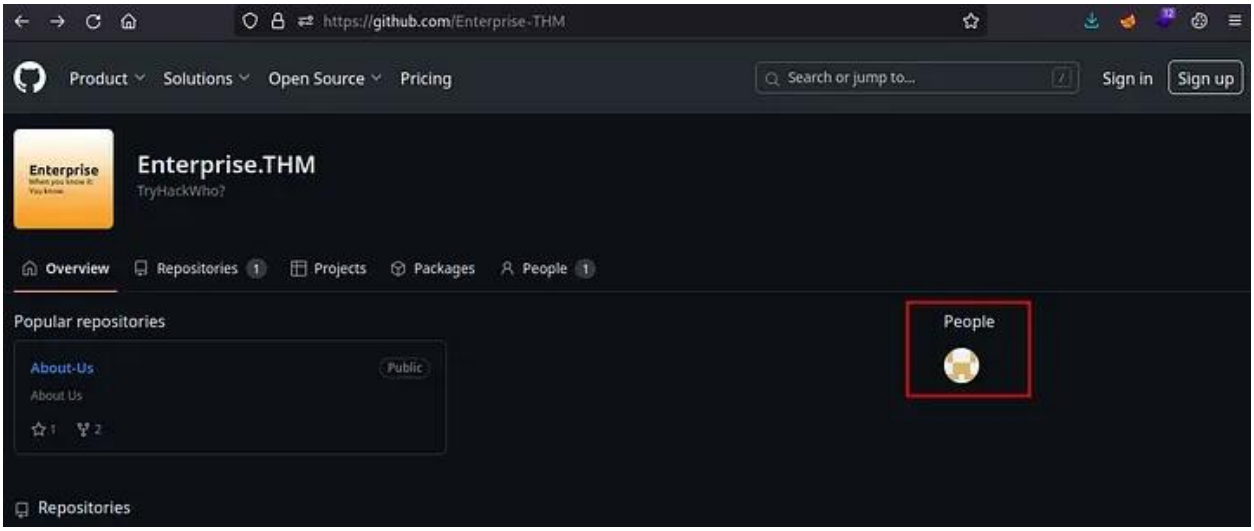
I discovered this was a domain server, so I focused primarily on SMB. This is the real goal, anyhow, getting on an AD machine.

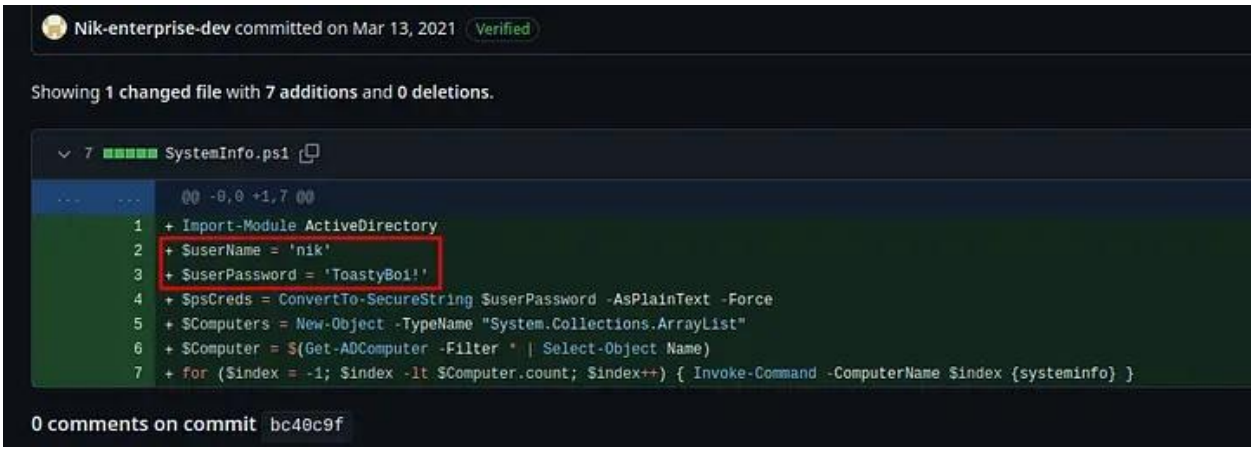


```
┌──(root㉿kali)-[~]
└─# smbclient -U '' //$target/Users
Password for [WORKGROUP\]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   DR        0  Fri Mar 12 02:11:49 2021
  ..                                  DR        0  Fri Mar 12 02:11:49 2021
  Administrator                        D        0  Thu Mar 11 21:55:48 2021
  All Users                        DHSrn        0  Sat Sep 15 07:28:48 2018
  atlbitbucket                         D        0  Thu Mar 11 22:53:06 2021
  bitbucket                            D        0  Fri Mar 12 02:11:51 2021
  Default                            DHR        0  Fri Mar 12 00:18:03 2021
  Default User                     DHSrn        0  Sat Sep 15 07:28:48 2018
  desktop.ini                        AHS      174  Sat Sep 15 07:16:48 2018
  LAB-ADMIN                            D        0  Fri Mar 12 00:28:14 2021
  Public                              DR        0  Thu Mar 11 21:27:02 2021

                15587583 blocks of size 4096. 9911034 blocks available
smb: \>
```

By pure luck, I got the guest account without issue. But I was a bit lost until I went on port 7990. This had Atlassian on it but that lead down a rabbit whole on access until part this learning curb, had a git hub account (this most likely won't be covered or tested in the oscp but part of this challenge is using OSINT).



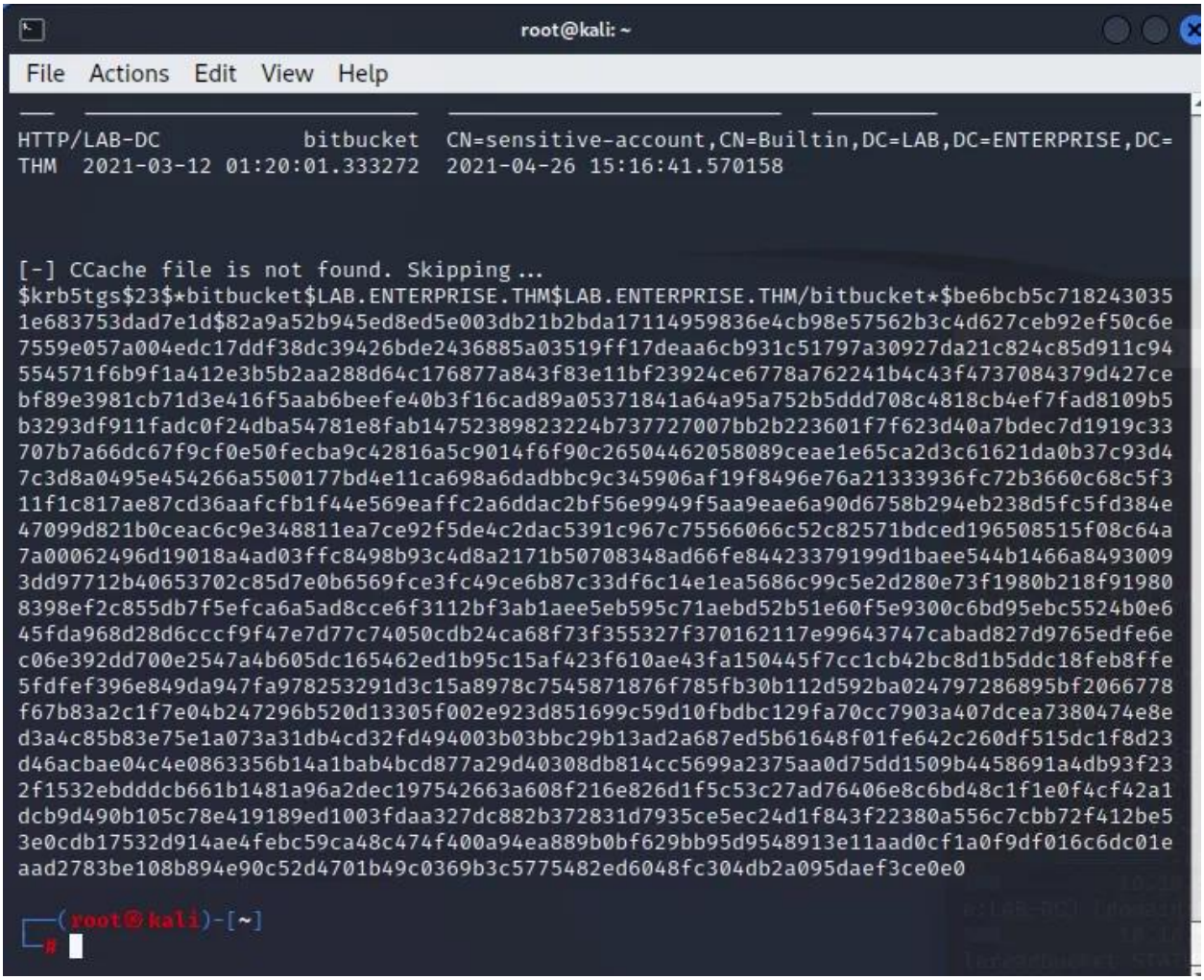


Got a set of credentials next, now that they were there, I went to dump any hashes or users but found my first

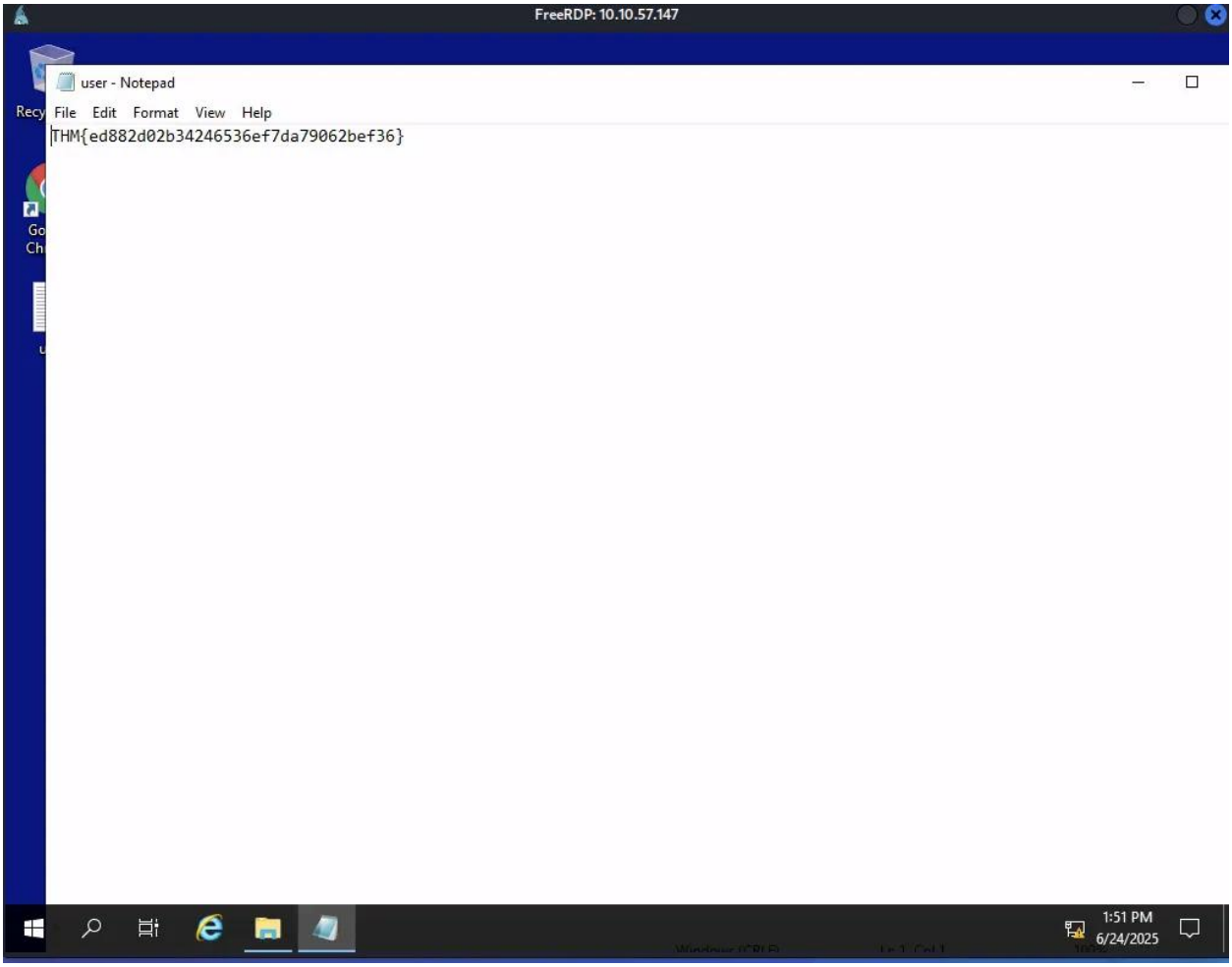
User:

```
Brute
Administrator
Guest
krbtgt
Domain
Domain
Domain
Domain
Domain
Cert
Group
Read-only
Cloneable
Protected
Key
RAS
Allowed
Denied
atlbitbucket
LAB-DC$
DnsAdmins
DnsUpdateProxy
ENTERPRISE$
bitbucket
nik
replication
spooks
korone
banana
Cake
Password-Policy-Exemption
Contractor
sensitive-account
contractor-temp
varg
adobe-subscription
joiner
```

Nik was a user on the domain, the next thing to test was kerbroasting.

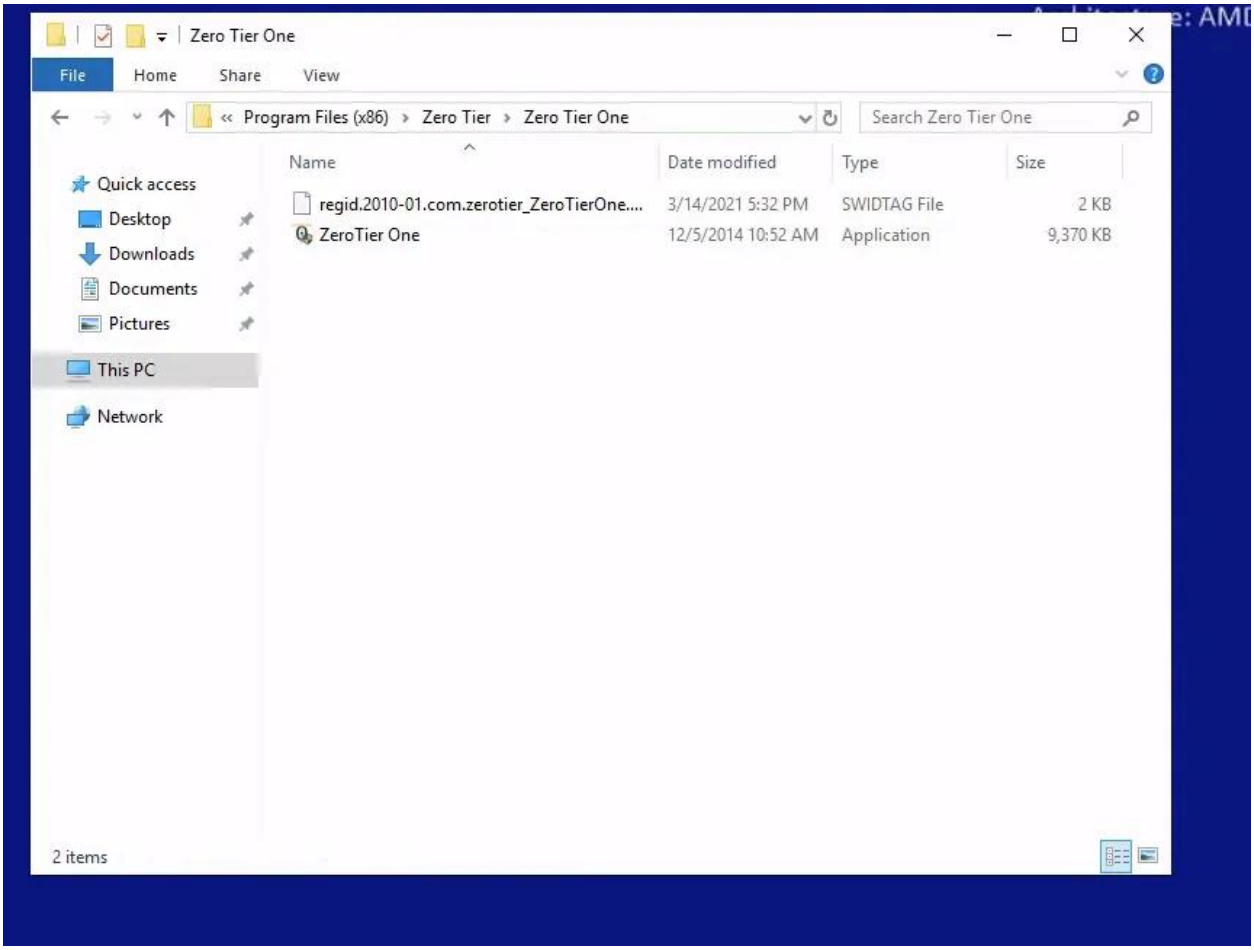


I got a hash, and this user's password was Bitbucket: the little red bucket, which was easily cracked with the RockYou list. RDP was next to try since that was open and I was able to get on the server with bitbucket:



Got the first flag, but next was the privilege escalation:

Moving around the folder for software and dll's found a zero tier install



https://security.snyk.io/vuln/SNYK-UNMANAGED-ZEROTIERZEROTIERONE-2636060

Looking here to exploit it, but also researching the issue a bit more. Rated high as 8.8. Bitbucket had all rights to the services, at that point, I just needed to make an revserse shell from msfvenom and get on the server and get the flag for root.

Crital issues CVE-2022-1316 and weak passwords.