

Forum: [Hack Forums](#)

Thread: [Forensics WorkShop](#)

CyberStrike - March 8, 2018, 3:45 am

Requirements:

Linux

Volatility

rekall

strings

Autopsy/foremost/DFF

AntiVirus

pdf-parser

pdftinfo

sha256sum

Google

<http://jsunpack.jeek.org/>

<https://blog.didierstevens.com/programs/pdf-tools/>

Machine : Windows XP

Resources:

<https://github.com/volatilityfoundation/volatility/wiki>

<https://www.howtoforge.com/tutorial/how-to-install-and-use-volatility-memory-forensic-tool/>

https://downloads.volatilityfoundation.org/releases/2.4/CheatSheet_v2.4.pdf

Image: https://www.honeynet.org/challenge2010/downloads/hn_forensics.tgz

Scenario: At your work there was a breach, so far one machine has been compromised now management wants you to put your skills to work and figure out what happened.

1. List Processes running on the victim machine
2. List all connections on victim machine
3. List all urls, note any suspicious urls
4. Management believes that the local Administrator password may have been compromised, find and crack the password. Ensure it is a good password
5. Locate any files that can be recovered from memory if you were able to recover these files were they safe?
6. What command's were issues to our victim machine if any?
7. Are there any Event Logs that can be recovered?
8. Anything suspicious in the Registry?

(This originally was released in 2010, now a few things are different for our work so we can actually focus on learning. Since it will be quite a bit of informatoin maybe hastebin/ghostbin/pastebin can be used, when you are done)

sophrosyne - March 8, 2018, 5:27 am

This is a very nice thread man. Good challenge for people. I sent you a PM if you don't mind getting back to me.

CyberStrike - March 8, 2018, 6:09 am

Awesome I hope that we get some people to participate, I will post the solution on Monday, as to give others time to get familiar. While this might not be so much in the "hacking" as in exploits or payloads, still it gives one the perspective of what an analyst/investigator would look at when they analyse memory, which now a days is very much used in the field. Although before 2008 or so it was considered common practice to turn off a compromised machine by pressing the power button or pulling the plug this has changed. So hopefully, although perhaps this isn't the best way to introduce a new user to Digital Forensics and Incident Response, often times being thrown into a situation is very important to developing skills in a short amount of time.

I urge everyone to at least try, if you get stuck it happens post a response lets figure it out. Best of luck to all.

Edit: Just finished... whew that was 4 hours of goodness, as I said I will be waiting till Monday. Also you don't need Kali or DEFT/CAINE (Forensics/IR geared Linux Distros) I was able to do everything on Ubuntu. PDF-Parser after download worked with no issues.

Tips: use psxview/ps tree also timeliner will help greatly in showing events as the system fell and in figuring this out. Remember this is a Windows XP machine so some volatility commands may not apply meanwhile other commands are perfect also appears as though our user visited a "bank" site.

CyberStrike - March 12, 2018, 1:44 am

Due to the amount of downtime on Sunday perhaps we can push this back to Wednesday.

CyberStrike - March 14, 2018, 3:11 am

Foreword: Vmem is basically going to be a memory dump of a virtual machine. Using various free tools you can dump processes as well as all the ram, which can be rather time consuming, of a machine. This can be done in both Windows as well as NIX

Extracting the tgz file

```
tar xvf hn_forensics.tgz
```

Now we can start working with our file there is a lot of output so we want to output to text using ">> file.txt". But before we do that lets see what all volatility has we use 'volatility --info | less' in another terminal to make our lives easier or you can use "man volatility"

1. Using volatility pscan also I used ps tree as well as psxview we find our processes are:
2. connscan/connection/

<https://pastebin.com/t0sxjxWW>

3. using strings filename | grep "^http://" | sort | uniq we get our urls:

<https://pastebin.com/Bs4eeaLY>

From the sites we see our employee visited a banking site, which looked interesting we remember that for later as we will recover this file from the memory as seen below

938bf771e971f1ae16cc5e93687d1669efccb3ab538d3dbba96f5a626608d326 executable.644.exe

But winlogon is started after our employee decided to download the pdf. So we can assume it's probably infected.

4. Dumping passwords isn't too hard we use hashdump feature of volatility and for cracking we use john; remember that the Guest generally is not enabled and is a blank password.

```
volatility hashdump -f Bob.vmem >> passwd
```

```
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eae8fb117ad06bdd830b7586c:::
```

```
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

```
HelpAssistant:1000:9f8ac2eaeabcd2e3a6f94d53c19803662:d95e38a172b3ddaa1ce0b63bb1f5e1fb:::
```

```
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:ad052c1cbab3ec2502df165cd25d95bd:::
```

```
john --show passwd
```

```
Administrator:PASSWORD:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eae8fb117ad06bdd830b7586c:::
```

```
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

```
SUPPORT_388945a0::1002:aad3b435b51404eeaad3b435b51404ee:ad052c1cbab3ec2502df165cd25d95bd:::
```

4 password hashes cracked, 2 left

As we can see in our report we will tell management that their admin screwed the pooch on the PASSWORD

5. Here we are going to do most of our foremost work. There is a bit of guess work but we saw a banking site and that acroread32 (PID 1752) opened and from our connections it makes a connection to an unknown site. So we need our pdf's. The first step is to memdump the resulting files will have a dmp extension, which is perfect for foremost. Our command here will be

```
foremost -i filename.dmp -t pdf -o output
```

Also it is strongly suggested using the timeliner function so you can have a good idea of how the system fell to this attack. Being that we recovered a ton of PDF's we need to figure out which PDF is the culprit using grep. (We could use pdftinfo although we can't use a wildcard such as so it is going to be lengthy.

```
grep -i java *.pdf
```

```
Binary file 00601560.pdf matches
```

Extracted PDF Analysis:

If you are wondering why we are using the -i because often we see in payloads jAvAScRiPt or any number of combinations to thwart analysis.

So when looking using pdf-parser we see :

PDF Comment

```
'%}\xffb\xb3\xec\x04\x00:\t\x00\x00\xf6\x00\x00\x00\xb4\x08\xa1\x0c\x12\xe0\x04\x000\n'
```

There is much more shellcode so it appears as though our user had gotten a pdf after the user downloaded this pdf.. so now we use an AV to check the sha256sum against VT, of course if VT doesn't have our hash we upload.

We go ahead and use sha256sum and search VT finding

<https://www.virustotal.com/#/file/0bd1a5731f70dbf77c03e09822e2b3d68a4f25064baff7371f281410114fc936/detection>

Now we use jsunpack to figure out what all of this shellcode is trying to do and what exploits are included:

malicious: Utilprintf CVE-2008-2992 detectedmalicious: collectEmailInfo CVE-2007-5659 detected

hxxp://search-network-plus.com/load.php?a=a&st=Internet Explorer 6.0&e=2 -- this is the malicious site that the payload is downloaded from

After resolving the host we have a better idea of more URLs to search for

```
hxxp://search-network-plus.com/cache/PDF.php?st=Internet%20Explorer%206.0
hxxp://search-network-plus.com/load.php?a=a&st=Internet%20Explorer%206.0&e=2
hxxp://search-network-plus.com/load.php?a=a&st=Internet Explorer 6.0&e=1
hxxp://search-network-plus.com/load.php?a=a&st=Internet Explorer 6.0&e=2
hxxp://search-network-plus.com/load.php?a=a&st=Internet Explorer 6.0&e=3
```

(Note this is an old host dnstrails can help but this was a very old host)

Using pstree to find program run under other programs:

Volatility Foundation Volatility Framework 2.6

```
.. 0x81e5b2e8:winlogon.exe          644   548   21   521 2010-02-26 03:34:04
UTC+0000
```

```
... 0x82256da0:services.exe        688   644   16   293 2010-02-26 03:34:05
```

UTC+0000

```
... 0x82129da0:lsass.exe           700   644   22   416 2010-02-26 03:34:06 UTC+0000
```

Volatility Foundation Volatility Framework 2.6

```
. 0x82068020:firefox.exe           888  1756    9   172 2010-02-27 20:11:53 UTC+0000
```

```
.. 0x820618c8:AcroRd32.exe         1752   888    8   184 2010-02-27 20:12:23 UTC+0
```

Now we figure out what the file is that got dropped using filedump:

DataSectionObject 0x82264028 644

\Device\HarddiskVolume1\WINDOWS\system32\sdra64.exe

volatility filesan -f Bob.vmem | grep sdra

Volatility Foundation Volatility Framework 2.6

```
0x000000000230ff28    1    0 -WD--- \Device\HarddiskVolume1\WINDOWS\system32\sdra64.exe
```

```
0x0000000002464028    1    1 R----- \Device\HarddiskVolume1\WINDOWS\system32\sdra64.exe
```

We now we see where the file was dropped to disk and later we will hivescan the registry for two things one figure out what has been changed and also we can get some indicators of compromise (IOC) so we can now create YARA ruleset to scan files being downloaded by users and block malicious files.

Now a quick run to various Google and threatfeeds we are looking at Zeus Bot

https://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99&tabid=2

Using foremost we go ahead and extract all exe's for that PID 1752

```
foremost -i 1752.dmp -t exe -o exe
```

Then using grep we search for our payload file

```
grep "^http://" | uniq -u
```

Binary file 00000016.exe matches

A quick sha256sum gives us:

```
sha256sum 00000016.exe
```

```
94aa18f7e5961469acd1e80805a5ef8a0a804bd85e99fe927cd00eaff23429bd 00000016.exe
```

We plugin our sha256sum into VT

<https://www.virustotal.com/#/file/94aa18f7e5961469acd1e80805a5ef8a0a804bd85e99fe927cd00eaff23429bd/detection>

6. Here we will be using our cmdline and cmdscan, this is helpful because if we start finding lots of commands like "net users" and so on we can tell if in fact we got an attacker who had enough time to start issuing commands, perhaps continuing down the kill chain for further exploitation.

<https://pastebin.com/h2wMF9Qd>

7.EventLogs were recovered Secevents/AppEvents/SysEvents

8. Registry hivescan/hivedump/hivelist will be our tools here

Remember that winlogon.exe is also infected it is running from memory with no file on disk, it is was really winlogon I would think it'd be on disk.

Now we have an idea where we are looking from hivelist, lets dump that hive we know what we will be looking for winlogon.exe and or sdra64.exe as well so after we dump we are going to grep for our results. Dumping the hive will take a while so keep that in mind.

```
volatility dumpregistry -f Bob.vmem --dump-dir text/registry/
```

```
grep -i winlogon
```

```
Binary file registry.0xe1035b60.system.reg matches
```

```
Binary file registry.0xe1526748.software.reg matches
```

```
Binary file registry.0xe15a3950.default.reg matches
```

```
Binary file registry.0xe17a3820.NTUSERDAT.reg matches
```

```
Binary file registry.0xe17deb60.NTUSERDAT.reg matches
```

```
Binary file registry.0xe1de0b60.NTUSERDAT.reg matches
```

```
grep -i userinit *  
Binary file registry.0xe1035b60.system.reg matches  
Binary file registry.0xe1526748.software.reg matches
```

Now we know were the keys we need to focus on are going to be looking at we can use multiple tools more than just volatility like reglookup

<https://pastebin.com/51Y7YU4h>

Now I had issues with using Volatility and printkey I was only seeing subkeys either way we have to be comfortable with using anything to get our mission accomplished

Now we have clear proof that we know that we were on the correct path as to be able to quickly craft a powershell script to remotely test-key to see if the path is on other machines, in addition with our sha256sum we can quickly see what programs are loaded in memory and get ourselves the sha256sum values for all the programs as to prevent further compromise. Also we can now go ahead and craft up YARA rules and block hosts to filter such malicious files before they are transfered and compromise a user, and if a user was to open a compromised PDF and this same payload was going to be dropped we can prevent it from doing so.

Edit: Yes I went a bit above by extracting out the payload from memory which was not required, but it's important that users do see that your payloads and everything is fair game to an analyst. Let us remember that there is a good percentage of InfoSec professionals who have been hired much like privateers to strike back at hackers.

Korvo - March 16, 2018, 6:48 pm

Wow man..this is def an awesome challenge. Got me motivated to get back to learning forensics.

Now I don't know half of the stuff you listed, but it looks a hellu interesting. Might have to give this a crack sometime. Looking forward to seeing more of these, keep up the great work.

CyberStrike - March 17, 2018, 6:24 am

(Mar 16, 2018 06:48 PM)Megatrøn~?? Wrote: [\[CITE\]](#) Wow man..this is def an awesome challenge. Got me motivated to get back to learning forensics.

Now I don't know half of the stuff you listed, but it looks a hellu interesting. Might have to give this a crack sometime. Looking forward to seeing more of these, keep up the great work.

When you see that the tools are not hard to use, and really best thing is hands on, just reading doesn't get us to that point of proficiency you know. Like I had issues with volatility getting the registry keys, that's fine I used reglookup. Keep in mind that this is just an everyday Ubuntu not anything like DEFT/CAINE/SANS Sift or any distro geared at forensics. Also grep/stirngs are invaluable to parsing through a lot of information quickly, none of that was rocket science just using commands we all know, If you want maybe next week we can do another. I can probably get us another RAM dump or image maybe something where we just focus on having a pcap and recovering files from it.

Originalkillit - July 6, 2018, 9:27 am

Nice thread buddy soon I will be getting my hands on this

CyberStrike - July 7, 2018, 1:18 pm

(Jul 6, 2018 09:27 AM)Originalkillit Wrote: [\[CITE\]](#) Nice thread buddy soon I will be getting my hands on this

Give it a shot, I think that this memory dump is still up, you will find that memory forensics takes a bit of time but also pretty fun, it helps you see how others attack and improve yourself.

CheGuevara? - September 30, 2018, 8:52 pm
Doing good work Silentwatch ?

CyberStrike - September 30, 2018, 9:21 pm
(Sep 30, 2018 08:52 PM)CheGuevara? Wrote: [\[CITE\]](#) Doing good work Silentwatch ?
Thank you, I have found that when it comes to forensics you want to be somewhat well rounded and being a competent attacker is extremely helpful also.

Blackhawke2002 - October 1, 2018, 2:23 am
Man i wish i would have found this a couple days ago! would have been a great weekend project. now i'll have to see what i can do sometime this week!

CyberStrike - October 1, 2018, 8:50 am
(Oct 1, 2018 02:23 AM)Blackhawke2002 Wrote: [\[CITE\]](#) Man i wish i would have found this a couple days ago! would have been a great weekend project. now i'll have to see what i can do sometime this week!
It doesn't take too long to do it I think that this was like no more than 4hrs. Post if you have solutions/questions.

Blackhawke2002 - October 1, 2018, 5:00 pm
(Oct 1, 2018 08:50 AM)SilentWatch Wrote: [\[CITE\]](#) It doesn't take too long to do it I think that this was like no more than 4hrs. Post if you have solutions/questions.
oh sweet! thanks! i'll hit this thread up for sure

Whiz_ - October 1, 2018, 5:29 pm
Hi there,
First of all thanks a lot for posting this, though it looks like there's not much interest in this till now. You are going to give out the solutions today I guess? regardless I'll try to solve this.

CyberStrike - October 1, 2018, 5:51 pm
(Oct 1, 2018 05:00 PM)Blackhawke2002 Wrote: [\[CITE\]](#) oh sweet! thanks! i'll hit this thread up for sure
Good stuff I did this more to show the significance of what an attacker leaves behind and also to show how important being a competent attacker can lead to using those same skills in a different way.

(Oct 1, 2018 05:29 PM)Whiz_ Wrote: [\[CITE\]](#) Hi there,
First of all thanks a lot for posting this, though it looks like there's not much interest in this till now. You are going to give out the solutions today I guess? regardless I'll try to solve this.
It's already up,we did this a while back, but don't let that dissuade you from trying learning new things is always important. :

<https://hackforums.net/showthread.php?tid=5809120&pid=56810368#pid56810368>

Whiz_ - October 1, 2018, 5:54 pm
(Oct 1, 2018 05:51 PM)SilentWatch Wrote: [\[CITE\]](#) It's already up,we did this a while back, but don't let that dissuade you from trying learning new things is always important. :
Thank God, I didn't went through all the comments.
Going to try this today.

CyberStrike - October 1, 2018, 5:59 pm

(Oct 1, 2018 05:54 PM)Whiz_ Wrote: [\[CITE\]](#) Thank God, I didn't went through all the comments.
Going to try this today.
Definitely give it a shot, feel free to post your solutions/questions/issues.