

Forum:[Hack Forums](#)

Thread: [Thread here recently about a client being a honeypot?](#)

HFGreyDeadpool - January 21, 2019, 1:11 pm

It was like 4:3 resolution or something

my VMWare is 1024x768 so maybe that, unsure if that's the usual?

and maybe the mouse moved around a little bit every once in awhile but that was it.

Can anyone help me find that thread?/give me the right details on the resolution and stuff and any other additional details appreciated. I want to make a script/program/plugin not sure what to call it but to detect these and flag for my inspection or remove them.

I.M.P - January 22, 2019, 4:45 am

If you don't know what a honey pot is you probably shouldn't be ratting or botting, if your trying to make a honey pot that's different but still. HF isn't always the best answer, google exists, did you know that ?

JamesHarden - January 22, 2019, 4:46 am

(Jan 22, 2019 05:45 AM)Atroxcity Wrote: [\[CITE\]](#) If you don't know what a honey pot is you probably shouldn't be ratting or botting, if your trying to make a honey pot that's different but still. HF isn't always the best answer, google exists, did you know that ?
stop worrying about bytes and answer the fucking question

I.M.P - January 22, 2019, 4:48 am

(Jan 22, 2019 05:46 AM)JamesHarden Wrote: [\[CITE\]](#) stop worrying about bytes and answer the fucking questionI did ?

Alles auf Rot - January 22, 2019, 6:23 am

(Jan 21, 2019 02:11 PM)HFGreyDeadpool Wrote: [\[CITE\]](#) It was like 4:3 resolution or something

my VMWare is 1024x768 so maybe that, unsure if that's the usual?

and maybe the mouse moved around a little bit every once in awhile but that was it.

Can anyone help me find that thread?/give me the right details on the resolution and stuff and any other additional details appreciated. I want to make a script/program/plugin not sure what to call it but to detect these and flag for my inspection or remove them.

There are several, very usefull but simple ways to detect Honey Pots.

#1 Check if the File name is the same or contains the MD5 Hash of the file itself. Most Honeypots/Scanners name the File like the MD5 Hash of it.

#2 Make simple, random based, webrequests to websites

#3 Check if there are printers installed (Not the default ones)

#4 Try to execute "net view", get a error message back and you know its a honeypot.

#5 Check for hints that's a VM, checking processor ID's, GPU Names, check if microsoft.ini is on desktop

#6 Check if these Files exist:

Windows\system32\drivers\VBBoxMouse.sys
Windows\system32\VBBoxControl.exe
Windows\system32\drivers\vmusbmouse.sys
Windows\system32\vbboxmrnp.dll
Windows\system32\vbboxhook.dll
Windows\system32\drivers\vmhgfs.sys

#7 Check if processes running:

vboxservice
vmwaretray
vmsrvc
prc_cc
xenservice
qemu-ga

Remember, honeypots want to gain as much information as possible about the attacker, you shouldn't do anything before completing the checks. Create a random loop thread when detected, do not do anything suspicious after detecting it (no self kill/delete, etc.)

Hope i was able to help you a little

El Lobo - January 22, 2019, 6:50 am

(Jan 22, 2019 07:23 AM)Alles auf Rot Wrote: [\[CITE\]](#) There are several, very usefull but simple ways to detect Honey Pots.

#1 Check if the File name is the same or contains the MD5 Hash of the file itself. Most Honeypots/Scanners name the File like the MD5 Hash of it.

#2 Make simple, random based, webrequests to websites

#3 Check if there are printers installed (Not the default ones)

#4 Try to execute "net view", get a error message back and you know its a honeypot.

#5 Check for hints that's a VM, checking processor ID's, GPU Names, check if microsoft.ini is on desktop

#6 Check if these Files exist:

Windows\system32\drivers\VBBoxMouse.sys
Windows\system32\VBBoxControl.exe
Windows\system32\drivers\vmusbmouse.sys
Windows\system32\vbboxmrnp.dll
Windows\system32\vbboxhook.dll
Windows\system32\drivers\vmhgfs.sys

#7 Check if processes running:

vboxservice
vmwaretray
vmsrvc
prc_cc
xenservice
qemu-ga

Remember, honeypots want to gain as much information as possible about the attacker, you shouldnt do anything before completing the checks. Create a random loop thread when detected, do not do anything suspicious after detecting it (no self kill/delete, etc.)

Hope i was able to help you a little

Oh God, what have I read. This might work in 2013 and even then it would work only on shitty honeypots.

Now lets go one by one point and describe why it will not work:

#1 : Why would anyone rename the original filename. Besides if you are mass spreading your file, dropper might change the filename, installer might change the filename etc. Its bad idea to hardcode filename in the binary and nobody with who has some knowledge would do so. It can only have false positives and ergo useless detections.

#2 : This used to work, but not in a way you have described it. The proper way of doing it is, try to send a request to the nonexisting website and see will it fail. If it doesnt fail we know that we are being run in the virtual machine. This worked because honeypots would intercept request and respond to it to emulate the connection thinking that you have established the communication with the server. Its flawed in multiple ways so it wouldnt be very usefull in the wild to detect honey pots.

3# : Not everyone has a printer and I am sure there are some registered in the virtual environments along with mouse movement etc.

4# : Its silly to rely to the honeypot will have that disabled. Again a lot of false positives.

5#: Wont comment on this, one would need to compile a list of processor ids, gpu names etc and even then its flawed just as it is looking for a windows serial number bios serial number etc.

#6 & #7 : There is usually a driver that filters these files, processes and services so even if you try looking for them you wont find any.

Junx - January 23, 2019, 5:38 am

2019-01-23 10:30:04 RU | ... QYS6Z-PC(QyS6z) Windows 7 Professional(x32) 1029

3 | 0 | 0 | 0 E|A Open DL 44.7K Del

Soft name URL Username Password ReportID

MozillaFirefox <https://accounts.google.com> *****@gmail.com ***** 1029

MozillaFireFox <https://www.linkedin.com> *****@gmail.com ***** 1029
MozillaFireFox <https://www.facebook.com> *****@gmail.com ***** 1029

This is a honeypot, funny bc it even has some logs.

SUI-3183372 - January 25, 2019, 2:14 pm

(Jan 22, 2019 07:23 AM)Alles auf Rot Wrote: [\[CITE\]](#) There are several, very usefull but simple ways to detect Honey Pots.

#1 Check if the File name is the same or contains the MD5 Hash of the file itself. Most Honeypots/Scanners name the File like the MD5 Hash of it.

#2 Make simple, random based, webrequests to websites

#3 Check if there are printers installed (Not the default ones)

#4 Try to execute "net view", get a error message back and you know its a honeypot.

#5 Check for hints thats a VM, checking processor ID's, GPU Names, check if microsoft.ini is on desktop

#6 Check if these Files exist:

Windows\system32\drivers\VBoxMouse.sys
Windows\system32\VBoxControl.exe
Windows\system32\drivers\vmusbmouse.sys
Windows\system32\vboxmrnp.dll
Windows\system32\vboxhook.dll
Windows\system32\drivers\vmhgfs.sys

#7 Check if processes running:

vboxservice
vmwaretray
vmsrvc
prc_cc
xenservice
qemu-ga

Remember, honeypots want to gain as much information as possible about the attacker, you shouldnt do anything before completing the checks. Create a random loop thread when detected, do not do anything suspicious after detecting it (no self kill/delete, etc.)

Hope i was able to help you a little

I think El Lobo pretty much hit the nail on the head, but to add to what he said...

#1 What I'm currently using does not rename the executable to it's md5, rather is creates a copy of the executable, renames that to its md5, and stores it in a storage location. The executable that we are analyzing/working with does not get modified.

#2 See <https://hackforums.net/showthread.php?tid=5932297&pid=58164593#pid58164593>

#3 My household has 7 or 8 windows machines and 0 printers. Both of my desktops have NEVER been connected to a printer. If you infected my household would you then discard all of us because we don't print? I also wouldn't be surprised to learn of honeypots that connect you to a virtual print server.

#4 and #5 See <https://hackforums.net/showthread.php?tid=5932297&pid=58164593#pid58164593>

#6 and #7 I'd imagine both of these are extremely low success rates. I can't imagine many modern honeypots that don't mask these.

(Jan 23, 2019 06:38 AM)Junx Wrote: [\[CITE\]](#) 2019-01-23 10:30:04 RU | ... QYS6Z-PC(QyS6z)
Windows 7 Professional(x32) 1029

```
3 | 0 | 0 | 0 E|A Open DL 44.7K Del
Soft name URL Username Password ReportID
MozillaFireFox https://accounts.google.com *****@gmail.com ***** 1029
MozillaFireFox https://www.linkedin.com *****@gmail.com ***** 1029
MozillaFireFox https://www.facebook.com *****@gmail.com ***** 1029
```

This is a honeypot, funny bc it even has some logs.

Many honeypots do this. HoneyPoint for example, claims their honeypot includes a feature called "HoneyBees are programs that simulate unencrypted POP3 and HTTP connections, in order to create bogus authentication traffic that an attacker might sniff."