

Forum:[Hack Forums](#)

Thread: [Build a AntiVirus VMs to test FUD servers](#)

aerohacker - December 2, 2024, 5:52 am

I'm think to build some Windows Virtual Machines and install AntiVirus in each guest to test FUD servers in Realtime/Scantime.

- 1) What is better?! VirtualBox or VMWare?!
- 2) Which and how many AntiVirus it's be good to start?! I think about 10 AVs.
- 3) After copy and execute the server, would be better update the AV and disconnect the VM from Internet to avoid the AV share the stub?!

DramaKing - December 2, 2024, 5:57 am

(Dec 2, 2024 06:52 AM)aerohacker Wrote: [\[CITE\]](#) I'm think to build some Windows Virtual Machines and install AntiVirus in each guest to test FUD servers in Realtime/Scantime.

- 1) What is better?! VirtualBox or VMWare?!
- 2) Which and how many AntiVirus it's be good to start?! I think about 10 AVs.
- 3) After copy and execute the server, would be better update the AV and disconnect the VM from Internet to avoid the AV share the stub?
VMware Workstation is free now, so you should consider that.

That is a lot of VMs.

Turning off sample submission is better for the most accurate results without reporting.

Bastille - December 2, 2024, 6:00 am

That's an interesting topic but I don't think that's as simple as that, it's usually not recommended to install more than 1 AV on a computer, or at least to have them all active at the same time because they work on the same spaces and there is a chance to get errors / conflicts.

Besides, nowadays many malware have anti-VM detection, which means that you need to custom your VM to obfuscate every artifact related to virtualization (machine name, services, drivers, and so on ...)

I know that some people of HF worked on alternative of Kleenscans and so on, maybe they could share some info

aerohacker - December 2, 2024, 6:04 am

(Dec 2, 2024 07:00 AM)Bastille Wrote: [\[CITE\]](#) That's an interesting topic but I don't think that's as simple as that, it's usually not recommended to install more than 1 AV on a computer, or at least to have them all active at the same time because they work on the same spaces and there is a chance to get errors / conflicts.

Besides, nowadays many malware have anti-VM detection, which means that you need to custom

your VM to obfuscate every artifact related to virtualization (machine name, services, drivers, and so on ...)

I know that some people of HF worked on alternative of Kleenscans and so on, maybe they could share some info

1 VM to each AV (It would be separated)

The servers are mine so my intention is only to scan in realtime and scantime without to need any sites and avoid the same share the stub, and i won't use any anti in the server.

aerohacker - December 2, 2024, 6:27 am

(Dec 2, 2024 07:09 AM)m0hx Wrote: [\[CITE\]](#) no. 1 VM and multiple snapshots to different AVs i think is better to save u resources.

Yeah, I'm think about to test most popular and best AntiVirus, but I think some AVs shared the same engine.

aerohacker - December 2, 2024, 6:36 am

(Dec 2, 2024 07:29 AM)m0hx Wrote: [\[CITE\]](#) yea, i think AVG, Avast have same engine.

When a server is FUD, It doesn't matter if the AntiVirus it's default or set to maximum, the server will bypass anyway?!

DramaKing - December 2, 2024, 7:43 am

(Dec 2, 2024 07:29 AM)m0hx Wrote: [\[CITE\]](#) yea, i think AVG, Avast have same engine.

I checked to verify. Norton owns Avast, and Avast owns AVG.

(Dec 2, 2024 07:36 AM)aerohacker Wrote: [\[CITE\]](#) When a server is FUD, It doesn't matter if the AntiVirus it's default or set to maximum, the server will bypass anyway?!

Just check for the 'set to maximum' setting. ?

aerohacker - December 2, 2024, 10:14 am

(Dec 2, 2024 07:29 AM)m0hx Wrote: [\[CITE\]](#) yea, i think AVG, Avast have same engine.

Avast bought AVG and both use the same engine and even the GUI is similar.

darkterror - December 3, 2024, 12:51 am

(Dec 2, 2024 06:52 AM)aerohacker Wrote: [\[CITE\]](#) I'm think to build some Windows Virtual Machines and install AntiVirus in each guest to test FUD servers in Realtime/Scantime.

1) What is better?! VirtualBox or VMWare?!

2) Which and how many AntiVirus it's be good to start?! I think about 10 AVs.

3) After copy and execute the server, would be better update the AV and disconnect the VM from Internet to avoid the AV share the stub?!

1. Doesn't really matter, for testing purposes of samples both are sufficient, for me it comes really to user experience. (Using Oracle VM)

2. Well focus mainly on AVs you need to penetrate and which are most common. Usually from what i saw people use ootb WD (might be wrong here) or "free ones" like AVG, Avira, Avast. I would suggest to check this annual report

<https://www.security.org/antivirus/antivirus-consumer-report-annual/> for more information

10 vm with 10 avs is quite useless, i would use one of the scanning services like <https://scanner.to/> or check forum, there are other sites available as well, its not that expensive and it saves you a lot

of time, but if you are developer, than i would go for it.

3. Well, this is very hard question to answer, because some AVs collect data from scanning/detections even when you turn off sample submission. (referring to AVG in this case) more info here:

https://businesshelp.avg.com/Content/Products/AVG_Antivirus/AntivirusManagement/ConfiguringPrivacySettings.htm

3.1 You could turn off the internet to test the sample, but you would loose Cloud Based Detections which are quite strong these days so your results would be "inaccurate".

Donrulezz - December 31, 2024, 8:47 am

Based on my experience, I have observed the following:

Instead of installing multiple antivirus programs, especially for runtime scan, I recommend installing Comodo Firewall and Antivirus. You can perform a scan in runtime mode.

If the scan bypasses Comodo, it is likely to bypass all other antivirus programs in runtime as well, as, to the best of my knowledge, Comodo is the strongest in runtime detection.

DramaKing - December 31, 2024, 9:40 am

(Dec 31, 2024 09:47 AM)Donrulezz Wrote: [\[CITE\]](#) Based on my experience, I have observed the following:

Instead of installing multiple antivirus programs, especially for runtime scan, I recommend installing Comodo Firewall and Antivirus. You can perform a scan in runtime mode.

If the scan bypasses Comodo, it is likely to bypass all other antivirus programs in runtime as well, as, to the best of my knowledge, Comodo is the strongest in runtime detection.

Based on its static detection, I am very surprised.

7 - December 31, 2024, 9:45 am

QubesOS is great though for type 1 virtualisation just build the Qube and clone for multiple AV's
I personally love Qubes but you need the spec

Infinity. - October 16, 2026, 11:02 am

(Dec 31, 2024 10:45 AM)7 Wrote: [\[CITE\]](#) QubesOS is great though for type 1 virtualisation just build the Qube and clone for multiple AV's

I personally love Qubes but you need the spec

Sorry to bump this thread (also not stalking you at all) but I came to this thread from this thread
<https://hackforums.net/showthread.php?tid=6329750&pid=63012041#pid63012041>

but I am developing and very close to releasing my online AV scanner both scantime and runtime and I am curious about what you mean here.. can you elaborate?

(Dec 3, 2024 01:51 AM)darkterror Wrote: [\[CITE\]](#) 1. Doesn't really matter, for testing purposes of samples both are sufficient, for me it comes really to user experience. (Using Oracle VM)

2. Well focus mainly on AVs you need to penetrate and which are most common. Usually from what i saw people use ootb WD (might be wrong here) or "free ones" like AVG, Avira, Avast. I would suggest to check this annual report

<https://www.security.org/antivirus/antivirus-consumer-report-annual/> for more information

10 vm with 10 avs is quite useless, i would use one of the scanning services like <https://scanner.to/>

or check forum, there are other sites available as well, its not that expensive and it saves you a lot of time, but if you are developer, than i would go for it.

3. Well, this is very hard question to answer, because some AVs collect data from scanning/detections even when you turn off sample submission. (referring to AVG in this case) more info here:

https://businesshelp.avg.com/Content/Products/AVG_Antivirus/AntivirusManagement/ConfiguringPrivacySettings.htm

3.1 You could turn off the internet to test the sample, but you would loose Cloud Based Detections which are quite strong these days so your results would be "inaccurate".

why is 10 vm with 10 avs useless? There's QEMU VM pooling which should be sufficient enough to manage them without any overhead

7 - October 16, 2026, 11:24 am

(20 hours ago)Infinity. Wrote: [\[CITE\]](#) Sorry to bump this thread (also not stalking you at all) but I came to this thread from this thread

<https://hackforums.net/showthread.php?tid=6329750&pid=63012041#pid63012041>

but I am developing and very close to releasing my online AV scanner both scantime and runtime and I am curious about what you mean here.. can you elaborate?

why is 10 vm with 10 avs useless? There's QEMU VM pooling which should be sufficient enough to manage them without any overhead

Well multiple instance one computer and not on xen.. but to be honest I use proxmox now

Infinity. - October 16, 2026, 5:25 pm

(19 hours ago)7 Wrote: [\[CITE\]](#) Well multiple instance one computer and not on xen.. but to be honest I use proxmox now

Thanks I checked Qubes OS and it looks interesting