

Forum:[Hack Forums](#)

Thread: [Online Games Emulation \[Server Emulation\]](#)

KTried - February 27, 2014, 12:25 am

Hello,

Online Games Emulation [Server Emulation]

I Knew that server emulation based on that i know the packets which is sent to the server then analyse it .

then i'll have to make an application on a server that belongs to me which receive the packets etc ...

So , can anyone help me , from where to start ?

how can i analyse packets , send packets , ...

just want to know how emulators work , and how to reverse engineering online games .

Thanks

Only3 - February 27, 2014, 12:34 am

check dragonhunter threads he the only1 here that done it

ShadowCloud - February 27, 2014, 12:47 am

(Feb 27, 2014 01:34 AM)Only3 Wrote: [\[CITE\]](#) check dragonhunter threads he the only1 here that done it

Is he still around? I haven't seen him in a while.

1. Essentially you'll need to monitor the traffic to see the requests and responses (I'd suggest reading up on packet sniffers for this)
2. From there you'll need to "trick" your pc into sending the request to your server instead of the actual server (take a look at something like your host file or how DNS works)
3. Then you'd need to write the actual software/server to accept the traffic being sent (depending on your results in 1 above and then provide the desired response)
4. Test it.

KTried - February 27, 2014, 12:55 am

(Feb 27, 2014 01:34 AM)Only3 Wrote: [\[CITE\]](#) check dragonhunter threads he the only1 here that done it

All his needed threads are removed and included videos in it are removed as well .

(Feb 27, 2014 01:47 AM)ShadowCloud Wrote: [\[CITE\]](#) Is he still around? I haven't seen him in a while.

1. Essentially you'll need to monitor the traffic to see the requests and responses (I'd suggest

reading up on packet sniffers for this)

2. From there you'll need to "trick" your pc into sending the request to your server instead of the actual server (take a look at something like your host file or how DNS works)

3. Then you'd need to write the actual software/server to accept the traffic being sent (depending on your results in 1 above and then provide the desired response)

4. Test it.

Thanks , ?

But Is there any thing to start with ?

Website , Tutorial , Thread here or something else ?

ShadowCloud - February 27, 2014, 1:02 am

(Feb 27, 2014 01:55 AM)KTried Wrote: [\[CITE\]](#) All his needed threads are removed and included videos in it are removed as well .

Thanks , ?

But Is there any thing to start with ?

Website , Tutorial , Thread here or something else ?

I pointed you in the right direction so you could learn and not just copy and paste things? I'm not here to spoon feed people information.

If you have a specific question feel free to ask, but I'm not here to provide anything other than guidance, most certainly not code snippets you could copy nor Google results.

Someone else might be in that line of posting, but unfortunately unless you have a specific question, I can't help you any more than that.

KTried - February 27, 2014, 1:05 am

(Feb 27, 2014 02:02 AM)ShadowCloud Wrote: [\[CITE\]](#) I pointed you in the right direction so you could learn and not just copy and paste things? I'm not here to spoon feed people information.

If you have a specific question feel free to ask, but I'm not here to provide anything other than guidance, most certainly not code snippets you could copy nor Google results.

Someone else might be in that line of posting, but unfortunately unless you have a specific question, I can't help you any more than that.

Yes , you are right .

I Mean , What should i start with in C# Programming .

I Know the basics .

should i learn Network Programming , Reverse Engineering , etc .. ?

that's what i mean , the way i start from [i mean in programming]

Thanks again

ShadowCloud - February 27, 2014, 1:11 am

(Feb 27, 2014 02:05 AM)KTried Wrote: [\[CITE\]](#) Yes , you are right .

I Mean , What should i start with in C# Programming .

I Know the basics .

should i learn Network Programming , Reverse Engineering , etc .. ?

that's what i mean , the way i start from [i mean in programming]

Thanks again

That completely depends on what you want to do? I couldn't for a moment make a recommendation based on the information available in either this thread nor your profile. So it's impossible to say at this point, without you providing more information on what you want to do? Do you purely want to program for server emulation?

KTried - February 27, 2014, 1:19 am

(Feb 27, 2014 02:11 AM)ShadowCloud Wrote: [\[CITE\]](#) That completely depends on what you want to do? I couldn't for a moment make a recommendation based on the information available in either this thread nor your profile. So it's impossible to say at this point, without you providing more information on what you want to do? Do you purely want to program for server emulation?

- I Want to Find online games exploits .
- I Want to Program Bots [Which move , attack , etc .. by it self] . [I Mean Tools for the game] *
- And understand the emulation process , so that i can find exploits in emulators which are already done by others .

Thanks For your help btw ;)

6e756c6c - February 27, 2014, 6:28 am

(Feb 27, 2014 02:19 AM)KTried Wrote: [\[CITE\]](#) - I Want to Find online games exploits .

- I Want to Program Bots [Which move , attack , etc .. by it self] . [I Mean Tools for the game] *
- And understand the emulation process , so that i can find exploits in emulators which are already done by others .

Thanks For your help btw ;)

If you want to get into hacking games / making bots then you should learn some basics such as..

- Pointers and Offsets (Used just about everywhere.)
- Hexadecimal (Used in memory editing and packet analysis)
- Binary (Used in encryption, hashing, flags, high & low bits, etc)
- Binary Operations (Or, Xor, Not, shifting, etc. See above.)
- Basic Networking (Ports, host names, port forwarding, etc.)
- Tcp Protocol (Connecting, binding, listening, buffers, etc.)
- Udp Protocol (Probably won't need this but it may be worth looking into.)
- Memory Editing (ReadProcessMemory and WriteProcessMemory)
- Sending Input (SendInput, SendMessage, etc. For simulating KB&M)
- GDI+ (CopyFromScreen, can be useful when sending input)

I suggest you start off with something simple, like flash games. You have a long road to travel and it's going to be a while until you are able to do what you want but just hang in there and stick to your guns. :)

Tools:

HxD (Hex editor for files and memory)
WireShark (Packet analyzer)
WPE Pro (Packet analyzer and editor)
Cheat Engine (Memory editor and searcher)

DragonHunter - February 27, 2014, 11:14 am

(Feb 27, 2014 01:47 AM)ShadowCloud Wrote: [\[CITE\]](#) Is he still around? I haven't seen him in a while.

1. Essentially you'll need to monitor the traffic to see the requests and responses (I'd suggest reading up on packet sniffers for this)
2. From there you'll need to "trick" your pc into sending the request to your server instead of the actual server (take a look at something like your host file or how DNS works)
3. Then you'd need to write the actual software/server to accept the traffic being sent (depending on your results in 1 above and then provide the desired response)

4. Test it. Yep I'm still around here coding 'n doing stuff ? mostly only posting to threads when it's sometimes interesting

For reverse engineering the network you mainly only need WireShark which is the 1 I'm using to analyze traffic and to create Man-In-The-Middle Attack programs in C#

What I mostly do is checking if the x amount of packets are like having headers and static data
Well the first few requirements you need is a good understanding of Reverse Engineering, Assembly(most normal games are native), Networking

These requirements are written down in a small list but there is a lot more to play with since games could be packed, obfuscated etc

Game Server Emulators are pretty much servers which are emulating the real server

Oh well if you wanna see a little from my work, mainly MITM but oh well ?

<https://hackforums.net/showthread.php?tid=4048467>

<https://hackforums.net/showthread.php?tid=3166960>