Forum:Hack Forums

Thread: MetaSploit framework vs Community

CyberStrike - *October 10, 2017, 2:59 pm*

Well I am looking into starting my own security company money is a bit tight, so spending 2500 for express or Cobalt Strike would be hard in the first year, until I get a contract or two. So I have looked at ExploitPack for 1600 which is the cheapest option yet most people start with msf or community. So they would be comfortable although it wouldn't be the most efficient thing going on, although we are not going to use pirated software so everything has to be legit.

I should tell you that I plan on doing full pentests just vulnerability scanning honestly while it is not as fun and it really ends up being how much of your report can you export into excel isn't really what I want to do. Also I want to do Adversarial Simulations for clients, so our techniques will be closely modeled after APT groups. I plan on having a total of four pentesters (1 dedicated coder will be in the bunch) in the beginning including myself. Lets assume that I have 5000 dollars to start this up with. If I get my guys brand new laptops we are looking at 3200 dollars taken out of that budget, assuming that they go for 800 a piece, which would leave 1800. I could also look into getting cheaper laptops that is an option I am willing to explore.

We look at getting a VPS a couple of IPs and a couple of domains we are up to maybe 240 or so . So now at 1560 or so. I am sure that we will need wifi adapter here and there as well as notepads, a bit of advertising maybe 50-100 per month. Have to be a monthly basis till the first couple of clients. So lets say we are at 1200. We probably would need a dedicated business line for our internet, which will eat up a bit more money about 100-200 per month. One thing I will spend the cash on is going to be Burp Suite Pro at 150 a pop.

Keeping this in mind which would you go with if you were to create your startup Metasploit FrameWork or Community or would you hold to save up more money or start a crowd funding campaign?

Spacefiller - *October 10, 2017, 3:48 pm*

I personally use MEtasploit Framework, because it comes preloaded with all of the exploits, and I am not afraid of the command line. Community, I have never used, but I heard it has a GUI. IMHO, Cobalt Strike is just a fancier Armitage with 0days. I do like your idea though, and you would be right for it to be expensive, but it doesn't have to be. Buying all of these pre-made tools are expensive because they don't want people who don't know what they are doing having these powerful tools. Usually if you have that much money to buy a more powerful version of MS, you will get better exploits, because people there don't upload shit to virustotal.

If you are ever planning on taking in a remote member, or you just happen to be located in Augusta, GA, hit me up, I'd like to be a part of this :)

CyberStrike - *October 10, 2017, 4:23 pm*

SpaceFiller yeah metasploit community/express/pro all can use a web interface. Express and Pro can help automate exploitation.(exploits aside) You can still have a CLI in msf express and pro. I'd really hate to come across as a cheap SOB or not having my act together, but I am absolutely looking into starting up.

13uNkNoWn - *October 10, 2017, 6:47 pm*

(Oct 10, 2017 04:23 PM)sirru5h Wrote: [CITE] SpaceFiller yeah metasploit community/express/pro all can use a web interface. Express and Pro can help automate exploitation.(exploits aside) You can still have a CLI in msf express and pro. I'd really hate to come across as a cheap SOB or not having my act together, but I am absolutely looking into starting up.
I think if it was easy to get into this without:
A. Knowing how to do this stuff manually in combination with using free open source tools.

B. Having money to buy tools or pay someone to work with you.

Then a lot more people would be doing this and making money.. myself included...

There are all kinds of lists of free vulnerability scanners out there... actually exploiting targets is not something your gonna find cheap or free... otherwise everyone would be using those tools and having a field day and most exploits would get patched fairly quickly due to all the exploiting going on..

CyberStrike - *October 10, 2017, 7:12 pm*
Well the manual option I am comfortable with and have done the manual stuff for say privilege escalation from User to Local Administrator on the target machine, then manually do post exploitation, persistence then go from local Admin to Domain/Enterprise Admin . If it takes me an extra week to manually do an engagement manually then that is what it would have to be. At least until I have enough for tools to automate exploitation and post exploitation. So 13uNkNoWn what do you think time factor trade off with manually (time/money of doing it by hand), should I hold until I can properly fund my start up?

13uNkNoWn - *October 10, 2017, 8:17 pm*
(Oct 10, 2017 07:12 PM)sirru5h Wrote: [CITE] Well the manual option I am comfortable with and have done the manual stuff for say privilege escalation from User to Local Administrator on the target machine, then manually do post exploitation, persistence then go from local Admin to Domain/Enterprise Admin . If it takes me an extra week to manually do an engagement manually then that is what it would have to be. At least until I have enough for tools to automate exploitation and post exploitation. So 13uNkNoWn what do you think time factor trade off with manually (time/money of doing it by hand), should I hold until I can properly fund my start up?
You seem like you have a good plan, so I'd suggest you should do what you ARE capable of, and not have too much expectations at this point. Then you can't fail in my opinion.

If you haven't already, maybe just start off as a consultant of sorts, gain more of the real world experience, because nothing beats that. Once you've gotten a few consults under your belt then I'd look at making a legit business out of it.

Now I am by no means experienced in the business side of this myself, I just have a 5+ year background in sysadmin for 2 companies...
I'm just adding my 2 cents.

Oh and I dunno if google still offers it, but when I signed up for the free trial of their cloud stuff, they gave $300 in free money towards the offerings once the trial is over, which is great for hosting a simple web page, or google ad-sense etc

CyberStrike - *October 10, 2017, 8:38 pm*
(Oct 10, 2017 08:17 PM)13uNkNoWn Wrote: [CITE] You seem like you have a good plan, so I'd suggest you should do what you ARE capable of, and not have too much expectations at this point. Then you can't fail in my opinion.

If you haven't already, maybe just start off as a consultant of sorts, gain more of the real world experience, because nothing beats that. Once you've gotten a few consults under your belt then I'd look at making a legit business out of it.

Now I am by no means experienced in the business side of this myself, I just have a 5+ year background in sysadmin for 2 companies...
I'm just adding my 2 cents.

Oh and I dunno if google still offers it, but when I signed up for the free trial of their cloud stuff, they gave $300 in free money towards the offerings once the trial is over, which is great for hosting a simple web page, or google ad-sense etc
I apologize if I came across dismissive and I understand the points you have brought up, I currently do work as a pentester, and I am in the exploratory phase hence why I seek the opinions of others, and 13uNkNoWn I do value the points you brought up. Consulting maybe an option although my contract with my current employer prohibits it, which would mean I would end up leaving. I will check on the Google Cloud pricing and I appreciate the recommendation, thank you.

notluther - *October 12, 2017, 6:43 am*
(Oct 10, 2017 07:12 PM)sirru5h Wrote: *[CITE]* Well the manual option I am comfortable with and have done the manual stuff for say privilege escalation from User to Local Administrator on the target machine, then manually do post exploitation, persistence then go from local Admin to Domain/Enterprise Admin . If it takes me an extra week to manually do an engagement manually then that is what it would have to be. At least until I have enough for tools to automate exploitation and post exploitation. So 13uNkNoWn what do you think time factor trade off with manually (time/money of doing it by hand), should I hold until I can properly fund my start up?
If this is the case I would recommend that you follow through with it. Focus on your strengths and worry about your weaknesses (not having automated tools, etc) when the time comes for you to step your game up. I'm no business person by any means, but I don't see why a company that values their security wouldn't take you up on your offer for the right rate, week long engagement or not.

sulphur - *October 12, 2017, 2:38 pm*
Hello Guys,

I have one question guys, so if in real world you a re conducting a pentest as a service for a client and using MSF which comes pre-loaded with Kali, do you have to pay for using the Metasploit framework or not?

Thanks.

JebronLames - *October 12, 2017, 6:33 pm*
just out of complete curiosity did you have a specific laptop that you were planning on buying?
very random just curious.

notluther - *October 12, 2017, 8:17 pm*
(Oct 12, 2017 02:38 PM)sulphur Wrote: *[CITE]* Hello Guys,

I have one question guys, so if in real world you a re conducting a pentest as a service for a client and using MSF which comes pre-loaded with Kali, do you have to pay for using the Metasploit framework or not?

Thanks.

No, the version of Metasploit included in Kali is the community edition, which is free, just like the rest of the operating system.

CyberStrike - *October 13, 2017, 12:56 pm*

(Oct 12, 2017 06:43 AM)Ed25519 Wrote: [CITE] If this is the case I would recommend that you follow through with it. Focus on your strengths and worry about your weaknesses (not having automated tools, etc) when the time comes for you to step your game up. I'm no business person by any means, but I don't see why a company that values their security wouldn't take you up on your offer for the right rate, week long engagement or not.

Most full on pentests we do usually go for a month that includes recon, honestly a majority of a pentest is recon usually you are looking at 1 week maybe 2 weeks or actual from initial compromise to finish where we have full penetrated the network. So if it takes me an extra week to finish that portion I would ensure that the client knows that we are looking at a 5 week time frame, also I thought about the reasonable fee although it may take me an extra week I wouldn't pass that cost onto the client. I think an average for say medium sized business they pay about 25-30k for a one time pentest I was thinking I keep my prices reasonable (20K) for that one time pentest. i do want to do a bit more research on it, but with in one or two clients I can afford tools in short order.

Quote:just out of complete curiosity did you have a specific laptop that you were planning on buying?

very random just curious.

mmm nothing particular but if you are looking for a machine that will just work with linux look at chrome books. I had a buddy who picked up an HP machine about 6 months back with a 17 inch screen it's not a top of the line machine but he sold it to me for 40 bucks, then a couple of days later he called me with problems on his other machine so after fixing that he gave me back my 40 bucks. 17" screen and AMD CPU. WiFi works although I have a dedicated machine just for wifi pentesting. I am only running linux and took off Windows.

H3LL2 - *October 21, 2017, 2:33 am*

Being excellent in what you're doing doesn't translate the same when doing a business. You are focused on dealing with clients (which you might already be doing), negotiations (when your clients say they don't have budget), HR (how you want to deal with your own staff), financial planning (will you be able to cover your expenses with 1 or 2 clients a month, usually staffs are the costliest expenses)

CyberStrike - *October 22, 2017, 10:39 pm*

Well most companies they have their sales people who handle the negotiations/contracts generally you want one team member being there and I try to be the guy who goes either for face to face or video/phone conference at work right now so I can get some grasp for how sales does their thing.

FractumSeraph - *October 23, 2017, 12:50 pm*

I feel like you could save money on your laptops.

You can get an i7-7500 with 8gbs of RAM for around $570.

I can't see much benefit to any other laptops until you get in the $1000+ range. And you'd be saving enough money to buy everyone a WiFi Pineapple/Bash Bunny and still be under your $800 estimate.

I'm not working in the field myself, so take this with a grain of salt.

CyberStrike - *October 23, 2017, 3:34 pm*

(Oct 23, 2017 12:50 PM)Fallen Archangel Wrote: [CITE] I feel like you could save money on your laptops.

You can get an i7-7500 with 8gbs of RAM for around $570.
I can't see much benefit to any other laptops until you get in the $1000+ range. And you'd be saving enough money to buy everyone a WiFi Pineapple/Bash Bunny and still be under your $800 estimate.

I'm not working in the field myself, so take this with a grain of salt.
Pimp !!! That is a good find I appreciate it. That'd save about 900 bucks.

/wrists - *October 25, 2017, 10:08 am*
(Oct 12, 2017 02:38 PM)sulphur Wrote: *[CITE]* Hello Guys,

I have one question guys, so if in real world you a re conducting a pentest as a service for a client and using MSF which comes pre-loaded with Kali, do you have to pay for using the Metasploit framework or not?

Thanks.
No. You answered your own question.