Heather:

Welcome to the Hurricane Labs podcast. I'm Heather, and today we're going to be talking about open source security tools. Joining me, I have Eric, Josh, and Kurt from our SOC team to share what some of their favorite tools are. Thanks for joining me guys. I appreciate it. Why don't you go ahead and introduce yourselves and then we'll dive in.

Eric:

I'm Eric Patterson. I'm one of the SOC Tier 1 team leads here at Hurricane.

Josh:

Josh Neubecker, SOC architect.

Kurt:

I'm Kurt. I'm another one of the architects here at Hurricane labs.

Heather:

Before we get into the specific tools. Can you tell us a little bit about why open source specifically? What benefits do open source tools offer?

Kurt:

I like the features that the open source tools have to offer for them, on top of it being free. I mean, that's-

Josh:

Usually free.

Kurt:

Yeah.

Eric:

Yeah.

Kurt:

You can get some pretty decent products that work well, if you find bugs in it, you can submit bugs and have individual-

Eric:

A better collaboration.

Josh:

Yeah. Usually, the benefit of open source, is having a lot of eyes on the software, and it being secure, although it's not true for all open source projects, like Log4j, I'll mention.

Kurt:

I was literally just about to say, "Well, that was open source."

Eric:

Yeah. One of the things to always remember also with open source is never use any default passwords that are included in their configs. Always make sure you're changing that to something, personal.

Kurt:

That goes for anything, man.

Eric:

Yeah, anything, but especially using any kind of git open source software.

Heather:

All right. Let's go ahead and start with some of your favorite tools for just basic security measures. And then we'll look a little bit more specifically at testing attacks, and detections, and researching IoCs. What are your favorite tools to use when setting up or strengthening your security stance?

Eric:

Well, as far as for me, one of the things I like a lot, is a good password manager. It can definitely help, and keep an environment more secure, not having your users writing things down, or keeping things stored in plain text. And, as far as a good open source password manager, Bitwarden has always a go-to for me with that. It offers a pretty robust encryption, with salting, and pretty deep encryption on it. And, it also allows for OnPrem hosting, if you'd like to put it on your own Linux server, store it on-prem, have your own instance of it, manage it yourself, you can do that, or you can use the cloud-based service that they offer for free, which is very secure, and hosted very well. I've never had issues with it. They also have Android apps that tie in very well with it, and browser extensions that work great. It's a nice alternative to LastPass, which has shifted recently in their pricing model. And now, especially for personal use requires you to either use mobile or desktop, and if you want to use both, you have to pay. Whereas, Bitwarden, you can run it yourself, keep it free, and not have to worry about that.

Kurt:

I'll tell you what though, as far as Bitwarden, because I also use it personally, the mobile app does a fantastic job from the phone. I've had no problems with it. You can set up to unlock with your fingerprint, and from there you simply have it input or even create passwords for apps, as well as things on your browser.

Josh:

Yeah. I like the interface for it on the mobile link, even better than something like LastPass, and the sharing on it is also great.

Eric:

Yeah. It's definitely a lot cleaner interface.

Josh:

As far as general recommendations for security for everyday people, uBlock is open source, protect you from a lot of the nonsense on the internet.

Kurt:

Not only that, man, it makes YouTube not suck.

Eric:

Yeah. I would highly recommend uBlock, especially the ability to add custom block lists from various sites, there's a lot you can do with it, and it definitely is a big form of protection for-

Kurt:

I just think for even usability on sites, put the whole protection aspect out the window, if you turn that off and go to majority of websites... Hell, if you went to a news page website, the amount of intrusive advertisements and everything, that's just blasted everywhere, I'd say uBlock does a pretty good job getting rid of all that.

Eric:

Oh yeah. It's so effective. I've seen, there was a recent court case where people, they were trying to say that uBlock, and similar ad blockers were copyright infringement, because they were changing the structure of the website by blocking the ads, but that got tossed out.

Kurt:

Good, because literally what they do with some of the ads, is almost similar to malware in some ways, and how interested they can be on your browser. To fight the stupidity of ads.

Josh:

And, it doesn't just block ads either. It also will protect you from phishing, and malware. It maintains block lists for those as well, just shady sites.

Eric:

Yeah. It's definitely something, anytime I get a new PC or a new laptop or anything, it's the first thing I install on the browser. Because, trying to browse the web anymore without a competent ad blocker, is just annoying most of the time.

Kurt:

I don't know if we're going away from Open Source tools at this point, but two browser add-ons that are fantastic is HTTPS Everywhere. I think Firefox, now Chrome, if you go into settings, there's actually an option to force HTTPS browser wide. It won't let you do anything over HTTP, which I would recommend turning on, and then Dark Reader, maybe not from the security realm with things. But, if you're staring at a computer for eight hours a day, that helps your eyeballs from falling out, it basically just changed a lot of the light on the page, to more of a dark mode that you'd find in the Windows operating system, or Mac or something. That's pretty good.

Eric:

Yeah. I definitely like Dark Reader a lot. I know some sites are a little incompatible with it, but it's easy enough to flip it on and off for those. But, for working early mornings or something, in an office, in a dim environment, sometimes it's nice not getting blasted with a bright white light when you're visiting a webpage.

Heather:

What about your favorite tools for testing attacks and detections?

Josh:

I'm constantly using Splunk's Attack Range project, for building up test environments in AWS, to run attacks, test detections, tell write a lot of our searches, and come up with quality things that actually detect what we're looking for. It works with AWS, using Terraform, and it also has a local version using Vagrant and Virtual Box, if you want to go free. But, it takes a little work to get that working. It also includes another open source project that's built into Splunk Attack Range, which is Atomic Red Team, which is a project for simulating normal attacks that you would see on a network, or from a pentest team, things like dumping passwords, or installing some kind of persistence. You can run those Atomic Red Team, atomics, they're called, to test to run a detection, and you can have a search up and Splunk to see whether it detected the atomic.

Kurt:

Well on top of that, Josh, I just think the ease of use, of being able to set up the Splunk Attack Range, and be able to a) have all the data automatically forward to Splunk. So, we can not only write SPL quickly, we don't have to mess around with setting up forwarders or anything. You can literally choose if you need X amount of work stations, or your server PC whatnot, post AWS.

Josh:

It has a couple options. It limits you to one domain controller, and one server, unless you go and modify it yourself.

Kurt:

Gotcha. I just know we've done multiple workstations before.

Josh:

Yeah. I know, with the Azure integration, you can spin up windows clients, but not with the AWS version. For Windows, that's the downside to Attack Range, is that you're limited to the systems that they have, and you can turn them on and off, just with a flag and the config. You can have a DC, a server, an IDS, Splunk server, of course, Kali.

Kurt:

See, the thing that's been really nice in my opinion, is just being able to start a brand new AD set up, and it can figure what you need in it for a specific exploit you're trying to test, or even just trying to figure out what logs are created from specific settings getting changed in AD configurations.

Josh:

Yep. And, it has a lot of great logging, right out of the box, with syslog process monitoring, looking at registry. Also, all the Windows logging that's available, you can turn on, pretty much every single Windows log, just in the config. It also has Stream, so you can get HTTP, DNS logs from there. And, also once you spin it up, if you're trying to run a specific detection, you can always turn on that logging yourself, and the forwarder's already there, you just set up the monitor.

Kurt:

And, since it's hosting AWS, if you're collaborating with a team that is across the United States, so you don't have a VPN into the local network, which maybe you had your setup posted. It's really easy to log into the GUI's, you're just hitting a public IP.

Josh:

Yep. And, there's a configuration for a whitelist, so it's pretty safe. So, only the IPs on a whitelist can access the hosts.

Kurt:

Because, I don't think I've been with you Josh, when you've done some of the Atomic Red Team side of it, can you go through the process a bit, of how you would use that with an Attack Range?

Josh:

Yeah. I have a Docker container that you can pull, that has all the configuration and stuff. And, you have that on your local host. You pull down that Docker container, you configure the configuration file for it, tell it your AWS credentials, and you tell it what servers you want to spin up. And, you just run build, wait 15 minutes or so, and then you have that up in AWS. And, once you have that, you can just start running your tests, RDP into the Windows host, SSH into the Linux ones, run your attacks, see if the logs showed up in Splunk, and then start writing your detections around it.

Eric:

Cool. That's pretty cool. I've been meaning to look more into that since you've set up some of that, but it's really interesting all you can do with it, and the ability to double check your searches, make sure certain signatures are being generated by different...

Josh:

Yeah. It's certainly not as good as something you can set up yourself, but it's a whole lot more convenient, and being able to just tear it down and build it.

Kurt:

I was just about to say Josh, as far as, it's not as robust as setting up something at home, because I know when the Log4j stuff was coming out, I was looking at potentially trying to replicate that. And, it ended up being a real pain, trying to get the vulnerable version of Java installed, or to get that set up. You'd probably be better off spinning up a Docker image, on a local test network or something, to do that.

Josh:

Yeah. I remember, we also ran into an issue with LM relays, when we were trying to run and exploit using multicast traffic. And, we realized that there is no multicast traffic in AWS.

Kurt:

Yeah. We were sniffing for traffic that didn't even exist, because it was getting canned, so we were sitting there getting pretty frustrated, but there are limitations with it. But, I would say if you're doing anything that's Windows Active Directory-related, it does a pretty good job of letting you spin up the host quickly, and get some testing done.

Heather:

What about for OSINT, and researching IoCs and payloads, what do you guys use for those?

Kurt:

Eric, being the SOC T1 team, why don't you talk about some of the tools you guys are using daily? What's the one HL uses again,

Eric:

I assume you're talking about CyberChef, which is, it's a nice tool for doing some encryption decryption work. It's got a lot of different algorithms built into it. If we're looking anything like Encoded PowerShell, or things like that, it's got a nice, quick, Base64 encryption, so you can get right into figuring out exactly what was going on there. It also has a nice auto bake feature built into it, which tries to magic its way through a decryption. It'll analyze the inputted code, and try to figure out what encryption is being used there, and it'll spit out the decrypted code, and the method being used there. But, it's good for all kinds of things, URL decryption, sometimes when people are trying to do injection via URL, and decrypting some code through there. But, it's a really nice and really simple tool to set up.

Josh:

Yeah. There's nothing better for taking a payload and trying to figure out what it does. If it's basically foreword, or an any kind of other encoding, if it has compression, all that, you can just, very easy, step by step, modify the input, and I'll show you the output. Very easy to use GUI.

Kurt:

I was about to just say that is, out of everything Josh and Eric have mentioned, that in my opinion, the best part of it is, you have almost, a GUI that's broke into three parts. On the left side, you have for example, in code Base64, decode, you could have your rot. You could do all kinds of different decryption on it, or encodings. But, you drag and drop from the left to this queue list in the middle, where you can layer. You could be like, "Encode five different times with Base64, decode once." And then from there, you'll have your input box on the right, and the output of... So, I could input Hello World in the top right, via my keyboard, or text, or whatever payload I'm trying to decode, and it'll put that out in the bottom right of the screen. So, rather than trying to do all this via the command line, which can be a real pain, the GUI is what makes the tool really special in my opinion.

Eric:

Yeah, definitely. Anything, especially nice, like you said, for anything that's encrypted several layers deep, rather than trying to use multiple tools, and copy paste within things. Here, you can just layer it, and just build through the decryption as you go. And, it definitely reduces a lot of the time for hunting through that kind of stuff.

Josh:

Yeah. Perfect tool for CTFs too.

Kurt:

Yeah. Hands down.

Josh:

Every single odd algorithm that you run across in CTFs, it's probably in CyberChef.

Kurt:

And then top of it too, if you want to, it is hosted online, under the GitHub link for them, you could also host internally in your company if you'd choose to do so.

Josh:

And there's a Splunk add-on.

Kurt:

Oh really?

Josh:

Yeah. You can output things from an event in Splunk-

Kurt:

Is that new?

Josh:

... Some kind of Base64, and code and payload PowerShell, and you can have your recipe right there, and decode it.

Kurt:

Is that new Josh?

Josh:

Yeah, I think it's pretty new.

Kurt:

Okay.

Josh:

[inaudible 00:14:07] ...recently.

Eric:

Yeah, I was thinking it was within the last month or two, from what I heard.

Kurt:

That would explain why I'm like, "Whoa, that's cool." I'd be interested to play with that. But, I get, I can't say, I don't really frequently see a need decrypt the logs inside of Splunk itself. A lot of times if you're trying to break down malware, you had some kind of encrypted payload sent, you could normally just copy and paste it into a tool.

Josh:

Yeah. If you wanted to automate something, you have exclusion, you have like a Base64 payload that's constantly there, and you're looking for something specific in the Base64.

Eric:

Yeah. I can think of several specific instances, for reloading IDS events with encrypted URL connections in there, and you're trying to remove that specific payload instance that slightly changes each time.

Kurt:

That makes sense for that use case. I was thinking more so, from the malware side of it, but for tuning, I could totally see it. Eric, what's T1 use a lot for digging into IoCs.

Eric:

Oh, Machinae. Yeah. It's a really nice tool that we have here at Hurricane, that's managed on our own GitHub. But, you can plug in hashes, IPs, various things, and you can link it up with several different OSINT engines, based on your licenses, or keys that you might have, or things of that sort. And, it'll run through and give you a generated list at the end of, pretty much all the OsINT it can gather from those sources. So, rather than hitting 10 different sources, and plugging the IP into 10 different places, or a hash, just plugging into one all encompassing place, and it'll kick out all that information. It's something that we try to usually include in our tickets for any kind of extra, additional enrichment info for the client. And, it's a really nice tool that speeds up things. We even have started incorporating it more as an automated process, to always have that enrichment data provided for our alerts.

Kurt:

Cool. And, I used that a lot more when I was digging into stuff, not as frequently, doing more architect work. But, checking the GitHub real quick, it looks like probably 25, 30 different data sources, out of the box, or able to get used with Machinae. Is there a GUI or anything with that? Was that ever added, or is it all CLI?

Eric:

I believe it's all CLI. I don't think we've ever done any GUI with it. It's not too difficult to figure out. You can have it kick the results out to a file. You can have multiple hashes generated at once, ran through at once, just a little more time consuming. But, there's a lot of different options for different output types, and exactly how you want to scan and everything, it's pretty well crafted.

Josh:

Yeah. Something similar with a GUI, would be Spider Foot. I remember you showing that to me a couple years ago, Kurt.

Kurt:

Yeah. I found that early on. It's gotten a lot larger now. I haven't personally poked with it too recently, but back when I was doing T1, lead stuff here, I had an instant spun up. It's essentially, similar to what our Machinae tool is, or almost any OSINT tool you're going to see on the GitHub, or something special to a SOC. Except, the thing that's cool about Spider Foot is, like Josh said, you get a full fledged GUI with it. So, not only can you look at, I think there's 100 different, or 100 plus different website you can pull data from, with IoC. So, you can put an IP in there, and pull from, I've heard... Like I said, you'll have to look at the list yourself, but there's a lot of different places it can pull from. Needless to say though, the GUI on it, so let's say you put an IP in there... Josh, you might be aware of what I'm trying to think of, it's in Kali. I'm trying to think of what the investigation tool in Kali is called. Multigo, I think.

Josh:

Yeah. Multigo.

Kurt:

Yeah, it's very similar to, at least how it does the web, of incorporating connections and stuff. If you put an IP in there, and it does a DNS look up on the IP, it might find a domain, and then from there, you can almost... Almost like if you're using Burb Suite, and how it could spider from one domain, to one IP, to whatever it finds on the webpage, and group connections together, it's similar, but it'll give you a map of that. It's just a really cool tool if you find a specific URL or IP or something you're really trying to dig into, or make connections with. It took a while for the scans from what I recall. We did have it hosted internally. I think for a call, we did have it digging through... You could do tour connections with it, and have it go through the deep web on it, look relations of URLs, or even specific file hashes. You could do Bitcoin addresses as well, but I don't think we mess around with that very often. But, looking at the website now, they seem to have taken off a lot since I was looking at them two years ago. They were more heavily focused on the open source one. But, that looks to be more of their less functional option now. It might be worth playing with, setting up. I'm sure you can still get some useful information, but it looks like they moved more to a paid setup for all the GUI options. But, either way Josh, that was cool for sure. DNS dumpster, I've used that a lot for doing reverse DNS lookups, and telling you everything that's connected to an IP. That's a pretty solid...

Eric:

That'd be nice.

Kurt:

Not sure that's open source at this point, just talking about it.

Josh:

Cashless websites that we use.

Kurt:

Yeah. I'm just trying to think of tools that I've used on the daily that were really solid. I enjoyed that one. What's another one? Emailrep.io, I've used that for poking email addresses. That one just pretty straightforward. That one's looking for where, and how recently your email's been used. If someone just spun up a recent email for phishing purposes or something, and it'll basically tell you the age of the

email, and what sites it's registered to, so you can easily identify a user's email that's actively valid, and used for reasonable purposes, versus something used for phishing or trying to spoof.

Eric:

Another one we use is that EML analyzer. That's a really nice tool we have included in our recon, repo, that allows for taking an EML file, opening it, and breaking down everything that's included in the EML attachments. It's a nice tool when you're looking over something.

Kurt:

Is there a GitHub for that, Eric?

Eric:

Yeah. It's, I think, Nino Seki, EML analyzer.

Kurt:

Gotcha.

Eric:

Yeah.

Kurt:

I think that must have been added after I stopped poking in the T1 stuff.

Eric:

It was a fairly new thing that was added a couple months back, but I use for a couple ones where I don't have... When you don't have access to an environment, but you might have an EML file, it's nice to get a full picture of what exactly is being sent.

Kurt:

Makes sense.

Heather:

You know, at the start of the talk you guys mentioned, making sure to change default passwords and stuff like that. What other tips or suggestions can you make for someone who's going to start using some open source tools?

Kurt:

One thing I probably haven't mentioned yet, was the one cycled privacytools.io. While I'm not sure if all of them are open source on there, there's a fair share of applications, and browser extensions that I found on here, that have been quite useful. Probably the one I can call out that I use daily actually, is Standard Notes. I'm always pushing it on people, and trying to get more people to use it. But, essentially it's just a encrypted note pad, and I've been using it now for a while, just basically for, between notes at work, or even stuff as simple as keeping track of when I last changed the oil in my car. What's nice about it is, you can use it across multiple different platforms. It functions on Linux, iOS, Android, OS X, et

cetera, et cetera. I don't think there's a platform they don't use. I could ramble about all the different tools on here, but the site's worth checking out it's privacytools.io.

Josh:

Yeah. And, one thing to look for with open source software, to see whether it's secure, is how often it's updated. If a project's been abandoned and sitting there for four years, maybe avoid it. But, if something has tons of commits that are recent-

Kurt:

If it even works.

Josh:

People are still submitting issues, you can tell that people have eyes on it.

Eric:

Yeah. It's, like you said, definitely good to always make sure it's still being used. Things can fall by the wayside, and if it hasn't been updated in years, there's a chance that some vulnerability may affect it, that hasn't been tweaked yet.

Kurt:

This is more red team perspective, but you can find a lot of reconnaissance tools that are open source, through GitHub, or even in Kali at points. And, some of them, they're normally heavily based around email recon, or trying to link phone numbers to email addresses, and stuff to that extent. There's always new stuff getting made, and a lot of times tools that are, we're looking at something like Twitter, or scraping Facebook, to a certain extent, there's almost a constant battle between the third party companies and the people writing the tools, because they don't want that take. I remember there was a tool that was used for Twitter that you could scrape tweets without even having an account. And, Twitter's okay with letting you use an API, but they don't want you scraping that without knowing who's doing it or whatnot. I forget the exact name of the tool, but it would work for three days, and then Twitter would make a change, it'd be broke for a week, it would work for four more days. And, I think that's pretty common occurrence for more of the red team, open source tools for reconnaissance.

Heather:

Thank you very much for taking the time to sit on this call, I appreciate it.

Josh:

Yeah, no problem.

Eric:

Thanks for having us.

Heather:

That's all for today. Thanks for joining us. And, until next, time stay safe.