SEI Cyber Talk (Episode 5)

How to Fit the Internet into a Box
by Rotem Guttman and Gabe Somlo

Rotem Guttman: Hi, I'm Rotem Guttman.

Gabe Somlo: I'm Gabe Somlo.

Rotem Guttman: And so, Gabe, I understand that you've taken the Internet and shoved it in a box.

Gabe Somlo: Right, like on the IT cloud.

Rotem Guttman: Exactly, and so--

Gabe Somlo: Not actually got-- it doesn't have a blinking LED on it.

Rotem Guttman: There's no red light on the top?

Gabe Somlo: No.

Rotem Guttman: Then why even do it, I mean at that point?

Gabe Somlo: I'm sorry. I apologize. I should probably fix that as soon as possible.

Rotem Guttman: So, before we get to the how, because I do want to know that, but why? Why would you do this?

Gabe Somlo: Why not?

Rotem Guttman: See this is how you get in trouble.

Gabe Somlo: So, right-- so, we have a lot of-- I don't know. Are we-- geez man, I don't know. You're asking me this question, so I now have to go back and sort of give the official spiel of okay we're doing exercises, we're simulating offensive/defensive cyber forensic scenarios to teach people hacking skills and defense skills and forensic skills. Okay so, when we're doing that, we do that with a lot of VMs. And so, because we do that with a lot of VMs, and the VMs run on platforms and environments that are disconnected from the Internet for multiple reasons because they happen in secret installations that are air gapped because we don't want our viruses to escape on the Internet, and then we want the trainees to think or to sort of have the sense of realism that they are on some sort of thing that looks like the Internet. So, we scraped all the websites that we thought people might sort of be interested in for realism's sake, and we set up a bunch of other services that might look like they are out there on the real Internet and shoved them in a single VM to make it easy to start and stop a simulation.

Rotem Guttman: So, that's the first piece of it was just the websites, trying essentially-- so, when somebody's training their cyber skills in an environment that is safe and secure so that anything they do doesn't get out on the public Internet, they still have access for the sort of look and feel for-- as if they were on the public Internet from the perspective of websites.

Gabe Somlo: Right, you basically-- the first sort of prime directive was hey, we have all these webservers in our simulation, and they're all burning up with special VM for each one of them. And that gets heavyweight really fast, the more sort of realism and the more websites you want people to think they have access to in their games. And so, obviously, for a very long time, website operators have been doing virtual hosting. So, you have a webserver machine or sort of an installation serving three, four, or ten different companies' webservers. And that's called virtual hosting for the web. And that's been done on the Internet since the webserver was invented.

And so, I thought hey, wait a minute, right? I mean if we want five hundred thousand websites, can't we just vhost them off of the same server? So, the answer to that is obviously yes. It is just a matter of how much space you have on your hard drive because your root directory for the webserver software could have ten, twenty, five hundred thousand subdirectories. And you could just put different websites in there.

Rotem Guttman: Except for now, when you're looking at it from a network security perspective, or from a network forensics perspective, you can tell these are all being hosted at the same site. So, that kind of ruins the realism when you're trying to go to this website that's in one country, or this website that's in another country, and they're all coming in off the same pipe.

Gabe Somlo: Right so, we're never going to get over the fact that these aren't going to be actually-- they're like NPC characters in video games. They're not actually hackable websites because, if you hack one of them, now you've hacked the whole-- every webserver on the Internet. So, they're all served out of the same actual server. But we could make them look like they're in different places. First thing, we could have different IP addresses configured on the same server. So, if you go to IP address one for webserver one, you can go to IP address five hundred for webserver number five hundred. So, they're actually pretending to be coming back at you from different IP addresses. True but the addresses are all in the same box, but they're coming back from the same--

Rotem Guttman: But then if I start doing-- let's say I just start tracing routes to those IP addresses, I'm going to see they're all being served off the same route.

Gabe Somlo: Right, the traceroute to all websites is exactly the same. So, for that, then you need to add routers, virtual routers. And we had virtual routers to separate virtual machines, many different VMs running Quagga, which is Linux-- the Linux package that does sort of upscale routing protocols, not just sort of the bare bones stuff that you get on a user machine. So, running Quagga in a VM, running Quagga in another VM. Now, you have two routers. You have-- I don't know. How many routers do you want to start getting a feel for a realistic VM? You have the scaling problem again. You have like hundreds of virtual machines in an exercise that aren't dedicated to the students logging in and doing for forensics, or defensive, or offensive cybersecurity. It's just NPC machines sitting around there to pretend to have-- so, you can pretend you have routing infrastructure.

Rotem Guttman: So, to take the video game analogy of NPCs, this is-- you're dedicating all of these resources, and it's not for the player character, or the interactable characters. It's just for the background--

Gabe Somlo: To paint the background picture. So, we could probably-- I mean we thought we could do that more efficiently. So, Robert Beveridge and I were sitting in the hallway a few years ago. And we were thinking hey, wait a minute. Wouldn't it be nice if we could have all the routers on the same machine? And then I said, "Well, we should probably be able to do that with containers. And if only somebody wrote the simulator-- network simulator that was using containers." And then like all brilliant ideas that I have, typically a Google search will sort of disabuse me of my brilliance. And it's been done by somebody somewhere if it's at all useful.

Rotem Guttman: Or at least the eighty percent solution is--

Gabe Somlo: Right.

Rotem Guttman: Somebody started it.

Gabe Somlo: So, I Googled around for container-based simulators. And the thing that I found that was the most elaborate and sort of almost ninety-five percent ready to go was CORE, C-O-R-E, stands for Common Open Research Emulator, developed by the Naval Research Lab in collaboration with Boeing, open source project on GitHub. Download the thing. Install it. I've made it into an RPM because I'm a Fedora nut. So, I decided I'm going to use Fedora for most of the things that I do. So, I made an RPM. Installed the RPM.

And then the question was we just needed to come up with a map, an actual-- like a configuration file for the simulation that has many BGP routers, and the application service in there, like the websites and everything. And so, now you have a single machine running the simulator with containers. They're very lightweight containers. By the way, you don't want to wrap a heavy-duty sort of lots of files, Dockerfile thing, around just Quagga because it makes no sense. Quagga comes as a package on your Fedora installation. All you want-- all you really want to do--

Rotem Guttman: I'm just trying to do the routing here.

Gabe Somlo: Wraps on fake network cards around each Quagga process that shares the same kernel with your one Internet--

Rotem Guttman: So, how many BGP speakers do you have?

Gabe Somlo: The thing that we do currently has sixty-nine or seventy, plus one machine that runs-- or one container that runs the websites.

Rotem Guttman: And so, you picked-- using this CORE simulator, you picked that one because it was open source, correct?

Gabe Somlo: Well, yeah, I sort of generally tend to prefer open source software for everything that I do mainly because it's just easy to find. There's no process to obtain it or to pay for it. It is very easy, and then sort of it's easy to contribute back to it. And the reason why you want to contribute back to open source software that you use professionally is, typically, if you make changes to it-- okay now, the changes are yours. They're local. They're your-- it could be your secret sauce, or it could be just something that's a burden that you have to carry forward. As the upstream package evolves, it tends to evolve away from the change you made unless you put the change back and talk to the maintainers and contribute it back so that now it's kind of part of the project. And when they make changes to it and the software evolves, it actually evolves with the feature that you want it to have. And you're no longer responsible for reapplying your changes over and over as new versions get released.

Rotem Guttman: As you said, this was your ninety-five percent solution, but that five percent that you added then gets merged.

Gabe Somlo: Yeah, it had some words that I fixed and then contacted the developers and pushed the fixes back upstream so that I actually don't have to worry about them anymore because I would continue to have to worry about them if I didn't do that.

Rotem Guttman: Yeah, every time we updated it, we'd have to re-apply your--

Gabe Somlo: Every time we updated to their latest version, I would have to rebase the patches and figure out where they don't apply cleanly anymore and keep dealing with the same issues over and over. And once you've submitted the fix, obviously you're going to deal with new regressions with new issues that they introduce. But that would happen no matter what. You're no longer going to have to deal with your old issues that you already fixed.

Rotem Guttman: Just the new things that are broken.

Gabe Somlo: Right so, things that you fixed tend to stay fixed if you submit upstream. Otherwise, they don't. They just keep coming back.

Rotem Guttman: And so, now that you have that system up there-- now, as we know, websites aren't the sum of the Internet. So, we needed a little bit more realism there. It's not enough to just visit websites. We need other interactions happening there. So, we have the background scenery. We have the hills, the mountains, and the streams. But we need some--

Gabe Somlo: There's--

Rotem Guttman: Some trees, some birds.

Gabe Somlo: There's DNS. That's one of the big ones, right?

Rotem Guttman: Because how are you going to find the websites?

Gabe Somlo: So, you need to translate names of websites, among other things, into IP addresses. So, that's what DNS does. The problem is the Internet has a whole giant DNS infrastructure. It's not just the one name server that your company runs that helps you find things. It has to go and talk to a lot of different servers starting with the roots, and the top-level domain servers, and so on to find authority that can answer whatever query, whatever DNS translation queries the client comes up with. And so, just like there's a bunch of websites that you want to have in your pretend Internet, there had to be DNS server infrastructure components in the pretend Internet to help your name server find answers.

And interestingly enough, just like Apache and NGINX and sort of HTTP daemons can do virtual hosting, and essentially that means they have multiple personalities, you can configure it then to pretend to be different websites depending on how you talk to them, the same thing applies to name D or BIND the DNS server infrastructure. Except they don't call them vhosts. They call them views. And generally speaking, a DNS view is used to selectively tell different things to different clients. If you're the server, and you have a DMZ or an external presence, and people from the sort of Internet at large come and ask you questions, you may tell them only about your DMZ machines, like your public webserver and your public whatever infrastructure that you're offering to the outside of the Internet. You may have a private network that's not visible to the outside. And to that private network, you may tell more things about your services that you have on the inside.

Rotem Guttman: I don't want everybody on the public Internet to know that I have db.whatever as my backend database server. But I still want to be able to use that URL internally to access it. So, this lets me do that.

Gabe Somlo: So, generally, a DNS view is a virtual hosting option for DNS that allows you to discriminate against clients, where they come from. Are they your trusted internal clients, or are they just sort of random people on the Internet asking you questions? You could treat them differently based on where the query comes from. But interestingly enough, there's a facility and in the configuration file of the DNS server to discriminate not just based on the source of the query but on the destination of the query.

Rotem Guttman: Nice.

Gabe Somlo: So, if you have, like with the websites that we did multiple IP addresses configured on your machine, you have a machine with twenty different IP addresses, you could discriminate between DNS queries based on which of those IP addresses of yours they're talking to. So, you could pretend to be a different kind of server depending on who the client thinks it is talking to. So, just like with websites, now we could be the root DNS servers.

Rotem Guttman: Yeah, if you're coming in--

Gabe Somlo: In through M root-- if you think you're talking to a root server when you're addressing me--

Rotem Guttman: Then I'll be the root server.

Gabe Somlo: I'll act like I'm a root server. So, I'll be whoever you want me to be. And then I'll tell you go and talk to DNS delegation. The root will tell you okay, now that you want something.com, I will forward you, or I will tell you I don't know the answer, but go talk to the .com TLD server. And when you try to talk to that server's IP address, guess what? That's me again. I'm just going to now put on my talks like a domain hat and--

Rotem Guttman: It's like a bad comedy sketch. It's like, "No, you need the manager for that." Comes back with the--

Gabe Somlo: With the manager hat, and--

Rotem Guttman: Yeah.

Gabe Somlo: That is essentially what this project is. It is websites, DNS servers, mail domain servers that change their hat, basically, depending on who the client thinks they're talking to. So, that's how you get away with just one single virtual machine for everything.

Rotem Guttman: And for some of the more esoteric but still important use cases like having Blockchain running so we can do cryptocurrency transactions in there, or any of the use cases that are less common--

Gabe Somlo: For those kinds of things, you actually want not just-- those aren't NPCs anymore. Those are active participants. So, they could be their own container but still run on the same machine. You can have, or we do have, exercises where the simulation also has wired into this multiple router container plus application server infrastructure. We have maybe four or five onion nodes with a special endgame directory authority because we can't fake the real directory authority. If we could do that--

Rotem Guttman: That would be bad.

Gabe Somlo: The Internet would have a big problem. So, we have to use our own endgame directory authority. And so, if you want to participate in this, you have to download the configuration file from the landing page webserver that has all the information inside the simulation. And so, if you set up your onion demon with that configuration file, and you make it trust my endgame directory authority, then you could actually pop out from some of the-- one of the nodes in the simulation.

Rotem Guttman: And in this particular case though, to take the example of mining cryptocurrency, it could actually be useful for the exercise and for the training to have a smaller set than realism. So, if I want to have somebody do a fifty-one percent attack, that's going to be hard on a large public--

Gabe Somlo: It's always easier to do a fifty-one percent attack when you have five Bitcoin miners in the entire Internet. All you have to do is take over--

Rotem Guttman: We've seen that in the real world when the actual fifty-one percent attacks that have occurred lately because-- against some of the smaller cryptocurrencies because there's--

Gabe Somlo: That's what you get with the fragmentation. If for instance the original Bitcoin had-- if Satoshi would have been able to tell the future and add all the bells and whistles that time told us Bitcoin or any sort of cryptocurrency needed, if you could add that from the get-go, then it would have been just the one cryptocurrency to rule them all that everybody used. And life would have been good. But with-- different people came up with different fixes for perceived--

Rotem Guttman: Ring signatures--

Gabe Somlo: Whatever, ring signatures, and anonymity, and all these things, and so, now you have this fragmentation where there's, I don't know--

Rotem Guttman: What features do you want?

Gabe Somlo: Five hundred plus different cryptocurrencies-- or I don't even know. I just made up that number. There's a very large number of cryptocurrencies and maybe, I don't know, the majority of them are even maybe just scams, or they're pre-mined, or there somebody's attempt to capitalize on the buzz that--

Rotem Guttman: I don't know about the majority, but there's certainly some that have been--

Gabe Somlo: There's a lot of them that are weird and shady. And then there's a lot of them that are just clones of Bitcoin. They took the source code. They cloned it, named it something else, and hey, now I have my own cryptocurrency. Why don't you?

Rotem Guttman: But why don't you? the point being that there's a certain safety in numbers there that's inherent. You can build another zebra, and it will be just as effective camouflage as any other zebra. But unless it's in the herd with all the other zebras, the lions are still going to get it.

Gabe Somlo: Right, well also, I'm not exactly for-- if I agree or disagree with that analogy, I'm not even sure I got it one hundred percent. But if you have many miners participating in the same network, then there's your herd. And you have safety in numbers because it is hard to perpetrate a fifty-one percent attack. If you have fifty different Bitcoin, the networks that are all clones of each other, then they necessarily have small numbers of nodes each. So, you could perpetrate a fifty-one percent attack against one of them much more easily than if they had just stuck together and not forked the software and started a separate network of cryptocurrency.

Rotem Guttman: But my point is that it's not so much forking the software. It's forking the community or the amount of resources that are being dedicated to maintaining the blockchain that's really the issue.

Gabe Somlo: I meant forking the network.

Rotem Guttman: Yes.

Gabe Somlo: You have the Bitcoin network. And then you have the clone of Bitcoin, which forked the software and started a new peer-to-peer overlay community. And the software is sort of kind of almost inconsequential to the fact that they now have a separate like hey, this is our cryptocoin network.

Rotem Guttman: Absolutely.

Gabe Somlo: And everybody has their own little cryptocoin network. It's so easy to do a fifty-one percent attack against one of those little ones.

Rotem Guttman: So, just to make it clear for anybody that might not be familiar with what a fifty-one percent attack is, this is where if you have more than half of the processing power or essentially the resources, whatever is being done in order to-- proof of work, you can kind of hijack the history of what transactions have happened. So, you can spend money, and then go back and revise history and put that money back in your wallet.

Gabe Somlo: So, I would say-- I would say in cryptocoin networks the guarantee of being able to only spend your own money, not being able to spend somebody else's money, so like basically fraud prevention, in a cryptocoin network goes with the fact that a majority, more than fifty percent, of the participants in any given cryptocoin network are honest and abide by the rules. The idea is if--

Rotem Guttman: Well, just to be clear--

Gabe Somlo: If more than half of them are cheating or more than half of them are in collusion, then they could basically rewrite history and invalidate otherwise valid transactions. And that's kind of the fifty-one percent attack.

Rotem Guttman: Right, exactly.

Gabe Somlo: It's collusion or cooperation between--

Rotem Guttman: I just want to be clear though, it's not fifty-one percent of the number of people. It's of the resources.

Gabe Somlo: Right.

Rotem Guttman: So, you could have one person with enough resources to dwarf everybody else, they can take it. If everybody else is five containers running in the simulation, then it's doable.

Gabe Somlo: Right.

Rotem Guttman: By your training--

Gabe Somlo: So, if I only have five containers doing Bitcoin mining in my simulation, and you come up with six Bitcoin miners of your own, then you could overwhelm the network and sort of impose your view of what transactions are valid.

Rotem Guttman: Which allows us to simulate those kinds of situations in the environment, whereas that would be a lot more difficult, thankfully, on the public Internet with a large traded currency. And for good reason, we wouldn't want to do that.

Gabe Somlo: Right.

Rotem Guttman: But we still want to be able to train, okay how do you detect that this is happening? How do you tell that this is going on? How do you defend against it?

There's a certain critical number of nodes that would have to collude in order to violate the security guarantees of that network.

Gabe Somlo: In order for some unsuspecting victim to actually end up using the same organization's nodes both for their entry and for their exit point because that's when you could do traffic analysis and correlation and actually sort of tie where they're going to where they're coming from together.

Rotem Guttman: So, just as one final question for you, are there any Easter eggs, is there anything in that environment that you think is really interesting that people could kind of find as their looking around, whether you put it in there intentionally or not?

Gabe Somlo: Well, okay, so the first iteration of our scraped content-- so the scraped content isn't part of the open source software that we wrote. It's called TopGen and GreyBox for the applications, sort of websites and DNS, and for the containers, respectively. TopGen is the top five hundred most popular websites on the Internet scraped automatically and sort of served out of this simulation. And there was, to begin with, an inadvertent Easter egg in TopGen. So, that top five hundred list was--

Rotem Guttman: Filtered? Or just straight--

Gabe Somlo: It never occurred-- so, it's kind of interesting to have people really familiar with computers and programming and the Internet, have been on the Internet for a long time. And so, it never occurred to any of us while we were doing the scrape that well, the top five hundred Internet sites might include some content that's not safe for work. And that was a--

Rotem Guttman: Just a little bit.

Gabe Somlo: That was just a huge surprise, like hey, wait a minute. We just scraped a whole bunch of stuff. Oh, we better sanitize this, right? So, there was like an original Easter egg, and then we got rid of it because it was not the kind of Easter egg you want to be known for to your customers. Absolutely.

Rotem Guttman: So, well, first of all, thank you for sitting down with us.

Gabe Somlo: Well, thanks for having me.

Rotem Guttman: Absolutely, and if you'd like some more information about the work that we do or specifically about TopGen or GreyBox, please visit the website below. This has been Rotem Guttman and Gabe Somlo. We look forward to hearing from you.

Related Resources

Helping You Reach the Next Level of Security - 6 Free Tools for Creating a Cyber Simulator

Download source code from our tool repository (GreyBox, TopGen)

SEI Cyber Minute: SEI's Internet in a Box Spurs Realistic Training