



External Scans Overview Video Transcript

Welcome. In this video, we're gonna cover external scans in CyberCNS. So, as a little tip, if you're going to use external scans out of the system, you want to make sure that we're up, you got traffic allowed. These are the IP addresses that the scans will come from based on the region you're in. So, if you look at your CyberCNS URL when you're logged in, you'll see a signal to the region right in that URL string and you just want to make sure that you've got a traffic rules set for this. So, if you have any trouble with that, you can contact our support team and we can help you out but this is something that you'll want to take into account if you're going to use externals and external scan or scans that are performed outside of the network that you're in on the scene. So, let's go ahead and get logged in to CyberCNS. We'll take you guys through the overview here.

So, external scans are available at the company level. So, when you're in the company level view, you'll find your external scans sitting under your scan results, scan results, and then over here on the left vendor external scans.

And so, this is where we can fill in the information for the scan. And when we run a scan, we can run it on an IP range. So, if you have a range of IPs, we can run it against the static address. So, if you have just a static IP that you want to scan against, or we can scan against the domain name. I'll go ahead and just do a sample scan here with you guys. We'll call this our Google sample. We're going to go ahead and use domain name and we're going to use google.com for our scan.

And we've got a scan profile. So, there's three different options here to choose from. You can do the quick scan, a detailed scan or a deep scan. So, your quick scan is the most common ports up to 1000 of them or we're going to scan the most commonly used ports. Deep details scan goes a little deeper when we expand that to 3500 ports. And then the Deep Scan does the full port scan 65,000 Plus ports can take a little bit of time. So, on this we're going to just go with our quick scan for purposes of our video.

If you want to include tags on the scan for sorting, reporting and filtering later, you're able to do that.

And you can also add any ports here that are considered secure ports. You can go ahead and comma separate them if you want to add them in prior to the scanner.

Go ahead and save that profile.

So, we've got the Google sample added in there. And then, as I mentioned our scan type, on the Profiles tab within the external scanning is where you can see the scan types we've got. So, we've got a quick scan the detailed and the deep.

And we've also got the little you custom scanning. So, if you want if you're looking to do a very targeted type of scan on very particular protocol across maybe even certain ports that you're targeting, you can

do a customization here so if you hit add, we can create a custom profile I call this Ryan's customers scaling.

And from here, you can choose your port height, so either the top ports that I mentioned where we're going to use, you know the top ports, we've got a range of 100 500 so on all the way down to a full which would be at 65,000.

You can also do custom ports. So, if you wanted to just scan a few ports, specifically you can target them comma separated there if you want to do multiples and once you choose the port you're going to scan for you can choose the protocols. So, we've got Syn, we've got Connect, we've got Xmas scan, got some information for you guys about what those protocols are. Generally, we're using the Connect scan profile when we want to scan so by default our scans do use that connect protocol and then we've also got service detections for the scan. So, you can signal on your custom profile scan, if there's very particular service detections and what learnability is that we're looking for. You can go ahead and select those here. So, SSL cert so on and so forth. You can check the boxes for what you want to include when you're doing your scans. And when you're done. You can give that a save so connect and then that'll give you a save and whenever you save your profile, it gives you a little recap here so if you were to have multiple scan profiles, you will see them here indicating what type of scan what ports we're scanning, what protocol we're scanning with, and what service detections we're looking for. So, that would be an example of one of our customers.

Results are where results will get published to you once the scans are done. So, you can see here there's a scan from google.com. That was from an earlier scan that we just ran. So, from this last job, I should build it then tap on that scan and get the results from that quick scan that we did again this is this 1000 ct, very quick scan. And we can see here we've got some grading and it gives you the information about what ports were open and communicating. What protocols were running on will give you some vulnerability scanning we've got some detail along with these to show you the CVSS scores against them the severity remediations how they impact the network, and a description of what we're actually protecting against. So, the results of those scans can be drilled down. I'll go ahead and close that detail. Again, that's that details page. Again, if you hit details, it'll give you this information that you're seeing in the vulnerability section. It'll break out each one of those with the details to give you a bit more information about how we're scanning what we're finding.

We'll show you a common SSL vulnerabilities. So, drown pool and heartbeat, giving you certificate information about the SSL certs connected to the domain.

And then additional, you know, certificate information, any ciphers, what protocols are being run, what the grades are. Here, we can see an insecure version of TLS 1.1.

You can see they've got one two that looks good when three is looking good. So, this is again a quick result of an external scan against the domain

and then your jobs. This is going to show you any jobs that you're running. So, as you configure and do additional scan endpoints, those will show up on our jobs. back we'll go ahead and do one more here just for sake of our recording here. Say let's think next year. Let's say domain.connectsecure.com will say give me detail. And again, you can see here there's that custom scan profile that I've made so if I wanted to use my scanning I could give that a Save As soon as you save that configuration and you go into jobs.

You can see already that scans running. And you can see it's done resolute DNS resolution for us. And once that job is completed, it'll show up here under our results pane, roll over then tap on to it and get the detail. You can also tap there to get that detail.

So again, depending on what job you're running, what scan you're running, the port you're scanning, you can vary results here anywhere from you know, less than a minute to a couple of minutes, maybe upwards to an hour or more if you're doing a full scan.

But those are your external scans. Pretty simple again found a better cost a company level. You can define those scan endpoints from there.

For those of you that like the documentation side of this I want to remind you guys we do got this documented so if you're out at our website, connectsecure.com, come up to those resources and go to support.

Click on View documentation.

And right here, you can navigate to the left and go to the external scans but we've also got it just sitting right on that part of the page there. So, he just kept that external scan to take you out to the dock. And we'll give you some information about the scan features and it'll kind of walk you through it. And as I mentioned, if you'd like to view it from the left panel, you can also just tap over there on that left panel. And again we'll take you to that dock and we'll give you the information and there is that the region's along with the IPs that I mentioned at the very beginning of the video, so if you need that information, it's in the dock and then this will be a step by step walkthrough of everything we basically covered on that video today with a bit more information about some of the protocols some of the service detections that we're using. So, if you guys are interested in the docs, documentation is out there. Otherwise, you know any questions any content anything else you guys want to see even regarding external standards, let us know and comment on this video. You can hit us with an email education@connectsecure.com
Thanks again for watching.