CONNECTSECURE

Assessment Overview Video Transcript

Welcome. In this video we're gonna cover assessment scanning within CyberCNS. So, assessment scanning is essentially a way for you guys to bring CyberCNS into a prospects environment. Gonna scan, get the results, get them uploaded to the CyberCNS portal and then provide some insights and reporting right away. And this allows you to scan and network without leaving behind an installation or any software or write any footprints about the scan that took place.

Kidding. So, let's go ahead and get logged in here and we will set up and run a scan together.

So once we get logged into CyberCNS we're going to want to navigate on our toolbar at the very top here we're going to check to the assessment view.

Once we're here, this will work similar to how the company view works as in from the drop down menu, we've got different companies so in this list, we'll find the names of the companies or prospects, where we do assessment scans.

And you can remove these companies once if you no longer need them. So, like if, you know we've got this test company sitting here and say, you know, hey, we ran the scan on this data we don't need it anymore. You can just tap Delete a yes, it will remove that customer out of the list and you will no longer find test.

So you can remove your test companies out of the view just tap on the Delete to add a new company that will take place automatically when we upload a new assessment. So, once we start this process, when we get the reports, we're going to upload them back to CyberCNS. It will then create the company in the list for us as part of that import process.

So let's go ahead and get started here. We're going to we're going to download the assessment agent to create our first or a new customer or new prospect. It will hit download. This will pull up the setup, operating system options just like your normal probes and agencies ever seen as that so Windows Linux, Mac, air and Raspberry Pi support. And depending on which one you choose, you will get a different set of instructions below based on that operating systems requirements. So, we're going to use our windows one nice and easy today. And we can see here we've got a five step process. Okay. So, first thing is downloading the zip file. So, you tap download that will begin our zip file download. Okay, if you just go back and hit the download and get the instructions back.

Once the download is done, we need to extract that zip file Alright, so let's go ahead and kind of stuck through this together.

There is my downloads folder that we just downloaded.

And I right click on that I can say extract all we're going to just extract this right back out to our desktop into its own folder.

So there's that folder. It's currently extracting, we're going to let that thing run.

And once this is done, we're going to open up that folder. And within that folder, we're going to have a batch file to start the assessment. Okay, so here's the extracted folder. We're going to open that folder up. And within here we have a start assessment batch file.

So we're just going to right click run that as administrator. This will launch it potentially going to launch your Windows Defender SmartScreen if you have a running or if you have any kind of third party security software that might know warn you, which is go ahead and say yeah, we're gonna go and run this anyway.

And then we'll get a command prompt to open up and it will let you know go ahead and browse to HTTPS://localhost:808. And you will be able to start the assessment wizard. So, a web browser, I'm just going to go ahead and open up our Google Chrome browser. We're going to go to localhost:8088 And you will land on the assessment wizard. Now, for those of you that have never done this I want to make sure that you don't get confused because you will be prompted for credentials the first time you log in so let me launch this with our incognito Chrome. So, this is what you'll see when you first navigate to that localhost:8088. It's going to take you to this login screen where you're going to provide credentials admin as the username and its password, all lowercase. As the password. This is the assessment master credentials by default.

You can tap Change Password and you can update this in your system. Otherwise, it's admin and password. Once you hit sign in, it'll take you to the assessment.

So once we're in the assessment wizard, this is where we're going to provide our parameters and any info we have to better do a scan and provide better data.

So, what we're going to do is tap next to start and the first thing is at the IP range, what are we going to scan.

So I'm here if you there's nothing in here the window you'll just get no data. We're going to tap Add if it doesn't automatically pop up for you. And we're going to tell it what we're scanning. So, if we were doing multiple networks or multiple sets of IPs, you might use the name appear to be just descriptive to arrange them. Otherwise it'll default to set one. Your discovery type fighter, an IP range, a static IP or a domain name.

In this case, we're going to use an IP range just so we can do a scan today without wasting a ton of time.

So starting IP, so we're going to start at 10.0.1 And we're going to end up 10.0 dot we'll just say ft about that around 450 here.

If you want to enter any tags for scanning or exclude from scanning the tags, those are your tags within CyberCNS. You can exclude them if you needed to go ahead and say once you say that parameter will show up in the window and I'll let you know how it's scanning. And if you want to add additional again you can just tap that and it's maybe you said hey set to I'm going to do a cider scan this time and this time I'm going to scan the 192.168.0.1 IP for a slash 24 network. And we're going to do too and you can add as many in the screen as you needed to write to scan as much or as little as you need to. So, for purposes of our scanning on video today, we're going to remove this one because we don't want to scan 250 Something devices here. So, I'm going to remove it as you can see we've got some actions here we can edit and change the parameters. If we've made a mistake. We'll remove it if you no longer need those in the window.

So we'll just leave our two and your one to fit we'll tap next once you get your IP range defined. Next we've got SNMP support. So, if you want to provide SNMP credentials, or any other version in here, you can tap the version and then add again give it a name.

What protocol

unsaved and this will allow you to do discovery around any of the SNMP enabled devices on the network.

We've got credentials, Windows Firewall credentials to provide so then tap Add tell it what they are no third you know if you got a local admin credentials or security group credentials, whatever you got, you give them a name. Usually password if there's a domain you can provide it.

The more credentials you provide, the better you're scanning, obviously, right.

Once you get all the credentials filled in, you'll go next. And then you've got same thing Active Directory credentials. So, example database server or the Active Directory server or if it's a backup Domain Controller whatever you're using, credentials, store them. The more credentials we've got, the better your scans gonna be.

And we're gonna get to the discovered assets screen. This is where we're going to go ahead and start scanning for assets. So, we'll tap on that blue scan for assets we will get a little window out input and output here and then we'll get a little progress just letting us know that scannings happening. And this should kind of step us through some of the progress.

scanning performance is going to obviously vary based on your normal network scanning and you know, network based software performance is needing, you know, what kind of bandwidth what kind of hardware is it running on? How big is a network we're scanning.

So depending on your parameters, you can expect a little bit of different performance. I've done some pretty intense scanning testing over the last couple of months on these assessments. And in generally, I'm seeing them finish in about a HELOC.

On a larger network, smaller ones sometimes it's just a couple of minutes. I'm hoping that our 50 Scan here is going to not make me a liar on our video today.

And you can see here as it scans it will just let us know hey, we've got 50 IPs that we're scanning. So, again, if you were scanning your slash 24 normal slash 24 site or network scan, which is probably the most popular you would, you know get your 255 or 256 there with the number of IPS it's going to be scanning so this will just give you a little indicator and then as the scans are running, it will populate and tell you what IP is it scan if it detects a device that will light up with a green check. And then we'll also try to resolve for host names. So, we can see here looks like we've got our Comcast modems at net 0.1.

So there's our first 10 You can see and then, as it discovers additionals we should be able to kind of scroll through that list up and down.

So we're gonna let this thing kind of scan away. And while this is scanning I want to take just a moment to talk about the documentation.

We've got a step by step guide, or the assessment scanning that I'm doing here. So, if you'd like to look at documentation and not try to follow the video you can you can grab the doc and it's got step by step instructions, you know, with screenshots on how to how to run this scan, we each of those fields are in some examples of how to fill in some of the credentials if you're not sure

though, for those of you that like to follow the docs, those are out there. Alright, I will navigate to those docs at maybe at the end of this video. Just to show you guys so if there's anyone that wants to find them, they know where they're at. This is almost done you can kind of see is scanning in groups of 10 done done is 40 So far, so it looks like just a couple more moments and we will be we'll be wrapping up our first 50 Scan here.

So again, depending on your IP range, that first or second step we defined when we told you what we wanted to scan this time, may take a little bit longer or shorter depending on what you're doing.

And then again, credentials are really important on the scans, write them the credentials. If we if we can get into devices we can get into the servers we can get into get into equipment. We're going to be able to give you better insight, better scanning capabilities, better asset discovery that will take place.

And there we go. So, we've got a couple you can see we've picked up a couple of different Comcast devices. So, if we got a couple of modems looks like we've got some kind of Amazon device and turned out 50 That should show that should just about be wrapping this up here.

And again, you can see our output window, date and time stamps this thing as the scans running and also if it's been what's been what's failing, right and failing is failing, meaning we can't log into the device or we can't do a vulnerability scan on set device.

Right because we made a tech a device, a smart device or internet connected device that is on the network does have an IP but that doesn't mean we can necessarily at peace, I'm sorry, vulnerability scan for it right.

So now that we're done when the scan is complete, your next button will light up blue. That's how you know you're ready to go to the next step.

So once we get here, we've got two options. You can download now, which will let us literally download. I hit Next it's going to download the assessment report that it just collected.

And then we're going to use that download and we're going to upload it back to our CyberCNS instance.

Now this is a great option if you're mobile. Maybe you don't have access to internet, because you could obviously run a scan on a network that doesn't have internet.

And then you can't upload to the server. Right? You can't upload it if there's no internet so you could just download it and then bring it back to the office later and then do your upload.

Alternatively, if you do have internet, you can go ahead and provide your login to your CyberCNS instance here and then it will allow you to go ahead and upload.

So you can choose either option here, I'm gonna go ahead and just do our download here. Make it a little faster. So, that will download the folder. It's just found in my downloads location. It's letting you know okay, you're all done and we're ready for a new assessment. You just tap Finish and this will take you back to step one and now we're ready to run another assessment scan here. So, maybe I wanted to do a second network, another small from two range, I could go ahead and select that.

Otherwise, I am ready to go back to our CyberCNS back to the assessment view and then I'm going to tap that upload assessment.

This is where we're gonna give it a name. So, enter company name so maybe I was at a prospect site right and I'm just gonna say prospects. company

so I entered that prospects company name in here, choose my file, and then I'm going to go ahead and upload my assessment so my downloads folder I've got the the files called assessment download, if you download it, okay, so we're going to grab that assessment download.

We're going to tap Save.

We will get a process initiation at the top right, that'll let you know that it's uploading the assessment report. And then what we should see in the top window is that company name should appear in the list. So, I can see here prospects company name a few seconds ago.

I tap on that. This will load up the information that we've collected from that from the assessment scanning.

It will default by taking to the open source dashboards where you've got all these standard reports that come with CyberCNS and you could run against that data. You can also look down the menu on the left and start to see active assets. So, out of that scan. I found and picked up these assets. So, again I can see I've got some kind of device at this address looks like our Comcast modem. It does not support vulnerability scanning. Otherwise I would have got some additional info. But you can kind of see that here just by kind of looking. Same thing here. Couple internet connected devices that we don't have vulnerability scanning for. But I did pick up this one looks like we got a workstation, our STL legend and you can see this one did pick up and do a vulnerabilities in and then just like all your other CyberCNS assets, we bring you the same information across we can see the remediation. So, this particular assets got a old version of Snagit right, so we've got a recommended 2023 version there on Snagit 13. We've got two vulnerabilities here. And again, there's the evidence right there to show you there's the installed version numbers and then how that's impacting this particular machine scoring.

So any of the assets we discover in any of the scans that are done, they will populate these windows and then under our remediation plans. You know, hopefully you've got, you know, 100 assets that you've scanned. And this is where we would start to gather all of that intel about what we've scanned and how vulnerable those machines are.

We can go the standard report section and then we could use any of the standard reporting to produce perhaps a vulnerability report or a compliance report or the asset report for the client right on the spot. So, you know, we've got our asset vulnerabilities here or vulnerability overviews. So, I can output these right on the spot and then maybe I'll just use my word option one here. So, just tap on that word I Word icon. This will start your download and open up this word back here.

So again, this is prepared for that prospects name.

Discovery settings on the instance we didn't actually use a probe wouldn't nothing's going to show up there. But again, there's the asset that we discovered during our scan. You picked it up, telling you what product what severity what that score looks like against the vulnerability and then what CVE article particular than that vulnerability is that NIST provides to us. So, you know, if I if I knew this article, I can go and look this up. And then obviously that assets got that information in real time. Right? So if I'm if I'm looking at a machine and I want to look at the vulnerabilities I can see right here, here's that CVE for that machine for Snagit by tap that it will take us straight out to the NIST site, link us out to that detail. And we can see right here in Techsmith Snagit version through injection of XML.

And it'll talk about solutions and how to fix it and known issues and so on and so forth. So, really good data. Write really quickly about what's out there, what's vulnerable.

And then again, down our left menu you're able to use any of the scan results data against that customers scan that just took place. So, again, the vulnerabilities this is kind of your Overview Dashboard and heads up of all the vulnerabilities broken out by operating system and then the counts based on severity, and how the risk score is weighted against those vulnerabilities that we found.

If you were doing your Active Directory, had you provided Active Directory credentials or Active Directory info, this would have populated the customer's Active Directory data. Again, if you're using this on any of your normal companies, this would allow you to get some quickly digestible heads up information about their environment, how many users how many computers, how many years how many GPO so on and so forth. Right network scan findings this will do some known scans of different ports across SSL certificates and different web protocols and bring some awareness to how they're impacting again, the overall compliance and vulnerability scoring will show you the severity what the score is for CDSS. And what the assets are affected are and again, if you tap these golden, we'll break them down and tell you hey, that's this is the particular asset.

And it'll link actually linked history to it. You can see how it took me straight down to that asset I'll click any one of these that you drill to do this.

And then you've got the asset level network scan. So, this is basically everything in one view, buys by the CVE. This is by the asset with the CVE is broken out across the plains and then you can kind of see here the accounts again.

So network scan findings.

And then lastly would be your jobs. So, jobs are just going to show you any of the uploads that you're doing so if you're doing a bunch of scans and a bunch of uploading, this will will kind of let you know what's going on. If you're waiting to see Job's process.

And then lastly, again, you talked about the standard reports. But then you've got the overview. The overview is where you can go back to the main company view for that for that customer and it will populate any of the dashboard any the reporting data that we've collected about them.

And again, we're just on the overview, but we would be able to you know, change this to any of the any of the reports right that we got would be available to this got to this prospects data. So, again, if you wanted to pull, you know, certain reports or certain data out you can you can switch these using our reports for the overviews and that is our assessment view.

So that is really it in a nutshell, right? It's the ability to do a quick scan, not leave behind an agent not leave behind any software insight and some discovery and be able to have a more intelligent conversation about how your security services and potentially managed services kind of coexist there right this is a really great sales enablement tool to allow you to show how quickly you can come in.

Take an x ray and more importantly have a have the prescription to fix it right when when we're done.

So this is a this is a great way to do that a prospects level and it's so I talked about documentation. So, before we leave today, if you know where the docks at, you know how to find documentation, you know, this is a good starting point.

Thank you for watching otherwise, for those of you going to stick around just for another few seconds here. I'm going to show you where the docs are at for this in case anyone has any trouble finding right so I'm going to just go navigate out to our connectsecure.com website and we're going to go up to the resources support.

We're going to go to View documentation.

And then from here, I'll just type the word assessment. So, you just start typing assessment.

You can either enter or click that or click the result but it's that one off assessment skins it's the very first result of the type assessment. This doc will walk you through step by step with screenshots about how to install each of the different supported OS types. And then how to run the wizard.

The credentials I mentioned to access the assessment wizard or their admin password again if you want to change it again. But this doc will walk you through screenshot by screenshot how to set this thing up with examples. So, if you guys want to use the doc it's out here. Got the video, let us know if there's other content we can do around this. Be happy to do a part two, comment the video or drop us an email at education@connectsecure.com. Let us know and if you have any issues with it. Let us know get in touch with our support team at support@cybercns.com. Thank you guys again for watching.