Identify Vulnerable Devices in Your Network Automatically

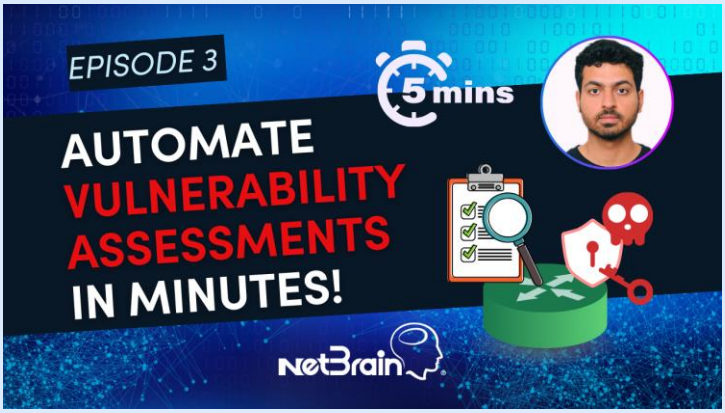
Automation Skills Drill

SKILLS DRILL #3

Are my devices vulnerable?

See how engineer, Sahil, checks each device in the network for CVE vulnerabilities automatically using NetBrain in just **five** minutes without coding!

Watch Video ▶



Ready to start automating? Learn the exact skills used in the video to build your own custom continuous assessments with self-paced tutorials from NetBrain University!

- NetBrain Parser Course 1: Overview of the NetBrain Visual Parser (17 minutes)
- NetBrain Parser Course 2: Parse CLI output quickly with Auto-Parser (7 minutes)

- NetBrain Intents Course 1: Overview of NetBrain no-code Network Intents (8 minutes)
- NetBrain Intents Course 2: Choose the correct Parser (6 minutes)
- NetBrain Intents Course 3: Learn the basics of building your diagnosis logic (7 minutes)
- NetBrain Intents Course 4: Configure diagnosis result messages and alerts (12 minutes)

Want to automate checks for CVE vulnerabilities?

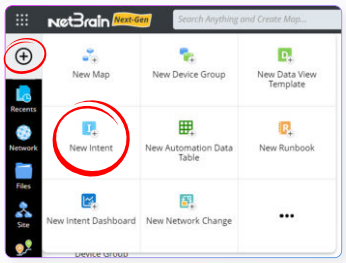
Our quick reference guide condenses the key concepts into one handy resource to create automated checks of each device in your network for CVE threats in under 5 minutes! Can you beat the clock?

Go to the Cheat Sheet ❱

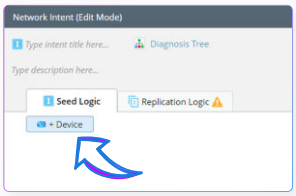
Step 1. Create a Network Intent

Automation in 5 minutes! 05:00

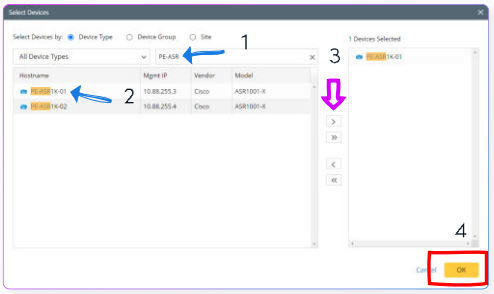
a. Click "⊕" to create a "New Intent".



b. Click "+ Device" to add a seed device.



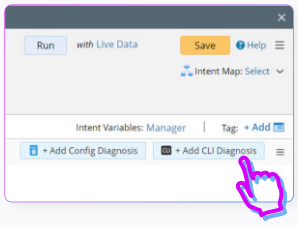
c. Search for and select any device potentially affected by a CVE.

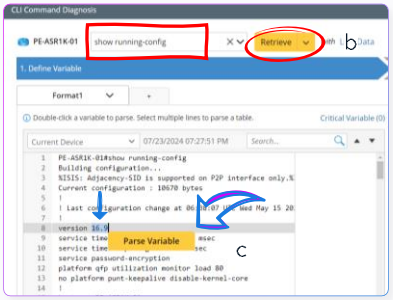


Step 2. Define Your Variables

04:40

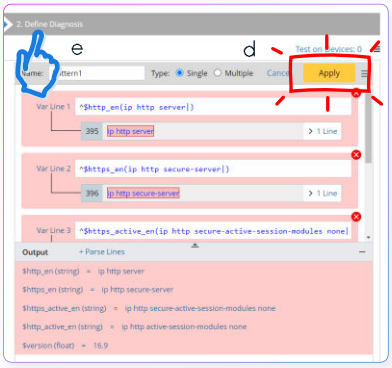
a. Click "+ Add CLI Diagnosis" to add your assessment logic.





b. Type the command to identify the vulnerability like "show version" or "show run" and click "Retrieve".

c. Highlight any output identifying a potential vulnerability & click "Parse Variable".



d. Click "Apply" at the top right to save the output as variables.

e. Click "Define Diagnosis" to build out your assessment logic.

03:30

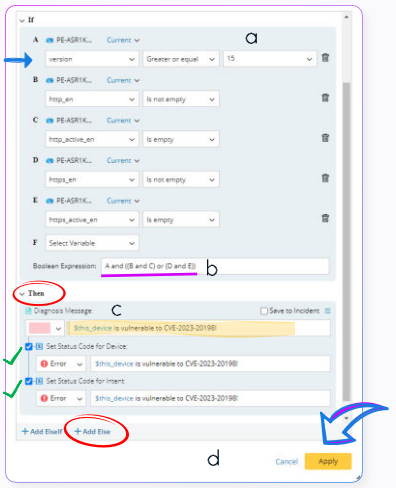
Step 3. Build Your Automation Logic

a. Under "If", choose the variables you want to examine, apply argument operators such as "Greater or equal", and add the compare values.

b. Write a Boolean expression that defines when a device is vulnerable.

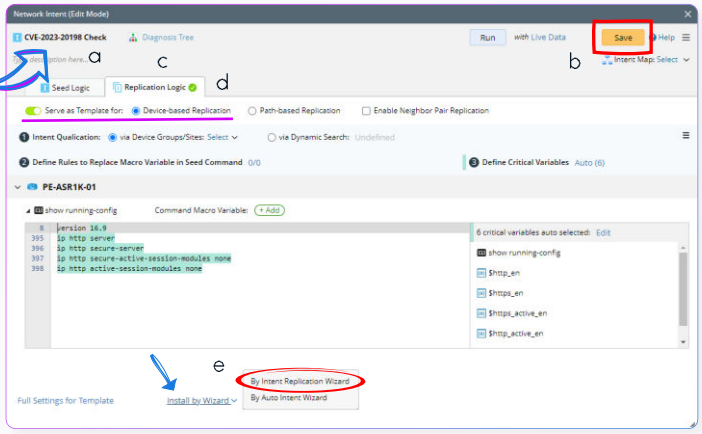
c. Under "Then", write a message to communicate vulnerability and set that as the device and Intent status codes.

d. Click "+ Add Else" and write a message to communicate the device is not vulnerable and click "Apply".



Step 4. Save Your Intent

Beat the clock! 02:30



a. Edit the name and give your Network Intent a name.

b. Click "Save" and choose a save location within the Intent Manager.

c. Click the "Replication Logic" tab.

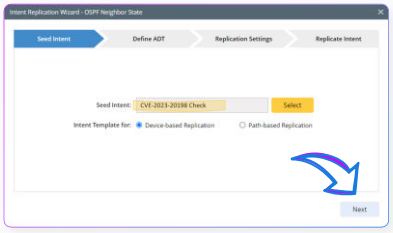
d. Select "Serve as Template for:" and "Device-based Replication".

e. Click on "Install by Wizard" and select "By Intent Replication Wizard".

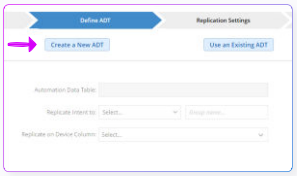
Step 5. Replicate and Assess Continuously

01:40

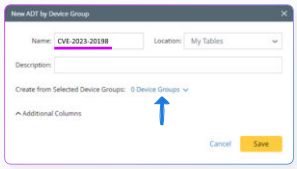
a. Select your Intent as the "Seed" and click "Next".

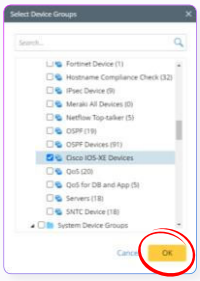


b. From the "Define ADT" tab, select "Create a New ADT" to store your automation results.



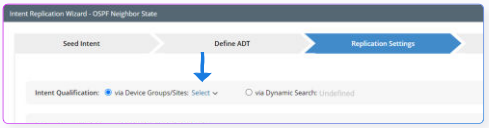
c. Choose your ADT name and device group.





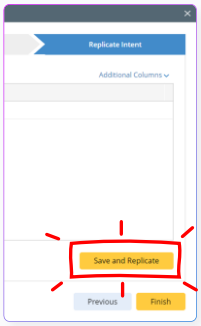
d. Create or select a device group that identifies affected device types.

e. Click "OK" and then "Next".

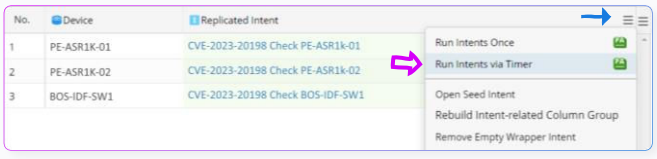


f. From "Replication Settings", select "via Device Group" and choose the affected group again.

g. From "Replicate Intent", click "Save and Replicate" and then click "Open Output ADT" to see assessments for every firewall.



h. Click "Run Intent via Timer" from the burger menu on the Intent column to continuously assess.



i. Set the frequency you'd like and click "OK".

00:00