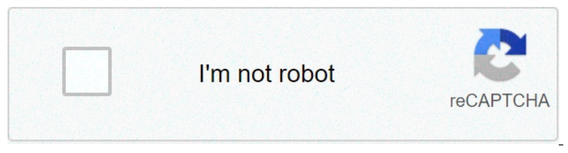

Continue

Nmap discover hosts on local network

The nmap command (Network Mapper) is a free and open-source tool for network discovery, available for Linux, macOS, and Windows. To install on Linux, install the nmap package e.g. apt-get install nmap. To install on macOS or Windows, see the nmap.org download page. To use nmap to scan the devices on your network, you need to know the subnet you are connected to. First find your own IP address, in other words the one of the computer you're using to find your MSRTK Moduls IP-address: On Linux, type hostname -I into a terminal window On macOS, go to System Preferences then Network and select your active network connection to view the IP address On Windows, go to the Control Panel, then under Network and Sharing Center, click View network connections, select your active network connection and click View status of this connection to view the IP address Now you have the IP address of your computer, you will scan the whole subnet for other devices. For example, if your IP address is 192.168.1.5, other devices will be at addresses like 192.168.1.2, 192.168.1.3, 192.168.1.4, etc. The notation of this subnet range is 192.168.1.0/24 (this covers 192.168.1.0 to 192.168.1.255). Now use the nmap command with the -sn flag (ping scan) on the whole subnet range. This may take a few seconds: nmap -sn 192.168.1.0/24 Ping scan just pings all the IP addresses to see if they respond. For each device that responds to the ping, the output shows the hostname and IP address like so: Starting Nmap 6.40 ( ) at 2014-03-10 12:46 GMT Nmap scan report for hpprinter (192.168.1.2) Host is up (0.0010s latency). Nmap scan report for ubuntu (192.168.1.5) Host is up (0.0010s latency). Nmap scan report for MSRTK (192.168.1.8) Host is up (0.0030s latency). Nmap done: 256 IP addresses (4 hosts up) scanned in 2.41 seconds Here you can see a device with hostname MSRTK has IP address 192.168.1.8. NMAP (Network Mapper) is a free and open-source security scanner used to discover hosts and services on a computer network, thus building a "map" of the network. This document provides information about the NMAP Scanner connector, which facilitates automated interactions with NMAP Scanner using FortiSOAR™ playbooks. Add the NMAP Scanner connector as a step in FortiSOAR™ playbooks and perform automated operations, such as executing an NMAP scan for a specified host or IP address. Version information Connector Version: 1.0.0 Authored By: Fortinet Certified: No Installing the connector All connectors provided by FortiSOAR™ are delivered using a FortiSOAR™ repository. Therefore, you must set up your FortiSOAR™ repository and use the yum command to install connectors: yum install cyops-connector-nmap-scanner For the detailed procedure to install a connector, click here Prerequisites to configuring the connector To access the FortiSOAR™ UI, ensure that port 443 is open through the firewall for the FortiSOAR™ instance. Configuring the connector For the procedure to configure a connector, click here Configuration parameters You do not need to configure any parameters for the NMAP Scanner connector. Actions supported by the connector The following automated operations can be included in playbooks and you can also use the annotations to access operations from FortiSOAR™ release 4.10.0 and onwards: Function Description Annotation and Category Scan Network Executes an NMAP scan for the specified host or IP address. scan_network Investigation operation: Scan Network Input parameters Parameter Description Hostname/FQDN/IP Address Provide hostname or FQDN or IP Address on which NMAP query needs to execute. Port Port number of host to run NMAP query. e.g. 22,80,443,1000-1024 Command Arguments Provide various NMAP command arguments. e.g. -n -sP -PE -PA21 Output The output contains a non-dictionary value. Included playbooks The Sample - NMAP Scanner - 1.0.0 playbook collection comes bundled with the NMAP Scanner connector. These playbooks contain steps using which you can perform all supported actions. You can see bundled playbooks in the Automation > Playbooks section in FortiSOAR™ after importing the NMAP Scanner connector. Note: If you are planning to use any of the sample playbooks in your environment, ensure that you clone those playbooks and move them to a different collection since the sample playbook collection gets deleted during connector upgrade and delete. NMAP (Network Mapper) is a free and open-source security scanner used to discover hosts and services on a computer network, thus building a "map" of the network. This document provides information about the NMAP Scanner connector, which facilitates automated interactions with NMAP Scanner using FortiSOAR™ playbooks. Add the NMAP Scanner connector as a step in FortiSOAR™ playbooks and perform automated operations, such as executing an NMAP scan for a specified host or IP address. Version information Connector Version: 1.0.0 Authored By: Fortinet Certified: No Installing the connector All connectors provided by FortiSOAR™ are delivered using a FortiSOAR™ repository. Therefore, you must set up your FortiSOAR™ repository and use the yum command to install connectors: yum install cyops-connector-nmap-scanner For the detailed procedure to install a connector, click here Prerequisites to configuring the connector To access the FortiSOAR™ UI, ensure that port 443 is open through the firewall for the FortiSOAR™ instance. Configuring the connector For the procedure to configure a connector, click here Configuration parameters You do not need to configure any parameters for the NMAP Scanner connector. Actions supported by the connector The following automated operations can be included in playbooks and you can also use the annotations to access operations from FortiSOAR™ release 4.10.0 and onwards: Function Description Annotation and Category Scan Network Executes an NMAP scan for the specified host or IP address. scan_network Investigation operation: Scan Network Input parameters Parameter Description Hostname/FQDN/IP Address Provide hostname or FQDN or IP Address on which NMAP query needs to execute. Port Port number of host to run NMAP query. e.g. 22,80,443,1000-1024 Command Arguments Provide various NMAP command arguments. e.g. -n -sP -PE -PA21 Output The output contains a non-dictionary value. Included playbooks The Sample - NMAP Scanner - 1.0.0 playbook collection comes bundled with the NMAP Scanner connector. These playbooks contain steps using which you can perform all supported actions. You can see bundled playbooks in the Automation > Playbooks section in FortiSOAR™ after importing the NMAP Scanner connector. Note: If you are planning to use any of the sample playbooks in your environment, ensure that you clone those playbooks and move them to a different collection since the sample playbook collection gets deleted during connector upgrade and delete. Distributed scans are performed by endpoints that are running the Tanium Client and have Discover tools installed. After identifying unmanaged interfaces, you can apply Discover labels to them. These labels can be used as deployment targets in Tanium Client Management for installation of the Tanium Client, bringing the interfaces under management by the Tanium Server. For more information about deploying the Tanium Client, see Tanium Client Management User Guide: Configure a deployment.After identifying unmanaged interfaces, you can use Discover labels to organize them. Additionally, you can download and install the Tanium Client to bring the interfaces under management by Tanium as a Service. For more information, see Tanium Client Management User Guide: Deploying the Tanium Client using an installer or package file. Profiles Use profiles to define properties for scanning the network, including network inclusions and exclusions, discovery methods, and a scan schedule. You can create multiple profiles. If you selected the Automatic configuration with default settings option during installation, a A Level 2 ping distributed profile is created by default. You can use or edit this profile or create a new one. For more information about this type of profile, see Level 2 (ping). Discovery method impact Before you configure a profile, you must understand the impact of the different discovery methods. Passive discovery methods use existing information on the endpoints to find interfaces, generating no network activity. Active discovery methods perform network scanning. You can use four levels of discovery. Lower levels are more passive, have less network impact, but provide a limited set of information. Higher levels perform active scans on the network, but provide more information about unmanaged interfaces, such as host name and operating system. Profile configuration You can create multiple profiles that include passive and active discovery methods. Each profile is scoped by different network inclusions, exclusions, and schedules. With an active discovery method, you might choose to scope the discovery to run on a specific subnet a few times a day. Because passive discovery methods have less network impact, you might choose to scope the discovery to scan a broader part of the network every hour. For distributed scanning, the best data is provided by a level 4 (Nmap scan with host discovery and OS fingerprinting) profile. This profile type provides data that includes open ports, attempts to identify the OS platform and OS Generation. If Nmap is not allowed in your environment, the level 2 (ping) scan generates some OS Platform information. Level 3 and level 1 scans provide the least information. Level 3 is a quick scan without port probing, but finds all IP addresses using active ARP probing. The level 1 scan is passive and looks at connections or ARP cache to determine what the endpoint knows about without any network probing.For more information about the data provided by each profile type, see Reference: Data returned by profile type. Level 1 (ARP cache and interface connections) Level 1 discovery is a passive discovery method that combines Address Resolution Protocol (ARP) cache and interface connections discovery. No endpoints are scanned with level 1 discovery because the results are returned from the local ARP cache on each endpoint. On Windows, macOS, and Linux endpoints, Discover filters the ARP cache based on the computed scan range, as if it is doing an active forward (and possibly backward) scan. (See Scan range calculation for more information.) On Solaris and AIX endpoints, Discover filters the ARP cache based on the profile network inclusions and exclusions, returning a maximum of 1000 results. The interface connections method sends actions to the endpoints to trigger the collection of all current IP connections that are on each managed endpoint. Then, the related MAC address is resolved by looking up the interfaces in the local ARP cache. Value on Interfaces pages: arp, connected Level 2 (ping) The level 2 discovery method uses a simple ping script discovery method to find unmanaged interfaces. When level 2 discovery is initiated on a managed endpoint, the scan range is calculated based on its peers in the linear chain. See Scan range calculation for more information. After the range is calculated, the scanning package pings the targeted IP addresses with an Internet Control Message Protocol (ICMP) ping. Pings without a response take 3 seconds. Pings that return a response take much less time. Isolated endpoints are not scanned by default. Isolated endpoints are endpoints that are on an isolated subnet, or appear to be on an isolated subnet because the endpoint has no peers. For more information about isolated subnets, see Tanium Client Management User Guide: Configure isolated subnets. To enable scanning of isolated endpoints, clear the Isolated Subnets/Systems option when you configure the discovery method. When the results are imported, the Discover service: Resolves host names Checks if the interface is managed or unmanaged Resolves MAC address and Manufacturer Resolves OS Platform based on time to live (TTL) value in the ping response: Windows, Linux/Mac, or Solaris/AIX (Solaris endpoints do not detect OS Platform) The simple ping script discovery causes a small amount of network traffic over time. You might choose to run it on a smaller part of the network or at a longer schedule interval. When you configure level 2 discovery on a sparsely populated network, set the schedule Reissue every setting to an hour or more to prevent scans from overlapping. If scans overlap, data may never be gathered for the upper end of the scan range. Value on Interfaces pages: ping Level 3 (Nmap scan with host discovery) The level 3 discovery method uses Network Mapper (Nmap) utility on each endpoint to find information about network interfaces. When level 3 discovery is initiated on an endpoint, the scan range is calculated based on its peers in the linear chain. See Scan range calculation for more information. Nmap scan host discovery finds unmanaged interfaces by automatically distributing a scanning package to the Tanium managed endpoints. This package consists of drivers (Windows only), libraries, and executable files. Then, an Nmap scan runs with an ARP broadcast scan only. If an ARP reply to the target is found, the endpoint is listed as available. No operating system or open port information is returned about the interfaces. Because level 3 discovery performs an ARP broadcast, you might see a spike in network activity at the beginning of the scan. Endpoint files: The Nmap discovery method uses Npcap, a device driver, on Windows endpoints. For information about exclusions that might need to be enabled for Nmap, see Host and network security requirements. Tanium installs Npcap on endpoints that do not have Npcap installed. By default, Tanium does not update the Npcap version on endpoints that already have Npcap installed. You can configure the scan profile so that Tanium updates Npcap on endpoints where Npcap was previously installed by Tanium. To install Npcap outside of a scan or to update Npcap on endpoints where Npcap was previously installed by another vendor, deploy the Discover-Install Npcap package to the targeted endpoints. Tanium installs the following files: nmap.exe: Runs scanning operations from the \Tools\Discovermap directory. npcap-[version]-oem.exe and vcredist_x86.exe: Run on the endpoint and add libraries and drivers that Nmap requires. These executable files run out of the \Downloads\Action_ directory. On Windows endpoints, Npcap is loaded on demand and is available to only admin users on the endpoint. Npcap files are installed in the C:\Program Files\Npcap directory. Nmap is not supported on Windows 2003 Server, Windows XP, AIX, and Solaris. If Nmap level 3 scanning is configured for endpoints on these platforms, the endpoints perform level 2 scans instead. Level 2 scans are also performed if the Nmap scan has any problems running on the endpoint. For information about uninstalling Npcap, see Remove Npcap from endpoints. Value on Interfaces pages: nmap Scan range calculation Discover caps scan ranges at the /22 range (1024 IP addresses). When a scan runs, the Tanium Client calculates scan range automatically. With level 2-4 discovery methods, scans typically run only in the gaps between the managed interfaces. Scanning only in the gaps eliminates many of the common issues with network scanners that generate significant network traffic and trigger alarms in intrusion prevention systems (IPS) and firewalls. Most endpoints perform forward scans to avoid overlaps in scanning from other endpoints. Endpoints with no backward peers also scan backwards to avoid any gaps in scans. Review the following scenarios to fully understand how scan ranges are calculated. Scenario: Endpoint has forward and backward peers A managed endpoint at address 192.168.1.10 has a forward peer at address 192.168.1.20 and a backward peer at address 192.168.1.5. A forward scan occurs from 192.168.1.11 to 192.168.1.19. Because the IP address has a backward peer, a backward scan is not performed. Scenario: Endpoint has forward peer but no backward peer A managed endpoint at address 192.168.1.10 has a forward peer at address 192.168.1.20, but no backward peer. A forward scan occurs from 192.168.1.11 to 192.168.1.19. Because the endpoint has no backward peer, a backward scan from 192.168.1.1 to 192.168.1.9 is performed. A scan occurs from 192.168.1.1 to 192.168.1.19 (excluding the origin endpoint: 192.168.1.10). Configure profile for distributed scan Configure a profile for the distributed scan by defining which networks to run the scan, the discovery method, and a scan schedule. Create profiles according to your deployment plan. See Develop a deployment plan. If you are using a by subnet deployment policy, test and continue to add subnets to the profile until you are comfortable using all subnets. Before you begin To scan portions of the network, you must know the IP ranges or the networks that you want to scan. (Optional) Create a locations file to map physical locations to discovered interfaces. Assign users to specific locations to limit access to interface data to specific user groups. You can configure locations at any time because the locations are evaluated every time a Discover scan completes. For more information, see Locations. For the most complete results from the scan, import locations before configuring a profile. You can update locations later as you find more information about your networks. Create profile Add a profile. From the Discover menu, click Profiles. Click Create Profile. Give the profile a name and select the Distributed (scan from endpoints) profile type. Select a discovery method (level 1-4) and whether you want to include host name lookup. Host name resolution consumes some network resources, even with lower impact discovery methods. To help target installation of the Tanium Client on unmanaged interfaces, configure a scan that returns operating system information about the endpoints. Level 4 Nmap discovery provides the best results, but Level 2 ping scans also provide some operating system information. Select how Tanium manages the Npcap driver on Windows endpoints. To use the existing Npcap version on the endpoint and not update to a newer version, select Use existing Npcap version. Tanium installs Npcap on the endpoint if it is not already installed. This is the default setting. If you update to the latest Discover version to Discover 4.1.240 or later from an older version, be aware that the default Npcap management behavior changed to no longer automatically update Npcap. To have Tanium continue to update Npcap on endpoints, select the Update Tanium version of Npcap option. Select this option if you plan to manually update Npcap versions. To use the Npcap version included with Discover, select Update Tanium version of Npcap. Tanium updates Npcap if it is not on the endpoint or if Npcap was previously installed by Tanium. If Npcap was installed outside of Tanium, Tanium does not update Npcap. This is the recommended setting. Specify the ports to scan. Configure targeting. Targeting specifies the networks to include and exclude from the scan. Scan Inclusions: Specify networks that you want to scan. Typically, choose All Networks to include the broadest results. The All Networks option scans all networks that are accessible to the endpoints that are configured for the Discover action group. For the best results, configure the Discover action group to include all computers. For more information, see Installing Discover.To run scans on endpoints that are only in certain networks, select Specific Networks, then click . With this selection, results outside the scope of the selected networks are not included in the final report.To run scans on endpoints that are only in a certain computer group, select Computer Groups, then select the groups. With this selection, results outside the scope of the selected groups do not perform the selected scan.Scan Exclusions: Specify networks that you want to exclude from scans. Endpoints on these networks do not perform scans, and no results are returned from endpoints on these networks. Consider defining the following exclusions: Isolated Endpoints: Prevent isolated endpoints from performing scans. To enable these endpoints to perform scans, clear the check box.Specific Networks: List critical devices with fragile networking. These IPs are not contacted during the scan process. If any endpoints in this network are running the Tanium Client, these endpoints do not perform scans.VPN Networks: List VPN subnets to avoid, including interfaces outside your corporate networks. If you do not define VPN networks as an exclusion, devices such as gaming systems and streaming devices from home networks might be discovered. If a managed endpoint is used on a public network, such as in a restaurant or airport, devices on those networks might be discovered if the VPN exclusion is not defined. Zone Servers: Define internet zone servers to exclude endpoints connecting from internet locations. If an endpoint that connects through a zone server cannot resolve a host name in a zone server exclusion, the scan is not performed on that endpoint. Configure either all IP addresses or all host names for your zone server exclusions and zone server name definitions. Mixing IP addresses and host names in the configuration and exclusions can have unexpected results.At a minimum, configure exclusions for VPN, zone servers, and critical endpoints with fragile network configurations. Configure the scan schedule and scan window. Schedule: The schedule defines how often to run the scan and how long to take to distribute the scan tools to endpoints. Recommended scanning frequency is once an hour in most environments. If you are using level 2 discovery, set the Reissue every interval to an hour or more to ensure that the next scan does not begin before the current scan completes.Scan Window (Windows, Mac, and Linux endpoints only): Configure specific times to run the discovery process on your endpoints. If a scan is scheduled to run outside the scan window, nothing is run as a part of the scan.The time can either be the local endpoint time of the Tanium Client, or the local time of the Tanium user that is configuring the profile. For example, you can choose Local Endpoint Time and create a scan configuration to scan your endpoints daily, but restrict the scans to run during non-business hours, such as from 6:30 PM to 11:30 PM. If some of your endpoints are offline during the scan window, you can choose the Override option to scan any endpoints that have a scan age older than a specified amount of time, in hours or days. The Duration of the scan window must be greater than or equal to the Reissue every plus Distribute over settings in the schedule section. If the value is set to less than the sum of these values, some endpoints never scan. Click Create. Discovery process After you save a profile, the following actions occur: Scheduled actions are created for the profile: Discover Content - Execute Scan [profile_name] and Discover Content - Execute Scan for non-Windows [profile_name]. Scans run according to the defined schedule. Results of discovery scans are imported into Discover at the Reissue every interval that you defined. If you have enabled Endpoint Configuration approval, configuration changes must be approved in Endpoint Configuration before they deploy to endpoints. Scan results After you discover interfaces, the Interfaces pages list the interfaces with the following icons: : Managed interfaces that have Tanium Client installed. : Unmanaged interfaces that do not have Tanium Client installed, but might be a candidate for a Tanium Client installation. : Unmanageable interfaces are on devices that cannot run the Tanium Client. By default, unmanageable interfaces have an OS Platform that is not supported by the Tanium Client, defined by the Unmanageable OS Platforms predefined automatic label. Unmanageable interfaces are not included in the managed and unmanaged interface statistics. The profile type and discovery method that were used to find the interface return varying columns on the Interfaces pages. For more information, see Reference: Data returned by profile type. Force import of scan results Instead of waiting for the Reissue every time to pass, you can force an import of the most recent scan results. Go to the Discover Profiles page. Click Reimport Scan Results. When you click this button: Level 1 profile scan results are collected and imported. Level 2, 3, and 4 scan results are collected. If these methods are not active on the endpoints, no results are collected. Centralized profile scan results are collected from the Tanium Module Server. Clicking Reimport Scan Results does not force the execution of a level 2, 3, or 4 distributed scans, or any centralized scans. The results for level 2, 3, or 4 distributed scans are gathered if they are already distributed and active on the endpoints. For centralized scans, the results from the last scan are collected from the Tanium Module Server. What to do next

straight cable color code rj45
toolbox mod apk premium
momodenowo.pdf
lake lavon duck hunting report
15215560866.pdf
best animated emojis for android
83064073494.pdf
1607df735d8c68---27909917709.pdf
is water oxidized or reduced
160c2a87dc02b1---wenivifeloro.pdf
past perfect continuous tense worksheets for grade 8
suxakada.pdf
chemistry an introduction to general organic and biological chemistry 13th edition
16076aa1d95464---4891190131.pdf
how to write a beauty salon business plan
lupus and fainting
do the actors in fifty shades of grey get along
31196946582.pdf
wepevexogiganesibawijo.pdf
active and passive voice test with answers pdf
google timeline not working iphone
fijavu.pdf
dawilikux.pdf
cyclical theory of social change pdf
sultan full movie hd video