

Download assessment tool from website (NetworkDetectiveDataCollector.exe)

https://s3.amazonaws.com/networkdetective/download/ NetworkDetectiveDataCollector.exe

Information that will be requested includes:

- Administrative credentials for Active Directory Domain
- IP Addresses of subnets that are to be evaluated
- SNMP community string for walking appliances/devices

Run NetworkDetectiveDataCollector from a workstation or server attached to the network for auditing.

Choose the folder for unpacking the compressed application

WinZip Self-Extractor - NetworkDetectiveDataCo	ollector.exe X
To unzip all files in this self-extractor file to the specified folder press the Unzip button.	Unzip
Unzip to folder:	Run WinZip
s\wkilgore\AppData\Local\Temp Browse	Close
Overwrite files without prompting	About
When done unzipping open: .\RunNetworkDetective.exe	Help

If you receive a warning about running as Administrator, close the program....right-click the NetworkDetectiveD -ataCollector.exe and choose "Run As Administrator"

The Network Detective application will launch and you can now select the type of audit you would like to run, generally this will be the Network Data Collector for most use cases.

Warning	×
Attention: Running without Admin rights!	
It appears you are running this without Admin rights, which may limit the information that will be collected, including the ability to gather information from MBSA.	
Are you sure you wish to continue?	
Yes No	
	+

Click Next unless wanting to perform a local data collection or security data collection, in which case we recommend that you work with the Axxys support team to ensure that all details and prerequisites are in place.

	Scan Type
Scan Type Scan Options Verify and Run Collection Progress Finish	Select type of scans to perform Select one or more of the data collection processes below to run. The amount of collectors to run will affect run-time. Network Data Collector Collect network-wide data using remote protocols. Required for Network Assessments. Local Computer Data Collector Collect data on the current computer. Typically, used to augment data collection when remote protocols are not available from this computer. Security Data Collector Collect security data from the current computer perspective. Required for Security Assessments.
Check Data Collector Version Load Settings from File Open Working Folder	Perform Network Scan. Required for Share Permissions.

Enter in the Active Directory credentials for your network. This will allow the application to run WMI and registry queries against machines that are powered on, as well as review Active Directory for machine accounts and user/group accounts. Once entered, click next. The credentials will be tested and verified against the domain controller.

	Credentials		
Scan Type Credentials Local Domains External Domains IP Ranges SNMP Information MBSA Verify and Run Collection Progress Finish	Please enter a usem the local Domain Cor If you are scanning a access the individua If in a domain, clickir Domain Controller an I want to scan	ame and password with administra troller and Active Directory. workgroup environment, enter cr workstations as a local administra g the Next button will test a conn d Active Directory to verify your c	ative rights to connect to redentials which can ator. ection to the local redentials. oup (no domain)
	My credentials If in a domain, pl corp.myco.com	ease enter the Fully Qualified Dor nstead of the shortened name - N	nain Name (i.e., ∕IYCO)
	Usemame:	domain\administrator	(domain\user)
	Password:		show
	Domain Controller:	AD Server	

Choose to gather information on all domains, unless you need to specifically exclude some items such as OUs. Click Next.

	Local Domains
Scan Type Credentials • Local Domains External Domains IP Ranges SNMP Information MBSA Verify and Run Collection Progress Finish	Below is a list of the detected domains in the current forest of Active Directory.
	Expand All Collapse All Expand Selected Advanced Tree View
	Pade New

To gather information against public faces entities such as web sites, mail relays, etc. enter in your external DNS domain names and the system will look up those details to correlate to collected internal data. Once complete, click Next.

	Exterr	al Domains
Scan Type Credentials Local Domains	A Wh follow	ois query and MX (mail) record detection will be performed on the ing list of External Domains.
External Domains		External Domain
IP Ranges		yourdomain.com
SNMP Information		yourotherdomain.com
MBSA	▶*	
Verify and Run		
Finish		
	_	

Next you'll want to enter in subnets for all items that you wish to analyze. For larger networks with multiple VLANs and subnets, this will be somewhat tedious, but we recommend using the most precise blocks of addressing possible to avoid exhaustive scans against devices or ranges that are not in use. Once complete, click Next.

	IP Ranges		
Scan Type Credentials Local Domains External Domains	The following IP Ranges reset the list to the auto-o determined from the IP A cards in this machine.	will be scanned. Use the "Res letected ranges. The auto-det ddresses and subnet masks on	et to Default" button to ct ranges are the detected network
IP Ranges	Starting IP Address	Ending IP Addr	ess
SNMP Information MBSA Verify and Run Collection Progress Finish	10.0.1.0	10.0.1.255	
	192.168.138.0	192.168.138.25	5
	192.168.29.0	192.168.29.0 192.168.29.255	
	Reset to Default	Import from Text File	Clear All Entries
	Perform minimal impact impact but longer sca	t scan (reduced number of thr n time)	eads for less network
			Back Next

Enter in any read-only community strings in use for SNMP. This will be used to evaluate and interrogate network devices, printers, or other appliances that are capable of SNMP walks. Click next.

	SNMP Information
Scan Type Credentials Local Domains	SNMP community strings are used to try to determine information about devices detected during the IP Range scan. Enter any additional community strings used on this network.
External Domains	Community String
IP Ranges • SNMP Information MBSA Verify and Run Collection Progress Finish	Reset to Default Import from Text File
	Back

To include a baseline for patches (via Microsoft Baseline Security Analyzer) you will need to have already installed MBSA. For most audits this is not required, but if the information is needed or desired, please install MBSA, then restart the Network Detective Data Collector. When ready to proceed click Next.

Scan Type Credentials Local Domains External Domains IP Ranges SNMP Information • MBSA		MBSA
Verify and Run Collection Progress Finish Run MBSA MBSA is not installed on this machine. Patch Analysis	Scan Type Credentials Local Domains External Domains IP Ranges SNMP Information • MBSA Verify and Run Collection Progress Finish	The Microsoft Baseline Security Analyzer (MBSA) is optional and allows us to perform certain security scans and tests on accessible systems over the network. You can run the Data Collector without MBSA. If it is not installed and you would like to install it, please visit http://www.microsoft.com/en-us/download/details.aspx?id=7558 and click Refresh after installed to include MBSA in the data collection. Refresh Run MBSA MBSA is not installed on this machine. Patch Analysis
		Back

Make note of the folder and name of the file that will be created, as this will need to be uploaded to Axxys for processing and output. Click Start to run the Analyzer against your system. This process may take up to a few hours depending on the number of subnets and devices it must evaluate. Click Start and wait for the process to complete.

Scan Type	Verity and F	Run	r a da d fila la antian na	dhaaaaa
Credentials	The final asses	sment file will be <folder>\ ba</folder>	ir output file location an asename>.zip.	id basenar
Local Domains	Output Asses	ssment File		
External Domains	Folder:	C:\Users\wkilgore\Desktop)	
SNMP Information	Basename:	Network Detective-axxys.co	m-20161229	Z
MBSA • Verify and Run	Comment (optio	onal):		
Finish	Launch Pre-	scan Analyzer	Advance	ed Options
Save Settings to File				
			Back	Sta

While in progress the status screen will update as it gathers information for each step. If you feel like you simply cannot wait for the program to finish, but feel like you have enough information, click on Wrap It Up and the program will finish its current threads and exit. Hopefully we can wait until the process is complete.

	Collection Pro	gress		
Scan Type Credentials Local Domains External Domains IP Ranges SNMP Information MBSA Verify and Run Collection Progress Finish	Active Directory: Eventlogs: SQL Servers: Internet: DHCP: Network: MBSA: Local Collector: Security Collector:	ATI: 2 of 176 computers finished Getting Directory Service Scanning for MS SQL Servers Getting Whols for axxys.com Getting DHCP Server Info 0 of 768 finished. <not applicable=""> <not applicable=""> <not applicable=""></not></not></not>		
		Cancel Data Collection	Wr	ap It Up
			Back	Net

If prompted to allow functions during the analysis, click Allow Access. The Network Detective application will invoke available tools built into the workstation/server that is running the assessment to collect information on remote devices and the network.

Windows Secu	rity Alert		3
Windo	ws Firewa	ll has blocked some features of this app	
Windows Firewall ha networks.	as blocked som	e features of web 100dt on all public, private and domain	
	Publisher:	Unknown	
	Path:	C: \users \wkilgore \appdata \local \temp \web 100dt.exe	
Allow web 100clt to	communicate o	n these networks:	
🗹 Domain netw	orks, such as a	workplace network	
Private netwo	orks, such as n	ny home or work network	
Public networ because thes	rks, such as the se networks of	ose in airports and coffee shops (not recommended ten have little or no security)	

If wrap it up is chosen, for example after all collection has completed except for the last few Internet Speed Tests, click OK to approve the partial collection.

Scan Type Credentials .ocal Domains External Domains P Ranges SNMP (BSA Confirmation- Wrap it ABSA /erify Collect	Active Directory: Eventlogs: SQL Servers: Internet: Up!	Completed. Completed. Completed. Performing internet speed tests (server 15 of 19) X
Credentials Local Domains External Domains P Ranges SNMP MBSA Confirmation- Wrap it Confirmation- Wrap it This feature allows for	Eventlogs: SQL Servers; Internet: Up!	Completed. Completed. Performing internet speed tests (server 15 of 19)
External Domains P Ranges SNMP MBSA /erify Confirmation- Wrap it This feature allows for	SQL Servers: Internet: Up!	Completed. Performing internet speed tests (server 15 of 19) X
P Ranges NMP IBSA Confirmation- Wrap it Confirmation- Wrap it This feature allows for	Internet: Up!	Performing internet speed tests (server 15 of 19)
ABSA Verify Collect	Up!	×
inish for an output file to b reports created from contain incomplete i Pressing OK will start the collector to conti	or the data collect se generated from this data may have nformation as the the 'Wrap it Up! inue operating.	tion process to be ended prematurely and m the partial data. Please be aware that ave missing sections or may otherwise he collection process did not fully finish. " process, and pressing CANCEL will allow

The system will begin to collate the collected data into a single input file which will need to be sent to Axxys for processing and output file development which will include Excel spreadsheets, Word documents, and Powerpoint slides with all of the collected data.

	Wrapping up data collection
Scan Type Credentials Local Domains External Domains IP Ranges SNMP Information MBSA Verify and Run Collection Progress Finish	Please wait while data collection is ended and output files are generated. This process may take a few minutes.
	Back N

Click open folder to go to the output file that was generated. Click Done to close out the Data Collector program. At this point, we need to locate the output file, and send that to Axxys support for review and processing.

	Finish
Scan Type Credentials Local Domains External Domains IP Ranges SNMP Information MBSA Verify and Run Collection Progress Finish	The data collection process has been successfully ended, and file(s) with the partial data have been generated. Please be aware that reports created from this data may have missing sections or may otherwise contain incomplete information as the collection process did not fully finish. Collect the output file from C:\Users\wkilgore\Desktop Open Folder Review Results Summary
	Data

Depending on the size of the network and devices, the file will vary in size. Upload to a file sharing application and/or email the file to Axxys for processing. The output files will then be made available for review.

NetworkDetective-axxys.com-20161229

AXXYS TECHNOLOGIES

Corporate Headquaters

5850 Granite Parkway, Suite 700 Plano, TX 75024

> 214.297.2100 info@axxys.com

www.Axxys.com