March 2020

CYBER TOOL WITH VULNERABILITY SCANNER

HP INC

Cyber tool with Vulnerability scanner

This disclosure relates to the field of networking and describes how network troubleshooting can be done faster by detecting the network issues in few minutes. Also, to make sure the systems that are connected to the network e.g. servers, switches, etc don't have any vulnerability assigned to them in order to reduce the risk of cyber-attacks.

The network tool that is disclosed has several features. The first feature is to simplify the network troubleshooting. For that by connecting this tool to any network jack it can detect if the network jack is activated and can display the VLAN ID, Port ID, Chassis ID, Firmware version and the MAC address of the end switch that is connected to. This information is so necessary for a network/IT engineer to make sure the network jack has the proper configuration on it. The way that this tool gathers this information is by capturing Link Layer Discovery Protocol (LLDP) packets by TShark which contains the following.

Chassis ID (M)	Port ID (M)	Time To Live TLV (M)	Optional TLVs	End of LLPDU TLV (M)

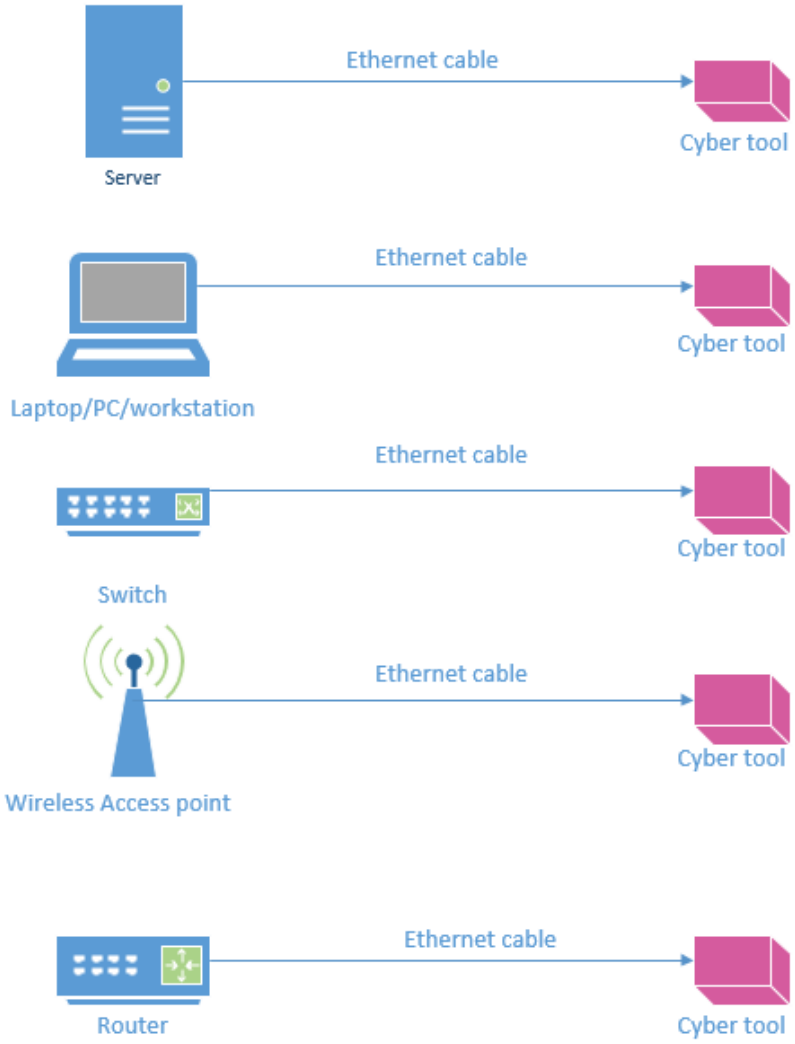
LLDP exchanges information through LLDPDU which contains TLVs. LLDP standard IEEE 802.1AB has three TLVs that are mandatory at the beginning of an LLDPU in the following order:

Type 1 = Chassis ID (Identifies the device)
Type 2 = Port ID (Identifies the port)
Type 3 = Time to live (Tells the receiving device how long the received information should remain valid)
Following these mandatory TLVs, an LLDPDU can include additional, optional TLVs:
Type 4 = Port description (displays details about the port)
Type 5 = System name (displays given name for the device)
Type 6 = System description (displays version of the software)
Type 7 = System capabilities (tells the primary function and capabilities of the device)
Type 8 = Management address (shows the IP or MAC address of the device)

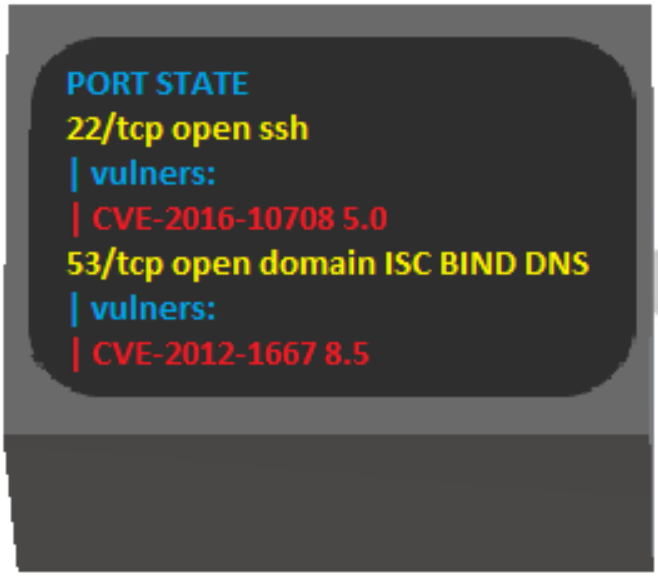
In parallel to capturing the LLDP packets this tool would start running speedtest-CLI to measure the download/upload internet speed, it also shows the IP address of the DHCP and DNS servers making sure the network jack is pointing to the right servers.

Fig#1- Example result of the network troubleshooting feature

Another feature of this tool is that it can connect directly to any network equipment such as: servers, switches, routers, wireless access points and even PCs and run vulnerability scans and display the report along with remediation steps. This tool detects vulnerabilities that could allow unauthorized control and allowing to access sensitive data on a system. It shows misconfigurations- missing patches and checks for the registry keys and ciphers. It also checks the system's password strength by launching a dictionary attack. The way it works is by connecting this tool to any system it would act as a DHCP server which then the connected system would acquire IP address from it and create an RFC1918 network. After the relationship is formed and they become part of the same network it then would run NMAP vuln scripts to run the vulnerability scan which would show the vulnerable ports and the CVEs assigned to them. It then would look up the CVE numbers from its internal database and shows how to fix and remediate each of those CVEs and generate the report.



Fig#2- Shows how this tool can be connected to any network equipment



Fig#3 – Example of vulnerability scan report

With this user-friendly tool, anyone with no networking knowledge can troubleshoot the network and make sure the connected systems have no vulnerabilities.

Disclosed by Mahi Haghpanahi and Ed Fulford, HP Inc.