Dumpforconduit.py: Python script for running tcpdump with user defined options

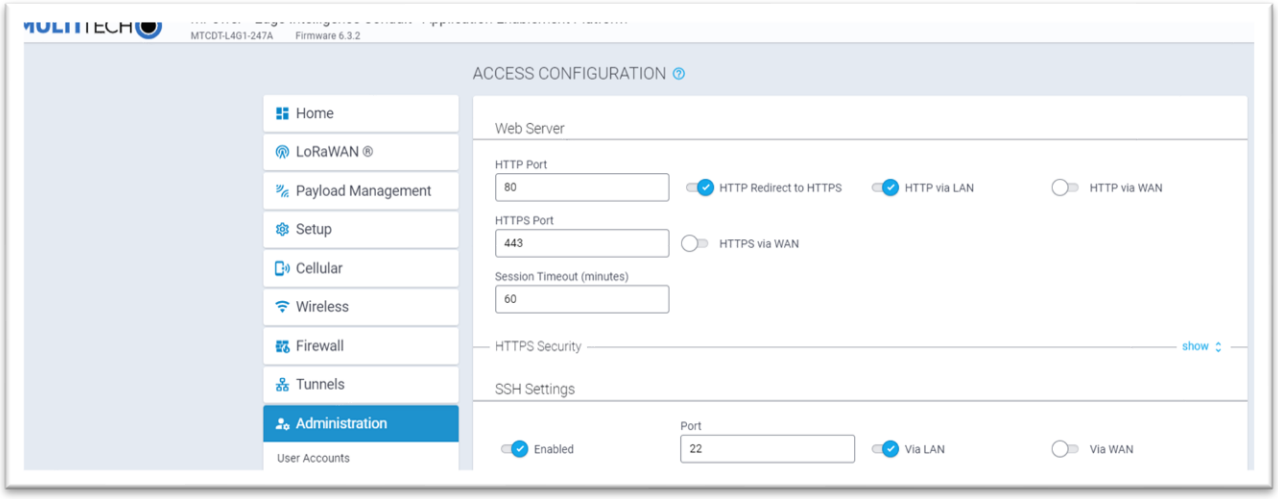
This Python script was designed to run on a MultiTech Conduit gateway to capture TCP/IP packets for further analysis and troubleshooting. It can be used to determine if there is excess or inappropriate traffic flowing between the gateway and a remote host.

After the script is run, the user must download the resulting tar.gz file, untar it and analyze the underlying pcap file in a tool such as Wireshark.

The script was designed to clean up any remaining files generated by the program, either by rerunning the program or deleting the files on reboot if they are stored in the default location of /var/volatile.

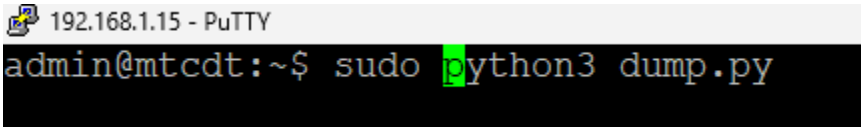
To use the program, you must enable SSH access on the gateway, and use a tool like Putty to connect to the gateway command line.

To enable SSH access, open the mPower interface to the gateway and choose Administration on the left-hand side. Choose Access Configuration, and enable SSH. Choose Via LAN. Click Submit, Save and Apply. You will be prompted to reboot the gateway.

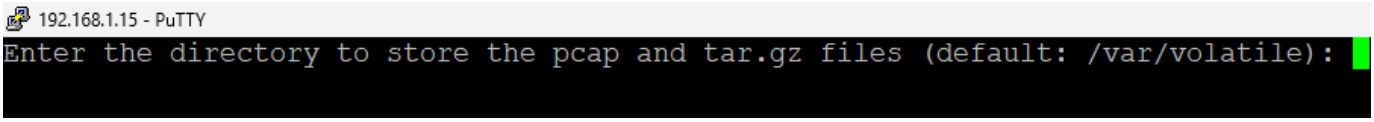


After you have enabled SSH and rebooted, use Putty or similar tool to connect to the gateway command line, using the gateway's IP address and the appropriate port – typically 22 unless you have changed it.

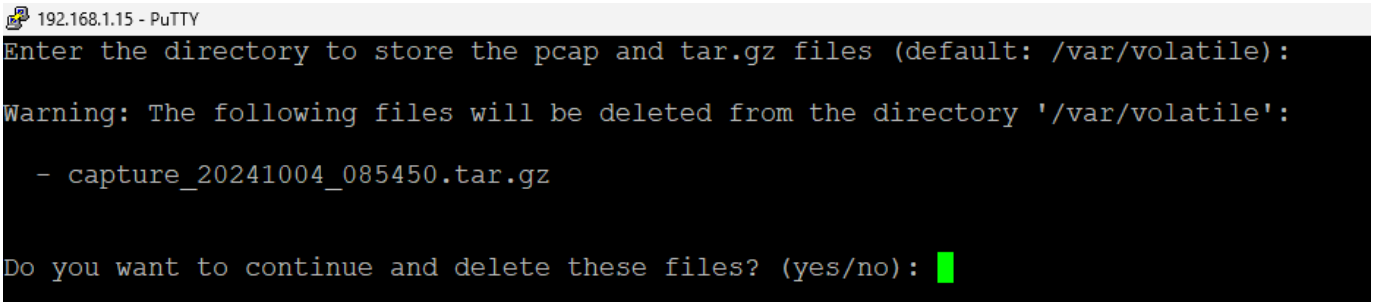
You must copy the Python script to the gateway. This can be done in a variety of ways, such as SCP, WinSCP, or you can copy the contents of the file and paste into a new text file on the gateway, using a tool like Nano text editor on the gateway. The file should be placed in /home/admin or other home directory. The program must be run as sudo.



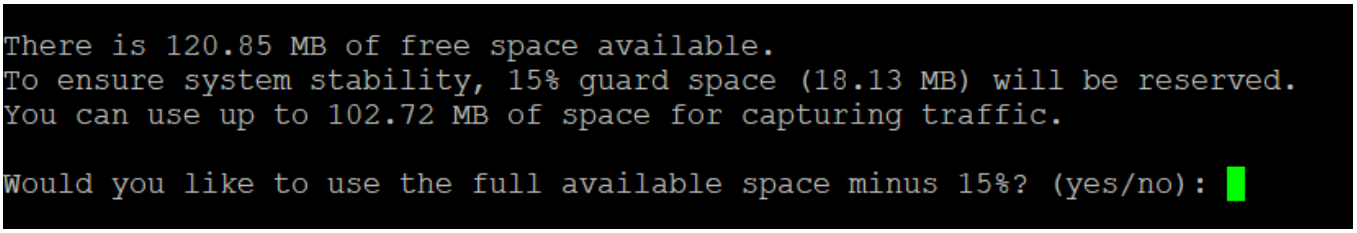
The user is prompted for a location to store the files that are produced by this script. On a Conduit, the default location is /var/volatile. This location was chosen because files in this directory will be erased upon reboot and we don't want large temporary files being retained on the gateway. However, the user can choose a different location.



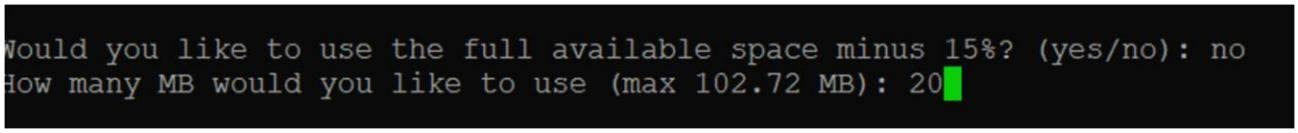
If there are existing tar.gz or pcap files in the chosen directory, the user is prompted to delete them, but they can back out of the program if they don't want to. The idea is to not leave any of these files hanging around on a device with limited disk space, so the user is encourage to download the files right after running the program.



The user is notified as to how much space is available on the drive, and is given the option to use all of the free space (minus 15% for safety), or they can choose a smaller number if desired.



In this case the user has chosen to limit the size of the pcap file to 20 MB.



The user is presented with a list of interfaces on which to capture traffic.

```
Listing available network interfaces...

1. 1.eth0 [Up, Running]
2. 2.br0 [Up, Running]
3. 3.lo [Up, Running, Loopback]
4. 4.any (Pseudo-device that captures on all interfaces) [Up, Running]
5. 5.bluetooth-monitor (Bluetooth Linux Monitor) [none]
6. 6.nflog (Linux netfilter log (NFLOG) interface) [none]
7. 7.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
8. 8.gre0 [none]
9. 9.gretap0 [none]
10. 10.erspan0 [none]
11. 11.ip_vti0 [none]
12. 12.ip6tnl0 [none]
13. 13.ip6gre0 [none]
14. 14.ip6_vti0 [none]
15. 15.tunl0 [none]
16. 16.sit0 [none]


Enter the number of the interface you want to capture on:
```

The user is asked if they want to exclude traffic between their PC and the gateway. If this traffic is not excluded, there will be a lot of SSH traffic as part of the capture.

```
SSH traffic between your PC and this host is often considered 'noise' and you may not want to include it as part of the traffic capture. Do you want to exclude traffic from your PC? (yes/no):
```

If the user says yes, they are prompted to enter the IP address of their PC.

```
Enter the IP address of your computer to exclude from capture: 192.168.1.162
```

The user has the option of restricting the capture to certain ports.

```
Do you want to limit the traffic collection to certain IP ports? (yes/no): yes
Enter the port(s) to include, separated by commas (e.g., 80,443):
```

The user has the option of restricting the capture to certain host IP addresses.

```
Do you want to limit the traffic collection to certain IP addresses? (yes/no): yes
Enter the IP address(es) to include, separated by commas (e.g., 192.168.1.1,10.0.0.1):
```

The user has the option of restricting the capture to a certain number of minutes.

```
How many minutes would you like to run tcpdump?
```

The tcpdump starts to run with the user-selected options. Note that the program will stop collecting after the number of minutes chosen has expired or the file size limit has been reached, whichever comes first.

```
Starting tcpdump on br0, saving to /var/volatile/capture_20241004_104932.pcap

tcpdump will run for 2 minute(s) or until the pcap file reaches 20 MB, whichever comes first.

Excluding traffic from IP: 192.168.1.162

Including only traffic to and from ports: 80

Including only traffic to and from IP addresses: 10.1.1.1
```

When finished, the program will compress the pcap file and place it in a tar.gz file with a title of the current time and date. The user should download the file so as not to lose it when running the program again or rebooting the gateway.

```
Stopping tcpdump after 2 minute(s).


Archiving /var/volatile/capture_20241004_104932.pcap to /var/volatile/capture_20241004_105132.tar.gz

Deleting original pcap file /var/volatile/capture_20241004_104932.pcap

Capture saved as /var/volatile/capture_20241004_105132.tar.gz

Note: Download the tar.gz file before rebooting, as files in /var/volatile will be erased on the next reboot.
```