Select one of the seven network problems and develop a troubleshooting and tool report that details the solution.

1. On Day 2 of full operational capability (FOC), our connection to the internet was becoming intermittent. We could establish connections to our globally hosted servers some of the time. The connection would drop at seemingly random periods and we don't know why. We have experienced this day and night, and it has been consistent for the past three days.
2. When our connection to the internet is working, we seemingly cannot reach out to our globally dispersed servers from our hosts. We use the globally dispersed servers for command and control and must be able to connect to them. We need a method to determine where the packets are going and why they are not reaching their destination. Because these servers are globally distributed, we can't just pick up and deploy to them.
3. Our internal network servers are also spotty. Sometimes they are up, and sometimes they are down. For example, the DHCP server appears to provide IP addresses to hosts that are turned on sometimes, but other times when the host is turned on, it receives an Automatic Private IP Address (APIPA). These hosts can communicate with our networked hosts locally, but they can't reach out to our global servers. These hosts enable our persistent engagement capability, so they must be functional, and we need to determine the problem ASAP!
4. We have a team that can troubleshoot from afar, but the members are located 25 miles west of this location. We have one of the tech support personnel deployed on site, but there are just too many issues for one person. The support team that is 25 miles west is centrally located to support multiple operational outfits. That team has a virtual private network (VPN) and secure access to our internal servers. At times, support team members need to determine which of our hosts are functioning. We use both Microsoft Windows and Linux operating systems, but we don't know what tool will help determine host functionality from afar.
5. This next part is classified, but I need your help, and I need it fast. Bottom line, we believe there may be an insider threat. At times, we have reason to believe a nonapproved device is connecting to the network and reaching out to the internet. We need a method to determine what devices exist on the same subnet of our network. What can help us do that?
6. When we begin operations in 72 hours, it will be of utmost importance for us to know what device name is associated with what IP address. This will allow us to know what exists internally and what we need to defend should the adversary begin operations against us. We need to understand what options exist to achieve this task.
7. When we first arrived and established our connection to the internet, we noticed inbound connection requests. What tool can we use to determine if any adversary is reaching into our systems through a particular port or protocol?

Your report should be about a page in length and address the following:

* Choose and restate one of the problems identified as you understand it and explain why it is a problem.
* Describe how you would apply the steps in the Network+ troubleshooting model to this problem.
* Name and provide a brief overview of the tool that could solve this problem (refer to Lesson 17 in uCertify).
* Describe how the tool can be used to solve similar problems in the future.
* Provide a detailed overview of the tool's functionality and options.
* Include a screenshot of your selected tool from the appropriate uCertify lab.

The [SITREP (Situation Report) Sample Report](https://learn.umgc.edu/d2l/common/dialogs/quickLink/quickLink.d2l?ou=613829&type=lti&rcode=UMUC-5977637&srcou=552138) is provided so that you can understand what Cyber Command is expecting in your report. Your report will vary depending on the problem and tool selected.

|  |
| --- |
| **How Will My Work Be Evaluated?**  Troubleshooting refers to the process of identifying problems with a network through a rigorous and repeatable process and then solving those problems using testable methods. An important part of your duties in the networking field will be to troubleshoot and solve problems. In fact, most of your time will be spent with this focus to include optimizing performance. Networks are dynamic in implementation and are built to be resilient, but problems arise due to many unforeseen reasons. Developing the knowledge, skills, and experience to successfully troubleshoot and recommend solutions will show you are value-added to the organization.  For this assignment, you are asked to review a scenario, understand the problems, apply your knowledge and skills gained in this class, and propose a solution. Use the template provided and complete the assignment. An example solution is provided for you.  The following evaluation criteria aligned to the competencies will be used to grade your assignment:   * 1.2.3: Explain specialized terms or concepts to facilitate audience comprehension. * 1.3.5: Adhere to required attribution and citation standards. * 1.4.1: Produce grammatically correct material in standard academic English that supports the communication. * 2.1.1: Identify the issue or problem under consideration. * 2.3.1: State conclusions or solutions clearly and precisely. * 10.1.1: Identify the problem to be solved. * 13.1.1: Create documentation appropriate to the stakeholder. |

If you haven't already done so last week, download the [Troubleshooting and Tools Report Template](https://learn.umgc.edu/d2l/common/dialogs/quickLink/quickLink.d2l?ou=613829&type=lti&rcode=UMUC-5977646&srcou=552138) and use it to record your work.

When you are finished, delete the instructional text from the template before you submit. Click "add a file" to upload your work, then click the Submit button.