FAQ

Have any questions?

Frequently asked questions related from the ICS Cybersecurity Virtual Training.

Session 2 - Network Discovery and Mapping

Q 1. How can Nmap be dangerous to ICS and embedded devices?

Embedded devices can be limited on resources. Layers of the network protocols they use are the same. If not used carefully, Nmap can essentially Denial-of-Service your own device as they try to keep up with all the queries from Nmap.

Q 2. Are the Nessus plugins for ICS safer to use as active discovery on a production environment?

The ICS plugins are for the specific vendors. Using them may be more appropriate. It is still good to exercise caution when doing any kind of scanning.

Q 3. Can you recommend something to help with remembering commands and ports?

Appendix A has many references.

Q 4. Are there any "Active" discovery tools recommended for ICS Administrators that can be used safely in a production environment?

Any tools covered in the course can be used so long as you are cautious. Backups, downtime, and recovery are extreme cases, but they are things you need to be prepared for. Map your network carefully and slowly.

Q 5. Is there something like Nmap that can be used on Windows?

Yes. Nmap is available for Windows. It will ask you to install a pcap driver as well. You can find it on Nmap's website.

Q 6. If an attacker is using Linux, would that change the way they interrogate/probe an unknown Windows network?

Using Linux as a platform to attack from provides an environment with useful network tools. If those same tools were available on other platforms, it would likely be just as effective, and not change the approach. The focus of the attack is the vulnerability and equipping yourself to exploit that. The attacker would not restrict themselves to one preferred platform

Q 7. Is there a passive tool available to conduct everything shown in the demonstration, or are these tools just active?

At the start of the lecture, we discussed command examples and ideas of where to look in a network are the "passive tools" for doing passive discovery. The later section of the lecture involves Nmap, which is not passive.

Q 8. Is Nmap dangerous, or is the nature of any active probing dangerous?

If not performed carefully, active scanning can be dangerous on any kind of network.

Q 9. nmap.org shows there is a Windows version available. Are the flags we learned about a direct match in the Windows version of the program?

The flags, or rather switches, are the same. The output also appears the same. However, the Windows port is not quite as efficient as on Unix. There are some known limitations.

Q 10. Are there more streamlined and automated solutions for scanning ICS?

If you are looking for a streamlined approach, you might not be taking a conservative approach. The idea is to be careful. If you use a streamlined solution, it may not make the safest choices for your unique environment.

Q 11. Regarding active scanning, can you elaborate on some specific impacts to ICS type systems?

Many old control systems are limited on memory, and literal on protocol. Nmap can create thousands of network requests to a single target. Devices with limited memory will do what they can to keep up. If these devices are in service, they may become interrupted. Also, keep in mind not all ICS devices have the logic to handle anomalies when presented with network packets they are not expecting to process.

Q 12. Is there a flow chart as to when or how you would approach utilizing these types of tools?

Each tool has a different purpose. You need to decide what your goal is and then select the tool that helps you to best accomplish it. It is important to understand each of the tools so you can better create your own flow charts.

Q 13. Are there any other network discovery utilities worth looking into?

For Windows, Angry IP scanner. SolarWinds is also common and makes a port scanning utility for Windows. Free IP Scanner is another lightweight tool. Vulnerability scanners, extremely heavy and noisy, are also something to consider. A free one called OpenVAS exists. It can also perform tests on targets to determine known weaknesses. Consider using tcpdump / windump (with a pcap lib installed) to observe traffic, though these are not scanners. If you do not know what you are expecting, then just start watching. Remember Wireshark as well.

Q 14. Under what circumstances would you see discussing with Critical Infrastructure owner operators the use of Active and Passive discovery as part of ICS protection.

The purpose of discussing Passive and Active scanning to ICS owners, is to give them a means to try and safely map an unknown network already in production. This scenario is common, due to change in system administrators and lack of documentation. This is an attempt to equip someone with talent to carefully gain confidence of a sensitive network. Accomplish this, and security will be in reach.

Q 15. What was the most interesting catch you have made with network discovery? What type of follow up was required as an account of that discovery?

In the field, Nmap has helped find poorly configured service networks. There have been times, where as an Internet Service Provider, I have found multiple customers on the same network space, which was thought to have been private down to one customer per link. It has been useful to discover lazy configurations. Something as simple as noticing private home printers appearing. You start to realize that one customer probably does not have 16 printers. Restoring the private segments was required and needed to be done carefully to avoid interruptions.

Q 16. Do you have a reference guide/cheat sheet for typical commands for scanning, port numbers used?

Appendix A includes many references.

Q 17. Is there a reference guide to command line flags for Nmap?

There is an official guide available for purchase. It is called "Nmap Network Scanning" and was written by Gordon Lyon himself.

Q 18. If Nmap and Nessus do not understand popular protocols (E/IP or profinet) what else is the freeway to provide network visibility?

Neither Nmap nor Nessus are tools for analyzing protocols. Nmap is a tool for interacting with ports, ICMP, and Ethernet. Nessus is used to access network ports that lead to known vulnerabilities. Remember to not confuse port numbers with protocols. The concepts covered in Network Mapping and Discovery are very manual flight, to give you strong foundation of exploration concepts.

Q 19. How could you recreate a working sandbox of a replicated control environment using the tools in Session 2 and a memory dump program?

Dumping firmware or dumping memory, other than cache, is not a focus in Session 2. Digging for cached data is. To create a sandbox environment, many approaches can be considered. Typically, virtualization is the go-to. There are many virtualizing methods that both emulate hardware and avoid emulating hardware. Depending on your preferences, you can mix them for your objective. Many exploits do require the hardware to be emulated.

Q 20. What are loopbacks used for?

If your host did not have a physical network interface with a network IP, you would likely still be running network applications. These applications can communicate to each other through ports and sockets, bound to the loopback interface, instead of a physical interface. It is a software interface to network with, for your applications that never need to leave the host. A local web browser accessing a database that you host locally, is one example.

Q 21. How can we perform passive discovery scans for cloud-based hosts?

The word “scan” implies active discovery. However, you can passively collect traffic and analyze it to draw a picture. If you have moved some of your components to the cloud, and they communicate with on premise devices, you can collect copies and analyze them passively.

Q 22. Do you have any recommendations on where I can get some more basic information around this material?

Appendix A includes additional information

Q 23. I would like to know if there are any VMs for ICS that can be used in a home lab.

The OpenPLC Project. https://openplcproject.com/getting-started/ They have three components that can turn your embedded project devices, such as a Raspberry Pi, into a device. This is not virtual, but it is much more compact. Our Appendix A also has some links.

Q 24. Can you please provide more details on the Kali Linux you mentioned for practicing Nmap on Windows?

Kali is the name of a distribution of the Linux operating system. It is not Windows. Nmap comes with Kali already installed. If you are running Windows on your computer, you can visit www.kali.org and download a virtual machine of the Kali Linux distribution. VMware makes a free player for virtual machines called “VMware Player”. You could also directly install Nmap for Windows.

Q 25. What tools can we use to begin to display the network topology as we move through discovery phase?

GrassMarlin is a great choice. Best of all, it is free.

Q 26. If you are a consultant or auditor, who should you get system information from to discuss and assess the impact of network inventories?

Typically, from the network admin or system admin. They should have the details you need.

Q 27. Passive mode does not show a complete anomaly. Is that correct?

You can slowly discover an anomaly in your environment with both Passive and Active approaches. If you passively collect information, and sort what you find, it may reveal an

anomalous finding. As for specific modes, the tools we covered do not really have a “mode” for being passive or active. Some tools are more obviously active, such as Nmap. Other commands can be either, depending on how you execute them.

Q 28. During the risk assessment of any organization, is the assessment team allowed to use Nmap on the organization network IPs and ports to assess and analyze their network vulnerabilities?

This will come back to two items. What is the policy in place that either allows for you or a third party to perform the action and -- meaning is Nmap approved for use on your network to be used -- keep in mind software base line comes into play. The other item to keep in mind is what alarms and notifications will be triggered when such actions are taken. Will this be passive or active?