Eric Guzman

11/8/23

Professor Cannistra

Network Security

Techniques and Tools of Active Discovery

In our world, defending data and peoples information is extremely important, and effective active discovery is crucial to this defense. Active discovery on a network is very important to finding what vulnerabilities and security threats exist in it. There are many different tools and techniques when performing active discovery. Some of the ones we will talk about today mostly have to do with scanning the network, looking for open ports or unsecure services that a malicious person might take advantage of for their own benefit. This helps organizations and businesses stay one step ahead of cybercriminals to keep their digital assets private and safe. These techniques need the proper authorization though, since scanning a network without the proper permission can be illegal and unethical.

One of the most well known active discovery tools is wireshark. It has one main function, to capture and display network traffic in real time. It is quick to set up and easy to use, making it extremely useful for anyone that wants to analyze the data going through a certain network. It is great for a network professional to monitor their network, looking for any anomalies or security threats that may arise. For example, “Network professionals, security experts, developers, and educators around the world use it regularly.”, “It can capture traffic from the air and decrypt it into that format which aids administrators to trace down those problems which causes poor performance,

intermittent connectivity using appropriate driver support.(Jain & Anubha, 2021)” This shows us that even at the higher level of network security, this tool is useful. It also could be useful to a malicious person who wants to view a network's traffic. They can view unencrypted sensitive data going through the network, which is a serious security concern.

Another active discovery tool that was found is the Angry IP scanner. This tool allows for someone to do a scan of a subnet and look for all available IP addresses. For example, “If you are permitted to hook up your computer and get an IP address, you can quickly scan a subnet and find out which IP addresses really are available and which are not. (Bisset, J., 2014)” This tells us that anyone able to get an IP address on this network can look at its structure and available hosts. This is useful for someone doing active discovery since it gives a fast and efficient way to map out the network's address space and identify any target that could use more investigation. It can find active devices and services which are valuable uses for anyone doing active discovery, malicious or not.

The final activity discovery tool found was OpenVas. This tool allows an organization to identify, analyze and assess vulnerabilities that may exist within their network and find ways to prevent anyone from exploiting them. This tool is primarily used by organizations doing active discovery on their own network to protect their digital assets and maintain the availability of their systems. For example, “The OpenVAS scanning plugin is also written for known vulnerabilities. When a new vulnerability is discovered, a scan plugin for the vulnerability can be written in time to quickly discover the vulnerability. Using the combination of the update vulnerability library and the

self-developed vulnerability scanning plug-in can better improve the vulnerability discovery probability and increase the security of the entire network. (Xia, Y., Wang, j., Liu, C., & Yu, K., 2020)" This tells us that this tool can discover known vulnerabilities on a network ensuring that the organization in use of this tool can prevent threats. This tool can also be used by bad actors looking for a vulnerable organization to attack. It is crucial for all network oriented businesses to use this tool to at least prevent the easily exploitable weaknesses in their network before someone punishes them for not using this tool.

In conclusion, we looked at three network scanning tools and saw how useful they are for active discovery. Wireshark, Angry IP Scanner and OpenVas all provide very important capabilities that allow for active discovery of a network. These tools offer pretty similar but different approaches. All of these tools should be used to prevent exploitation of a network, before a malicious actor makes you regret it.

References

1. Jain, G., & Anubha. (2021). Application of snort and wireshark in network traffic analysis. *IOP Conference Series: Materials Science and Engineering*, *1119*(1), 012007. doi:10.1088/1757-899x/1119/1/012007
2. Bisset, J. (2014, Mar 12). Simple switch resets sluggish monitor. Radio World, 38, 10-10,12.
3. Xia, Y., Wang, j., Liu, C., & Yu, K. (2020). Design and implementation of vulnerability scanning tools for intelligent substation industrial control system based on openvas. IOP Conference Series.Earth and Environmental Science, 440(4) doi:https://doi.org/10.1088/1755-1315/440/4/042031