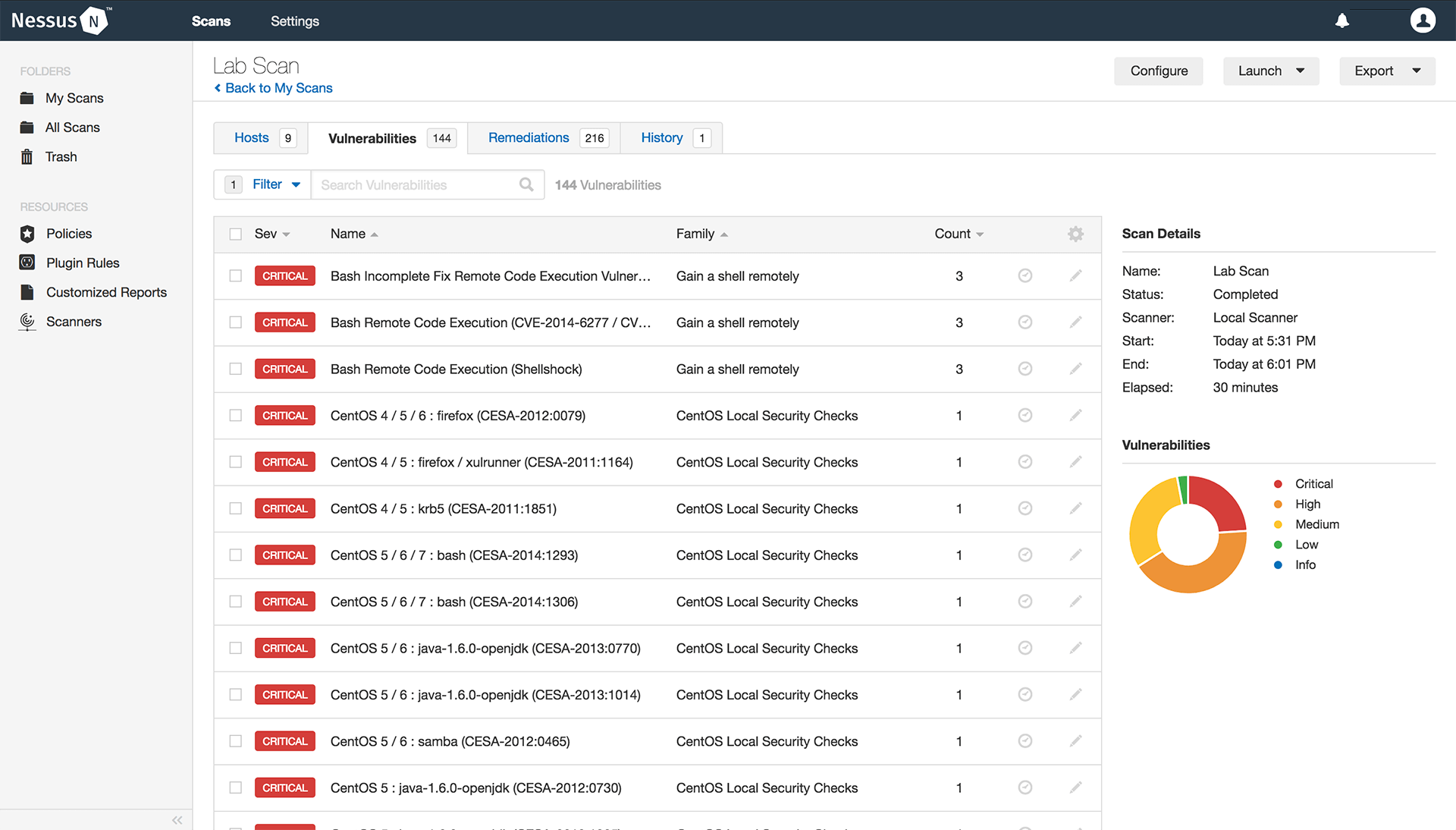
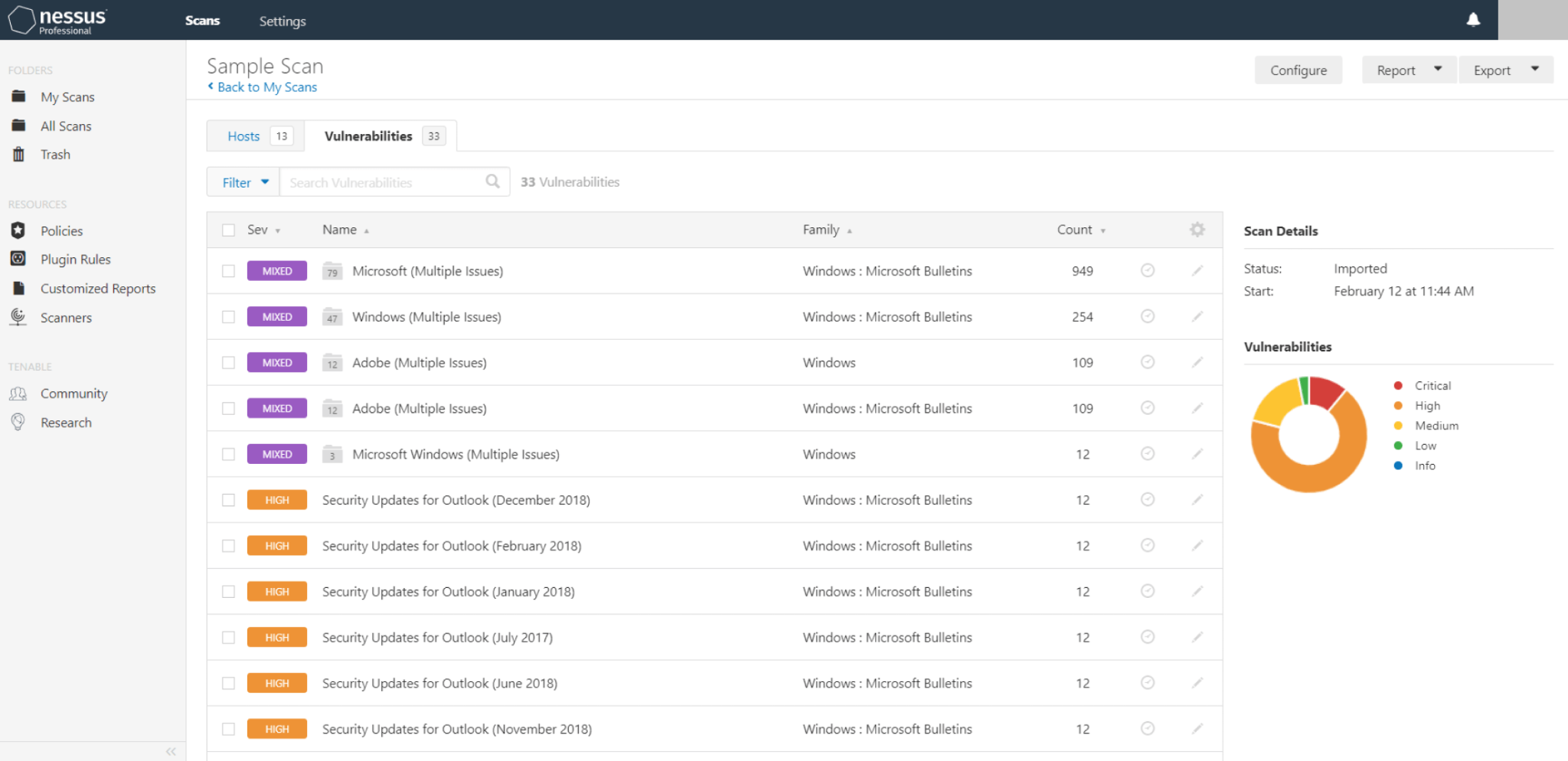
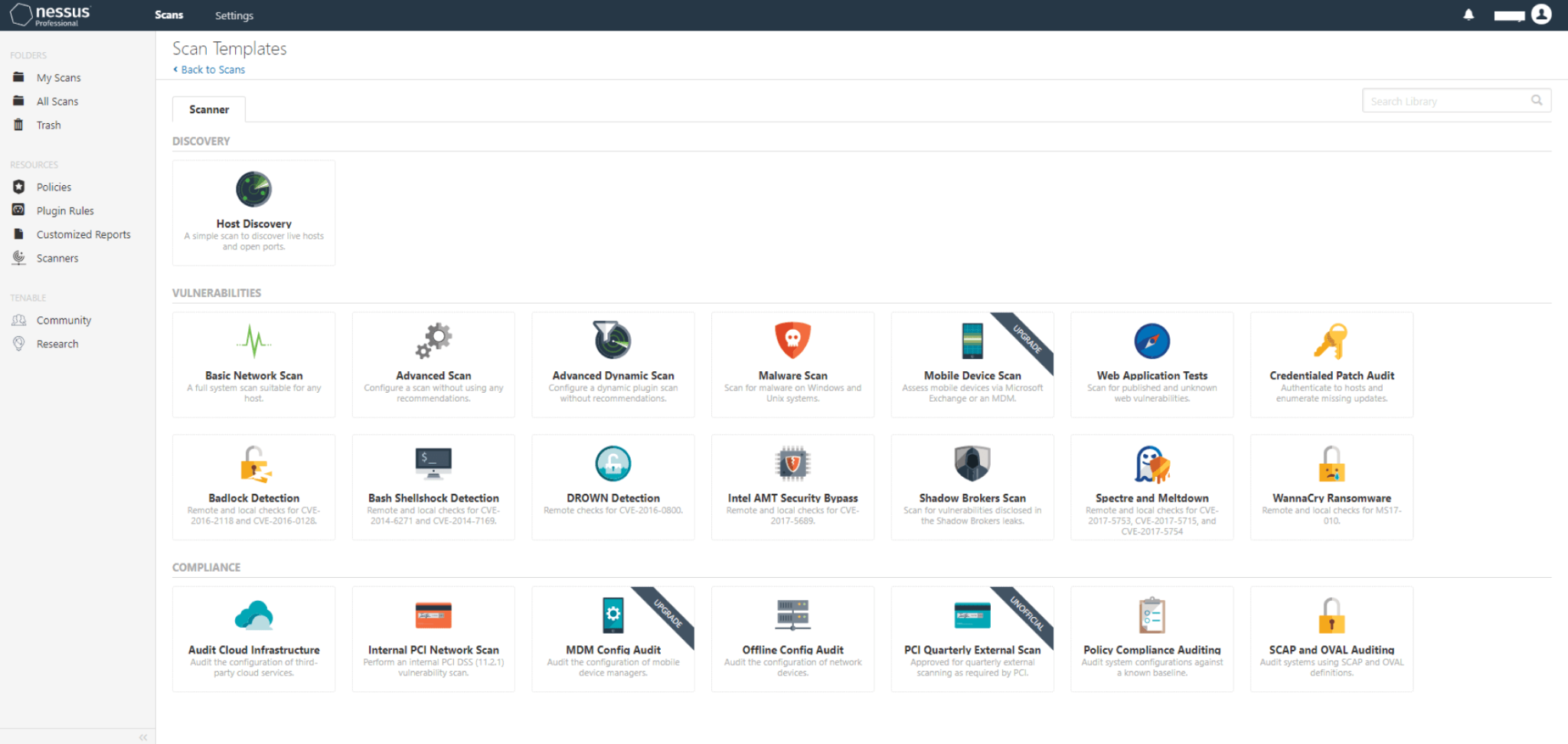
**Group Assignment 14**

**Member Present: Sylas, Eros Absent: Andrew**

Visit the <http://sectools.org/> site and identify two open-source tools that perform network scanning (other than NMAP). Then list the type of data that a hacker can obtain by using the tools. Provide examples and be very specific

**Nessus**:

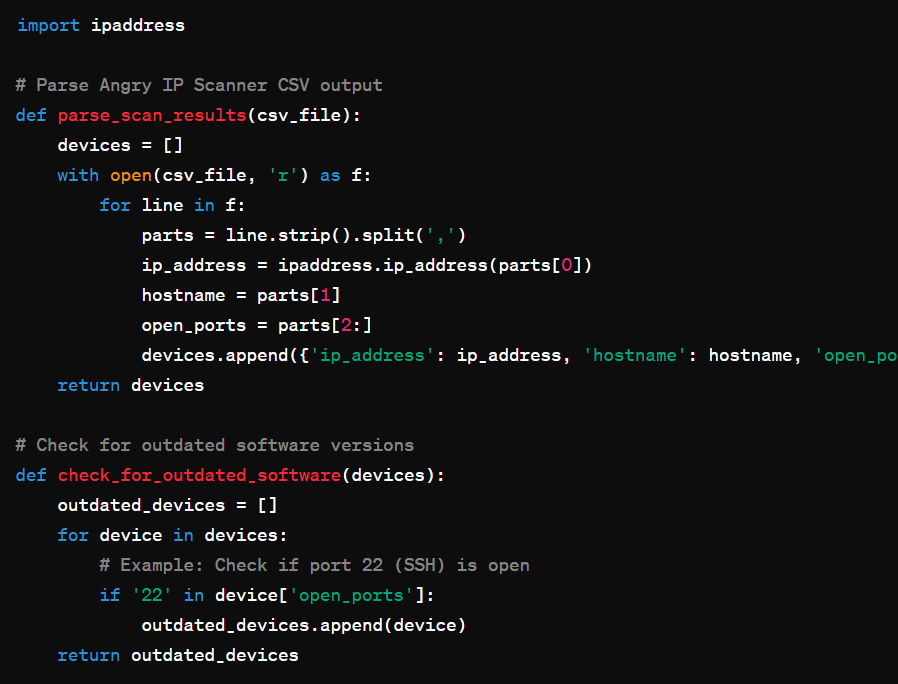
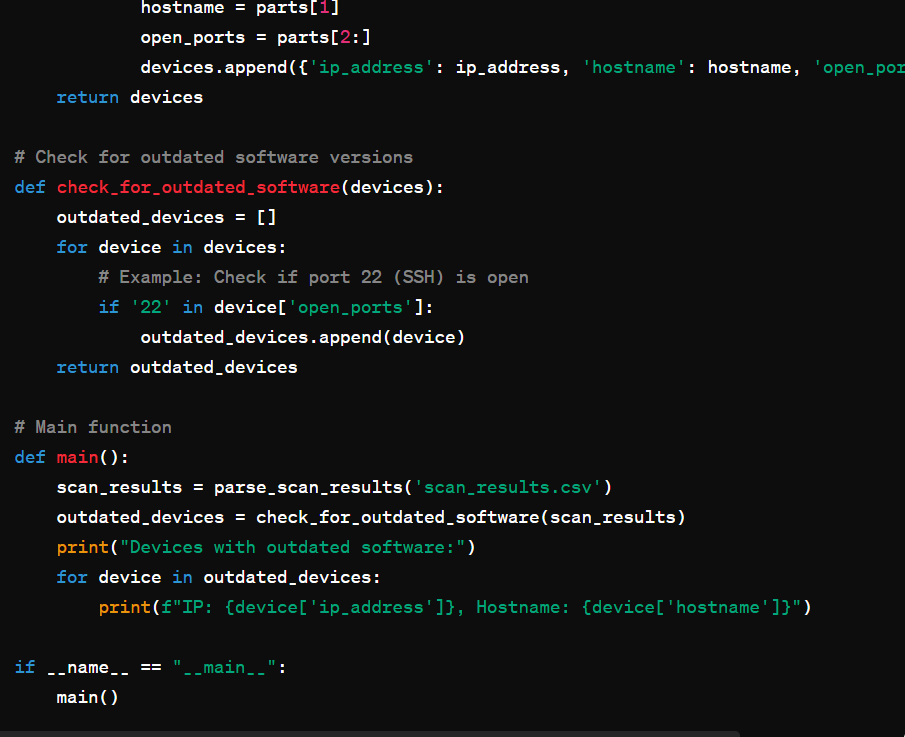
As the image shows, this tool will list the scanned result (vulnerabilities) according their level of threat (from critical to mild)



This tool is a Unix system based, popular & powerful vulnerability scanning tool, it used to be open-source, but later the developer closed source code in 2005, and removed its free version in the year of 2008. However, there is still a free “Nessus Home” version, which is only licensed to be used in home networks. Although it is no longer a freeware, its cost still beats many of its competitors (~$2190 a year). Later the developer upgraded their free version “Home” to “Essentials” which allowed it to be operating in a business environment, and it is able to scan up to 16 devices for free.

This tool is constantly upgraded with numerous (70k+) plugins, also including an embedded scripting tool to write one’s own plug-in and help understand existing ones. This tool can be used for (authenticated) security scanning in local/remote hosts, as author mentioned before, this scan can collect vulnerability information in the designated network and hopefully help the user to patch it. It can scan for vulnerabilities in web servers, databases, network devices, and other systems that are exposed to the internet.

**Angry IP Scanner**:

Angry IP Scanner is an open source tool that allows users to obtain information about information that a target has. They can obtain an IP address, which informs the attacker what kind of network the user is using. They can also obtain the Hostname associated with the detected IP Address which shows the device name available which allows them to know more vulnerabilities. This tool can also scan ports that allow hackers to know services and applications are running on those devices. Custom scripting is another function that is useful for hackers because these scripts can automate tasks, gather additional information, or perform specific actions beyond the default capabilities of the scanner. By having this ability they can perform basic vulnerability assessments by identifying outdated software versions, weak configurations, or common security misconfigurations on scanned devices. So knowing this just makes it easier for them to narrow down their attack method. 

This script reads Angry IP Scanner's CSV output, checks for devices with port 22 (SSH) open, and prints the IP addresses and hostnames of devices running SSH, which might indicate potential security risks due to outdated software versions.