Trent

Ch 13 Vulnerability Assessment and Data Security

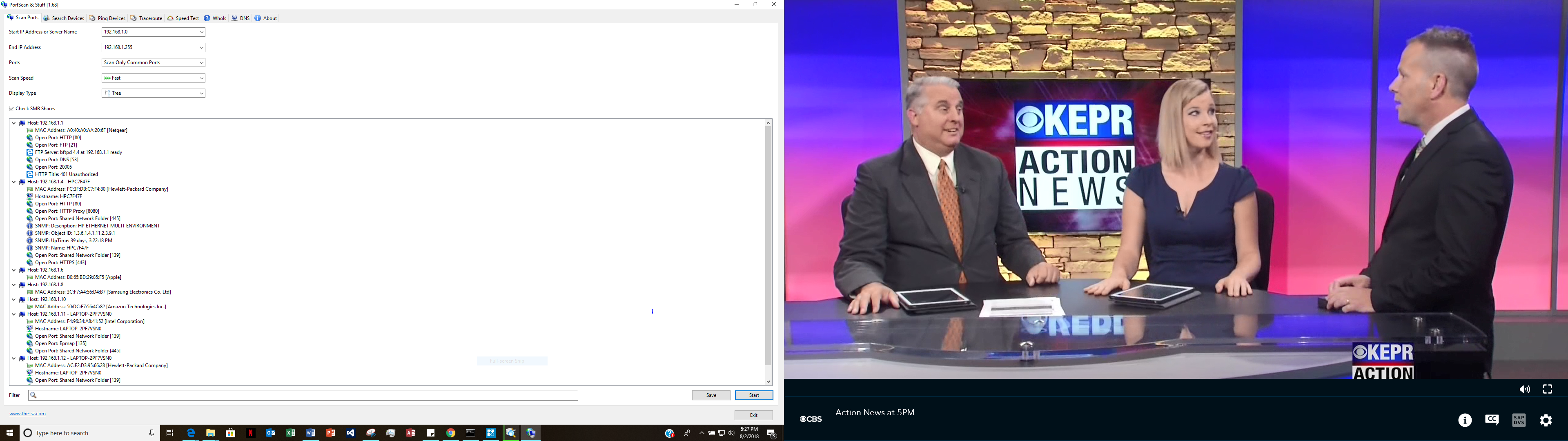
8/218

13-3 Compare port scanners

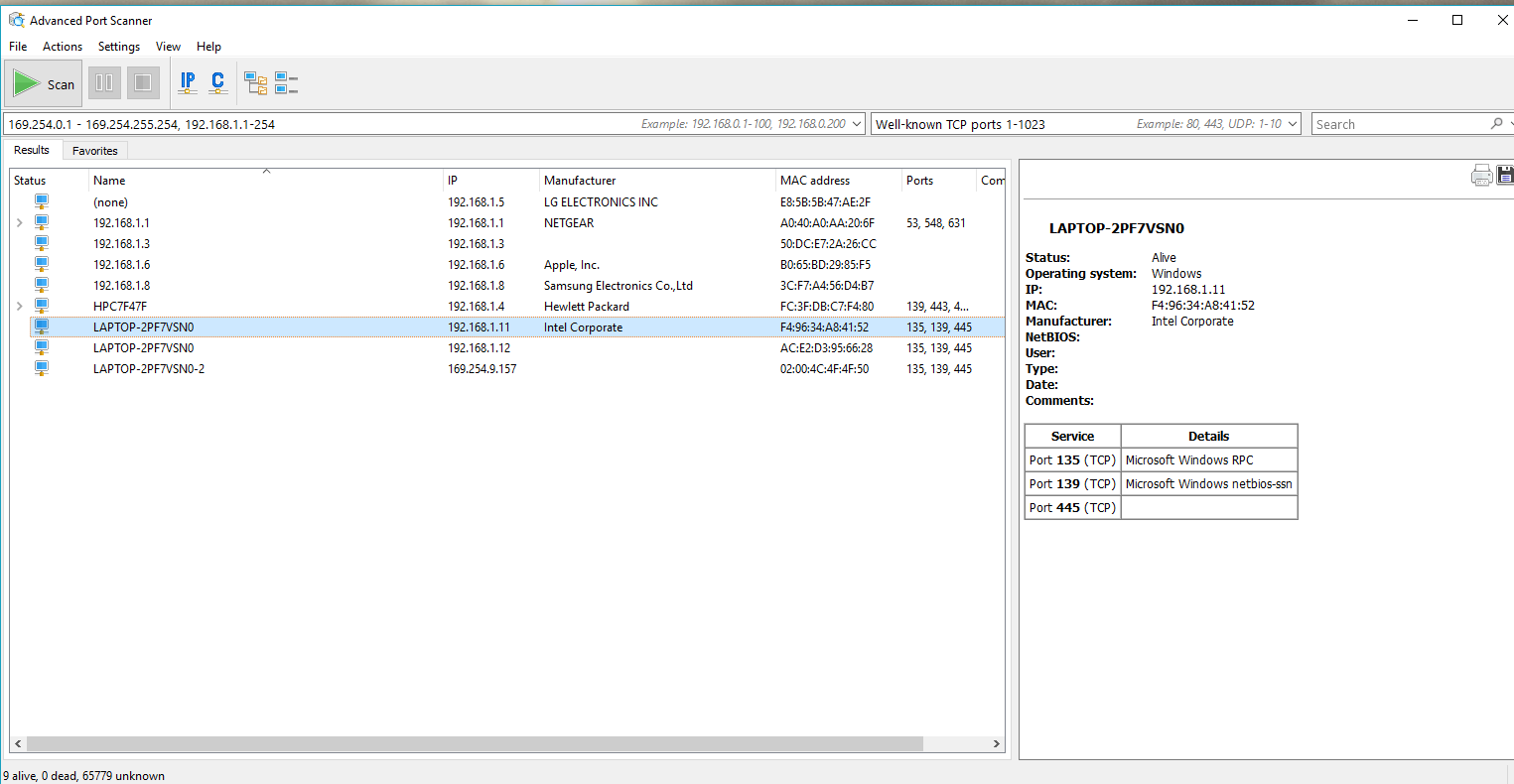
Many people don’t know much about computer ports, or that some items allow the user to choose the port number. For many IT workers use port scanners to check vulnerabilities, while others use it to find a vulnerability. The importance of port scanners could help stop silly mistakes with port settings.

The first port scanner I used was the one from the lab which was Zenmap, and it provided the open port, but not the description of the port. It also required the configuration of each IP address to be entered manually and is unrealistic in a large corporation with a large network. It is however fast and finished one laptop in .4 seconds. The test is very limited and is more made for home user. The tester is not recommended compared to the others.

The second port scanner I used is called PortScan & Stuff and provides a quick scan of the entire system and sends also the information of what the port is used for. And for smart devices that don’t have ports, like a smart tv gave the MAC address from the scan. The scan takes less than 5 minutes to do a complete scan, and to me gives all the needed items for someone to get an idea of the devices on the network. The only limitation is not allowing remote computer to run the program.



The third program is Advanced Port Scanner. The scanner allows remote scanning of a system with ability to run commands, and allows computers turned off to be woken up. The system is much more advanced but is extremely slow and takes over an hour to scan the network from every possible IP address on a network that are common. The items it finds has port numbers and information, but not as complete for all the ports the system uses compared to PortScan & Stuff. For a corporation this would be the best, but for a home user this is not usable for being slow.



Overall a port scanner is useful. But has limitations depending on which software using, and if it is made more for a home user or a corporation level network need. The scanner I would recommend is PortScan & Stuff because of the speed that it works on the network creating little down time. Port scanners are useful, but at the same time a vulnerability risk in the hands of an attacker.

# References

Chen, K. (2016, April 16). *3 powerful free portable network TCP port scanners for windows.* Retrieved from nextofwindows: https://www.nextofwindows.com/3-powerful-free-portable-network-tcp-port-scanners-for-windows