Alan Thomas

CSI337-Information Sec.

Nmap Findings

Dr. Dutta

25FEB18

Originally created by Gordon Lyon, Nmap is a powerful tool that is utilized to scan open ports on a single host or a range of hosts, in addition to scanning for open ports, the software also has the ability to determine the most likely operating system along with running services. Although this tool is over twenty years old, it remains a staple in any penetration testers tool kit.

I began my exploration of Nmap by beginning with the basic scanning techniques section. My initial target was localhost, and as I suspected (and hoped), no open ports were found. This leads me to believe that since software firewalls are almost a standard now for nearly all operating systems, Nmap has lost some of its functionality, though it’s still a powerful tool. In light of the fact that there are no open ports on my desktop, I changed my query to something I knew would have open ports; a NAS device that I store and stream movies from.

Upon completion of a single target scan of this device, I found a number of ports that were open. There are roughly ten ports open on this device, in the event, I was an attacker I would more than likely be most interested in the fact that the FTP, HTTP, and SSH ports are open as they provide an attack surface to conduct a brute-force attack.

The next command that I investigated was that of scanning random hosts, which is a function of this tool that I had never used before. I decided to scan a relatively small number of targets and resulted in some interesting results. On one of the host, a service called FMSAS was discovered on port 1600. I had never heard of this service or port and decided to do some research as to what its function was. From my understanding, FMSAS is a service that allows system administrators to log into a system. Though I am not certain, it’s functionality may be similar to Window’s Remote Desktop or TeamViewer. Unfortunately, the host was not running a web server, so I wasn’t able to learn any more about the host or why they may have been running this service.

Following the scanning of random hosts, I attempted to scan my NAS device once again, but this time instead of using the simple one target scan, I opted to use SYN packets to investigate if it was possible to determine if any other services were running that had not been discovered during the initial scan. Though there were no changes in the results, I believe in the hands of a skilled penetration tester, the use of scanning with SYN packets may prove to illicit more results.

Upon completion of the SYN scan, I decided to use a functionality that we are all familiar with, traceroute. I was more curious if Nmap would produce any additional information as opposed to what Linux and Windows offer with the built-in traceroute functionality. To my surprise and disappointment, Nmap was not very accurate when determining hops. I’m not sure if it’s designed this way on purpose, but when running a traceroute through Nmap, it showed that there were only two hops between my system and the McKendree web server. This would mean that as soon as packets left my system they went directly to McKendree; it didn’t even count my router as a hop, not to mention all of the other routers that I had to touch in order to reach McKendree’s site. Upon seeing the results that Nmap produced, I decided to execute traceroute using Windows. The results were along the lines of what I was expecting. There were a total of 19 hops, and this included my gateway. If I were troubleshooting network issues, at least with exiting the network, I’m not sure Nmap would be the best choice as far as tools.

I’ve used Nmap quite a bit in the past, and I’m in awe by how impressive this tool is. However, I hadn’t used the tool in a couple of years, and I noticed, almost immediately, that it isn’t nearly as effective as it used to be. From the standpoint of someone wanting to snoop around someone’s network, it’s disappointing. However, from the perspective of someone that does banking online and routinely sends information over the internet, I’m glad to see that software firewalls have become much more effective. Though I am no expert, I suspect that the days of scanning for open mail servers or open FTP servers are long gone. I suspect that serious attackers have pivoted to easily accessible services such as web apps and SQL servers. In short, it’s an amazing tool, but like any tool, it has its uses and limitations.