Anonymous Port Scanning
Performing Network Reconnaissance Through Tor
Rodney Rohrmann, Dr. Mark W. Patton, Dr. Hsinchun Chen
University of Arizona
Department of Management Information Systems
Tucson, AZ 85721, USA
rodneyr@email.arizona.edu, mpatton@email.arizona.edu, hchen@eller.arizona.edu

Abstract—The anonymizing network Tor is examined as one method of anonymizing port scanning tools and avoiding identification and retaliation. Performing anonymized port scans through Tor is possible using Nmap, but parallelization of the scanning processes is required to accelerate the scan rate.

Keywords—Scanning, Tor, Anonymization

Scans of web traffic in a hostile part of the web have the potential to result in retaliatory attacks. The anonymizing network Tor is examined as one method of anonymizing port scanning tools and avoiding identification and retaliation. One recipient of retaliatory threats is the University of Michigan, which used ZMap and Masscan and has been researching its speed. They used an opt-out email address, and 15 of the 145 responses threatened retaliatory action [1]. Developing a method to perform rapid scanning through Tor eliminates this risk.

The industry standard tool Nmap was chosen due to its benefits and capabilities, as well as the likelihood of its performing well through Tor. Nmap can use TCP when scanning instead of UDP [4]. The –sV flag allows for version scanning and does not leak the scanner’s IP address. The –O (OS Detection), and -A (OS detection, version detection, script scanning, and traceroute) [5] did reveal the IP address because Nmap bypassed Proxychains during part of the execution.

Scan rates dropped dramatically through Tor. Using Proxychains prevented Nmap from using multiple processes so it could no longer scan hundreds of ports a second [6]. Scanning ports serially resulted in roughly one port per second. As Nmap cannot run scans in parallel through Proxychains, parallelization work was undertaken to run multiple separate Nmap processes. To test parallelization, three scans of 1,000 ports each were run and recorded, with durations of 17 to 19 minutes. Ports 1-150 scan more slowly than other ports so were broken out separately. Scans for ports 151 and above were scanning at around 1.5 scans per second.

In conclusion, performing anonymized port scans through Tor is possible using Nmap, but parallelization of the scanning processes is required to accelerate the scan rate. Anonymization is not automatic and the correct flags must be set. Future work includes scanning larger organizations and using more powerful machines to run hundreds or thousands of processes to test scalability limits.

REFERENCES