Internet Scanning

- Internet-wide scanning can help reveal new kinds of vulnerabilities, monitor deployment of mitigations, and shed light on previously opaque distributed ecosystems [1]
- ZMap applications [1]:
    - Measuring protocol adoption (e.g. HTTP to HTTPS)
    - Analysis of distributed systems, such as certificate authority ecosystem
    - High-speed vulnerability scanning
    - Uncovering unadvertised services, e.g. Tor bridges

ZMap: Fast Internet-Wide Scanning and its Security Applications [1]

- Sends probes as quickly as possible (limited by the source's NIC and CPU); generates Ethernet frames directly, skipping TCP/IP stack.
- Uses 97% of the theoretical max speed of gigabit Ethernet, searching entire IPv4 address space in under 45 mins on a mid-range machine
- Doesn't use per-connection state (doesn't store addresses already scanned)
- Doesn't use retransmission - always sends a fixed number (default 1) of probes per target
- Scans addresses using a random permutation of the address space to avoid overloading destination networks and inconsistent results in the case of distant transient network failures
- Uses libpcap in the receiving component to capture network traffic and filter the received packets. Because incoming traffic is significantly less than outgoing traffic (overwhelming majority of hosts unresponsive to probes), performance requirements not as strict

An Internet-Wide View of Internet-Wide Scanning [2]

- Horizontal scanning: scanning a large number of hosts on a single port
- 80% of scan traffic originates from large scans targeting > 1% of the IPv4 address space
- Scans often conducted by academic researchers
- Large portion of scans target services associated with vulnerabilities (e.g. Microsoft RDP)
- Dataset - traffic received by a darknet between 1 January 2013 and 1 May 2014; 5.5 million addresses in darknet (0.145% of public IPv4 space)
- A scan: an instance where a source address contacted 100 or more unique addresses in the darknet on the same port and protocol
- Traffic processes using libpcap

MASSCAN: Mass IP port scanner [3]

-

References

[1] Durumeric, Z., Wustrow, E., & Halderman, J. A. (2013). ZMap: Fast Internet-wide Scanning and Its Security Applications ZMap: Fast Internet-Wide Scanning and its Security Applications. In Proceedings of the 22nd USENIX Security Symposium. Retrieved from https://zmap.io/.

[2] Durumeric, Z., Bailey, M., & Halderman, J. A. (2014). An Internet-Wide View of Internet-Wide Scanning. Proceedings of the 23rd USENIX Security Symposium (USENIX Security 14), 65–78. Retrieved from https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/durumeric

[3] R. Graham. MASSCAN: Mass IP port scanner. https://github.com/robertdavidgraham/masscan