Nmap and Routing algorithms

Day 23/365

Nmap commands Summary

Option	Explanation
`-sL`	List scan – list targets without scanning
Host Discovery	
`-sn`	Ping scan – host discovery only
Port Scanning	
`-sT`	TCP connect scan – complete three-way handshake
`-sS`	TCP SYN – only first step of the three-way handshake
`-sU`	UDP Scan
`-F`	Fast mode – scans the 100 most common ports
`-p[range]`	Specifies a range of port numbers – `-p-` scans all the ports
`-Pn`	Treat all hosts as online – scan hosts that appear to be down
Service Detection	
`-O`	OS detection
`-sV`	Service version detection
`-A`	OS detection, version detection, and other additions
Timing	
`-T<0-5>`	Timing template – paranoid (0), sneaky (1), polite (2), normal (3), aggressive (4), and insane (5)
`--min-parallelism <numprobes>` and `--max-parallelism <numprobes>`	Minimum and maximum number of parallel probes
`--min-rate <number>` and `--max-rate <number>`	Minimum and maximum rate (packets/second)
`--host-timeout`	Maximum amount of time to wait for a target host
Real-time output	

Option	Explanation
`-v`	Verbosity level – for example, `-vv` and `-v4`
`-d`	Debugging level – for example `-d` and `-d9`
Report	
`-oN <filename>`	Normal output
`-oX <filename>`	XML output
`-oG <filename>`	`grep`-able output
`-oA <basename>`	Output in all major formats

Routing Algorithms

- **OSPF (Open Shortest Path First)**: OSPF is a routing protocol that allows routers to share information about the network topology and calculate the most efficient paths for data transmission. It does this by having routers exchange updates about the state of their connected links and networks. This way, each router has a complete map of the network and can determine the best routes to reach any destination.
- **EIGRP (Enhanced Interior Gateway Routing Protocol)**: EIGRP is a Cisco proprietary routing protocol that combines aspects of different routing algorithms. It allows routers to share information about the networks they can reach and the cost (like bandwidth or delay) associated with those routes. Routers then use this information to choose the most efficient paths for data transmission.
- **BGP (Border Gateway Protocol)**: BGP is the primary routing protocol used on the Internet. It allows different networks (like those of Internet Service Providers) to exchange routing information and establish paths for data to travel between these networks. BGP helps ensure data can be routed efficiently across the Internet, even when traversing multiple networks.
- **RIP (Routing Information Protocol)**: RIP is a simple routing protocol often used in small networks. Routers running RIP share information about the networks they can reach and the number of hops (routers) required to get there. As a result, each router builds a routing table based on this information, choosing the routes with the fewest hops to reach each destination.