**PORT SCANNER PROJECT!...**

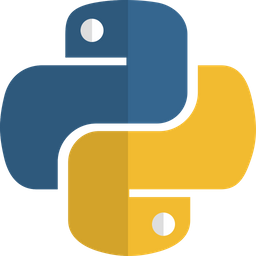
**A SCANNER… is a device that allows you to digitize physical documents, images, or even objects, and convert them into a digital format that can be viewed, edited, and stored on a computer. It's like a digital photocopier that captures the content of a document or image and saves it as a file.**

**A PORT SCANNER….is a tool or software used to identify or check which ports on a network device (like a computer, server, or router) are open, closed, or filtered. Port scanning helps identify active services, potential vulnerabilities, and network security configurations and sending connection requests.**

**It helps identify active services, security risks, and misconfigurations. Commonly used for security audits, troubleshooting, and ethical hacking, tools like Nmap, Zenmap and Masscan automate the process.**

**Unauthorized scanning can be illegal, so permission is required before probing external systems.**

**To create a port scanner, you can use a combination of programming languages, libraries, and development tools**



**JavaScript Python C++ Go [Golan]**

**SOME OF THE PLATFORM OR THE TOOLS TO CREATE A PORT SCANNER!...**

**1: JavaScript-Useful for web-based scanners.**

**2: Python-Easy to used, has a great Networking Libraries.**

**3: C++…Very fast and low level, used in advanced application/scanners.**

**4: GO [Golang]…Fast Concurrent great for the Network application.**

**Python, JavaScript, and C++ can collaborate to build a port scanner by leveraging each language’s strength: Python handles scanning logic and network requests, C++ boosts performance for intensive tasks, while JavaScript powers a web interface to display results. Together, they create a robust, user-friendly tool, combining speed, flexibility, and interactive visualization for efficient port scanning.**

**What is the work of a port scanner / how does a port scanners do!...**

**A port scanner is a tool (software or script) used to discover open ports and services available on a target device (like a server, computer, or network device).**

**Its help by…………**

**CHECKS FOR OPEN PORTS:  
It tries to connect to a range of ports on a target IP to see which ports respond. Each open port means a service is listening there.**

**IDENTIFIES SERVICES:  
Some scanners also try to determine what service (e.g. HTTP, FTP, SSH) is running on each open port.**

**HELPS WITH SECURITY AUDITS:  
Network admins use port scanners to find unintended open ports, which might be security risks. Attackers also use them to find vulnerabilities.**

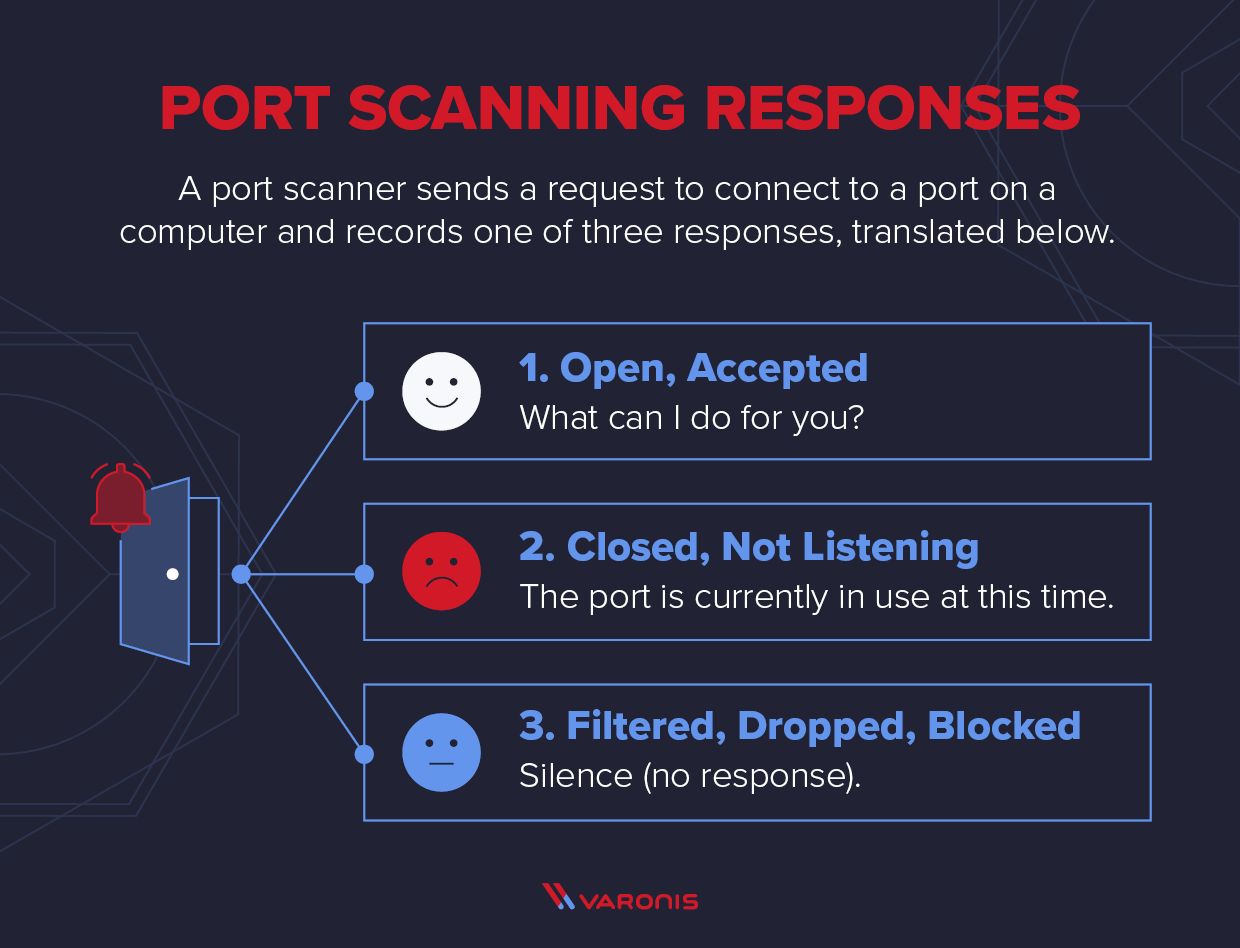
**TROUBLESHOOTING:  
It helps diagnose network issues — like checking if a firewall is blocking certain ports.**

**In short….port scanner main work on how to find open ports and services on a networked device and to secure networks, discover vulnerabilities, and troubleshoot connectivity.**

**WHAT ARE THE KEYS PURPOSE OF A PORT SCANNERS!...**

**A port scanner sends a network request to connect to a specific TCP or UDP port on a computer and records the response.**

**So what a port scanner does is send a packet of network data to a port to check the current status. If you wanted to check to see if your web server was operating correctly, you would check the status of port 80 on that server to make sure it was open and listening.**

**The status helps network engineers diagnose network issues or application connectivity issues, or helps attackers find possible ports to use for infiltration into your network.**

**A port scanner also sends a TCP or UDP network packet and asks the port about their current status.**

**The three types of responses are below:**

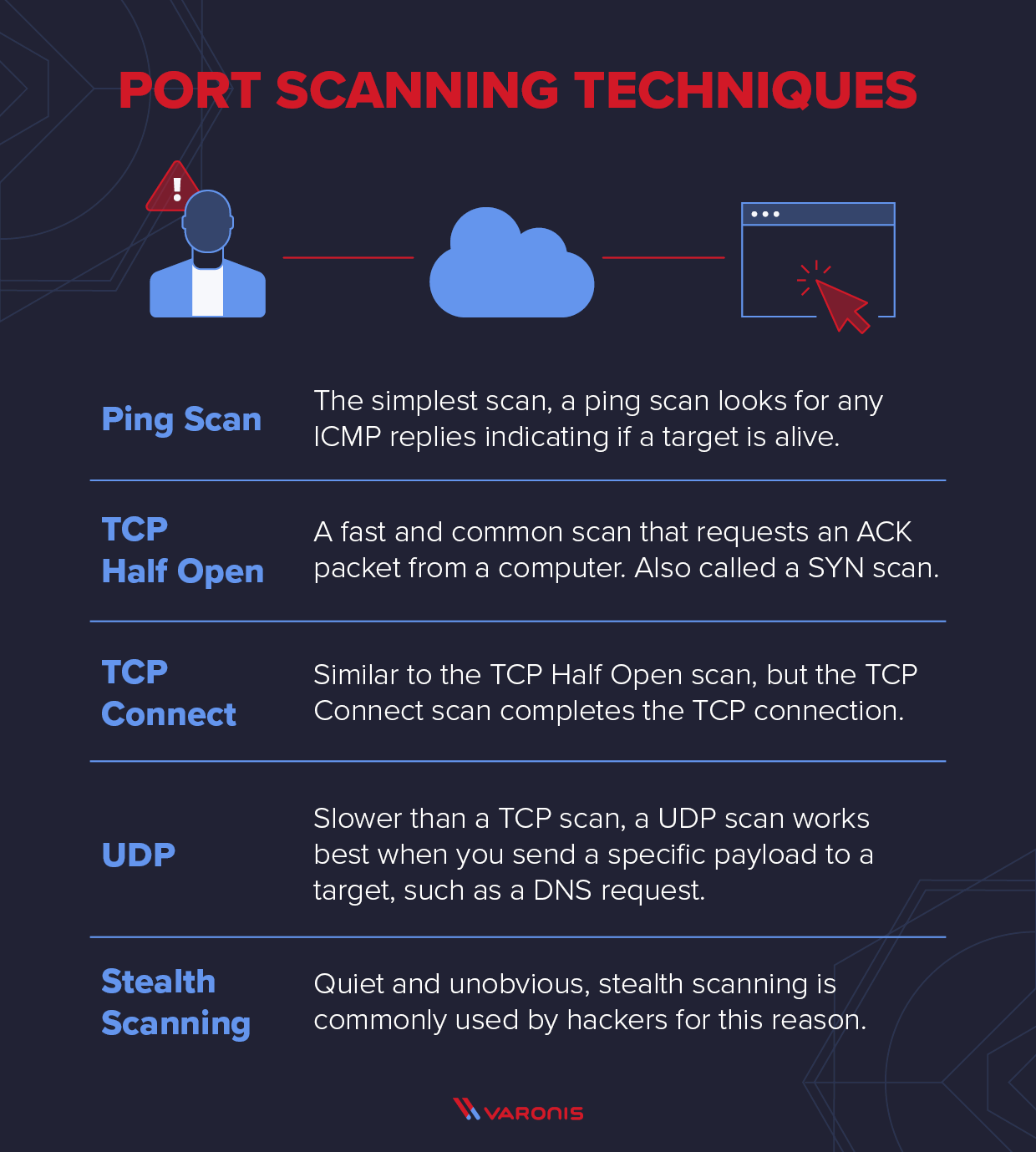
**Open, Accepted: The computer responds and asks if there is anything it can do for you.**

**Closed, Not Listening: The computer responds that “This port is currently in use and unavailable at this time.”**

**Filtered, Dropped, Blocked: The computer doesn’t even bother to respond.**

**How Does a Port Scanner Operate?**

**PORT SCANNING TECHNIQUES!..**

****

[**Nmap**](https://nmap.org/)**is one of the most popular open-source port scanning tools available. Nmap provides a number of different port scanning techniques for different scenarios.**

**Ping Scanner**

**A PING.. is an**[**Internet Control Message Protocol (ICMP)**](https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol)**echo request – you are looking for any ICMP replies, which indicates that the target is alive. A ping scan is an automated blast of many ICMP echo requests to different targets to see who responds. Ping scans aren’t technically port scanning techniques, as the best you can get back is that there is a computer on the other end, but it’s related and usually the first task before you do a port scan.**

**Administrators usually disable ICMP (ping) either on the firewall or on the router for external traffic, and they leave it open inside the network. It’s quick and easy to turn off this functionality and make it impossible to scout the network this way. However, ping is a useful troubleshooting tool, and turning it off makes tracking down network problems a little more difficult.**

**TCP HALF OPEN**

**One of the more common and popular port scanning techniques is the TCP half-open port scan, sometimes referred to as an SYN scan. It’s a fast and sneaky scan that tries to find potential open ports on the target computer.**

**SYN packets request a response from a computer, and an ACK packet is a response. In a typical TCP transaction, there is an SYN, an ACK from the service, and a third ACK confirming message received.**

**This scan is fast and hard to detect because it never completes the full TCP 3 way-handshake. The scanner sends an SYN message and just notes the SYN-ACK responses. The scanner doesn’t complete the connection by sending the final ACK: it leaves the target hanging.**

**Any SYN-ACK responses are possibly open ports. An RST(reset) response means the port is closed, but there is a live computer here. No responses indicate SYN is filtered on the network. An ICMP (or ping) no response also counts as a filtered response.**

**TCP half-open scans are the default scan in NMAP.**

**TCP CONNECT!**

**This port scanning technique is basically the same as the TCP Half-Open scan, but instead of leaving the target hanging, the port scanner completes the TCP connection.**

**It’s not as popular a technique as the TCP half-open. First, you have to send one more packet per scan, which increases the amount of noise you are making on the network. Second, since you complete the target’s connection, you might trip an alarm that the half-open scan wouldn’t.**

**Target systems are more likely to log a full TCP connection, and intrusion detection systems (IDS) are similarly more likely to trigger alarms on several TCP connections from the same host.**

**The advantage of the TCP connect scan is that a user doesn’t need the same level of privileges to run as they do to run the Half-open scan. TCP connect scans use the connection protocols any user needs to have to connect to other systems.**

**UDP**

**UDP scans are slower than TCP scans, but there are plenty of exploitable UDP services that attackers can use, DNS exfiltration, for example. Defenders need to protect their UDP ports with the same voracity as their TCP ports.**

**UDP scans work best when you send a specific payload to the target. For example, if you want to know if a DNS server is up, you would send a DNS request. For other UDP ports, the packet is sent empty. An ICMP unreachable response means the port is closed or filtered. If there is a service running, you might get a UDP response, which means the port is open. No response could mean that the port is open or filtered.**

**One more logical use of a UDP scan is to send a DNS request to UDP port 53 and see if you get a DNS reply. If you do get a response, you know that there is a DNS server on that computer. A UDP scan can be useful to scout for active services that way, and the Nmap port scanner is preconfigured to send requests for many standard services.**

**HOW PORT SCANNER STRUCTURE LOOK IN Nmap!.**

**A port is a logical endpoint on a computer or network device used to identify specific processes or services. It works together with an IP address to direct data to the right application.**