Attack Surface Management

What is an Open Port, and Why are they Dangerous?

Abi Tyas Tunggal
updated Oct 02, 2020

Table of contents

In cybersecurity, the term open port refers to a TCP or UDP port number that is configured to accept packets. In contrast, a port which rejects connections or ignores all packets, is a closed port.

Ports are an integral part of the Internet's communication model. All communication over the Internet is exchanged via ports. Every IP address contains two kinds of ports, UDP and TCP ports, and there are up to 65,535 of each for any given IP address.

Services that rely on the Internet (like web browsers, web pages, and file transfer services) rely on specific ports to receive and transmit information. Developers use

file transfer protocols (FTPs) or SSH to run encrypted tunnels across computers to share information between hosts.

Once a service is running on a certain port, you can't run other services on it. For example, starting Apache after you've already started Nginx on port 80 will lead to a failed operation because the port is already in use.

Open ports become dangerous when legitimate services are exploited through security vulnerabilities or malicious services are introduced to a system via malware or social engineering, cybercriminals can use these services in conjunction with open ports to gain unauthorized access to sensitive data.

Closing unused ports reduces your security risk by reducing the number of attack vectors your organization is exposed to.

Are open ports dangerous?

There's a common misconception that an open port is dangerous. This is largely driven by a lack of understanding of how open ports work, why they are open, and which ones shouldn't be open.

A quick Google search will produce hundreds of pages suggesting you should close open ports. And this advice is often appropriate, but it's not entirely accurate to say an open port is dangerous.

As outlined above, open ports are necessary to communicate across the Internet.

Open ports can be dangerous when the service listening on the port is misconfigured, unpatched, vulnerable to exploits, or has poor network security rules. Of particular danger are wormable ports which are open by default on some operating systems, such as the SMB protocol which was exploited by a zero-day exploit called EternalBlue that resulted in the WannaCry ransomware worm.

Open ports aren't dangerous by default, rather it's what you do with the open ports at a system level, and what services and apps are exposed on those ports, that should prompt people to label them dangerous or not.

The reason people call for closed ports because less open ports reduces your attack surface.

Why do attackers scan for open ports?

Attackers use open ports to find potential exploits. To run an exploit, the attacker needs to find a vulnerability.

To find a vulnerability, the attacker needs to fingerprint all services that run on a machine, including what protocols it uses, which programs implement them, and ideally the versions of those programs.

To do this, attackers commonly rely on finding a publicly accessible port via port scanning.

For example, nmap will fingerprint and report software and applications found running on a server, sometimes with version information. Outdated versions may have publicly-known vulnerabilities (like those listed on CVE), which software such as metasploit can target.

What are the common open ports?

There are many port scanners, some built for specific tasks, others included in continuous security monitoring tools. No matter how you use them, understand port scanning is a must for discovering open ports.

Additionally, different operating systems will also have a number of default ports open. Windows, OS X, and Linux run different core daemons, so a port open on one could be closed on another.

The most common ports are:

- **FTP (21):** FTP or File Transfer Protocol is used to transfer files across the Internet.

- **SMTP (25):** SMTP or Simple Mail Transfer Protocol ensures email messages are communicated over the network securely.
- **WHOIS (43):** Used to obtain the registration of ownership of domain names and IP addresses
- **DNS (53):** DNS or Domain Name System uses relational databases to link the hostnames of computers or networks to their respective IP addresses.
- **DHCP (67, 68):** DHCP or Dynamic Host Configuration Protocol assigns IP Address related information to clients on a network automatically. This information may be comprised of subnet mask, IP address, etc. Port 67 performs the task of accepting address requests from DHCP and sending data to the server, while port 68 responds to all requests of DHCP and forwards the data to the client.
- **TFTP (69):** TFTP or Trivial File Transfer Protocol is a simple lockstep File Transfer Protocol that allows a client to get a file from or put a file onto a remote host. One of its primary uses is in the early stages of nodes booting from a local area network.
- **HTTP (80):** Assigned to web servers and directly associated with the Hypertext Transfer Protocol.
- **POP3 (110):** POP3 or the Post Office Protocol is used by email clients to retrieve data from remote email servers.
- **SFTP (115):** SFTP or Secure File Transfer Protocol, is a separate protocol packaged with SSH that works in a similar way over a secure connection
- **IMAP (143):** IMAP or Internet Message Access Protocol retrieves emails from a remote server without having the need to download the email.
- **SNMP (161):** SNMP or Simple Network Management Protocol is used to collect and organize information about managed devices on IP networks and for modifying that information to change device behavior.
- **HTTPS (443):** Allows you to connect to the Internet by establishing a secure connection between web pages and the browser.
- **LPD (515):** LPD or Line Printer Daemon Protocol is a networking printing protocol for submitting jobs to a remote printer.

- **rsync (873):** rysnc is used to transfer and synchronize files between a computer and external hard drive, and across networked computers by comparing the modification times and sizes of files.
- **IMAP SSL (993):** IMAP protocol that supports SSL encryption.
- **POP3 SSL (955):** POP3 protocol that supports SSL encryption.
- **SOCKS (1080):** SOCKS or SOCKet Secure is an Internet protocol that exchanges network packets between a client and a server through a proxy server.
- **Proxy (3128):** Currently the port often used by proxies.
- **MySQL (3306):** Used by MySQL databases.
- **RDP (3389):** RDP or Remote Desktop Protocol establishes a connection with a remote computer, allowing you to access it from anywhere in the world.
- **PostgreSQL (5432):** Used by PostgreSQL databases.
- **VNC (5900):** A graphical desktop-sharing system that uses the Remote Frame Buffer protocol (RFB) to remotely control another computer.
- **TeamViewer (5938):** A proprietary software application for remote control, desktop sharing, online meetings, web conferencing, and file transfer between computers.
- **HTTP (8080):** An alternate port for HTTP.

How do open ports affect confidentiality, integrity, and availability?

Open ports can impact the confidentiality, integrity, and availability of your organization:

- **Confidentiality:** Open ports, and the programs listening and responding at them, can reveal information about the system or network architecture. They can leak banners, software versions, content, the existence of the system itself, and what type of system it is.
- **Integrity:** Without open port controls, software can open any candidate port and immediately communicate unhindered. This is often relied upon for legitimate programs, as well as different types of malware.
- **Availability:** Your network and the services running on open ports still process incoming traffic, even if the requests are invalid. This can result in denial of service attacks.

How can I monitor my open ports?

On a small network with relatively few IP addresses, finding and closing open ports isn't a massive task. However, as you likely know, on larger networks with a content flow of new devices, monitoring and managing open ports can be extremely time-consuming.

In addition to the ports themselves, the underlying services using those ports need to be monitored too.

The good news is that these open ports and services are facing the public Internet, so they can be scanned by continuous monitoring technology like UpGuard's security ratings platform.

Our platform explicitly checks for nearly 200 services running across thousands of ports, and reports on any services we can't identify, as well as any open ports with no services detected.

How UpGuard help you manage your cybersecurity risk exposure

Companies like Intercontinental Exchange, Taylor Fry, The New York Stock Exchange, IAG, First State Super, Akamai, Morningstar, and NASA use UpGuard's security ratings to protect their data, prevent data breaches and assess their security posture.

UpGuard Vendor Risk can minimize the amount of time your organization spends assessing related and third-party information security controls by automating vendor questionnaires and providing vendor questionnaire templates.

We can help you continuously monitor your vendors' external security controls and provide an unbiased security rating.

We can also help you instantly benchmark your current and potential vendors against their industry, so you can see how they stack up.

For the assessment of your information security controls, UpGuard BreachSight can monitor your organization for 70+ security controls providing a simple, easy-to-understand cyber security rating and automatically detect leaked credentials and data exposures in S3 buckets, Rsync servers, GitHub repos and more.

The major difference between UpGuard and other security ratings vendors is that there is very public evidence of our expertise in preventing data breaches and data leaks.

Our expertise has been featured in the likes of The New York Times, The Wall Street Journal, Bloomberg, The Washington Post, Forbes, Reuters, and TechCrunch.

You can read more about what our customers are saying on Gartner reviews.

If you'd like to see your organization's security rating, click here to request your free Cyber Security Rating.

Book a demo of the UpGuard platform today.

who is liable with this in-depth...

Download eBook

Tags: Attack Surface Management Cybersecurity

See UpGuard In Action

Book a free, personalized onboarding call with one of our cybersecurity experts.

Contact sales Free demo

Related posts

Learn more about the latest issues in cybersecurity.

UpGuard

14 Cybersecurity Metrics + KPIs to Track

14 Cybersecurity Metrics + KPIs to Track

Cybersecurity metrics and key performance...

Abi Tyas Tunggal
October 19, 2020

UpGuard

Why is Cybersecurity Important?

Why is Cybersecurity Important?

Learn about why cybersecurity is...

Abi Tyas Tunggal
October 1, 2020

UpGuard

What is Typosquatting?

What is Typosquatting?

Typosquatting is a form of cybersquatting whe...

Abi Tyas Tunggal
October 19, 2020

UpGuard

The Top Cybersecurity Websites and Blogs of 2020

The Top Cybersecurity Websites and Blogs of 2020

This is a complete guide to the best...

Abi Tyas Tunggal
September 21, 2020

UpGuard

What are Security Ratings?

What are Security Ratings?

This is a complete guide to security ratings and...

Abi Tyas Tunggal
October 19, 2020

UpGuard

The 36 Biggest Data Breaches [Updated for 2020]

The 36 Biggest Data Breaches [Updated for 2020]

Read about the 36 biggest data breaches...

Abi Tyas Tunggal
September 17, 2020

View all blog posts >

Sign up to our newsletter

Get the latest curated cybersecurity news, breaches, events and updates in your inbox every week.

Email address*

Subscribe