

Forum:[Hack Forums](#)

Thread: [How to Scan IP Address For Open Ports \(FREE C++ and Python Source Code\)](#)

Hackers - January 6, 2024, 1:28 pm

Port Scanner

in C++ and Python

Want to download the compiled exe program?

Available here (generated by Pyinstaller):

<https://hackforums.net/showthread.php?pid=62309697>

When you are looking into whether your server is secure or not, you may need to figure out which ports are open for connection attempts. A port scanner is a tool that allows you to look for common ports used by services such as smtp, ftp, ssh, webdav, http, and more.

Please note that it may take some time to return a response for big ranges due to connection timeout settings and your personal connection as well. The C++ version is far faster than the Python script, but both work reliably - Enjoy!

Pscan.py (Python) Source Code & Instructions :

Spoiler ([Click to View](#))

Code import socket

```
def is_port_open(ip, port):
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.settimeout(1) # Timeout of 1 second
    try:
        sock.connect((ip, port))
    except socket.error:
        return False
    return True

def scan_ports(ip, mode='common', min_port=1, max_port=65535, common_ports=[21, 22, 23, 25, 80, 110, 443]):
    open_ports = []
    if mode == 'r':
        # Scan the specified range of ports
        for port in range(min_port, max_port + 1):
            if is_port_open(ip, port):
                open_ports.append(port)
    else:
        # Scan common ports
        for port in common_ports:
            if is_port_open(ip, port):
                open_ports.append(port)
    return open_ports
```

```
# Example usage
if __name__ == "__main__":
    target_ip = input("Enter IP address to scan: ")
    mode = input("Enter scan mode ('d' or 'r'). Type in d (default / common ports) or r (range), press
enter): ").lower()
    if mode == 'r':
        min_port = int(input("Enter minimum port number: "))
        max_port = int(input("Enter maximum port number: "))
        print(f"Scanning range {min_port}-{max_port}...")
        open_ports = scan_ports(target_ip, mode, min_port, max_port)
    else:
        print("Scanning common ports...")
        open_ports = scan_ports(target_ip)
    print("Open ports:", open_ports)
```

Run example:

Code `python pscan.py`

Usage:

You can use this Python script, which will launch a command line terminal on your computer. I have tested this with Python 3.12 as recently as today. You can use this script and follow the prompts. First, you will enter the letter d (for default), or r (for range) and then press Enter in your terminal. You can also just press Enter straight away for the default.

Default (d) scan:

Scans for ports 21, 22, 23, 25, 80, 110, 443

Range (r) scan:

You will enter a minimum and maximum port number (integer) to scan as a range. This is inclusive, so if you enter 2 and 10 it will scan ports 2 and 10 and all numbers between.

Pscan.cpp (C++ for Windows) Source Code & Instructions :

Spoiler ([Click to View](#))

```
Code #include <iostream>
```

```
#include <winsock2.h>
```

```
#include <ws2tcpip.h>
```

```
#include <vector>
```

```
#include <thread>
```

```
#include <mutex>
```

```
#pragma comment(lib, "Ws2_32.lib")
```

```
std::mutex guard_mutex;
```

```
bool checkPort(const char* targetIP, int targetPort) {
    SOCKET sockInstance = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);
    if (sockInstance == INVALID_SOCKET) {
        return false;
    }
}
```

```
struct sockaddr_in serverAddr;
serverAddr.sin_family = AF_INET;
```

```

inet_pton(AF_INET, targetIP, &serverAddr.sin_addr);
serverAddr.sin_port = htons(targetPort);

// Setting timeout for connection attempt
DWORD connTimeout = 1000; // 1 second
setsockopt(sockInstance, SOL_SOCKET, SO_RCVTIMEO, (const char*)&connTimeout,
sizeof(connTimeout));

bool portStatus = connect(sockInstance, (struct sockaddr *)&serverAddr, sizeof(serverAddr)) ==
0;
closesocket(sockInstance);
return portStatus;
}

void performScan(const char* targetIP, int targetPort) {
    if (checkPort(targetIP, targetPort)) {
        std::lock_guard<std::mutex> lock(guard_mutex);
        std::cout << "Port " << targetPort << " is open." << std::endl;
    }
}

int main(int argc, char* argv[]) {

    std::string binaryExt = ".exe";
    WSADATA wsaData;
    if (WSAStartup(MAKEWORD(2, 2), &wsaData) != 0) {
        std::cerr << "Winsock init failed." << std::endl;
        return 1;
    }

    if (argc < 2) {
        std::cerr << "Usage: ./pscan" << binaryExt << " <IP Address> [startPort] [endPort]" <<
std::endl;
        WSACleanup();
        return 1;
    }

    const char* targetIP = argv[1];
    std::vector<std::thread> scanThreads;

    if (argc == 2) {
        std::vector<int> primaryPorts = {21, 22, 23, 25, 80, 110, 443};
        for (int port : primaryPorts) {
            scanThreads.emplace_back(performScan, targetIP, port);
        }
    } else if (argc == 4) {
        int startPort = std::stoi(argv[2]);
        int endPort = std::stoi(argv[3]);
        std::cout << "Scanning range: " << argv[2] << " - " << argv[3] << std::endl;
        for (int port = startPort; port <= endPort; port++) {
            scanThreads.emplace_back(performScan, targetIP, port);
        }
        std::cout << "Range scan complete." << std::endl;
    }
}

```

```

} else {
    std::cerr << "Incorrect usage. Options:\n";
    std::cerr << ". /pscan" << binaryExt << " <IP Address>\n";
    std::cerr << ". /pscan" << binaryExt << " <IP Address> <startPort> <endPort>\n";
    WSACleanup();
    return 1;
}

for (auto& thread : scanThreads) {
    thread.join();
}

WSACleanup();
return 0;
}

```

Compilation example:

Code g++ pscan.cpp -o pscan -static -lws2_32

Usage example:

Code ./pscan.exe 192.168.1.1

./pscan 192.168.1.1 1 2000

In example 1, it scans the IP for common ports (21, 22, 23, 25, 80, 110, 443)

In example 2, it scans the IP for a range of ports (inclusive range with min and max - example: 1 to 99 will scan 1 and 99, and all numbers between)

Please note that I am still learning C++ and this scanner is pieced together from examples. It works and is tested, but I have not looked into some of the edge cases that could arise here possibly.

You can feel free to use my code above in your own programs or compile & use as-is, for educational purposes or authorized, legal use.

wtf - January 6, 2024, 1:35 pm

Thats excellent nodes ty i usually used zenmap for it

13K_HOPE - January 6, 2024, 1:49 pm

i use nmap why i should use yours whats the secret sauce of your tool?

Hackers - January 6, 2024, 2:01 pm

(Jan 6, 2024 02:35 PM)wtf Wrote: [\[CITE\]](#) Thats excellent nodes ty i usually used zenmap for it
Thanks, glad you like it!

(Jan 6, 2024 02:49 PM)13K_HOPE Wrote: [\[CITE\]](#) i use nmap why i should use yours whats the secret sauce of your tool?No secret sauce, I just like coding and figure some people would prefer to have a small example / source code to use in their own automatic programs.

13K_HOPE - January 6, 2024, 2:03 pm

(Jan 6, 2024 03:01 PM)nodes Wrote: [\[CITE\]](#) Thanks, glad you like it!

No secret sauce, I just like coding and figure some people would prefer to have a small example / source code to use in their own automatic programs.
now im curious to see the code

Hackers - January 6, 2024, 2:05 pm

(Jan 6, 2024 03:03 PM)13K_HOPE Wrote: [\[CITE\]](#) now im curious to see the code
It's in my post.

wtf - January 6, 2024, 2:26 pm

(Jan 6, 2024 03:05 PM)nodes Wrote: [\[CITE\]](#) It's in my post.
Stop hiding the code from us nodes

hamdaanisystems - January 6, 2024, 4:25 pm

Got a question here.... Just like the guy above... I use nmap... The CLI version of zenmap but I'm just now getting into this port scanning thing. Recently I've been scanning devices on my local network and when I scan for TCP protocol I only get port:22 ssh.... So I figured this was good and that my device was perfectly secure as long as no one knew my ssh password or had my key. But my question is dealing with another protocol....when I scanned for UDP I find that there are various ports open running Netbios-ns, Netbios-dgm, llmnr, ect but the scan returns open/filtered? I understand what open means but what does open / filtered mean and how does this have a negative impact on exploitation?

DramaKing - January 6, 2024, 4:51 pm

(Jan 6, 2024 03:03 PM)13K_HOPE Wrote: [\[CITE\]](#) now im curious to see the code
It's uncompiled python and C++ code.

vycka69 - January 6, 2024, 5:24 pm

where can I use this?

DramaKing - January 6, 2024, 7:16 pm

(Jan 6, 2024 05:25 PM)hamdaanisystems Wrote: [\[CITE\]](#) Got a question here.... Just like the guy above... I use nmap... The CLI version of zenmap but I'm just now getting into this port scanning thing. Recently I've been scanning devices on my local network and when I scan for TCP protocol I only get port:22 ssh.... So I figured this was good and that my device was perfectly secure as long as no one knew my ssh password or had my key. But my question is dealing with another protocol....when I scanned for UDP I find that there are various ports open running Netbios-ns, Netbios-dgm, llmnr, ect but the scan returns open/filtered? I understand what open means but what does open / filtered mean and how does this have a negative impact on exploitation?

It returns open/filtered because open UDP ports don't respond to packets. Networking is important. Good networking knowledge would help you understand what NetBIOS and LLMNR do.

(Jan 6, 2024 06:24 PM)vycka69 Wrote: [\[CITE\]](#) where can I use this?
Computer networks

hamdaanisystems - January 6, 2024, 8:14 pm

Thanks for the advice. Is there a particular course that you advise for me to take in understanding networks? I'm in prison and I have nothing but time. Please point me in the right direction....or else I would just hit YouTube up and watch Network Chuck videos.

(Jan 6, 2024 08:16 PM)DramaKing Wrote: [\[CITE\]](#) It returns open/filtered because open UDP ports don't respond to packets. Networking is important. Good networking knowledge would help you understand what NetBIOS and LLMNR do.

Computer networks

(Jan 6, 2024 09:14 PM)hamdaanisystems Wrote: [\[CITE\]](#) Thanks for the advice. Is there a particular course that you advise for me to take in understanding networks? I'm in prison and I have nothing but time. Please point me in the right direction....or else I would just hit YouTube up and watch Network Chuck videos. (Jan 6, 2024 08:16 PM)DramaKing Wrote: [\[CITE\]](#) It returns open/filtered because open UDP ports don't respond to packets. Networking is important. Good networking knowledge would help you understand what NetBIOS and LLMNR do.

Computer networks

Thanks for the advice. Is there a particular course that you suggest I take to gain a solid foundation in regard to networking? If so point me in the right direction. I'm in prison and have nothing but time.

Hackers - January 8, 2024, 6:54 am

(Jan 6, 2024 06:24 PM)vycka69 Wrote: [\[CITE\]](#) where can I use this? You can use this to scan any IP address, such as an IP of a website, your own internet connection, etc.

(Jan 6, 2024 09:14 PM)hamdaanisystems Wrote: [\[CITE\]](#) Thanks for the advice. Is there a particular course that you suggest I take to gain a solid foundation in regard to networking? If so point me in the right direction. I'm in prison and have nothing but time.

I am not a networking expert, but I recommend looking into how routers and modems work in general. If you can learn about websites, learn DNS or general website routing, ports, and proxies.

Scofield112 - January 12, 2024, 7:02 pm

sounds veryyyyyyyyyy goooooooooooooodddd [warn]

DramaKing - January 13, 2024, 9:12 am

(Jan 8, 2024 07:54 AM)nodes Wrote: [\[CITE\]](#) You can use this to scan any IP address, such as an IP of a website, your own internet connection, etc.

I am not a networking expert, but I recommend looking into how routers and modems work in general. If you can learn about websites, learn DNS or general website routing, ports, and proxies. Network+, freecodecamp, NetworkChuck, and David Bombal are all good.

Hackers - February 9, 2024, 12:16 pm

(Jan 13, 2024 10:12 AM)DramaKing Wrote: [\[CITE\]](#) Network+, freecodecamp, NetworkChuck, and David Bombal are all good.

Not too familiar with the last two, but that sounds right.

mynameisoxana - February 25, 2024, 9:55 am

not bad not bad, usually i use nmap or zenmap but thx for that !

artemisiv - March 21, 2024, 3:11 pm

Thank you I like the nodes king

Diauno - April 5, 2024, 1:23 am

cool thank you lots for this!

Hackers - April 10, 2024, 6:01 am

(Apr 5, 2024 01:23 AM)Diauno Wrote: [\[CITE\]](#) cool thank you lots for this!

No problem, glad you like it :)

You can check out my other threads for free source code, programs, and more.

Devender - April 12, 2024, 10:15 am

This is showing only the ports but not the version of services which are running on them, how to evade firewall

Can any tell, ? Thanks in advance

Hackers - April 12, 2024, 11:24 am

(Apr 12, 2024 10:15 AM)Devender Wrote: [\[CITE\]](#) This is showing only the ports but not the version of

services which are running on them, how to evade firewall

Can any tell, ? Thanks in advance

That's correct, this tool only tells you what is open.

The reason is that it can be complicated to actually detect , but not impossible.

For example, let's take port 80 - http.

If I send data to <IP>:80 , I can get a response. Depending on response, I can tell if 80 is for http or not.

If a server is using port 80 to run SSH & I send http data to it, then perhaps I'll receive an SSH-related error from that port.

You need to send data & check response to see if the port is the actual service or not, and if not then you need to compare the response to known responses for all other services to determine what it is.

When people say "common ports" they mean defaults - for example if someone is running SSH on port 80, that's very odd and not the norm at all. Similarly, if someone is running http on port 5878, that would be weird. A lot of tools that show the service name are just showing what the port SHOULD be, and may not actually be confirming it is in fact that service type.

Long story short, no this tool does not show what service it is, but 99% of the time the port is going to be the default use case and when it's not, you can treat it like the exception and manually figure it out if you want. There may be other tools that handle this for you, but mine in this thread currently does not.

DramaKing - April 12, 2024, 12:58 pm

(Apr 12, 2024 10:15 AM)Devender Wrote: [\[CITE\]](#) This is showing only the ports but not the version of services which are running on them, how to evade firewall

I thinks you meant IDS/IPS, not firewall.

laiq__ - April 12, 2024, 1:24 pm

sounds veryy goooooood

Hackers - April 12, 2024, 1:48 pm

(Apr 12, 2024 01:24 PM)laiq__ Wrote: [\[CITE\]](#) sounds veryy goooooood
sounds like youuuuuuuu neeeeed 10 postssssss

Stanley - March 16, 2026, 8:35 pm

I'm Stanley HF's helper bot. The OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley