Nmap 7.97 scan initiated Mon Jun 23 21:20:55 2025 as: nmap -sS -oN scan.results.txt 192.168.56.1/24

Nmap scan report for 192.168.56.1

Host is up (0.000074s latency).

Not shown: 994 closed tcp ports (reset)

PORT STATE SERVICE

22/tcp open ssh

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

1042/tcp open afrog

1043/tcp open boinc

Nmap done at Mon Jun 23 21:21:36 2025 -- 256 IP addresses (1 host up) scanned in 40.96 seconds

Port 22 Details

threat/applicat

known port assignments and vulnerabilities

Port(s)	Protocol	Service	Details
22	udp	ssh	The Secure Shell (SSH) Protocol [RFC 4251] Old verson of pcAnywhere uses port 22/udp (no relation to ssh and port 22/tcp). The real pcAnywhere port is 5632. The value 0x0016 (hex) is 22 decimal; the value of 0x1600 (hex) is 5632 decimal. Some say that pcAnywhere had a byte-swapping bug that led to its incorrect use of port 22.
22	tcp,sctp	SSH	Secure Shell - most common use is command line access, secure replacement of Telnet. Could also be used as an encrypted tunnel for secure communication of virtually any service [RFC 4251], [RFC 4960] freeSSHd 1.2 and earlier allows remote attackers to cause a denial of service (crash) via a SSH2_MSG_NEWKEYS packet to TCP port 22, which triggers a NULL pointer dereference. References: [CVE-2008-0852] [BID-27845] [SECUNIA-29002] The SSH service on Dell PowerConnect 3348 1.2.1.3, 3524p 2.0.0.48, and 5324 2.0.1.4 switches allows remote attackers to cause a denial of service (device reset) or possibly execute arbitrary code by sending many packets to TCP port 22. References: [CVE-2013-3594], [XFDB-90595], [BID-65070] RUCKUS could allow a remote attacker to bypass security restrictions. An unauthenticated remote attacker with network access to port 22 can tunnel random TCP traffic to other hosts on the network via Ruckus devices. A remote attacker could exploit this vulnerability to bypass security restrictions and gain unauthorized access to the vulnerable application. References: [XFDB-84626] 360 Systems contains a default hard-coded password in the image server series. By logging into the device via TCP port 22, a remote attacker could gain root privileges on the system to modify or upload video to play immediately and affect the emergency broadcast system in the United States. References: [XFDB-82650], [BID-58338], [CVE-2012-4702]

Port 135 Details

threat/applicat

known port assignments and vulnerabilities

Port(s)	Protocol	Service	Details
135	tcp,udp	loc-srv	Remote Procedure Call (RPC) port 135 is used in client/server applications (might be on a single machine) such as Exchange clients, the recently exploited messenger service, as well as other Windows NT/2K/XP software. If you have remote users who VPN into your network, you might need to open this port on the firewall to allow access to the Exchange server. There is a RPC (a RPC's Endpoint Mapper component) vulnerability in Windows NT where a malformed request to port 135 could cause denial of service (DoS). RPC contains a flaw that causes it to fail upon receipt of a request that contains a particular type of malformed data. To restore normal functionality victim has to reboot the system. Alternatively, you can upgrade/patch your OS (there is patch downloadable from Microsoft), or you can close port 135. Port 135 is used by Messenger Service (not MSN Messenger) and exploited in popup net send messenger spam [MSKB 330904]. To stop the popups you'd need to filter port 135 at the firewall level or stop the messenger service. The service uses all the following ports: 135/tcp, 135/udp, 137/udp 138/udp, 139/tcp, 445/tcp. MS Security Bulletin [MS03-026] outlines another critical Buffer Overrun RPC vulnerability that can be exploited via ports 135, 139, 445, 593 (or any other specifically configured RPC port). You should filter the above mentioned ports at the firewall level and not allow RPC over an unsecure network, such as the Internet. W32.Blaster.Worm [Symantec-2003-081113-0229-99] - a widely spread worm that exploits the DCOM RPC vulnerability described above (MS Security Bulletin [MS03-026]). The worm allows remote access to an infected computer via ports 4444/tcp and 69/UDP, and spreads through port 135/tcp. To avoid being infected consider closing those ports. Port is also used by Messenger Service (not MSN Messenger) and exploited in popup net send messenger spam [MSKB 330904]. To stop the popups you'd need to filter port 135 at the firewall level or stop the messenger service. The service uses all the following ports: 135/tcp, 135/udp, 137/udp 138/udp, 139/tcp, 445/tcp.

Port 139 Details

threat/applicatic

known port assignments and vulnerabilities

Port(s)	Protocol	Service	Details
139	tcp,udp	netbios-ss	NetBIOS is a protocol used for File and Print Sharing under all current versions of Windows. While this in itself is not a problem, the way that the protocol is implemented can be. There are a number of vulnerabilities associated with leaving this port open. **NetBios services:** NETBIOS Name Service (TCP/UDP: 137) NETBIOS Datagram Service (TCP/UDP: 138) NETBIOS Session Service (TCP/UDP: 139) By default, when File and Print Sharing is enabled it binds to everything, including TCP/IP (The Internet Protocol), rather than just the local network, meaning your shared resources are available over the entire Internet for reading and deletion, unless configured properly. Any machine with NetBIOS enabled and not configured properly should be considered at risk. The best protection is to turn off File and Print Sharing, or block ports 135-139 completely. If you must enable it, use the following guidelines: 1. Use strong passwords, containing non-alphanumeric characters. 2. Attach "$" at the end of your share names (the casual snooper using net view might not see them). 3. Unbind File and Print Sharing from TCP/IP and use NetBEUI instead (it's a non-routable protocol). 4. Block ports 135-139 in your router/firewall. Keep in mind that you might still be leaking out information about your system that can be used against you (such as your computer and workgroup names) to the entire Internet, unless ports are filtered by a firewall. There is also a Critical Windows RPC vulnerability affecting ports 135,139 and 445, as detailed here: MS Technet Security Bulletin [MS03-026]

Port 445 Details

threat/applicat

known port assignments and vulnerabilities

Port(s)	Protocol	Service	Details
445	tcp	microsoft-ds	TCP port 445 is used for direct TCP/IP MS Networking access without the need for a NetBIOS layer. The SMB (Server Message Block) protocol is used for file sharing in Windows NT/2K/XP and later. In Windows NT it ran on top of NetBT (NetBIOS over TCP/IP, ports 137, 139 and 138/udp). In Windows 2K/XP and later, Microsoft added the possibility to run SMB directly over TCP/IP, without the extra NetBT layer, for this they use TCP port 445. Microsoft Lync server uses these ports: 444, 445, 448, 881, 5041, 5060 - 5087, 8404 TCP 80, 135, 443, 4443, 8060, 8061, 8080 TCP - standard ports and HTTP(s) traffic 1434 UDP - SQL 49152-57500 TCP/UDP - media ports Port 445 should be blocked at the firewall level. It can also be disabled by deleting the HKLM\System\CurrentControlSet\Services \NetBT\Parameters\TransportBindName (value only) in the Windows Registry. Leaving port 445 open leaves Windows machines vulnerable to a number of trojans and worms: W32.HLLW.Deloder [Symantec-2003-030812-5056-99] IraqiWorm (aka Iraq_oil.exe) W32.HLLW.Moega [Symantec-2003-080813-3234-99] W32.Korgo.AB [Symantec-2004-092415-4853-99] (2004.09.24) Backdoor.Rtkit.B [Symantec-2004-100115-0426-99] (2004.10.01) W32.Sasser.Worm [Symantec-2004-050116-1831-99] - exploits port 445 vulnerabilities, opens TCP ports 5554,9996. Trojan.Netdepix.B [Symantec-2005-011715-5404-99] (2005.01.16.) - trojan uses port 445, opens port 15118/tcp. Backdoor.IRC.Cirebot [Symantec-2003-080214-3019-99] (2003.08.02) - trojan that exploits the MS DCOM vulnerability, uses ports 445 & 69, opens backdoor on port 57005. Windows Null Session Exploit.

Port 1042 Details

threat/application/port search:

SEARCH

known port assignments and vulnerabilities

Port(s)	Protocol	Service	Details	Source
1042	tcp	trojans	ASUS Armoury Crate "NodeJS Web Framework" process uses TCP ports 1042 and 1043 Trojans that use this port: Bla1.1, MyDoom.L [Symantec-2004-071915-0829-99]	*SG*
1042	udp	games	Battlestations: Midway	*SG*
1042	tcp,udp	trojan	BLA trojan	*Trojans*
1042,2302,6500	udp	applications	Battlestations - Midway	*Portforward*
1042	tcp,udp	BLAtrojan	[trojan] BLA trojan	*Neophasis*
1042	tcp	threat	BLA trojan	*Bekkoame*
1042	tcp,udp	afrog	Subnet Roaming, registered 2004-11	*IANA*

For Checking Port 1042

```
C:\Users\vikas>netstat -aon | findstr :1042
  TCP    0.0.0.0:1042           0.0.0.0:0              LISTENING       10740
  TCP    127.0.0.1:1042         127.0.0.1:49731        ESTABLISHED     10740
  TCP    127.0.0.1:1042         127.0.0.1:49733        ESTABLISHED     10740
  TCP    127.0.0.1:49731        127.0.0.1:1042         ESTABLISHED     10452
  TCP    127.0.0.1:49733        127.0.0.1:1042         ESTABLISHED     10620
  TCP    [::]:1042              [::]:0                 LISTENING       10740

C:\Users\vikas>
C:\Users\vikas>tasklist /FI "PID eq <your_PID>"
ERROR: The search filter cannot be recognized.

C:\Users\vikas>tasklist /FI "PID eq 10740"

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
asus_framework.exe           10740 Console                    1     14,280 K

C:\Users\vikas>tasklist /FI "PID eq 10452"

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
AcPowerNotification.exe      10452 Console                    1      3,876 K

C:\Users\vikas>tasklist /FI "PID eq 10620"

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
ArmourySocketServer.exe      10620 Console                    1      1,460 K
```

PID	Process Name	Description	Safe?
10740	asus_framework.exe	Part of **ASUS Armoury Crate** – manages device tuning (RGB, fan, etc.)	✅ Yes, known
10452	AcPowerNotification.exe	Likely related to **power management** or AC plug/unplug notifications on ASUS	✅ Yes, low impact
10620	ArmourySocketServer.exe	Also part of **ASUS Armoury Crate**, used for internal communication	✅ Yes, expected

No immediate malware threat is present.
All ports/processes are being used by **legit ASUS software**, specifically **Armoury Crate** and related background services.

Port 1043 Details

threat/application/port search: SEARCH

known port assignments and vulnerabilities

Port(s)	Protocol	Service	Details	Source
1043	tcp	trojan	ASUS Armoury Crate "NodeJS Web Framework" process uses TCP ports 1042 and 1043 Dosh Backdoor.Win32.Mhtserv.b / Missing Authentication - Mhtserv.b listens on TCP port 1043, apparently there is no authentication required to access this backdoor. Accessing the backdoor using telnet you are greeted with a "Command" prompt, issuing a lowercase "L" char will get you a dir listing of system32. References: [MVID-2021-0059]	*SG*
1043	tcp	trojan	Dosh	*Trojans*
1043	tcp	boinc	BOINC Client Control or Microsoft IIS	*Nmap*
1043	udp	boinc	BOINC Client Control	*Nmap*
1043	tcp,udp	boinc-client	BOINC Client Control, registered 2004-11	*IANA*

```
C:\Users\vikas>netstat -aon | findstr :1043
  TCP    0.0.0.0:1043           0.0.0.0:0              LISTENING       10740
  TCP    [::]:1043              [::]:0                 LISTENING       10740

C:\Users\vikas>tasklist /FI "PID eq 10740"

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
asus_framework.exe           10740 Console                    1     14,504 K
```

Port 1043 is being used by:

- **PID**: 10740
- **Process**: asus_framework.exe

Meaning **ASUS Armoury Crate** is responsible for opening both ports **1042 and 1043**.

Port	Service	Description	Potential Risks
22	SSH	Secure remote login protocol. Could allow remote access if not secured.	Brute-force remote login
135	MSRPC	Microsoft RPC. Used by Windows for DCOM — often targeted by malware.	DCOM/RPC exposure
139	NetBIOS-SSN	File/printer sharing. Can be vulnerable if exposed outside the LAN.	SMB vulnerabilities
445	Microsoft-DS	SMB file sharing. Should be blocked from external access.	SMB vulnerabilities
1042	Afrog	Part of **ASUS Armoury Crate**	These ports are used by malware in the wild, they **can be abused** if Armoury Crate is vulnerable or misconfigured.
1043	BOINC	Part of **ASUS Armoury Crate**	These ports are used by malware in the wild, they **can be abused** if Armoury Crate is vulnerable or misconfigured.