Use three tools to analyze and get the result:

Nmap, Netcat and Wireshark

TCP Behavior:

send=SYN, recieve=SYN-ACK

Port Open

send=SYN, recieve=RST-ACK

Port Close

send=SYN, recieve=ICMP-Port-Unreachable

Blocked by Firewall (Filtered)

send=SYN, recieve=Nothing

Blocked by Firewall (Filtered)

UDP Behavior:

send=UDP, recieve=UDP-response

Port Open

send=UDP, recieve=ICMP-Port-Unreachable

Port Close OR Blocked by Firewall

send=UDP, recieve=Nothing

Port Close OR Blocked by Firewall OR Port Open but it is looking for specific data in UDP payload, nmap result: (Open|Filtered)

Victim:

nc -lnvp 1234

Attacker:

nc -nvv -w 1 -z 192.168.1.4 1234-1236 >>>> for tcp

nc -nvv -u -w 1 -z 192.168.1.4 135-139 >>>>> for udp

Follow this port on wireshark:

fillter >>> tcp.port>=1234

fillter >>> udp.port>=135

FTP

port: 21

nmap scripts

ls -l /usr/share/nmap/scripts/ftp\*

Check if anonymous FTP access is available:

ftp [host]

Username: anonymous

Password: anything

Test if you can navigate, list, read, get or put files:

cd .. # move up one directory

pwd # print working directory

dir -C # list files

mkdir [folder] # make a directory

get [file] # get a file

put [file] # send a file