# 7. POTENTIAL SECURITY RISKS FROM THE OPEN PORTS.

## Security Risks from These Open Ports

\*Port 445 - File Sharing (SMB)

This one's a nightmare for security folks. It's like leaving your front door not just unlocked, but wide open with a sign saying "come on in." This port has been the highway for some of the worst cyberattacks in history - remember WannaCry? That ransomware spread through networks by exploiting this exact service. Hackers love this port because once they get in through SMB, they can easily hop from computer to computer across your entire network. It's also a favorite for stealing login credentials and planting ransomware.

\*Port 135 - Windows RPC

Think of this as the master key to Windows systems. When attackers compromise this service, they basically get a backstage pass to your computer. It's been around forever in Windows, which means it's had plenty of time to accumulate vulnerabilities. Hackers use this to escalate their privileges - basically going from a regular user to an administrator. Once they own this service, they can pretty much do whatever they want on your system.

\*Port 5432 - PostgreSQL Database

Your database is where all the good stuff lives - customer data, financial records, personal information, you name it. If someone breaks into your PostgreSQL server, it's like giving them the keys to your company's vault. The scary part is that many people set up databases with weak passwords or default settings. Attackers will try to brute force their way in, and once they're inside, they can steal everything or hold your data hostage with ransomware.

\*Port 8080 - Web Proxy

This is often overlooked, but it can be just as dangerous. If this proxy isn't properly secured, attackers can use it to hide their tracks while launching attacks on other systems. It's like having someone use your internet connection to commit crimes - suddenly all the bad stuff looks like it's coming from you. Plus, these services sometimes have web interfaces with weak security that hackers can exploit.

\*Port 8090 - Operations Messaging

This might seem harmless since it's just for monitoring, but it's actually a goldmine of information for attackers. Through this service, hackers can learn about your network layout, what systems you're running, when they're having problems, and who has access to what. It's like having someone read all your internal company memos - they'll know exactly how your business works and where the weak spots are.

\*The Old and Weird Stuff

Those other ports running older services like Hotline or Interwise? They're actually super dangerous because nobody thinks about them anymore. These legacy systems often have known vulnerabilities that were never patched because everyone forgot they were still running. It's like having an old lock that everyone knows how to pick, but you forgot you even had a door there.