

# Port Scanning and its Legal Implications

by  
Adv. Abhinav Bhatt  
Asian School of Cyber Laws  
[ab@asianlaws.org](mailto:ab@asianlaws.org)

---

In the mind of a reader who has knowledge of the technology that I am about to throw light upon, the above statement, would surely cause some amount of apprehension if not criticism at my trying to knot together two diverse issues. I mean every one knows that the age-old adage means that 'before acting against another one must be ready to guard one's own actions.' I admit that at the onset, this meaning does not seem even distantly in the same context as the act of port scanning. However it will be my effort through this paper to bring one within the scope and the context of the other. This is because I feel that that most lawmakers have failed to appreciate the fact, that hacking or indeed getting access to another system, whether with authority or without, does not necessarily remain confined to itself but includes and involves many other smaller acts, that by themselves create legal ramifications. In this paper, I would like to explore some of the rights of the 'scanned' as against the liabilities of the 'scanner'.

## What is Scanning?

The term 'scan' has emerged from the Latin word '*scandere* - which means to climb or to *scale*'. The other meanings <sup>(1)</sup> attributed to this word include:

1. look at all parts successfully of (face, horizon etc.), intently or quickly
2. examine all parts to detect radio activity
3. cause (particular region) to be traversed by controlled (radar etc.) beam

What we are most interested in is the use of this term in modern day computer terminology. So, for the sake of understanding how far the English literary definitions hold well under the new use of this word, let us examine how the same word has been explained under the Indian Ministry of Information Technology Site Glossary <sup>(2)</sup>.

**Port:**An electronic connection that allows data to travel between a client PC and a server on the network.

**Port Scan:**Data sent by the cracker over the Internet to locate a PC or network and

determine whether it has open ports that will accept a connection.

'Port Scanning' refers to the act of using various open ended technologies, tools and commands to be able to communicate with another remote computer system or network, in a stealth mode, without being apparent, and be able to obtain certain sensitive information about the system functions and the properties of the hardware and the software being used by the remote systems.

Ports are basically entry exit points that any computer has, to be able to communicate with external machines. Each computer is enabled with 3 or more external ports. These are the ports used by the computer to communicate with the other computers, printer, modem, mouse, video game, scanner and other peripherals. The important characteristic about these 'external ports' is that they are indeed external and visible to the naked eye. One just has to look at the back of the CPU Tower, to be able to see the different sockets that are meant to be connected to various external devices. However these are not the only ports that any computer has. Every computer is also blessed with virtual ports that number in a few thousand ... Sixty five thousand five hundred and thirty six to be precise.

Your computer uses these numerous ports to virtually communicate with other systems when using specific protocols<sup>2</sup>. As you might know computers use a certain collection of protocols called TCP/IP suite to communicate and exchange information.

Protocols<sup>(3)</sup> like:

1. File Transfer Protocol (for uploading and downloading of information)
2. Simple Mail Transfer Protocol (used for sending / receiving emails)
3. Telnet Protocol (used to connect directly to a remote host)
4. Internet Control Message Protocol (used for checking network errors e.g. Ping<sup>(4)</sup>)

and many others are collectively known as the TCP/IP suite of protocols and are used to communicate with other computers for specific message formats. Most of these protocols are tied to specific port numbers that are used to transfer particular message formats as data. For example port number 21 is the FTP port. Port number 23 is the telnet port and all web pages are viewed using the Hyper Text Transfer Protocol (HTTP), which is tied to the port number 80.

But not all 65,000 and more port numbers are dedicated ports. Only ports 1 to 1024 are dedicated ports, the others are used as stand-bys and can be used by a network administrator for running any applications or establishing communication channels with other computer systems. Under normal circumstances all these ports are open and their status is said to be "listening for connections" which means that they are ready to establish communication with

other machines on a network. In such a case any external machine wishing to send data shall, unless restricted, be allowed to communicate directly with your machine.

This is definitely a very dangerous proposition that your machine is such a promiscuous mode that it can be accessed and even controlled by more than just yourself, in fact by many remote hosts. It leads us to the imminent risk that your computer might at anytime shut you out of its control, and may even start acting against you by sending your important files over to your enemies. Thus all netads and sysops as a rule will shut all ports that are not in use, and secure access to all the ports that are open so that no person may remotely use a port to send data to an unauthorized port in a clandestine fashion.

Whatever the case may be, the importance of port scanning cannot be under stated. All port-scanning tools give the user (adversary / assessor) the chance to assess the remote system for weaknesses or vulnerabilities, without letting the computer administrator know about such an audit. This enables the adversary to plan out an attack against the remote system, based on his previous reconnoiter, with the victim being none the wiser. Generally when any information is exchanged between two computer systems, some logs and records are created on both ends, as well as the users of the computers are required to participate in the exchange of information, however, in this case, the computer of one communicates with the network of another in a stealth mode that requires no dual participation or log recording.

Now let us examine the legality of port scanning.

Under the Indian Information Technology Act, 2000, the act of port scanning does not amount to hacking, <sup>(5)</sup>

which is defined as:

"Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking."

The essential elements of hacking are

1. Intention or Knowledge
2. Wrongful Loss to Public or Person
3. Deletion / Alteration / Destruction or
4. Diminishes Value or Utility

of information residing in a computer resource

Port Scanning will satisfy the first requirement of Knowledge or Intention.

But the second essential is not met, as port scanning does not necessarily cause any wrongful loss. E.g. if a network administrator, scans his own network for security reasons, then he will not intend to create any wrongful loss.

Also, all the other elements of hacking are also not invoked as port scanning merely scans the crust of the network without affecting any information resource residing within it.

Thus Port Scanning definitely does not attract the offence of 'hacking', unless it is used by a cracker, with the intention to crack the system, and in conjunction with any other tool that actually changes any information that resides in the computer.

Under the US Computer Fraud and Abuse Act, as well as under cyber laws of other countries, the element of "unauthorized access" is generally found to sufficiently cover the act of port scanning. Specifically 18 USC Sec. 1030(a)(5)(B) of the American Act has been applied to the act of port scanning in a previous case.

This subsection essentially has six elements that the prosecution must prove.

- a. The defendant intentionally accessed a protected computer,
- b. The defendant did not have authorization to access the computer
- c. As a result of the access, the defendant recklessly caused damage
- d. The damage impaired the integrity or availability of data, a program, a system, or information
- e. That caused a loss aggregating at least \$5000 or
- f. Threatened public health or safety

When we compare this section with the Section 66 of the Information Technology Act, 2000 we find a few similarities as far as 'causing intentional damage to data or information' however the similarity ends here as this section, under US law, also extends to unauthorized access of a protected computer, and covers unintentional or reckless damage, of the value of 5000 \$ or above. In the Indian scenario, intention and knowledge have to be present in the act of doing the damage also. Lastly, this section of the American Act, also takes in any act that threatens public health and safety which S. 66 of the IT Act, does not.

In November 2001 a federal US court has dealt with a case of port scanning in the Moulton v. VC3 case under 18 USC Sec. 1030(a)(5)(B), of the Computer Fraud and Abuse Act of America. The facts of the case were as follows.

Scott Moulton was a network security consultant, who had a service and maintenance contract with the county 911 Center to perform computer network related work. He was

arrested and charged with violating the Computer Fraud and Abuse Act after he port scanned the 911 center's computer network. The defendant stated that he was concerned with the security of the network and had been authorized by the county in the service contract to maintain the networks. The defendant scanned the vulnerability of the LAN network between the sheriff's office and the 911 Center and performed a series of remote port scans on the system. The system's network administrator was using a network analyzer and a firewall system and he was able to immediately notice the port scanning activity. The Sysop then e-mailed the defendant questioning him the reason and the motive for scanning the ports. On being challenged, the defendant behaved in a suspicious manner, by quitting the scanning activity and immediately emailed back, informing the administrator that he had a service contract with the county and he was authorized to check the security of the network.

Concerned about the network's security and the act of the defendant, the network administrator then contacted the sheriff, who in turn arrested the defendant on state and federal computer crime charges.

**Charge:**

Specifically, Moulton was charged with violating 18 USC Sec. 1030(a)(5)(B), which prohibits the *"intentional accessing [of] a protected computer without authorization, [that] as a result of such conduct, recklessly causes damage."*

**Argument:**

The county denied that they gave him authority or 'access' to conduct port scans on the system and argued that he accessed the computer unlawfully and with intention. Additionally the County alleged that it had to spend time and money to research the scanning and determine whether there were any penetrations of the system. But they admitted that Moulton caused no structural damage. In this case, the county argued that the act of port scanning itself was a crime. But the judge did not accept that argument.

**Held:**

The court said the statute clearly states that the damage must be impairment to the integrity and availability of the network. Since the county's network security was never actually compromised and no program or information was ever unavailable as a result of the defendant's activities. If there was no impairment from the scanning or the scans weren't so excessive or load bearing that the network's availability was interrupted, then there was no damage. Without damage, there is no crime, which is what the Courts held in the case. The court didn't need to address the *damage* element since the County failed to prove it conclusively.

Looking at the above case we do realize that in certain cases even though port scanning does not inherently cause any damage, yet the very act should create legal liability. This is because 'port scanning' is an inherently dangerous activity which although it does not cause

direct damage to any computer system, it enables a cracker to launch a successful attack against your system, and if an offence is a crime then the preparation should also be punishable, which sadly is not the case.

For example, the Criminal Procedure Code has made the carrying / possession of house breaking implements an offence for which the Police Officer may arrest without a warrant, and the burden of proving the reason for carrying the implements shall lie upon the possessor of those implements. The implements themselves are not illegal, but the possession of the implements shall authorize a Police Officer to arrest you on the mere suspicion that you might be involved in or preparing for a crime of house breaking. In such a case the person found with the implement would have to give the Police, the reason and the intention with which such person was in possession of the implements. In absence of a reasonable explanation, the Police Officer would have sufficient cause to arrest the person.

Though the Information Technology Act, 2000 does not cover acts like port scanning under the offence of 'hacking' yet in certain cases, where the security of certain systems is utmost priority like in case of defense and strategic installations, port scanning can be covered. Section 70 of the IT Act talks about unauthorized access of a protected system.

The sub section (3) states

*"Any person who secures access or attempts to secure access to a protected system<sup>(6)</sup> in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine." Thus although this section only covers systems that are notified as protected systems it is able to afford protection to the important and strategic installations and systems of the country from acts of port scanning by making access as well as attempt to secure access punishable up to 7 years, thus acting as a sufficient deterrent to crackers that might intend to launch attacks against the vital security of our nation.*

### **Conclusion:**

While port scanning is a useful reconnaissance technique used by crackers to locate vulnerabilities in systems that are running services on certain computer ports, it is essentially a passive query that works within the architecture of TCP/IP. Without the ability to query remote computer ports to determine the service that is running and its compatibility with other computers, the Internet would cease to function. Many argue that port scanning and other tools like network analyzers, packet sniffers etc. normally used for analyzing networks and their vulnerabilities are used for malicious purposes having the element of criminal intent. Thus, the use of these should be made illegal, even if the use was innocent and did not cause any real damage.

However, only when a cracker uses this tool to commit a crime, then such port scanning

should be illegal. But as with the "House Breaking" law, the criminal intent of the person is what turns a good tool bad. But since people can't read minds, intent is usually proven by the criminal act itself. Since there are legitimate uses for port scanning, it is impossible to determine the intent of the scanner unless he goes on to penetrate the system, which is a criminal act already u/s 66 of the Information Technology Act.

The recently passed USA Patriot Act dramatically changes the Computer Fraud and Abuse Act. However, it does not change the requirement that there must be damage and loss. Damage still requires impairment to the integrity or availability of data, a program, a system or information. Normal port scanning is not likely to cause such impairments. However, the USA Patriot Act does make it much easier to meet the definition of loss, which must exceed \$5,000. Victims can now add nearly every conceivable expense associated with the incident to arrive at the \$5,000 threshold.

The court in Moulton arrived at a logical conclusion to anyone even remotely familiar with network technology. However, the fact that the county decided to even prosecute under this obvious mistake of fact should be a word of caution to network security consultants and others involved in penetration testing. Many clients are unfamiliar with the details of the technology and can misinterpret harmless measures as criminal acts. It is highly recommended that the initial service or consulting contract with the client should grant enough leeway to ensure that they are authorized to conduct the tests and the scope of the access is essentially open-ended. If the consultant has such authorization, the only computer crime that the consultant can be liable for is causing intentional damage to the system under S. 66 in case of hacking but not unauthorized access. Thus, you see, those who live in glass houses ... shouldn't peep into others lives.

**(1)** As per the Concise Oxford Dictionary of Current English, 7th Edition.

**(2)** <http://www.itsecurity.gov.in>

**(3)** Protocols are like languages that computer use to communicate with each other for transmitting data across. Formal description of message formats as well as the rules that computers must follow to exchange those messages.

**(4)** Packet Internet Gopher -made famous by the "Ping of Death Attack" uses a small 32 bytes data packet to check if remote host is alive on the network.

**(5)** Section 66 (1) of the Information Technology Act, 2000

**(6)** The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system. S. 70 (1)

© 2002 Asian School of Cyber Laws. All Rights Reserved.

[Cyberlaws news archives](#) | [Information Security news archives](#)

## [ASCL Online Cyber Law Library Index](#)

---

[Cyber Crime](#)

[Electronic Signatures](#)

[Indian cyberlaw](#) (Cybercrimes | Digital signatures | General | Cyber law enactments)

[Cyber Laws](#) (Cybercrime laws of major countries | Ecommerce laws of major countries | Miscellaneous )

## [ASCL Online Information Security Library Index](#)

---

[Algorithms](#)

[Digital Signatures](#)

[General](#)

[PKI](#)

[Security Policies](#)

[Home](#) | [Disclaimer](#) | [Contact Us](#)