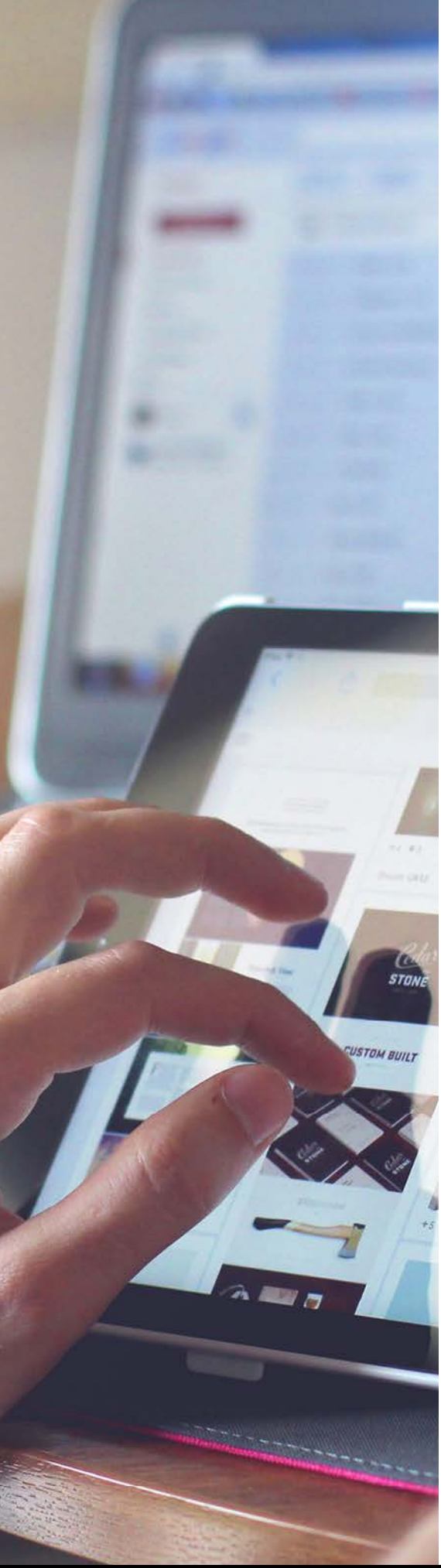
GlobalLogic®

Why do Hackers

IP SPOOF

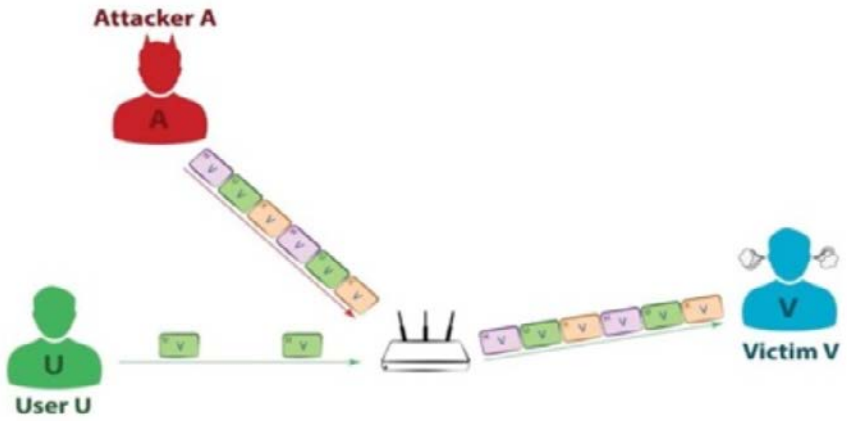
and How to Prevent It



What is IP Spoofing?

IP Spoofing is used to gain unauthorized access to a network by impersonating a source with authorized access. IP spoofing is a cyber attacking technique. The hacker pretends to be someone else and conceals their identity to gain access to a network and hijack the browser. IP spoofing is also called IP address forgery or host file hijack.

Initially the hacker will spend time finding the IP address of a trusted host and then modify the headers of the packets being sent, so it appears to the computer that the packets are coming from that trusted host.



How Does IP Spoofing Work?

A user accesses the Internet from their local computer which has the IP address “192.108.0.5”. When an IP spoofing attack occurs, this address is hidden and the user sends the packets indicating the spoofed IP address “192.108.0.6” which is an authorized IP address. These IP addresses are used to identify each computer in the network. In Internet communication, the data is transferred in the form of packets.

For example: the client sends web requests in the form of data packets to the server and the webserver sends back the responses in the form of data packets. When a client sends a packet to the server, the packet will have the IP address of the computer it is

coming from. When an IP spoofing attack occurs, this source details that IP address specifies the sender of the packet is not actual, but a fraudulent IP address which is permitted to access the website. This will make the server handle the request packet as it is coming from the permitted user. Then the server will grant access to the attacker causing various security threats.

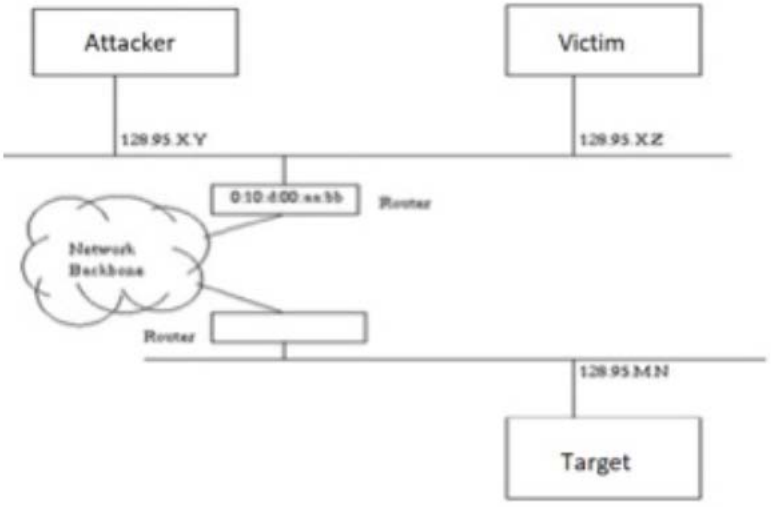
Types of IP Spoofing

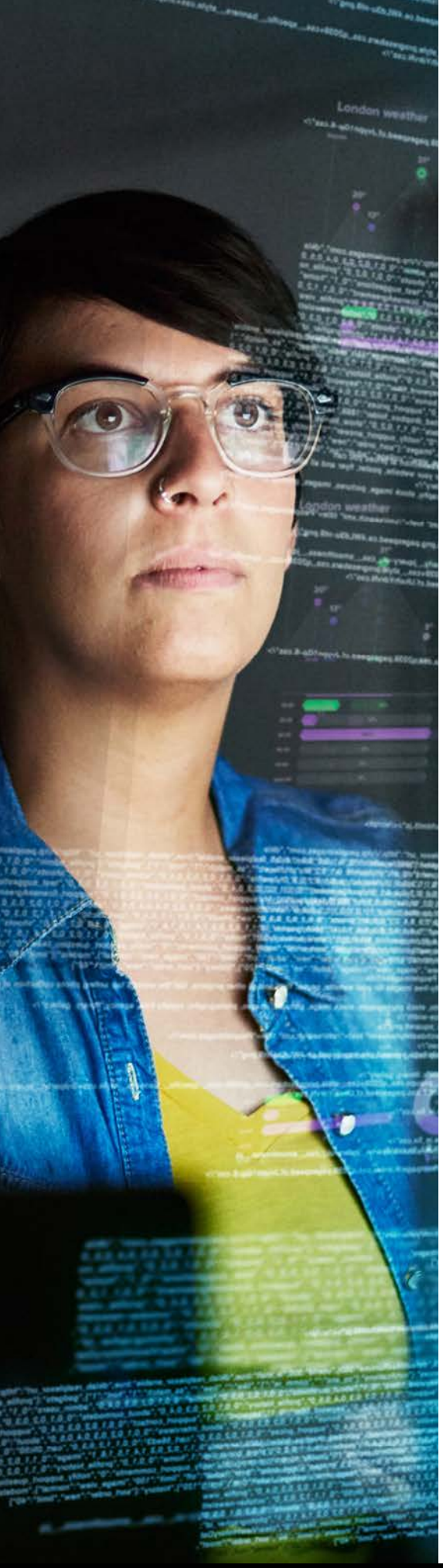
Non-Blind Spoofing

This type of attack takes place when the attacker is on the same subnet as the victim. The sequence and acknowledgement numbers can be sniffed, eliminating the potential difficulty of calculating them accurately. The biggest threat of spoofing in this instance would be session hijacking. This is accomplished by corrupting the data stream of an established connection, then re-establishing it based on correct sequence and acknowledgement numbers with the attack machine. Using this technique, an attacker could effectively bypass any authentication measures to build the connection.

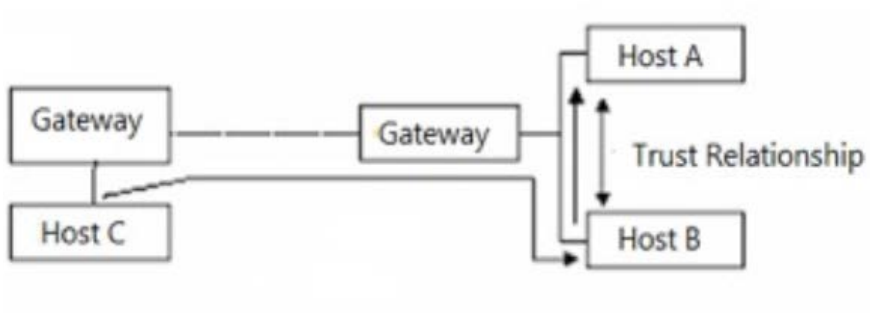
Blind Spoofing

This is a more sophisticated attack, because the sequence and acknowledgement numbers are unreachable. To circumvent this, several packets are sent to the target machine to sample sequence numbers. While not the case today, machines in the past used basic techniques for generating sequence numbers.



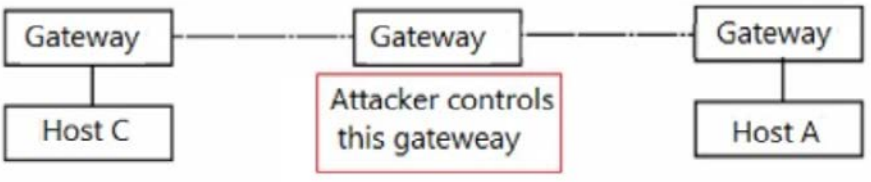


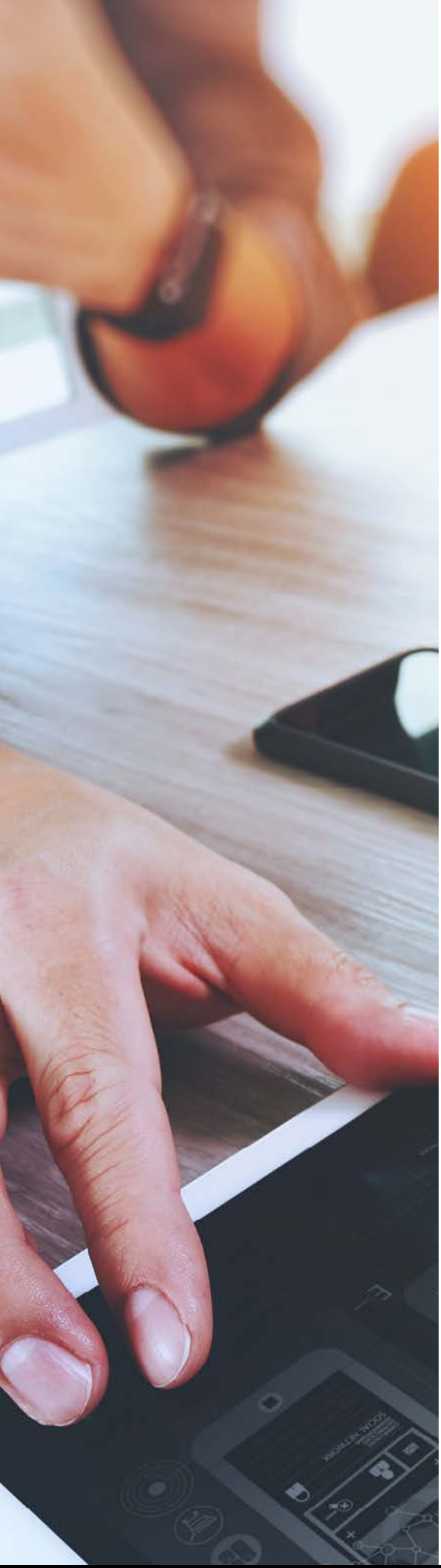
It is relatively easy to discover the exact formula by studying packets and TCP sessions. Today, most OSs implement random sequence number generation, making it difficult to predict them accurately. If, however, the sequence number was compromised, data can be sent to the target. Several years ago, many machines used host-based authentication services (i.e. Rlogin). A properly crafted attack could add the requisite data to a system (i.e. a new user account), blindly, enabling full access to the attacker who was impersonating a trusted host.



Man In the Middle

In MIM attacks, a malicious party intercepts a legitimate communication between two friendly parties. The malicious host then controls the flow of communication and can eliminate or alter the information sent by one of the original participants without the knowledge of either party. In this way, an attacker can fool a victim into disclosing confidential information by “spoofing” the identity of the original sender, who is presumably trusted by the recipient.





Denial of Service

IP spoofing is almost always used in what is currently one of the most difficult attacks to defend against – denial of service attacks, or DoS. Since hackers are concerned only with consuming bandwidth and resources, they need not worry about properly completing handshakes and transactions. Instead, they wish to flood the victim with as many packets as possible in a short amount of time. To prolong the effectiveness of the attack, they spoof source IP addresses to make tracing and stopping the DoS as difficult as possible. When multiple compromised hosts are participating in the attack, all sending spoofed traffic, it is very challenging to quickly block the traffic.

Misconceptions of IP Spoofing

While some of the attacks described above are a bit outdated, such as session hijacking for host-based authentication services, IP spoofing is still prevalent in network scanning and probes, as well as denial of service floods. However, the technique does not allow for anonymous Internet access, which is a common misconception for those unfamiliar with the practice. Any sort of spoofing beyond simple floods is relatively advanced and used in very specific instances such as evasion and connection hijacking.

How to Prevent IP Spoofing

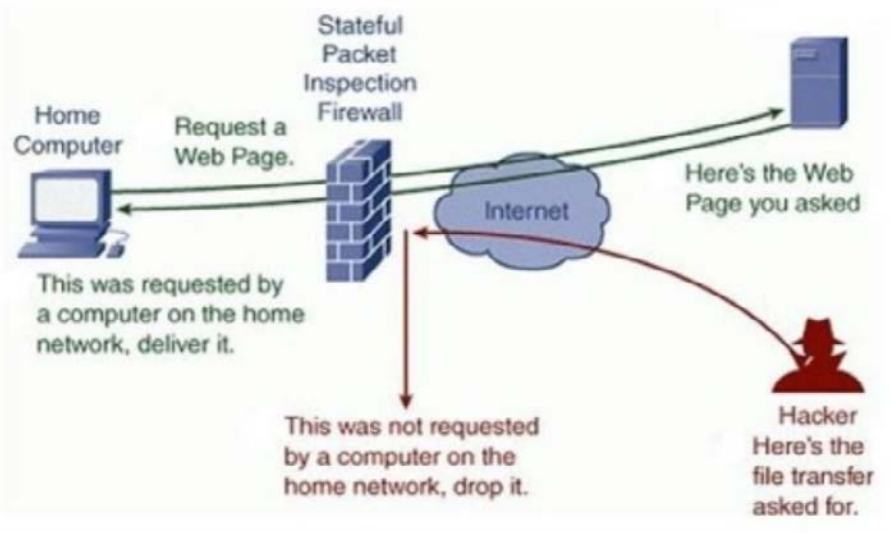
Organizations can take measures to stop spoofed packets from infiltrating their networks, including:

- Monitor networks for atypical activity.
- Deploy packet filtering systems capable of detecting inconsistencies, such as outgoing packets with source IP addresses that don't match those on the company's network.
- Use robust verification methods for all remote access and for systems on the enterprise intranet to prevent accepting spoofed packets from an attacker who has already breached another system on the enterprise network.

  - Authenticating IP addresses of inbound IP packets.
  - Use a network attack blocker.

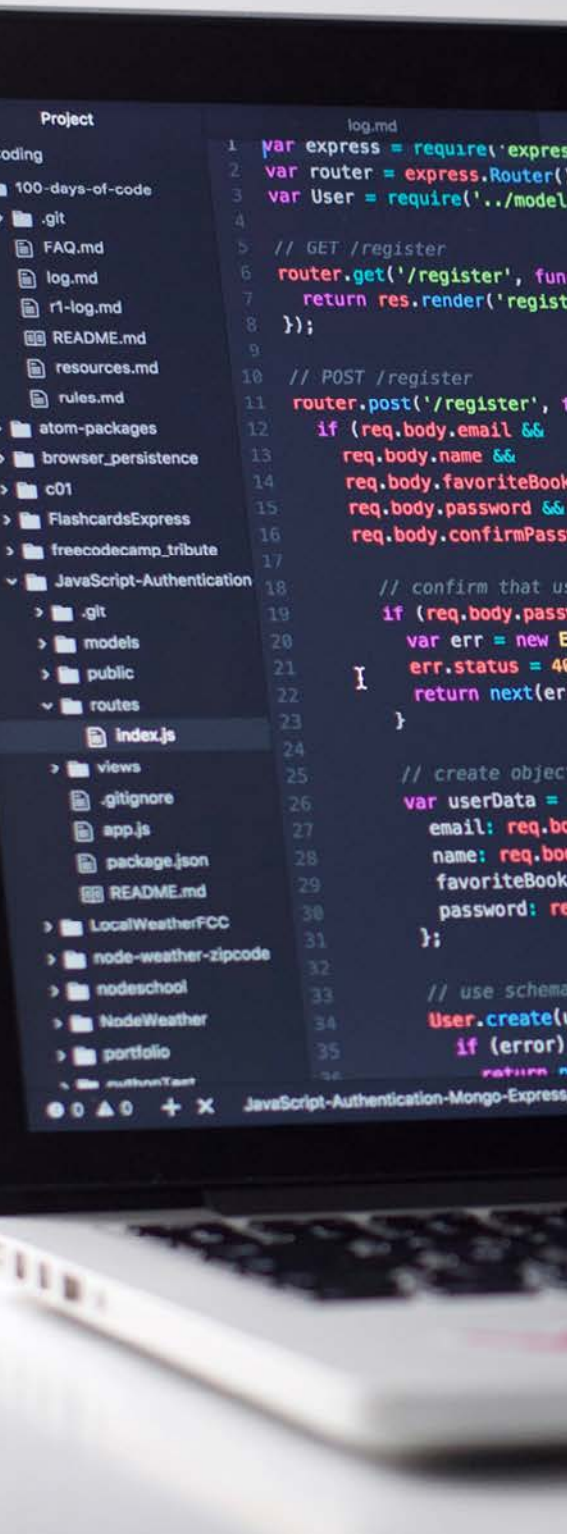
Firewalls are an important tool for blocking IP packets with spoofed addresses. All enterprise routers should be configured to reject packets with spoofed addresses. Some basic considerations include:

- Configuring routers and firewalls to reject packets with private IP addresses that originate from outside the enterprise perimeter.
- Block traffic that originates from inside the enterprise and spoofs an external address as the source IP address.



Conclusion

Spoofing takes advantage of a trust-based relationship. Spoofing can be prevented effectively if proper tactics are implemented. Learning about how and why these attacks are used, and implementing prevention, can help protect your network from these hidden hacking techniques.



Pseudo Code

1. Find IP Address of Computer Host.
2. Save the IP Address into Database.
3. Detect IP for Spoofed IP Address by comparing with the host IP address.
4. If Spoofed IP detected Then BLOCK User. Else go for Step 3 End If.
5. Apply Algorithm to compare data like Huffman, RLE (Run-Length Encoding).
6. Apply Encryption Algorithm.
7. Transition of data.
8. Apply Decryption Algorithm to data.
9. For Data Storage, apply decompression algorithm.
10. End.

References

Print Resources

- Hack Proofing Your Network (Ryan Russell)
- The Hacker's Handbook: The Strategy Behind Breaking into and
- Defending Networks(By Susan Young, Dave Aitel)

Online Resources

- http://www.securityfocus.com/infocus/1674
- http://www.iss.net/security_center/advice/Underground/Hacking/Meth
- ods/Technic al/Spoofing/default.htm
- http://www.linuxgazette.com/issue63/sharma.html
- https://en.wikipedia.org/wiki/IP_address_spoofing
- https://www.researchgate.net/publication/268585450_Efficient_Defens
- e_System_for_IP_Spoofing_in_Networks
- https://www.techtubby.com/spi-firewalls-how-it-works