Description

The purpose of spoofcheck is to let the server running spoofcheck to check the integrity of a client connection by looking for IP Address spoofing.

It performs this integrity check by using DNS to authenticate a client that has established a connection to the server. The spoofcheck implementation references the advertised IP Address against the client's official host name, aliases, and registered IP Address addresses.

A client must only establish a TCP connection with the spoofcheck server as no other protocol is used. After establishing a connection, the spoofcheck server checks if the client is spoofing the IP address or if it is an honest connection, then it immediately ends the connection.

Note that client connections are subject to be reported as spoofing if no DNS mapping exists for a client IPAddress, even if connections are actually authentic. For this reason, spoofcheck is not a sophisticated method of checking for actual IP Address spoofing.

The spoofcheck server will remain running until manually shut down. Multiple connections can be established through threaded operation on the supplied port number while the server is running.

Execution Output

client addr = 172.21.198.81 port = 39104

official hostname: uw1-320-01.uwb.edu

alias: none

ip address: 172.21.198.81 ... hit!

an honest client

client addr = 172.21.198.82 port = 36746

official hostname: uw1-320-02.uwb.edu

alias: none

ip address: 172.21.198.82 ... hit!

an honest client

client addr = 69.91.202.149 port number = 51434

official hostname: uw2-140-c0yb7y1.uwb.edu

alias: none

ip address: 69.91.202.149 ... hit!

an honest client

For both Linux computers and the Windows based machines, a DHCP obtained IP Address is used, and proper DNS forwarding was set up for those IP Addresses. The connections were successful using spoofcheck.

client addr = 10.102.54.225 port = 60583

gethostbyaddr error for the client( 10.102.54.225): 1

a spoofing client

client addr = 10.102.54.225 port = 60616

gethostbyaddr error for the client( 10.102.54.225): 1

a spoofing client

I do not have proper DNS forwarding set up on my laptop. My computer was connected to UW campus network through VPN. The first result was connecting directly through nc command on MAC terminal. The second result was using PuTTY in the virtual machine on my MAC. Both connections are categorized as spoofing connection. In conclusion, the computer and virtual machine are sharing the basic infrastructure including the networking service, which results in the same IP Address.

Discussions

1. To establish a connection, the client must simply initiate a TCP handshake with the listening spoofcheck server communicating on the same port number. Once connection has been established with the server, flow of control is left exclusively to the spoofcheck server. Server-initiated TCP disconnection occurs immediately after the spoofcheck server completes the verification process on the host-name-to-address mapping of the client. Since the spoofcheck server does not require or except the client to initiate disconnection, the connection is closed on the server end. This is important to ensure that connections are closed and do not end up simply timing out as a result of the client process being terminated.
2. Client verification while connecting through NAT may not work, depending on the network configuration. The most obvious failure is when DNS is not properly configured on the NAT WAN address. A pure NAT operating on IP Address alone may not correctly handle traffic where as soon as the protocol stack is traversed, basic protocols such as TCP and UDP can break unless NAT takes the proper action beyond the network layer, however devices operating behind a NAT are otherwise virtually indistinguishable from the other legitimate hosts.
3. Clients using DHCP obtained IP addresses are no more subject to errors in spoofcheck authentication than clients with statically assigned IP addresses. Due to the nature of how DHCP works, the DHCP server is typically closely tied to a DNS server, where proper forward DNS resolution is a requirement for spoofcheck to function properly. Therefore, the method that is used to obtain an IP Address is irrelevant so as long as the proper DNS records exist for spoofcheck to function. The actual process used to obtain the IP Address is transparent to TCP.