3. Command to get new MAC Address using command "net config rdr"

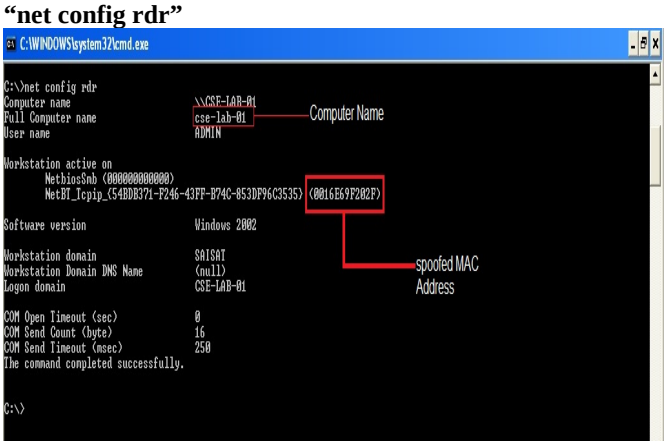

Figure 5.7

6. COUNTER MEASURES

There are certain countermeasures to reduce the above-mentioned vulnerable affects of MAC spoofing.Our OS is static but it should be dynamic so that it provide a utility that check after few second if any entry found in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}\0001 or 0005" with the name "network address" then the utility should delete it automatically [7],[8].

- Whenever ARP packets arrive it should not check the MAC address for the OS, it should retrieve it directly from LAN card or whenever ARP packets arrive it should compare the MAC address from OS to NIC and if it doesn't match it should delete the entry from OS or from registry[9].
- MAC address is stored in OS. Whenever MAC address is required it is retrieved from operating system. If we want to prevent MAC address to be spoofed then whenever we require MAC address we must retrieve it directly from NIC.
- You can lock your MAC address by introducing the router which support the MAC filtering and IP reservation. This is where you associate a DHCP IP address with a particular MAC address. By this way only that MAC gets associated with particular IP address.
- To prevent MAC spoofing you would need to encrypt the communication between the wireless PC and access point. Higher end AP's support IPSEC.

7. CONCLUSION

Spoofing is possible because the IEEE 802.11 standard does not provide per-frame source authentication, but in future it can be effectively prevented if a proper authentication is added into the standard. There is plan for such standard modification to support link-layer source authentication that covers both management and control frames. The key idea of this project is to leverage the sequence number field in the link-layer header of IEEE 802.11 frames without modifying STAs, APs, or the MAC protocol. If an intrusion detection system keeps track of the latest sequence number of each wireless node, to impersonate a node an attacker needs to spoof the source address as well as its corresponding sequence number. If the sequence number of a spoofed frame is equal to or smaller than the corresponding node's current sequence number, the spoofed frame is considered a retransmitted frame and thus has to have the same content as the authentic frame with the same sequence number. This means that the spoofed frame cannot possibly do any harm as it is just a duplicate.

MAC spoofing attacks in 802.3 networks exploit a fundamental vulnerability of the 802.3 protocols. The MAC addresses of the Ethernet LAN card can be easily forged, imposing a serious security challenge. With this we conclude that the dangerous security hole is in our OS. Our OS is static but if it will be dynamic it will resolve our many spoofed based problem. If a MAC is spoofed its entry is made in registry, a dynamic OS may have the utility to check its registry after few second if there is any entry with name network address then it should delete it therefore MAC cannot be spoofed.

REFERENCES

[1]. MACspoofing : http://en.wikipedia.org/wiki/
[2]. E.D Cardenas. MAC Spoofing An Introduction. http://www.giac.org/practical/GSEC/Edgar Cardenas GSEC.pdf
[3]. http://wn.com/Gerador_de_chaves_pre- defenidas_wpa2-psk_para_redes_d- link_da_sapo_por_MAC_address
[4]. J.Wright. Detecting Wireless LAN MAC Address Spoofing. http://home.jwu.edu/ jwright/papers/wlan-mac-spoof.pdf
[5]. Y. Liu, K. Dong, L. Dong, B. Li, Research of the ARP Spoofing Principle and a Defensive Algorithm, International Journal of Communications.
[6]. D.C. Plummer, An Ethernet Address Resolution Protocol, RFC-826, Network Working Group, November 1982
[7]. T. Pusateri, IP Multicast over Token-Ring Local Area Networks, RFC-1469, Network Working Group, June 1993
[8]. M.D.Spivey, Practical Hacking techniques and countermeasures
[9]. M.k.Choi1, R.J. Robles1, C.Hong, T.Kim1, Wireless Network Security: Vulnerabilities, Threats and Countermeasures, International journal of Multimedia and Ubiquitous Engineering, Vol.3, No. 3, July, 2008.