1. What are security attacks?

In [*computer*](https://en.wikipedia.org/wiki/Computer) and [*computer networks*](https://en.wikipedia.org/wiki/Computer_network) an **attack** is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset An attack can be *active* or *passive*.[[2]](https://en.wikipedia.org/wiki/Attack_(computing)#cite_note-rfc2828-2)

An "active attack" attempts to alter system resources or affect their operation.

A "[passive attack](https://en.wikipedia.org/wiki/Passive_attack)" attempts to learn or make use of information from the system but does not affect system resources. (E.g., [wiretapping](https://en.wikipedia.org/wiki/Telephone_tapping).)

An attack can be perpetrated by an *insider* or from *outside* the organization;[[2]](https://en.wikipedia.org/wiki/Attack_(computing)#cite_note-rfc2828-2)

An "inside attack" is an attack initiated by an entity inside the security perimeter (an "insider"), i.e., an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization.

An "outside attack" is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an "outsider"). In the Internet, potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

An attack usually is perpetrated by someone with bad intentions: [black hatted](https://en.wikipedia.org/wiki/Hacker_(computer_security)) attacks falls in this category, while other perform [penetration testing](https://en.wikipedia.org/wiki/Penetration_test) on an organization information system to find out if all foreseen controls are in place.

The attacks can be classified according to their origin: i.e. if it is conducted using one or more computers: in the last case is called a distributed attack. [Botnets](https://en.wikipedia.org/wiki/Botnet) are used to conduct distributed attacks.

Other classifications are according to the procedures used or the type of vulnerabilities exploited: attacks can be concentrated on network mechanisms or host features.

Some attacks are physical: i.e. theft or damage of computers and other equipment. Others are attempts to force changes in the logic used by computers or network protocols in order to achieve unforeseen (by the original designer) result but useful for the attacker. Software used to for logical attacks on computers is called [malware](https://en.wikipedia.org/wiki/Malware).

The following is a partial short list of attacks:

* Passive
  + Network
    - [Wiretapping](https://en.wikipedia.org/wiki/Telephone_tapping)
    - [Port scan](https://en.wikipedia.org/wiki/Port_scan)
    - [Idle scan](https://en.wikipedia.org/wiki/Idle_scan)
* Active
  + [Denial-of-service attack](https://en.wikipedia.org/wiki/Denial-of-service_attack)
  + [Spoofing](https://en.wikipedia.org/wiki/Spoofing_attack)
  + Network
    - [Man in the middle](https://en.wikipedia.org/wiki/Man-in-the-middle_attack)
    - [ARP poisoning](https://en.wikipedia.org/wiki/ARP_poisoning)
    - [Ping flood](https://en.wikipedia.org/wiki/Ping_flood)
    - [Ping of death](https://en.wikipedia.org/wiki/Ping_of_death)
    - [Smurf attack](https://en.wikipedia.org/wiki/Smurf_attack)
  + Host
    - [Buffer overflow](https://en.wikipedia.org/wiki/Buffer_overflow)
    - [Heap overflow](https://en.wikipedia.org/wiki/Heap_overflow)
    - [Stack overflow](https://en.wikipedia.org/wiki/Stack_overflow)
    - [Format string attack](https://en.wikipedia.org/wiki/Format_string_attack)

1. Explain ARP Spoofing and Poisoning Countermeasures

To avoid arp spoofing:

1)      Make sure your wireless router is [**configured to support WPA2-AES**](https://www.dbdr.com/how-to-protect-your-wireless-network/), and that you have a [**very strong password**](https://www.dbdr.com/how-to-strengthen-your-passwords/).

2)      Review the webpage[**“HOWTO : Protect you from being ARP spoofing”**](http://samiux.blogspot.com/2012/06/howto-protect-you-from-being-arp.html) for programs you can install that will help protect against ARP spoofing.

3)      If you’re connected to a public wireless network, don’t do any online banking, or make any online purchases.  The public network you are connecting to might be a hackers laptop.

4)      At your office, refer your network administrators to this page.  They probably already know all this (and more), but it will serve as a gentle reminder that protection doesn’t do you any good if you don’t turn it on.

An open source solution for anti ARP spoofing is ArpON "Arp handler inspectiON". It is a portable ARP handler which detects and blocks all Man In The Middle attacks through ARP poisoning and spoofing attacks with a static ARP inspection (SARPI) and dynamic ARP inspection (DARPI) approach on switched or hubbed LANs with or without DHCP. This requires an agent on every host that is to be protected.  
  
Another method to anti ARP spoofing, DHCP snooping, can be used on larger networks, but is limited to DHCP clients, and as such, can be easily circumvented.[clarification needed] The DHCP service on the network device keeps a record of the MAC addresses that are connected to each port, so it can possibly detect if a spoofed ARP has been received. This method is implemented on networking equipment by vendors such as Cisco, ProCurve, Extreme Networks, Dlink and Allied Telesis.  
  
Detection is another avenue of anti ARP spoofing. Given the separation of duties requirement in regulated industry, the ARPDefender appliance is widely used in financial institutions. Arpwatch is a Unix program which listens for ARP replies on a network, and sends a notification via email when an ARP entry changes. detection like: preventing locally static entries to be overwritten, detecting changes in the local mapping, checking integrity of ARP packets. Furthermore, the use of active network ARP discovery enables the validation of local network consistency as well as the detection of attackers. XArp run as protection version under Linux and can prevent attacks. Furthermore, XArp can e.g. send detected attack alerts by email. anti-arpspoof creates static ARP entries in the client and default gateway cache, and cleans poisoned dynamic entries. A simple **anti ARP spoofing** method that only works for simple ARP spoofing attacks is the use of static IP-MAC mappings. However, this only prevents simple attacks and does not scale on a large network, since the mapping has to be set for each pair of machines resulting in (n\*n) ARP caches that have to be configured.