MODULES

1. **Man in the Middle (MITM)**

**Level: Advanced  
Definition -** What does *Man-in-the-Middle Attack (MITM)* mean?

A man-in-the-middle (MITM) attack is a form of eavesdropping where communication between two users is monitored and modified by an unauthorized party. Generally, the attacker actively eavesdrops by intercepting a public key message exchange and retransmits the message while replacing the requested key with his own.   
In the process, the two original parties appear to communicate normally. The message sender does not recognize that the receiver is an unknown attacker trying to access or modify the message before retransmitting to the receiver. Thus, the attacker controls the entire communication.  
This term is also known as a janus attack or a fire brigade attack.

*Sources:* <http://www.techopedia.com/definition/4018/man-in-the-middle-attack-mitm>

*Examples:* <http://www.youtube.com/watch?v=-hd7XG-b6uk><http://www.youtube.com/watch?v=CVnOt0qJTa8&NR=1&feature=fvwp>

1. **DNS Spoofing**

**Level: Advanced**

**Definition:** DNS Spoofing is an attack method that is used by crackers to re-direct a request for a specific Internet site to another computer by means of fooling or hi-jacking the Domain Name Service session. A malicious user is able to “convince” your computer that the attacker’s site is to be trusted and in fact is the site you requested. A cracker would be capable of gaining access to all of the information from the trusted site. The Domain Name Service uses the UDP protocol, which, unfortunately, fails to provide for authentication services. Without authentication identities can't be verified.

**Its Relevance:** A Domain Name Service exploit can be particularly harmful and measures must be taken to avoid falling victim to such an attack. Infrastructure owners could avoid name service hijacking by encrypting traffic. By default a robust form of “authentication” (knowing the key) is put into place.

*Sources:* <http://www.computer-security-glossary.org/dns_spoofing.html>

*Examples:* [*http://www.youtube.com/watch?v=ZwfUFlpTUdc*](http://www.youtube.com/watch?v=ZwfUFlpTUdc)

<http://www.youtube.com/watch?v=vRuFB4ffxS0>

[*http://www.youtube.com/watch?v=Aak6-B3JORE*](http://www.youtube.com/watch?v=Aak6-B3JORE)

<http://www.youtube.com/watch?v=0hfYbQ90rZY>

1. **ARP Poisoning**

**Level: Advanced**

**Definition**: ARP spoofing[[1]](http://en.wikipedia.org/wiki/ARP_spoofing#cite_note-1) is a technique whereby an attacker sends fake ("[spoofed](http://en.wikipedia.org/wiki/Spoofing_attack)") [Address Resolution Protocol (ARP)](http://en.wikipedia.org/wiki/Address_Resolution_Protocol) messages onto a [Local Area Network](http://en.wikipedia.org/wiki/Local_Area_Network). Generally, the aim is to associate the attacker's [MAC address](http://en.wikipedia.org/wiki/MAC_address) with the [IP address](http://en.wikipedia.org/wiki/IP_address) of another [host](http://en.wikipedia.org/wiki/Host_(network))(such as the [default gateway](http://en.wikipedia.org/wiki/Default_gateway)), causing any traffic meant for that IP address to be sent to the attacker instead.

ARP spoofing may allow an attacker to intercept [data frames](http://en.wikipedia.org/wiki/Data_frame) on a LAN, modify the traffic, or stop the traffic altogether. Often the attack is used as an opening for other attacks, such as [denial of service](http://en.wikipedia.org/wiki/Denial_of_service), [man in the middle](http://en.wikipedia.org/wiki/Man-in-the-middle_attack), or [session hijacking](http://en.wikipedia.org/wiki/Session_hijacking)attacks.[[2]](http://en.wikipedia.org/wiki/ARP_spoofing#cite_note-Ramachandran-2005-p239-2)

The attack can only be used on networks that make use of the [Address Resolution Protocol](http://en.wikipedia.org/wiki/Address_Resolution_Protocol) (ARP), and is limited to local network segments.[[3]](http://en.wikipedia.org/wiki/ARP_spoofing#cite_note-Lockhart-2007-p184-3)

*Sources:* <http://en.wikipedia.org/wiki/ARP_spoofing>

*Examples* <http://www.youtube.com/watch?v=Yd9_HzfN-aQ>

<http://www.youtube.com/watch?v=VjlQny3LNlA>

1. **Buffer Overflow**

**Level: Beginner**

**Definition:** The condition wherein the data transferred to a [buffer](http://www.webopedia.com/TERM/B/buffer.html) exceeds the storage capacity of the buffer and some of the data "overflows" into another buffer, one that the data was not intended to go into. Since buffers can only hold a specific amount of data, when that capacity has been reached the data has to flow somewhere else, typically into another buffer, which can corrupt data that is already contained in that buffer.

Malicious [hackers](http://www.webopedia.com/TERM/H/hack.html) can launch buffer overflow attacks wherein data with instructions to corrupt a system are purposely written into a file in full knowledge that the data will overflow a buffer and release the instructions into the computers instructions.

*Sources:* [*http://www.webopedia.com/TERM/B/buffer\_overflow.html*](http://www.webopedia.com/TERM/B/buffer_overflow.html)

*Examples:* <http://www.youtube.com/watch?v=U0DISuWHXCw>

<http://www.youtube.com/watch?v=MI8UTpbk1HQ>

1. Sniffing Password

**Level: Beginner**

1. Port Scanning

Level: Beginner

1. Msql Injection

Level: Beginner

Other Attacks you may can consider

**Physical Access – Beginner**

**MAC Spoofing – Beginner**

**Rogue Access Points – Advanced**

**Password Cracking – Beginner**

**Cross Scripting Attack - Advanced**

**Resources for list of other attacks**

http://searchsecurity.techtarget.com/feature/A-list-of-wireless-network-attacks