**Ettercap**

Ettercap is an open-source tool that can be used to support man-in-the-middle attacks on networks. Ettercap can capture packets and then write them back onto the network. Ettercap enables the diversion and alteration of data virtually in real-time. Ettercap can also be used for the protocol analysis necessary to analyze network traffic.

Ettercap has a nice Graphical User Interface (UI) as well as a command line interface. While Ettercap can support network traffic analysis, the most frequent use of Ettercap is to set up man-in-the-middle attacks using ARP poisoning. Penetration testing you can emulate includes man-in-the-middle attacks, credentials capture, dns spoofing, and DoS attack.

Ettercap also supports both active and passive deep analysis of many protocols and includes many features for network and host analysis. Many “sniffing” modes are available – this includes MAC based, IP based, ARP based (full duplex), and PublicARP based (half duplex). Ettercap can also detect a switched local area network (LAN) and use the OS fingerprints to determine the total geometry of the LAN.

Ettercap is a necessary part of the tool inventory for any penetration tester or ethical hacker.

**Man-in-the-middle Attacks**

Man-in-the-middle attacks place a threat actor in the middle of secure communications traffic. The primary purpose of a man-in-the-middle attack is to steal data. If authentication data, then the man-in-the-middle can access resources used by the target. Many times there is little to no interaction other than for the interception of data.

There are two approaches to using Ettercap for man-in-the-middle attacks. These are ARP poisoning (Address Resolution Protocol) attacks and Domain Name System (DNS) attacks. In an ARP attack Ettercap is configured to “impersonate” the IP address of your router. The goal is to get the targeted computer to believe the threat actor’s computer is the router. The MAC address of the attacker is linked to the IP address of the router. Once this is in place the threat actor will receive all of the data from the targeted machine which is going to the router. All of this data which originates in HTTPS is accessible as regular HTTP communications.

DNS spoofing requires that the ARP poisoning utilities are running within Ettercap. Once this is set up you can specify the domain names in the format A which diverts all traffic from the targeted victim’s computer to the instead to the IP address. The interception provided by Ettercap’s ARP poisoning has to be operating on the local network for this attack to work.

**DoS Attacks**

Once the ARP poisoning is in place, you can add the available service for dos\_attack. Click on Plugins in the top Ettercap menu and select manage the plugins from the list. This will display available services. Scroll down the list to find the entry for dos\_attack plugin. This is usually the following line after the dns\_spoof entry. Double click on the dos\_attack line to activate the attack.

**Authentication Theft**

Once you have activated ARP poisoning, you can intercept packets and the data they contain. Ettercap also allows configurability to shut down the use of HTTPS.

**Supported Operating Systems**

Ettercap can be used with many different operating systems but Ettercap works best on most versions of Linux. Many penetration testers and security analysts favor Kali Linux as the preferred distribution.

Ettercap is available with Linux and Unix-variant operating systems such as:

* RHEL
* CentOS
* OpenSuSe
* Ubuntu
* Kali
* Debian
* BackTrack
* Mint
* Fedora
* Gentoo
* Pentoo
* FreeBSD
* OpenBSD
* NetBSD
* Solaris