

Session Hijacking

Subtask 1

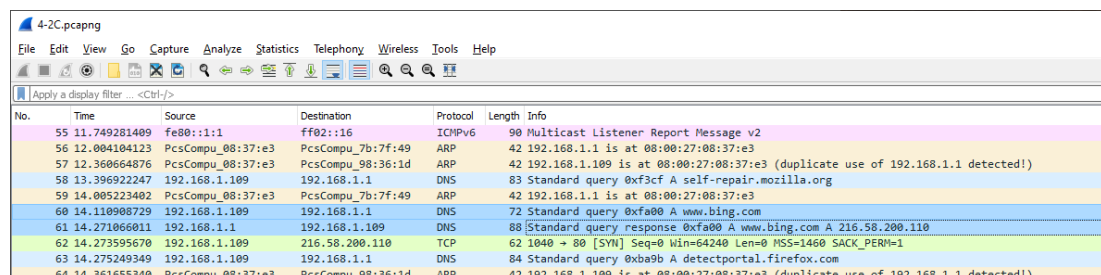
Instead of using ettercap to hijack the DNS session use dnsspoof. Capture the packets between your victim. Does this program work as well as ettercap? You should submit the following.

1. Submit a short explanation of why or why not the program works as well as ettercap, referencing the packet capture to describe any problems.

Submit a short explanation of why or why not the program works as well as ettercap, referencing the packet capture to describe any problems.

Running a DNS hijacking session using dnsspoof is definitely a longer process than using Ettercap, creating the hosts file, starting the ARP spoofing then starting the dnsspoof. This process took about twice as long as using Ettercap.

However I cannot be sure it was working successfully, the Kali machine did show the DNS packets being intercepted and spoofed packet being sent, the XP machine even showed the spoofed IP address when I pinged 'bing.com' however I could not get anything from Firefox other than an unable to connect error. This is probably a configuration error on my part.



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-------------------|-------------------|----------|--------|--|
| 55 | 11.749281409 | fe80::1:1 | ff02::16 | ICMPv6 | 90 | Multicast Listener Report Message v2 |
| 56 | 12.004104123 | PcsCompu_08:37:e3 | PcsCompu_7b:7f:49 | ARP | 42 | 192.168.1.1 is at 08:00:27:08:37:e3 |
| 57 | 12.360664876 | PcsCompu_08:37:e3 | PcsCompu_98:36:1d | ARP | 42 | 192.168.1.109 is at 08:00:27:08:37:e3 (duplicate use of 192.168.1.1 detected!) |
| 58 | 13.396922247 | 192.168.1.109 | 192.168.1.1 | DNS | 83 | Standard query 0xf3cf A self-repair.mozilla.org |
| 59 | 14.005223402 | PcsCompu_08:37:e3 | PcsCompu_7b:7f:49 | ARP | 42 | 192.168.1.1 is at 08:00:27:08:37:e3 |
| 60 | 14.110908729 | 192.168.1.109 | 192.168.1.1 | DNS | 72 | Standard query 0xfa00 A www.bing.com |
| 61 | 14.271066011 | 192.168.1.1 | 192.168.1.109 | DNS | 88 | Standard query response 0xfa00 A www.bing.com A 216.58.200.110 |
| 62 | 14.273595670 | 192.168.1.109 | 216.58.200.110 | TCP | 62 | 1040 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 |
| 63 | 14.275249349 | 192.168.1.109 | 192.168.1.1 | DNS | 84 | Standard query 0xba9b A detectportal.firefox.com |
| 64 | 14.361655340 | PcsCompu_08:37:e3 | PcsCompu_98:36:1d | ARP | 42 | 192.168.1.109 is at 08:00:27:08:37:e3 (duplicate use of 192.168.1.1 detected!) |