**“Tools utilized in conducting pentesting”**

*Table of Contents*

*Introduction…………………………………….……………………………(1)*

*Nmap…………………………………….…………………………………..(1-2)*

*Aircrack…………………………………….……………………………….(2-3)*

*Tcpdump…………………………………….………………………………(4)*

*W3af…………………………………….…………………………………..(5-6)*

*Hping…………………………………….………………………………….(7-8)*

Daniel Rao

Feb 22nd, 2021

Vince Skinner

**Tools utilized in pentesting**

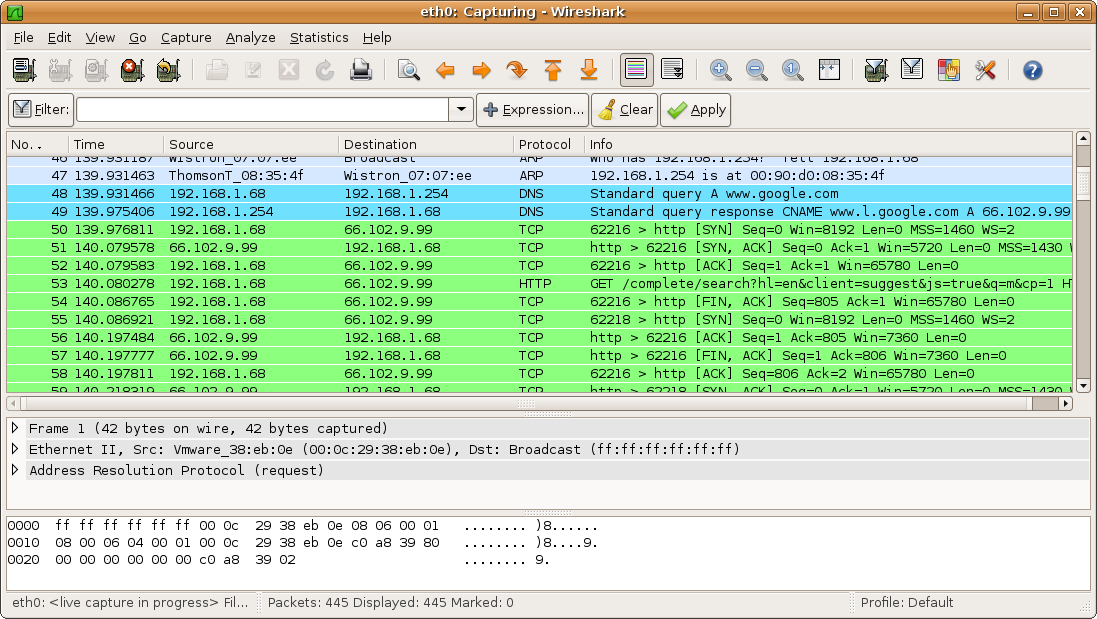
**Introduction**

As a security professional we need to know both hackers and pentesters use computer programming. Having a basic understanding in programming can also help us to develop a custom Security tool by modifying existing tools then we are conducting security tests. Most security tester positions require being able to create customized security tools. It's very similar to a carpenter being able to modify a tool to fit the job required according to his needs. C programming, Pearl, C++ are some of the more popular languages from which tools are built. Some other scripting languages include python and Ruby are also gaining a lot of popularity amongst security Professionals and pentesters. Some of the famous tools are as follows:

**Nmap:**

Map is a very popular tool among Security Professionals and pentesters that has been developed mainly in Lua, C and C++ programming languages. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer ([Zenmap](https://nmap.org/zenmap/)).

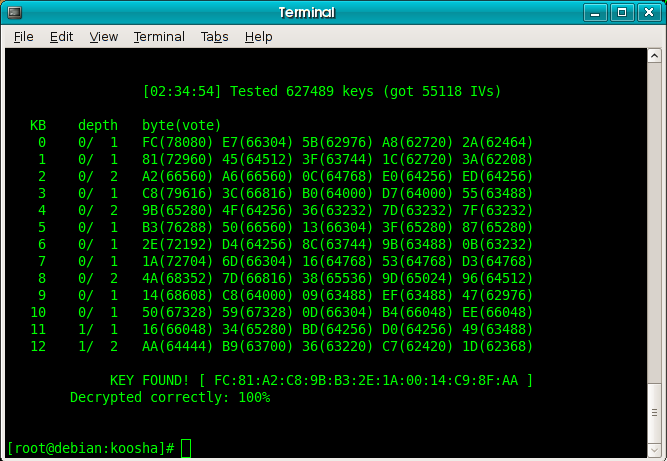
**Source:** <https://github.com/nmap/nmap>



**Aircrack:**

Aircrack is a suite of tools for 802.11a/b/g WEP and WPA cracking. It implements the best known cracking algorithms to recover wireless keys once enough encrypted packets have been gathered. . The suite comprises over a dozen discrete tools, including airodump (an 802.11 packet capture program), aireplay (an 802.11 packet injection program), aircrack (static WEP and WPA-PSK cracking), and airdecap (decrypts WEP/WPA capture files). Aircrack has been developed primarily in C.

**Source:** <https://github.com/aircrack-ng/aircrack-ng>



**Tcpdump:**

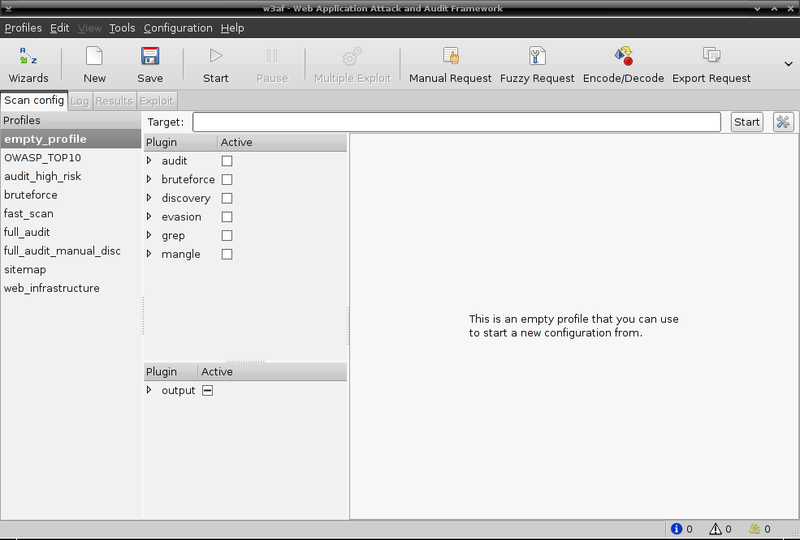
tcpdump has been mainly developed in the C programming language. It is the network sniffer we all used before Wireshark came into existence, and many of the pentesters continue to use it frequently. It may not have the bells and whistles (such as a pretty GUI and parsing logic for hundreds of application protocols) that Wireshark has, but it does the job well and with less security risk. It also requires fewer system resources. Tcpdump is actively maintained to fix bugs and portability problems. It is great for tracking down network problems or monitoring activity. There is a separate Windows port named WinDump.

**Source:** <https://github.com/the-tcpdump-group/tcpdump>

**W3af:**

W3af is an extremely popular, powerful, and flexible framework for finding and exploiting web application vulnerabilities. It is easy to use and extend and features dozens of web assessment and exploitation plugins. In some ways it is web-focused. It has been developed in Python language.

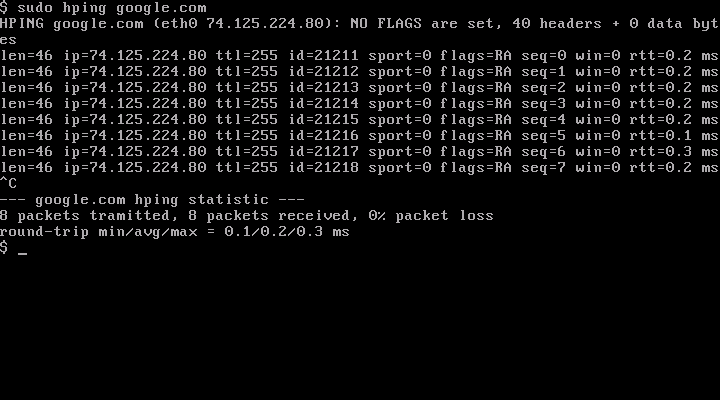
**Source:** <https://github.com/andresriancho/w3af>



**Hping:**

Hping is another tool developed in C. This handy little utility assembles and sends custom ICMP, UDP, or TCP packets and then displays any replies. It was inspired by the ping command, but offers far more control over the probes sent. It also has a handy traceroute mode and supports IP fragmentation. Hping is particularly useful when trying to traceroute/ping/probe hosts behind a firewall that blocks attempts using the standard utilities. This often allows you to map out firewall rule sets. It is also great for learning more about TCP/IP and experimenting with IP protocols.

**Source:** <https://github.com/antirez/hping>



**Citations:**

[**https://nmap.org/**](https://nmap.org/)