Security Research ToolsSeptember 27, 2017

15 Essential Open Source Security Tools for Blue Teams

There are thousands of open source security tools with both defensive and offensive security capabilities.

The following are ~~10~~ **15*** essential security tools that will help you to secure your systems and networks. These open source security tools have been given the essential rating due to the fact that they are effective, well supported and easy to start getting value from.

Nmap

Nmap - map your network and ports with the number one port scanning tool. Nmap now features powerful NSE scripts that can detect vulnerabilities, misconfiguration and security related information around network services. After you have nmap installed be sure to look at the features of the included ncat - its netcat on steroids.
Check out our NMAP Cheat Sheet

OpenVAS

OpenVAS - open source vulnerability scanning suite that grew from a fork of the Nessus engine when it went commercial. Manage all aspects of a security vulnerability management system from web based dashboards. For a fast and easy external scan with OpenVAS try our online OpenVAS scanner.
Check out our Install OpenVAS on Kali and OpenVAS Tutorial and tips

OSSEC

OSSEC - host based intrusion detection system or HIDS, easy to setup and configure. OSSEC has far reaching benefits for both security and operations staff.
Check out our OSSEC Intro and Installation Guide

Security Onion

Security Onion - a network security monitoring distribution that can replace expensive commercial grey boxes with blinking lights. Security Onion is easy to setup and configure. With minimal effort you will start to detect security related events on your network. Detect everything from brute force scanning kids to those nasty APT's.

Metasploit Framework

Metasploit Framework - test all aspects of your security with an offensive focus. Primarily a penetration testing tool, Metasploit has modules that not only include exploits but also scanning and auditing.

OpenSSH

OpenSSH - secure all your traffic between two points by tunnelling insecure protocols through an SSH tunnel. Includes scp providing easy access to copy files securely. Can be used as poor mans VPN for Open Wireless Access points (airports, coffee shops). Tunnel back through your home computer and the traffic is then secured in transit. Access internal network services through SSH tunnels using only one point of access. From Windows, you will probably want to have putty as a client and winscp for copying files. Under Linux just use the command line ssh and scp.
Check out our SSH Examples Tips & Tunnels

Wireshark

Wireshark - view traffic in as much detail as you want. Use Wireshark to follow network streams and find problems. Tcpdump and Tshark are command line alternatives. Wireshark runs on Windows, Linux, FreeBSD or OSX based systems.
Check out our Wireshark Tutorial and cheatsheet and tshark tutorial and filter examples.

Kali Linux

Kali Linux - was built from the foundation of BackTrack Linux. Kali is a security testing Linux distribution based on Debian. It comes prepackaged with hundreds of powerful security testing tools. From Airodump-ng with wireless injection drivers to Metasploit this bundle saves security testers a great deal of time configuring tools.

Nikto

Nikto - a web server testing tool that has been kicking around for over 10 years. Nikto is great for firing at a web server to find known vulnerable scripts, configuration mistakes and related security problems. It won't find your XSS and SQL web application bugs, but it does find many things that other tools miss.
Check out our install and tutorial

Trucecrypt

Trucecrypt - As of 2014, the TrueCrypt product is no longer being maintained. Two new security tools, CipherShed and VeraCrypt were forked and have been through extensive security audits.

Updated 2017 to include another 5 high quality open source security tools. These additional projects are all very much focused on the defenders side. With in depth traffic analysis, intrusion detection and incident response all covered. Interesting to see sponsors of these projects include Facebook, Cisco and Google.

Arkime Full Packet Capture (formerly Moloch)

Arkime - is packet capture analysis ninja style. Powered by an elastic search backend this makes searching through pcaps fast. Has great support for protocol decoding and display of captured data. With a security focus this is an essential tool for anyone interested in traffic analysis.

ZEEK formerly Bro IDS

ZEEK - totes itself as more than an Intrusion Detection System, and it is hard to argue with this statement. The IDS component is powerful, but rather than focusing on signatures as seen in traditional IDS systems. This tool decodes protocols and looks for anomalies within the traffic.
Check out our Bro-IDS install and tutorial

Snort

Snort - is a real time traffic analysis and packet logging tool. It can be thought of as a traditional IDS, with detection performed by matching signatures. The project is now managed by Cisco who use the technology in its range of SourceFire appliances. An alternative project is the Suricata system that is a fork of the original Snort source.
Check out our Suricata install and tutorial

OSQuery

OSQuery - monitors a host for changes and is built to be performant from the ground up. This project is cross platform and was started by the Facebook Security Team. It is a powerful agent that can be run on all your systems (Windows, Linux or OSX) providing detailed visibility into anomalies and security related events.

GRR - Google Rapid Response

GRR - Google Rapid Response - a tool developed by Google for security incident response. This python agent / server combination allows incident response to be performed against a target system remotely.

* **Updated in 2017 to include an additional 5 essential security tools.**