2020

# Security Tools

OPEN SOURCE

DILLIP A. THAKUR

CYBER ADVISERS INC.

# Contents

## Maltego

Originally developed by Paterva, Maltego is a forensics and open-source intelligence (OSINT) app designed to deliver a clear threat picture for the user's environment. It will demonstrate the complexity and severity of single points of failure as well as trust relationships that exist within the scope of one's infrastructure. It pulls in information posted all over the Internet, whether it's the current configuration of a router on the edge of the company network or the current whereabouts of your company's vice president. The commercial license does have a price tag, but the community edition is free with some restrictions.

## OWASP Zed Attack Proxy (ZAP)

The Zed Attack Proxy (ZAP) is a user-friendly penetration testing tool that finds vulnerabilities in web apps. It provides automated scanners and a set of tools for those who wish to find vulnerabilities manually. It's designed to be used by practitioners with a wide range of security experience, and is ideal for functional testers who are new to pen testing, or for developers: There’s even an official ZAP plugin for the Jenkins continuous integration and delivery application.

## Samurai Web Testing Framework

The Samurai Web Testing Framework is a virtual machine packed with some of the other items you'll see in this slideshow, and functions as a web pen-testing environment. You can download a ZIP file containing a VMware image with a host of free and open source tools to test and attack websites. Tools include the Fierce domain scanner and Maltego. For mapping it uses WebScarab and ratproxy. Discovery tools include w3af and burp. For exploitation, the final stage, it includes AJAXShell, the browser exploitation framework BeEF and others. There’s a trade-off for all this convenience, though: The developers’ mailing list has been dormant for the last couple years, and the latest SamuraiWTF release, 3.3.2, was packaged in 2016 so many of the tools it contains are outdated versions.

## Kali Linux

Kali Linux is the Linux-based pen-testing distribution previously known as BackTrack. Security professionals use it to perform assessments in a purely native environment dedicated to hacking. Users have easy access to a variety of tools ranging from port scanners to password crackers. You can download ISOs of Kali to install on 32-bit or 64-bit x86 systems, or on ARM processors. It’s also available as a VM image for VMware or Hyper-V. Kali’s tools are grouped into the following categories: information gathering; vulnerability analysis; wireless attacks; web applications, exploitation tools, stress testing, forensics, sniffing and spoofing, password attacks, maintaining access, reverse engineering, reporting, and hardware hacking.

## Fierce Domain Scan

Another venerable tool, Fierce Domain Scan was last updated by developer Robert Hansen (RSnake) back in 2007. As he described on his ha.ckers blog, it "was born out of personal frustration after performing a web application security audit. Fierce pinpoints likely targets inside and outside a corporate network by looking at DNS entries. It is essentially a reconnaissance tool, a Perl script built to scan domains within minutes, using a variety of tactics. Although Hansen has shut down his blog, Fierce lives on in this Github repository. Because the underlying principles of DNS haven’t changed in the last decade, Fierce still works.

## The Harvester

The Harvester is an OSINT tool used to obtain subdomain names, email addresses and usernames relating to a domain, drawing on public sources such as Google and LinkedIn. A favorite among pen testers, it lets the user conduct passive reconnaissance and build target profiles that include a list of usernames and email addresses -- or research the exposure of their own domain.

## Hping

Hping is a command-line tool that can be used to assemble and analyze custom TCP/IP packets. It can be used for firewall testing, port scanning, network testing using different protocols, OS fingerprinting and as an advanced traceroute. It runs on Linux, FreeBSD, NetBSD, OpenBSD, Solaris, MacOs X, and Windows. It hasn't been updated in years but then, neither has TCP/IP.

## John the Ripper

John the Ripper is a password cracker available for many flavors of Unix, Windows, DOS, BeOS, and OpenVMS — although you'll likely have to compile the free version yourself. It's mainly used to detect weak Unix passwords. Besides several crypt(3) password hash types most commonly found on various Unix systems, supported out of the box are Windows LM hashes, plus lots of other hashes and ciphers in the community-enhanced version. An enhanced community version includes support for GPUs to accelerate the search.

## Nessus

Nessus is one of the world's most popular vulnerability and configuration assessment tools. It started life as an open-source project, but developer Tenable switched to a proprietary license way back in version 3. As of October 2020, it's up to version 8.12.1. Despite that, Nessus is still free for personal use on home networks, where it will scan up to 16 IP addresses. A commercial version will allow you to scan an unlimited number of IP addresses. According to the Tenable website, Nessus features high-speed discovery, configuration auditing, asset profiling, sensitive data discovery, patch management integration and vulnerability analysis.

## NMap

Nmap is an open-source tool for network exploration and security auditing, and its developers are still updating it, over 20 years after its launch. It's built to rapidly scan large networks, though it also works against single hosts. According to the NMap website, the scanner uses raw IP packets to determine what hosts are available on the network, which services those hosts are offering, what operating systems they are running, what types of packet filters/firewalls are in use, and dozens of other characteristics. It's not just for security audits: it can also be used for network inventory, managing service upgrade schedules or -- if you believe its appearances in various Hollywood films -- for hacking brains and tracking superheroes. A versatile tool indeed.

## OpenVPN

OpenVPN is an open-source SSL VPN tool that works in a wide range of configurations, including remote access, site-to-site VPNs, Wi-Fi security, and enterprise-scale remote access solutions. It offers load balancing, failover, and fine-grained access controls. A packaged installer is available for Windows machines, and the code can also run on OpenBSD, FreeBSD, NetBSD, Mac OS X, and Solaris.

## Ophcrack

Ophcrack is a free tool for cracking Windows passwords using rainbow tables. It runs on multiple platforms and has a graphical user interface showing real-time graphs to analyze the passwords. It can crack passwords using LM (Windows XP) and NTLM (Vista, 7) hashes using the free rainbow tables available on the site. It also has a brute-force module for simple password and can even dump and load hashes from an encrypted Security Account Manager (SAM) recovered from a Windows partition.

## OWASP Python Security Project

The OWASP Python Security Project set out to create a hardened version of Python allowing developers to build applications for use in high-risk environments and ended up building the largest collection of information about security in the Python programming language. The team focused on two areas: the functional and structural analysis of python applications and open-source code, and on a black-box analysis of the Python interpreter. The project website has a wiki listing all the security concerns they identified.

## Wireshark

Wireshark is a network protocol analyzer that lets users capture and interactively browse traffic running on a computer network. In its more than 20-year development history, it has acquired a long list of features including live capture and offline analysis, and deep inspection of hundreds of protocols, with more being added all the time. It is multi-platform, running on Windows, Linux, OS X, Solaris, FreeBSD, NetBSD and others. Among its more esoteric features it can analyse VOIP traffic; decrypt SSL/TLS, WEP and WPA/WPA2 traffic, and read traffic carried over USB, Bluetooth and even Frame Relay (remember that?)

## ModSecurity

ModSecurity is a web application monitoring, logging and access control toolkit developed by Trustwave's SpiderLabs Team. It can perform full HTTP transaction logging, capturing complete requests and responses; conduct continuous security assessments; and harden web applications. You can embed it in your Apache 2.x installation or deploy it as a reverse proxy to protect any web server.

## Burp Suite

Burp Suite is a web app security testing platform. Its various tools support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities. Tools within the suite include a proxy server, web spider, intruder and a so-called repeater, with which requests can be automated. Portswigger offers a free edition that’s lacking the web vulnerability scanner and some of the advanced manual tools.

## Metasploit

HD Moore created the Metasploit Project in 2003 to provide the security community with a public resource for exploit development. This project resulted in the Metasploit Framework, an open source platform for writing security tools and exploits. In 2009, Rapid7, a vulnerability management solution company, acquired the Metasploit Project. Prior to the acquisition, all development of the framework occurred in the developer's spare time, eating up most weekends and nights. Rapid7 agreed to fund a full-time development team and keep the source code under the three-clause BSD license that is still in use today.

## Aircrack-ng

What Wireshark does for Ethernet, Aircrack-ng does for Wi-Fi. In fact, it's a complete suite of tools for monitoring packets, testing hardware, cracking passwords and launching attacks on Wi-Fi networks. Version 1.2, released in April 2018, brings big improvements in speed and security and extends the range of hardware Aircrack-ng can work with.

## TAILS

The Amnesiac Incognito Live System (TAILS for short) is a live Linux operating system that you can run from a DVD or USB stick. It's amnesiac because it doesn't keep track of your activities from one session to the next, and incognito because it uses Tor for all internet communications. It's possible to reveal your identity to someone monitoring your Tor connection if you log in to, say, your social networking account, but if you don't do anything stupid like that, TAILS can go a long way to keeping your online activity secret.

## Qubes OS

Qubes OS modestly describes itself as "a reasonably secure operating system." It uses the Xen hypervisor to compartmentalize functions in different virtual machines or "qubes". This allows different activities to be isolated in different qubes. How far you go with this is up to you. If you're only slightly worried, you might perform your internet banking in one qube, and all your other online activities in another. If you're really concerned, you might create a new, disposable qube for every email attachment you open, providing some level of assurance that a malicious attachment can't take over your whole machine. It's a free download, but you'll need a 64-bit Intel or AMD machine with 4GB of RAM and 32GB of disk space.

## Signal

Signal is a messaging and voice-and-video-calling app offering end-to-end encryption: That means that even its developers can't intercept or decrypt your conversations. It's free for use on Android, iOS or desktop machines running macOS, Linux or Windows. It offers functions such as disappearing messages (that vanish a sender-selectable time after they are read), encrypted group chats, and picture messaging. The Electronic Frontier Foundation suggests using Signal as part of its "Surveillance Self Defense" guide.