7 Great open source security apps you may not know yet

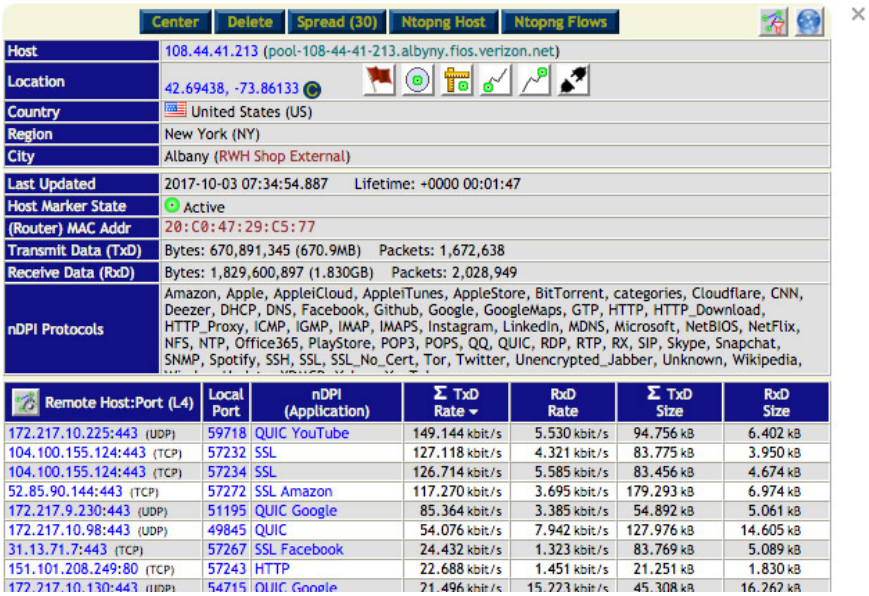
To protect you from increasing online threats, you need to use a variety of security applications. For an ordinary home user, it can be as simple as an antivirus software suite and an anti-malware tool.

Security issues continue to generate bad news at an alarming rate. It seems that most companies have been affected by this problem. Data leakage, hacked accounts, and basic security vulnerabilities are common concerns.

To protect you from increasing online threats, you need to use a variety of security applications. For an ordinary home user, it can be as simple as an antivirus software suite and an anti-malware tool. When your network is configured more complex, you also need more sophisticated security applications.

In this article, we will look at some of the best open source security applications available. We will introduce you to a variety of tools that can perform many different functions.

1. Network Security Toolkit



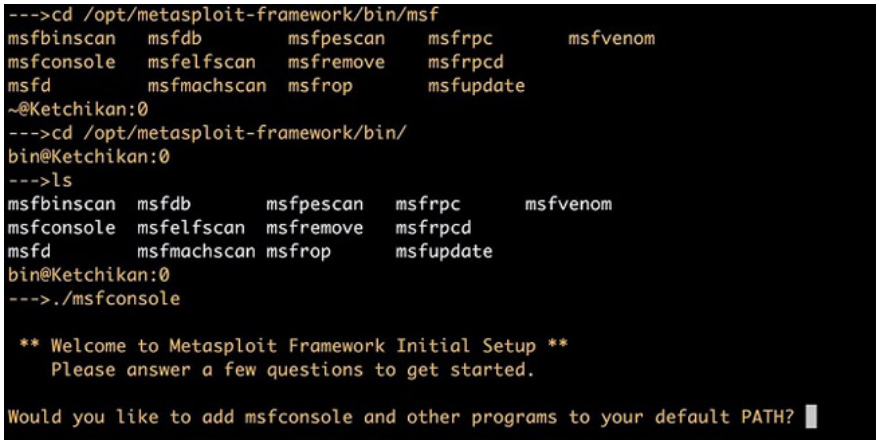
Network Security Toolkit is a bootable ISO file and can be loaded with a CD or USB disk. It is based on Linux Fedora distro, but will work on most x86 and x64 systems.

The download contains more than 100 open source security applications aimed at users who are network administrators. It includes tools for traffic management, intrusion monitoring, vulnerability testing and more.

Although theoretically, you can install all individual applications, Network Security Toolkit provides a unique Web Interface that you can use to configure many applications in a larger toolkit. .

Link reference: http://www.networksecuritytoolkit.org/nst/index.html

2. Metasploit Framework



Metasploit Framework is a small project in the big project Metasploit.

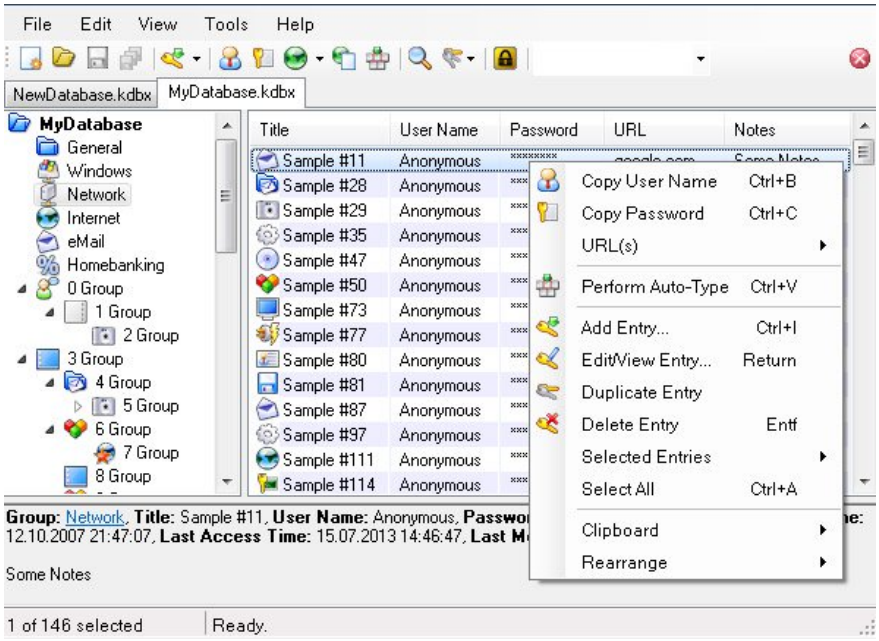
This application is an penetration testing framework. Formulated from a partnership between open source developers and software company Rapid7, the software has become one of the most used penetration testing applications in the world.

Metasploit Framework includes 900 known bugs for Windows, macOS and Linux operating systems. You can load the code you want to check, then set it to check whether the operating system is vulnerable. You can also add payloads (transport data of a packet between two partners that do not contain protocol data or metadata, only be sent for custom payload transport).

Any payload can be combined with any exploit thanks to the application's modular system.

Linh download: https://www.metasploit.com/

3. KeePass



If you do not use the password manager (and you do not have photo memory), it is completely wrong for you to do online security. The browser-based password manager is known for its poor security and not using passwords encourages people to use weaker passwords.

The most famous password manager is LastPass, but there are many other alternatives.

One of the best alternatives is KeePass. It is open source but there is a fairly large user community. The app stores all your passwords in a single database that is then locked. The database uses AES and Twofish encryption methods.

Link reference: https://keepass.info/

4. Certbot

Certbot is a project from the Electronic Frontier Foundation (EFF).

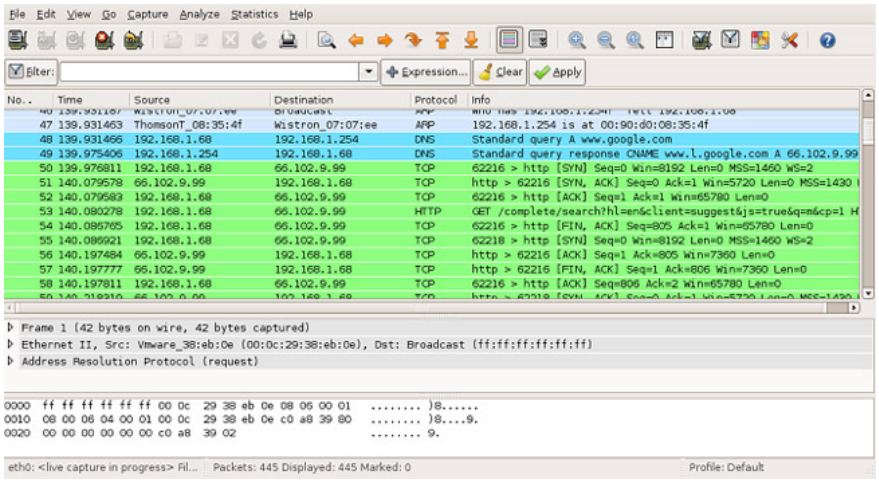
To explain why it is useful, we need to rethink how EFF wants to help create a website where all traffic is encrypted by default. Initially, the platform helped create the add-on HTTPS Everywhere for the browser, then the company turned into Let's Encrypt (a free certification service).

The latest release of EFF is Certbot. Let's Encrypt auto-connect application to fetch and deploy SSL / TLS certificate on web server.

It uses the Automated Certificate Management Environment (ACME) protocol, so it is easy to work with other certification agencies.

Download link: https://certbot.eff.org/

5. Wireshark



Wireshark is a network protocol analyzer. So popular that it has become the standard protocol analyzer for thousands of organizations, including government agencies, schools and commercial enterprises.

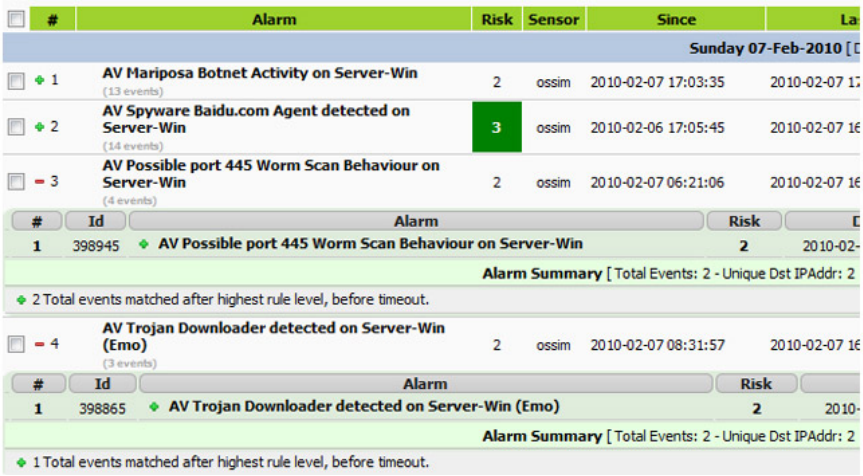
Using the application, you can check data from online networks or capture files on disk. You can explore your data at a level of detail.

Additional features include a rich display filter language, rebuilt TCP streams and support for hundreds of protocols and media types.

Link download: https://www.wireshark.org/

1. Use Wireshark to analyze data packets in the network

6. OSSIM



OSSIM (Open Source Security Information Management) is a set of open source applications that together constitute a security and event management system (SIEM). SIEM systems often provide real-time analysis of security alerts from other network applications and hardware.

OSSIM includes all the features you expect from the SIEM system, including event collection, normalization and correlation.

It uses AlienVault Open Threat Exchange to allow users to send and receive real-time information about malicious servers.

Unfortunately, the basic application does not provide log management, AWS and Azure cloud monitoring or integration with third-party ticketing applications. For those features, you will need to pay to register.

Link download: https://www.alienvault.com/products/ossim

7. CipherShed

CipherShed starts as a branch of the TrueCrypt project (no longer available). Available for Windows, Mac and Linux, the application can create unique encrypted files or encrypt the entire drive. This software also uses external storage media such as USB sticks and external hard drives.

The application will attach to the drive after being encrypted. While mounted, encryption is transparent to the operating system and installed applications. You can use the drive to read and write as usual. When you disconnect the drive, the contents of the drive will be hidden.

You can move encrypted drives between operating systems without compatibility issues.

Link to reference: https://www.ciphershed.org/

Why are open source applications important?

If an application is open source, its source code will allow other users to view, modify and share.

From a security standpoint, that means you can be sure a spy application installs malware on your computer. And even if you don't have the technical ability to study the code yourself, you can be confident that the community will discover any errors if they exist.

Open source applications are also attractive because they are often free. Why spend hundreds of dollars on security software when open source content can almost always meet user demand?

In this article, we have introduced you to the seven best open source security applications. Each application specializes in a different part of the network or computer security.

Unfortunately, the nature of open source software means there are hundreds of great applications that we can't mention. Please read the next article!

See more:

1. 5 Security application you should consider removing and replacing
2. 11 free open source applications for small businesses
3. 15 open source applications you should know