WMLUG January 2016

Desktop Linux Security Basics

Patrick TenHoopen

Desktop Linux Security Basics

There are some basic steps you can take to improve security and to protect your desktop running Linux.

Linux server security is a lot more extensive and beyond the scope of this presentation.

Threats and Attack Vectors

- Weak passwords
- Phishing schemes
- Compromised installation sources
- Running as root user
- Unpatched vulnerabilities
- Unneeded software/services
- Viruses, malware, rootkits

Passwords

Password Strength

- Avoid weak passwords that are easily guessed

Password Generators

- Create strong, unique passwords

Password Keepers

- Let software manage passwords for ease of use (no writing them down)

Password Strength

https://www.grc.com/haystack.htm

A strong password has both entropy and length.

Entropy is determined by the character set used, upper case letters, lower case letters, numbers, and symbols.

Use all character types to increase the entropy.

The longer a password is, the harder it is to crack.

Password Padding

You can create easy to remember padding for the beginning, middle, or end of a password to make it longer thus very hard to guess/crack.

(((((MySecr3tPassw0rd)))))

MySecr3tPassw0rd==========

---My---Secr3t---Passw0rd

Password Generators

GRC Perfect Passwords

https://www.grc.com/passwords.htm

Secure Password Generator

http://passwordsgenerator.net/

Password Keepers

Lastpass

https://lastpass.com/

KeePass Password Safe

http://keepass.info/

Phishing Schemes

Scammers send bogus emails to users hoping that they will trick them into opening attachments or clicking on links.

This type of attack uses human behaviors against them and is referred to as Social Engineering.

Installing Software

Be wary of installing software from untrusted/unverified installation sources such as Personal Package Archives (PPA) and third-party sites.

Try to use your package manager for all software installations.

User Account Usage

Don't login as the root user for normal, every day tasks.

If malicious software gets access, using a normal account would reduce the area of impact compared to the root user.

However, this doesn't prevent attacks from ransomware that encrypt your user's files.

Unpatched Software

Unpatched software can have vulnerabilities that malware can use to gain access to a system.

Be sure to patch software on a frequent basis.

Uninstall unused software and disable services that you don't need (e.g., Bluetooth) to reduce chances of running vulnerable software and to reduce potential points of entry.

Viruses, Malware, and Rootkits

Malware is short for malicious software that is intended to damage or disable computer systems. Subtypes include viruses, worms, ransomware, trogan horses, keyloggers, rootkits, spyware and adware among others.

A virus is malware that is capable of copying itself to spread the infection and potentially corrupt other software or destroy data.

Rootkits are malware that hide compromised files from the operating system to allow malware and viruses to exist undetected.

Virus Detection

Anti-virus software is designed to detect viruses and other malware by scanning files and comparing the contents to signatures of known malware.

The effectiveness of anti-virus software varies by vendor.*

Although there are fewer Linux malware than compared to on Windows, it may still be prudent to run anti-virus software.

*http://www.networkworld.com/article/2989137/linux/av-test-lab-tests-16-linux-antivirus-products-against-windows-and-linux-malware.html

Malware Detection

Linux Malware Detect (LMD)

LMD is a malware scanner for Linux released under the GNU GPLv2 license, that is designed around the threats faced in shared hosted environments.

https://www.rfxn.com/projects/linux-malware-detect/

Rootkit Detection

chkrootkit

http://www.chkrootkit.org/

Rootkit Hunter

https://rootkit.nl/projects/rootkit_hunter.html

Firewalls

Although a firewall will not stop the installation of malware, using one can help block the activity of malicious software by filtering incoming and outgoing packets.

Browser Protection

You can protect your browser from malicious web pages by installing a blocker such as uBlock Origin.

You can make sure your browser uses a secure connection to sites (as much as possible) by installing HTTPS-Everywhere.

Encryption

Consider using full disk encryption to protect data in case computer is lost or stolen.

Use secure connections to web sites when possible.

Backups

Having complete and recent backups of data will help in case your computer gets infected with ransomware. Instead of paying the ransom to get access to your data back, you can just restore the data.