Hardening Your Linux Systems

Andrew Mallett

Linux Author and Trainer

@theurbanpenguin www.theurbanpenguin.com

Overview

Hardening Linux

- Remove Unneeded Services
- Remove Insecure Services
- Implement M-ACL
- Securing with Sysctl
- List Unused Users
- List Password Changed Dates
- Lock Users on Password Failure

Lab Systems

Ubuntu 20.04

- New vagrant system
- vagrant destroy ubuntu
- vagrant up ubuntu
- vagrant ssh ubuntu

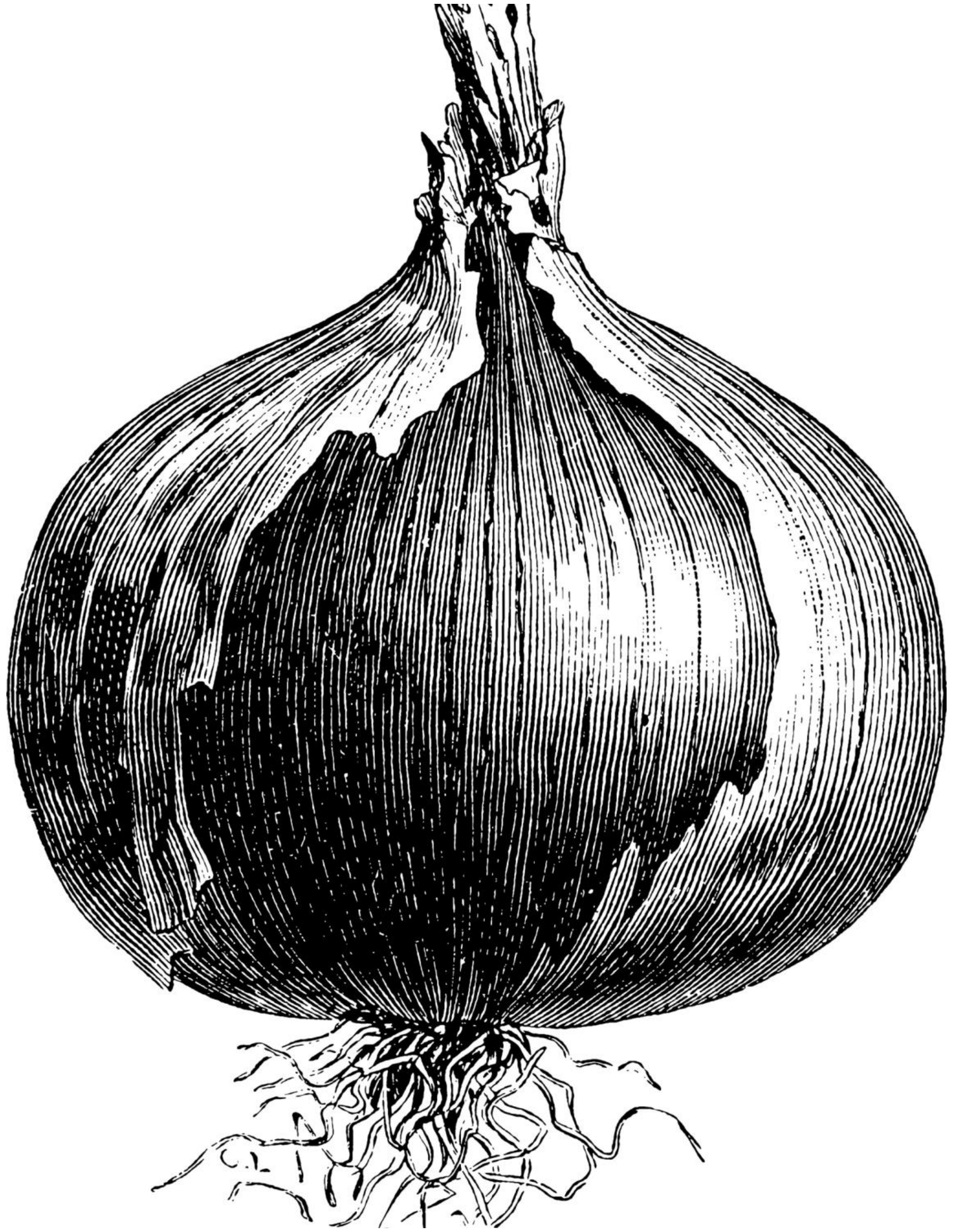
Security is Your Responsibility

- Defaults show lack of thought
- What services are enabled
- Do you have insecure services

Out of the box, more services may be enabled than you need

Understanding tools you have to find valuable information

The Security Onion



Think of your security as an onion:

It has many layers and is never implemented in just one place

Get it wrong and you will cry

TELNET insecure and blocked by the firewall so it doesn’t matter that it is running

- What if the firewall fails or is compromized?
- What if someone has gained access to your internal network?
- Internal users can always be trusted?

Always assume the worst and work with this in mind

```
$ ss -ntl

$ ss -l '(sport = :ssh)'

$ systemctl status
```

Listing Services

We can list listening services easily, but we can always drill down to specific services. To list all services; we can use the status sub-command without arguments

```
$ sudo apparmor_status
$ sudo getenforce
```

Checking Mandatory ACLs

M-ACLs such as SELinux and AppArmor can go a long way to securing your systems, validate that they are running

Demo

Discovering Security

- Listing Default Services
- Listing Default Ports
- Reduce Listening Addresses

Demo

Discovering Security

- Remove Unneeded Services
- Validate M-ACL

```
$ sysctl -a
$ sysctl -ar 'icmp'
$ ping localhost
$ sudo vim /etc/sysctl.d/99-icmp.conf
net.ipv4.icmp_echo_ignore_all=1
$ sudo sysctl --system
$ sysctl -ar 'icmp'
$ ping localhost
```

Kernel Tuning Using Sysctl

The kernel is tuned using the procfs, files below /proc. We can display and configure settings using the command sysctl. Persisting configuration using files below /etc/sysctl.d. Higher number files are applied AFTER lower numbers becoming the most effective.

Demo

Investigating the Procfs:

- Searching with sysctl
- Writing values with sysctl
- Persisting settings

```
$ last
$ lastlog
$ lastlog | grep -v "Never logged in"
```

Listing Last Login Times

The command last will show reboot history as well as login information. Lastlog shows last login time for all accounts

```
$ for u in $(awk -F: '{ if ($3 >= 1000) print $1}' /etc/passwd; do
> echo $u
> sudo chage -l $u | grep '^Last'
> done
```

Listing Password Last Changed

The command, chage, can be used to list password aging data, but for all users we can create a lost using awk

Demo

Listing Users:

- Login times
- Password Changed

```
$ man pam_tally2
$ sudo vim /etc/pam.d/common-auth
...
auth    required        pam_tally2.so deny=3 unlock_time=300
...
```

Lock Failed Login Attempts

We can lock accounts with failed login attempts. By default, this does not include the root account as it becomes a means of a denial-of-service attack

Demo

PAM and Locking Failed Login Attempts:

- pam_tally2
- common-auth

Summary

Implementing Security Hardening

- Security is in every aspect of Linux
- Services
- Users
- Passwords

Implementing Firewalls with Firewalld