The Beauty of Simple

Michael Boelen
NLUUG - May 16th, 2017
Today

- Define ‘simple’
- Challenge complexity
- Simplify your life

@mboelen
“Simple”
Simplicity is the ultimate sophistication.

Introducing Apple II, the personal computer.
Keep it simple, stupid.

Kelly Johnson, KISS principle
Simplicity is prerequisite for reliability.

Simplicity is the shortest path to a solution.

Ward Cunningham, "The Simplest Thing that Could Possibly Work"
Simplicity — the art of maximizing the amount of work not done — is essential.

Less is more.

Robert Browning, Andrea del Sarto (1855).
Complexity
Choices

OMEN by HP
Gaming reinvented. Ominous power.

HP EliteBook 850
Sophisticated travel pro.

HP EliteBook x360 1030 G2
New and innovative security solutions

HP Spectre
Artisan materials and striking craftsmanship.

HP ENVY 15
Impossibly thin. Enviably engineered.

HP Pavilion 17
Watch more, play more, store more.

HP ProBook 640
Built for performance
MacBook Pro

A touch of genius.

Learn more ›   Buy ›
Choices

Hardening-- [0]# nmap
Nmap 7.01 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [options] [target specification]

TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  EX: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file

HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sN: Ping Scan - disable port scan
  -PR: Treat all hosts as online -- skip host discovery
  -PS:PA/PU/PM[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host

SCAN TECHNIQUES:
  -sS/S/T/S/N/S: T CP SYN/Connect()/ACK/Window/Maimon scans
  -SU: UDP Scan
  -SN/SF/SX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  --SA <zombie host[=probeport]>: Idle scan
  --SY/SZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan

PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
  Ex: -p22, -p1-65535; -p U:53,111,137,1:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don’t randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
Up VS ....?
Lyins 2.4.8

Lyins comes with ABSOLUTELY NO WARRANTY. This is free software, and you are welcome to redistribute it under the terms of the GNU General Public License. See the LICENSE file for details about using this software.

Enterprise support available (compliance, plugins, interface and tools)

Initializing program

Usage: lyins command [options]

Command:

    audit
    audit system [options]          : Perform local security scan
    audit system remote <host>      : Remote security scan
    audit dockerfile <file>         : Analyze Dockerfile

    show
    show all commands               : Show all commands
    show lyins version              : Show Lyins version
    show help                       : Show help

    update
    update info                     : Show update details
    update release                  : Update Lyins release

Options:

    --no-log                        : Don't create a log file
    --no-verbose-logging           : Non-privileged scan (useful for pentest)
    --profile <profile>             : Scan the system with the given profile file
    --quiet (-q)                    : Quick mode, don't wait for user input

    --no-colors                     : Don't use colors in output
    --no-output                    : No output
    --reverse-colors               : Optimize color display for light backgrounds

Misc options:

    --debug
    --help [command]                : Display version number and quit
    --manage (-m)                   : View man page
    --version (-V)                  : Show more details on screen
Confusion

jacurtis 12 hours ago
I am glad im not the only one confused by this. I went to the webpage first, couldnt really figure out what exactly it did. So i went to HN comments to see if i could figure out the purpose of this product through the comments. Turns out everyone is confused as well, lol.

akerro 11 hours ago
BUT DOES IT SCALE ON THE CLOUD
Useless Errors
Good software design is simple and easy to understand. Unfortunately, the average computer program today is so complex that no one could possibly comprehend how all the code works. This concise guide helps you understand the fundamentals of good design through scientific laws—principles you can apply to any programming language or project for which you are responsible.
Chartjunk

https://upload.wikimedia.org/wikipedia/commons/c/c9/Chartjunk-example.svg
How to kill complexity?

● First impression
● Simplicity
● Next step
Example: Open Source Projects

- Good description, “Get started”
- Colors, sane defaults
- Show log file, link with more details
Simplify Life
How?

- Identify
- Reduce
- Organize
Method: 5S

- **Seiri (整理)**: Sort
- **Seiton (整頓)**: Set in order
- **Seisō (清掃)**: Shine
- **Seiketsu (清潔)**: Standardize
- **Shitsuke (躾)**: Sustain
The wet weather continues.
Rain for the rest of the day.
Uncopyright

This entire blog, and all my ebooks, are uncopyrighted (since January 2008).

That means I've put them in the public domain, and released my copyright on all these works.

There is no need to email me for permission — use my content however you want! Email it, share it, reprint it with or without credit. Change it around, put in a bunch of swear words and attribute them to me. It's OK.

Attribution is appreciated but not required.

I'd prefer people buy my ebooks, but if they want to share with friends, they have every right to do so.
Thanks
(and enjoy the conference!)
Programming

- You aren't gonna need it (YAGNI)
- Don’t repeat yourself (DRY)
- Minimum Viable Product (MVP)
- Feature creep, creeping featurism or featuritis
- Principle of good enough
- Wirth's law (software VS hardware)