Daniel Hautzinger - Jaeda Nowacki
Computing and Information Sciences

Abstract

This multifaceted project has investigated a number of security-related instruments in order to build a set of recommended tools for Information Technology practitioners constrained by minimal resources. Criteria for tool selection were identified, including operational complexity and reusability, to refine the possibilities found to a workable number of options. This list was largely informed by several available well-known platforms and suites; a secondary goal was to define a toolkit suitable for classroom instruction**.** Initial investigation led to the identification of the Raspberry Pi and Kali Linux. This combination provided a very large range of options and a portable/mobile capability. The main challenges to this project revolved around two goals: (1) locating tools that had little to no cost, and (2) identification of tools that are both easy to learn and suitable for those looking to create more secure network and host configurations with limited time, expertise, and financial resources.

Motivation/Initial Selection

Increasingly, many institutions maintain a somewhat complex set of technologies to provide a variety of capabilities. For non-profits, small- and mid-size businesses, and local governments, there are resource limitations that can make having even routine IT expertise difficult to obtain, even discounting the premium for the specialized skills for cyber security. Current US Bureau of Labor Statistics figures show median salaries of >$83,000/year for the former [1] and >$99,000/year for the latter [2]. This project sought, in part, to see if high proprietary software costs could be eliminated through use of free/open/low-cost applications that could be used by an individual who was IT/etc. familiar rather than a fully professional practitioner.

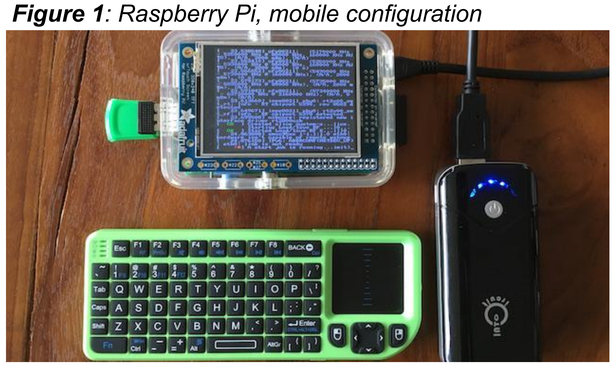
Two platforms immediately stood out after the initial review of options: Kali Linux [3] and the Raspberry Pi Single Board Computer [4], which can host a mobile security testing tool suite [5] based on the Kali GNU/Linux Distribution.

Selected Tools

Raspberry Pi Portable Hacking Device (Fig.1):

Raspberry Pi *Battery Pack (Optional)*
WiFi Card *8GB SD Card*
PiTFT touch screen Keyboard
Total cost: ~$75 - $100 (US)

Figure 1*: Raspberry Pi, mobile configuration*



The Kali GNU/Linux distribution was selected as the main platform because of its well-known reputation in the security field and large user/support community. The combination of tools provides one of the most extensive collections of software security tools in one place and is available as one bootable download.

Kali Linux – included software tools [1]:

Wireshark *Nmap*
Faraday *Skipfish*
Ettercap *NST*
….and over 40 others [3]
Total cost: Removable media ~$20

Kali Logo

(to avoid necessity of a full local install through use of bootable media, leaving system available for other tasks)

Figure 2: Kali Tools List/Menu Screenshot

Following initial investigation, only four were evaluated (Full set seen in figure 2, and [3]):

Wireshark *Nmap*
Faraday *NST*

(Concerns about regulatory and appropriate use considerations led to the elimination of several initially identified, as the risks for misuse or harm effectively eliminated them as appropriate for use.)

Observations

The assessment of tools quickly settled on flexibility, ease of immediate use, capability across multiple areas, and the overall availability of information/help.

The Raspberry Pi + Kali Linux

The Pi+Kali combination performed well across all the listed categories and was a successful portable mobile network sweeping tool. It allowed testing of WiFi security and password strength while also providing solid tools for general network testing and diagnostics, plus a library of reusable common exploits. The equipment required is commonly available, remarkably small, and has easy to follow setup and configuration.

The Kali Linux "Subset" – on Desktop

For desktop operation, the standout choices based on the identified criteria were Wireshark, Nmap, NST and Faraday. Nmap and Wireshark had the most available support. Faraday, being newer, had less in this category but it is expected the user and developer communities will remedy this over time. Collectively, these four tools provide powerful but approachable security testing/assessment capability.

Conclusions

The identification of the tools, equally available on a highly mobile/portable and standard desktop platform, demonstrates that significant capabilities can be found within resource constrained groups. Longer-term challenges include obtaining the knowledge required to navigate the ecosystem of available options; even factors as simple as the colloquial "insider" naming traditions for these tools make finding suitable options difficult. An effort by the IT community to support less experienced groups or resourced institutions, even through a "getting started" guide, would help to close the expertise gap that is needed to improve security practices. Future work will include investigation of how to build a sustainable training suite for these tools, which is a particular challenge given the rapid evolution of this space.

References

1. US Bureau of Labor Statistics, Occupational Outlook Handbook (Network & Computer Systems Administrators) - 2020, at https://www.bls.gov/ooh/computer-and-information-technology/network-and-computer-systems-administrators.htm
2. US Bureau of Labor Statistics, Occupational Outlook Handbook (Information Security Analysts) - 2020, at https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
3. https://tools.kali.org/tools-listing
4. https://www.raspberrypi.org/
5. https://lifehacker.com/how-to-build-a-portable-hacking-station-with-a-raspberr-1739297918

Acknowledgements

Thanks to the NSF EPIC Scholarship (Grant Award Number 1564855) and the Valparaiso University Department of Computing and Information Sciences for financial and hardware support. Thanks, also, to our project advisor Professor Nicholas S. Rosasco, DSc.