ePortfolio Activity

Brief

Read the following articles on Kali Linux:

- Leroux, S. (2020) The Kali Linux Review You Must Read Before You Start Using It. It's FOSS. Available from: **https://itsfoss.com/kali-linux-review/**
- Bhatt, D. (2018) Modern Day Penetration Testing Distribution Open-Source Platform - Kali Linux - Study Paper. *International Journal of Scientific & Technology Research* 7(4): 233-237.

  - **What does the article teach you about carrying out vulnerability scans using Kali?**
    - Kali Linux has a default “root” user installation, so all scans are executed as “root” user.
    - Executing vulnerability scans for penetration testing is relatively simple using Kali Linux given that it comes pre-installed with several tools to start with penetration testing. However, if a penetration tester has no prior experience of using Linux, there will be a slight learning curve to understand the Linux operating system and by extension, *what* different tools scan for.
    - Vulnerability scanning is a valuable practice which organisations must incorporate into their secure software development processes.

  - **What issues might you encounter?**
    - Inadvertently editing system files that could destabilise a Kali Linux installation for instance, editing the `/usr/sbin/update-rc.d` file to whitelist several services. Forgetting to remove the services when no longer needed, would leave the installation open and vulnerable.
    - Adding new source repositories by editing the `/etc/apt/sources.list` file can lead to a mishmash of installed software that no longer works well with the default Linux installation.
    - Software might be installed from source code tarballs which thereafter cannot be removed using the APT packaging system.
    - Software may be installed from untrusted sources.

- **How would you overcome them?**
  - Do not install video card drivers directly from a manufacturer's website because their drivers are designed to work for the current Linux kernel and may not work when a new version is available.
  - Install software from official repositories, for example from the Debian Security Team.
  - Install software using the APT packaging system.
  - Do not rely on Personal Package Archives (PPA) as they are community-generated and may suffer from poor security.

- Bhingardeve, N. & Franklin, S. (2018) A Comparison Study of Open-Source Penetration Testing Tools. *International Journal of Trend in Scientific Research and Development* 2(4): 2595-2597.

  - **How do their results compare with your initial evaluation?**

VI. COMPARISION OF VARIOUS TOOLS

Features	Nmap	Metaploit	Wireshark	Aircrack	John the Ripper	Sqlmap
Flexible	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Powerful	*Yes*	*Yes*	*Yes*	*Yes*		
Portable	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Easy	*Yes*	*Yes*		*Yes*	*Yes*	*Yes*
Free	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Well-documented	*Yes*		*Yes*		*Yes*	
Supported	*Yes*		*Yes*		*Yes*	*Yes*
Acclaimed	*Yes*	*Yes*	*Yes*			
Popular	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*

Figure 1 Table of tools comparison (Bhingardeve & Franklin, 2018).

My initial evaluation of the tools listed above are categorised as:

Features	Nmap	Metasploit	Wireshark	Aircrack	John the Ripper	SqlMap
Flexible	*Yes*	*Yes*	*Yes*			
Powerful	*Yes*	*Yes*	*Yes*			
Portable	*Yes*	*Yes*	*Yes*			*Yes*
Easy	*Yes*	*No*	*Yes*	*Yes*	*Yes*	*Yes*
Free	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Well-documented	*Yes*					
Supported	*Yes*		*Yes*		*Yes*	*Yes*
Acclaimed	*Yes*	*Yes*				
Popular	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*

Unfortunately, at this moment in time, I do not have tremendous exposure to Aircrack, John the Ripper and SqlMap other than reading available documentation related to these tools.

- **What do you think of their criteria?**

  I think the criteria of the authors is rather weak, since they state, "The researcher has used secondary data which were gathered from diverse source, including archival sources, journals, articles and internet sites and blogs" and yet the references section lists three entries that are not research papers of any kind, mere general internet searches.

  My impression from reading this paper is that the researchers performed a general search of Kali Linux tools and chose the ones that often appear in most search results related to "Kali" and "Penetration Testing". On the surface, this is not bad, because they do state they looked for tools that were "well supported and easy to start getting value from"

"Kali Linux is a well-respected collection of open-source pen testing tools, including metasploit, nmap, wireshark and sqlmap amongst many others. It has the benefit of being available as a 'live distro' which means that there is no requirement to install it – it will run from a DVD or a USB/ thumb drive. For these reasons, we recommend that Kali Linux is the tool of choice for this assignment." (UoEO Computing Team, 2020).

Based on your evaluation in the previous session and the articles above, consider the recommendation given above:

- **What are the pros and cons of using Kali Linux vs. Nessus?**

KALI LINUX

Pros	Cons
- Contains several tools useful for penetration testing such as Wireshark, John the Ripper and Metasploit. - License cost is free. - Original source code is open sourced allowing cybersecurity professionals to tweak Kali.	- Available only for Linux installations. - There is a learning curve required to understanding a Linux environment and the various free tools. - Some hardware may require non-free firmware files to operate. -

- Used mainly by cybersecurity and ethical hackers. - Can be run from a USB stick. - Supports ARM architecture and can therefore be installed on Android devices. - The Kali Linux team is trusted to commit packages using multiple secure protocols.	

NESSUS

Pros	Cons
- Can perform scheduled security audits. - Detects security holes in local or remote hosts. - Can simulate attacks to pinpoint vulnerabilities. - Supports detection of missing security updates and patches. - Can perform internal network scans as required by the PCI DSS 11.2.1 requirement. - Available for Windows and Linux installations.	- Costs around $3000 USD per annum. - Cannot be used on systems with a Host-based Intrusion Prevention System (HIPS)

- **Has this changed your original evaluation score?**

  No, having used Kali Linux in as part of the scanning exercises, I feel it is the right choice to advise for those looking to obtain a set of free tools to perform penetration testing. However, I do understand that some organisations may not permit Linux distributions within their environment, and would opt for paid-for products that have known Software Lifecycle Agreements in place, thus guaranteeing some level of technical support and training.