E Useful Tools

E.1 Introduction

NIST SP800-115 proposes a list of tools for applying some techniques. However, it is important to note that a great part of these tools is only supported in the Linux operating system and thus, for example, not on Windows. However, various tools are aimed to analyze captures or dumps of information offline. Hence, these tools are also well candidates for being scripted so that they can be automated.

Furthermore, the list proposed in the standard is mostly outdated and relates to the former version of Kali Linux which was called BackTrack. The remainder of this document presents tables, by category of technique as explained in the standard, that show some samples of tools from NIST SP800-115 merged with a list of other ones that are commonly used today in security assessments.

Legend

🐧: Linux	🪟: Windows	🐧🪟Linux, Windows(, Mac OS X)

E.2 Review Techniques

Technique	Tools
System Configuration Review	🐧OpenSCAP 🪟ASA, MSBA
Network Sniffing	🐧Wireshark, Dsniff, Ettercap, SMB Sniffer 🪟Wireshark
File Integrity Checking	🐧🪟Autopsy, SleuthKit 🐧Foremost, RootkitHunter

Note that, for the *System Configuration Review* technique, especially useful at the *System* perimeter, a workbench running on Windows exists for writing compliance tests but the tool that actually executes the compliance checking only exists in a Linux version. In general, as most organizations use Windows products, using ASA and MSBA is a must, allowing to analyze up to the *System* perimeter.

It can pointed out that Wireshark exists either on Linux or Windows and, furthermore, provides a command-line tool and can then be scripted, which is a very interesting advantage, especially for assessments up to the *Network* perimeter. Moreover, Foremost (only running on Linux) can extract files from network traffic captures so that they can be analyzed for malicious traces. Frameworks like Autopsy and SleutKit perform the same kind of operations and are then also good candidates for automation. Some other tools are only supported by Linux and then cannot serve for any assessed software product.

E.3 Target Identification and Analysis

Technique	Tools
Network Discovery	🐧Nmap, Firewalk, Netdiscover 🪟Nmap
Network Port & Service Identification	🐧Nmap, Amap, AutoScan, Netdiscover 🪟Nmap
Vulnerability Scanning	🐧🪟Metasploit 🐧Firewalk, GFI LANguard, Hydra, OpenVAS
Wireless Scanning	🐧Kismet, WifiTAP, GFI LANguard, Airsnort, Airsnaf

It is important to note that the tools in this category all relate to the *Network* perimeter. One can point out that Nmap, available either for Linux or Windows, is a multi-purpose tool that could be very interesting for covering multiple techniques. OpenVAS, discussed in Subsection 2.3.2, is a nice solution as an external system to scan the vulnerabilities of Web application servers.

E.4 Target Vulnerability Validation

Technique	Tools
Password Cracking	🐧John The Ripper, Hydra, RainbowCrack, TFTP-Brute, WebCrack, VNCrack 🪟Cain & Abel
Social Engineering	🐧SET[1]
Penetration Testing	🐧Metasploit, Armitage, MsfVenom, Kismet, Driftnet, SPF[2]

For *Password Cracking*, hashes can be dumped into a file so that these can be analyzed regardless of the operating system. *Social Engineering* is typically a technique that applies from the *Network* perimeter. About the *Penetration Testing*, Metasploit is a perfect framework, only available on Linux, for making payloads when preparing attacks, e.g. a Word or Excel document with a malicious macro. A reasonable part of these tools can also be scripted.

[2] Social Engineering Toolkit

[2] Smartphone Pentesting Framework