Appendix B. Key Resources

This chapter will give you information on several resources that can be used to expand your knowledge on the penetration testing world. We will list the following resources:

- Websites on vulnerability disclosure and tracking
- Companies that will pay for vulnerabilities and exploit disclosure
- Websites for learning about reverse engineering, exploit development, and penetration testing
- A penetration testing environment to learn penetration testing
- A list of common network ports you may find during penetration testing journey

Note that the websites listed here are just the starting points and are not intended to be exhaustive. We suggest that you use the search engines to help you find the other resources.

Vulnerability disclosure and tracking

The following is a list of online resources that may help you tracking the vulnerability information. Many of these websites are best known for their open vulnerability disclosure program, so you are free to contribute your vulnerability research to any of these public/private organizations. Some of them also encourage a full disclosure policy based on the paid incentive program to reward the security researchers for their valuable time and effort they put into vulnerability investigation and the development of **proof of concept** (**PoC**) code.

The following are some of the vulnerability disclosures and tracking websites that you can use:

URL	Description
http://www.osvdb.org/	The Open Source Vulnerability Database
http://www.securityfocus.com/	Public vulnerabilities, mailing lists, and security tools
http://www.packetstormsecurity.org/	Exploits, advisories, tools, and whitepapers
http://www.vupen.com/	Security advisories, PoCs, mailing lists, and research publications
http://www.secunia.com/	Advisories, whitepapers, security factsheets, and research papers
http://www.exploit-db.com/	Exploits database, Google Hacking Database (GHDB), and papers
http://web.nvd.nist.gov/view/vuln/search	NVD is a U.S. government repository for a vulnerability database based on CVE
https://access.redhat.com/security/updates/advisory/	RedHat errata notification and security advisories
http://lists.centos.org/pipermail/centos-announce/	CentOS security and general announcement mailing list
http://www.us-cert.gov/ncas/alerts	DHS US-CERT reports security issues, vulnerabilities, and exploits techical alerts
http://xforce.iss.net	ISS X-Force offers security threat alerts, advisories, vulnerability database, and whitepapers.
http://www.debian.org/security/	Debian security advisories and mailing lists

URL	Description
http://www.mandriva.com/en/support/security/	Mandriva Linux security advisories.
https://www.suse.com/support/update/	SUSE Linux Enterprise security advisories.
http://technet.microsoft.com/en-us/security/advisory	Microsoft security advisories.
http://technet.microsoft.com/en-us/security/bulletin	Microsoft security bulletins.
http://www.ubuntu.com/usn	Ubuntu security notices.
http://www.first.org/cvss/	First **Common Vulnerability Scoring System** (**CVSS-SIG**).
http://tools.cisco.com/security/center/publicationListing.x	Cisco security advisories, responses, and notices.
http://www.security-database.com	Security alerts and dashboard and CVSS calculator.
http://www.securitytracker.com/	Security vulnerabilities information.
http://www.auscert.org.au/	Australian CERT publishes security bulletins, advisories, alerts, presentations, and papers.
http://en.securitylab.ru/	Advisories, vulnerability database, PoC, and virus reports.
http://corelabs.coresecurity.com/	Vulnerability research, publications, advisories, and tools.
https://www.htbridge.com/	Security advisories and security publications.
http://www.offensivecomputing.net/	Malware sample repository.
http://measurablesecurity.mitre.org/	MITRE offers standardized protocols for the communication of security data related to vulnerability management, intrusion detection, asset security assessment, asset management, configuration guidance, patch management, malware response, incident management, and threat analysis. **Common Vulnerabilities and Exposures** (**CVE**), **Common Weakness Enumeration** (**CWE**), **Common Attack Pattern Enumeration and Classification** (**CAPEC**), and **Common Configuration Enumeration** (**CCE**) are a few of them.

Paid incentive programs

The following table lists several companies that will give incentives to researchers who inform them about zero-day exploits:

URL	Description
http://www.zerodayinitiative.com/	Zero-Day Initiative (3Com / TippingPoint division) offers paid programs for security researchers
http://www.netragard.com/zero-day-exploit-acquisition-program	Netragard offers to buy zero-day exploits
https://gvp.isightpartners.com/	iSIGHT partners offers the **Global Vulnerability Partnership** (**GVP**) program

URL	Description
https://exploithub.com	ExploitHub is a marketplace for vulnerability testing
http://www.beyondsecurity.com/ssd.html	The SecuriTeam Secure Disclosure program offers researchers to get paid for discovering vulnerabilities