
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

---

Reverse engineering resources

The following table contains several websites that can help you learn about reverse engineering:

URL	Description
http://www.woodmann.com/forum/index.php	Reverse code engineering forums, collaborative knowledge, and tools library.
http://www.binary-auditing.com/	Free IDA Pro binary auditing training material.
http://www.openrce.org/	Open reverse code engineering community.
http://reversingproject.info/	This provides tools, documents, and exercises to learn software reverse engineering.
http://www.reteam.org/	Reverse engineering team with various projects, papers, challenges, and tools.
http://www.exetools.com/	Tutorials, file analyzers, compressors, hex editors, protectors, unpackers, debuggers, disassemblers, and patchers.
http://tuts4you.com/	Tutorials and tools for reverse code engineering.
http://crackmes.de/	Here, you can test and improve your reversing skills by solving the tasks (usually called crackmes).
http://fumalwareanalysis.blogspot.com/p/malware-analysis-tutorials-reverse.html	This site contains malware analysis tutorials. The analysis is done using a reverse engineering approach.
http://quequero.org/	The UIC R.E. academy is aimed at teaching reverse engineering for free to anybody willing to learn. It contains malware analysis articles and several reverse engineering tools.

Penetration testing learning resources

The following table lists several websites that you can refer to in order to deepen your knowledge in the penetration testing field:

URL	Description
http://www.kali.org/blog/	Kali Linux blog.
http://pen-testing.sans.org	SANS penetration testing resources: blogs, white papers, webcasts, cheatsheets, and links useful for penetration testing.
http://resources.infosecinstitute.com/	This contains articles on various topics in information security, such as hacking, reverse engineering, forensics, application security, and so on.
http://www.securitytube.net/	This contains various videos on information security. Out of these, the ones that are especially useful for learning are the megaprimer videos such as Metasploit framework expert, Wi-Fi security expert, exploit research, and so on.
http://www.concise-courses.com/	This provides web shows and an online course related to information security. The course may not be free.
http://opensecuritytraining.info/Training.html	This provides training material for computer security classes on any topic that are at least one day long.
https://pentesterlab.com/bootcamp/	This provides information on how to become a pentester. The material is divided into a 15-week bootcamp session. It contains the reading list and hands-on practice.
http://www.pentesteracademy.com/	This provides online information security training. It covers several topics such as web application pentesting, network pentesting, and so on. Some of the videos can be downloaded for free, while for the others, you need to become a member to access them.
http://www.pentest-standard.org	This is a new standard designed to provide both businesses and security service providers with a common language and scope for performing penetration testing.
http://www.ethicalhacker.net/	Free online magazine for security professionals.
https://community.rapid7.com/community/metasploit/blog	Metasploit Blog.
http://www.blackhatlibrary.net/Main_Page	This contains security tutorials and tools.
http://www.offensive-security.com/metasploit-unleashed/Main_Page	This website provides free training for the Metasploit framework.
http://www.codecademy.com/learn	This website provides various tutorials to learn the programming language.

URL	Description
http://www.social-engineer.org/framework/Computer_Based_Social_Engineering_Tools:_Social_Engineer_Toolkit_%28SET%29	Social engineering toolkit tutorial
http://technet.microsoft.com/en-us/library/cc754340%28WS.10%29.aspx	Windows Server command-line reference.
http://www.elearnsecurity.com/	eLearnSecurity is a provider of IT security and penetration testing courses for IT professionals.
http://www.offensive-security.com/	The developer of Kali Linux and provider of information security training and certification.
http://www.dirk-loss.de/python-tools.htm	Python tools for penetration testing.

Exploit development learning resources

The following table lists several websites that you can use to learn about software exploit development:

URL	Description
https://www.corelan.be/index.php/articles/	This contains various articles on information security. It is famous for providing detailed exploit writing tutorials.
http://fuzzysecurity.com/tutorials.html	It contains exploit development tutorials for Windows and Linux users.
http://www.thegreycorner.com/	It provides exploit tutorials and a vulnerable server application to practice.

Penetration testing on a vulnerable environment

The following sections list online web application challenges and virtual machine and ISO images that contain vulnerable applications. These resources can be used to learn penetration testing in your own system environment.

Online web application challenges

The following table lists several websites that provide several challenges, which you can use to learn penetration testing:

URL	Description
https://pentesteracademylab.appspot.com/	It contains four free challenges in the web application area such as form bruteforcing and HTTP basic authentication attack.
https://hack.me/	Hack.me is a free, community-based project powered by eLearnSecurity. The community can build, host, and share vulnerable web application code for educational and research purposes.
https://www.hacking-lab.com/caselist/	Hacking-Lab provides a security lab with various security challenges that you can try. They even provide a Live CD that will enable access into the 'Hacking-Lab's remote security lab.
https://google-gruyere.appspot.com/	This codelab shows how web application vulnerabilities can be exploited and how to defend against these attacks.
http://www.enigmagroup.org/	Enigma Group provides its members with a legal and safe security resource where they can develop their pen-testing skills on the various challenges provided by this site. These challenges cover the exploits listed in the **OWASP** (**The Open Web Application Security Project**) top 10 projects and teach members many other types of exploits that are found in today's applications, thus helping them to become better programmers in the meantime.
https://www.owasp.org/index.php /OWASP_Hackademic_Challenges_Project	The OWASP Hackademic Challenges Project is an open source project that helps you to test your knowledge on web application security. You can use it to actually attack web applications in a realistic but controllable and safe environment.
https://www.hackthissite.org/	Hack This Site is a free, safe, and legal training ground for hackers to test and expand their hacking skills. It also has a vast selection of hacking articles and a huge forum where users can discuss hacking, network security, and just about everything.

Virtual machines and ISO images

The following table lists several virtual machines and ISO images that can be installed on your machine as targets to learn penetration testing:

URL	Description
http://vulnhub.com/	It contains various VMs to allow anyone to gain a practical hands-on experience in digital security, computer application, and network administration.
http://exploit-exercises.com/	This provides a variety of virtual machines, documentation, and challenges that can be used to learn about a variety of computer security issues, such as privilege escalation, vulnerability analysis, exploit development, debugging, reverse engineering, and general cyber security issues.
https://www.pentesterlab.com/exercises/	This provides various web application security exercise materials, such as SQL injection, Axis2 and Tomcat manager, and MoinMoin code execution. In each exercise, you will have an explanation tutorial and also the vulnerable application in the ISO image.

URL	Description
http://hackxor.sourceforge.net	Hackxor is a webapp hacking game where players must locate and exploit vulnerabilities to progress through the story. It contains XSS, CSRF, SQLi, ReDoS, DOR, command injection, and so on.
https://www.mavensecurity.com/web_security_dojo/	A free open-source, self-contained training environment for web application security and penetration testing.
http://www.bonsai-sec.com/en/research/moth.php	Moth is a VMware image with a set of vulnerable web applications and scripts, which you may use for: • Testing web application security scanners • Testing **Static Code Analysis** (**SCA**) tools • Giving an introductory course on web application security
http://exploit.co.il/projects/vuln-web-app/	The exploit.co.il vulnerable web app is designed as a learning platform to test various SQL injection techniques, and it is a fully functional website with a content management system based on fckeditor.
http://sourceforge.net/projects/lampsecurity/	LAMPSecurity training is designed to be a series of vulnerable virtual machine images along with complementary documentation designed to teach Linux, Apache, PHP, and MySQL security.
https://bechtsoudis.com/work-stuff/challenges/drunk-admin-web-hacking-challenge/	The challenge includes an image hosting web service that has various design vulnerabilities. You must enumerate the various web service features and find an exploitable vulnerability in order to read system-hidden files.
https://code-google-com.db19.linccweb.org/p/owaspbwa/	OWASP Broken Web Applications Project, a collection of vulnerable web applications, is distributed on a virtual machine in VMware compatible format.
http://sourceforge.net/projects/bwapp/files/bee-box/	bee-box is a custom Linux VMware virtual machine preinstalled with bWAPP. bee-box gives you several ways to hack and deface the bWAPP website. It's even possible to hack bee-box to get root access. With bee-box, you have the opportunity to explore all bWAPP vulnerabilities!
http://information.rapid7.com/download-metasploitable.html?LS=1631875&CS=web	The Metasploitable 2 virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities.

Network ports

Assessing the network infrastructure for the identification of critical vulnerabilities has always been a challenging and time-consuming process. Thus, we have fine-tuned a small list of known network ports with their respective services in order to help penetration testers to quickly map through potential vulnerable services (TCP/UDP ports 1 to 65,535) using Kali Linux tools.

To get a complete and a more up-to-date list of all network ports, visit http://www.iana.org/assignments/port-numbers.

However, bear in mind that sometimes the applications and services are configured to run on different ports than the default ones, shown as follows:

Service	Port	Protocol
Echo	7	TCP/UDP
Character Generator (CHARGEN)	19	TCP/UDP
FTP data transfer	20	TCP
FTP control	21	TCP
SSH	22	TCP
Telnet	23	TCP
SMTP	25	TCP
WHOIS	43	TCP
TACACS	49	TCP/UDP
DNS	53	TCP/UDP
Bootstrap Protocol (BOOTP) server	67	UDP
Bootstrap Protocol (BOOTP) client	68	UDP
TFTP	69	UDP
HTTP	80	TCP
Kerberos	88	TCP

Service	Port	Protocol
POP3	110	TCP
Sun RPC	111	TCP/UDP
NTP	123	UDP
NetBIOS (Name service)	137	TCP/UDP
NetBIOS (Datagram service)	138	TCP/UDP
NetBIOS (Session service)	139	TCP/UDP
IMAP	143	TCP
SNMP	161	UDP
SNMPTRAP	162	TCP/UDP
BGP	179	TCP/UDP
IRC	194	TCP/UDP
BGMP	264	TCP/UDP
LDAP	389	TCP/UDP
HTTPS	443	TCP
Microsoft DS	445	TCP/UDP
ISAKMP	500	TCP/UDP
rexec	512	TCP
rlogin	513	TCP
Who	513	UDP
rsh	514	TCP

Service	Port	Protocol
Syslog	514	UDP
Talk	517	TCP/UDP
RIP/RIPv2	520	UDP
Timed	525	UDP
klogin	543	TCP
Mac OS X Server administration	660	TCP/
Spamassassin	783	TCP
rsync	873	TCP
IMAPS	993	TCP
POP3S	995	TCP
SOCKS	1080	TCP
Nessus	1241	TCP
IBM Lotus Notes	1352	TCP
Timbuktu-srv1	1417 to 1420	TCP/UDP
MS SQL	1433	TCP
Citrix	1494	TCP
Oracle default listener	1521	TCP
Ingres	1524	TCP/UDP
Oracle common alternative for listener	1526	TCP
PPTP	1723	TCP/UDP

Service	Port	Protocol
radius	1812	TCP/UDP
Cisco SCCP	2000	TCP/UDP
NFS	2049	TCP
Openview Network Node Manager daemon	2447	TCP/UDP
Microsoft Global Catalog	3268	TCP/UDP
MySQL	3306	TCP
Microsoft Terminal Service	3389	TCP
NFS-lockd	4045	TCP
SIP	5060	TCP/UDP
Multicast DNS	5353	UDP
PostgreSQL	5432	TCP
PCAnywhere	5631	TCP
VNC	5900	TCP
X11	6000	TCP
ArcServe	6050	TCP
BackupExec	6101	TCP
Gnutella	6346	TCP/UDP
Gnutella alternate	6347	TCP/UDP
IRC	6665 to 6670	TCP
Web	8080	TCP

Service	Port	Protocol
Privoxy	8118	TCP
Polipo	8123	TCP
Cisco-xremote	9001	TCP
Jetdirect	9100	TCP
Netbus	12345	TCP
Quake	27960	UDP
Back Orifice	31337	UDP