CEH/Pentest+ Helpful Links

Supporting information to be used to help study for CEH and Pentest+
Extra information included for continuing study and further development

Contents

10 Commandments of Ethical Hacking

https://en.wikipedia.org/wiki/Ten_Commandments_of_Computer_Ethics

Important NIST Publications

https://csrc.nist.gov/publications
NIST Computer Security Resource Center Publications homepage

https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments

https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final
NIST SP 800-34, Rev. 1, Contingency Planning Guide for Federal Information Systems

https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
NIST SP 800-37, Rev. 2, Risk Management Framework for Information System and Organizations: A System Life Cycle Approach for Security and Privacy

https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
NIST SP 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems (IS) and Organizations

https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final
NIST SP 800-88, Rev. 1, Guidelines for Media Sanitization: clear, sanitize, destroy

https://csrc.nist.gov/publications/detail/sp/800-115/final
NIST SP 800-115, Technical Guide to Information Security Testing and Assessment

US Laws (for Pentest+)

https://www.govinfo.gov/content/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap47-sec1029.pdf
US Code 2011, Title 18, Chapter 47, Section 1029 – governs fraud and related activity in connection with access devices (e.g. using a counterfeit or illegally modifying an access device, or creating/obtaining unauthorized access credentials)

https://www.govinfo.gov/content/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap47-sec1030.pdf
US Code 2011, Title 18, Chapter 47, Section 1030, governs fraud and related activity in connection with computers (e.g. accessing a computer without authorization or elevating privileges beyond authorized levels, illegally causing a system damage through unauthorized access, or using unauthorized access credentials)

Vulnerability Research

https://attack.mitre.org
MITRE database that contains a knowledge base of adversary tactics and techniques that have been observed live in the wild, sorted by category and then by process

https://resource.elq.symantec.com/LP=6819?inid=symc_threat-report_istr_to_leadgen_form_LP-6819_ISTR-2019-report-main&cid=70138000001Qv0PAAS
Symantec ISTR (Internet Security Threat Report) for 2019, an analysis of types of attacks against targets, techniques of the attacks and the probability or frequency of success, free to download after completing information form

https://cve.mitre.org/
MITRE CVE database

https://nvd.nist.gov/
National Vulnerability Database, managed by NIST

https://www.securityfocus.com/bid
Large vulnerability database, searchable by vendor or by CVE, managed by Symantec

http://cwe.mitre.org/
Common Weakness Enumeration database, managed by MITRE

http://capec.mitre.org/
Common Attack Pattern Enumeration and Classification database, managed by MITRE

Metasploit Module Tree

https://github.com/rapid7/metasploit-framework/tree/master/modules
Metasploit Framework utilities in a browsable file tree, reference only

NMAP Scanning/Netcat usage

https://nmap.org/book/man-briefoptions.html
NMAP options summary (man page)

https://nmap.org/book/performance-timing-templates.html
NMAP default timing templates for each scan speed (in a table)

https://nmap.org/book/man-port-scanning-basics.html
NMAP port state explanations when returned by a scan

http://man7.org/linux/man-pages/man1/ncat.1.html
Ncat options summary (man page)

Pentesting Tools Usage Cheat Sheets

https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/
Penetration testing tools cheat sheet, ordered by testing stage and use, with examples and some syntax

http://0daysecurity.com/penetration-testing/enumeration.html
List of tools to use for service enumeration, ordered by service name and use with some syntax and examples

Impacts on Business – Definitions (BCP, BIA, DRP)

https://www.ready.gov/business/implementation/continuity
BCP – business continuity plan

https://www.ready.gov/business-impact-analysis
BIA – business impact analysis

https://www.ready.gov/business/implementation/IT
DRP – disaster recovery plan

https://www.flashcardmachine.com/ceh-certifiedethicalhacker31250businesscontinuitypl.html
Flashcards with basic information on all business impact terms for CEH

CEH Supporting Test Information

https://medium.com/@petergombos/lm-ntlm-net-ntlmv2-oh-my-a9b235c58ed4
Windows versions and the hashes used in each, an explanation of all Windows hashes and their uses

https://support.microsoft.com/en-us/help/243330/well-known-security-identifiers-in-windows-operating-systems
Well-known security identifiers in Windows OS

http://www.pearsonitcertification.com/articles/article.aspx?p=1868080
List of common port numbers and services
*Note: not included – port 445 – used for NetBIOS null sessions and the SMB service (major vulnerabilities used recently by WannaCry and other high-profile ransomware and trojan malware)

https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml
ICMP parameters in full

https://www.lifewire.com/top-network-routing-protocols-explained-817965
Dynamic routing protocols explained

https://www.solarwindsmsp.com/blog/stateful-vs-stateless-firewall-differences
Stateful vs Stateless packet filtering by firewalls
https://www.cryptomathic.com/news-events/blog/differences-between-hash-functions-symmetric-asymmetric-algorithms
Symmetric and Asymmetric cryptology differences

Pentest+ Supporting Test Information

http://www.cengage.com/resource_uploads/downloads/143548360X_429597.pdf
Sample Pentest Agreement form, legal signoff by company to begin

https://pentest-tools.com/public/Terms-of-Service.pdf
Sample Pentest MSA (Master Service Agreement also/or Terms of Service)

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/CMS-Penetration-Testing-Rules-of-Engagement-Template.html
Sample Pentest RoE (Rules of Engagement)

http://www.pentest-standard.org/index.php/Pre-engagement#Rules_of_Engagement
Detailed list on pre-engagement requirements, before the pentest begins

https://rhinosecuritylabs.com/penetration-testing/four-things-every-penetration-test-report/
Reporting – what every post-action report should contain at a minimum

http://www.pentest-standard.org/index.php/Reporting
More detailed list on suggested report contents

https://dsxte2q2nyjxs.cloudfront.net/reporting_guide.pdf
Another detailed reporting “guide” for Pentesting
*Note: this guide also includes guides on what you need BEFORE a pentest as well

https://en.wikipedia.org/wiki/Export_of_cryptography_from_the_United_States
The International Traffic in Arms Regulation restricts (but does not totally forbid) the export of certain types of cryptography from the US

https://en.wikipedia.org/wiki/IEEE_802
IEE 802.x standards list, know 802.3 (Ethernet), 802.11 (Wireless) and 802.15 (Bluetooth and PAN, personal area networks) at the very lease

Post-class Resources

Privacy/Anonymity, Operating Systems and Search Engines

https://tails.boum.org/index.en.html
Tails Project page, an operating system designed for privacy and anonymity

https://www.kali.org/
Kali Project page, the most popular operating system used by Pentesters and hackers, maintained by Offensive Security

https://kali.training/downloads/Kali-Linux-Revealed-1st-edition.pdf
Kali Linux Revealed, Kali Project's inclusive how-to for building, optimizing and using Kali, also one of the text books for the Penetration Testing with Kali Linux certification (highly recommended before attempting OSCP)

https://www.torproject.org/
Tor Project page, browser designed for privacy and anonymity (included on Tails and Kali by default)

https://duckduckgo.com/
Search engine, super anonymous

http://www.metacrawler.com/
Metasearch engine, a search engine that searches other search engines for information and aggregates that information into a single set of results, also serves to hide your searches from being tracked

https://www.shodan.io/
Shodan, a search engine for the Internet of Things (IoT), used to discover and track devices that are directly connected to the internet (includes things like smart TVs and refrigerators that are connected to a home Wi-FI, and security systems/cameras that have web management access)

Coding/Scripting Help and Reinforcement/Training

http://www.tutorialspoint.com/codingground.htm
Online terminals, compilers and interpreters for dozens of languages, does not require client software for compiled languages like Java and C or interpreter software for languages like Perl or Python

https://www.w3schools.com/
Various coding tutorials, including HTML, XML, CSS, JavaScript, SQL, PHP, Python, Java and C++ with references and exercises

https://www.codewars.com/dashboard
Sign up for a free account and attempt coding challenges in various languages that have been created by the community, does not require client software
http://linuxcommand.org/index.php
Look in left window pane for guided lessons on Linux command line (shell) and guided lessons on writing shell scripts

https://www.w3schools.com/tags/ref_urlencode.asp
HTML URL Encoding reference

Pentesting Tools

https://sectools.org/
Top 125 network security tools, to note (mostly all freeware), to note: Wireshark, Metasploit, Aircrack, Snort, Cain & Abel, Netcat, tcpdump, John the Ripper, NetStumbler, PuTTY, Burp Suite, Nikto, Hping, Sysinternals Suite, nmap

https://www.paterva.com/buy/maltego-clients/maltego-ce.php
Maltego CE, a data mining tool that renders graphs for link analysis between target relationships, capable of automatic information gathering (limited) from places like social media and can discover registered accounts and emails and phone numbers, freeware after free site registration
*Note: read the documentation (link at the top of the page) carefully to understand how to use and manipulate "transforms"

https://docs.microsoft.com/en-us/sysinternals/
"Windows" Sysinternals home page, look for downloads in the left pane or use them directly from the cloud at https://live.sysinternals.com/.
*Note: you can download these tools from the command line (maybe after getting a shell on a target?) using wget on Linux or bitsadmin on Windows (native). Example to download psexec to your current working directory on Linux: wget https://live.sysinternals.com/psexec.exe

https://defcon.org/html/links/dc-tools.html
Archive list of downloadable tools that have been released at DEFCON

Open Source Intelligence Gathering

https://www.exploit-db.com/google-hacking-database
Google Hacking Database, use the search bar to find results based on keywords

https://osintframework.com/
Clickable, expandable list of resources to use for open source intelligence gathering, take special note of the Exploits & Advisories and Threat Intelligence sections near the bottom of the list

https://www.osinttechniques.com/osint-tools.html
Open Source Intelligence tools, a huge list of open source information gathering resources

https://dnslytics.com/
Domain search, DNS lookup, whois lookup, reverse IP, SPF lookup, traceroute, ping, MX and NS lookup

Password Lists and INFOSEC Resources

https://github.com/danielmiessler/SecLists/tree/master/Passwords
TONS of password lists that you can download and use, available to download through web or through command line tools directly to your box

https://infocon.org/
Digital archive of every hacking conference presentation or talk going back decades, also includes documentaries and podcasts
*Note: also available: precompiled rainbow tables (with software to create your own) and a decent number of wordlists (some of them are massive 10+ GB)

Pentesting Practice

https://www.hackthebox.eu/
"Hack" into the website for an invite code (requires source code review and XSS scripting of sorts), user-created machines that you can practice against and compare strategies/results with others and gain ranks according to the difficulty and number of machines you compromise, totally anonymous
*Note: ALWAYS use OpenVPN from a non-volatile (USB) or virtual machine to connect to these machines, you are given a generated connection profile to download for use
*Note 2: There is a "careers" section where companies will post job offers. You can only apply to the jobs if your minimum rank matches or exceeds the requirements of the offer, and you can provide contact details directly and only to the poster if you wish them to contact you

https://www.root-me.org/?lang=en
Hundreds of challenges and whole environments, each challenge has a multitude of solutions by other users

http://overthewire.org/wargames/
Online-only Web Application vulnerability challenges presented in the form of games

https://www.vulnhub.com/
Download intentionally vulnerable whole virtual machines to practice against at home, you will need a VM client (VMWare, Hyper-V, VirtualBox). These machines do not contain malicious code or programs but take appropriate precautions anyway

https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project
WebGoat, an intentionally vulnerable web application, where different parts of the websites are vulnerable to different types of attacks, maintained by OWASP

Professional Development – The Road to OSCP

https://www.netsecfocus.com/oscp/2019/03/29/The_Journey_to_Try_Harder-_TJNulls_Preparation_Guide_for_PWK_OSCP.html
The single best and most comprehensive guide I've ever seen on how to pass the OSCP