View Recommended Resources

This document shows all the links from each chapter plus some extra resources that you might find useful. Keep in mind that Internet links can change over time, and resources can be moved or removed from the Internet without notice. If the link does not work, try searching in your search engine for the resource in question or a similar resource to take its place.

Chapter 1

AAA RFC documents: http://tools.ietf.org/wg/aaa/

Chapter 2

For readers who want to brush up on their CompTIA A+ or Network+ topic, see my personal website: www.davidlprowse.com

Windows Firewall with Advanced Security tutorial: http://www.davidlprowse.com/articles/?p=896

ZoneAlarm Firewall: http://www.zonealarm.com/software/free-firewall/

TrendMicro HouseCall: https://www.trendmicro.com/en_us/forHome/products/housecall.html

Malwarebytes Anti-Malware: https://www.malwarebytes.com/

Microsoft Safety Scanner: https://www.microsoft.com/en-us/wdsi/products/scanner

Spybot Search & Destroy: https://www.safer-networking.org/private/

Knoppix Live Linux CD/DVD: http://knoppix.net/

Barracuda Networks: https://www.barracuda.com/

chkrootkit (for Unix-based systems): http://www.chkrootkit.org/

Microsoft: “Windows BitLocker Drive Encryption Step-by-Step Guide”: https://technet.microsoft.com/en-us/library/cc766295(WS.10).aspx

National Cyber Alert System links:

- https://www.us-cert.gov/ncas/tips/ST05-017
- https://www.us-cert.gov/ncas/tips/ST04-020

Chapter 3

Open Source HIDS SECurity (OSSEC): https://ossec.github.io/

Verisys File Integrity Monitoring: https://www.ionx.co.uk/products/verisys

Tripwire File Integrity Monitoring: https://www.tripwire.com/products/tripwire-file-integrity-manager/

Adblock Plus (add-on): https://adblockplus.org/en/chrome

IronKey: http://www.ironkey.com/en-US/

Chapter 4

Linux MAN pages: https://linux.die.net/man/

VirtualBox: https://www.virtualbox.org/wiki/VirtualBox

VMware Workstation Player: https://my.vmware.com/en/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/12_0

Windows Virtual PC: https://www.microsoft.com/en-us/download/details.aspx?id=3702

Microsoft: “Hyper-V Security Guide”: https://technet.microsoft.com/en-us/library/dd569113.aspx

Using and securing VMware:
https://www.vmware.com/products/vsphere.html#resources

Chapter 5

Firefox add-on links:

- Adblock Plus Firefox add-on: https://addons.mozilla.org/en-US/firefox/addon/adblock-plus/
- NoScript Firefox add-on: https://addons.mozilla.org/en-US/firefox/addon/noscript/

FileZilla Server download: https://filezilla-project.org/download.php?show_all=1&type=server

FileZilla Client download: https://filezilla-project.org/download.php?show_all=1

CERT Secure Coding Tools: http://www.cert.org/secure-coding/tools/

Chapter 6

For readers who wish to brush up on their networking topics:

- Video: "OSI Model Primer": http://www.davidlprowse.com/articles/?p=905
- Barker, Keith. *CompTIA Network+ Cert Guide* (First Edition)
- Comer, Douglas. *Computer Networks and Internets* (Sixth Edition). Prentice Hall. 2014
- TCP/IP Protocol Architecture: https://technet.microsoft.com/en-us/library/cc958821.aspx

Pure-FTPd: https://www.pureftpd.org/project/pure-ftpd

FileZilla: https://filezilla-project.org/

More information on SYN flood attacks:
https://tools.ietf.org/html/rfc4987

Microsoft Security Bulletin: "Vulnerabilities in Kerberos Could Allow Elevation of Privilege (2496930)":
https://technet.microsoft.com/library/security/ms11-013

> **NOTE** For more vulnerabilities to IIS (and other Microsoft software), visit the Security TechCenter and bookmark the following link: https://technet.microsoft.com/en-US/security/bb291012.

> **NOTE** A list of common vulnerabilities and exposures (CVE) to Apache HTTP Server (and the corresponding updates) can be found at the following link: http://httpd.apache.org/security/vulnerabilities_22.html.

Chapter 7

Port numbers: http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

Video: "TCP, UDP, and Ports Refresher":
http://www.davidlprowse.com/articles/?p=911

Nmap: https://nmap.org/

Ncat: https://nmap.org/ncat/

GRC's ShieldsUP!: https://www.grc.com/x/ne.dll?bh0bkyd2

Chapter 8

Video: “Setting up virtual servers and port forwarding on a typical SOHO router/firewall”: http://www.davidlprowse.com/articles/?p=916

Adding firewall rules with `netsh.exe`: https://technet.microsoft.com/en-us/library/dd734783(v=ws.10).aspx

iptables MAN page: http://ipset.netfilter.org/iptables.man.html

Chapter 9

NetStumbler: http://www.netstumbler.com/

The Password Meter: http://www.passwordmeter.com/

Kaspersky Secure Password Check: https://password.kaspersky.com/

Chapter 10

Recommended reading:

HID door access control systems:
https://www.hidglobal.com/products/readers

802.1X links:

- Official IEEE 802.1X PDF download: http://standards.ieee.org/getieee802/download/802.1X-2004.pdf
- Intel: “Wireless Networking” (802.1X overview): https://www.intel.com/content/www/us/en/support/network-and-i-o/wireless-networking/000006999.html
- Cisco: “Deploying 802.1X Technology with Cisco Integrated Services Routers”: http://www.cisco.com/en/US/prod/collateral/routers/ps5853/prod_white_paper0900aecd806c6d65.html

LDAP links:

- IETF Technical Specifications (RFC 4510): https://tools.ietf.org/html/rfc4510
- Microsoft: “How to enable LDAP over SSL with a third-party certification authority”: https://support.microsoft.com/en-us/help/321051/how-to-enable-ldap-over-ssl-with-a-third-party-certification-authority

Kerberos links:

- Microsoft: “Kerberos Explained”: https://technet.microsoft.com/en-us/library/bb742516.aspx
- “Kerberos: The Network Authentication Protocol”: http://web.mit.edu/Kerberos/

RADIUS and TACACS+ links:

- Microsoft: “RADIUS Protocol Security and Best Practices”: https://technet.microsoft.com/en-us/library/bb742489.aspx
- The FreeRADIUS Project: http://freeradius.org/
- Cisco: “TACACS+ and RADIUS Comparison”: http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml

Chapter 11

Password and UAC resources:

- Microsoft: “Best Practices for Enforcing Password Policies”: https://technet.microsoft.com/en-us/library/ff741764.aspx
- Microsoft: “Password Policy”: https://technet.microsoft.com/en-us/library/hh994572(v=ws.11).aspx

- Microsoft: “User Account Control Step-by-Step Guide”: https://technet.microsoft.com/en-us/library/cc709691(WS.10).aspx

Microsoft: “Interactive logon: Do not require CTRL+ALT+DEL”: https://docs.microsoft.com/en-us/windows/device-security/security-policy-settings/interactive-logon-do-not-require-ctrl-alt-del

“Department of Defense Trusted Computer System Evaluation Criteria” (TCSEC), a.k.a. The Orange Book: http://csrc.ncsl.nist.gov/publications/secpubs/rainbow/std001.txt

Department of Defense Directive 8500.01E (replacement for the TCSEC): http://dodcio.defense.gov/Portals/0/Documents/DIEA/850001p.pdf

“An Introduction to Role-Based Access Control” (NIST/ITL bulletin): http://csrc.nist.gov/groups/SNS/rbac/documents/design_implementation/Intro_role_based_access.htm

Chapter 12

ISO 31000:2009: “Risk Management—Principles and Guidelines” download: https://www.iso.org/standard/43170.html

Open Source Security Testing Methodology Manual (OSSTMM) download: http://www.isecom.org/research/osstmm.html

NIST Special Publications: http://csrc.nist.gov/publications/PubsSPs.html

Open Vulnerability and Assessment Language repository website: http://oval.mitre.org/

Network Topology Mapper trial download: http://www.solarwinds.com/network-topology-mapper

Microsoft Visio trial: https://products.office.com/en-au/visio/visio-professional-free-trial-flowchart-software

Spiceworks: https://www.spiceworks.com/app/

PRTG Network Monitor: https://www.paessler.com/prtg

Nessus Vulnerability Scanner: http://www.tenable.com/products/nessus-vulnerability-scanner/nessus-professional

Nmap: https://nmap.org/

Wireshark protocol analyzer: https://www.wireshark.org/

Chapter 13

Windows Server 2008: Windows Reliability and Performance Monitor: https://technet.microsoft.com/en-us/library/cc755081(WS.10).aspx

Wireshark protocol analyzer: https://www.wireshark.org/

Microsoft Network Monitor 3.4: https://support.microsoft.com/en-us/help/933741/information-about-network-monitor-3

Microsoft System Center Configuration Manager (SCCM) 2007: https://www.microsoft.com/en-us/cloud-platform/system-center-configuration-manager

Windows Server "Manage Event Logs": https://technet.microsoft.com/en-us/library/cc766178(v=ws.11).aspx

Microsoft, administrative shares: https://support.microsoft.com/en-us/help/954422/how-to-remove-administrative-shares-in-windows-server-2008

Chapter 14

Recommended books:

Applied Crytograph: Protocols, Algorithms, and Source Code in C. Schneier, Bruce. Wiley, 1996.

Introduction to Modern Cryptography: Principles and Protocols. Katz, Lindell. Chapman and Hall, 2007.

Cryptography Demystified. Hershey. McGraw-Hill Professional, 2002.

Archived: *Schneier on Security*. Schneier. Wiley, 2008.NIST: "Data Encryption Standard (DES)": http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

NIST: "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher": http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-67r1.pdf

NIST: "Advanced Encryption Standard (AES)": http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

Microsoft: "Configure Server Authentication and Encryption Levels": Concerns RDS Encryption: https://technet.microsoft.com/en-us/library/cc770833.aspx

RSA Public Key Cryptography Standards (PKCS): https://www.emc.com/emc-plus/rsa-labs/standards-initiatives/public-key-cryptography-standards.htm

RSA Laboratories: RC6 Block Cipher: https://www.emc.com/emc-plus/rsa-labs/historical/rc6-block-cipher.htm

Disabling the storage of LM hashes in Windows: https://support.microsoft.com/en-us/help/299656/how-to-prevent-windows-from-storing-a-lan-manager-hash-of-your-passwor

Bruce Schneier Blog: https://www.schneier.com/

Microsoft TechNet: Pass-the-Hash video: https://technet.microsoft.com/en-us/security/dn785092

Chapter 16

Intel PRO/1000 MT Dual Port Server Adapter: https://www.intel.com/content/www/us/en/products/network-io/ethernet/gigabit-adapters.html?eu-cookie-notice

Microsoft: “How multiple adapters on the same network are expected to behave”: https://support.microsoft.com/en-us/help/175767/how-multiple-adapters-on-the-same-network-are-expected-to-behave

Microsoft: “Data Backup and Recovery”: https://technet.microsoft.com/en-us/library/bb727010.aspx

Chapter 17

DuPont FM-200 web page: https://www.chemours.com/FE/en_US/products/FM200.html

Chapter 18

ISO/IEC 27002:2013: https://www.iso.org/standard/54533.html

ISO 9001:2008: “Quality management systems–Requirements”: https://www.iso.org/standard/62085.html

NIST: Computer Security Incident Handling Guide: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NIST: Framework for Improving Critical Infrastructure Cybersecurity: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Privacy Act of 1974: http://epic.org/privacy/laws/privacy_act.html

SpinRite data recovery software: https://www.grc.com/sr/spinrite.htm

Kroll Ontrack data recovery software: https://www.krollontrack.com/products/data-recovery-software/

Journal of Digital Forensics, Security and Law:
http://commons.erau.edu/jdfsl/

The International Journal of Forensic Computer Science:
http://ijofcs.org/