AUD 507 Tools Quickreference

Tool	Site	Description
AccessEnum	https://technet.microsoft.com/en-us/Library/bb897332.aspx	A free Microsoft tool for enumerating domain level shares with permissions.
Autoruns	https://technet.microsoft.com/en-us/sysinternals/bb963902.aspx	A free Microsoft tool for enumerating all processes/programs/applications/services that are configured to autorun on a Windows system.
Burp Suite	http://portswigger.net	Web Application Auditing/Security Testing tool. Very full featured. Java based. Supports virtually any test you might want to run against a web application with some advanced cryptographic attacks for session stores. Commercial tool with a yearly license fee.
Cain & Abel	http://oxid.it	Cain & Abel is a password assessment tool. It is very common for this tool to set of antivirus and malware reporting software though the software will not do anything on its own. It is capable of breaking most types of passwords in addition to being useful in both sniffing and breaking CHAP, NTLM and NTLMv2 authentications.
Calculate Sample Size & Margin of Error	https://github.com/dhoelzer/AuditcastsScripts/tree/master/Statistics	Spreadsheet to easily calculate standard sample sizes and measure margin of error.
CSDiff	http://www.componentsoftware.de/Products/CSDiff/download.htm	This is a free visual comparison tool. Two files can be opened simultaneously and visually compared for differences. Very useful in identify baseline variations.
diffutils	http://www.gnu.org/software/diffutils/	These are the canonical difference analysis utilities from the Free Software Foundation
DumpEVT	http://www.systemtools.com/somarsoft/?somarsoft.com	DumpEVT is a free tool from Somarsoft software. It allows you to dump selected event logs from the command line of a Windows system. This is an older tool for older systems that you might have. WMIC is a far better option for extract logs at a command line.
DumpUsers	http://ntsecurity.nu/toolbox/dumpusers/	This is an older tool that can be used to dump user and group information without credentials from improperly configured Windows domains.
GHDB	http://www.hackersforcharity.org/ghdb/	Somewhat out of date... Useful database of queries that can be run into Google to discover misconfigured and vulnerable applications. See also "Googledorks"
GoogleDorks	http://www.exploit-db.com/google-dorks/	Up to date database of useful queries that can be run using Google to discover misconfigured and vulnerable applications. See also GHDB.

hping3	http://www.hping.org	Network experimentation and testing tool. Allows you to create arbitrary packets using command line arguments.
Hydra	https://www.thc.org/thc-hydra/	Hydra is an excellent GUI based password brute forcing tool. PLEASE NOTE that the version on the USB stick is quite old. There are no official distributions available for the binary version of Hydra on Windows today. You must either use the old version or create a build environment to compile the most recent version. As of this writing Hydra is at version 8.1.
InSSIDer	http://www.metageek.com/products/inssider	Wireless LAN analysis tool for network discovery and signal analysis.
J-Baah	https://github.com/sensepost/JBaah	FOSS (Java based) tool for fuzzing and attacking session IDs within web applications.
Mapper.rb	http://github.com/dhoelzer/AuditcastsScripts/tree/master/DNS	DNS Auditing tool written in Ruby. Enumerates host names by directly querying a DNS server. Can be used to discover sites that have failed to configure a Split DNS.
Nemesis	http://nemesis.sourceforge.net	Network experimentation and testing tool. Allows you to create arbitrary packets using command line arguments. Advantage over Hping is that it does not wait for responses.
NetScanTools Pro	http://www.netscantools.com	A commercial Windows based tool that provides the ability to perform most tests that an auditor would want to run against virtually any network service including SMTP, DNS, SNMP and others.
Nipper	https://code.google.com/p/nipper-ng/	The version in the link is not exactly what's provided on the DVD. This tool is pretty hard to find these days since it has gone commercial. Wonderful tool for analyzing the configuration of most routers, switches and firewalls.
Nipper Studio	https://www.titania.com	Commercial version of Nipper. (See Nipper)
Nmap	http://insecure.org	The gold standard of network scanning tools. Available for most platforms including Windows. Many find the Windows version to be unreliable.
Nmap Tools	http://www.unspecific.com/nmap/	Set of scripts and automation tools to configure automatic network scans using Nmap. Also provides very handy reporting and searching tools for accessing the data.
OWASP ZED Attack Proxy	https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project	Web application proxy tool that is the successor to WebScarab. Java based tool. Supports most features offered by WebScarab but not all; offers a few features WebScarab doesn't.
PAE (Packet Analysis Engine)	http://enclaveforensics.com	Generate statistical data from raw packet captures. Source of the screenshot on Day 1 with the "Network Traffic Baseline" image.

PBNJ	http://pbnj.sourceforge.net	Ports Binaries & Junk - Nmap automation scripts with a basic database backend and interface for managing results and producing simple reports.
PCI Validation Tools	http://github.com/dhoelzer/Auditcasts Scripts/tree/master/PCI	Set of Perl and Bash scripts that automate the validation requirement of a firewall according to the PCI/DSS standard. Also includes a script to extract SSL Cipher details and add them to the report.
Perms	https://technet.microsoft.com/en-us/library/Cc786603(v=WS.10).aspx	Perms is a free Windows resource kit tool for determining the permissions that a particular user or group has to a file, directory or tree.
ProcessExplorer	https://technet.microsoft.com/en-us/sysinternals/bb896653.aspx	Process Explorer is a free tool from Microsoft that is extremely useful for analyzing running processes on a Windows system.
PSTools	https://technet.microsoft.com/en-us/sysinternals/bb896649.aspx	PSTools is a set of free tools useful for retrieving many types of information out of a Windows system both locally and remotely. Original created by Winternals.com, they are now officially Microsoft tools.
Putty	http://www.chiark.greenend.org.uk/~sgtatham/putty/	Putty is a free Telnet, FTP, SFTP and Secure Shell client.
SSH	See Putty	
Strings	http://en.wikipedia.org/wiki/Strings_(Unix)	UNIX command line tool for extracting printable strings from arbitrary input.
Visual Regex	http://laurent.riesterer.free.fr/regexp/	Visual Regexp is a Windows GUI tool that makes the design and modification of regular expressions interfactive.
VLC	http://www.videolan.org/vlc/index.html	VLC is Video Lan Client. This is a very well known and very popular free video and audio rendering application that is available for most platforms.
VMWare Player	http://www.vmware.com	Free virtualization platform for using pre-made virtual machines.
VMWare vSphere	http://www.vmware.com	Management client for the VMWare ESXi Hypervisor and vCenter management server.
WebScarab	https://www.owasp.org/index.php/Category:OWASP_WebScarab_Project	Full featured web application audit/attack tool. FOSS tool written in Java. Project has stalled.
Wikto	http://sensepost.com	Free windows interface to the Nikto web application scanner. Basic scanner that can identify most configuration issues.
Windows Server 2003 AdminPak	https://www.microsoft.com/en-us/download/details.aspx?id=16770	The Windows 2003 AdminPak is a set of useful administration tools and control panels that can be installed on a Windows workstation to allow easy administration of a Windows server or domain. While older, this remains a very useful toolkit since the more modern versions support a very limit set of operating systems.

Wireshark	http://wireshark.org	FOSS sniffer. Widely considered to be the best sniffer currently available. A great tool for understanding precisely what is happening on a network and for collecting a copy of everything that you do during a vulnerability scan.
Yersinia	http://www.yersinia.net	Layer 2 and VLAN attack/testing tool. DANGEROUS. :)