* Antimalware
* EMET
  + Includes DLP capabilities
  + ASLR: prevents buffer overflows
* Sysinternals
* Syslog
  + 7 = debugging
  + 0 = emergencies
  + USe central monitoring system
  + Syslog & Kiwi Syslog
* Syslog-ng: provides greater capabilities than syslog
  + Can write to a database, greater formatting support and flow control
* SIEM
  + ArcSight
  + QRadar
  + Splunk
  + AlienVault
  + OSSIM (AlienVault open source product)
* Splunk
  + Large scale data analysis
* AlienVault USM
  + SIEM, asset discover, vuln scanning/assessment, behavior analysis
* OSSIM
  + Open source
  + Includes:
    - OpenVAS
    - Suricata IDS
    - Nagios monitoring
    - OSSEC host IDS
    - Munin traffic analysis
    - FProbe netflow
* Network monitoring
  + Cacti
    - Uses RRDtool data logging
    - Polls network devices on a regular basis, can pull SNMP data
    - Relatively dated
  + SolarWinds Orion
    - Centralized monitoring
    - Network monitoring, flows, support for other monitoring
  + Netflow analyzer
    - Commercial
  + Nagios
    - Both open source (Nagios Core) and commercial versions
    - One of the most popular monitoring tools
  + MRTG
    - Multi Router Traffic Grapher, uses SNMP to monitoring traffic on network connections
    - Also PRTG
* Scanning
  + NMAP
* Network vulnerability scanning
  + Nessus
  + QualysGuard
  + Nexpose
  + OpenVAS (free)
  + MBSA (not supported any longer)
* Web application scanning
  + Nikto: open source
* Exploit frameworks
  + Metasploit
  + Can integrate with NexPose and Nessus
* Password cracking/recovery
  + Fgdump
  + Pwdump
  + SAMdump2
* Password/hashing cracking
  + John the ripper (open source)
    - Can be used against linux, windows, kerberos and more
  + Cain and Abel (windows)
    - May be outdated, yet very powerful
  + Ophcrack
    - Uses large set of rainbow tables
* Firewalls
  + Check point
  + Palo Alto
  + Cisco
  + Juniper
* IDS
  + Snort
  + Firepower/Sourcefire
  + Bro
* File integrity monitoring
* Packet capture
  + Wireshark
  + tcpdump
  + Aircrack-ng (wireless)
* Command line tools
  + Netstat (network connections)
  + Ping
  + Traceroute
  + Ipconfnig (ifconfig on mac)
  + nslookup
  + Dig (nslookup for Linux/MacOS, provides more detail than nslookup)
* Proxy servers
  + Content filtering
  + Caching
  + Kproxy (anonymous proxy)
* OpenSSL
* Web application firewalls
  + Site Defender
  + CloudFlare
  + F5 ASM
  + Fortinet Fortiweb
  + SecureSphere
  + AppWall
  + NAXSI (open source)
  + ModSecurity (open source)
  + WAF as a service
    - Cloudflare
    - Radware
    - AWS
* Interception proxies
  + Zed attack proxy
  + Burp Proxy
  + Vega
* Fuzzers
  + Peach fuzzer
  + Untidy fuzzer (part of the peach toolkit)
  + Minifuzz file fuzzer
  + SDL regex fuzzer
* Forensics tools
  + Hashing
    - MD5 (in linux: md5sum)
    - SHA (in linux: shasum)
  + Imaging formats
    - RAW
    - AFF
    - E01
  + Standalone imaging utilities
    - Dd (built into linux and unix)
    - OSFClone (free bootable imaging tool)
    - FTK imager
  + Forensic suites
    - FTK, provides GUIs (commercial)
    - EnCase (commercial)
    - SANS SIFT, built using open source tools and based on Ubuntu
      * Provides timeline and other useful capabilities
    - Sleuthkit (CLI) and Autopsy (GUI)
    - Helix 3 Enterprise and Pro (commercial)
      * In bootable format
  + Mobile forensics
    - Cellebrite
    - SecureView
    - Forensic Analyst
    - Mobile Forensic Bundle
* Port scanners
  + NMAP/zenmap
  + Angry IP scanner (install fetchers)
* Metasploit
* Vulnerability scanners
  + Nessus
  + Qualysguard
  + Nexpose
  + OpenVAS
  + Nikto
  + MS Baseline Security Analyzer
* Netflow analyzers
  + PRTG
  + SolarWinds
* Cisco, Palo Alto, and Check Point firewalls,
  + Show log
  + <https://www.cisco.com/c/en/us/about/security-center/identify-incidents-via-syslog.html>
* Packet capture
  + Wireshark
* Utilities
  + Netstat
  + Sysinternals
* Information gathering
  + theHarvester: uses search engines to gather information about targets
  + Maltego: builds relationship maps
  + Shodan
* Powershell commands
  + Netsh wlan/lan show profiles
  + netsh wlan show profile WiFi-name key=clear
    - wlan show profile galileo key=clear
  + Netstat -o
  + Get-process -ID (PROCESS-ID)
  + Netstat -e
  + rsop
  + Netstat -nr
* Image metadata: Exiftool
* Immersion: email information gathering
* Historical website information
  + <http://timetravel.mementoweb.org/>
  + <https://archive.org/>
* Social engineering
  + Social engineering toolkit (SET)
  + Creepy
  + Metasploit
* Dig DNS tool
* ITSM
* <https://bgp.he.net/>
* Debugging
  + Windbg