RSC
Ripple Software Consulting

Pentest +
Pen-test Tools

Author: Joseph Lee
Email: joseph@ripplesoftware.ca
Mobile: 778-725-3206

Tool Use Cases

- Reconnaissance
- Enumeration
- Vulnerability scanning
- Credential attacks
- Persistence
- Configuration compliance
- Evasion
- Decompilation
- Forensics
- Debugging
- Software assurance

Categories of Pentest Software Tools

- Documentation
- Reconnaissance
- Scanners
- OSINT
- Remote Access
- Credential Testing
- Wireless
- Networking
- Debuggers
- Web proxies
- Mobile Tools
- Software Assurance Testing
- Social Engineering
- Exploitation Frameworks

Specific Tools By Category

Documentation

- **XML documentation**
  - **WSDL – Web Services Description Language**
    - RFC – https://www.w3.org/TR/2001/NOTE-wsdl-20010315
    - XML format for **describing functionality of network services**
    - Contains either **document-oriented** or **procedure-oriented** information
    - WSDL is extensible to work with any endpoint / protocol
  - **SOAP – Simple Object Access Protocol**
    - Info: https://www.w3schools.com/xml/xml_soap.asp
    - SOAP APIs work over **HTTP / HTTPS**
    - Documentation can describe the API
  - **XSD – XML Schema Definition Language**
    - W3C: https://www.w3.org/TR/xmlschema11-1/
    - Specifies how to formally describe the elements in an Extensible Markup Language (XML) document
    - Can provide detailed information about how a specific XML syntax works
- **API – Application Programming Interface documentation**
  - Various API standards come with their own syntax
  - **Swagger**
    - https://swagger.io
    - Open-source API tools
  - **Oracle Apiary**
    - https://apiary.io/
    - API Design Stack
  - **RAML**
    - https://raml.org/
    - RESTful API Modelling Language
    - Describing practically-RESTful APIs in a way that's highly readable

Information Sharing

- **dradis**
  - https://dradisframework.com/ce/
  - Open-source framework to enable team **sharing of information** red-team in a penetration test
  - **Web-application** keeps a centralized repository of information
  - Has **plugins** collect the output of a variety of network scanning tools, like **Nmap, Burp Suite,** and **Nikto**

Web-Application Scanners

- **W3af**
  - https://w3af.org/
  - Works on Mac, Linux, Windows
  - Extremely popular, powerful, and flexible framework for finding and exploiting **web-application vulnerabilities**
  - **Extensible** and features **dozens of web assessment and exploitation plugins**
  - Referred to as a web-based Metasploit
  - **Fuzzing** and **brute-force login** credential tools
- **WebScarab**
  - https://github.com/OWASP/OWASP-WebScarab
  - Works with Mac, Linux, Windows
  - Records the **requests and responses** between browser and web-servers
  - Allows the operator to review them in various ways
  - Exposes the workings of an HTTP(S) based application
  - Can assist **debugging** otherwise difficult problems
  - Allows security specialists to identify vulnerabilities in the web-application design or implementation
- **Arachni**
  - http://www.arachni-scanner.com/
  - FOSS for Mac, Linux, Windows
  - **Ruby framework** for evaluating the security of web-applications
  - Vulnerability scans **JavaScript / JQuery / AngularJS, HTML5, DOM manipulation and AJAX**
  - **Command line** and **WebUI**
  - **Vulnerability Scans** for
    - DOM-based vulnerabilities
    - XSS (with DOM variants)
    - SQL injection
    - NoSQL injection
    - Code injection
    - File inclusion variants
    - More
- **Subgraph Vega**
  - https://subgraph.com/vega/index.en.html
  - Written in Java
  - Free and open-source works with Mac, Linux, Windows
  - SQL Injection, Cross-Site Scripting (XSS), SSL/TLS security scans, inadvertently disclosed sensitive information, remote code execution
  - GUI based
- **OWASP Samurai Web-Testing Framework**

  - https://www.samurai-wtf.org/
  - Web-application testing framework
  - Live Linux VM image / environment that has been pre-configured to function as a web pen-testing environment
  - Contains good open-source and free tools that focus on testing and attacking websites
- **sqlninja**
  - https://tools.kali.org/vulnerability-analysis/sqlninja
  - Mac, Linux, Windows
  - Exploits web-applications that use **Microsoft SQL Server** as a database backend
  - Attempts to **attain a running shell** on the remote host
  - Doesn't find an SQL injection, but automates the exploitation after one is discovered
- **Wappalyzer**
  - https://www.wappalyzer.com/
  - Desktop and web-application GUI available
  - Scan a website for services and versions, **JS scripts, OS detection, and 3rd party software such as Google Analytics, Database version, source code language, CMS, web-server, etc.**
  - Extracts **social media accounts, email addresses, phone numbers, location information**
- **WebSurgery**
  - http://sunrisetech.gr/?page=websurgery&tab=overview
  - Windows Only
  - Suite of tools for security testing of web applications
  - Tools include crawler, bruteforcer, fuzzer, proxy, editor
- **FireFox Development**
  - https://getfirebug.com/
  - Mac, Linux, Windows
  - **Firefox Development** provides access to browser internals
  - Editing of **HTML and CSS, a DOM viewer,** and **JavaScript debugger**

Network Scanners

- **Nikto / Nikto 2**
  - https://cirt.net/Nikto2
  - Works on Mac, Linux, Windows with many plugins availble
  - Open-source scanner which performs comprehensive tests against **web servers** for multiple items
    - Lists over **6400** potentially **dangerous files/CGIs**
    - Checks for **outdated versions** of over **1200** servers
    - **Version specific** problems on over 270 servers

    - Checks for **server configuration**
        - Presence of multiple index files
        - HTTP server options
        - Attempt to identify installed web servers and software
- **OpenVAS**
    - https://www.openvas.org/
    - Open-source for Mac, Linux, Windows
    - **Vulnerability scanner** that was forked from Nessus
    - Plugins are still written in the **Nessus NASL language**
- **NetSparker**
    - https://www.netsparker.com/
    - Paid software for Mac, Linux, Windows
    - Support for both **detection** and **exploitation** of vulnerabilities
    - Aims to be **false positive–free** by only reporting confirmed vulnerabilities
- **QualysGuard**
    - https://www.qualys.com/qualysguard/
    - Popular SaaS vulnerability management software
    - Web-based UI offers **network discovery** and **mapping**
    - Asset prioritization, vulnerability assessment, and reporting
    - Remediation tracking according to business risk of asset value / priority
    - Scans handled by **Qualys appliances** that communicate to c**loud-based system**
- **MBSA – Microsoft Baseline Security Analyzer**
    - https://www.microsoft.com/security/blog/2012/10/22/microsoft-free-security-tools-microsoft-baseline-security-analyzer/
    - Designed to help **small and medium-sized businesses assess security** state
    - Accordance with Microsoft security recommendations
    - Built on the Windows Update Agent and Microsoft Update infrastructure
    - MBSA ensures consistency with
        - Microsoft Update (MU)
        - Windows Server Update Services (WSUS)
        - Systems Management Server (SMS)
        - Microsoft Operations Manager (MOM)
- **SQLMap**
    - https://sqlmap.org/
    - Automates the process of **detecting and exploiting SQL injection** flaws and taking over of back-end database servers
    - **Database fingerprinting**
    - **Extracting data** from the database
    - **Accessing the underlying file system** and **executing OS commands** via out-of-band connections
- **Nessus**

    - https://www.tenable.com/products/nessus
    - One of the most popular and capable vulnerability scanners, particularly for UNIX systems
    - Costs $2,190 per year
    - Free **Nessus Home** version is also available
    - Constantly updated, with more than **70,000 plugins**
    - **Remote and local** (authenticated) security checks
    - Client/server architecture with a **web-based interface**
    - **Embedded scripting language** for writing your own plugins or understanding the existing ones
- **Nexpose**
    - https://www.rapid7.com/products/nexpose/
    - Paid software as stand-alone, Metasploit plugin
    - Discovery, detection, verification, risk classification, impact analysis, reporting and mitigation
    - Integrates with Metasploit to give you a comprehensive vulnerability sweep
- **SolarWinds**
    - https://www.solarwinds.com
    - Paid software – costs about $1500
    - **Automated network discovery**
    - **Real-time monitoring and alerting**
    - Powerful diagnostic capabilities
- **Nmap**
    - https://nmap.org/
    - Documentation: https://nmap.org/docs.html
    - Command flags
        - **-sS –** TCP SYN scan for ports: does not respond with SYN/ACK
        - **-sT –** complete 3-way handshake
        - **-sU –** UDP only scan
        - **-sV –** service version detection
        - **-O –** OS detection
        - **-Pn –** Disable the ping scan
        - **-T –** Timing / aggressiveness of the speed of scan
            - Numeric value (0-5)
            - Text value (paranoid, sneaky, polite, normal, aggressive, insane)
        - **-IL –** Input from target file
        - **-o** output
        - **-oX XML –** Output to XML
        - **-oN**- normal
        - **-oG**- greppable
        - **-oA**- All

  - **smb-enum-shares –** Enumerate Samba (SMB) server for shares
  - **smb-enum-users –** Enumerate Samba (SMB) server for users

- **THC Amap**
  - https://www.thc.org/
  - Network service mapping
  - Good 2nd opinion or if **Nmap fails** to detect a service

- **host (command)**
  - Manual: https://linux.die.net/man/1/host
  - Linux command line application simple utility for performing **DNS lookups**
  - Converts names to IP addresses and vice versa
  - **Zone transfers, MX records, NS servers, TXT records**, etc
- **traceroute**
  - Manual: https://linux.die.net/man/8/traceroute
  - Map devices and appliances on the network that simply forward traffic
    - Switches, hubs, main back-bone infrastructure
    - Particularly useful in the local-network
    - Switches may allow VLAN-hopping
    - Discovery of Firewall / IDS / IPS applicances
  - Sends **ICMP** packets with **incrementing TTL** to discover devices on the route
- **dig – Domain Information Groper**
  - https://linux.die.net/man/1/dig
  - Flexible tool for interrogating DNS name servers
  - Performs DNS lookups
  - Command-line arguments and batch mode of operation (-f)
  - **dig [@server] [name] [type]**
    - **@server** = IP addresses (IPv4 / IPv6 / hostname)
    - **name** = name of resource record to be looked up
    - **type** = type of query ANY, A, MX, SIG
- **snmpwalk**
  - Manual: https://linux.die.net/man/1/snmpwalk
  - **SNMP GETNEXT** requests to query a network entity for a tree of information
  - Enumerate users / hosts on the network
- **snmpcmd**
  - Manual: https://linux.die.net/man/1/snmpcmd
  - Options and behaviour common to most of the Net-SNMP command-line tools
  - Several commands: **snmpbulkget, snmpbulkwalk, snmpdelta, snmpget, snmpgetnext, snmpnetstat, snmpset, snmpstatus, snmptable, snmptest, snmptrap, snmpdf, snmpusm , snmpwalk**
- **samrdump**
  - Info: https://www.hackingdna.com/2012/12/samrdump-on-backtrack-5.html

    - Built-into Kali linux
    - **Enumerates users on Samba fileshare** using Samba protocol
- **NBTScan**
    - http://www.unixwiz.net/tools/nbtscan.html
    - Manual: https://manpages.debian.org/testing/nbtscan/nbtscan.1.en.html
    - Source code: https://github.com/scallywag/nbtscan
    - Works on Mac, Linux, Windows
    - scanning **IP networks for NetBIOS name information**
    - Similar to **Windows nbtstat** tool
    - It sends a **NetBIOS status query** to each address in a supplied range
    - Lists received information in human readable form
    - For each responded host it lists **IP address, NetBIOS computer name, logged-in user name and MAC address**
- **ike-scan**
    - Source Code: https://github.com/royhills/ike-scan
    - Manual: https://linux.die.net/man/1/ike-scan
    - Works on Mac, Linux, Windows
    - Command-line tool that uses the **IKE protocol to discover, fingerprint and test IPsec VPN servers**
    - Sends a specially crafted **IKE packet** to each host within a network
    - Monitors retransmission packets
    - Responses are recorded, displayed and **matched against** a set of **known VPN product fingerprints**

OSINT

- **WHOIS**
    - https://www.whois.com/
    - **Find information about domain**
        - Status (i.e. if a domain is currently available or registered)
        - The creation, expiry, and updated dates
        - Registrar name
        - Registrant name*
        - Administrative and technical contact information*
    - Built-in command line tool for Mac, Linux
    - Online web-applications
        - https://lookup.icann.org/
    - Historical WHOIS info is provided by:
        - https://whoisrequest.com/history/
- **nslookup**
    - https://linux.die.net/man/1/nslookup
    - Built in command-line tool tool for Mac, Linux, Windows

  - Querying the Domain Name System (DNS) to obtain domain name or IP address mapping, or other DNS records.
- **FOCA – Fingerprinting Organizations with Collected Archives**
  - https://www.elevenpaths.com/innovation-labs/technologies/foca
  - Open-source for Widows only, requires **Win 7-10, 64bit**
  - **MS .NET** framework **4.7.1**
  - **MS Visual Studio C++ 2010 x64** or greater
  - **MS SQL Server 2014** or greater
  - Find metadata and hidden information in the documents its scans
  - Searches web pages to downloaded and analyze documents
  - **Microsoft Office, Open Office, or PDF files**, although it also analyzes **Adobe InDesign or SVG files**, for instance
  - Uses search engines: **Google, Bing, and DuckDuckGo**
  - Local files to extract the EXIF information from graphic files
- **traceroute / tracert**
- **theHarvester**
  - https://github.com/laramies/theHarvester
  - Gathering information
    - Emails
    - Sub-domains
    - Hosts
    - Employee names
    - Open ports and banners
    - Uses public sources like search engines, PGP key servers, and Shodan
- **sublist3r**
  - https://github.com/aboul3la/Sublist3r
  - Python tool designed to **enumerate subdomains** of websites using OSINT
  - Uses many search engines such as Google, Yahoo, Bing, Baidu and Ask
  - Also enumerates subdomains using Netcraft, Virustotal, ThreatCrowd, DNSdumpster and ReverseDNS
- **Shodan**
  - https://www.shodan.io/
  - Search engine that lets the user find specific devices connected to the internet using a variety of filters
- **Maltego**
  - https://www.maltego.com/
  - Not open-source software but community edition is free
  - Available for Mac, Linux, Windows
  - Written in Java
  - A forensics and **data mining application**
  - Capable of **querying various public data sources**

    - Graphically depicting the relationships between entities such as **people, companies, web sites, and documents**
    - Has paid plugins and services
- **Recon-ng**
    - https://github.com/lanmaster53/recon-ng
    - https://hackertarget.com/recon-ng-tutorial/
    - Full-featured **web-reconnaissance framework** written in **Python**
    - Interface similar to Metasploit with command line
    - Configure options, perform recon and **output results to different report types**
    - Modular framework with **plugins available**
- **Censys**
    - https://search.censys.io
    - Reduces your Internet **attack surface**
    - **Discovers unknown assets** and helps remediate Internet facing risks
- **Internet Archives**
    - A historical cache of websites on the Internet
    - May provided access to **private classified documents** that were previously exposed but later removed
    - **Wayback Machine**
        - https://archive.org

Remote Access

- **SSH Secure Shell**
- **nc / Ncat / NetCat**
    - https://nmap.org/ncat/
    - Simple utility r**eads and writes data** across **TCP or UDP** network connections
    - Designed to be a reliable back-end tool to use directly or easily drive by other programs and scripts
    - Feature-rich **network debugging** and exploration tool
    - Can create almost any kind of connection you would need, including **port binding to accept incoming connections**
    - Remote shell capabilities useful for pentesting
- **Proxychains**
    - Source code: https://github.com/haad/proxychains
    - Source code (NG) – https://github.com/rofl0r/proxychains-ng
    - Technique of **bouncing your Internet traffic** through multiple machines to **avoid detection**
    - **Hides the identity** of the original machine or to overcome network restrictions
    - Can use programs with **no built-in proxy support through a proxy**
    - Can use proxies to hide their true identities while executing an attack

Credential Testing

- **Aircrack-ng**
  - https://www.aircrack-ng.org/
  - Available for Mac, Linux, Windows
  - Aircrack is a suite of tools for **802.11a/b/g WEP and WPA cracking**
  - Conduct **disassociation attacks** on APs and devices
  - **Rouge AP** and **evil twin attacks** capabilities
  - Includes over a dozen tools
    - **Airodump** (an 802.11 packet capture program)
    - **Aireplay** (an 802.11 packet injection program)
    - **Aircrack** (static WEP and WPA-PSK cracking)
    - **Airdecap** (decrypts WEP/WPA capture files)
- **Hashcat**
  - https://hashcat.net/hashcat/
  - Open-source for Mac, Linux, Windows
  - Password cracking tool to **reverse hashed passwords**
  - **Uses GPU** to crack passwords faster
  - Supports **distributed cracking networks**
- **Medusa**
  - http://foofus.net/goons/jmk/medusa/medusa.html
  - Works on Mac and Linux
  - Speedy, multiprocessing (parallel), modular, **login brute-forcer**
  - Password cracking tool to **reverse hashed passwords**
  - Brute-forcing can be performed against multiple hosts, users or passwords concurrently
  - Flexible user input
  - Target information (host/user/password) can be specified in a variety of ways
- **Hydra / TCH Hydra**
  - https://github.com/vanhauser-thc/thc-hydra
  - https://tools.kali.org/password-attacks/hydra
  - Password cracking tool to reverse hashed passwords
  - Parallelized login cracker which supports numerous protocols to attack
  - List of protocols
    - Cisco AAA, Cisco auth, Cisco enable, CVS, FTP, HTTP(S)-FORM-GET, HTTP(S)-FORM-POST, HTTP(S)-GET, HTTP(S)-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MySQL, NNTP, Oracle Listener, Oracle SID, PC-Anywhere, PC-NFS, POP3, PostgreSQL, RDP, Rexec, Rlogin, Rsh, SIP, SMB(NT), SMTP, SMTP Enum, SNMP v1+v2+v3, SOCKS5, SSH (v1 and v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC and XMP
- **CeWL**
  - https://tools.kali.org/password-attacks/cewl

    - Wordlist generator that searches websites for keywords that maybe used in password brute force attack
- **John the Ripper**
    - https://www.openwall.com/john/
    - Documentation: https://www.openwall.com/john/doc/
    - Open-source password security auditing and password recovery tool
    - Password cracking tool to reverse hashed passwords
    - Available as cloud image for higher compute power
- **Cain and Abel**
    - https://sectools.org/tool/cain/
    - Windows-only password recovery tool handles many tasks
    - Password cracking tool to reverse hashed passwords
    - Recovers passwords by sniffing the network
    - Cracks encrypted passwords using dictionary
    - Brute-force and cryptanalysis attacks
    - Recording VoIP conversations
    - Decoding scrambled passwords
    - Revealing password boxes, uncovering cached passwords and analyzing routing protocols
- **Mimikatz**
    - https://github.com/gentilkiwi/mimikatz/wiki
    - Scrapes Windows system memory for sensitive credentials
    - Extract plain-texts passwords, hash, PIN code and kerberos tickets from memory
    - Comes in `x64` or `Win32`, depending on your Windows version (32/64 bits)
    - Some operations need administrator privileges, or SYSTEM token, so be aware of UAC from Vista version
    - Pass instructions on Mimikatz command line
    - Many modules available
- **Patator**
    - https://github.com/lanjelot/patator
    - Password cracking tool to reverse hashed passwords
- **OWASP DirBuster**
    - https://tools.kali.org/web-applications/dirbuster
    - Mac, Linux, Windows
    - Developed by OWASP
    - Enumerates files and directories on web-server / fileserver
    - Searches for hidden pages and directories on a web server
- **W3AF**
    - See above in **Scanners** section
- **fgdump / pwdump**
    - https://sectools.org/tool/fgdump/

  - Available for Windows only
  - **fgdump** is a newer version of the **pwdump** tool for extracting **NTLM and LanMan password hashes** from Windows
  - Also can of displaying password histories
  - Outputs the data in L0phtCrack-compatible form
- **L0phtCrack**
  - https://www.l0phtcrack.com/doc/Introduction.html
  - Windows only
  - attempts to crack Windows passwords from hashes
  - Obtains passwords from stand-alone Windows workstations, networked servers, primary domain controllers, or Active Directory
  - Some cases it can sniff the hashes off the wire
- **Ophcrack**
  - https://www.objectif-securite.ch/en/ophcrack
  - Runs on Linux, Windows, and Mac
  - Rainbow-table based cracker for Windows passwords
  - LM and NTLM hash cracking
  - Ability to load hashes from encrypted SAM recovered from a Windows partition
- **RainbowCrack**
  - https://project-rainbowcrack.com/
  - A hash cracker that makes use of a large-scale time-memory trade-off
  - Does computation in advance and store the results in rainbow tables
- **Wfuzz**
  - https://github.com/xmendez/wfuzz/
  - A tool for bruteforcing web-applications
  - Can find resources not linked (directories, servlets, scripts, etc)
  - Bruteforcing GET and POST parameters for different kinds of injections (SQL, XSS, LDAP, etc.), fuzzing, and more
- **Brutus**
  - https://www.darknet.org.uk/2006/09/brutus-password-cracker-download-brutus-aet2zip-aet2/
  - Windows only
  - Brute-force against **network services** of remote systems **using dictionary** and **permutations of dictionary**
  - **HTTP, POP3, FTP, SMB, TELNET, IMAP, NNTP**, and more
  - Similar to THC **Hydra**
- **Ncrack**
  - Info: https://nmap.org/ncrack/
  - Documentation: https://nmap.org/ncrack/man.html
  - Info: https://tools.kali.org/password-attacks/ncrack
  - Can be compiled for Mac, Linux, Windows

  - Binaries available for Mac, Windows
  - Password brute-forcing tool
  - Tests all network hosts and networking devices for poor passwords
  - Security professionals also rely on Ncrack when **auditing their clients**
  - Command-line syntax similar to Nmap
  - Dynamic engine that can **adapt its behaviour** based on network feedback
  - **Protocols supported**
    - SSH, RDP, FTP, Telnet, HTTP(S), POP3(S), IMAP, SMB, VNC, SIP, Redis, PostgreSQL, MySQL, MSSQL, MongoDB, Cassandra, WinRM and OWA

Wireless

- **Aircrack-ng**
  - https://www.aircrack-ng.org/
  - Suite of tools for **802.11a/b/g WEP and WPA cracking**
  - See above
- **Kismet**
  - https://www.kismetwireless.net/
  - A console based **802.11 layer-2 wireless network detector**, **sniffer**, and **IDS**
  - Identifies networks by **passively sniffing** (as opposed to more active tools such as NetStumbler)
  - Can **de-cloak hidden (non-beaconing) networks** if they are in use
  - Can automatically **detect network IP blocks** by sniffing **TCP, UDP, ARP, and DHCP** packets
  - Logs traffic in **.cap / .pcap Wireshark/tcpdump** compatible format
  - **Plot detected networks** and estimated ranges on downloaded maps
  - Commonly used for **wardriving**
- **WiFite / Wifite 2**
  - https://github.com/derv82/wifite
  - https://github.com/derv82/wifite2
  - Designed to use all known methods for retrieving the password of a wireless AP
    - WPS: The Offline **Pixie-Dust attack**
    - WPS: The **Online Brute-Force PIN attack**
    - WPA: The **WPA Handshake Capture + offline crack**
    - WPA: The **PMKID Hash Capture + offline crack**
    - WEP: Various known attacks against WEP, including **fragmentation, chop-chop, aireplay, etc**
- **NetStumbler**
  - https://www.netstumbler.com/
  - Windows only
  - Best known Windows tool for finding **open wireless access points / wardriving**
  - Also distribute a **WinCE** version for PDAs and such named **MiniStumbler**

- **InSSIDer**
  - https://www.metageek.com/products/inssider/
  - Wireless network scanner for Windows, OS X, and Android
  - Find open wireless access points, track signal strength over time, and **save logs** with GPS records / **wardriving**
- **Reaver**
  - Implements a brute force attack against Wifi Protected Setup **(WPS) PINs**
  - Discovers PINs in order to recover WPA/WPA2 passphrases
  - Recovers the target AP’s plain text WPA/WPA2 passphrase in 4-10 hours

Active and Passive Networking / Packet Capture / MiTM

- **Wireshark / Tshark / tcpdump**
  - https://www.wireshark.org/
  - Open-source multi-platform network **protocol analyzer**
  - Captures and examines data from a live network or from a capture file on disk
  - Rich packet display filters
- **EtherApe**
  - https://etherape.sourceforge.io/
  - Works on Mac, Linux
  - Uses **link layer, IP, and TCP** modes
  - Displays **network activity graphically** with a **colored protocols display**
  - Hosts and links change in size with traffic
  - Supports Ethernet, **WLAN, FDDI, Token Ring, ISDN, PPP and SLIP** devices
  - Can filter traffic to be shown, and can read traffic from a file as well as live from the network
- **Ettercap**
  - https://www.ettercap-project.org/
  - Available for Mac, Linux, Windows
  - Suite for **man in the middle** attacks on **LAN**
  - Sniffing of **live connections, content filtering**, and many other features
  - **Active and passive** dissection of many protocols (**including encrypted ones**)
  - Includes **network and host analysis**
- **Ntop**
  - https://www.ntop.org/
  - Shows **network usage** in a way similar to what **top** does for processes
  - Displays the network status on the user's terminal
  - Can acts as a Web server, creating an HTML dump of the network status
  - **NetFlow/sFlow emitter/collector**, an **HTTP-based client interface** for creating **ntop-centric monitoring applications**,
  - RRD for persistently storing traffic statistics
- **dsniff**

    - https://www.monkey.org/~dugsong/dsniff/
    - Older and not updated recently – many attacks are outdated
    - Well-engineered suite by Dug Song works on Mac, Linux, and partial Windows port
    - Webspy passively monitor a network for interesting data such as **passwords, e-mail, files**, etc.
    - **arpspoof, dnsspoof, and macof** facilitate the interception of network traffic normally unavailable to an attacker by attacking layer-2
    - **sshmitm and webmitm** implement active **MiTM attacks** against redirected **ssh and https sessions** by exploiting **weak bindings in ad-hoc PKI**
    - Includes many tools:
        - dsniff
        - filesnarf
        - mailsnarf
        - msgsnarf
        - urlsnarf
- **Network Miner**
    - https://www.netresec.com/?page=networkminer
    - Winodws only
    - **Passive** network sniffer/packet capturing tool
    - **Detects operating systems, sessions, hostnames, open ports etc**
    - Does not put any traffic on network
    - Parse pcap files for off-line analysis and to regenerate/reassemble transmitted files and certificates from pcap files
- **P0f**
    - https://lcamtuf.coredump.cx/p0f3/
    - **Good tool for stealth** does not generate any additional network traffic
    - Able to **identify the operating system of a target host**
    - Advanced users, P0f can d**etect firewall presence, NAT use, existence of load balancers**, and more

Networking Security Tools / Firewalls / IDS / IPS

- **Snort**
    - https://www.snort.org/
    - Paid software licence
    - Available for Mac, Linux, Windows
    - Network **IDS / IPS** excels at **traffic analysis** and packet logging on IP networks
    - **Protocol analysis, content searching, and various pre-processors**
    - **Detects worms, exploit attempts, port scans**, and other suspicious behavior
    - Flexible **rule-based language** to describe traffic that it should collect or pass, and a modular detection engine
- **Netfilter**

  - https://www.netfilter.org/
  - Collaborative FOSS project for the Linux 2.4.x and later kernels
  - Enables **packet filtering, network address [and port] translation (NA[P]T), packet logging, userspace packet queueing and other packet mangling**
  - Linux kernel integration allows kernel modules to register callback functions at different locations of the Linux network stack
  - **nftables** is similar to **iptables**, but allows for much more flexible, scalable and performance packet classification
  - **Features include**
    - Stateless packet filtering (IPv4 and IPv6)
    - Stateful packet filtering (IPv4 and IPv6)
    - All kinds of network address and port translation, e.g. NAT/NAPT (IPv4 and IPv6)
    - Flexible and extensible infrastructure
    - Multiple layers of API's for 3rd party extensions
- **IPFilter / ipf**
  - Open-source software package that provides **firewall services and network address translation (NAT)** for many *nix OSs
- **PF – Packet Filter**
  - BSD licensed stateful packet filter
  - Originally developed for OpenBSD but removed in May 2001
  - **OpenBSD PF**
    -
- **pfSense**
  - https://www.pfsense.org/
  - Source code: https://github.com/pfsense/pfsense
  - Firewall / router / IDS / IPS / VPN software distribution
  - OS based based on FreeBSD
  - Community edition is free, open-source
  - Professional version owned by **Netgate** not open-source
- **OSSEC HIDS**
  - https://www.ossec.net/
  - Open-source free software licence for Mac, Linux, Windows
  - Performs **log analysis, integrity checking, rootkit detection, time-based alerting and active response**
  - Commonly used as a **SIEM / SEM / SIM** solution
  - **ISPs, universities and data centers** use **OSSEC HIDS** to **monitor and analyze** their firewalls, IDSs, web servers and authentication logs
- **OSSIM Open Source Security Information Management**
  - https://cybersecurity.att.com/products/ossim
  - Maintained by **AT&T, Linux only**
  - Provide a comprehensive set of tools

  - Provides detailed view over all aspect of **networks, hosts, physical access devices, and servers**
  - Incorporates several other tools, including **Nagios** and **OSSEC HIDS**
- **Sguil**
  - https://bammv.github.io/sguil/index.html
  - Linux, *BSD, Solaris, MacOS, and Win32
  - Pronounced **sgweel**
  - Intuitive GUI that provides access to r**ealtime events, session data, and raw packet captures**
  - Facilitates the practice of **Network Security Monitoring** and **event driven analysis**
- **Archsight SIEM Platform**
  - https://www.microfocus.com/en-us/cyberres/secops/arcsight-esm
  - Paid Software, for Linux only
  - Provides a **suite of tools for SIEM, security information and event management**
  - ArcSight Enterprise Security Manager (ESM), described as the "brain" of the SIEM platform
- **Honeyd**
  - http://www.honeyd.org/tools.php
  - Small daemon that **creates virtual hosts on a network**
  - Hosts can be configured to **run arbitrary services, and certain versions** of services and OSs
  - Enables a single host to claim **multiple IP addresses** on a LAN for network simulation (Software defined network)
  - **Services on the VM can be simulated** according to a simple configuration file
  - Also possible to **proxy services to another machine** rather than simulating them
  - **Many library dependencies**, which can make **compiling/installing Honeyd difficult**
  - Several other tools available on website
    - **Arpd**
      - Listens to ARP requests and answers for IP addresses that are unallocated
    - **Nttlscan**
      - Network topology scanner and functions as a highly parallel traceroute
    - **honeydsum.pl**
      - log analyzer that generates text summaries from Honeyd logs
    - **Honeycomb**
      - Plugin for Honeyd that automatically generates signatures for IDS Snort

Debuggers / Reverse Compilers

- **Ghidra**
  - https://ghidra-sre.org/
  - Written in Java
  - Works with Mac, Linux, Windows
  - Software reverse engineering (SRE) suite of tools developed by **NSA's** Research Directorate in support of the Cybersecurity mission
  - Released in March 2019 at NSA conference
- **OllyDbg**
  - https://www.ollydbg.de/
  - Windows debugger with free licence
  - Works on **x86 binary code assembly language level**
  - Traces registers, recognizes procedures, API calls, switches, tables, constants and strings
- **Immunity Debugger**
  - https://www.immunityinc.com/products/debugger/
  - Paid software, available for Mac, Linux, Windows
  - Immunity has multiple other products and services available
    - **Canvas –** automated exploitation system / exploit development system
    - **El Jefe –** Windows-based process monitoring solution
    - **INNUENDO –** Post-compromise implant that models data exfiltration attacks
    - **SILICA –** Wifi assessment tools
  - Specifically designed for pen-testing and **reverse engineering malware**
  - Reverse engineer binary files
- **GDB**
  - https://www.gnu.org/software/gdb/
  - Open-source **Linux debugger** for **variety of programming languages**
  - Supports languages:
    - Ada, Assembly, C, C++, D, Fortran, Go, Objective-C, OpenCL, Modula-2, Pascal, Rust
- **WinDbg**
  - https://www.microsoft.com/en-ca/p/windbg/9pgjgd53tn86
  - Created by Microsoft and is Windows specific
  - Distributed as part of the free **Debugging Tools for Windows** suite
  - Used for debugging kernel-mode memory dumps, created after **Blue Screen of Death**
  - Works back-end for **KD Debugger, NTSD Debugger,** and **Microsoft Console Debugger**
- **IDA**
  - https://hex-rays.com/ida-pro/
  - Commercial debugger / reverse compiler
  - Windows, Mac, Linux platforms

    - Disassembler is capable of creating maps of execution showing the binary instructions/ assembly language executed by the processor in a symbolic representation
    - Can generate assembly language source code from machine-executable code and make this complex code more human-readable
    - Supports multiple debugging targets and can handle remote applications

Web proxies

- **OWASP ZAP**
    - https://owasp.org/www-project-zap/
    - Source Code: https://github.com/zaproxy/
    - Free Open-source **web-application scanner**
    - Automation, scheduling, paid add-ons
- **Burp Suite**
    - https://portswigger.net/burp
    - Professional version is paid soffware licence
    - **Community edition is installed built-into in Kali Linux**
    - Automated scanning across their entire portfolios
    - Schedules scanning
- **Paros Proxy**
    - https://resources.infosecinstitute.com/topic/introduction-paros-proxy-lightweight-web-application-tool/
    - No updates in long time, works on Mac, Linux, Windows
    - Written in Java
    - Web proxy for assessing web-application vulnerability
    - Supports **editing/viewing HTTP/HTTPS** messages on-the-fly to change items such as **cookies and form fields**
    - Web traffic recorder, web spider, hash calculator
    - Scanner for testing common web-application attacks such as **SQL injection and cross-site scripting**
- **Tamper Data**
    - https://sectools.org/tool/tamperdata/
    - Add-on for Firefox, Chrome
    - Allows viewing and modification of HTTP requests
    - Shows data included in communication with web-server such as such as cookies and hidden form fields
    - Identifies web applications that trust the client data input

Mobile Tools

- **Drozer**
    - https://labs.f-secure.com/tools/drozer/

  - Security audit and attack framework for Android devices and apps
  - **Sieve** includes common Android security issues
- **APKX**
  - https://github.com/b-mueller/apkx
  - Decompile Android application packages (APKs)
  - Java decompilers and DEX converters that allow the extraction of Java source code from Android packages (APKs)
- **APK Studio**
  - https://github.com/vaibhavpandeyvpz/apkstudio
  - Decompile Android application packages (APKs)
  - IDE designed to reverse engineer Android applications
- **iGoat**
  - https://owasp.org/www-project-igoat-tool/
  - **OWASP** has iOS application pen-testing tools called **iGoat** for testing iOS applications

Software assurance

- **SpotBugs**
  - https://spotbugs.github.io/
  - Program which uses static analysis to look for bugs in Java code
  - Free open-source
- **FindBugs / find-sec-bugs**
  - Download: https://find-sec-bugs.github.io/
  - Source Code: https://github.com/find-sec-bugs/find-sec-bugs
  - Perform static analysis of Java code
  - 138 different vulnerability types with over 820 unique API signatures
- **Peach / MoxPeach**
  - https://github.com/MozillaSecurity/peach
  - MozPeach is a fork of Peach v2.7 by Mozilla Security
  - **data-model** uses XML specification used that tree to generate fuzzed output
  - **target** is used to define how the target process will get fuzzed
- **AFL – American Fuzzy Lop**
  - Source Code: https://github.com/google/AFL
  - Brute-force fuzzer
  - Uses an instrumentation-guided genetic algorithm
  - Relies on coverage signals to select a subset of interesting seeds from a massive, high-quality corpus of candidate files, and then fuzz them by traditional means
  - Fuzzing tool
- **SonarQube**
  - https://www.sonarqube.org/
  - Documentation: https://docs.sonarqube.org/latest/

    - Open-source software testing tool
    - Works to fuzz 27 programming languages
        - Java, C#, C, C++, JS, TS, Python, Go, Swift, COBOL, Apex, PHP, Kotlin, Ruby, Scala, HTML, CSS, T-SQL, XML, Objective-C, VB6
- **YASCA – Yet Another Source Code Analyzer**
    - https://www.scovetta.com/yasca/
    - Source Code: https://github.com/scovetta/yasca
    - Will not be updated in the future
        - Scott is not working on **DevSkim** for **Microsoft**
            - https://github.com/Microsoft/DevSkim
            - **IDE extensions** and language analyzers that **provide security analysis in the dev environment**
            - Supports languages: **C, C++, C#, Cobol, Go, Java, Javascript/Typescript, Python, and more**
    - Open-source software testing tool
    - Can scan wide variety of languages
    - YASCA uses **FindBugs**
- **skipfish**
    - https://code.google.com/p/skipfish/
    - Info: https://tools.kali.org/web-applications/skipfish
    - Source Code: https://github.com/spinkham/skipfish
    - Mac, Linux, Windows
    - Active **web-application security recon** tool
    - Creates **interactive sitemap** for the targeted site by **doing a recursive crawl** and **dictionary-based** probes
    - **Annotated with** the output from a number of **active security checks**
    - Final report generated by the tool is meant to serve as a foundation for professional web-application security assessments
- **Wapiti**
    - https://wapiti.sourceforge.io/
    - Info: https://owasp.org/www-community/Automated_Audit_using_WAPITI
    - Free Open-source
    - Simple command line to tool to **automate auditing of a web-application**
    - Performs **black-box scans**
    - Looks for **scripts and forms to inject data**
    - Acts like a **fuzzer**, injecting payloads to see if a script is vulnerable
    - **Modules supporting**
        - SQL Injections
        - XPath Injections
        - Cross Site Scripting (XSS) reflected and permanent
        - File disclosure detection (local and remote include, require, fopen, readfile...)

    - Command Execution detection (eval(), system(), passtru()...)
    - XXE (Xml eXternal Entity) injection
    - CRLF Injection
    - Brute Force login form (using a dictionary list)
    - Checking HTTP security headers
    - Checking cookie security flags (secure and httponly flags)
    - Cross Site Request Forgery (CSRF) basic detection
    - Fingerprinting of web-applications using the Wappalyzer database

Social Engineering

- **SET – Social Engineering Toolkit**
  - https://www.trustedsec.com/tools/the-social-engineer-toolkit-set/
  - Source code: https://github.com/trustedsec/social-engineer-toolkit
  - Incorporates many useful **social-engineering attacks** all in one interface
  - **Automates** many social-engineering attacks
  - Automatically generates **exploit-hiding web pages** or **email messages**
  - Can use **Metasploit payloads** to connect back with a shell once the page is opened
- **BeEF – Browser Exploitation Framework**
  - https://beefproject.com/
  - Mac, Linux, Window
  - Browser exploitation framework
  - Collecting of **zombie browsers** and browser vulnerabilities **in real-time**
  - **Command and control interface** which facilitates the targeting of **individual or groups of zombie browsers**

Exploitation Frameworks

- **SearchSploit**
  - Manual: https://www.exploit-db.com/searchsploit
  - Source Code: https://github.com/offensive-security/exploitdb
  - Exploit binaries: https://github.com/offensive-security/exploitdb-bin-sploits
  - White-papers: https://github.com/offensive-security/exploitdb-papers
  - **Command line tools** that allows you to **search through database of known exploits**
  - Perform detailed **off-line searches** through a local copy of the repository
- **PowerSploit**
  - Documentation: https://powersploit.readthedocs.io/en/latest/Recon/
  - Source Code: https://github.com/PowerShellMafia/PowerSploit
  - Windows centric sets of **PowerShell scripts** that may be used to **automate penetration testing tools**

  - Modues for **code execution, script modification, persistance, anti-virus bypass, exfiltration, privlilege escalation, reconnaissance**
- **Responder**
  - Info: https://tools.kali.org/sniffingspoofing/responder
  - Source code: https://github.com/SpiderLabs/Responder
  - Video tutorial: https://www.youtube.com/watch?v=rjRDsXp_MNk
  - Maps a Windows Domain Controller for running services
  - If the domain controller does not have the location stored in cache, it will request other machines on the network
  - Responder responds to queries from a Windows Domain Controller
    - Answers NetBIOS queries from Windows systems on a network
    - **LLMNR** and **NBT-NS responder**
    - Answers **NBT-NS (NetBIOS Name Service) queries** based on their name suffix
    - http://support.microsoft.com/kb/163409
    - Answers **SMB File Server Service requests**
  - Can set **-r option to 1** via command line to answer to the **Workstation Service request name suffix**
- **Impacket**
  - https://www.secureauth.com/labs/open-source-tools/impacket/
  - Source code: https://github.com/SecureAuthCorp/impacket
  - Python: https://pypi.org/project/impacket/0.9.15/
  - A set of network tools that provide low level access to network protocols
  - Collection of **Python classes** for working with network protocols
  - Providing **low-level programmatic access to the packets**
  - For some protocols (e.g. **SMB1-3 and MSRPC**) the protocol implementation itself
  - Packets can be **constructed from scratch**
  - Packets can be **parsed from raw data**
  - Works at standard user level
  - Work with **deep hierarchies** of protocols:
    - Ethernet, Linux "Cooked" capture
    - IP, TCP, UDP, ICMP, IGMP, ARP
    - IPv4 and IPv6 Support
    - NMB and SMB1, SMB2 and SMB3 (high-level implementations)
    - MSRPC version 5, over different transports: TCP, SMB/TCP, SMB/NetBIOS and HTTP
    - Plain, NTLM and Kerberos authentications, using password/hashes/tickets/keys
    - Portions/full implementation of the following MSRPC interfaces: EPM, DTYPES, LSAD, LSAT, NRPC, RRP, SAMR, SRVS, WKST, SCMR, DCOM, WMI
    - Portions of TDS (MSSQL) and LDAP protocol implementations
- **Core Security**
  - **Has a number of products**

    - **Core Impact –** Automated penetration tests
    - **Cobalt Strike –** Threat emulation tool for simulations and Red team exercises
    - **Network Insight –** Network traffic analysis
  - **Python Libraries**
    - https://www.coresecurity.com
    - https://www.coresecurity.com/products/cyber-threat-solutions
    - https://www.coresecurity.com/core-labs/open-source-tools
    - https://github.com/SecureAuthCorp/impacket
- **Empire Powershell**
  - https://www.powershellempire.com/
  - Source code: https://github.com/EmpireProject/Empire
  - Info: https://alpinesecurity.com/blog/empire-a-powershell-post-exploitation-tool/
  - Pure PowerShell **post-exploitation** toolkit
  - **Cryptologically-secure communications** and a flexible architecture
  - Implements **PowerShell agents without needing powershell.exe**
  - **Post-exploitation modules** such as **key-loggers**, and **Mimikatz**
  - Adaptable communications to **evade network detection**
  - Commands are similar to Metasploit
- **Metasploit Framework**
  - https://www.metasploit.com/
  - Documentation: https://docs.rapid7.com/metasploit/msf-overview/
  - Most popular network exploitation framework
  - Set target, payload, and configure payload settings
  - Supports **3rd party plugins**
  - Ruby-based, modular framework enables you to **write, test, and execute exploit code**
  - **msfconsole** is command line interface
  - Plug-ins are often developed quickly after vulnerability announcements
  - **Versions**
    - Metasploit Framework
    - Metasploit Pro
    - Metasploit Community (web-interface)
    - Metasploit Express
    - Armitage – GUI for Metasploit
  - Metasploit Unleashed
    - https://www.offensive-security.com/metasploit-unleashed/
    - A free course in ethical hacking
  - Exploits have hierarchal naming structure
  - **Exploit Quality Ratings**
    - Metasploit can filter the plugins based on quality settings using **-r [quality]**
    - **Excellent –** Will never crash the service

- **Great –** The exploit will autodetect target / version and use specific settings
- **Good –** Is the common case for the target
- **Normal –** Reliable but requires a specific version that can't be autodetected
- **Average –** Unreliable or difficult to exploit
- **Low –** Unlikely to succeed (< 50%) used against most platforms
- **Manual –** unstable, difficult to exploit, may result in denial of service, difficult to configure

- **Searching for Exploits**
  - Use the following keyword flags when searching for exploits
  - OpenVAS includes CVE number which can help searching for specific exploit
  - Web-based search: https://www.rapid7.com/db/?type=metasploit
  - **Keywords**
    - **app –** Client or server attack
    - **author** – Search or module by author
    - **bid** – Search by Bugtraq ID
    - **cve** – Search by CVE ID
    - **edb** – Search Exploit-DB ID
    - **name** – Search by descriptive name
    - **platform** – Search by platform (Windows, Linux, Unix, Android, etc.)
    - **ref** – Modules with a specific ref
    - **type** – Search by type: exploit, auxiliary, or post
    - **Example:** search **type:exploit author sinn3r**
- **Payloads**
  - Type: **show payloads** after module is loaded to list payloads
  - **getsystem** command can escalate privileges once exploit is successful (???)
  - **Staged payloads –** load the payload in stages so are good for memory restricted environments
  - **Meterpreter –** a payload that works via DLL injection on Windows systems and remains memory resident
  - **PassiveX –** ActiveX via Internet Explorer
  - **NoNX –** payloads are designed to counter modern memory protection like Data Execution Prevention (AKA No Execute)
  - **ORD –** (ordinal) load a .ddl into a compromised process on Windows system
  - **IPv6 –** payloads are designed for IPv6 networks
  - Reflective DLL injection modules also target Windows systems

- **Mimikatz**
  - See above description

Exploitable Test Environments

- **Metasploitable V2 and V3**
  - https://information.rapid7.com/download-metasploitable-2017.html

  - VM’s that have vulnerabilities for practice
- **OWASP WebGoat** project
  - https://owasp.org/www-project-webgoat/
  - Deliberately insecure J2EE web-application
- **Standard OS or Applications**
  - **Older versions** with known vulnerabilities
  - Windows XP, 7, 2008 Server, Older Linux OS
  - OS installed without security patches
- **No So Secure** provides VM with vulnerable **Docker container**
  - https://notsosecure.com/vulnerable-docker-vm/

Forensics

- **Helix**
  - http://www.e-fense.com/products.php
  - Last release was 2009 / Not free software
  - Ubuntu live CD customized for **computer forensics**
  - Designed very carefully to ***not* write to the host** computer in any way
  - Will **not auto-mount swap space**, or **auto-mount any attached devices**
  - Has a special **Windows autorun** side for **incident response and forensics**
- **The Sleuth Kit / Autopsy**
  - https://www.autopsy.com/
  - Collection of **UNIX-based command line file and volume system forensic analysis tools**
  - File system tools allow you to **examine file systems** in a **non-intrusive fashion**
  - Tools do not rely on the operating system to process the file systems
  - **Deleted and hidden content is shown**
  - GUI based tool is called **Autopsy**
- **Encase**
  - https://security.opentext.com/encase-forensic
  - Paid software
  - Commonly **used by law enforcement**
  - De-facto standard in forensics
  - Collect data from a computer in a forensically sound manner
    - Employing checksums to **detect tampering**
- **MAGNET**
  - **MAGNET Axiom**
    - https://www.magnetforensics.com/products/magnet-axiom/
    - Complete digital investigation platform
    - Paid software for Windows only
    - Direct support for **Windows and Mac** filesystems

        - Create forensic images of **mobile devices**
        - Uses **GPU** to speed up process
        - **Decrypt iOS app data** using Keychain and GrayKey
    - **MAGNET Ram Capture**
        - Captures the contents of RAM memory
        - Has small RAM footprint
        - Malware processes and services, network connections, encrypted files and keys may be found in memory
    - **MAGNET Encrypted Disk Detector**
        - Only runs on Windows 7 or higher
        - Incidence response tool-kits
        - Checks local drive for encrypted volume
- **Cellebrite BlackLight / Inspector**
    - https://www.cellebrite.com/en/inspector/
    - Paid software available for Mac and Windows
    - Direct support for **Windows and Mac** filesystems
    - Can attempt to decrypt full disk encryption
    - Find internet history, downloads, recent searches, top sites, locations, media, messages, recycle bin, USB connections, and more
    - Create forensic images and analyze **iOS / Android mobile devices**
- **AccessData FTK Imager**
    - https://accessdata.com/products-services/forensic-toolkit-ftk/ftkimager
    - Free software available for Mac and Windows
    - Data preview, memory dump, and drive imaging tool
    - Also works for **Linux filesystems (XFS)** and **Mac filesystems (AFS)**
- **UnifiedLogReader / mac_apt / MacForensics**
    - https://www.swiftforensics.com/
    - Source code: https://github.com/ydkhatri
    - **mac_apt**
        - macOs (& iOS) Artifact Parsing Tool
    - **UnifiedLogReader**
        - A parser for Unified logging tracev3 files
    - **MacForensics**
        - Scripts to process macOS forensic artifacts
- **Browser History Capturer and History Reviewer**
    - Captures browser history files from hard-drive
- **SIFT – SANS Investigative Forensics Tool Kit**
    - A computer forensics **full OS distribution** created by the SANS Forensics team
    - Includes most tools for digital forensics and incident response examinations
- **CrowdResponse**
    - Gather information for incident responses

    - Build by industry leader CrowdStrike
    - CrowdStrike **has other incident response / digital forensics tools available as well**

Stress Test Tools

- **Siege 3.0.3 and URL Encoding**
    - https://www.joedog.org/2013/07/siege-3-0-3-url-encoding/
    - HTTP/FTP load tester and benchmarking utility
    - Measure the performance of their applications under load
- **Tsung Tsunami**
    - http://tsung.erlang-projects.org/
    - Source code: http://tsung.erlang-projects.org/dist/
    - Documentation: http://tsung.erlang-projects.org/user_manual/
    - High-performance benchmark framework for various protocols including HTTP, XMPP, LDAP, etc
- **Hping**
    - http://www.hping.org/download.html
    - Artificially generate network traffic and specific packet types
    - Can act as a scanner to confirm host is listening at IP address
    - Many flags including:
        - **-c –** count
        - **-i –** interval
        - -a **–** spoof hostname
        - --rand-source **–** sets a random source IP
        - -1 **–** ICMP
        - -2 **–** UDP
        - -8 **–** scan
- **Wbox**
    - http://www.hping.org/wbox/
    - Benchmark time it takes to generate content for your web-application
    - Web server and web-application stressing
    - Check if your redirects are working correctly emitting the right HTTP code
    - HTTP compression is working and if it is actually serving pages faster

Penetration Testing Operating Systems

- https://medium.com/lotus-fruit/top-10-operating-systems-for-ethical-hackers-and-penetration-testers-2020-list-b523b611cdbb
- https://www.guru99.com/best-os-hacking.html
- https://techlog360.com/top-ethical-hacking-operating-systems/
- **Kali Linux**

- **BackBox**
- **Parrot Security OS**
- **Live Hacking OS**
- **DEFT Linux**
- **Samurai Web Testing Framework**
- **NST – Network Security Toolkit**
- **BlackArch Linux**
- **Fedora Security Lab**
- **Dracos Linux**
- **Bugtraq / Bugtraq II**
- **CAINE – Computer-Aided Investigation Environment**
- **DemonLinux**
- **ArchStrike**
- **Cyborg Hawk Linux**
- **GnackTrack**
- **NodeZero**
- **Pentoo**
- **BlackBuntu**
- **Knoppix STD**
- **Weakerthan**
- **Matriux Linux**
- **URIX OS**

Root-kit detectors / Virus Scanners

- **Sysinternals**
- **rkhunter**
- **Chkrootkit**
- **LMD**
- **ClamAV**
- **Tripwire**
- **DumpSec**
- **HijackThis**
- **AIDE**

Pen-test Field Kit

- **Battery Power Bank**
  - Anchor PowerCore
- **Mobile phone**

  - Sim-card Tool Kit / Sim-card adapters
  - Disassembly tools
- **Hack5 Products**
  - Bash bunny
  - Lan Turtle
  - Shark-Jack
  - Packet Squirrel
  - Screen Crab
  - Plunder Bug
  - Wifi Pineapple
  - Key logger
  - USB Rubber Ducky
- Red Team / Blue Team Field Manuals
- Long Range Ratio Antennas
- Battery / USB powered lights
- USB Drive with encryption code (???)
- USB Wireless modem (air capture packets)
  - Alpha USB wireless model
  - TP-Links USB wireless modem
- SD Drive / USB Drives
- USB to Ethernet adapter
- R-pi 3 Kali box
- Mini keyboard
- Multi adapter (C, micro,)
- Ethenet cable (compact rolled)
- Switch – low-powered
- Rav travel power router
- Portable Router
- USB volt-meter
- Cable splicer
- USB expansion array adapter
- Micro-SD card adapters
- Ethernet Extender
- Loopback & | cross-over cable adapter
- Powerjack proof adapter / prevention USB key
- Key logger usb mitm
- Raspberry Pi
- Arduino
- Lockpicking kit