CEH Tools

Sniffers

- **Wireshark**: The most popular packet sniffer with cross platform support.
- **Tcpdump**: A popular CLI sniffer available for both the Unix and Linux platforms.
- **Windump**: Windows version of tcpdump.
- **Cain & Abel**: Its an all-in-one tool to capture packets and record passwords being used in a MiTM. It can create an ARP and DNS poisoning events and the cracker works with methods such as network packet sniffing, dictionary, brute force and cryptanalysis such as rainbow attacks.
- **Kismet**: Wireless sniffing tool used to locate and discover hidden SSID's. It can be used to passively sniff the traffic and gain the password that way.
- **Ntop**: High speed web based traffic analysis.
- **Network Miner**: Packet sniffer, with built in OS finger printer. Drop down navigator for filtering specific traffic. Automatically extracts files for packet capture; it will also extract images. It will also pull some credentials for specific sites. It can also filter out "keywords" to allow for filtering of specific information being sent across the network.

CEH Tools

Scanners

- **Nmap**: uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.
- **Zenmap**: Nmap with a GUI and ability to plot a map for reference.
- **Angry IP Scanner**: (or simply ipscan) is an open-source and cross-platform network scanner designed to be fast and simple to use. It scans IP addresses and ports as well as has many other features.
- **hping2 & 3**: Custom packet-crafting tool that can be used to precisely package packets to scan and penetrate networks and bypass known security features.
- **SuperScan**: allows you to quickly scan a range of IP addresses and do TCP port scanning. It can check all ports, or the ones you select. It is a very fast and powerful tool. Supports banner grabbing, ping, whois, tracert. Recently bought by McAfee.
- **Zanti (mobile)**: An Android software used to Scan Ports, MiTM, Session Hijack, Redirect URL traffic, used for Pentesting with a noble device.
- **NBTScan**: It sends a NetBIOS status query to each address in a supplied range and 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. **SUPER FAST SCANS**
- **hping2 & 3**: Custom packet-crafting tool that can be used to precisely package packets to scan and penetrate networks and bypass known security features.
- **NetScan Tools**: Created in 1999 to automate the plethora of internet tools to work with one GUI supported by Windows platforms. OS Fingerprinting, Packet sniffing, port scanning, packet flooding, mail exchange validation.
- **Nessus**: Vulnerability scanner that is used by pentesters, hackers, and enterprise security engineers.

CEH Tools

Enumeration

- **DumpSec**: Reveals users, groups, printers, shares, registry info in an easy to digest human readable format from a targeted system. Very useful for finding out intimate information about the specific system for privilege escalation purposes.
- **SuperScan**: Also used for enumeration. *See Scanning
- **Netcat**: A simple tool that can read and write data across a TCP or UDP connection. It's very useful because it can create almost any type of connection. Including session binding. It allows actors to create shell and reverse shell connections between two endpoint. Allowing them to send / receive files and execute commands on both the host and compromised systems. It has since lost support; consequently the Nmap project has incorporated an upgraded version called Ncat. Other remakes: Socat, OpenBSD's nc, Cryptcat, netcat6, pnetcat, etc.
- **Cryptcat**: A variant of netcat that encrypts communication; making it useful to evade the detection of IDS or traffic sniffing.
- **TCPView**: It will enumerate all TCP and UDP connections on the end point running the application. Will resolve domain names for the IP's connected to the system. Monitors changing connections and can close existing connections.
- **Sysinternals Suite**: A suite of sysinternal tools made by Microsoft for troubleshooting.
- **NirSoft Suite**: A suite of tools used to automate the troubleshooting of Windows.

CEH Tools

Password Cracking Tools

- **L0phtCrack**: A password cracking application used for locally or remotely locating user account information and cracking the corresponding passwords. Windows/Unix/Linux/ FreeBSD/ etc. Can be used for periodically scanning and cracking system passwords.
- **Ophcrack**: Free version of Ophcrack. Less features. Not as robust.
- **John the Ripper**: CLI password cracking utility that can have custom rules created as well as use custom password lists to crack passwords.
- **Trinity Rescue Kit**: Live Linux distribution that aims specifically at recovery and repair operations on Windows machines, but is equally usable for Linux recovery issues. Since version 3.4 it has an easy to use scrollable text menu that allows anyone who masters a keyboard and some English to perform maintenance and repair on a computer, ranging from password resetting over disk cleanup to virus scanning.
- **Medusa**: Remote, speedy, modular brute force cracker for network services. HTTP, MySQL, SMB, SMTP, SNMP, SSHv2
- **RainbowCrack**: Cracks hashes referenced against rainbow tables. It's different from traditional brute force crackers in that it uses large pre-computed tables called "rainbow tables"; which reduces the amount of time the brute force takes.
- **Brutus**: Older remote password cracker.

CEH Tools

Wireless Tools

- **Kismet**: A sniffing tools and also a multi-purpose wireless tool. It can be used for IDS and many other things.
- **inSSIDer**: Used to monitor local WiFi traffic and identify the channels different networks are communicating on. It was originally designed for optimizing Office / Home network WAP placement to reduce interference and produce the most optimal signals for the environment.
- **Reaver**: WPS brute forcing tool. This tool waits to intercept the WPS beacon; once it's captured it will brute force the WPS PIN and the PSK password.
- **Netstumbler (Old but useful on 32bit systems)**: Similar to inSSIDer, but not as feature rich.
- **Bluesnarfer**: A tool used to steal information from a mobile device through the bluetooth connection.
- **Aircrack-ng**: Is a tool suite used to assess WiFi security. It focuses on monitoring, attacking, testing and cracking a WAP. It can capture and analyze packets; create replay attacks, deauthentication with injection techniques; test WiFi cards and their driver capabilities; and crack WEP and WPA PSK (1 and 2). It can also conduct fragmentation attacks.
- **Airmon-ng (Aircrack)**: Aircrack's sniffing tool.
- **Airodump-ng (Aircrack)**: Used to capture 802.11 packets, especially good at capturing WEP IV's to be used with Aircrack-ng. It can also be used to log the GPS coordinates of found WAP's if the a GPS receiver is connected to your device.

CEH Tools

Logging and Event Viewing Tools

- **Log Parser Lizard**: A Microsoft based log viewing tool that presents the information in a GUI based format. It's capable of presenting data from individual systems, SQL servers, AD, IIS, and many other types of log / event creating applications or systems.
- **Splunk**: An enterprise tool used to store and parse logs on a large scale to monitor network activity and functionality.
- **SolarWinds**: An enterprise tool similar to Splunk, with the exception that it can create a database for network monitoring. It's useful in visualizing the configuration of the network in a live environment which reduces the need for static network topology tools like Vizio.

Other Tools

- **Snort**: A freeware IDS / IPS.
- **Metasploit**: This is an automated framework capable of exploiting vulnerabilities with many tools across many platforms.

CEH Tools

Hardware Tools

- **Minipwner**: A small device that can be connected to the target network and left behind to allow the actor to gather information remotely. It can be configured with battery or power cord. It's low power consumption allows the device to be used a WAP on battery power for several hours.
- **USB Rubber Ducky**: A flash drive that is recognized as a Human Interface Device (HID). It can bypass most enterprise DLP software since the software thinks the device is a keyboard. It is capable of running scripts and gathering data among many other uses that can be dreamt up for it.
- **Wi-Fi Pineapple**: A small discrete device that has powerful application for pentesting. It can be used as a potential Evil Twin WAP. It comes with an impressive suite of applications that helps to analyze the data collected by the device.
- **LAN Turtle**: A Small USB-to-Ethernet adapter that can be placed on a victims computer inside the target network. I can fingerprint and enumerate the network and be used to create an SSH into the network. It can also spoof DNS entries on the network for a redirection / session hijacking attack.
- **AirPcap**: A USB designed to provide a hardware based pentesting tool. It works in conjunction with other common tools. It can be used on wireless networks and may conduct packet injection to active connections. It can function as an Evil Twin, or Rogue AP.
- **Ubertooth One**: A USB device that can be used to scan for Bluetooth communication.