Network Reconnaissance
The reason to learn "how to hack" is to get a better idea of networks are attacked, so a better defense can be mounted. It is the principle of "know your enemy".

Types of Attacks and Computer Crimes
Denial of Service, Destruction of Information, Dumpster Diving
Emanation Eavesdropping: act of intercepting and analyzing unintended electromagnetic or acoustic emissions from electronic devices to extract sensitive information
Embezzlement, Espionage
Fraud
Information Warfare
Illegal Content
Malicious Code
Masquerading
Social Engineering
Software Piracy
IP Address Spoofing
Terrorism
Theft of Passwords
Use of exploit scripts, network intrusions

There are a lot of attacks

Motivations behind attacks: Money, fame, war, politics, it can differ

The Cyber Kill Chain: a framework to model the stages of a cyberattack
Reconnaissance -> Weaponization -> Delivery -> Exploitation -> Installation -> Command & Control -> Actions on Objectives

Reconnaissance: Information gathering, passive and active

Collecting Information from Public Sources:
Public Databases
Dumpster Diving (shred your documents)
Social Engineering
Domain Name System or searching services
Physical Break Ins

Changing Caller-ID: very easy, some legit reasons to do this

Google Dorking/Hacking: advanced search engine technique, uses operators in the google search engine
site:example.com
intitle:
inurl:
related:
Google Hacking Database, and reconnaissance using google can be easily automated
Maltego: An OSINT platform for cyber investigations, has scripts that can go to specific sites and find information
Some places for individuals: Their social network profile
Metadata Leakage, Tone, Frequency, Location Awareness, Social Media Presence
Cree.py: can gather geo location data, deprecated

Network Range (scanning and enumeration)
Whois database/command on Unix: query and response protocol that is used for querying databases that store an Internet resource's registered users or assignees

When you register a domain name with an authorized regitrar, you must provide a valid name, address, and phone number of the person responsible for the domain - this can be used against you in an attack
ARIN: American Registry for Internet Numbers
Registered IP blocks based on geographical location

DNS Record Types:
A - IPv4
AAAA - IPv6
MX - Mail Exchange, IP address of the Server which handles mail for the domain
NS: Name server, domain name servers which serve this domain
CNAME: Canonical Name, Aliases for host names
SOA: First Line of DNS File, Indicates that this server is the Best Source of Information for this domain
SRV: Service Record, information about available service in the domain. SIP and XMPP use this.
RP: Responsible Person. Assign an emaill address to a specific host.
PTR: Pointer record, allows for reverse DNS lookup, typically required for MX Hosts.
TXT: Originally for human readable information, but now used for things such as Domain-Keys
HINFO: Host Info. Supplies OS and other info about a host. Generally not a good idea.

MXtoolbox: A tool to gain info on DNS records

Shodan: IoT search engine

DNS Zone Transfer: A vulnerability that doesn't work anymore, it makes a copy/duplicate of a DNS zone to another. It is by default turned off.
Brute Force Forward DNS: guess DNS names
Split DNS: Two DNS servers, one external and one internal

Host Discovery:
Traceroute: maps the path from your computer to a destination
War Dialing: Dialing a sequence of phone numbers searching for modems or open PBXs
Port Scanning: Sending TCP and UDP packets to various ports to determine if a process is active

Port Open: gets a response, like an ACK
Port Closed: Gets a RST
Port Filtered: ICMP destination Unreachable
No Response: Network error

nmap: port scanner
TCP Scan Types:
TCP Connect Scan: Completes the 3-way handshake, then closes it with a FIN. Open ports respond with SYN/ACK, closed ports respond with RST.
SYN Scan: Half open, only the first part of the TCP handshake. Open ports respond with SYN/ACK, closed Ports respond with RST.
FIN Scan: Sends a FIN packet to the target port. Closed ports send back an RST.
Null Scan: No flags set. If OS implemented TCP per RFC 793, will respond with an RST.
XMAS: FIN, URG, and PSH flags set. Closed ports should respond with a RST.
FIN, NULL, XMAS, used to identify OS based on the response.
ACK Scan: If a RST packet returned, it means the port is either open or closed. If ICMP destination unreachable is sent, port is filtered. Used to map out firewall rulesets.
FTP Bounce Attack: Use an FTP server to bounce an attack
Version Scanning: tries to determine the version number of the program listening on the port - for example Apache2 on port 80
Fragmented Scans: Can get around some router ACL packet filters that do not examine the port number in fragmented packets. Fragments the packets.
TCP Sequence Prediction: useful in spoofing attacks

UDP Scanning:
Port is open, a UDP probe gets a response.
If Port is closed, a UDP probe gets an icmp destination unreachable.
No Response: Filtered by firewall, network error

UDP Scanning takes a long time: 1 second per port

FTP Bounce Scan: A scan type in which an anonymous FTP server is used to perform scans. Nmap opens a connection an FTP server, log into server and try to open ports on the target machine.

Firewalk: does a traceroute using any application data port.
Traceroute does it using ICMP/pings