Red Teaming lock picking

Name: Priyali Poojari

🔐 1. Padlocks

Combination Padlocks

How It Works: Operates by aligning internal rotating discs to a specific combination.
Bypass Methods:

- *Shimmying*: Inserting a shim between the shackle and body to disengage the locking mechanism.
- *Manipulation*: Applying tension and feeling for subtle clicks to determine the correct combination.

Keyed Padlocks

How It Works: Uses a pin tumbler mechanism activated by a specific key.
Bypass Methods:

- *Shimming*: Inserting a thin metal shim to bypass the locking pawls.
- *Lock Picking*: Manipulating the pins inside the lock to align them with the shear line.

Shrouded Padlocks

How It Works: Features a protective casing to shield the shackle.
Bypass Methods:

- *Bolt Cutters*: Applying significant force to cut through the shackle.
- *Hacksaw*: Using a hacksaw to cut through the shackle or body.

Smart Padlocks

How It Works: Operates via Bluetooth or Wi-Fi, often controlled by a smartphone app.
Bypass Methods:

- *Signal Jamming*: Disrupting the communication between the lock and the controlling device.
- *App Exploits*: Utilizing vulnerabilities in the mobile application to gain unauthorized access.

🔐 2. Deadbolts

Single Cylinder Deadbolt

How It Works: Operated by a key on the outside and a thumb turn on the inside.
Bypass Methods:

- *Lock Picking*: Manipulating the pins to align with the shear line.

- *Bumping*: Using a specially crafted key to jolt the pins into place.

Double Cylinder Deadbolt

How It Works: Requires a key on both sides, providing additional security.
Bypass Methods:

- *Lock Picking*: Similar to single-cylinder, but both sides need to be manipulated.
- *Bumping*: Requires precise alignment of pins on both sides.

Lockable Thumb Turn Deadbolt

How It Works: Features a thumb turn that can be locked with a key from the outside.
Bypass Methods:

- *Lock Picking*: Manipulating the pins to unlock the thumb turn.
- *Bumping*: Using a bump key to align the pins and unlock.

🔐 3. Knob Locks

How It Works: Integrated into the door knob, often used in residential settings.
Bypass Methods:

- *Lock Picking*: Manipulating the pins to align with the shear line.
- *Bumping*: Using a bump key to jolt the pins into place.

🔐 4. Lever Handle Locks

How It Works: Operated by a lever handle, commonly found in commercial settings.
Bypass Methods:

- *Lock Picking*: Manipulating the pins inside the lock.
- *Bumping*: Using a bump key to align the pins.

🔐 5. Mortise Locks

How It Works: Installed into a pocket within the door, providing robust security.
Bypass Methods:

- *Lock Picking*: Manipulating the pins or wafers inside the lock.
- *Bumping*: Using a bump key to align the pins.

🔐 6. Rim Locks

How It Works: Mounted on the surface of the door, often used in addition to other locks.
Bypass Methods:

- *Lock Picking*: Manipulating the internal mechanism.
- *Bumping*: Using a bump key to unlock.

🔐 7. Cam Locks

How It Works: Operates by rotating a cam to secure or release the lock.
Bypass Methods:

- *Lock Picking*: Manipulating the pins or wafers inside the lock.
- *Bumping*: Using a bump key to align the pins.

🔐 8. Euro Cylinder Locks

Single Cylinder

How It Works: Operated by a key from one side.
Bypass Methods:

- *Lock Snapping*: Applying force to break the cylinder at its weakest point.
- *Lock Bumping*: Using a bump key to align the pins.

🔐 9. Magnetic Locks

How It Works: Uses an electromagnet to secure the door.
Bypass Methods:

- *Power Interruption*: Cutting power to the electromagnet to release the lock.
- *Magnetic Field Disruption*: Using strong magnets to interfere with the lock's mechanism.

🔐 10. Keycard Locks

How It Works: Operates by reading a magnetic stripe or RFID chip on a keycard.
Bypass Methods:

- *Cloning*: Duplicating the keycard's magnetic stripe or RFID signal.
- *Signal Interception*: Capturing and replaying the keycard's signal.

🔐 11. Smart Locks

Fingerprint Locks

How It Works: Scans and matches a fingerprint to grant access.
Bypass Methods:

- *Fake Fingerprint*: Creating a replica of a fingerprint to deceive the sensor.
- *Sensor Manipulation*: Interfering with the sensor's ability to read fingerprints.

Bluetooth/Wi-Fi Locks

How It Works: Controlled via Bluetooth or Wi-Fi, often through a smartphone app.
Bypass Methods:

- *Signal Jamming*: Disrupting the communication between the lock and the controlling device.
- *App Exploits*: Utilizing vulnerabilities in the mobile application to gain unauthorized access.

Voice-Activated Locks

How It Works: Responds to specific voice commands.
Bypass Methods:

- *Voice Mimicry*: Imitating the authorized voice command.
- *Recording Playback*: Playing a recorded authorized voice command.

🔐 12. Chain Locks

How It Works: Secures the door with a chain and latch.
Bypass Methods:

- *Force*: Applying force to break the chain or latch.
- *Manipulation*: Using tools to unlatch the chain from outside through the door gap.

🔐 13. Barrel Bolt / Slide Bolt

How It Works: A simple manual bolt slides into a catch or socket, often used on internal doors or gates.
Bypass Methods:

- *Credit Card Shim*: Sliding a flexible card between the door and frame to push the bolt back (if installed loosely).
- *Wire Bypass*: If there’s a gap (e.g. in bathroom or shed doors), a looped wire or hook can pull or slide the bolt from outside.
- *Force Entry*: Weak screws or wood around the bolt can be kicked or pried apart.

🔐 14. Disc Tumbler Locks *(Abloy / Disc-Detainer Locks)*

How It Works: Uses rotating discs that align to a sidebar when the correct key is inserted. Commonly used in high-security applications like vending machines and padlocks.
Bypass Methods:

- *Specialized Disc Pick Tools*: Manipulating the discs individually to align them with the sidebar.

- *Impressioning*: Creating a working key by analyzing wear or markings on a blank key.
- *Destructive Entry*: Drilling or grinding as a last resort (these locks are highly resistant to most attacks).

🔐 15. Wafer Locks

How It Works: Uses flat wafers instead of pins; typically found in cabinets, vehicles, and mailboxes.
Bypass Methods:

- *Lock Picking*: Requires flatter tools due to less spring tension.
- *Jiggler Keys*: A set of master-like keys exploiting loose tolerances.
- *Impressioning*: Decoding the lock by marking a blank key.

🔐 16. Locking Bars

How It Works: A metal bar secured across a door, cabinet, or shutter, often locked with a padlock or integrated mechanism.
Bypass Methods:

- *Remove Fasteners*: Unscrewing or prying off brackets.
- *Cutting Tools*: Using bolt cutters, hacksaws, or grinders on the bar or padlock.
- *Hinge/Frame Attacks*: Targeting the structure if the bar itself is too strong.

🔐 17. Combination Locks

How It Works: Uses a series of rotating discs or cams that align notches when the correct combination is dialed, allowing the lock to open.
Bypass Methods:

- *Manipulation*: Feeling for subtle clicks under tension to determine the combination.
- *Shimming*: Inserting a shim between the shackle and lock body to disengage the mechanism.
- *Dialing Techniques*: Using patterns or trial-and-error to deduce the combination.

🔐 18. Biometric Locks

How It Works: Authenticates users via fingerprints, facial recognition, or iris patterns, comparing scanned data with stored templates.
Bypass Methods:

- *Fingerprint Replication*: Using materials like gelatin or silicone to mimic fingerprints.
- *Facial Spoofing*: Employing high-resolution images or 3D models.
- *Voice Mimicry*: Replaying recorded voice commands.

🔐 19. Cable Locks

How It Works: Uses a flexible steel cable and locking head, commonly for securing bikes or electronics.
Bypass Methods:

- *Cable Cutting*: Severing the cable with bolt cutters or hacksaws.
- *Lock Picking*: Manipulating the lock mechanism.
- *Shimmying*: Inserting a shim to release the locking latch.

🔐 20. T-Handle Locks

How It Works: A T-shaped handle rotates to retract internal bolts; common on toolboxes and trucks.
Bypass Methods:

- *Lock Picking*: Manipulating pins or wafers.
- *Bumping*: Using bump keys to align pins.
- *Force Entry*: Breaking or prying the handle.

🔐 21. Shackle Locks

How It Works: The U-shaped shackle fits into the lock body and is secured by internal latches.
Bypass Methods:

- *Shimming*: Slipping a thin shim to release the latches.
- *Bolt Cutters*: Severing the shackle.
- *Hacksaw*: Cutting through the shackle.

🔐 22. Cylinder Locks

How It Works: Uses pin tumblers aligned by a key to rotate the cylinder and unlock.
Bypass Methods:

- *Lock Picking*: Aligning pins at the shear line.
- *Bumping*: Jolting pins with a bump key.
- *Drilling*: Destroying pins to rotate the core.

🔐 23. Antique/Vintage Locks

How It Works: May use warded or lever mechanisms; common in older furniture and doors.
Bypass Methods:

- *Key Impressioning*: Creating a key based on contact points.
- *Lock Picking*: Manipulating levers or avoiding wards.
- *Force Entry*: Brute force on aging materials.

🔐 24. High-Security Locks

How It Works: Incorporates advanced features like restricted keyways, trap pins, and anti-drill plates.
Bypass Methods:

- *Lock Picking*: Requires specialized tools and techniques.
- *Key Duplication*: Cloning from photos or impressions.
- *Drilling*: Precision drilling to destroy components.

🔐 25. Furniture Locks

How It Works: Small-scale locks in cabinets and drawers, usually wafer or pin tumbler types.
Bypass Methods:

- *Lock Picking*: Using small tools to manipulate pins.
- *Bumping*: Applying bump keys for quick entry.
- *Force Entry*: Prying or drilling to break the lock.

🔐 26. Time Locks

How It Works: Prevents access to a safe or vault until a preset time has elapsed, used as a secondary security layer.
Bypass Methods:

- *Tampering*: Attempting to override or manipulate timing components.
- *Destructive Entry*: Drilling or cutting to bypass entirely.

🔐 27. Pivot Locks

How It Works: Uses a rotating bolt or pin to secure a door or latch, often in specialty enclosures.
Bypass Methods:

- *Lock Picking*: Aligning internal components to allow pivoting.
- *Force Entry*: Breaking the pivot mechanism or supporting structure.

🔐 28. Drop Bolts / Electronic Strike Locks

How It Works:

- *Drop Bolts*: Electromechanical bolts that extend vertically into the frame to secure the door when powered.
- *Electronic Strike Locks*: Replace traditional strike plates and release electronically when access is granted.

Bypass Methods:

- *Power Interruption*: Disabling power can either lock or unlock the door, depending on whether it's fail-secure or fail-safe.
- *Access Control Exploits*: Exploiting vulnerabilities in the access control system, software, or wiring.
- *Magnet or Shim*: Misaligned or poorly installed strikes can be bypassed using a strong magnet or thin shim.

🔐 29. Rim Latches

How It Works: Surface-mounted latching mechanisms that lock automatically when the door closes, often used with night latches.
Bypass Methods:

- *Credit Card Bypass*: Flexing a card into the gap to depress the latch.
- *Wire Hook Tools*: Reaching inside through a gap or mail slot to retract the latch manually.
- *Lock Picking*: Applicable if there's an exterior key cylinder.

🔐 30. Multipoint Locks

How It Works: Operated by a single handle or key, these locks engage multiple bolts along the door edge (top, middle, bottom).
Bypass Methods:

- *Lock Cylinder Attack*: Snapping, picking, or bumping the main cylinder to disengage all bolts.
- *Frame Manipulation*: Prying or spreading weak door frames to bypass engaged bolts.

🔐 31. Tubular Locks

How It Works: Circular key and pin layout where pins are arranged radially; commonly found in vending machines and ATMs.
Bypass Methods:

- *Tubular Lock Picks*: Tools that pick all pins at once.
- *Drilling*: Targeting the center to disable pins.
- *Impressioning*: Making a key based on tool marks or resistance feedback.

🔐 32. Cross Locks (Cruciform)

How It Works: Uses a four-way pin layout and a cruciform key; pins are arranged on all four sides of the keyway.
Bypass Methods:

- *Specialized Picks*: Cross-lock picks with multiple probing prongs.
- *Impressioning or Bumping*: Possible on lower-quality models.

🔐 33. Restricted Keyway Locks

How It Works: Employs patented keyways and proprietary blanks to prevent unauthorized duplication.
Bypass Methods:

- *Advanced Lock Picking*: Requires high skill and specialized tools.
- *Key Duplication via Imaging*: 3D-printing or cutting a key based on high-resolution photos.
- *Insider Threats*: Acquiring key access through social engineering or internal breaches.

🔐 34. Keyless Mechanical Locks (e.g., Simplex)

How It Works: Mechanical push-button or rotary dial locks requiring no power or electronics; often used on internal doors.
Bypass Methods:

- *Combination Discovery*: Observing wear patterns or feeling for differences in resistance.
- *Manipulation Tools*: Devices that apply torque while attempting sequences.
- *Force Attack*: Prying off the faceplate or disassembling the lock.

🔐 35. RFID Locks

How It Works: Uses radio-frequency signals to read keycards, fobs, or embedded tags and grant access via an electronic actuator.
Bypass Methods:

- *Card Cloning*: Reading and duplicating RFID credentials.
- *Relay Attacks*: Intercepting and transmitting a legitimate signal from a distance.
- *Signal Jamming*: Blocking or overwhelming the RFID signal to interfere with operation.

🔐 36. Safe Locks

🔸 ***Dial Locks (Mechanical Combination)***

- **How It Works**: Rotating a dial aligns internal wheels or cams to a specific combination, allowing a fence to drop into a gate and retract the bolt.
- **Bypass Methods**:
  - Manipulation (using feel and sound)
  - Radiological Attacks (dust/graphite to reveal digits)
  - Drilling (precision access to internals)

🔸 ***Digital Locks (Electronic Keypad Safes)***

- **How It Works**: User inputs a numeric code; if correct, a solenoid retracts to release the bolt.
- **Bypass Methods**:
  - Default Codes (unchanged factory settings)
  - Power Cycling (reset behavior on power loss)
  - Brute Forcing (if no lockout/attempt limits)
  - Circuit Shorting (manually triggering solenoid)

🔐 37. Chain-and-Hasp Locks

- **How It Works**: A chain loops through a hasp or anchor and is secured with a padlock.
- **Bypass Methods**:
  - Bolt Cutters or Saws
  - Shimming or Picking Padlock
  - Exploiting Weak Anchoring (prying/breaking the hasp)

🔐 38. Surface-Mounted Locks

- **How It Works**: Externally mounted (e.g., night latches), typically using a bolt or latch.
- **Bypass Methods**:
  - Credit Card or Shim (spring-loaded latch)
  - Through-the-Door Attacks (via mail slots or gaps)
  - Picking or Bumping (if cylinder-based)

🔐 39. Gate Locks

- **How It Works**: Commonly padlocks or latch/bolt systems on fences and gates.

- **Bypass Methods**:
    - Reach-Through Tools (exploiting gaps)
    - Cutting Tools (bolt cutters, angle grinders)
    - Hinge Attacks (removing unsecured gate hinges)

🔐 40. Vehicle Locks

🔸 ***Ignition Locks***

- **How It Works**: Mechanical lock cylinder tied to the ignition system, operated by key.
- **Bypass Methods**:
    - Lock Picking or Bumping
    - Slide Hammer Pulling (extracting the cylinder)
    - Hotwiring (direct wire ignition—obsolete on modern vehicles)

🔸 ***Steering Wheel Locks***

- **How It Works**: Physical lock device on steering wheel to prevent rotation.
- **Bypass Methods**:
    - Cutting (with hacksaws or bolt cutters)
    - Freezing and Breaking (with freeze spray)
    - Steering Wheel Cut (cutting the wheel to slide lock off)
