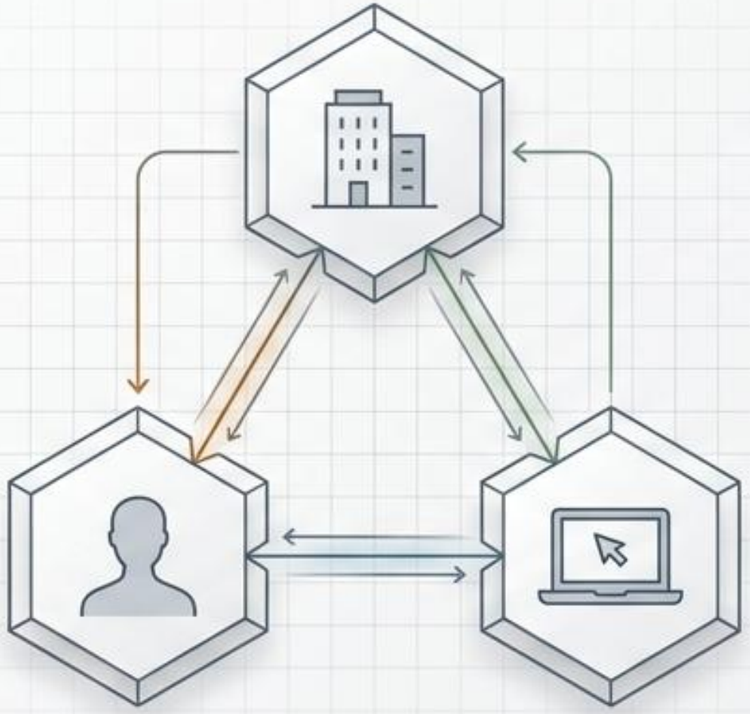
Threat Intelligence Briefing – Authorized Personnel Only



Beyond the Firewall

A Strategic Playbook for Vulnerability Assessment and Penetration Testing

True security requires a unified defense across three distinct perimeters

The Facilities Perimeter

Exploiting weaknesses in buildings, access controls, and hardware.

The Insider Perimeter

Misuse of authorized access by malicious, negligent, or compromised users.

The Client-Side Perimeter

Exploiting vulnerabilities in software, browsers, and user workstations.

Even the strongest digital defenses can be bypassed if attackers gain physical access or exploit trusted insiders.

Physical Penetration Attacks bypass digital locks by exploiting facility weaknesses

Tailgating (Piggybacking): Following authorized personnel without authentication.

Impersonation: Pretending to be maintenance, delivery, or a contractor.

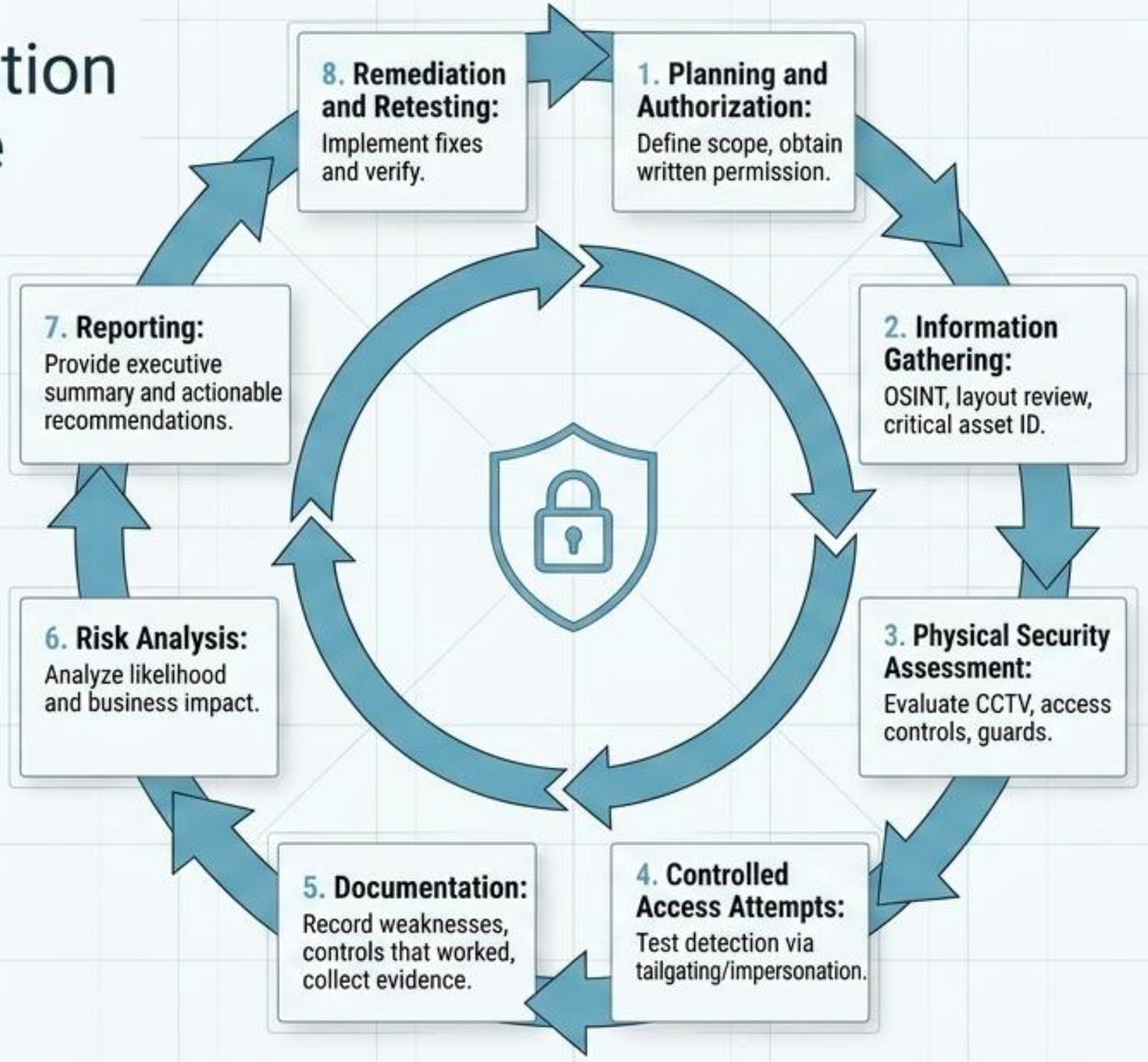
RFID/Card Cloning: Duplicating access cards for restricted areas.

Dumpster Diving & Shoulder Surfing: Searching discarded docs or observing typed PINs.

USB Drop Attack: Leaving infected drives hoping employees connect them.

Lock Picking: Bypassing physical locks with specialized tools.

The Authorized Physical Penetration Testing Lifecycle



Securing the physical perimeter requires overlapping layers of access control

Strong Access Control

Mantraps, turnstiles, badge readers, biometrics.

Visitor Management

Registration, temporary badges, escorts in restricted zones.

Employee Awareness

Anti-tailgating rules, challenging unfamiliar individuals.

Surveillance & Patrols

CCTV at entrances/exits, active security guards.

Secure Sensitive Areas

Additional controls specifically for server rooms and data centers.

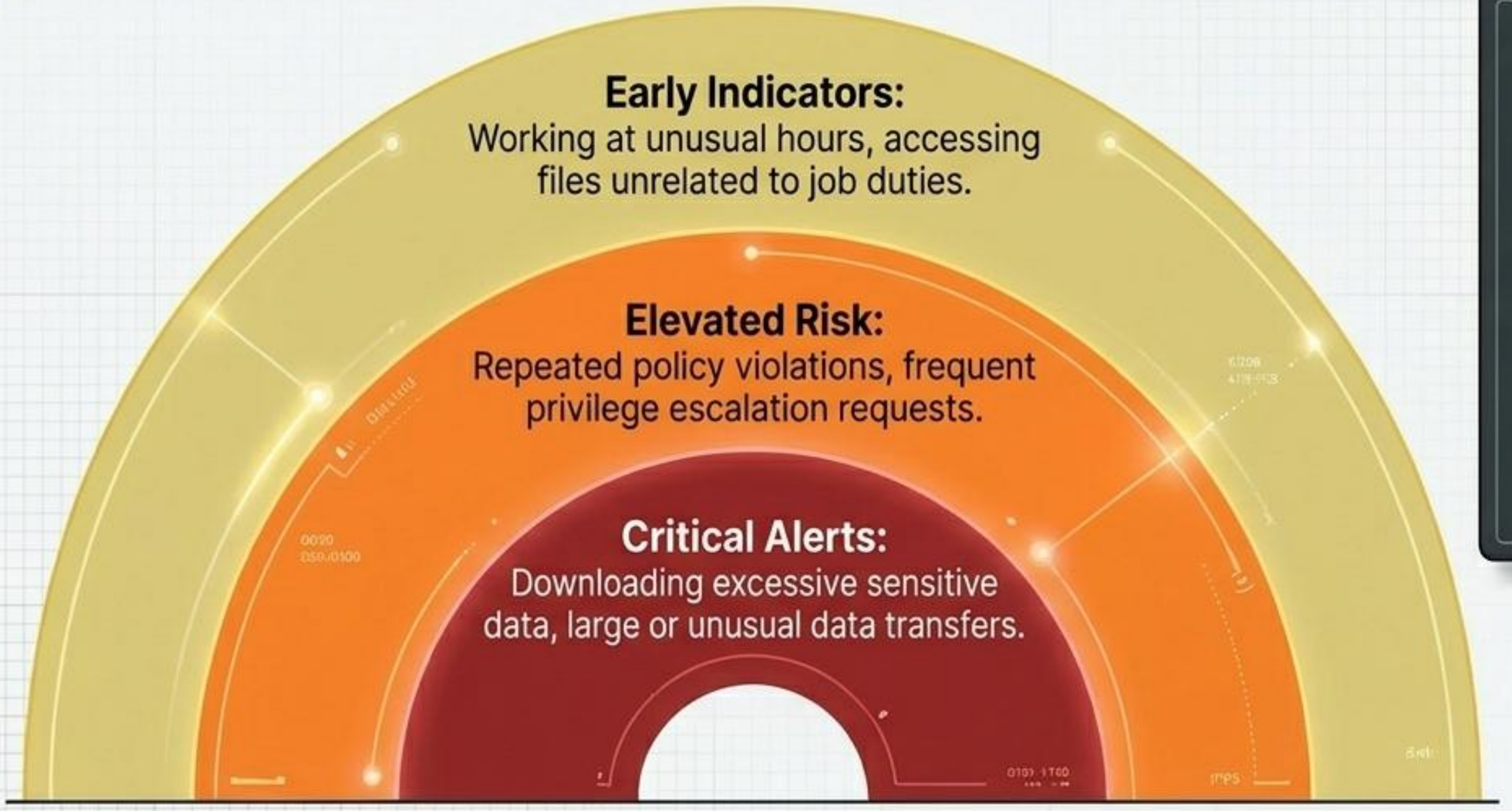
Clean Desk Policies

Protecting visible information and credentials.

The Insider Threat Matrix categorizes risks originating from trusted users

 **Malicious Insider**	 **Negligent Insider**	 **Compromised Insider**
Intent:	**Intent:**	**Intent:**
Intentional abuse.	Unintentional / Carelessness.	External attacker using hijacked internal access.
Methods:	**Methods:**	**Methods:**
Stealing data, sabotage, installing malware, selling information.	Clicking phishing links, using weak passwords, losing devices.	Stolen login credentials, malware-infected workstations.

Detecting insider anomalies before they escalate to catastrophic breaches



The Cost of Failure

- ⚠ Data breaches
- ⚠ Operational disruption
- ⚠ Regulatory penalties
- ⚠ IP theft
- ⚠ Loss of customer trust

Defending human trust starts with the Principle of Least Privilege

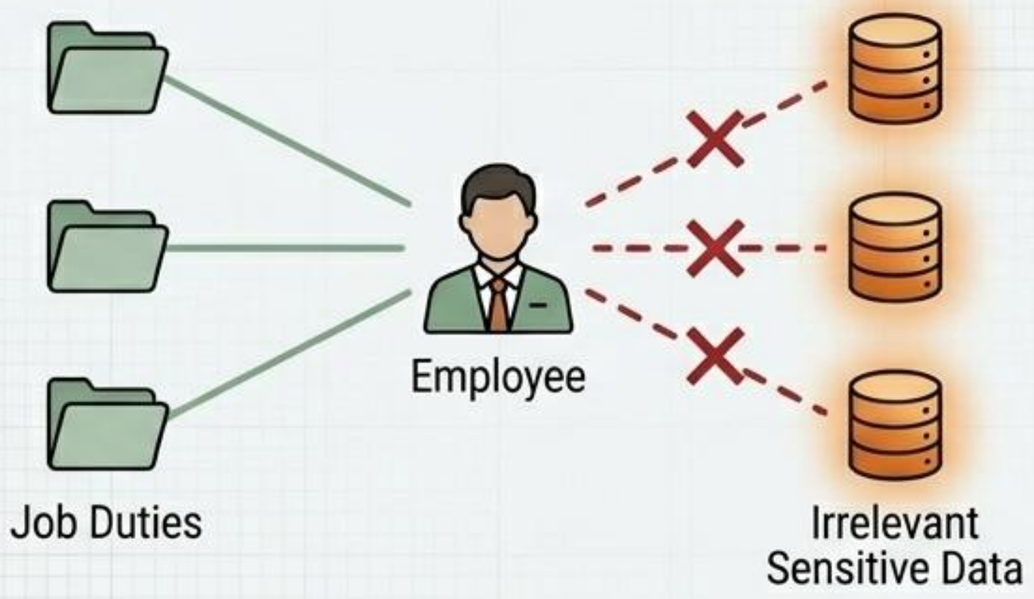
Core Concept: Give employees only the access necessary to perform their job duties, severely limiting the impact of a compromised or malicious account.

Multi-Factor Authentication (MFA)

Protecting accounts even if passwords are stolen.

User Activity Monitoring

Tracking logins and identifying excessive downloads.



The Least Privilege Access Model

Data Loss Prevention (DLP)

Detecting and stopping unauthorized transfers of sensitive data.

Regular Access Reviews

Auditing privileges and revoking access for terminated employees.

Client-side attacks exploit vulnerabilities in software running on the user's system

The Client-Side Exploit Chain

The Vector

Drive-by downloads, malicious PDFs/Office docs, phishing emails, vulnerable plugins, malvertising.

The Malicious Content

The attacker's web server delivers an exploit.

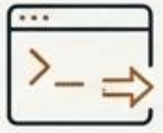
The Vulnerable Client

The user's browser, plugin, or document reader triggers the flaw.

The Exploit

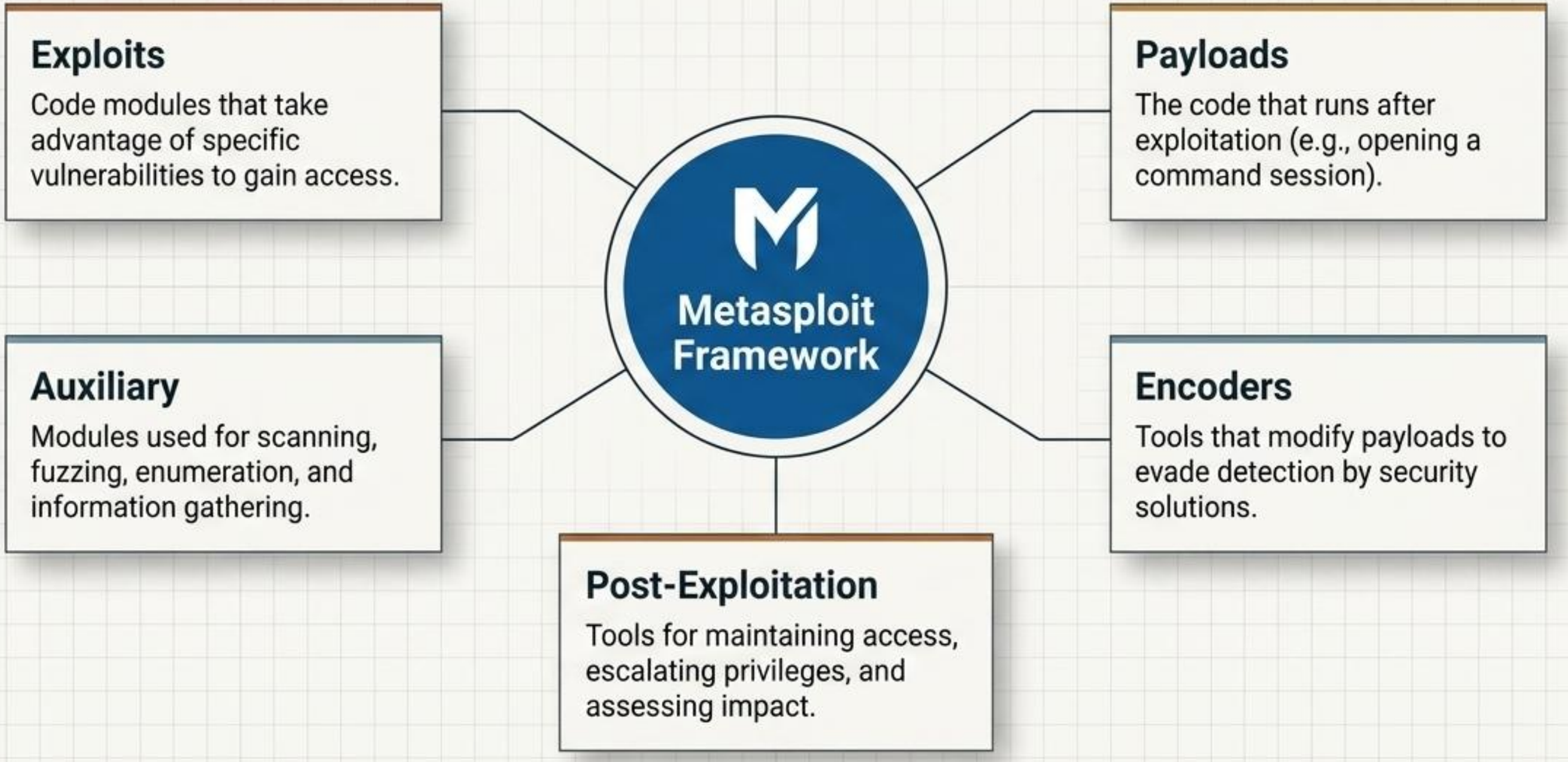
Code executes, establishing a persistent connection.

The Session

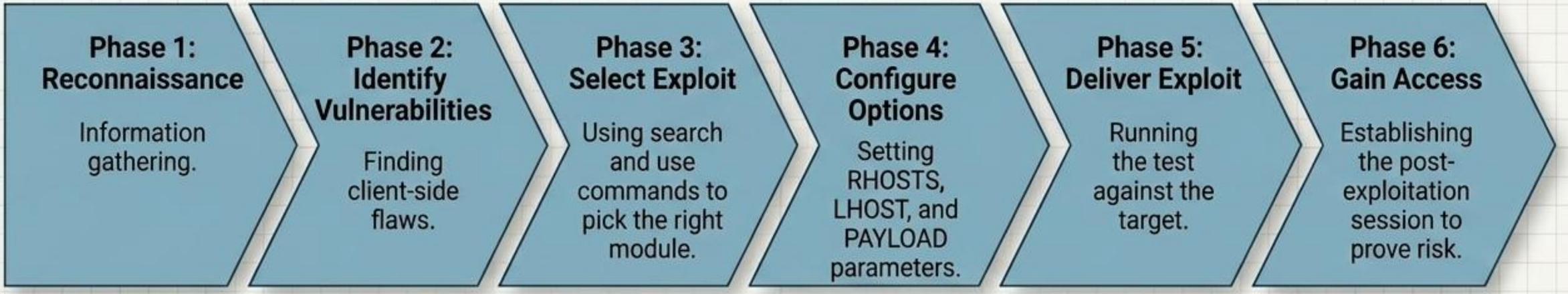


Attacker gains a Meterpreter session for post-exploitation.

The Metasploit Framework: The primary engine for finding and validating vulnerabilities



The Metasploit Client-Side Exploitation Workflow



⚠ Always obtain written permission before testing. Use only in authorized, controlled environments.

The Holistic Defense Matrix: A unified view of organizational vulnerability

Domain	Target	Primary Attack Vectors	Assessment & Defense
Physical Security	Facilities & Hardware	Tailgating, Impersonation, Lock Picking	Assessment: 8-Step Physical Pen-Test. Defense: Perimeter Access Control.
Human Trust	User Privileges	Malicious Intent, Phishing, Stolen Credentials	Assessment: Access Reviews & Scenarios. Defense: Principle of Least Privilege.
Digital Endpoints	Client Software	Malicious Docs, Drive-by Downloads	Assessment: Metasploit Framework. Defense: Patching & Endpoint Detection.

True organizational resilience is a continuous cycle, not a final destination

Vulnerabilities exist in the seams between domains. An An attacker doesn't care if they breach your network via a misconfigured firewall, a tailgating incident, or a compromised PDF.

Defense requires integration. A combination of technology, strict processes, and security-aware people is essential to reduce risk.

Identify, validate, and remediate weaknesses across all perimeters before adversaries exploit them.