Network Penetration Testing

Why Hack Your Own Network?

What is Network Penetration Testing?

Network penetration testing—often called "pentesting"—is a **simulated cyberattack** authorized by an organization to evaluate the security posture of its network infrastructure.

The Primary Goal: To identify and exploit vulnerabilities in a controlled, professional environment *before* a real attacker discovers them.

Think of it like hiring a team of ethical hackers to test your building's locks, alarms, and security guards. You're stress-testing your defenses to find the weak points.

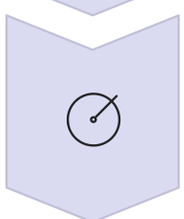
The Pentesting Methodology

The Attacker's Roadmap: A 5-Phase Playbook

Almost every penetration test follows a structured methodology known as the "kill chain." This systematic approach ensures comprehensive security assessment and mirrors how real attackers operate.

Information Gathering

Who is the target?

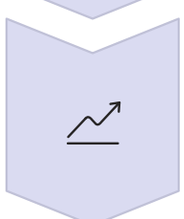


Enumeration

What systems exist?

Exploitation

How can I get in?



Privilege Escalation

How do I gain admin rights?

Post-Exploitation

What can I do now?

Types of Penetration Tests

How Much Information Do You Start With?

Penetration tests are categorized by the amount of prior knowledge the tester has about the target environment. Each type simulates different threat scenarios.

Black Box

Knowledge Level: Zero

Real-World Analogy: An external attacker with no insider information

The tester receives nothing but the organization's name—simulating how a malicious hacker would begin an attack from the outside.

Gray Box

Knowledge Level: Partial

Real-World Analogy: An insider threat scenario

The tester is provided with a standard user account, simulating threats from disgruntled employees or compromised credentials.

White Box

Knowledge Level: Complete

Real-World Analogy: A comprehensive security audit

The tester has full access to network diagrams, source code, and admin credentials—enabling the most thorough assessment possible.

Phase 1: Passive Reconnaissance

Gathering Intel from the Shadows

Passive reconnaissance involves collecting information **without directly interacting** with the target's systems. This approach is undetectable and carries zero risk of triggering security alerts.

Key Techniques:

Google Dorking

Advanced search operators uncover leaked documents, exposed login pages, and sensitive files.

Example: `site:target.com filetype:pdf confidential`

Social Media Mining

Employee profiles reveal technology stacks, org structure, and security practices.

Example: Job postings mentioning "Cisco ASA firewall experience" expose infrastructure details.

Advanced Passive Techniques

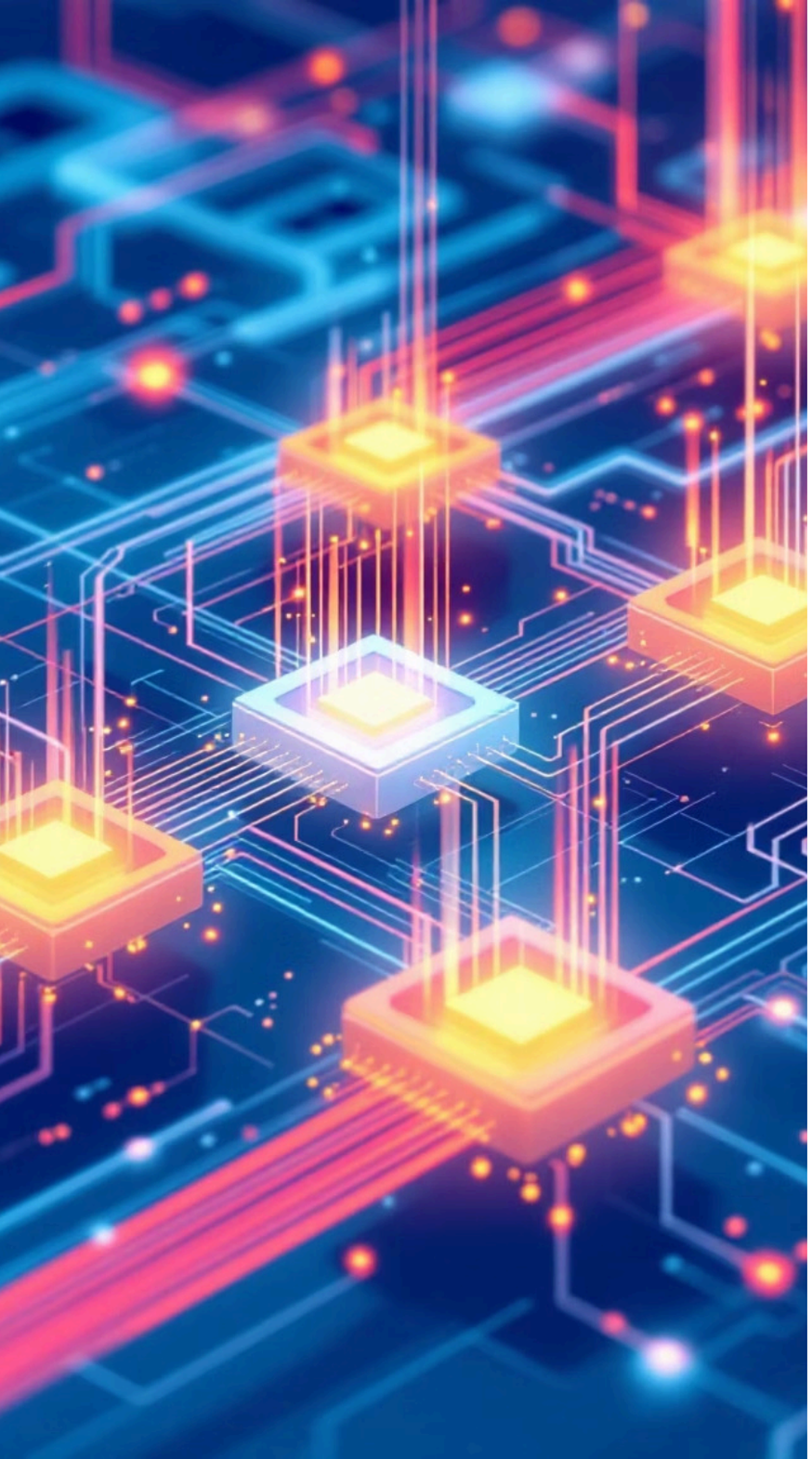
Reading the Public Records

Whois Lookup

Domain registration records reveal the registered owner, administrative contacts, email addresses, and IP address blocks owned by the organization. This public data provides crucial starting points for mapping the target's digital footprint.

Shodan.io: The Hacker's Search Engine

Unlike Google, Shodan indexes *devices* instead of websites. It reveals public-facing servers, industrial control systems, webcams, routers, and IoT devices—often with default credentials still enabled.



Phase 2: Active Reconnaissance

Knocking on the Digital Doors

Active reconnaissance shifts from passive observation to **direct network probing**. While more effective at discovering live systems and services, this phase is "louder" and can trigger intrusion detection systems.

The Primary Objective

- Identify live hosts on the network
- Discover open ports (entry points)
- Enumerate running services and versions
- Fingerprint operating systems

The King of Tools: Nmap

Network Mapper (Nmap) is the industry-standard tool for network discovery and security auditing. It's free, open-source, and used by security professionals worldwide.

Deep Dive: Nmap in Action

How the Network Mapper Works

Nmap systematically probes all 65,535 potential "ports" (digital doorways) on target systems to identify which services are accessible and how they're configured.

Sample Nmap Command

```
nmap -sV -A -T4 target-ip-address
```

-sV: Service Detection

Identifies running services and their versions (e.g., "Apache web server 2.4.52" or "OpenSSH 8.2p1")

-A: OS Fingerprinting

Determines the target's operating system (e.g., "Linux 5.15" or "Windows Server 2019")

-T4: Timing Template

Aggressive timing for faster scans—balances speed with detection avoidance

The Result: A comprehensive map of the target's network-facing attack surface, complete with potential vulnerabilities.

The Final Phases: From Entry to Full Control

Phase 3: Exploitation

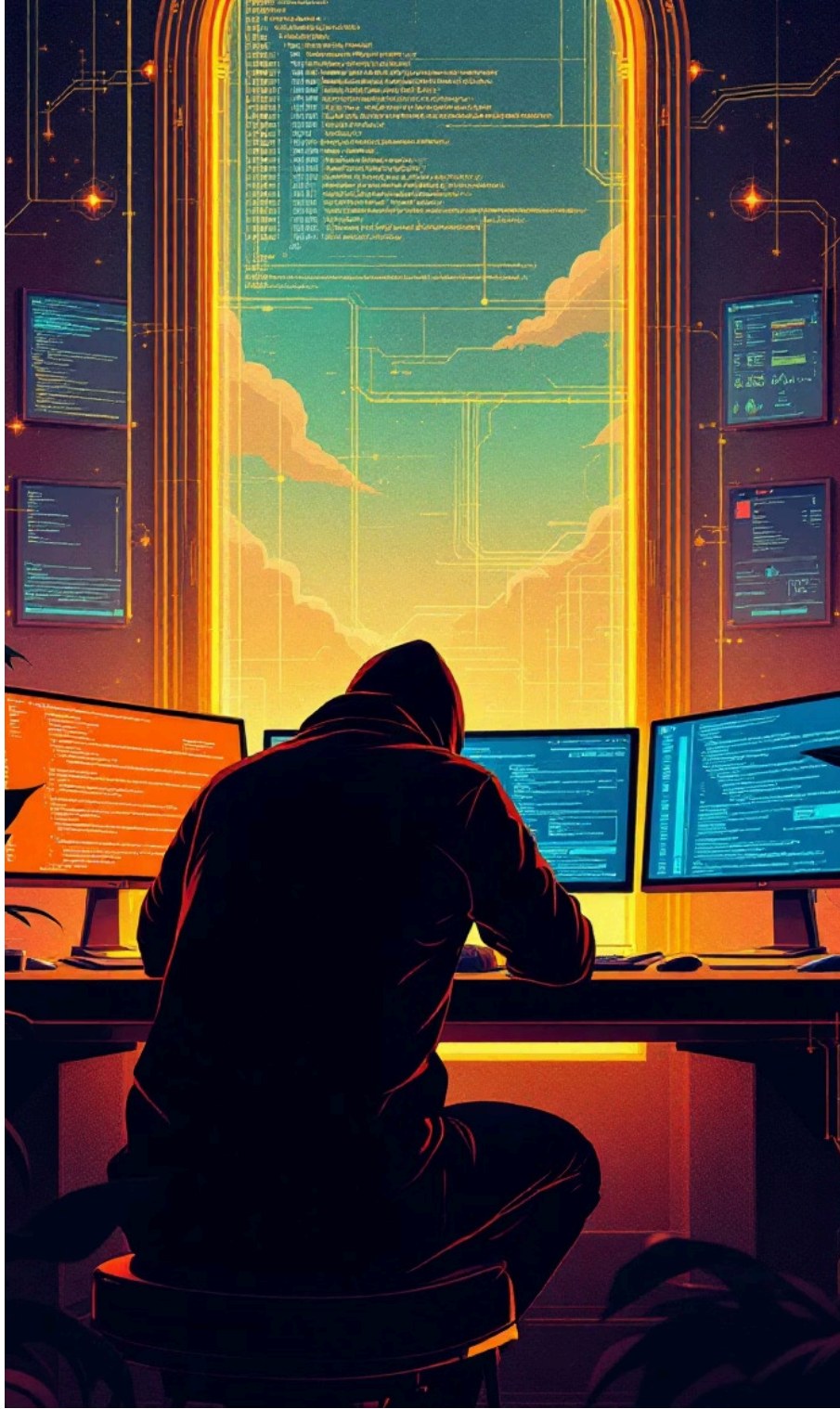
Leveraging discovered vulnerabilities to gain initial access. Example: An outdated web server version with a known remote code execution exploit provides the entry point.

Phase 4: Privilege Escalation

Elevating a low-privilege user account to "root" (Linux) or "Administrator" (Windows). Misconfigurations, kernel exploits, and weak permissions are common escalation vectors.

Phase 5: Post-Exploitation

Achieving the engagement objectives: exfiltrating sensitive data, establishing persistent backdoors, or pivoting laterally to compromise additional systems on the internal network.



Why We Hack Ourselves

Key Takeaways from Network Penetration Testing

Structured Methodology

Penetration testing isn't a single action but a disciplined, repeatable process that mirrors real-world attack patterns.

Recon is Critical

Reconnaissance—both passive and active—forms the foundation. A comprehensive map of the target is 90% of successful penetration testing.

Essential Toolset

Tools like Nmap, Shodan, and Google Dorking are indispensable for identifying attack surfaces and potential entry points.

> "To secure a network, you must first think like someone who wants to break it."