On Day 5, types of servers, spotting the risks of shared hosting environments is a key insight in offensive security and reconnaissance. Reverse IP lookup (also called reverse DNS or host lookup) is indeed a powerful recon technique, especially when evaluating a target's attack surface.

Server:
It is a computer that stores data, runs applications, responds to client request(browser, mobile app, API)
Example: User => Browser => Server => Website

Based on Hosting (Resource Allocation), servers are divided into two types

1) Shared Server(Shared Hosting)
   A server where multiple websites share the same resources and the same IP address
2) VPS Server(Virtual Private Server)
   A server is created by virtualizing a physical server into isolated environments.

Differences among them are that the shared server is more vulnerable to hackers because it shares multiple hosts and an IP address, lacks isolation, has a low cost, a high reverse IP value, and low security compared to a VPS.

Why Shared Hosting Can Be Risky
Many budget-friendly hosting plans put dozens, hundreds, or even thousands of websites on a single server sharing the same public IP address. While modern hosts use isolation techniques (like containerization, CageFS, or CloudLinux) to limit damage, older or poorly configured setups often leave gaps:

• Cross-site contamination — If one site is vulnerable (e.g., outdated WordPress with an exploitable plugin), an attacker could gain server-level access and pivot to other sites on the same server.

• File permission issues — Poorly set permissions might allow one user to read or write files belonging to others.

• Reputation impact — Spam or malicious activity from a "neighbor" site can get the shared IP blacklisted, affecting email deliverability or search rankings for everyone.

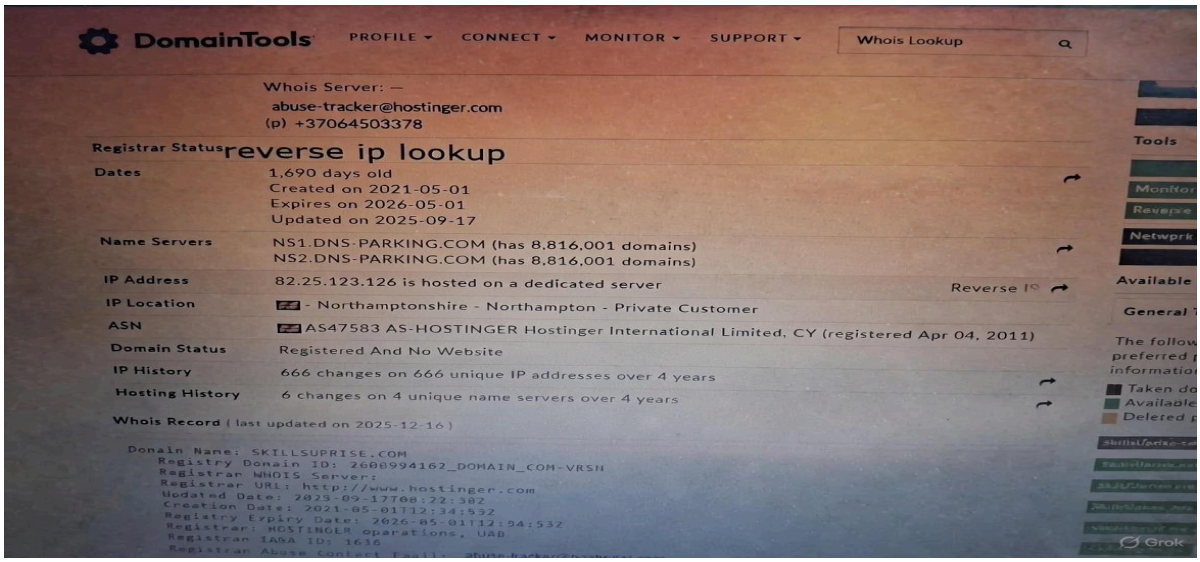
How Reverse IP Lookup Fits In
By resolving a domain to its IP and then querying which other domains resolve to that same IP, you can map the server's "neighborhood." Tools like:

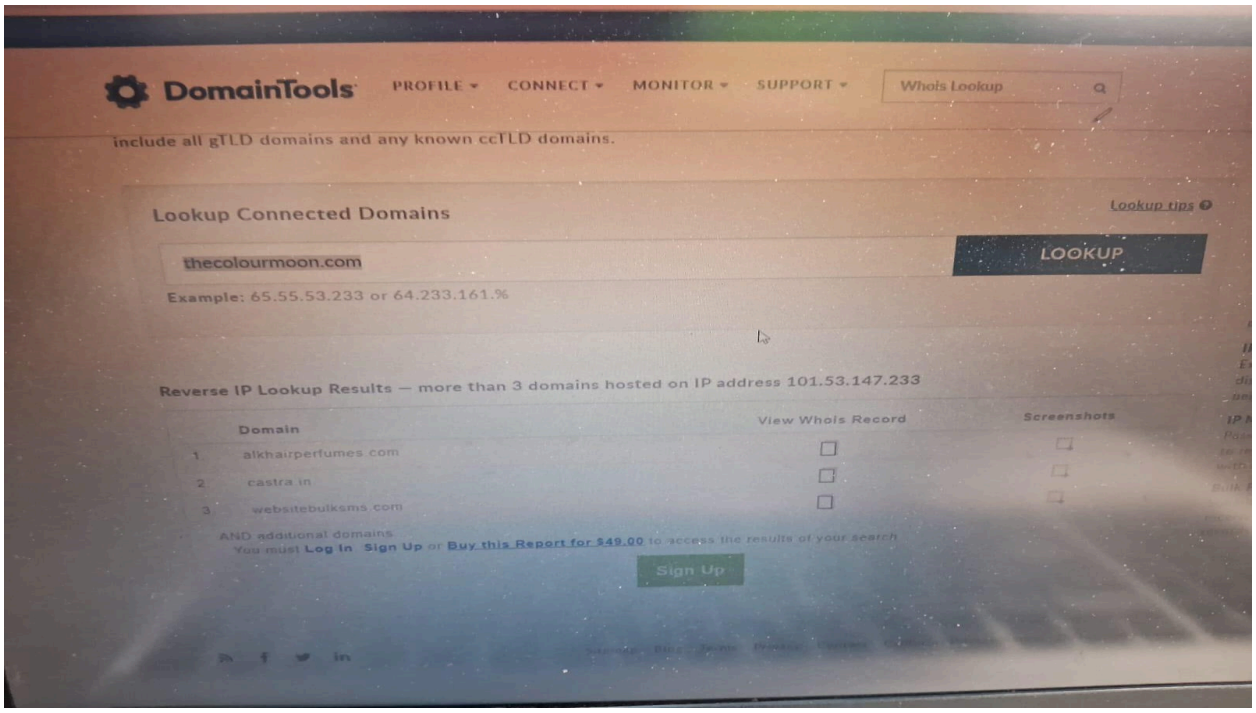
• HackerTarget.com/reverse-ip-lookup
• ViewDNS.info/reverseip
• YouGetSignal.com/tools/web-sites-on-web-server

• DomainTools.com/reverse-ip

...often reveal hundreds of sites. In penetration testing or bug bounty hunting, attackers might:

1. Target a seemingly secure site.
2. Find a weaker "neighbor" site via reverse IP.
3. Exploit the weak site to gain access.
4. Use that foothold to target the original site (bypassing its defenses indirectly).





Real-World Examples
This tactic has been used in mass compromises, such as:

• Darkleech (early 2010s) — Attackers broke into shared servers via vulnerable apps (WordPress/Joomla) and injected phishing/malware into all hosted sites.
• Phishing campaigns where attackers compromise low-security sites on shared hosts to host phishing pages that appear legitimate.

In practice, while complete server takeover from one site is harder now due to better isolation, it's still a valid vector — especially on cheaper shared (server) plans.

Darkleech's name itself dark=operates in security, hidden from normal users and admins,
leach = sucks resource or exploits traffic silently, like a parasite.

Darkleech is a sophisticated malware campaign that primarily targets Apache web servers to compromise websites and deliver malicious payloads to visitors. It operates by installing a malicious module on the server, which dynamically injects code into web pages, redirecting users to exploit kits (EKs) that exploit browser vulnerabilities to install malware. First identified in 2012, it has been responsible for compromising tens of thousands of websites, often in shared hosting environments, leading to widespread drive-by downloads of ransomware, trojans, and other threats.