WHOIS & Domain Lookups Cheat Sheet

What is WHOIS?

WHOIS is a query and response protocol used to retrieve information about domain registrations, including details about the owner, registrar, creation/expiration dates, and name servers.

WHOIS is a valuable tool for OSINT investigations, cybersecurity research, and identifying potential phishing or scam websites.

Basic WHOIS Commands

To perform a WHOIS lookup, use the following commands in a terminal:

Command	Description
`whois example.com`	Fetch WHOIS information for a domain.
`whois -h whois.verisign-grs.com example.com`	Query a specific WHOIS server (useful for .com and .net domains).
`whois -h whois.arin.net`	Perform WHOIS lookup on an IP address.
`whois -h whois.nic.xyz`	Query the WHOIS server for new TLDs

Some domains have privacy protection enabled, limiting the information visible in a WHOIS query.

What Information Can You Find with WHOIS?

A WHOIS lookup typically provides:

- **Domain Owner** (if not hidden by privacy protection)
- **Registrar Details** (the company where the domain is registered)
- **Creation & Expiration Dates**
- **Name Servers** (which control DNS settings)
- **Contact Information** (admin, technical, and registrant contacts, if available)

Online WHOIS Lookup Tools

If WHOIS queries are blocked on your system, you can use web-based tools:

- Whois Lookup (ICANN)
- Whois.com
- DomainTools
- ViewDNS.info

Domain Lookups with `nslookup`

`nslookup` (Name Server Lookup) is a command-line tool used for querying DNS records associated with a domain.

Basic `nslookup` Commands

Command	Description
`nslookup example.com`	Get the IP address of a domain.
`nslookup -type=NS`	Retrieve the name servers of a domain.
`nslookup -type=MX`	Find mail servers associated with a domain.
`nslookup -type=TXT example.com`	Fetch TXT records (useful for SPF, DKIM, and security checks).
`nslookup -type=CNAME sub.example.com`	Check if a subdomain is an alias (CNAME record).

Reverse WHOIS & Historical WHOIS

Sometimes, you may want to check the past records of a domain, or find all domains registered by a specific entity. Use the following tools:

- ViewDNS Reverse WHOIS
- DomainTools Historical WHOIS
- SecurityTrails WHOIS History

These tools can help identify old ownership details even if current WHOIS data is hidden.

Using WHOIS for OSINT Investigations

WHOIS and domain lookups can help:

✅ Identify malicious websites and phishing attempts.
✅ Track down domain owners for investigative journalism.
✅ Monitor domain expiration to prevent domain squatting.
✅ Verify website legitimacy for business and security research.

⚠️ **Note:** Many registrars offer privacy protection, meaning WHOIS data may not always reveal personal information. Always use this tool **legally and ethically**.

WHOIS and domain lookups are essential tools in OSINT, cybersecurity, and research. Understanding how domains are registered and managed helps uncover hidden connections and potential security risks.

Use responsibly, and happy investigating! 🔍