OSINT Investigation with WHOIS – Unmasking Suspicious Websites

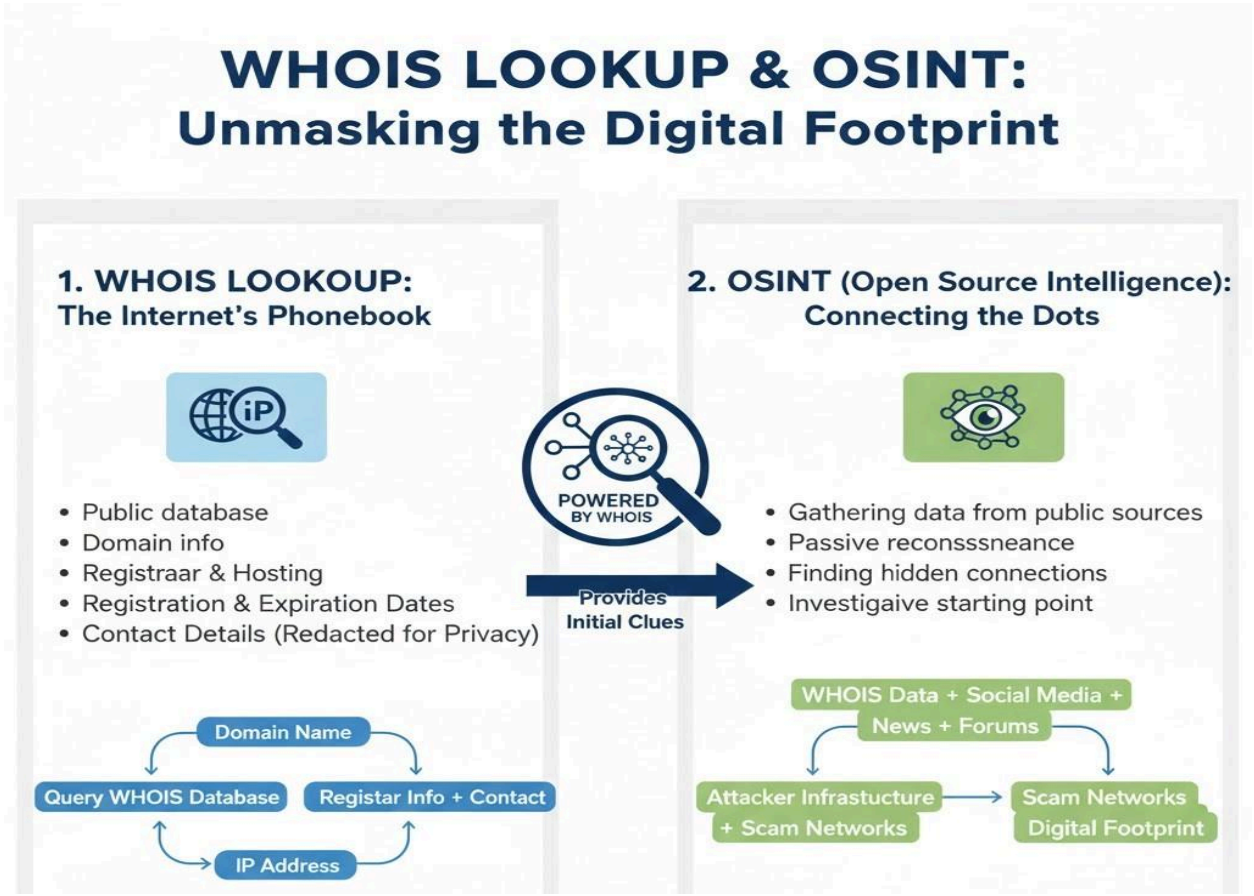
Subject: Ethical Hacking – Open Source Intelligence (OSINT) in Practice
Objective: To demonstrate how WHOIS lookups can expose domain registration details and help identify fraudulent or suspicious websites.

Introduction

In today's digital world, cyber threats often originate from deceptive websites posing as legitimate businesses.
As part of a cybersecurity learning exercise, I decided to move beyond guesswork and use WHOIS, a fundamental **OSINT** tool, to investigate several types of websites:

1. A Suspicious job consultancy
2. School website
3. Tech firm's website
4. Hospital's website

WHOIS provides registration data about domain names, including registrar, hosting provider, creation date, and contact details. This information can reveal patterns of fraud, link multiple fake sites, and preserve digital evidence.



1. Suspicious Job Consultancy Website
A website contacted me offering a job in exchange for a “security deposit.” Such requests are red flags for advance-fee scams.
I performed a WHOIS lookup on the domain (e.g., fakejobconsultancy.com).

Example:
Registrar: A registrar known for anonymity services
Creation Date: Registered only 2 weeks ago
Registrant Info: “Privacy Protection Service” or generic details like “Admin, Country: Panama”
Name Servers: Hosted on a cheap, offshore hosting provider
OSINT Insights:
New Domains: Scammers frequently create new domains to avoid being blacklisted.
Privacy Shields: Use of privacy protection services to hide identity is common in fraudulent sites.
Hosting Patterns: Many scam sites use the same hosting provider or IP block.
Conclusion:
If a job website asks for money and its WHOIS shows recent registration + privacy protection + offshore hosting, it’s likely a scam. This can be reported to the hosting provider and registrar for takedown.

2. School Website
I chose a local school’s website to learn how legitimate educational institutions appear in WHOIS records.
Example:
Registrant: “Greenwood Public School” or the school trust name
Admin Contact: Official school email (e.g., admin@greenwood.edu)
Creation Date: Several years old (e.g., 2010)
Registrar: Reputable (e.g., GoDaddy, Namecheap)
Name Servers: Often tied to established hosting or the school’s own server
OSINT Insights:
Transparency: Legitimate organizations usually have clear, identifiable registrant details.
Longevity: Established domains indicate credibility.
Consistency: Contact emails match the domain.
Conclusion:
WHOIS can help verify the authenticity of an educational website. Discrepancies (like personal email addresses or very recent creation) could signal a phishing site mimicking the school.

3. Tech Firm Website

Tech companies often have professional online presence. I analyzed one to see corporate registration patterns.

Example:

Registrant: The company's legal name (e.g., "TechSolutions Inc.")
Tech Contact: Often includes the IT department's email
Creation Date: Aligns with company founding or rebranding
Registrar: Corporate-friendly registrars (e.g., MarkMonitor, Cloudflare)
DNS Hosting: May use enterprise-level services like AWS Route 53 or Cloudflare
OSINT Insights:
Brand Protection: Legitimate companies often register domains years in advance and use professional registrars.
Linked Domains: They may own multiple related domains (e.g., typosquatting protection).
Security: Some use domain privacy for corporate security but still have verifiable business details.

Conclusion:

For tech firms, WHOIS can reveal how seriously they take their digital footprint. Missing or hidden details in a "tech" website could indicate a fake site used for social engineering or malware distribution.

4. Hospital / Healthcare Website

Hospitals are critical infrastructure and often targeted for phishing or misinformation. I examined a hospital site's WHOIS record.

Example:

Registrant: Often the hospital's full legal name or parent healthcare system
Contact: Email with hospital domain (e.g., it@cityhospital.org)
Creation Date: Many years old
Registrar: Reputable, with possible extra security (DNSSEC)
Hosting: May be managed by a healthcare IT provider
OSINT Insights:
High Stakes: Legitimate healthcare sites avoid anonymity.
Regulatory Compliance: They may show clear contact information in line with regional regulations.
Impersonation Risk: Fake hospital sites can be spotted via recent registration + privacy-enabled WHOIS.

Conclusion:

A fake hospital site could be used for stealing patient data or spreading medical scams. WHOIS helps quickly differentiate real from fake, protecting potential victims.
How WHOIS Serves as an OSINT Starting Point
Identifying Scam Networks:
By comparing WHOIS data across multiple suspicious sites, you can find common registrants, email addresses, or name servers—exposing a network of fake websites.
Linking Multiple Fake Websites:
Example: If fakejobconsultancy.com and faketechfirm.com share the same admin email or hosting IP, they're likely operated by the same threat actor.
Preserving Evidence:
WHOIS records can change or be hidden. Screenshots and archived queries (using tools like Wayback Machine) help maintain evidence for reporting or legal action.
Supporting Further Investigation:
WHOIS provides leads for deeper OSINT:
IP history checks
SSL certificate analysis
Associated domains search (e.g., using whoisxmlapi.com)

Conclusion:
WHOIS is a powerful, accessible tool for initial domain intelligence. Whether investigating a suspicious job scam or verifying a legitimate institution, WHOIS data reveals patterns that help in:
Risk assessment
Fraud detection
Evidence collection
Cyber hygiene awareness
As cybersecurity professionals, incorporating WHOIS into our OSINT toolkit enables us to proactively identify threats and protect users from online deception.

Note: Always perform a WHOIS check on unknown or unsolicited websites.
Look for red flags: recent creation, privacy protection, mismatched contact info.
Use complementary tools: VirusTotal, Shodan, and SSL checks for fuller analysis.
Report suspicious domains to hosting providers and authorities like ICANN's Abuse Contact.