DAY -5

- **Reverse IP Lookup Concept:**
- Discovering other sites on the same server.
  OSINT for uncovering network fontprit.

- **Shared Hosting Vulerability:**
- Cross-site contamination
  Exploting misconfgurations.
- Resource monopolization
  Resource monopolization

Firewall configurations (physical & digital).

- **Server Infrastucture Security:**
- HUMAN ERROR (phishing, weak passwords
- **Weakest Link of Websites:**
- Outdaed software
  Misconfigured plugins/themes.
- Lack of encryption (SSL/TLS).

REVERSE IP LOOKOUP

- Process of finding all domain names on a single IP address
- Discover other websites sharing th a same server infrastrcture
- Works by Query DNS records in reverse – from IP to domain to idatify all domain names instead otof domain to IP

Advantages:

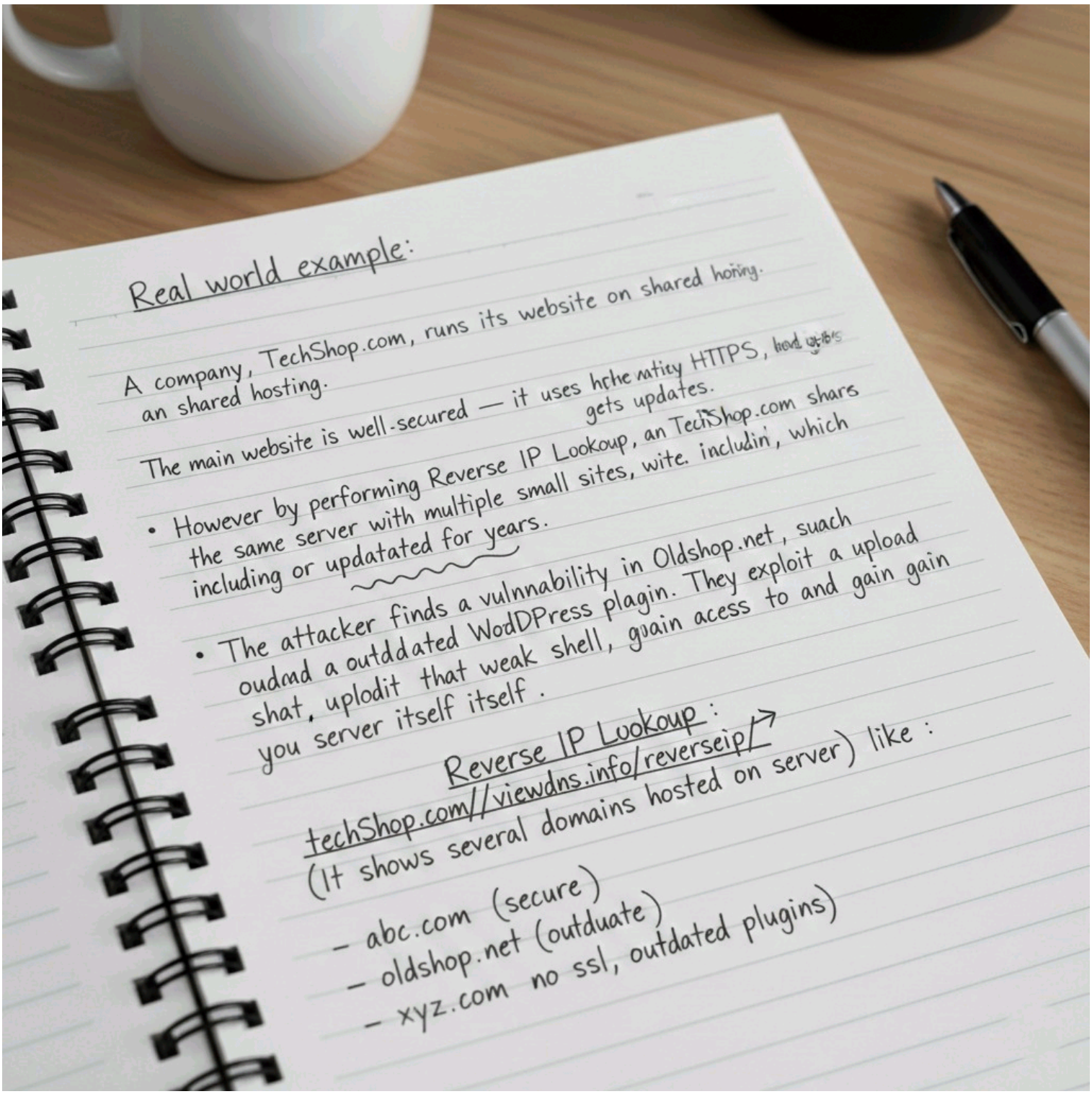
- One IP address can host multiple domains (virtual hosting)
- Reveals the complete picture of server infrastrcture
- Useful for findify all assetd websites and hidden assets

Online Tools used:
viewdns.info, yougetsignal.com, hackertarget.com

SHARED HOSTING

- Multiple websites hosted: the same physical server sharing resources
- Hundreds for small buisands sites on one IP address
- Resource Abuse: One site consuming website can affect all others
- Resource Abuse: One site consuming excesive resources all others
- Security Isolation Issues: Weak file permssions allow other sites' files
- SSL/TLS Certificate Issues: Shared IP compliate SSL implementation

- Real world attacks: Neighnbor Attack, Privilege Leakgae, Backdoor Persitence


Real world example:
A company, TechShop.com, runs its website on shared hosting.
The main website is well-secured — it uses HTTPS, and gets updates.
• However by performing Reverse IP Lookoup, an TechShop.com shares the same server with multiple small sites, including or updatated for years.
• The attacker finds a vulnnability in Oldshop.net, suach oudnd a outddated WodDPress plagin. They exploit a upload shat, uplodit that weak shell, gpain acess to and gain gain you server itself itself.
Reverse IP Lookoup:
techShop.com//viewdns.info/reverseip/
(It shows several domains hosted on server) like:
- abc.com (secure)
- oldshop.net (outduate)
- xyz.com no ssl, outdated plugins)

Now target the weak site :

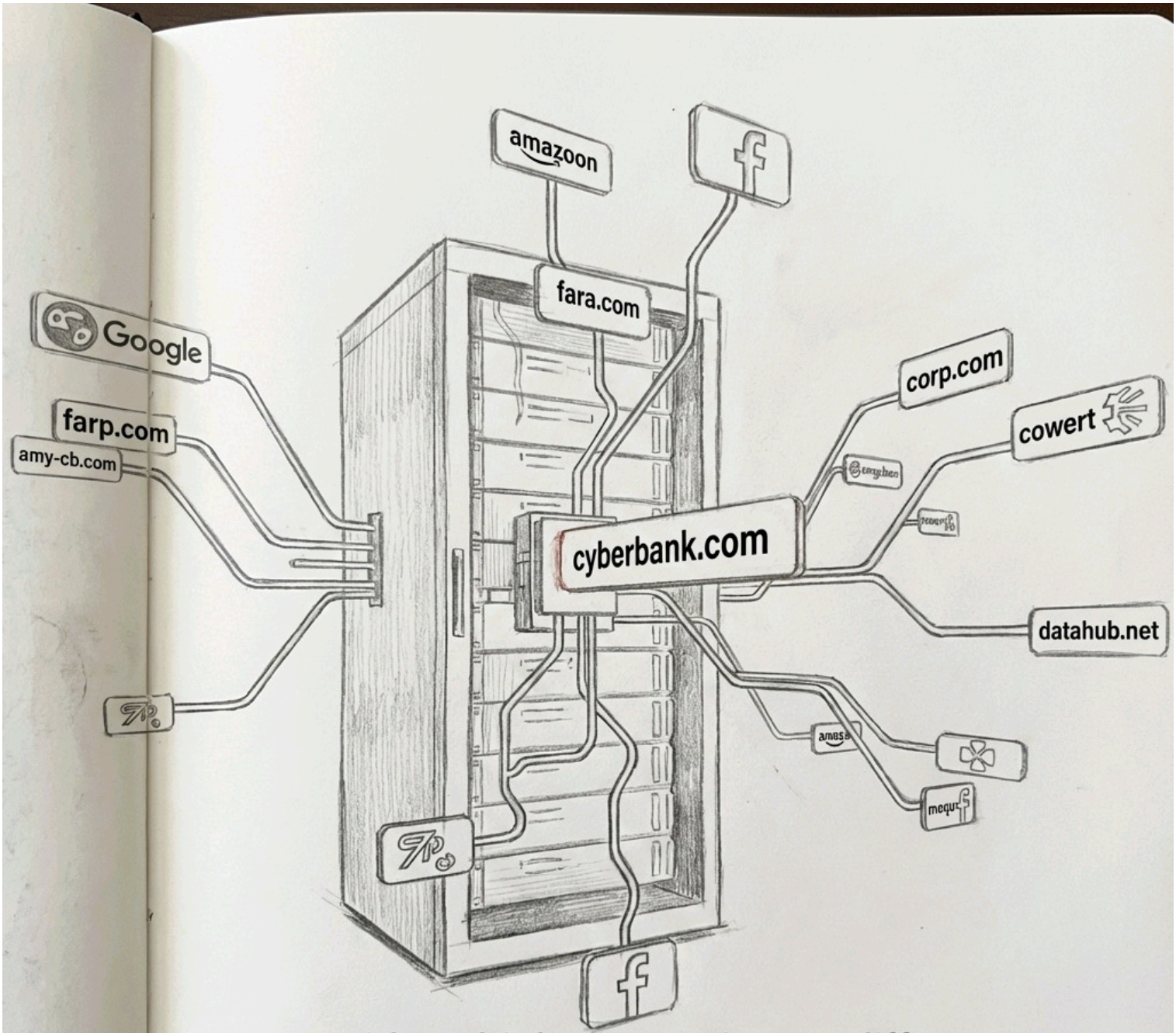
nikto -h oldshop.net (it finds the outdated plugins with a RCE (remote emote code execution)

Now exploit vunearbility :

{<>php system(<GET'cmd)}->}

Access the simple web shell :
http://oldshop.net,com/shell.php?cmd.ls
(Now we can access to the other websites on the same server)

Finally we can say that, One weak door (a vunerable website) can give access to the whole building (the server, even if another door (the main site) is locked.



A server with multiple connections to different websites domains, if one connection is breached it effect all the connections.