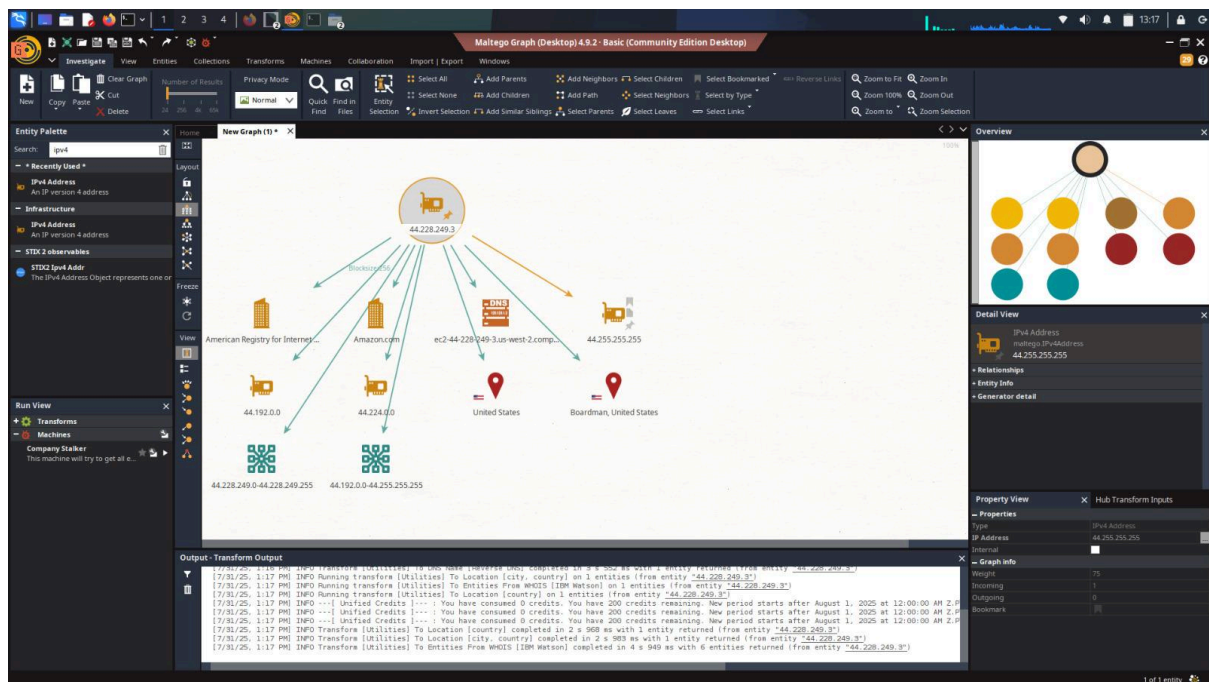


1: Maltego



Maltego is open source intelligence and it is designed to gather and visualize information from various public sources on the internet.

2.dig testphp.vulnweb.com , whois 44.228.249.3

```
(rohinish@kali) ~$ dig testphp.vulnweb.com

;<<>> DiG 9.20.9-1-Debian <<>> testphp.vulnweb.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 21297
;; Flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;testphp.vulnweb.com.      IN      A
;; ANSWER SECTION:
testphp.vulnweb.com.      3442    IN      A      44.228.249.3

;; Query time: 7 msec
;; SERVER: 10.46.101.98#53(10.46.101.98) (UDP)
;; WHEN: Thu Jul 31 13:18:53 IST 2025
;; MSG SIZE rcvd: 53

(rohinish@kali) ~$ whois 44.228.249.3

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy\_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#

# start
NetRange: 44.192.0.0 - 44.255.255.255
CIDR: 44.192.0.0/10
NetName: AMAZO-4
NetHandle: NET-44-192-0-0-1
Parent: NET44 (NET-44-0-0-0-0)
NetType: Direct Allocation
OriginAS:
```

```
OrgName: Amazon.com, Inc.
OrgId: AMAZO-4
Address: Amazon Web Services, Inc.
Address: P.O. Box 81226
City: Seattle
StateProv: WA
PostalCode: 98108-1226
Country: US
RegDate: 2005-09-29
Updated: 2022-09-30
Comment: For details of this service please see
Comment: http://ec2.amazonaws.com
Ref: https://rdap.arin.net/registry/entity/AMAZO-4

OrgRoutingHandle: ARMP-ARIN
OrgRoutingName: AWS RPKI Management POC
OrgRoutingPhone: +1-206-555-0000
OrgRoutingEmail: aws-rpki-routing-poc@amazon.com
OrgRoutingRef: https://rdap.arin.net/registry/entity/ARMP-ARIN

OrgNOCHandle: AAN01-ARIN
OrgNOCName: Amazon AWS Network Operations
OrgNOCPhone: +1-206-555-0000
OrgNOCEmail: amzn-noc-contact@amazon.com
OrgNOCRef: https://rdap.arin.net/registry/entity/AAN01-ARIN

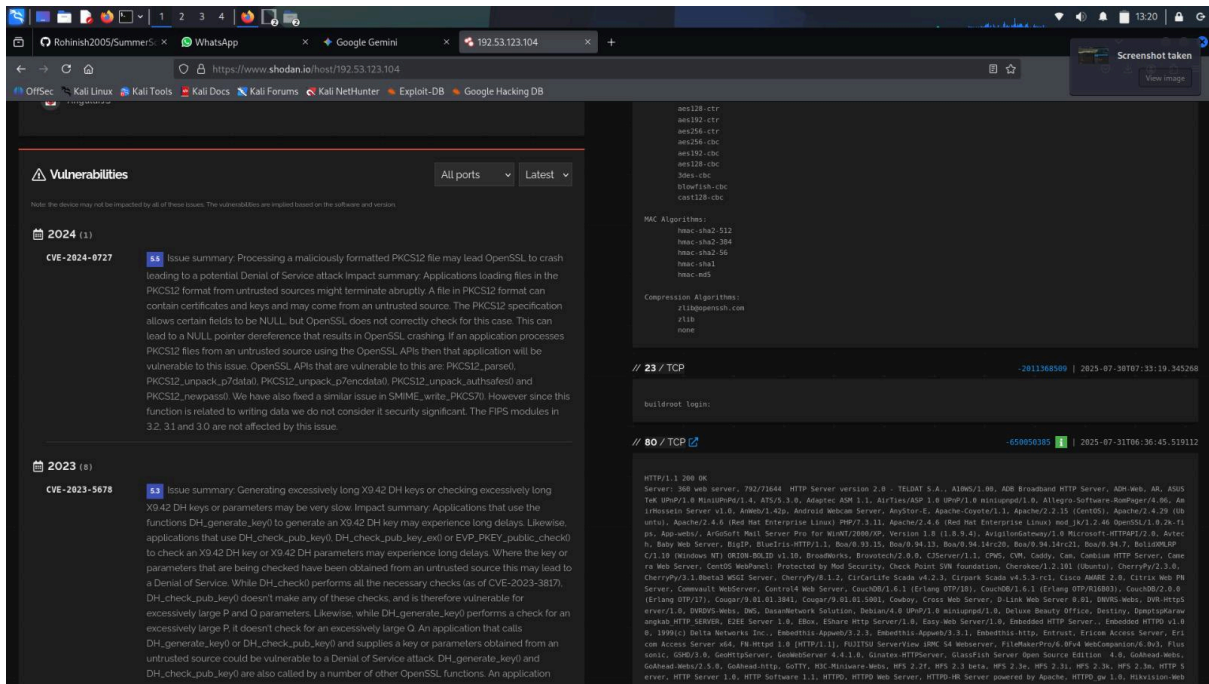
OrgAbuseHandle: AEAS-ARIN
OrgAbuseName: Amazon EC2 Abuse
OrgAbusePhone: +1-206-555-0000
OrgAbuseEmail: trustandsafety@support.aws.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/AEAS-ARIN

OrgTechHandle: ANO24-ARIN
OrgTechName: Amazon EC2 Network Operations
OrgTechPhone: +1-206-555-0000
OrgTechEmail: amzn-noc-contact@amazon.com
OrgTechRef: https://rdap.arin.net/registry/entity/ANO24-ARIN

OrgRoutingHandle: IPROU3-ARIN
OrgRoutingName: IP Routing
OrgRoutingPhone: +1-206-555-0000
OrgRoutingEmail: aws-routing-poc@amazon.com
```

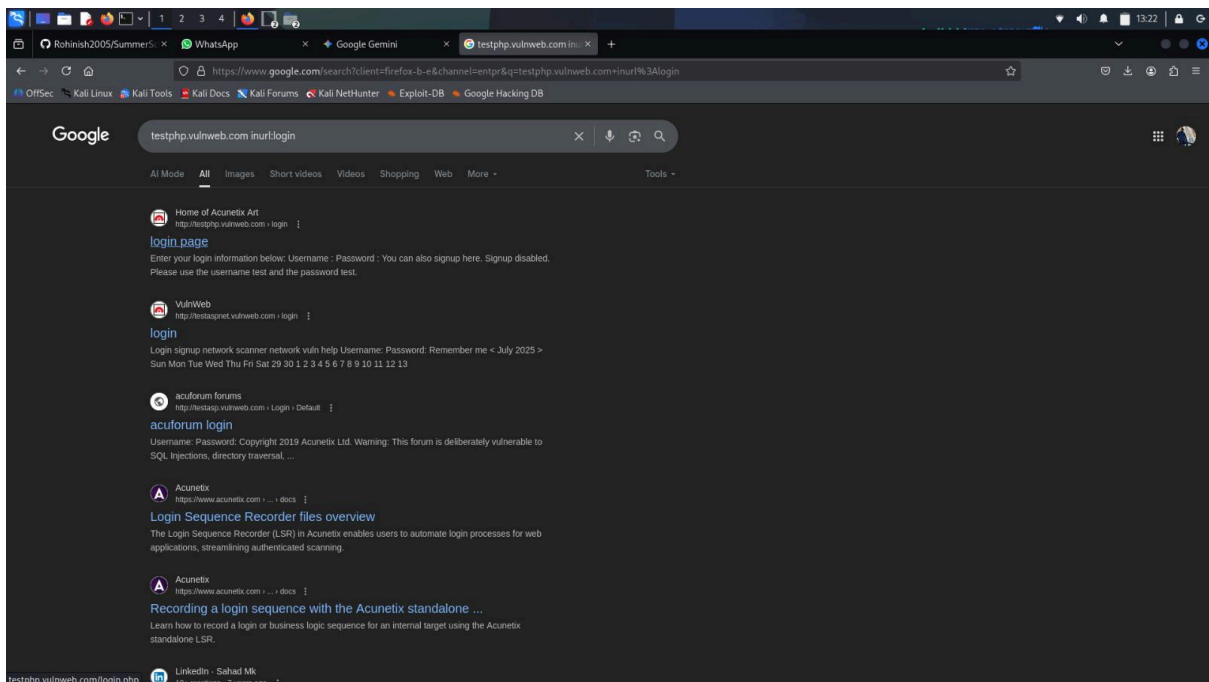
Dig and whois commands are both used in network troubleshooting and information gathering.

3.Shodan.io/host/192.53.123.104



Shodan is a search engine for internet connected devices, often referred to as the search engine for hacker due to its utility in cyber security

4. testphp.vulnweb.com



Here we are performing footprinting via Google Dorks on a test website :testphp.vulnweb.com

5.Loginpage

