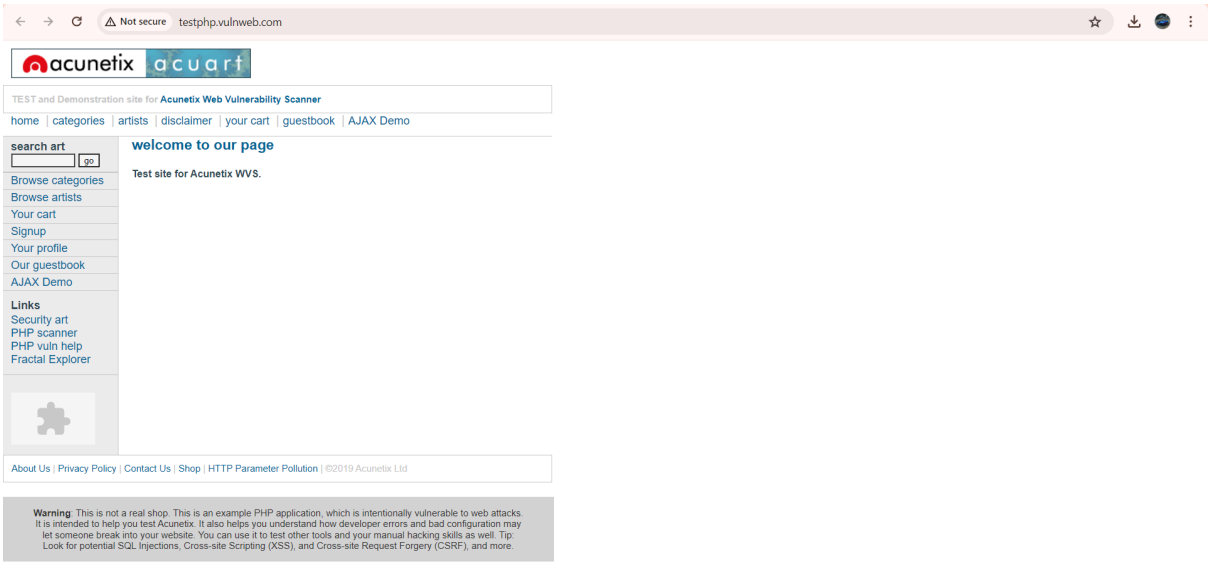
Name: SHAIK ABDUR RAAZIQ
Regd.No: 721128805397
College: Dr.Lankapalli BullayyaCollege

Assignment 1

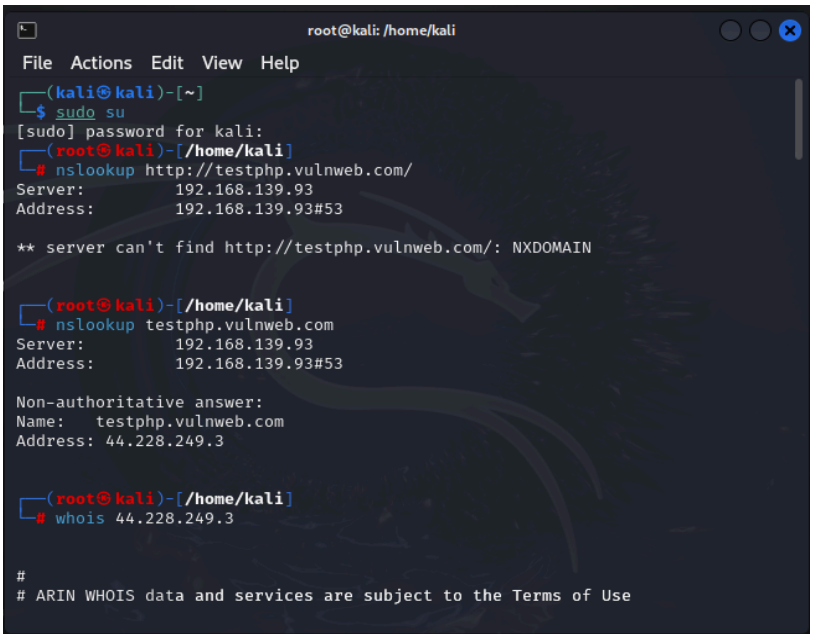
Step 1 -

The demo site is http://testphp.vulnweb.com/

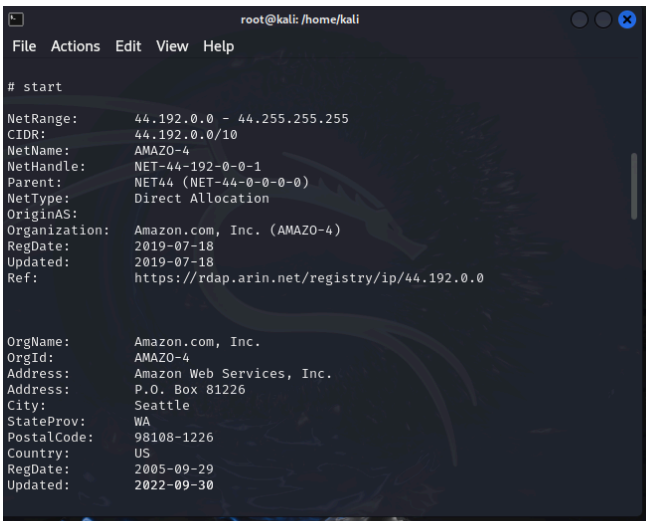


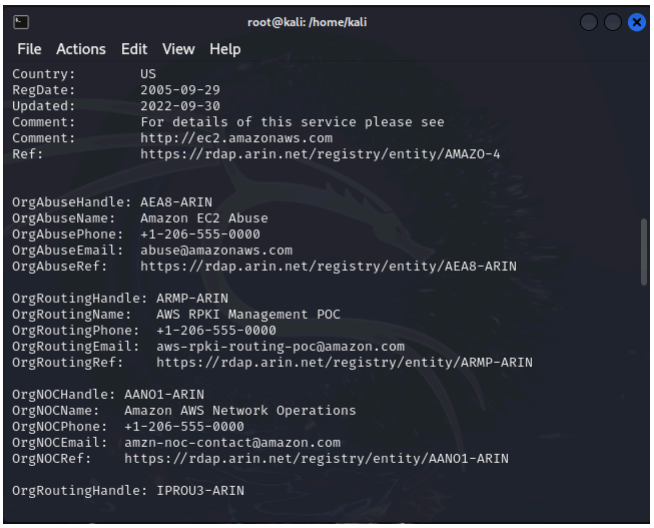
Step 2: Perform footprinting and reconnaissance -

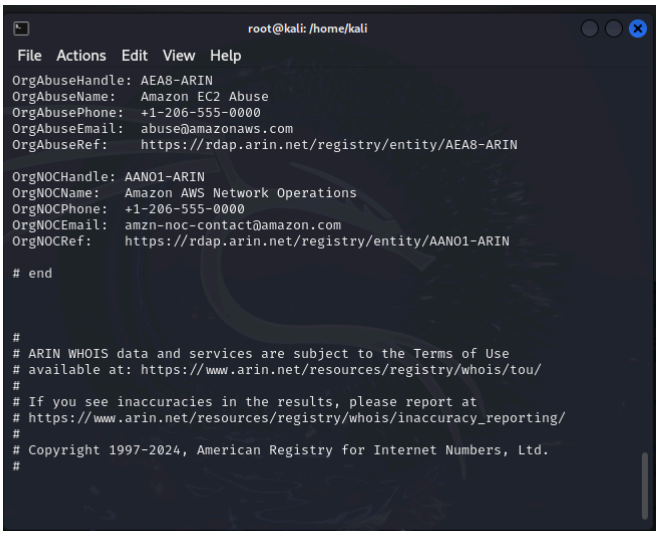
Using nslookup find the ip address of the target and use whois command to get further details



The ip address is 44.228.249.3


root@kali: /home/kali
File Actions Edit View Help
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:
Organization: Amazon.com, Inc. (AMAZO-4)
RegDate: 2019-07-18
Updated: 2019-07-18
Ref: https://rdap.arin.net/registry/ip/44.192.0.0
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


root@kali: /home/kali
File Actions Edit View Help
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
OrgAbuseHandle: AEA8-ARIN
OrgAbuseName: Amazon EC2 Abuse
OrgAbusePhone: +1-206-555-0000
OrgAbuseEmail: abuse@amazonaws.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/AEA8-ARIN
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: AANO1-ARIN
OrgNOCName: Amazon AWS Network Operations
OrgNOCPhone: +1-206-555-0000
OrgNOCEmail: amzn-noc-contact@amazon.com
OrgNOCRef: https://rdap.arin.net/registry/entity/AANO1-ARIN
OrgRoutingHandle: IPROU3-ARIN


root@kali: /home/kali
File Actions Edit View Help
OrgAbuseHandle: AEA8-ARIN
OrgAbuseName: Amazon EC2 Abuse
OrgAbusePhone: +1-206-555-0000
OrgAbuseEmail: abuse@amazonaws.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/AEA8-ARIN
OrgNOCHandle: AANO1-ARIN
OrgNOCName: Amazon AWS Network Operations
OrgNOCPhone: +1-206-555-0000
OrgNOCEmail: amzn-noc-contact@amazon.com
OrgNOCRef: https://rdap.arin.net/registry/entity/AANO1-ARIN
end
#
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 1997-2024, American Registry for Internet Numbers, Ltd.
#

Step 3: Using Nmap, a network scanning tool -

After using nmap it is clearly found that one port is open.