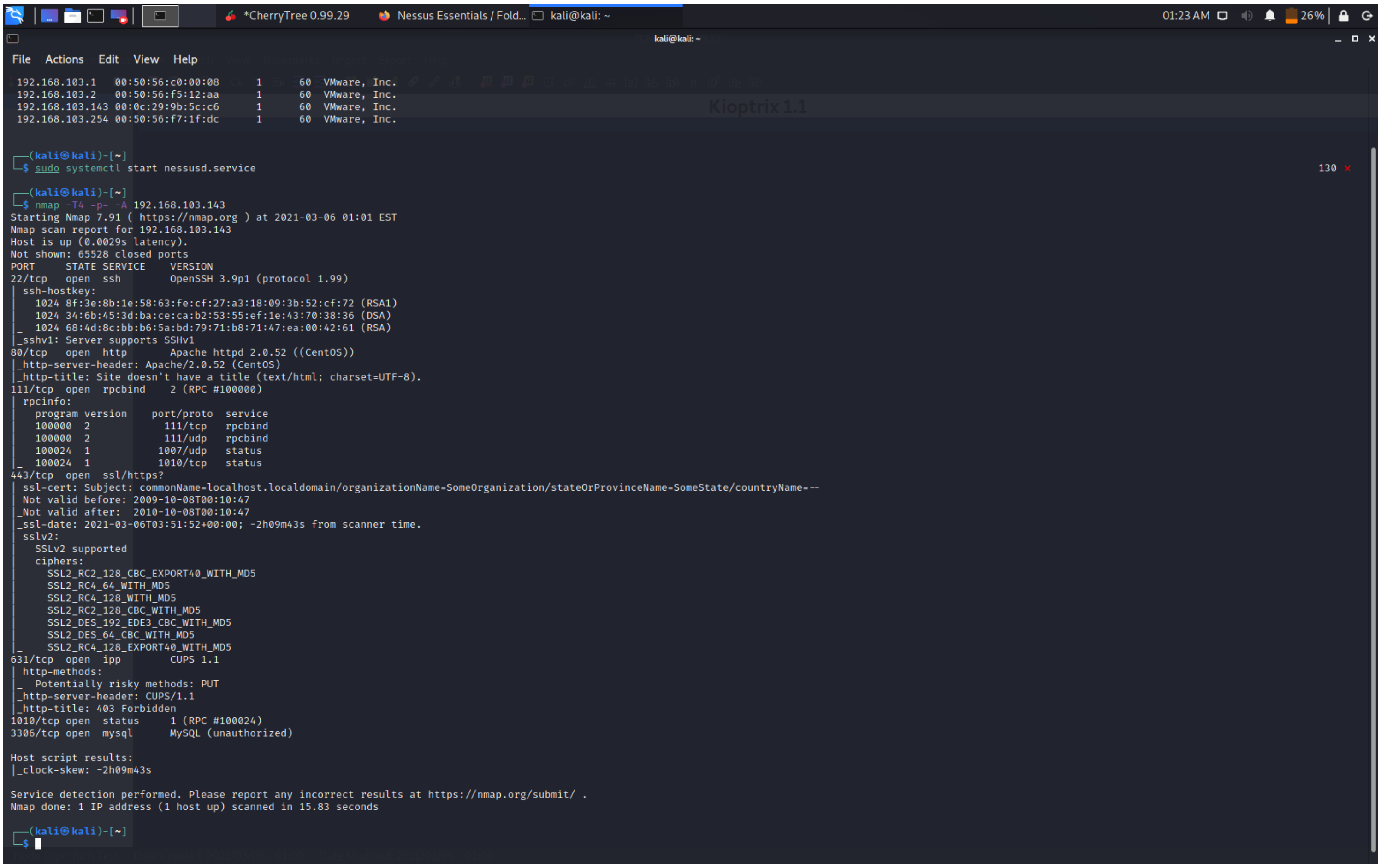
Kioptrix 1.1



```
 192.168.103.1   00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.103.2   00:50:56:f5:12:aa      1      60  VMware, Inc.
 192.168.103.143 00:0c:29:9b:5c:c6      1      60  VMware, Inc.
 192.168.103.254 00:50:56:f7:1f:dc      1      60  VMware, Inc.


┌──(kali㉿kali)-[~]
└─$ sudo systemctl start nessusd.service

┌──(kali㉿kali)-[~]
└─$ nmap -T4 -p- -A 192.168.103.143
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-06 01:01 EST
Nmap scan report for 192.168.103.143
Host is up (0.0029s latency).
Not shown: 65528 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 3.9p1 (protocol 1.99)
| 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)
|_sshv1: Server supports SSHv1
80/tcp   open  http       Apache httpd 2.0.52 ((CentOS))
|_http-server-header: Apache/2.0.52 (CentOS)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
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           1007/udp   status
|_  100024  1           1010/tcp   status
443/tcp  open  ssl/https?
| 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
|_ssl-date: 2021-03-06T03:51:52+00:00; -2h09m43s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_64_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
631/tcp  open  ipp        CUPS 1.1
| http-methods:
|_  Potentially risky methods: PUT
|_http-server-header: CUPS/1.1
|_http-title: 403 Forbidden
1010/tcp open  status     1 (RPC #100024)
3306/tcp open  mysql      MySQL (unauthorized)

Host script results:
|_clock-skew: -2h09m43s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.83 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

22/tcp

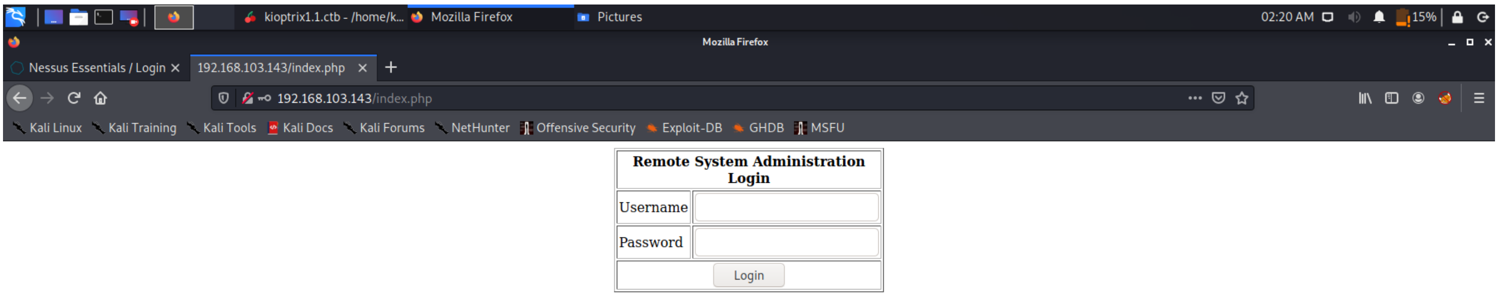
PORT	**STATE**	**SERVICE**	**VERSION**
22/tcp	open	ssh	OpenSSH 3.9p1 (protocol 1.99)

OpenSSH 8.5 was released on 2021-03-03. It is available from the mirrors listed at https://www.openssh.com/.

80/tcp

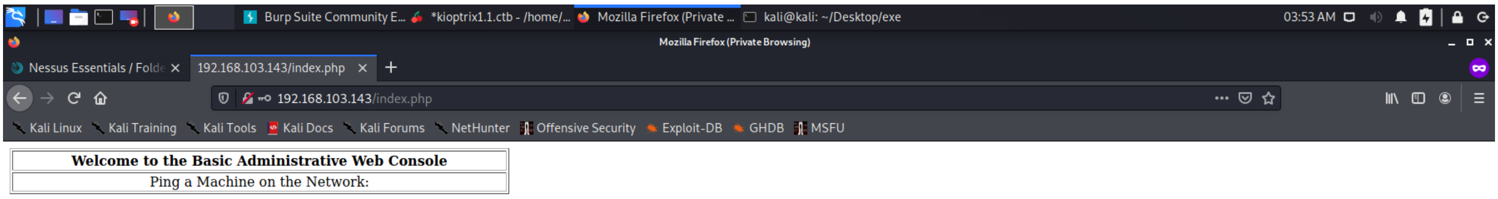
80/tcp   open http   Apache httpd 2.0.52 ((CentOS))

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.103.143
+ Target Hostname:    192.168.103.143
+ Target Port:        80
+ Start Time:         2021-03-06 02:22:10 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.0.52 (CentOS)
+ Retrieved x-powered-by header: PHP/4.3.9
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Apache/2.0.52 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ Uncommon header 'tcn' found, with contents: choice
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ Server may leak inodes via ETags, header found with file /icons/README, inode: 357810, size: 4872, mtime: Sat Mar 29 13:41:04 1980
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8725 requests: 1 error(s) and 17 item(s) reported on remote host
+ End Time:           2021-03-06 02:22:51 (GMT-5) (41 seconds)
---------------------------------------------------------------------------
```



Remote System Administration Login	
Username	
Password	
Login	

SQL Injection


Burp Suite Community E...
*kioptrix1.1.ctb - /home/...
Mozilla Firefox (Private ...
kali@kali: ~/Desktop/exe
03:53 AM
Mozilla Firefox (Private Browsing)
Nessus Essentials / Folde
192.168.103.143/index.php
192.168.103.143/index.php
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU

Welcome to the Basic Administrative Web Console

Ping a Machine on the Network:

Server: Apache/2.0.52 (CentOS)

Server: Apache/2.0.52 (CentOS)

> modules/arch/win32/mod_isapi.c in mod_isapi in the Apache HTTP Server 2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7, when running on Windows, does not ensure that request processing is complete before calling isapi_unload for an ISAPI .dll module, which allows remote attackers to execute arbitrary code via unspecified vectors related to a crafted request, a reset packet, and "orphaned callback pointers."

exploit: https://www.exploit-db.com/exploits/11650

111/tcp

111/tcp open rpcbind   2 (RPC #100000)

443/tcp

443/tcp open ssl/https?

```
| 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
|_ssl-date: 2021-03-06T03:51:52+00:00; -2h09m43s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_64_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
```

631/tcp

```
631/tcp  open  ipp       CUPS 1.1
| http-methods:
|_  Potentially risky methods: PUT
|_http-server-header: CUPS/1.1
|_http-title: 403 Forbidden
```

Exploit Result:

```
┌──(kali㉿kali)-[~/Desktop/exe]
└─$ python 41233.py -a 192.168.103.143 -b 631 -
f                                                                                         1 ×

           lol ty google
           0000000000000
        0000000000000000000   00
      00000000000000000000000000000
     0000000000000000000000000000000
   000000000           0000000000
  00000000             0000000000
  0000000              000000000000
 0000000             000000000000000
 000000            000000000  000000
0000000          000000000    000000
000000          000000000     000000
000000         000000000       000000
000000        00000000         000000
000000      000000000          000000
0000000   000000000          0000000
 000000   000000000           000000
 0000000000000000            0000000
  0000000000000             0000000
   00000000000            00000000
   00000000000          000000000
  0000000000000000000000000000000
   00000000000000000000000000000
    000  0000000000000000000
```

0000000000000
@0x00string
https://github.com/0x00string/oldays/blob/master/CVE-2015-1158.py

```
[*]    locate available printer
[-]    no printers
```

1010/tcp

```
1010/tcp open  status     1 (RPC #100024)
```

3306/tcp

```
3306/tcp open  mysql      MySQL (unauthorized)
```