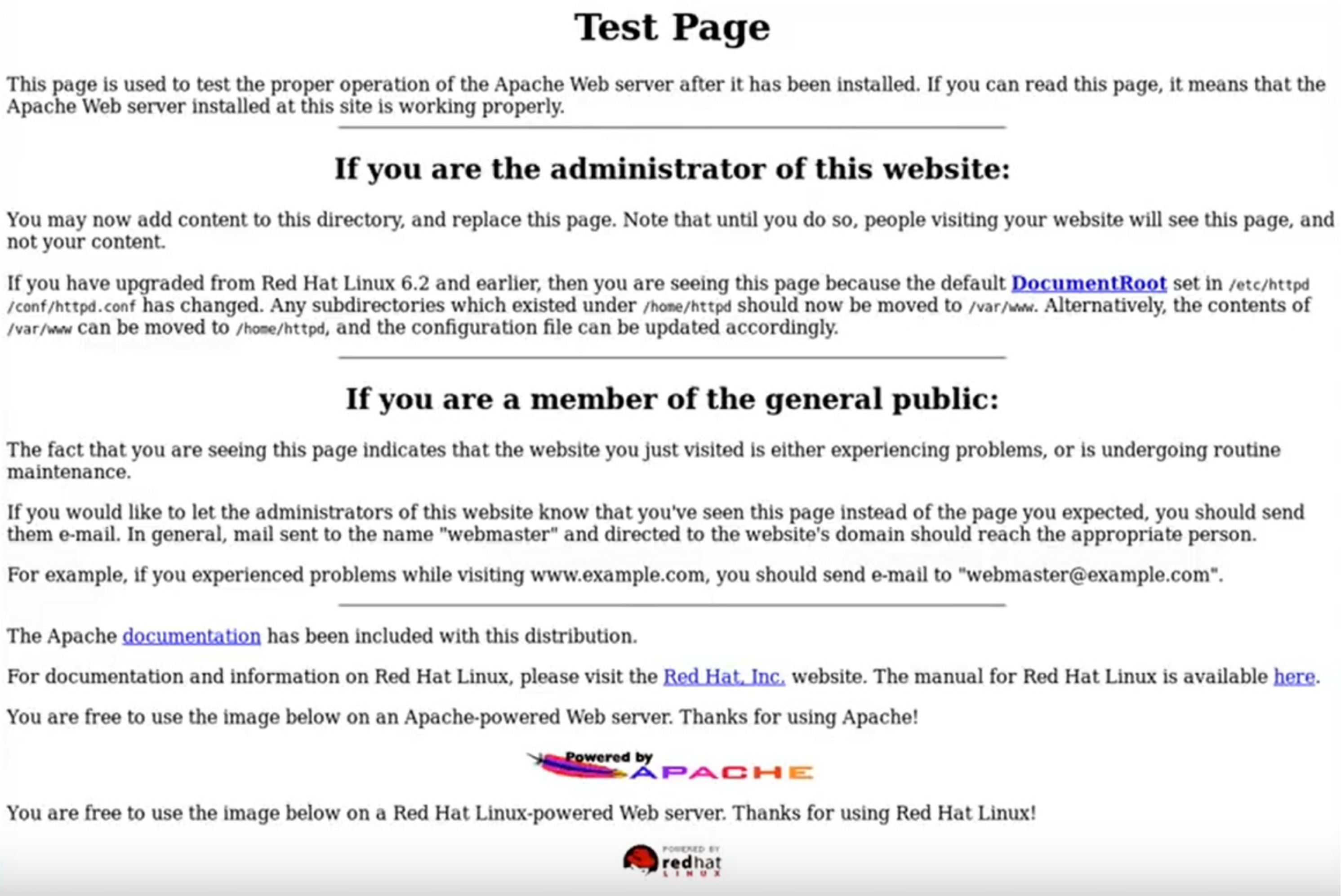
Kioptrix

Vulnerabilities

Default Web Page (Low)

default apache test page out in the open (not critical issue but it gives away information for free + it’s poor hygiene

IP.addr = 192.168.202.130



Test Page

This page is used to test the proper operation of the Apache Web server after it has been installed. If you can read this page, it means that the Apache Web server installed at this site is working properly.

If you are the administrator of this website:

You may now add content to this directory, and replace this page. Note that until you do so, people visiting your website will see this page, and not your content.

If you have upgraded from Red Hat Linux 6.2 and earlier, then you are seeing this page because the default DocumentRoot set in /etc/httpd/conf/httpd.conf has changed. Any subdirectories which existed under /home/httpd should now be moved to /var/www. Alternatively, the contents of /var/www can be moved to /home/httpd, and the configuration file can be updated accordingly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

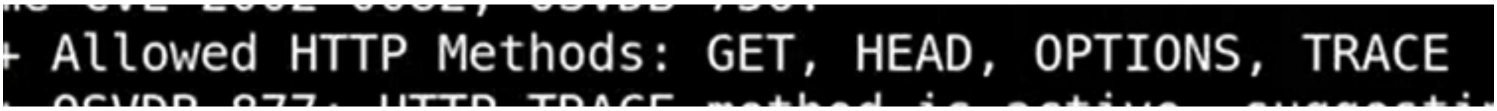
The Apache documentation has been included with this distribution.

For documentation and information on Red Hat Linux, please visit the Red Hat, Inc. website. The manual for Red Hat Linux is available here.

You are free to use the image below on an Apache-powered Web server. Thanks for using Apache!

You are free to use the image below on a Red Hat Linux-powered Web server. Thanks for using Red Hat Linux!

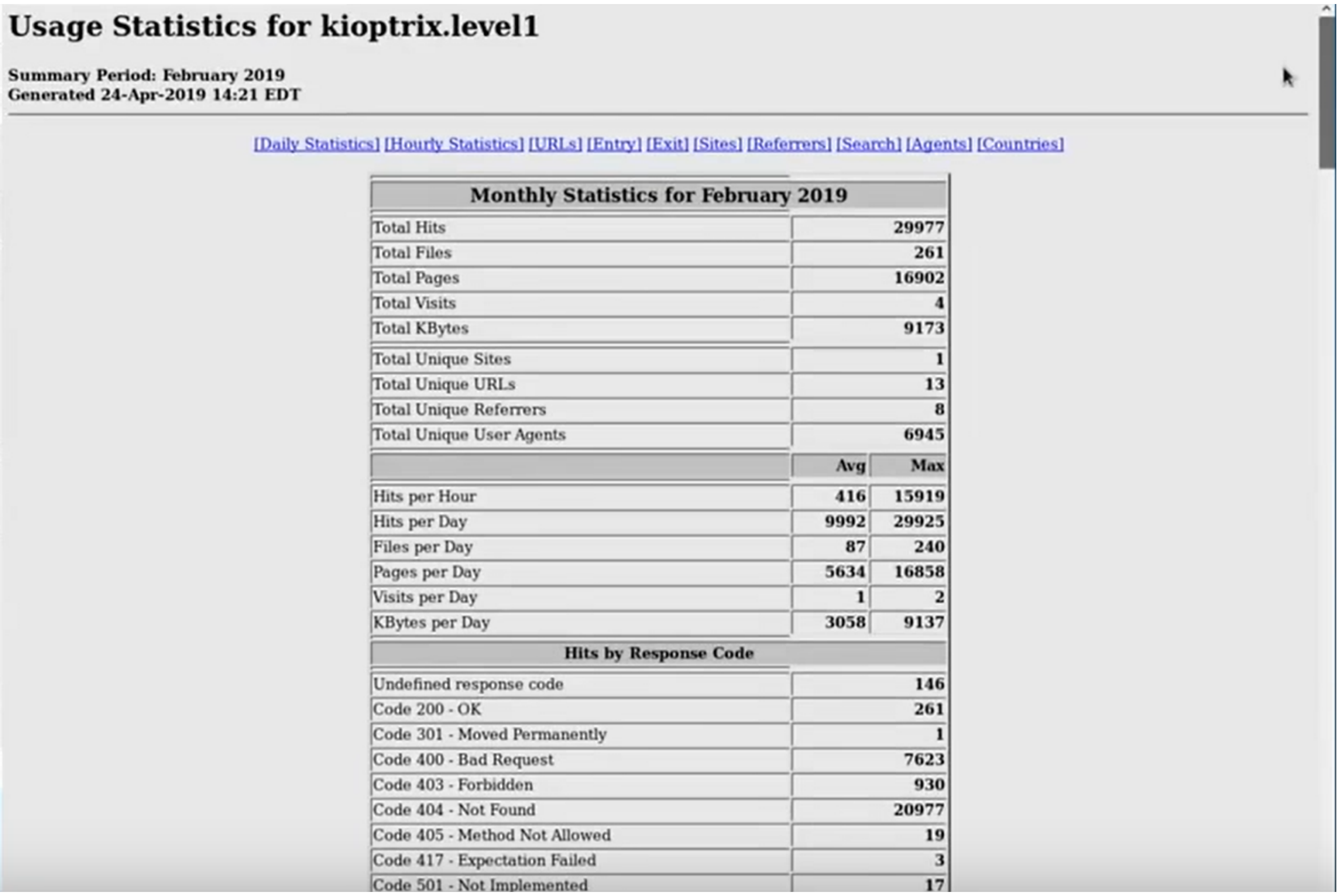
HTTP TRACE Method allowed (Low)



```
+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
```

Usage statistics (Low)

Is there a reason this is visible for non-adnim users?



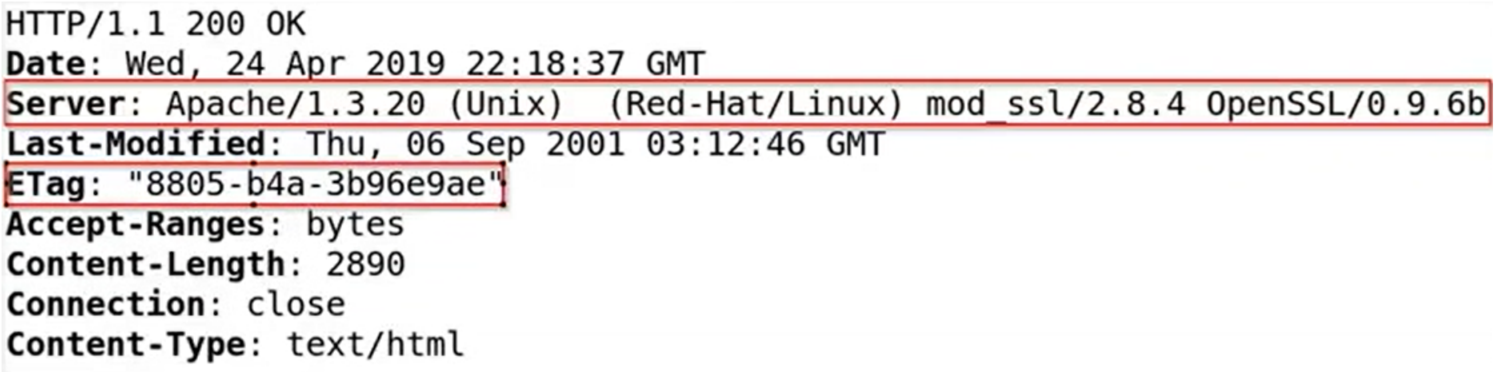
Usage Statistics for kioptrix.level1

Summary Period: February 2019
Generated 24-Apr-2019 14:21 EDT

[Daily Statistics] [Hourly Statistics] [URLs] [Entry] [Exit] [Sites] [Referrers] [Search] [Agents] [Countries]

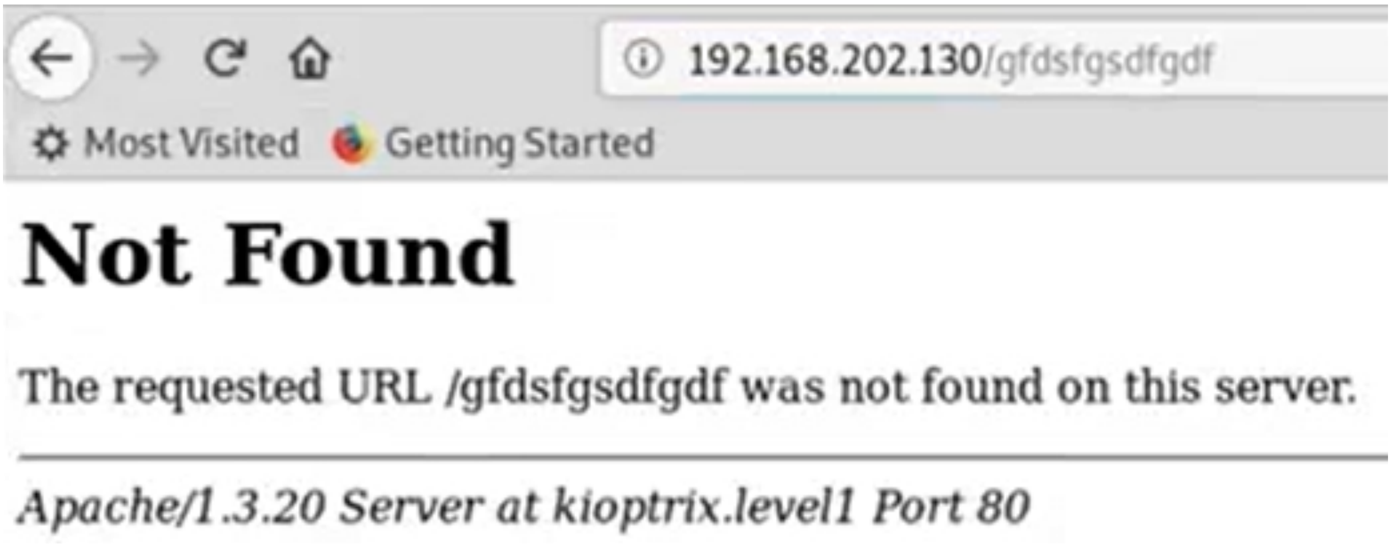
Monthly Statistics for February 2019		
Total Hits		29977
Total Files		261
Total Pages		16902
Total Visits		4
Total KBytes		9173
Total Unique Sites		1
Total Unique URLs		13
Total Unique Referrers		8
Total Unique User Agents		6945
	Avg	**Max**
Hits per Hour	416	15919
Hits per Day	9992	29925
Files per Day	87	240
Pages per Day	5634	16858
Visits per Day	1	2
KBytes per Day	3058	9137
Hits by Response Code		
Undefined response code		146
Code 200 - OK		261
Code 301 - Moved Permanently		1
Code 400 - Bad Request		7623
Code 403 - Forbidden		930
Code 404 - Not Found		20977
Code 405 - Method Not Allowed		19
Code 417 - Expectation Failed		3
Code 501 - Not Implemented		17

Server Header Info Disclosure (Low)



```
HTTP/1.1 200 OK
Date: Wed, 24 Apr 2019 22:18:37 GMT
Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Last-Modified: Thu, 06 Sep 2001 03:12:46 GMT
ETag: "8805-b4a-3b96e9ae"
Accept-Ranges: bytes
Content-Length: 2890
Connection: close
Content-Type: text/html
```

Default 404 info disclosure (Low)

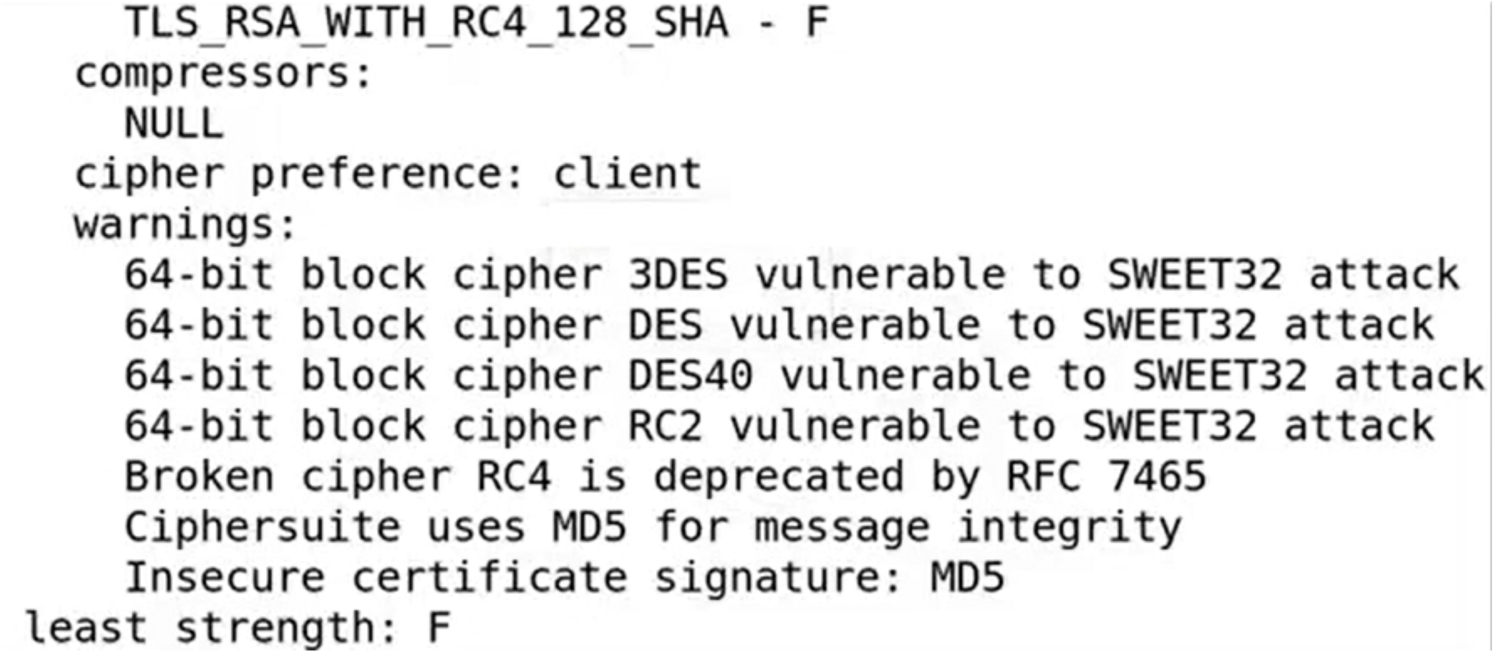


Not Found

The requested URL /gfdsfgsdfgdf was not found on this server.

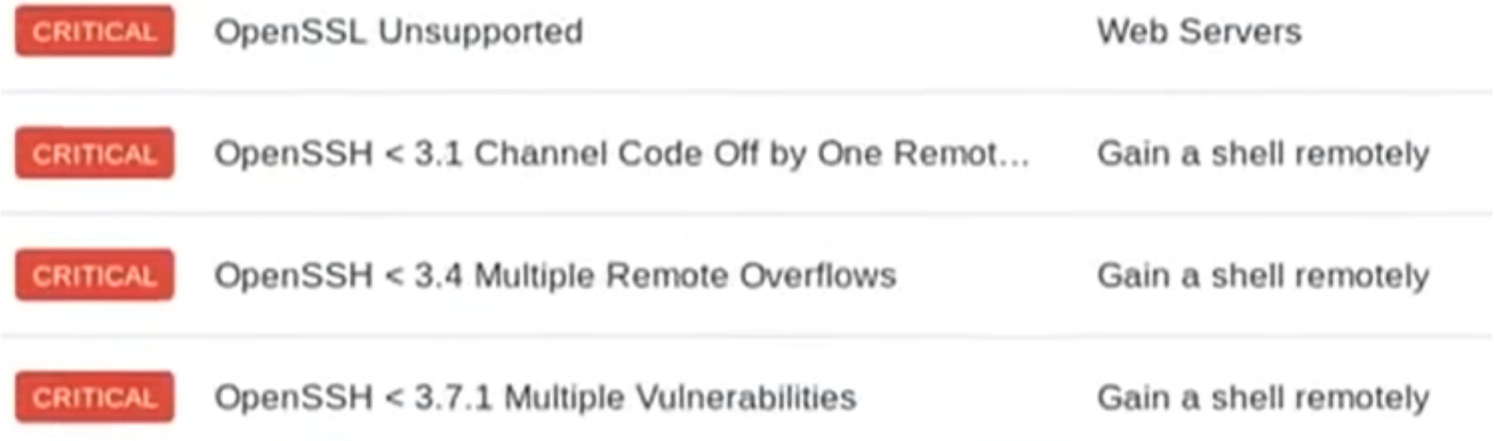
Apache/1.3.20 Server at kioptrix.level1 Port 80

Weak Ciphers



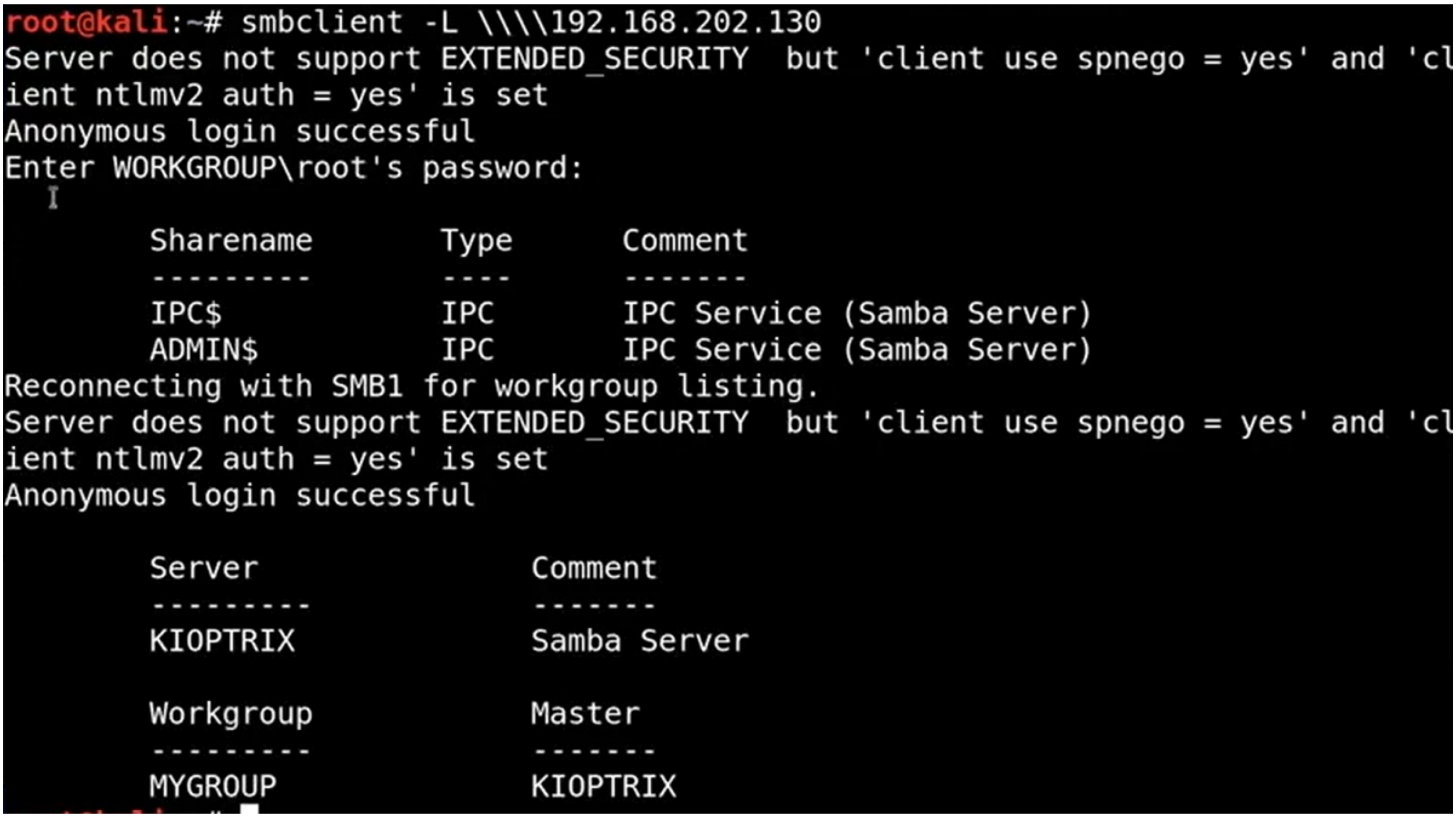
```
     TLS_RSA_WITH_RC4_128_SHA - F
   compressors:
     NULL
   cipher preference: client
   warnings:
     64-bit block cipher 3DES vulnerable to SWEET32 attack
     64-bit block cipher DES vulnerable to SWEET32 attack
     64-bit block cipher DES40 vulnerable to SWEET32 attack
     64-bit block cipher RC2 vulnerable to SWEET32 attack
     Broken cipher RC4 is deprecated by RFC 7465
     Ciphersuite uses MD5 for message integrity
     Insecure certificate signature: MD5
 least strength: F
```

OpenSSL/SSH (Critical)



CRITICAL	OpenSSL Unsupported	Web Servers
CRITICAL	OpenSSH < 3.1 Channel Code Off by One Remot...	Gain a shell remotely
CRITICAL	OpenSSH < 3.4 Multiple Remote Overflows	Gain a shell remotely
CRITICAL	OpenSSH < 3.7.1 Multiple Vulnerabilities	Gain a shell remotely

SMB (High)

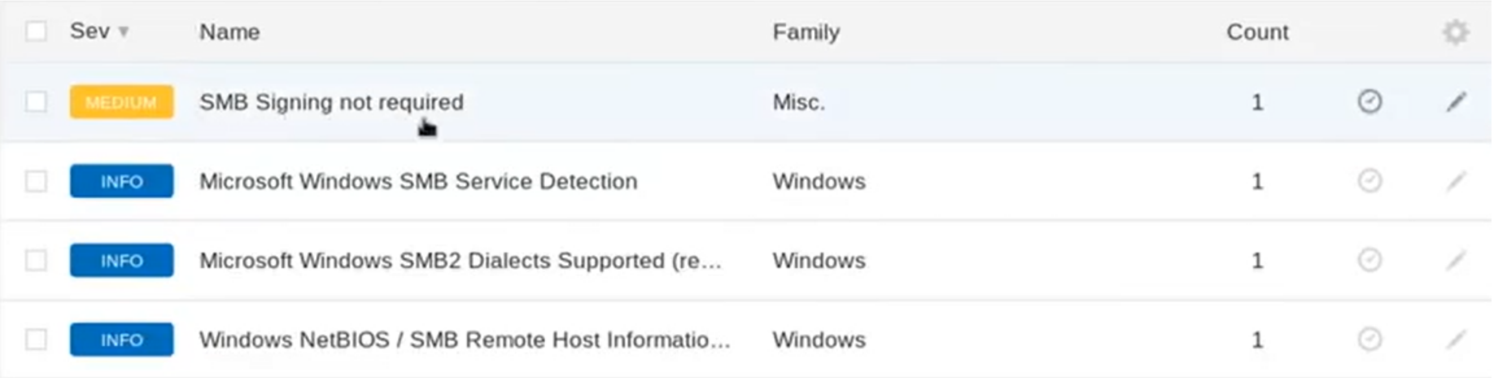


```
root@kali:~# smbclient -L \\\\192.168.202.130
Server does not support EXTENDED_SECURITY  but 'client use spnego = yes' and 'cl
ient ntlmv2 auth = yes' is set
Anonymous login successful
Enter WORKGROUP\root's password:

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       IPC Service (Samba Server)
        ADMIN$          IPC       IPC Service (Samba Server)
Reconnecting with SMB1 for workgroup listing.
Server does not support EXTENDED_SECURITY  but 'client use spnego = yes' and 'cl
ient ntlmv2 auth = yes' is set
Anonymous login successful

        Server               Comment
        ---------            -------
        KIOPTRIX             Samba Server

        Workgroup            Master
        ---------            -------
        MYGROUP              KIOPTRIX
```



□	Sev ▾	Name	Family	Count		
□	MEDIUM	SMB Signing not required	Misc.	1	✓	✎
□	INFO	Microsoft Windows SMB Service Detection	Windows	1	✓	✎
□	INFO	Microsoft Windows SMB2 Dialects Supported (re...	Windows	1	✓	✎
□	INFO	Windows NetBIOS / SMB Remote Host Informatio...	Windows	1	✓	✎